

User Guide

Arista Guardian for Network Identity AGNI

Version 2025.2.0



Arista.com

Arista Networks

DOC-06557-05-02

| 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 |
| | | |

© Copyright 2025 Arista Networks, Inc. All rights reserved. The information contained herein is subject to change without notice. The trademarks, logos, and service marks ("Marks") displayed in this documentation are the property of Arista Networks in the United States and other countries. Use of the Marks is subject to the Arista Networks Terms of Use Policy, available at www.arista.com/en/terms-of-use. Use of marks belonging to other parties is for informational purposes only.

Contents

| Chapter 1: AGNI Cloud Overview | 1 |
|---------------------------------------|---|
| 1.1 User Interface (UI) Theme | 1 |
| 1.2 Viewing Licensing Details | 2 |
| 1.3 Accessing the User Interface (UI) | 3 |

| 2.1.1 Configuring AGNI to Integrate EST Server | 5 |
|--|---|
| 2.2 Arista CV-CUE Integration | 7 |
| 2.3 Arista CloudVision Integration | 9 |
| 2.4 Configuring CVaaS Instances | |
| 2.5 Adding Multiple CVaaS Instances in AGNI | |
| 2.6 Arista NDR Integration | |
| 2.6.1 Configuring Arista NDR | |
| 2.6.2 Configuring Segment Policies | |
| 2.6.3 Using Risk Action in Segment Policies | |
| 5 5 | |

| 3.2 Palo Alto Firewall Integration | |
|---|----|
| 3.2.1 Configuring the Palo Alto Firewall/Panorama | 27 |
| 3.3 Medigate Integration | 29 |
| 3.4 Microsoft Intune Integration | |
| 3.5 Jamf Integration | 31 |
| 3.6 ServiceNow CMDB Integration | 32 |
| 3.7 Splunk Integration | 34 |
| 3.8 Sumo Logic Integration | 35 |
| 3.9 CrowdStrike Integration | |
| 3.10 Workspace ONE Integration | 37 |

| Chapter 4: Configuring Identity Providers (IDPs) | |
|--|--|
| 4.1 Microsoft Entra ID 365 (Azure) | |
| 4.2 OneLogin | |
| 4.3 Okta | |
| 4.4 Google Workspace | |
| 4.5 Local | |

| Chapter 5: Configuring the Networks | 51 |
|--|----|
| 5.1 Configuring Client Certificate Network | 51 |
| 5.1.1 Configuration Steps | 51 |
| 5.1.2 Authenticating Users with Email Codes (as against IDP) | 54 |
| 5.1.3 Wireless Configuration on Devices | 58 |
| 5.2 Configuring Unique PSK (UPSK) Network | 75 |
| 5.2.1 Configuring the UPSK Settings | |
| 5.2.2 Configuring the Device Count Limit for Authentication | 77 |

| 5.3 Configuring Wireless Captive Portal Network | 79 |
|---|----|
| 5.3.1 Configuration Steps. | |
| 5.4 Configuring Wireless MAC Authentication Network | |
| 5.4.1 Configuration Steps | |

| Chapter 6: Configuring Wired 802.1X Network | |
|--|--|
| 6.1 Configuration Steps | |
| 6.2 Configuring Wired MAC Authentication Network | |
| 6.2.1 Configuration Steps | |
| 6.3 Configuring Wired Captive Portal Network | |
| 6.3.1 Configuration Steps | |
| 6.4 Configuring Guest Portal Network | |
| 6.4.1 Configuring AGNI | |
| 6.4.2 Configuring EOS | |

| Chapter 7: Configuring Segmentation Policies | 100 |
|--|-----|
| 7.1 Status | |
| 7.2 Conditions | |
| 7.3 Actions | 100 |
| 7.4 Configuration | |
| 7.4.1 Sample Segments | 101 |

| Chapter 8: Configuring the Devices | |
|---------------------------------------|--|
| 8.1 Adding an Access Device | |
| 8.2 Importing Devices in Bulk to AGNI | |

| hapter 9: User Configurations | |
|-------------------------------|--|
| 9.1 Users | |
| 9.1.1 All Users | |
| 9.1.2 External Users | |
| 9.1.3 Local User | |
| 9.2 User Groups | |
| 9.2.1 Local User Groups | |

| Chapter 10: Client Configuration | 113 |
|--|-----|
| 10.1 Clients | |
| 10.2 Client Details | |
| 10.3 Creating Client Certificates Manually in AGNI | |
| 10.3 Creating Client Certificates Manually In AGNI | |

| Chapter 11: Guest Onboarding Features | 124 |
|---|-----|
| 11.1 Guest Onboarding Using AGNI | |
| 11.1.1 Guest User in AGNI | 124 |
| 11.2 Guest Onboarding Offerings in AGNI | 134 |
| 11.2.1 Portal Based Guest Onboarding | 134 |
| 11.2.2 Guestbook Based Onboarding. | 139 |
| 11.2.3 UPSK Based Guest Onboarding | |
| 11.3 Configuring UPSK for Onboarding Guest (Wireless) | 147 |
| 11.3.1 Configuring AGNI | 147 |
| 11.3.2 Configuring CV-CUE | |
| 11.3.3 Onboarding the User | 153 |

| 11.0.4 Onthe ordination the Quest User Using URQK (OR Code) | 100 |
|--|-----|
| 11.3.4 Onboarding the Guest User Using UPSK (QR Code) | |
| 11.3.5 Authenticating Guests via SMS Auth | |
| 11.4 Configuring Guest Portal Using Guestbook (Wireless) | |
| 11.4.1 Configuring the Portal on AGNI | |
| 11.4.2 Configuring the Network | |
| 11.4.3 Configuring CV-CUE | |
| 11.5 Configuring Guest Portal Using Guestbook-Host Approval (Wireless) | 173 |
| 11.5.1 Configurations on AGNI | 174 |
| 11.5.2 Configuring the Network | |
| 11.5.3 Configuring CV-CUE | |
| 11.5.4 User Onboarding | |
| 11.6 Configuring Guest Portal Using Self Registration (Wireless) | 181 |
| 11.6.1 Configuring the Portal on AGNI | |
| 11.6.2 Configuring the Network | |
| 11.6.3 Configuring CV-CUE | |
| 11.6.4 User Onboarding | |
| 11.7 Configuring Guest Portal in AGNI for Wired Clients | 187 |
| 11.7.1 Configuring AGNI | |
| 11.7.2 Configuring EOS | |
| 11.8 Configuring Guest Portal Using Guestbook (Wired) | |
| 11.9 Configuring Guest Portal Using Guestbook-Host Approval (Wired) | |
| 11.10 Configuring Guest Portal Using Self-Begistration (Wired) | 191 |
| | |

| Chapter 12: Generating Client Certificates for RadSec | .192 |
|---|------|
| 12.1 Viewing the Certificates | 195 |
| 12.2 Configuring Device Groups | 196 |

| Chapter 13: Overview - TACACS Plus with AGNI | 198 |
|--|-----|
| 13.1 Configuring Arista Cloud Gateway on Arista Switches | 198 |
| 13.2 Configuring Arista Cloud Gateway on AGNI | |
| 13.3 Configuring TACACS Plus on Arista Switches | 205 |
| 13.4 Debug commands on Arista Cloud Gateway | |
| 13.5 Enabling Device Administration on AGNI. | |
| 13.6 Configuring TACACS Plus on AGNI | |
| 13.7 Monitoring TACACS Plus on AGNI | 211 |
| 13.8 Accessing Self Service Portal on AGNI | |
| - | |

| Chapter 14: Configuring DHCP Containers | 219 |
|---|-----|
| 14.1 Installing Docker Container | |
| 14.2 Configuring Arista Switch for DHCP Messaging | |
| 14.3 Debugging Workflow | |
| | |

| Chapter 15: System | |
|---|-----|
| 15.1 Audit Viewer | |
| 15.2 License | |
| 15.3 Self-Service Portal Settings | 224 |
| 15.4 RadSec Settings | |
| 15.5 Support Logs | |
| 15.6 System Events | 231 |
| 15.7 Notification Settings | |
| 15.7.1 Configuring Email Settings on AGNI Cloud | 231 |
| 15.7.2 Configuring SMS Gateway | |

| Chapter 16: Sessions - AGNI Cloud | 238 |
|--|-----|
| 16.1 On-Demand Disconnecting a Client from the Network | |

| Chapter 17: Troubleshooting | |
|-----------------------------|--|
| 17.1 Monitoring | |
| 17.2 Dashboards | |
| 17.3 Sessions | |

| Appendix A: Appendix | |
|--|-----|
| A.1 OIDC Vs SAML | |
| A.2 Identity Providers | 247 |
| A.2.1 Microsoft Azure Active Directory | |
| A.2.2 Google Workspace | |
| A.2.3 OneLogin | |
| A.2.4 Okta | |
| A.2.5 URLs and Open Ports in Firewall | |

AGNI Cloud Overview

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.

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.

Log in as an administrator to access and configure the AGNI portal.

1.1 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).

| agni I | | | | | | | | | | | | | | | | | | | | | | | | Ğ | • @ | • |
|---|--------------|---------------------|------------------------|----------|-------|-------|-------|-------|-------|-------|-------------------------|-------------|-------|------------|-------|-------|-------|-------|----------|---------------------------|--------------|-----------|-------|----------|-------|-------|
| MONTOKING | 1 | | ashboar ny Analyti | rd 19 | | | | | | | | | | | | | | |) | bm19.ag | mi sje arist | anetworks | | Naviga | ition | - |
| Sessions Access contract Networks Is Segments Acces | | USERS Click here | 2 to view Us | ers. | | | | | | CLIEN | rts 4 here to vie | rw Clients. | | | | | | | ACCESS D | evices 10 to view A | ccess Dev | ces. | 19 | Color Sc | hemes | |
| S Identity Provider | | Session | s Trend | | | | | | | | | | | | | | | | | | | | | | | |
| ± User □ Client #" Cuest CONFIGURATION | 5 5 5 | | | | | | | | | | | | | | | | | | | \wedge | | | | | | |
| Access Devices | . *) | G 0.7 | | | | | | | | | | | | | | | | | | | | | | | | |
| Device Administration | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Gertificates | | 01.04 | 01.06 | 0106 | 01.06 | 01.06 | 0106 | 0106 | 01.06 | 6106 | 0106 | 01.05 | 0106 | 0106 | 01.06 | 01.07 | 0107 | 01.07 | 21.07 | 0107 | 0107 | 01/07 | 01.07 | 01.07 | 01.07 | 01.07 |
| System | | 10.30 | 11.30 | 12:30 | 13:30 | 14:30 | 15:00 | 16.00 | 17:30 | 18:30 | 19:30 | 20:30 | 21.30 | 22:30 | 29:00 | 00:00 | 01:00 | 02:30 | 00:00 | 04:30 | 05:30 | 06:30 | 07.30 | 06:30 | 09:30 | 10:30 |
| concounts | | | | | | | | | | | | | • 2 | a of aller | | | | | | | | | | | | |

1.2 Viewing Licensing Details

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

| Dashboard | | License License Details | |
|---|------|----------------------------|---------------------|
| Sessions | Lice | ense Details | |
| Networks | ту | rpe | Trial |
| Segments | Lic | cense count | 1000 |
| ACLS | Va | ulid until | 03/01/2026 01:14:57 |
| ☐ Client [¶] Guest CONFIGURATION | ~ | | |
| Access Devices | ~ | | |
| Device Administration | × | | |
| Certificates | ~ | | |
| | ~ | | |
| System | | | |
| System | | | |

Figure 1-2: AGNI License Details

1.3 Accessing the User Interface (UI)

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

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

Figure 1-3: Arista Launchpad

| RISTA | DASHBOARD ADMIN | | | | | | A (|
|---------------------------|---------------------|---------------------------|---------------|-----------|-----------|-------------|----------------|
| CV-CUT - Beca | cvw | CY-CUE (Cloud/Vision W/F) | Guest Manager | Packets | Carvas | Nano | Will Resources |
| Willi Device Registration | ev prod us-central1 | 8 AGNI - Beta | (B) AGNI | 8 AGNI | 8 AGNI | (B) ACNI | |

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



Figure 1-4: Arista Dashboard

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 AGNI EST Server Integration

The Enrolment over Secure Transport (EST) server is integrated with AGNI to process certificate enrolment requests that conform to RFC 7030. The EST server accepts Certificate Signing Requests (CSRs) from the client systems and securely returns the X.509 certificate as specified by the RFC.

To install and configure AGNI EST, perform the following steps.

- On the AGNI side:
- · Add Network Access Devices (NADs) or EOS switches to the AGNI network prior to client enrolment.
- Install the AGNI EST server through the Concourse App.
- · ON EOS Devices:

- Upgrade the software version to EOS 4.34.0F or later on the EOS devices to support auto-enrolment of client devices.
- Copy the AGNI Certificate Chain to the EOS devices.
- · Execute a few EOS commands as mentioned in the following sections.

For more details on EOS configurations, see the <u>Integration and Configuration of AGNI EST Server</u> document.

2.1.1 Configuring AGNI to Integrate EST Server

For integrating EST Server with AGNI, perform the following configurations:

- · Add or Import Network Access Devices (NADs) to AGNI
- Install the AGNI EST Server

2.1.1.1 Adding or Importing NADs to AGNI

To add or import the Network Access Devices (NADs) to AGNI:

 On the AGNI portal, navigate to Configuration > Access Devices > Devices: Figure 2-2: Access Devices List

| agni i myorg1.o | om | | | | | | | | | G | 0 | • |
|---|----|---|-------|---|------------------------------|---------------|-------------------------------|---------------|---------------------|--------------|----------|-------|
| MONITORNO | | | Ac | ccess Devices t of Access Devices allowed for RadDec | connections as on 02/05/2025 | 12:57:57 | | | | + Add or Imp | port Der | vices |
| ACCESS CONTROL | | | | | | | | | | c | C | |
| Vetworks | | ٩ | Searc | n by Name, MAC Address, IP Address or s | acation | | | | All Device | 6 | | • |
| ACLs | | | | NAME | MAC ADDRESS | VENDOR | LOCATION | RADSEC STATUS | UPDATE TIME | | | |
| DENTITY | | | 1 | PE1-gzd500 | 38-38 a6 a5 9c ac | Arista Switch | | • | 29/04/2025 15:17:54 | | 1 | |
| Identity Provider | | | 2 | KK_Arista_AS-88:27 | 30.86.2d.a5.8b.2f | Aduta WVFI | */india/Bengaluru/Marathahali | 0 | 24/04/2025 14:38:47 | | 1 | |
| Client | 2 | | 3 | Hasan_Arista_C230_6E A0: | 30.86.2d.6e.a0.8f | Ansta WFI | | | 24/04/2025 12:41:20 | | 1 | |
| # Guest | Q. | | 4 | EOS-Switch-2 | 28:e7.1d ca.0e.11 | Arista Switch | | ۰ | 14/04/2025 17:20:16 | | 1 | 8 |
| CONFIGURATION | ~ | | 5 | E05-Switch-1 | ac:3d:94×8:27.9c | Arista Switch | | 0 | 09/04/2025 04:51:51 | | 1 | 0 |
| E Devices | 1 | | 6 | Arista W318 | e4:d1:24:10:0c:5f | Arista WPI | | • | 03/04/2025 03:39:07 | | 1 | 8 |
| Device Groups Cloud Gateways | | | 7 | KK_Aruba_20:4C:03:42:20 | 20-40 03-42-20-60 | Anuba | | | 24/09/2024 19:49:21 | | 1 | 8 |
| Device Administration | * | | | | | | | | | | | |
| G Certificates | ~ | | | | | | | | | | | |
| System | ۲ | | | | | | | | | | | |
| III Explore | | | | | | | | | | | | |
| IF Installed Apps | | | | | | | | | | | | |

- 2. Click the +Add or Import Devices button. Select Add Device or Import action.
 - a. Select the Access Device Group.
 - **b.** Upload the devices list CSV file.

c. Click the Import button.

Figure 2-3: Importing Access Devices

| Dashboard | 6 | Add or Import Access Devices Provide details to add a new device or import devices from a file | Get Base |
|--|-----|---|--------------|
| Sessions | c | Choose Action: O Add Device Import | |
| Networks Segments | | Access Device Group Test-Device-Group | × ~ 🕀 |
| ACLS | | Optional Upload CSV file Browse | |
| Identity Provider | ~ c | columns: name*, mac*, vendor*, ipAddress, serialNumber, location | Sample |
| Client Guest | * | | Cancel Impor |
| ONFIGURATION | ~ | | uncer mpe |
| Access Devices | - | | |

2.1.1.2 Installing the AGNI EST Server

To install the AGNI EST server:

1. Navigate to Concourse > Explore and click the AGNI EST Server tile to install.

Figure 2-4: Concourse Tile

| Inchertorikwo III Dashboard | | Concourse Explore Appe | | | | | | |
|---|--------|---------------------------------------|---|---|-----------|--|--|---|
| Sessions Access control. Networks | | Q. Search by forms, | | | | | Canageri Any | • |
| ACLS | | agni | | agni | | | | |
| Identity Provider User Client Client | × | AGNI EST Server Network Management | | AGNI Event Notification Network Access Control | Installed | Arista CV-CUE Network Management | Arista CloudVision Network Management | |
| Client Groups | a l | | | 0 | | | jamf | |
| Access Devices Devices Device Groups Cious Gateways | * | Arista NDR Englasini Indection | | Cortex XDR Endpoint Protection | t Putaled | CrowdStrike Endpoint Protection | Jant Device Munispeniert | |
| Device Administration C Access Policy TACACS+ Profiles | * | 83 | | Ŧ | | 111 paloeto | | |
| Certificates System | ж Ж | Medigate Endpoint Protection | 1 | Microsoft Intune Device Management | (value) | PAN Firewall Network Access Control | ServiceNow CMDB Device Management | * |
| Explore | - 1 | | | 0 | | | | _ |
| 🕅 Installed Apps | | splank > | | s u mo | | Contract (Me | (47)))) | |
| | | Splunk SEM | | Sumo Logic SEM | | Workspace ONE Device Management | eduroam Network Access Control | |
| | | | | | | | | |

- **2.** Enter the following details:
 - a. The Name field is auto-populated to AGNI EST Server.

- b. Add the Client Certificate Validity (in days) and click the Install button.
- c. Generate the API Token



Note: The token is displayed only once when the token is generated; copy and save the token for later usage.

- d. Download the Certificate Chain.
- e. Save the following EST server details (needed for configuration on the EOS side):
 - EST URL
 - · EST (API) Token
 - AGNI Certificate Chain

Figure 2-5: EST Server - Generating Token

| ONITORING | _ | AGNI EST Server | | (n |
|-----------------------|---|---|--------|-----------|
| Dashboard | | Enter the following fields to update the selected app. | | € ва |
| Sessions | | | | |
| CESS CONTROL | | AGN/EST Server | | |
| Networks | | | | |
| Segments | | Client Certificate Validity (days) | | |
| ACLs | | | | |
| INTITY | | Max validity is 1095 days. | | |
| Identity Provider | | ① This app provides EST service to securely provision RadSec client certificates for network devices. | | |
| User | ~ | | | |
| Client | ~ | | Cancel | Update |
| Guest | ~ | | | |
| FIGURATION | | EST server details | | |
| Access Devices | ~ | | | |
| Device Administration | ~ | Use the following EST URL to enroll your devices. | | |
| Certificates | ~ | ESTUR | | |
| System | ~ | https://qa.agnieng.net/pki/E8820a6a4-4c19-4ea6-a1e7-18b0655e5567 | Сору | |
| NCOURSE | | | | |
| Explore | | For security reasons, API token is shown only once. Use the following token henceforth. | | |
| Installed Apps | | EST Token | | |
| | | ••••••••••••••••••••••••••••••••••••••• | Copy | |
| | | O To trust the AGNI Server, download the HTTPS Server Certificate chain and install them in the network device. | | |
| | | Download Certificate Chain | | |
| | | Application Logs | | Show Logs |
| | | | | _ |
| ≪ Collapse Sidebar | | | | ← Bac |

2.2 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 2-6: Verify CV-CUE Application

| agni I | | | | | |
|--|-----|---|--------|--------|---------|
| MONITORINO | | Arista CV-CUE Enter the following fields to update the selected app. | | | (+ Back |
| ACCESS CONTROL | - [| html Arists 0/2 CUE 0/2 078/070 | | | |
| ACLs IDENTITY ACLs Identity Provider | - (| кт талпоказе пист Огод ну Wei | | | |
| LUser | . [| Landgas KNVK. https://aundrpad.wih.ansta.com/api/v2 | | | |
| | ÷ | | Cancel | Verify | Update |

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

Figure 2-7: Installing CV-CUE Application

| agni I Achi-d | imo | | | | استىتىتىتى يىتىتى | | G. | 0 💽 |
|---|-----|---|--------|--------|-------------------|------|----|-----|
| Monaroana S Dashboard A Seasions | 4 | Arista CV-CUE Error the following fields to configure the app. | | | + Back | | | |
| Notiverks Notiverks Segments ACLs Dentity Mentity Provider L User | | Anisi Shi Cuili Vi Vi Vi Vi U Xi Yi AMAGIYAYE 2433 Vi Vi Vi Vi Vi Vi Vi Vi Vi Vi Vi Vi Vi V | | | 0 | | | |
| Chent M Guest | ž | | Cancel | Verify | instal | | | |
| Access Devices Cercip Administration Cercipicates System Concounts | | | | | | | | |
| III Kaplore | | | | | | | | |

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 2-8: Synchronizing CV-CUE App

| MONETORNIO SE Dashboard Sessions ACCESS CONTROL Networks 414: Segments S ACLS | Arista CV-CUE Enter the following fields to update the selected app. | (* Bod |
|---|--|---|
| DDMTY 3) Identity Provider 4) User ~ Client ~ R) Guest ~ Controlutation ~ | Invertigat XPT UR. Interpret XPT UR. https://faunchoped.wifi.arista.com/api/v2 Synchronization Details | Cancel Verify Upduite |
| □ Device Administration ∨ □ Certificates ∨ □ System ∨ concountst □ Explore □ Installed Apps | Location and Access Device information will be synced from CV-CUE. Last Successful Sync At Last Sync At Sync Status | 16/07/2023 10:30:03 07/01/2025 11:30:04 (Partist Soccess) Sync Now |
| | Application Logs | Show Logs |

You can view the synchronized Access Points by navigating to:

Configuration > Access Devices > Devices (see image).

| Figure 2-9: | Synchronized | Access | Points |
|-------------|--------------|--------|---------------|
|-------------|--------------|--------|---------------|

| agni I | | | | | | | | | ५ ७ 🙆 |
|--------------------------|---|---|---------------------------|--------------------------------|---------------------------|-------------|-----------------------------|---------------------|-------|
| MONITORING | | | Access Devices | lowed for RadSec connections a | is on 07/01/2025 12:43:14 | | | | |
| CESS CONTROL | | | | | | | | | 8 |
| Networks #1= Segments | | ٩ | Search by Name, MAC Addre | ss, IP Address or Location | | | | Arista WiFi | • |
| ACLs | | | NAME | IP ADDRESS / SUBNET | MAC ADDRESS | VENDOR | LOCATION | UPDATE TIME | |
| IDENTITY | | 1 | Arista_CA:9A:OF | 10.81.204.94 | 30-86-2d ca 9a-0f | Arista WiFi | */North America/Bassett Lab | 07/01/2025 05:22:38 | ø |
| (2) Identity Provider | | 2 | Arista_B1:D0:3F | | 30:86-2d:b1:d0:3f | Arista WFi | */Boston/Boston-CustomCert | 03/01/2025 03:14:34 | ø |
| Client | ~ | 3 | Atul-C200 | 192.168.0.163 | 30-86-2d-92-bd-9f | Arista WFi | */North America/Boston | 03/01/2025 03:14:34 | Ø |
| 们 Guest | × | 4 | Arista-C200-9155df | 172.21.1.58 | 30:86-2d:91:55:df | Arista WiFi | */North America/Bassett Lab | 03/01/2025 03:14:34 | Ø |
| Access Devices | ^ | | | | | | | | |
| Devices | | | | | | | | | |
| Device Groups | | | | | | | | | |

2.3 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 2-10: Installing Arista CloudVision Concourse Application

| MONITORING | | Arista CloudVision Enter the following fields to update the selected app. | ← Back |
|-----------------------|---|--|----------------------|
| CONTROL | | Con | |
| Networks | | Arista CloudVision | |
| I Segments | | https://www.arista.io/ | |
| IDENTITY | | | |
| L User | ¥ | To add secondary CloudVision Servers, click here | |
| Client | ~ | | |
| Guest | ~ | Secondary Servers | |
| Access Devices | ^ | Secondary Server https://www.arista.lo | / 0 |
| Devices | | second | 2.5 |
| Cloud Gateways | | https://www.arista.jo/ | |
| Device Administration | ~ | | Cancel Verify Update |
| Certificates | | | |
| System | 4 | Synchronization Details | |

- 4. Click the Verify button to validate the credentials.
- 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).

2.4 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).

| NITORINO | Arista CloudVision | € B |
|-------------------------|--|---|
| Dashboard | Enter the following rests to quarte the selected app. | 13 |
| Sessions | Line - | |
| Networks | -Arista Clovavision | |
| Segments | 10L | |
| ACIs | (https://www.ansta.io) | |
| NUTY | 7000 | |
| Identity Provider | | |
| User | | |
| Client | 10 and secondary Cloudvision Servers, click here | |
| Guest | Secondary Servers | |
| NEIGURATION | Secondary Server | 1. C. |
| Access Devices | https://www.arista.io | / 1 |
| - | | |
| C Buildes | second https://www.arista.io/ | / 6 |
| Device Groups | | |
| Cloud Gateways | | Cancel Verify Update |
| Device Administration ~ | | |
| Certificates ~ | Synchronization Details | |
| System ~ | | |
| COURSE | Access Device information will be synced from Arista CloudVision | |
| Explore | | |
| Installed Apps | Last Successful Sync At | 31/03/2024 08:30 |
| | Last Sync At | 07/01/2025 12:30 |
| | Syne Status | Partial Succe |
| | Consultation . | Called to sure from course bilits Claudifician Considera Ca |
| | Mescaption | Pailed to sync from servers Ansta Cloud vision, Secondary Ser |
| | | Sync Now |
| | Application Logs | ShowLo |

Figure 2-11: Adding Secondary Servers (CVaaS Instances)

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

Figure 2-12: Adding Secondary Servers

| Add Cloud | Vision Server | aud Vision Conver | 2 |
|-----------------------|--------------------------------|-------------------|---|
| Provide the fo | llowing details to add a new C | oudvision Server | |
| Name | | | |
| CV/ toot doo | | | |
| CV-lest-doc | | | |
| LIDI | | | |
| ORL - | | | |
| https://www.arista-te | estlab.io/ | | |
| https://www.arista-to | estlab.io/ | | |
| https://www.arista-to | estlab.io/ | | |
| https://www.arista-to | estlab.io/ | | Ø |
| https://www.arista-to | estlab.io/ | | 0 |
| https://www.arista-to | estlab.io/ | | 0 |

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 2-13: CVaaS Synchronization

| Dashboard | Arista CloudVision Enter the following fields to update the selected app. | ← Bac | | | | | | | |
|------------------------------|---|---|--|--|--|--|--|--|--|
| Sessions | Secondary Server https://www.arista.io | / 0 | | | | | | | |
| Networks Segments ACLs | second https://www.arista.io/ | / 0 | | | | | | | |
| DENTITY | | Cancel Verify Update | | | | | | | |
| L User v | Synchronization Details | | | | | | | | |
| P Guest ~ | Access Device information will be synced from Arista CloudVision | | | | | | | | |
| Access Devices | Last Successful Sync At 31/03 | | | | | | | | |
| Devices Device Groups | Last Sync At | | | | | | | | |
| Cloud Gateways | Sync Status Description Failed to sync | From servers Arista CloudVision. Secondary Server | | | | | | | |
| Device Administration | Y ₁ | Sync Now | | | | | | | |
| System | Application Logs | ShowLogs | | | | | | | |
| Explore Installed Apps | Local * (Smith Debug *) (Smither Sm | * Beset Befresh | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

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.

| agni I | | | | | | | | | | G | 0 | M |
|---|----------|---|-------|---|-------------------------|----------------------|---------------------------------|---------------|-----------------|-------------------------|----------|-------|
| | | | Ac | ccess Devices t of Access Devices allo | wed for RadSec connecti | ons as on 07/01/2025 | 15:39:00 | | 1 | + Add or Im | 1port De | vices |
| | | | | | | | | | | | • | 3 88 |
| Networks 11 Segments | | ٩ | Searc | in by Name, MAC Address | IP Address or Location | | | | | lendor Arista Switch | | * |
| ACLS | | | | NAME | MAC ADDRESS | VENDOR | LOCATION | RADSEC STATUS | UPDATE TIME | | | |
| IDENTITY | | 0 | 1 | arista-710P | 2c:dd:e9.ff:39:d4 | Arista Switch | second/Tenant/San Jose | 0 | 01/11/2024 11:3 | 0:01 | 1 | 0 |
| Identity Provider User | <u>,</u> | | 2 | agni-720xp-24-1 | c0:d6:82:16:3f:59 | Arista Switch | second/Tenant/Bassett | 0 | 01/11/2024 11:3 | 0:01 | 1 | 0 |
| Client | ~ | | 3 | agni-720dp-24-1 | 28:e7:1d:ca:0e:f1 | Arista Switch | second/Tenant/Bassett | 0 | 01/11/2024 11:3 | 0:01 | 1 | 0 |
| 19 Guest | ~ | | 4 | at-arista720dp | 28:e7:1d:ca:0f:4b | Arista Switch | second/Tenant/AGNI_HQ | | 01/11/2024 11:3 | 0:01 | 1 | 0 |
| Access Devices | | | 5 | agni-722xpm-48 | ac:3d:94:c8:27:9c | Arista Switch | second/Tenant/AGNI_HQ | | 01/11/2024 11:3 | 0:01 | 1 | 0 |
| Devices | | | 6 | CV-CUE-12P-1 | 2c:dd:e9:fe:0f:ea | Arista Switch | second/Tenant/Undefined | • | 01/11/2024 11:3 | 0:01 | 1 | 0 |
| Device Groups | | | 7 | agni-720dp48-1 | 2c:dd:e9:ff:d4:a5 | Arista Switch | Secondary Server/Tenant/Bassett | 0 | 31/03/2024 08 | 30:00 | 1 | 0 |
| Cloud Gateways | | | 8 | Arista Switch | | Arista Switch | | 0 | 29/01/2024 11:1 |)4:49 | 1 | |

| Figure | 2-14: | 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 2-15: Arista NDR Integration

| MONITORING | | Arista NDR | A Rook |
|-------------------|---|---|-----------|
| Dashboard | | Fill in the following fields to configure the app | - Dack |
| ✓ Sessions | | Nona | |
| ACCESS CONTROL | | Arista NDR | |
| Vetworks | | | |
| ≟l≟ Segments | | (i) This app provides updates from Arista NDR about clients' behaviour to AGNI. | |
| ACLs | | | |
| IDENTITY | | Profile Synchronization: Disabled | |
| Identity Provider | | | |
| Luser | ~ | Enable to fetch profile information for clients from Arista NDR. | |
| 🛄 Client | ~ | | |
| 📌 Guest | ~ | Cancel Verif | y Install |

- 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 2-16: Arista NDR Integration API Details

Ę

| | | Arista NDR | | |
|--|---|---|------|-----------|
| Dashboard | | Fill in the following fields to update the selected app | | ← Bac |
| Sessions Sessions CESS CONTROL Networks Segments ACLs DENTITY Identity Provider User | v | Arista NDR This app provides updates from Arista NDR about clients' behaviour to AGNI. Profile Synchronization: Disabled The Disable of the profile information for clients from Arista NDR. | | |
| Client Guest | ~ | Notification API details | | |
| Access Devices Device Administration | * | Use the following API URL in Arista NDR configuration to push updates to AGNI. API URL https://systest.agnieng.net/api/concourse.app.aristaNDR.notification | Сору | |
| Certificates System ONCOURSE | ~ | No API token is present. | | |
| Explore Installed Apps | | Generate Token | | |
| | | Application Logs | | Show Logs |

| MONITORING | Arista NDR Fill in the following fields to update the selected app |
|---|---|
| Sessions ACCESS CONTROL Networks LA Segments ACLs IDENTITY Identity Provider | Arista NDR This app provides updates from Arista NDR about clients' behaviour to AGNI. Profile Synchronization: Disabled Enable to fetch profile information for clients from Arista NDR. |
| Client Client Configuration | Notification API details |
| Certificates System | API URL API URL Apt URL A |
| CONCOURSE Explore Installed Apps | |

Figure 2-17: 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).

| | E AM | /L query | Run 🕜 🕸 | 8 |
|----|---------------------------------|-------------|------------------------------|------|
| | 0 models s | elected 🖉 🗘 | Users Roles | eate |
| T. | Last Modified 🗑 | User | Action Rules Policy Lists | 旗 |
| | 13:06:13 Aug 01, 2023 | 🗭 Ava | Connected Services | |
| | 01:08:45 Jun 09, 2023 | 🗭 Ava | Integrations | |

Figure 2-18: Arista NDR Settings Page

Click on the Add Service option to add a new connected service in NDR (see image below).
 Figure 2-19: Arista NDR Configuration - Add Service

| ۹ 🔤 | A | | | | | D And, sperg | Ren. | 00 |
|------|----------------|-------|---------------------------|---|------------|--------------|------|-------------|
| Conr | ected Services | | | | | | ۷ ۵ | + All Since |
| | Nama 1 | Pracy | en. | | Crodentals | | | 7.0 |
| | | - | https://ga.agnieng.httlap | • | Header | | | |
| | | | | | | | | |

3. Add the AGNI API URL and API Token generated previously in the AGNI Integration section. Figure 2-20: Arista NDR Configuration Details

| Edit Service | |
|------------------------|---|
| * Name | |
| agni | |
| * URL | |
| https://qa.agnieng.net | t/api |
| * Header Name | |
| Authorization | |
| * Header Value | |
| Bearer eyJhbGciOiJFU | JzI1NiIsInR5cCl6lkpXVCJ9.eyJvcmdJRCl6lkU0NWZIZWNmMi040GNhLT |
| Proxy | |
| Discard Changes | Save |

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

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

Figure 2-21: Arista NDR Configuration Artifacts Details

| 습 | Home | | Artifacts / Polycom_Boardroom01a | |
|---|-------------------|---|--|--------------------------------------|
| 1 | Investigations | ^ | < Polycom_Boardroom01a | EntityIQ [™] Device Profile |
| | Situations | | Internal Type | |
| | Artifacts | | Polycom SoundPoint IP 550 | |
| | Feature Summaries | | os ? Unknown 💌 Unknown 💌 | |
| | IOC Matches | | Hierarchy | |
| | Model Matches | | Generic/Polycom SoundPoint IP 550 💌 | |
| | Advanced AML | | First Seen Nov 09, 2023 01:15:07(-3w 11h) | |
| Ø | Dashboards | * | Last Active Nov 30, 2023 11:52:11(-39m 33.833s) | |
| 6 | Manage Detections | * | IPs (recent) 10.201.110.34 | |
| | | | MAC Address 64:16:7f:30:00:92 | |

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 2-22: 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.

| agni I | | | | | | | | | | | G | 0 м | | | |
|--------------------------|---|------|--------|----------------------------|----------------------------------|-------------------|------------|--------------------|-------------------|-------------------------|---------|-------|-------------------------|--|---|
| MONITORINO | | ~ | Se | ssions t of Sessions as | on 27/06/2024 22:58:26 | | | | | | | | | | |
| M Sessions | 1 | Netw | rork A | cess Devi | ce Administration | | | | | | (| C 🔳 👪 | | | |
| Networks | | ٩ | Searc | h by Identity, MAI | C Address, IP Address or Session | 10 . | | | (MAC | Authentication * | | • | | | |
| II Segments | | | | | | | | | | | | | | | |
| ACLs | | ^ | | IDENTITY | TYPE | MAC ADDRESS | IP ADDRESS | STATUS | | TIMESTAMP | | | | | |
| IDENTITY | | ~ | т | Laptops | MAC Authentication | 38:ca:84:b4:d5:0b | | Success | | 26/06/2024 06:37:49.810 | | 0 | | | |
| (2) Identity Provider | | | | | | | | | | | | | | | |
| 🚨 User | * | × | 2 | Laptops | MAC Authentication | 38:ca:84:b4:d5:0b | | Success | 0 | 26/06/2024 05:37:49.540 | | 0 | | | |
| Client | v | ~ | 3 | Laptops | MAC Authentication | 38:ca:84:b4:d5:0b | | Success | • | 26/06/2024 04:37:49.267 | | 0 | | | |
| 行 Guest CONFIGURATION | | | | | ~ | 4 | Laptops | MAC Authentication | 38:ca:84:b4:d5:0b | 1:b4:d5:0b | Success | 0 | 26/06/2024 03:37:48.997 | | ۲ |
| Access Devices | * | ~ | 5 | Laptops | MAC Authentication | 38:ca:84:b4:d5:0b | | Success | | 26/06/2024 02:37:48.725 | | 0 | | | |
| Certificates | Ŷ | ~ | 6 | Laptops | MAC Authentication | 38:ca:84:b4:d5:0b | | Success | • | 26/06/2024 01:37:48.455 | | 0 | | | |
| System | • | ~ | 7 | Laptops | MAC Authentication | 38:ca:84:b4:d5:0b | | Success | • | 26/06/2024 00:37:48.183 | | • | | | |
| CONCOURSE III Explore | | ~ | 8 | Laptops | MAC Authentication | 38:ca:84:b4:d5:0b | | Success | • | 25/06/2024 23:37:47.912 | | 0 | | | |
| ID Installed Apps | | * | 9 | Laptops | MAC Authentication | 38:ca:84:b4:d5:0b | | Success | • | 25/06/2024 22:37:47.630 | | ۲ | | | |
| | | ~ | 10 | Laptops | MAC Authentication | 38:ca:84:b4:d5:0b | | Success | • | 25/06/2024 21:37:47.358 | | o | | | |

Figure 2-23: Sessions Details

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

Figure 2-24: Sessions Client Details

| MONITORING | | Session Details - Rcptmjpdtlc4c72slant0 | | | | |
|---|--------|---|------------------------------------|----------------------------|-----------------------|----|
| CCESS CONTROL | | Authentication Request | Success | Session Details | Clos | Ы |
| Vetworks | | Authentication Type | MAC Authentication | Client IP Address | | • |
| L Segments | | Segment | Default | Session Start Time | 26/06/2024 06:37:49.8 | 10 |
| DENTITY | | Location | Pune/ABZ | Session Stop Time | 26/06/2024 06:47:36.0 | 16 |
| Identity Provider User | v | L User | Client | Enabled | Actions | |
| Client Client Consideration | • • | Not available | 38:ca:84:b4:d5:0b WindowsLaptop | | Allow Access | |
| Device Administration Certificates | * * | Access Device Arista Switch | Network | Enabled | | |
| System | × | fc.bd.67:0e;f8:f5 PLM-Switch01-10.87:33.41 | MAC-AUTH Wired | | | |
| III Explore | | PLM-Switches | MAC Authentication | | | |
| | | Input Request Attributes | ~ | Output Response Attributes | | |

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

Figure 2-25: NDR Client Details

| agni I | | | | | | ତ ଡ 💌 |
|-----------------------|---|-------------------|--|---|---|-------------------------------|
| MONITORINO | | Clie View | ent Details - WindowsLapt client details and update the selec | ted client | | ← Back |
| ACCESS CONTROL | | 38;ca;84:b | 4.85.05 | | Client Details | |
| Vetworks | | Description | | | Device Type | Hardware Manufacturer:HP Inc. |
| ala Segments | | WindowsLa | aptop | | Machine Authenticated | No |
| O ACLS | | Client Group | | | Added At | 11/01/2024 17:54:27 |
| Identity Provider | | Laptops | | Updated At | 11/01/2024 17:54:27 | |
| 1 User | ~ | Status: E | nabled | | All and Filmen and a | |
| Client | × | Client Attributes | | × | | |
| 名 Guest | * | | | ference and the second s | | |
| CONFIGURATION | ~ | Arista ND | R-] | × | Last Session Details | Closed |
| Access Devices | | ~ | | Device Brand | | IP Address |
| Device Administration | × | | Device Hierarchy | P. Add Attribute | Location | Pune/ABZ |
| 🖶 Certificates | v | | Device Type | | | 2200 |
| System | ~ | | Risk Action | Cancel Update Client | Segment | Default |
| CONCOURSE | | | | | Authentication Status | Success |
| III Explore | | Netwo | ark | MAC Authentication | Access Device | Arista Switch |
| | | MAC-AUTH Wired | | | fc.bd:67:0e:18:15 PLM-Switch01-10.87:33:41 | |
| | | Sessions for | r this client | | | Show Sessions |

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 2-26: Add Segment Details

| agni I | | | | | ତ ଡ 💌 |
|--|--------|---|--------------------------------------|----------------------------------|--------------------|
| MONITORINO | | Segments Segmentation Policies | | | |
| Sessions ACCESS CONTROL Setworks | | Q Search by segment name or description | Add Segment Provide the following | ng details to add a new segment | le × |
| ±l± Segments | 1 | | Name | | |
| ACLS | | P ₆ Add Segment | Description AGNI NDR | | |
| L User | ~ | ✓ Default | Status: Enabled | | Disable Monitor |
| ☆ Guest | 0 | | Conditions MAT | CHES ALL | |
| CONFIGURATION | | | Client: Arista N | DR: | × |
| Access Devices Device Administration | ÷ | | | Device Brand Device Hierarchy | P+ Add Condition |
| Certificates System | v v | | Actions | Device Type Risk Action | |
| | | | | | P+ Add Action |
| Installed Apps | | | | | Cancel Add Segment |

2.6.3 Using Risk Action in Segment Policies

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

| agni I | | େ ୭ |
|---|--|--|
| MONITORING | Segments Segmentation Policies | |
| Sessions ACCESS CONTROL P Networks | Q. Search by segment name or description | Add Segment Provide the following details to add a new segment |
| +l+ Segments | ₩. Add Segment | NDR Decore |
| Identity Provider User Client | v Default | AGNI NDR Status: Enabled Disable Monitor |
| f [®] Guest CONFIGURATION | ~ | Conditions MATCHES ALL Client: Arista NDR:Risk Action is quarantine X |
| Device Administration Certificates | * | P+ Add Condition |
| System Concourse Explore Vinstalled Apps | · | Actions Assign VLAN Assign VLAN through RADIUS response × VLAN Quantine VLAN |
| | | #+ Add Action |
| | | Cancel Add Segmen |

Figure 2-27: 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 dequarantine 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 2-28: Update Client Details for Risk

| agni I | | | | ତ ତ 🕛 |
|-----------------------------|---|--|------------------------------------|------------------------------------|
| MONITORINO | | Polycom_Boardroom01a - Polycom SoundPoint IP Vex client details and update the selected client | | (+ Beck |
| Sessions access contract | | 64 10 71 20 00 M2 | Client Details Device Type | Generic Polycom SoundPort # 550 |
| Wetworks | | Constant Polycom_Boardtoom01a - Polycom SoundPoint IP 550 | Machine Authenticated | No |
| Ø ACLS | | Contras Home-201 | + Added At | 04/07/2024 04:27:43 |
| (1) Identity Provider | | | Updated Ar | 08(07/3024 01 15 16 |
| Client | • | Statu Ended w | Client Fingerprint | |
| Clients | | Client Attributes | Last Session Details | Open |
| Control and | * | Arista NDR, Device Herarchy a Generic/Polycom SourcePoly | X Location | Aviata Cloud Vision/Tenant/AGNL_HQ |
| Access Devices | | Arista NDR Device Type = Polycom SoundPoint IP 500 | X Segners | NDR-Polycom |
| C. Access Policy | | P. Add Anniput | Authentication Status | Success |
| Certificates | • | Cancel Update C | Sent | |
| CONCOURSE Explore | | Vetwork Client Cart | Cale Access Device | Avida Switch |
| 📴 Installed Apps | | AT-species-EAP Wired | ac3d94.c8.27.9c agni-722.cpm-48 | |
| | | Sensions for this client | | Show Services |
| | | Client Activity | | Shee Activity |

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

| ogni I | | 6 O O |
|--|--|-----------|
| I Suntane S | Eventer XDH Printer KDH Friendelle Frieder KDH Frieder KDH Frieder KDH Frieder KDH Frieder KDH Frieder KDH Frieder KDH Frieder KDH Frieder KDH Frieder Konnege Konnege Konnege Frieder Konnege Konnege Konnege Konnege Frieder Konnege K | |
| X teach, barder A tear | AND Along | |
| Annes Antonio v Derica Alexandrature v Gardiagean v Aprene v | The approximation of a stating to extract the specificant states for shares provided by Sortex CR. | |
| E fajore | | |

- 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 Palo Alto Firewall Integration

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

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

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

Benefits:

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

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

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

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

Pre-requisites:

 AGNI must have reachability access to the Palo Alto firewall or Panorama endpoints over port 443. However, this may not happen in some scenarios, as the firewall entities may not have inbound internet access. AGNI uses the Edge Gateway (Cloud Gateway) route to communicate with the firewalls.



Ξ.

Note: AGNI Edge Gateways are deployed as SWIX extensions on Arista EOS switches. They establish a secure tunnel with AGNI facilitating the communication of user-ID updates to on-premises Palo Alto Firewall or Panorama devices.

 Enable RADIUS accounting on the network access devices. The client's IP address is relayed through the RADIUS accounting packets. AGNI needs this information to relay user-ID bindings to Palo Alto Firewall or Panorama devices. You can integrate the Palo Alto PAN Firewall or Panorama with AGNI through the Concourse Application page on the AGNI portal.

3.2.1 Configuring the Palo Alto Firewall/Panorama

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

3.2.1.1 Palo Alto Firewall Configuration

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

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

Click the Verify button to verify and validate the credentials.

| SONI myorg1.c | om | | େ ଡ |
|-----------------------|----|--|-----|
| MONITORING | | M PAN Firewall | |
| Dashboard | | Enter the following fields to configure the app. | |
| V Sessions | | A DECEMBER OF | |
| CCESS CONTROL | | PAN Finewall | |
| P Networks | | | |
| 1 Segments | | Server Type: Firewall O Panorama | |
| ACLS | | Server Name | |
| DENTITY | | | |
| G Identity Provider | | Linear and Linear an | |
| User | ~ | Physiology and the second se | |
| Client | Υ. | Hamme | |
| Guest | v | u Sui Anne | |
| ONFIGURATION | | Record | |
| Access Devices | ~ | Passing | |
| Device Administration | × | | |
| Certificates | * | Cloud Gateway | |
| System | * | Cancel Verify Update | |
| Explore | | | |
| Finstalled Apps | | | |

Figure 3-2: Configure Firewall & Verify

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

To add additional firewall servers, click the here link.

Figure 3-3: Verify Details

| agni myorg1.com | | େ ଡ 💌 |
|--|---|---|
| MONITORING Dashboard Sessions ACCESS CONTROL Networks | PAN Firewall Enter the following fields to update the selected app. | Add Firewall Provide the following details. |
| Ala Segments ALLS DENTITY Dentity | Server Type: Frewall | Hostname |
| A Identity Provider User ✓ Client ✓ ff Guest ✓ | Venterer 34.145.15.90 Venterer antara | Usemame |
| CONFIGURATION Access Devices Contribution Contribution | Construint | Cloud Gateway * Cancel Verify Update |
| Concourse | ACG_HQ_139 To add additioal Firewalts, click bege | |
| Installed Apps | Cancel Application Logs | |
| << Collapse Sidebar | | |

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

| agni myorg1.com | | & @ ® |
|--|--|---|
| MONITORINO MONITORINO Dashboard Consolution Access control Access control Controlution Contro | PAN Firewall Enter the following fields to update the selected app. PAN Firewall Server Type: Personal PAN FW 90 Personal PAN FW 90 Personal Perso | PAR FW 16 Provide the following details Force have PAR FW 16 Passed Bassed 316 Userner admin Pessod Otop Sensey ACG_NDIA_62 Cancel Verify Update |
| System CONCOURSE EE Explore F Installed Apps | To add additional Firewalls, click <u>bare</u> Additional Firewalls PAN FW 16 1085243.16 Cancel Application Logs | |

Figure 3-4: Update Firewall Details

For more details on the Palo Alto Firewall/Panorama integration and configuration, see the document.

3.3 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 3-5: Installing Medigate Concourse Application

| ogni I | | 6 0 📀 |
|---|---|-----------|
| Barthart Barthart Barthart Barthart Polainn Polainn | Contex XXII Fit in the laborary fields to configure the age Vire Contex XXII Vire Contex XXII All UP, < | |
| Cardinges v Digener v Cardinges E Segues E Segues E Segues | | |

- 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).

| agni | |
|--|--|
| VORTORING Contrologies Versions Access control. Versions Nationals III: Segments Q: ACLs Control Control | Medigate Fit is the betwee Failts to applies the selected app Medigate Me |
| L User ~ L User ~ L User States La User Groups Client ~ | Canver Try Upstern |
| Clasts Clast Groups Control Groups C | Last Sync Al Alexandra Cale Society of the New gale Last Sync Al Alexandra Cale Society of the New gale Sync Status Sync Status |
| Administration Constitution System Consolutes Explore Functional for instanted Apps | Application Lage Blow Logs |

Figure 3-6: Installed Medigate Concourse Application

3.4 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 3-7: Installing Microsoft Intune Concourse Application

| agni | | | |
|-----------------------|---|--|------------|
| Dashboard Sessions | | Microsoft Intune Enter the following fields to configure the app. | ← Back |
| ACCESS CONTROL | | Name | |
| Networks | | Microsoft Intune | |
| ⊥l≟ Segments | | | |
| ACLS | | Directory(tenant) ID | |
| IDENTITY | | Application/clienth ID | |
| Identity Provider | | @arista.com | |
| Luser | ~ | Client Secret | |
| Client | ~ | | o |
| 🖞 Guest | ~ | | |
| CONFIGURATION | | Azure Government: Disabled | |
| Access Devices | ~ | | |
| Device Administration | ~ | This app helps to provision AGNI issued EAP-TLS client certificates to managed devices through Microso | oft Intune |
| Certificates | ~ | | |
| System | ~ | Cancel Verify | Install |

- 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 3-8: Installed Microsoft Intune

3.5 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 3-9: Installing Jamf Concourse Application

| agni I | | k | G | 0 | в |
|--|---|---|---|---|---|
| MONITORING Dashboard Sessions Access contract Potworks | Jamf Fill in the following fields to update the selected app | | | | |
| 414 Segments | This app provides ability to provision AGNI issued EAP-TLS client certificates to managed devices through Jamf. | | | | |
| Identity Provider User Client | Olient Certificate Enrollment Enabled | | | | |
| CONFIGURATION Access Devices Configuration Confi | 5000 Challenge 729309018-8812-4475-8556-dbc137e81eef Regenerate | | | | |
| Certificates ~ System ~ CONCOURSE | Use the following SCEP server URL for creating a SCEP profile in Jamf. SCEP server URL S | | | | |
| Installed Apps | Application Logs Show Logs | | | | |
| | Cancel Update | | | | |

- 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.

3.6 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 3-10: Accessing ServiceNow Application Registry

| servi | cenow | All | Favorites | History | Workspaces | Admin |
|-------|----------------------------------|-----------------|--------------|-----------|------------|-------|
| | Application | Re | \otimes | 段 | | |
| FA' | VORITES | | | | | |
| No | Results | | | | | |
| AL | L RESULTS | | | | | |
| | ✓ System App | lications | | | | |
| | Application | Restricte | ed Caller Ac | <u>:c</u> | | |
| | ✓ System OAu | ith | Application | Registry | | |
| | Application | <u>Registry</u> | Ć | ☆ 🗸 | | |
| | | | | | | |

- 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 3-11: Create a new Application for AGNI

| serv | Vicenow All Favorites | History Adm | nin : Application F | Registri 😭 🔍 🤉 Search | 🔹 🗣 ବ ଡ କ 🚳 |
|------------|---|-------------|------------------------|--|--|
| = 7 | Application Registries Name | - Search | | | Actions on selected rows New |
| All > Type | e = OAuth Client .or. Type = OAuth Provider | | | | |
| 0 9 | Name • | Active | Туре | Client ID | Comments |
| | Azure AD | true | OAuth Provider | Enter Client ID | |
| | Azure OAuth OIDC Entity | true | External OIDC Provider | <provide application="" azure="" id="" uri=""></provide> | 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 3-12: Select OAuth API Endpoint for External Clients

| servicenow | All | Favorites | History | Admin | 1 | OAuth application 🚖 | Q Search | - | ۲ | Q | 0 | ٩ | BN |
|--------------------------|------------|------------------|---------|-------|---|---------------------|----------|---|---|---|----|----------|--------|
| < OAuth application | | | | | | | | | | | Ed | it Inter | ceptor |
| What kind of OAuth | applica | ation? | | | | | | | | | | | |
| Create an OAuth API end | point for | rexternal client | ts | | | | | | | | | | |
| Create an OAuth JWT Al | Pl endpoi | nt for external | clients | | | | | | | | | | |
| Connect to a third party | OAuth Pr | ovider | | | | | | | | | | | |
| Configure an OIDC provi | der to ve | rify ID tokens. | | | | | | | | | | | |
| Connect to an OAuth Pro | vider (sin | mplified) | | | | | | | | | | | |
| | | | | | | | | | | | | | |

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

Figure 3-13: Provide CMDB OAuth details for AGNI

| TVICENOW All Favorites | History Workspaces Admin | Application Registries - New Record 🏠 | Q. Search | • | 8 | ٥ | ٥ (|
|--|--|---|-------------------------------------|---|---|-----|-----|
| Application Registries [View: Default*] | | | | | | 0 0 | Sub |
| Auth client application details. Name: A unique name. Client ID: Client ID automatically gene Client Secret: Client secret for the GA Refresh Token Lifespan Time is second Access Token Lifespan Time is second Reflect URL:The redicct URLs authon Enforce Token Restriction: Restricts to long Info | rated by ServiceNow OAuth server, uth application, Leave it empty for auto-genera is the Refresh Shoen will be valid, tablion server refrict to, They must be absolu autoins server refrict to, They must be absolu e access token usage to the API's defined in th | tion. He URLs and they are commus separated. REST API Access Policies. Unselecting this option would allow access token usage | across other REST APY's Learn more. | | | | |
| * Name | AGNI CMDB OAuth | Applicatio | Global | 0 | | | |
| * Client ID | 02dfdcefa04f4290206120bd3c179817 | Accessible from | All application scopes | | | | |
| Client Secret | | Activ | . 🖸 | | | | |
| Redirect URL | | 8 Refresh Token Lifespa | 8,640,000 | | | | |
| Logo URL | | Access Token Lifespa | 1,800 | | | | |
| Public Client | | Login UR | | | | | |
| Comments | | | | | | | |
| with Scopes | | | | | | 0 | - |
| Auth Scope | | | | | | | |
| + Insert a new row | | | | | | | |
| | | | | | | | |
| Submit | | | | | | | |
| | | | | | | | |
| | | | | | | | |

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

3.7 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 3-14: Installing Splunk Concourse Application

| agni I | | G | 0 | в |
|---------------------------|---|---|---|---|
| MONITORING | Splunk 6 Bask | | | |
| Dashboard | Fill in the following fields to configure the app | | | |
| × Sessions | | | | |
| ACCESS CONTROL | Soluti | | | |
| Networks | | | | |
| 414 Segments | Solutik Hostname | | | |
| ACLS | | | | |
| IDENTITY | 443 | | | |
| (4) Identity Provider | 445 | | | |
| 🙏 User 🔍 🗸 | Talan | | | |
| Client 🗸 | 1940 | | | |
| CONFIGURATION | | | | |
| 🖂 Access Devices 🗸 🗸 | Time app provides advicy to positive sessions intermation to Spicitik | | | |
| 🗔 Device Administration 🖂 | Cancel Verify Install | | | |
| 🖵 Certificates 🗸 🗸 | | | | |
| 🖸 System 🗸 🗸 | | | | |
| CONCOURSE | | | | |
| III Explore | | | | |
| 😳 Installed Apps | | | | |

- 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.

3.8 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 3-15: Installing Sumo Logic Concourse Application

| agni I | | | G | 0 | ₿ |
|---|-----|--|---|---|---|
| MONITORING Dashboard Sessions ACCESS CONTROL Networks | | Sume Logic C Bsck Fill in the following fields to configure the app Image: Configure the app | | | |
| ACLS | | Sumo Lógic URL | | | |
| (2) Identity Provider | | This app provides ability to puish sessions information to Sumo Logic | | | |
| Client | Č L | Cancel Verify Install | | | |
| CONFIGURATION | | | | | |
| Access Devices | ~ | | | | |
| Device Administration | ÷ . | | | | |
| Certificates | ~ | | | | |
| System | ¥. | | | | |
| III Explore | | | | | |
| Installed Apps | | | | | |

- 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.

3.9 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.

| IONITORING | CrowdStrike | |
|-------------------------|--|---------------|
| Dashboard | Fill in the following fields to update the selected app | ← Bad |
| Sessions | | |
| CCESS CONTROL | Tung | |
| P Networks | Crowdstrate | |
| = Segments | API URL | |
| ACLS | inde analysis commentation | |
| DENTITY | AP(CHMID) | |
| Identity Provider | 00010700000000000 | |
| User v | API Clevel Secret | ٩ |
| Client 🗸 | | |
| ° Guest 🗸 | This ann provides updates from CrowdStrike about clients' hebaviour to ACNI | |
| ONFIGURATION | | |
| 🗟 Access Devices 🛛 👻 | | |
| Device Administration 🗸 | Event Notification | Disabled |
| Certificates 🗸 | Enable to allow CrowdStrike to send notifications to AGNI for managed clients. | |
|] System 🗸 🗸 | | |
| ONCOURSE | Antibulation | (Association |
| Explore | Application Logs | ShowLogs |

Figure 3-16: 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 3-17: Event Notification Configuration for CrowdStrike

| Device Administration | ~ | Event Notification | | Enabled | -0 |
|---|---|--|-------------------------|-----------|-------|
| Certificates | × | Use the following details in CrowdStrike to send notifications to AGNI. | | | |
| CONCOURSE Explore Sinstalled Apps | Ŷ | NetReation Ville, https://dev.agnieng.net/api/concourse.app.crowdstrike.not/fication/Eb9107b0d-c35f-42e8-ad1f-48f2c39f6686 NetReation Secret XmRrv7_CBxUlyqSdyL9rXCI1qXXRDHF2 | Copy Copy Regenerate | | _ |
| | | Application Logs | | Show | Logs |
| | | | Cancel | Verify Uj | pdate |

3.10 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.

| | 0 | Workspace ONE Fill in the following fields to configure the app | | ← Ba |
|-----------------------|----------|--|--------|---------|
| Sassions | | | | |
| ACCESS CONTROL | - No | 04 | | |
| The works | W | orkspace ONE | | |
| ±]± Segments | 6 | | | |
| ACLs | | This app provides the ability to provision client certificates and retrieve managed client information from Workspace ONE. | | |
| IDENTITY | | | Cancel | Install |
| (1) Identity Provider | | | | |
| 🚨 User | ~ | | | |
| Client | . | | | |
| * Guest | ~ | | | |
| CONFIGURATION | | | | |
| Access Devices | ~ | | | |
| Device Administration | ~ | | | |
| Gertificates | | | | |
| System | | | | |
| CONCOURSE | | | | |
| Explore | | | | |
| Installed Apps | | | | |

Figure 3-18: Installing Workspace ONE

- 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.
- 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 <u>here</u>.

Figure 3-19: Configuring Workspace ONE Parameters

| agni I | | | ତ ୭ 💌 |
|----------------------------|-----|--|-------|
| MONITORINO | | Workspace ONE C Back Fill in the following fields to update the selected app C Back | |
| ACCESS CONTROL Networks | | Waxapace DNE | |
| ACLs | | This app provides the ability to provision client certificates and retrieve managed client information from Workspace ONE. | |
| (a) Identity Provider | | Client Information Synchronization | |
| L User | * * | Client Information Synchronization: Founded | |
| ft Guest | ÷ | APLOSE | |
| Access Devices | × | Client ID | |
| Device Administration | ~ | due fine . | |
| G Certificates | × | | |
| CONCOURSE | ~ | Venty | |
| Explore | | Event Notification: Divided | |
| | | Enable to allow Workspace DNE to send notifications to AGNE for managed clients. | |
| | | Client Certificate Enrollment | |
| | | Application Logs Show Logs | |
| | | Cancel Update | |

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 3-20: Configuring Workspace ONE Parameters

| MONITORING | Workspace ONE | | (1111) | |
|---|--|----------------------|-----------|--|
| Dashboard | Fill in the following fields to update the selected app | | e Back | |
| · Sessions | Client ID | | | |
| CESS CONTROL | Circland | | | |
| Networks | | | | |
| ACLS | | | Verify | |
| with the second s | Event Sectionation - Lanual - | | | |
| identity Provider | | | | |
| User v | Use the following details in Workspace ONE to send notifications to AGNI. | | | |
| Client | history of | 1000 | | |
| Guest v | under vider ableed we reference on a statistic construction of the reference of the second statistic construction of the s | () conv | | |
| Access Devices | eede2056-8afe-4430-ace7-8aee0fedc79c | (C copy | | |
| Device Administration | | | | |
| Certificates v | 729c0/bc-7c79-4801-6799-9w15c8303a14 | Copy Regenerate | | |
| System v | Note - Changes will be saved once you click on update. | | | |
| Emisse | | | | |
| Installed Apps | Client Certificate Enrollment | 0 | (nated | |
| | Use the following SCEP challenge for creating SCEP profile in Workspace OVE. | | | |
| | 10/0 Company 9500-860-601-6012-03.ce x7677640C36d | (D Copy) Beginnerate | | |
| | O Use the following SCEP server URS, for creating a SCEP profile in Workspace ONE. | | | |
| | 101P torne (H) https://qa.agsiang.set/envidement/scop/Eal131Fb/9-2a76-6463-ba16-2e27e546e045(scop-server/74816as9-5e02-55e3 | () copy | | |
| | Note : Changes will be saved once you click on update. | | | |
| | Application Logs | | Show Loga | |
| | | | | |
| | | Cance | el Update | |

Chapter 4

Configuring Identity Providers (IDPs)

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

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

The AGNI integration with IDPs requires:

- · Authentication of:
 - User onboarding workflows to onboard the client devices through UPSK, EAP-TLS, and Captive Portal.
 - · Admin login to the user interface.
 - · Admin login to the UPSK client portal.
 - · User login to the UPSK client portal.
 - Device Administration Portal.
- Authorization To gather user authorization attributes such as groups, account status, and user attributes from the identity providers.

Authorization is an optional process and the IDP configuration for authorization is required only when the network access policies providing access to the users are based on the user authorization attributes.

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

| agni I | | | |
|--|-------|---|-------------------|
| MONITORING Dashboard Sessions ACCESS CONTROL Networks LL Segments ACLs | | Add Identity Provider Provide the following details to add a new Identity Provider Name Azure-test Domain Name antaraaleng.onmicrosoft.com Identity Provider | ← Back |
| Identity Provider User Client Guest Configuration Access Devices | * * * | Microsoft Entra ID Identity Information Synchronization Directory(tenant) ID b07176f5-dca9-43d8-a2b4-b4ca914da8e1 Application(clent) ID | Enabled |
| Device Administration Certificates System System Explore | > > | b213aecd-b856-4c41-a895-6cd45ed186f9 Client Secret Sync Interval (hours) 24 | ⊘ |
| Installed Apps Collapse Sidebar | | | Cancel Verify Add |

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

Figure 4-2: Edit or Update Identity Provider

| Dashboard | Identity Provider Identity Access Manager | nent | | (+ A |
|----------------------------|--|-----------------------------|------------------------|---------------------|
| Sessions CCESS CONTROL | azure eng | Sync Enabled | agni365.net | Sync Enabled |
| Networks | Identity Provider | Microsoft Entra ID | Identity Provider | Microsoft Entra ID |
| Segments | Domain | antaraaieng.onmicrosoft.com | Domain | agni365.net |
| ACLS | Updated At | 13/09/2024 17:05:55 | Updated At | 01/08/2024 09:52:25 |
| Identity Provider | Last Sync Scheduled At | 08/01/2025 09:30:00 | Last Sync Scheduled At | 07/01/2025 21:30:00 |
| User | Sync Status | Success | Sync Status | Success |
| Guest | | / 0 | | / 0 |
| Access Devices | Y Azure Systest IDP | Sync Enabled | okta-test | Sync Disabled |
| Device Administration | V Identity Provider | Microsoft Entra ID | Identity Provider | O Okta |
| System | Domain | systestpoc.onmicrosoft.com | Domain | test.org |
| NCOURSE | Updated At | 24/04/2024 17:07:02 | Updated At | 03/04/2024 21:17:32 |
| Explore Installed Apps | Last Sync Scheduled At | 07/01/2025 21:30:00 | | |
| | Sync Status | Success | | |

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.

agni I Update Identity Provider + Back 1 Dashboard o update the selected identity Provide N Sessions Synchronization Details ACCESS CONTROL · Networks Last Sync Scheduled At 08/01/2025 09:30:00 ala Segments Success Sync Status ACLS IDENTITY Sync Now (2) Identity Provider ± User User Groups Client 4 Available Groups Synchronized Groups 疗 Guest Q Search by group na Access Devices Device Administration ŵ Selected 4 🕞 Certificates Engineering
 This is the Azure Engineering Group - Remove System 4 CONCOURSE All Company This is the default group for everyone in the network - Renova III Explore C Finance Installed Apps - Remove TK-Devices TK-Devices - Remove User Attributes Synchronized Attributes Preview ¥ Add User Attributes Synchronized User Attributes Department 🚷 CostCenter 🚷 < Collapse Sidebar

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

| Identity Provider | | | |
|-----------------------|---|---|----------------------|
| Luser | ~ | | |
| 🛄 Client | ~ | | |
| f Guest | ~ | User Attributes | |
| Access Devices | ~ | Common and the second se | |
| Device Administration | ~ | Synchronized Attributes Preview | |
| Gertificates | ~ | User Attributes | Add |
| System | ~ | - 3 | |
| CONCOURSE | | Synchronized User Attributes | |
| Explore | | Department 🔇 CostCenter 🔇 | |
| Installed Apps | | | Cancel Verify Undate |
| 🛠 Collapse Sidebar | | | verity Opuate |

• **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

| IONITORING | Update Identity Provider | 6 Ba |
|--|--|--|
| Dashboard | Fill in the fields below to update the selected Identity Provider | |
| V Sessions | | |
| CCESS CONTROL | Engineering | - Remove |
| Networks L+ Segments | Platform Engineering | - Remove |
| ACLS | Site Reliability Engineering (SRE) | - Remove: |
| L) Identity Provider | User Attributes | |
| - Obei | | |
| LUSERS | Synchronized Attributes Preview | |
| Users | Synchronized Attributes Preview User login name shane@systestpoc.onmicrosoft.com | Get |
| Users User Groups Client Clients | Synchronized Attributes Preview User login name shane@systestpoc.onmicrosoft.com User Attributes | Get |
| Users User Groups Client Client Clients Client Groups | Synchronized Attributes Preview User login name shane@systestpoc.onmicrosoft.com User Attributes Email | Cet shane@systestpoc.onmicrosoft.com |
| Users La User Groups Client Clients Client Groups ONFIGURATION Access Devices | Synchronized Attributes Preview User login name Email Login Name | Get shane@systestpoc.onmicrosoft.com shane@systestpoc.onmicrosoft.com |
| Users Lat User Groups Client Clients Client Groups ONFIGURATION Access Devices Certificates | Synchronized Attributes Preview User login name Email Login Name Name | Get shane@systestpoc.onmicrosoft.com shane@systestpoc.onmicrosoft.com shane |

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: | OneL | oain | and | Identity | Provider |
|--------|------|------|------|-----|----------|----------|
| | | ••= | | | | |

| ONITORING | | Add Identity Provider | ← Bac |
|-----------------------|---|---|---------|
| Dashboard | | Provide the following details to add a new Identity Provider | |
| Sessions | | - New - | |
| CESS CONTROL | | OneLogin | |
| Networks | | | |
| Segments | | benain Name | |
| ACLS | | (astory | |
| ENTITY | | klentity Provider | |
| Identity Provider | | O OneLogin | |
| User | ~ | | |
| Client | | Identity Information | |
| Guest | | OIDC1ssver URL | |
| INFIGURATION | | https://antara.onelogin.com/oldc/2 | |
| Access Devices | ~ | obciciento | |
| Device Administration | | 0oa4ltoi6gV0fkQ8q5d0oa4ltoi6gV0fkQ8q5d0oa4ltoi6gV0fkQ8q5d | |
| Certificates | | | |
| Certificates | Ť | Add the following URL in the redirect URI's for OIDC application. | |
| System | v | | |
| Explore | | https://dev.agnieng.net/sso/login/callback | Сору |
| Installed Apps | | | |
| | | Identity Information Synchronization | Enabled |
| | | API Client 10 | |
| | | b213aecd-b856-4c41-a895-6cd45ed186f9 | |
| | | API Client Secret | |
| | | | ٥ |
| | | Sync Interval (hours) | |
| | | | |

- 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).

| ITORNO | 200 Add Identity Provider | |
|--------------------------|---|---------------|
| Dashboard | Fill in the fields below to add a new Identity Provider | ← Back |
| Sessions | A fight transit fourier - | |
| ISS CONTROL | 24 | |
| Segments | User Groups | |
| nry Identity Provider | Available Groups Bynchrundised Oroups | |
| User | Q Search by proop name | |
| Client ~ | | (Selected: 3) |
| Access Devices v | CN=Executive,OU=Groups,OU=Employees,DC=myorg1,DC=com | - Renave |
| Certificates | CN=IT.OU=Groups.OU=Employees.DC=myorg1.DC=com | - Remon |
| System ~ | | |
| Evolution | CN+1H,OU+Groups,OU+Employees,OC+myorg1,OC+com | Renere |
| Installed Apps | | |
| | | |
| | | |
| | User Attributes | |
| | Synchronikevid Attributes Provincer | |
| | User Attributes | * Add |
| | | |

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

| IONITORING | Update Identity Provider |
|--|---|
| Dashboard | Provide the following details to update the selected Identity Provider |
| / Sessions | Name |
| CCESS CONTROL | Okta-testorg1 |
| Networks | |
| - Segments | Domain Name |
| ACLS | Leading room |
| DENTITY | Identity Provider |
| Identity Provider | O Okta |
| User | v |
| Client | Jentity Information |
| | |
| Guest | OIDC Domain |
| Guest | v OIDC Domain dev-01259439.okta.com |
| Guest | OIDC Domain dev-01259439.okta.com Application(client) ID |
| Guest ONFIGURATION Access Devices | OIDC Domain dev-01259439.okta.com Application(client) ID Ooa4ltoi6gV0fkQ8q5d7 |
| Guest ONFIGURATION Access Devices Device Administration Certificates | OIDC Domain dev-01259439.okta.com Application(client) ID Ooa4ltoi6gV0fkQ8q5d7 |
| Cuest Configuration Cuest Devices Cuest Device Administration Cuertificates System | CODC Domain dev-01259439.okta.com Application(client) ID Ooa4ltoi6gV0fkQ8q5d7 Add the following URL in the sign-in redirect URI's for OIDC application. |
| Guest ONFIGURATION Access Devices Device Administration Certificates System ONCOURSE | CIDC Domain dev-01259439.okta.com Application(client) ID Ooa4ltoi6gV0fkQ8q5d7 Add the following URL in the sign-in redirect URI's for OIDC application. Comparison Comp |

- 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).

| MONITORING | Update Identity Provider | 6 Back |
|-------------------------|--|---------------------|
| Dashboard | Provide the following details to update the selected identity Provider | |
| v Sessions | | |
| CCESS CONTROL | Identify Information Construction | [Faithed] |
| Networks | identity information synchronization | Energies - |
| Segments | ARTIN | |
| ACLS | | |
| DENTITY | C Sync Internal Houris | |
| Identity Provider | 24 | |
| User | | |
| Cleant | Synchronization Details | |
| 2 Gient V | Last Sune Schadulad & | 07/01/2025 21/20/00 |
| r Guest 🗸 | Loss dynt, achiedanica At | 01012023215000 |
| ONFIGURATION | Syne Status | Success |
| Access Devices V | | Sync New |
| Device Administration V | | (Channel) |
| Certificates ~ | | |
| System ~ | User Groups | |
| ONCOURSE | Analysis Courses Courses | |
| Explore | Available Groups Synchronized Groups | |
| Installed Apps | Q Sauch by avour name | |
| | Carl reserve at Brock range. | |
| | | Selected: 40 |
| | largegrouptest_1 | - Remove |
| | | |
| | Largegrouptest_1000 | - Remove |
| | largegrouptest_101 | - Remove |
| | largegrouptest_102 | Remove |

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

| ONITORING Dashboard | | Update Identity Provider Provide the following details to update the selected Identity Provider | ← Bad |
|---------------------------|----------|---|---------|
| Sessions | | Naine Antara Al Net | |
| Segments ACLs | | Dumin tene | |
| dentity Provider | | Meritr/Honder G. Google Workspace | |
| User Client Guest | * * * | Identity Information Synchronization | Enabled |
| Access Devices | v | C03abdef Account time alan@antaraal.net | |
| Certificates System | , | Uplias Service Account Creamins | |
| Explore Installed Apps | | oppose the first open control opening this will opening a strategy service account. Spot hered thereit | |

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.

| ONITORING Dashboard | Identity Provider Identity Access Management | |
|--|---|-------|
| Sessions | Local Users | |
| Networks | Identity Provider | local |
| l± Segments ⑦ ACLs DENTITY | Domain | local |
| Identity Provider | | |
| User | | |
| Access Devices ☐ Certificates ☑ System | | / 1 |
| ONCOURSE | | |
| Explore | | |

Figure 4-11: Local IDP Configurations

Configuring the Networks

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

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

| MONITORING | Add Network | C. A. Martin |
|-----------------------|--|--------------|
| Dashboard | Provide the following details to add a new Network | ← Back |
| ✓ Sessions | C Name | |
| CCESS CONTROL | Arista-corp | |
| Networks | | |
| La Segments | ssip | |
| ACLs | Arista-corp | |
| DENTITY | | |
| 🖇 Identity Provider | Status: Enabled | |
| User | v l | |
| Client | V Authentication | |
| Guest | Authentication Type | |
| ONFIGURATION | Client Certificate (EAP-TLS) | × |
| Access Devices | ~ | |
| Device Administration | Domain Machine Authentication: Enabled | |
| Certificates | Allowed Machine Domains | |
| System | v | |
| | Optional. Press ENTER after each domain. | |

- 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

| NSE-CORP Provide the following details to update the selected Network | ← Back |
|---|--------|
| Name | |
| Connection Type: Wireless Wired | |
| NSE-CORP | |
| Status: Enabled | |
| Authentication | |
| Authentication Type Client Certificate (EAP-TLS) | • |
| Domain Machine Authentication: Enabled | |
| domain.xyz 😵 pepsico.com 😵 | |
| Optional. Press ENTER after each domain. | |

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

E

- 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 <u>Authenticating Users with Email Codes (as against IDP)</u> section.

- c. Allow Local User Self Registration:
 - 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

| Onboarding | Enabled |
|--|---------------|
| Initial Passphrase for Onboarding | |
| testtttessss | |
| Initial Role for Onboarding | |
| testesdasdasda | Show Domains |
| Allow Email Code Login for IDP User: Enabled | |
| Allow Local User Self Registration: Enabled | |
| Configure the following URL as captive portal for this SSID to allow users to onboard their clients. | |
| https://dev.agnieng.net/onboard/Eb9107b0d-c35f-42e8-ad1f-48f2c39f6686/network/231 | Сору |
| Users can scan a Wi-Fi QR code to connect to this SSID for onboarding. | Print QR Code |

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

| llow Local User Self Registration: Enabled | | |
|--|------|---|
| | | - |
| Users can onboard their clients using the below URL. | | |
| https://qa.antaraops.net/onboard/Ee8eb46d1-d266-460d-9b41-a904b655234b/network/5 | Сору | |
| | | |



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

| ONITORING | | Test-docs | ← Back |
|--|-----------------|---|----------|
| Dashboard | | Provide the following details to update the selected instrumerk | |
| Sessions | | Test-docs | |
| Networks | | | |
| Segments | | Connection Type: Wireless Wireless Wireless | |
| ACLs | | Test-docs | |
| INTITY | | | |
| Identity Provider | | Status: Enabled | |
| User | ~ | | |
| Client | ~ | Authentication | |
| Guest | ~ | Authentication Type | |
| discusation Client Certificate (EAP-TLS) | | | |
| Access Devices | ccess Devices v | | |
| Device Administration | ^ | Domain Machine Authentication: Enabled | |
| C Access Policy | | Enable to allow machine authentication with domain machine certificates. | |
| TACACS+ Profiles | | | |
| Certificates | ~ | Trust External Certificates | Disabled |
| System | * | | |
| NCOURSE | | Enable this setting to accept client certificates issued by external CAs. | |
| Explore | | | |
| Installed Apps | | Onboarding | Enabled |
| | | Allow Email Code Login for IDP User: Enabled | |
| | | | |
| | | Belect Authorized User Groups | |
| | | | |
| | | Users can onboard their clients using the following URL. | |
| | | https://dev.agnieng.net/onboard/Eb9107b0d-c35f-42e8-ad1f-48f2c39f6686/network/378 | C copy |

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

| Sian | In | |
|--------------|------------------|--|
| UserID or Er | nail | |
| alan-test | -docs@arista.com | |
| | | |
| | Proceed | |

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

| | Hello <u>@arista.com</u> |
|------------|--|
| | You have requested for one-time passsord (OTP) to log in to AGNI Self-Service Portal. |
| | Login using the following details: |
| | Email: <u>@arista.com</u> |
| | OTP: yx57xa |
| | The one-time passsord (OTP) will expire at 01 Apr 24 08:46 UTC. |
| | This is an automated email notification. Please do not reply to this message. |
| Copy the (| OTP, paste that for the authentication against IDP, and click the Submit button |
| Figure 5-9 | 9: Verify OTP |
| | |
| | OGOI My Self Service Portal |
| | |
| | |
| | |
| | |
| | Verify one-time password |
| | Verify one-time password |
| | Verify one-time password (i) Check your email for one-time password. |
| | Verify one-time password Image: Check your email for one-time password. |
| | Verify one-time password Image: Construction of the password |
| | Verify one-time password Image: Check your email for one-time password. One-time password yx57xal |
| | Werify one-time password Image: Construction of the password One-time password yx57xal |
| | <section-header><section-header><text><text><text><text><text></text></text></text></text></text></section-header></section-header> |
| | Ore-time password yx57xal |

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

Figure 5-10: Register Client

| Register Client | |
|--|--|
| Provide the following details to register your client Description I's Mac OS X | |

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

| Ogni My Self Service Portal | |
|-----------------------------|--|
| | Register Client |
| | Your client is registered. To connect your client: |

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:

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

| Profile Downloaded | > |
|--------------------|------------|
| Airplane Mode | |
| ᅙ Wi-Fi | TLS-TEST > |
| Bluetooth | On > |
| (Wabila Data | |

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

Profile "AGNI-Wifi Config"

Unverified Profile

This profile is signed by "ANGI, Issuer CA", but that identity cannot be verified. Make sure that you trust the sender of this profile before installing.

Root Certificate

The certificate "ANGI, Root CA" will be added to the list of trusted certificates for this account. Any websites or services using this certificate will be trusted on this Mac.



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 |
|--------|-------|----------|--------------|
|--------|-------|----------|--------------|

| Keychain Access | 1 (i) (Q ANGI | | 0 |
|--|--|-------------------------|----------|
| All Items Passwords Secure Notes My Certificates | Keys Certificates | | |
| ANGI, Root CA Root certificate authority Expires: Sunday, 27 March 2033 at 10:17:39 This certificate is marked as trusted for t | 9 AM India Standard Time this account | Expires | Keychain |
| 💀 ANGI, Root CA | certificate | 27-Mar-2033 at 10:17:39 | login |
| | | | |

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



Onboard your client to connect to 'TLS-TEST' network
After the application is allowed to suggest networks, the device automatically connects to the network in range.

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

| Ogni Self-Service Portal | | ₹ |
|----------------------------|--|---|
| | Register Client | |
| | Your client is registered. To connect your client: 1. Click the Download button to proceed. 2. An executable file will be downloaded to your system. 3. Double-click the file to launch the AGNI Onboard app. 4. This app will configure the device to connect to the secure network. 5. When prompted, click Yes to install certificates. 6. Now you can connect to the secure network. | |
| | Download | |

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



Welcome test@test.com

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



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

Figure 5-27: Onboarding Success



Welcome test@testuser.com

Onboarding successful.

You may now connect to 'ssid-test' network

Close

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.
- Open the AGNI onboarding URL in the browser. You are redirected to the Self-Service Portal.
 Figure 5-28: Register Client

| agni Self Service Portal | | S |
|----------------------------|---|---|
| | Register Client | |
| | Provide the following details to register your client device. Decrypter Shuilendra's Chrome OS Register | |

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

| | 8 |
|---|---|
| Register Client | |
| Your client is registered. To connect your client: 1. Install CloudVision ACMI on your Chromebook. 2. After app is installated, Go to the bottom right, select the time. 3. Select Settings 4. In the "Apps" section, Select Manage your apps > CloudVision AGNI 5. Under Opening Supported Links , Select Open in CloudVision AGNI. 6. Click Launch App button to proceed. Launch App | |

- 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.

Select the Open in CloudVision AGNI app from the Opening supported links.
 Figure 5-30: CloudVision AGNI App

| Phone Hub, Quick Share | | |
|---|---|-----------|
| Accounts 4 accounts | CloudVision AGNI | Uninstall |
| Device | Pin to shelf | |
| Keyboard, touchpad, print | Allow notifications | |
| Wallpaper and style Dark theme, screen saver | Permissiona | |
| Privacy and security | Location Denied | |
| Lock screen controls | Manage permissions | Ø |
| Apps Notifications, Google Play | Preset window sizes Use presets for phone, tablet or resizable windows to prevent app from misbehaving | |
| Accessibility Screen reader, magnification | Opening supported links | |
| System preferences Storage, power, language | Open in CloudVision AGNI app | |
| About ChromeOS | O Open in Chrome browser | |

Click the Launch App button from the Self Service Portal.
 Figure 5-31: Launch App

| 9 | | |
|---|---|---|
| | Your client is registered. To connect your client: | |
| | 1. Install CloudVision AGM on your Chromebook. | |
| | 2. After app is installated, Go to the bottom right, select the time. | |
| | 3. Select Settings 🍅 | |
| | 4. In the "Apps" section, Select Manage your apps > CloudVision AGNI | |
| | 5. Under Opening Supported Links , Select Open in CloudVision AGNI. | |
| | 6. Click Launch App Itution to proceed. | × |
| | Launch App |) |

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

Figure 5-32: Onboarded Client



Welcome Shailu

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

Start

App Version 1.0.4

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





The network profile gets installed with the required certificates.

Figure 5-34: Installed Profile



The client is displayed in the session list in AGNI.

Figure 5-35: Session Details

| Dashboard | | 0 | | | | |
|---|---|---|--------|--|--------------------|--|
| Sessions | | Session Details - Rct9d3a2g12qs7 Details for Session | ← Back | | | |
| P Networks | | Authentication Request | | Success | Session Details | Closed |
| ACLS | | Authentication Type | | Client Certificate (EAP-TLS) | Client IP Address | 192.168.1.9 |
| ENTITY | | Segment | | Default | Session Start Time | 06/12/2024 15:57:52.192 |
| Identity Provider | ~ | Location | | | Session Stop Time | 06/12/2024 16:13 26:090 |
| Client | * | L User (6 | nabled | Client | Enabled | Actions |
| Access Devices Device Administration | | Shalu Shallendra | | 10:a0:54:b3:03:d1 Shailendra's Chrome OS | | Allow Access PAN Firewall Push User Information Target = PANFW 24316 |
| System NCOURSE | ÷ | Access Device | a WiFi | må Network | Enabled | |
| Explore Installed Apps | | e4:d1:24:10:2a:8f Shailendra:2a:8f | | Shailendra-TLS Shailendra-TLS Client Certificate (EAP-TLS) | | |
| // Colleges Eldeber | | for a family for the family star | - | | (| · · |

5.2 Configuring Unique PSK (UPSK) Network

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

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 should be configured to allow access to the required domains (more details under the Show Domains section in Step 8c of the Configuring the UPSK Settings section).

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

| igni | | |
|---------------------|--|-----------|
| | Fill in the fields below to update the selected Network | ← Back |
| Sessions | ACME-BYOD | |
| Networks Segments | Connection Type: Wireless Wireless Wireless | |
| ACLS | ACME-Byod | |
| G Identity Provider | Status: Enabled | |
| Client v | Authentication | |
| NFIGURATION | Authentication Type | |
| Access Devices 🗸 🗸 | Unique PSK (UPSK) | * |
| Certificates | | |
| System ~ | User Private Networks | Enabled - |
| Explore | Shared Clients: Thabled Available Clients Shared Clients | |
| | Q. Search by mac address or description | |
| | | Shared: 1 |
| | O0:23:68:0b:fc:1c Alaris Infusion Pump Module (8300 EtCO2 Module) | + Add |
| | Oa:65:bc:92:81:dd Maquet Ventilator (Servo) | + Add |
| | 00:23:68:31:d7:22 Alaris Infusion Pump Module (8110 Syringe Module) | + Add |
| « Collapse Sidebar | 00:17:23:2f:c3:9a Alaris Infusion Pump Module (8110 Syringe Module) | + Add |

- 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:
 - 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

| | Show Domain |
|---------------|-----------------------|
| | |
| Сору | |
| Print QR Code | |
| | Copy Print QR Code |

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

| MONITORING | | | Networks | | | | | | | |
|---|---|---|------------------------|-----------------|---------------------|----------------------|----------|---------------------|---------|-------|
| Dashboard | | 1 | Available Networks | | | | | + Add Network | Sel | tting |
| Sessions | | | letworks Wireless | Wired | | | | | | 8 |
| Networks | | Q | Search by Name or SSID | | | | | Authenticati | on Type | |
| II Segments | | | | | | | | | | |
| ACLs | | | NAME | CONNECTION TYPE | AUTHENTICATION TYPE | SSID | STATUS | UPDATE TIME | | |
| DENTITY | | 1 | AT-WIRED-EAP | Wired | Client Certificate | | Enabled | 28/11/2023 12:02:09 | 1 | C |
| Identity Provider User | | 2 | AT-WIRED-MBA | Wired | MAC Authentication | | Enabled | 15/11/2023 04:46:37 | 1 | C |
| Client | ~ | 3 | agni-arista-tis | Wireless | Client Certificate | agni-arista-tis | Enabled | 21/10/2023 00:38:14 | 1 | C |
| | | 4 | agni-arista-upsk | Wireless | Unique PSK (UPSK) | agni-arista-upsk | Enabled | 20/10/2023 23:16:39 | 1 | 0 |
| Device Administration | - | 5 | at_c200-upsk | Wireless | Unique PSK (UPSK) | at-c200-upsk | Enabled | 22/09/2023 04:05:34 | 1 | C |
| Certificates | v | 6 | AT-CP-WIRED | Wired | Captive Portal | | Enabled | 10/09/2023 22:59:06 | 1 | 0 |
| System | * | 7 | Copy of at_c200-upsk | Wireless | Unique PSK (UPSK) | Copy of at_c200-upsk | Disabled | 02/09/2023 02:41:33 | 1 | 0 |
| Explore | | 8 | AT-CP | Wireless | Captive Portal | AT-CP | Enabled | 02/08/2023 00:10:56 | 1 | 0 |
| Installed Apps | | 9 | AT-ARUBA-PSK | Wireless | MAC Authentication | AT-ARUBA-PSK | Enabled | 19/07/2023 01:47:00 | 1 | |

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

Figure 5-39: Manage Network Settings

| All N | letworks Wi | Manage Network Settings Update settings for UPSK and EAP-TLS Networks | | | | 8 |
|-------|-----------------|--|----------|---------------------|----------|---|
| Q | Search by Name | UPSK Settings | | Authenticatio | n Type — | 4 |
| | NAME | Maximum Number Of Clients Per User for UPSK Network | STATUS | UPDATE TIME | | |
| | AT-WIRED-EAF | User's Personal Passphrase Validity | Enabled | 28/11/2023 12:02:09 | 1 | Ō |
| | AT-WIRED-MB. | Expires Periodically | Enabled | 15/11/2023 04:46:37 | 1 | Ō |
| | agni-arista-tis | Personal Passporase Validity Penda (Uaya) | Enabled | 21/10/2023 00:38:14 | 1 | Ō |
| | agni-arista-up | | Enabled | 20/10/2023 23:16:39 | 1 | Ō |
| | at_c200-upsk | EAP-TLS Settings Maximum Number Of Clients Per User for EAP-TLS Network | Enabled | 22/09/2023 04:05:34 | 1 | Ô |
| | AT-CP-WIRED | 20 | Enabled | 10/09/2023 22:59:06 | 1 | Ō |
| | Copy of at_c20 | | Disabled | 02/09/2023 02:41:33 | 1 | Ō |
| | AT-CP | Default Cancel Update | Enabled | 02/08/2023 00:10:56 | 1 | Ō |

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

| Register Client |
|--|
| Provide the following details to register your client. Description Bob Smith's Mac OS X ① You have reached the maximum number of EAP-TLS clients allowed. |
| Register |

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* step in the Configuration Steps 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.

| agni | | |
|--|---|--------------|
| MONITORING | Fill in the fields below to update the selected Network | ← Back : |
| ACCESS CONTROL | ACME-Guest |] |
| Networks A Segments | Connection Type: Wireless Wired Sto | |
| ACLS | ACME-Guest | |
| Identity Provider User V | Status: Enabled | |
| 🛄 Client 🗸 | Authentication | |
| CONFIGURATION | Autoentication Type | |
| Access Devices 🗸 | Captive Portal | * |
| Certificates ~ | User Type: Organizational user O Guest user | |
| | Captive Portal | |
| III Installed Apps | total flats for Portal Automotivation agril-guest | Show Domains |
| | Authorized User Groups | • |
| | No-Authenticale Registered Clients Periodic | |
| | Re-Automication Period (step) | |

Figure 5-41: Wireless Captive Portal Network Page One

Figure 5-42: Wireless Captive Portal Network Page Two

| agni | | |
|--|---|------------|
| MONITORING Dashboard Sessions | ACME-Guest Fill in the fields below to update the selected Network ACME-Guest | (← Biack 1 |
| Networks ALLS | Status: Enabled Authentication | |
| Identity Provider User | Captive Portal | *) |
| Client | User Type: Organizational user Ouest user | |
| Access Devices Certificates System | Default Portal ASU-OUEST-2023-01-31_12-01-17 | |

- **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

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

5.4 Configuring Wireless MAC Authentication Network

The wireless network configuration enables you to authenticate end clients connected to the network through client MAC addresses. This process helps clients associate with the network based on various factors surrounding MAC addresses, such as allowing registered clients, all clients, and/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 access points.

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. Add MAC OUIs using the Authorized OUI field.
 - 2. Enable the toggle to associate different client groups for each MAC OUI.
 - **3.** Add New Clients to Group Specify the client group to associate the newly authenticated MAC addresses.
 - 4. Allow Registered Clients and Authorized OUIs This option behaves similarly to Allow Registered Clients Only and Authorized OUIs Only combined.
- **d.** 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

| TORINO | | Add Network | (Annual) | |
|----------------------|------|---|-----------|--|
| ashboard | | Provide the following details to add a new Network | C BARA | |
| iessions | | Cara | | |
| IS CONTROL | | test-admin | | |
| etworks | | Connection Type: Wireless Wired | | |
| egments | | | | |
| CLs | | admin | | |
| TTY | | Protect Textilat | | |
| lentity Provider | | Status, analysis and | | |
| ser | ×. | | | |
| lient | 10 C | Authentication | | |
| uest | . 9 | . Automotive Type | | |
| OURATION | | MAC Autoentication | | |
| ccess Devices | 1 | | | |
| evice Administration | ¥. | MAC Authentication Settings | | |
| ertificates. | ~ | Mac Automatication Type | | |
| rstem | ~ | Allow Registered Clients and Authorized OUIs | · · · · · | |
| xplore | | Disallow user-associated clients: Enabled | | |
| nstalled Apps | | Enable to disallow user associated clients on this network. | | |
| | | Authorized OUI | Add | |
| | | OUI is a new atting of 6 characters Ex: 00052A | | |
| | | Selected Authorized OUIs | | |
| | | 00052A (3) 00053A (3) | | |

F

Note: When you select *Allow Authorized OUIs Only* or *Allow Registered Clients and Authorized OUIs*, you can add individual MAC OUIs and associate each MAC OUIs to individual client groups separately.

Note: You can add or import clients to client groups using the "+" sign in the Client Group field.

Click the Add Network or Update Network button to save and update the network configuration.
 Figure 5-45: Wireless MAC Authentication Network (cont..page)

| | | <u>د او </u> |
|---|---|--|
| MONITORINO E Dashboard V Sessions | Add Network Fronde the following details to add a new Network | |
| ACCESS CONTROL | | |
| P Networks | MAC Authentication Settings | |
| L Segments | MC Antentization Type | |
| ACLs | | |
| 1 Identity Provider | Disallow user-associated clients: Involved | |
| L User v | Enable to disation user associated clients on this network. | |
| Guest ~ | bbA IIU bestoritud | |
| Access Devices ~ | OUI Is a hex atting of 6-characters Ex: 00052A | |
| Device Administration 🗸 | Selected Authorized Oblis | |
| Certificates ~ | 000524 🔕 000534 🕲 | |
| System v | Enable to associate different Client Group for each MAC OU: Enabled | |
| Explore firstalled Apps | MAC OUI CLIENT OROUP | |
| | 00052A III.Primer-1719537347 ~ 💮 | |
| | 00053A IIT-Printer-1719776460 ~ 🕢 | |
| | Cancel Add Network | |
| Collapse Sidebar | | 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.

| Add Network Provide the following details to add a new Network | ← Back |
|--|--|
| Wired EAP-TLS | |
| Connection Type: O Wireless Wired |) |
| Access Device Group | - 🕀 |
| Group. Status: Enabled | and us mixed to the same Access Device |
| Authentication | |
| | |
| Authentication Type | |
| Authentication Type Client Certificate (EAP-TLS) | • |
| Authentication Type Client Certificate (EAP-TLS) Domain Machine Authentication: | • |

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

| Trust External Certificates | Disabled Obs |
|-----------------------------|--------------|
| | |

- **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)

| Trust External Cert | tificate | | Enabled |
|---------------------|----------|---------|---------|
| CRL Verification: | - | Enabled | |
| OCSP Verification: | - | Enabled | |

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)

| Fallback To MAC Authentication | Disabled |
|--------------------------------|----------|
| | |

- 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)

| allback To MAC Authentication | Enabled |
|---|---------|
| MAC Address Authentication Settings- Allow All Clients | v |
| Add New Clients To Group | Ŧ |

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)

| allback To MAC Authentication | Enabled |
|---------------------------------------|---------|
| - MAC Address Authentication Settings | |
| Allow Registered Cliente Only | |

- **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. You can associate an individual client group for each MAC OUI, which is the same as for wireless MAC authentication.
 - O. Add MAC OUIs using the Authorized OUI field.
 - P. Enable the toggle to associate different client groups for each MAC OUI.
 - **Q.** Add New Clients to Group Specify the client group to associate the newly authenticated MAC addresses.
- d. Allow Registered Clients and Authorized OUIs This option behaves similar to Allow Registered Clients Only and Authorized OUIs Only combined

Note: Enable Fallback to MAC Authentication, if required.

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

| | entication | Enabled |
|--|--|---------|
| MAC Authentication Type | | |
| Allow Authorized OUIs | Only | |
| Authorized OUI | | Add |
| OUI is a hex string of 6 c | haracters Ex: 00052A | |
| elected Authorized C | UIS | |
| | | |
| 00052B 🔇 00052A | 0 | |
| 00052B 🚫 00052A | 8 | |
| 00052B 🚫 00052A | 8 erent Client Group for each MAC OUI: Enabled | |
| 00052B 🚫 00052A hable to associate dif | CLIENT GROUP | |
| 00052B 😒 00052A nable to associate dif MAC OUI 00052B | CLIENT GROUP | |
| 00052B 😣 00052A nable to associate dif MAC OUI 00052B | S ierent Client Group for each MAC OUI: Enabled CLIENT GROUP IT:Printer-1718998990 | |

- c. Captive Portal Settings for Unauthorized MAC Addresses (Optionally) enable the toggle if Fallback to MAC Authentication is enabled.
 - Select the captive portal type as Internal or External.
 - Select the internal or external portal.
 - Select the Initial ACL for portal authentication.
 - Enter the captive portal session timeout (optional).

For details on captive portal configuration, see the Configuring Wired Captive Portal Network section.

| Figure 6-8: Ca | ptive Portal Setting | Unauthorized MA | C Address | (Internal) |
|----------------|----------------------|-------------------------------------|-----------|------------|
| J | J | | | · · · · / |

| aptive Portal Settings for Unauthorized MAC Addresses | Enabled |
|---|----------------------------|
| aptive portal type: 💿 Internal 🔘 External | |
| Select internal portal | |
| click-only | - Preview |
| Initial ACL For Portal Authentication | |
| test1234 | Hide Domains |
| Domains that must be allowlisted: | Сору |
| onelogin.com login.microsoftonline.com aadcdn.msftauth.net accounts.google.com www.google.com | next.agnieng.net |
| ok12static.oktacdn.com login.okta.com okta.com login.live.com ssl.gstatic.com www.gstatic.com | play.google.com |
| accounts.youtube.com web-login-v2-cdn.onelogin.com dev-01259439.okta.com aadcdn.msauth.net ap | s.google.com |
| cdn.onelogin.com antara.onelogin.com fonts.gstatic.com | |
| Note: Depending on your environment, additional domains may be part of the allow list. Access the portal directly and inspectomains are required. | t to see if any additional |
| Optionally, configure session timeout | |
| Captive Portal Timeout (seconds) | |
| 100 | |

Figure 6-9: Captive Portal Setting - Unauthorized MAC Address (External)

| Captive portal type: O Internal 💿 External | |
|--|---------|
| Select external portal | |
| Default Portal | Preview |
| Guest Portals are configured in Arista CV-CUE Guest Manager application. | |
| Initial ACL For Portal Authentication | |
| portal-role | |
| | |
| ptionally, configure session timeout | |
| Captive Portal Timeout (seconds) | |
| odbure i orași rimear (orașino) | |

d. 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 6-10: Onboarding

| Unboarding | Enabled |
|---|---------|
| Allow Local User Self Registration: Disabled Om | |
| | |
| Authorized User Groups | |

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

| Dashboard | Add Network Provide the following details to add a new Network | ← Back |
|--|---|---------------|
| Sessions CESS CONTROL Networks | Select an Access Device Oroug to make this Nervork only applicable to a subset of Access Devices. Multiple Nervorks card be level to the same Access Devices Oroug. Status: Evalued | |
| ACLs | Authentication | |
| Identity Provider User A | Clevel Certificate (IAP-TLS) Domain Machine Authentication. Enabled w | * |
| L Users | Enable to allow machine authentication with domain machine certificates. | |
| Access Devices | Trust External Certificates | Distinct Ori |
| System V | Enable this setting to accept client certificates issued by external CAs. | |
| I Explore I/ Installed Apps | Antown Registered Clients Only | (1000) · |
| | Disatew user associated clients: Enumeral |) |
| | Onloarding | (Disabled) () |

Figure 6-11: 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 and 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 6-12: Add Network

| M ^A Authentication Tune | |
|------------------------------------|-----|
| Ro Authentication Type | |
| llow All Clients | Ť |
| | |
| dd Now Cliente To Crown | - @ |

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 6-13: Add Network (MAC Address Authentication Settings)

| CAuthentication Type | | |
|-------------------------|--------------------|---|
| ow Registered Clients (| Only | × |
| sallow user associate | d clients: Enabled | |

- **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.
 - 1. Add MAC OUIs using the Authorized OUI field.
 - 2. Enable the toggle to associate different client groups for each MAC OUI.
 - **3.** Add New Clients to Group Specify the client group to associate the newly authenticated MAC addresses.

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



Note: You can add or import clients to client groups using the "+" sign in the Client Group field.

Figure 6-14: Add Network (Authorized OUIs)

Ę

| Authentication Type | | |
|---|---|-----|
| MAC Authentication | | * |
| | | |
| C Authentication | Settings | |
| AC Authentication Type — | | |
| Allow Authorized OUI | is Only | * |
| | | |
| Authorized OUI | | Add |
| | | |
| Ill is a hey string of 6 (| characters Ex: 000524 | |
| UI is a hex string of 6 o | characters Ex: 00052A | |
| UI is a hex string of 6 o | characters Ex: 00052A | |
| Ul is a hex string of 6 of lected Authorized (00052B (2) 00052A | characters Ex: 00052A DUIs | |
| Ul is a hex string of 6 d lected Authorized (10052B 8 00052 | Characters Ex: 00052A | |
| Ul is a hex string of 6 d lected Authorized (10052B 🚫 00052A able to associate di | Characters Ex: 00052A DUIs A Solution fferent Client Group for each MAC OUI: Enabled | |
| Ul is a hex string of 6 of lected Authorized (0052B S 00052A able to associate di MAC OUI | CLIENT GROUP | |
| Ul is a hex string of 6 d lected Authorized (10052B 8 00052/ able to associate di MAC OUI | characters Ex: 00052A DUIs fferent Client Group for each MAC OUI: Enabled CLIENT GROUP | |
| Ul is a hex string of 6 of lected Authorized (10052B S 000527 able to associate di MAC OUI | characters Ex: 00052A DUIs fferent Client Group for each MAC OUI: Enabled CLIENT GROUP IT:Printer-1719776460 | |
| Ul is a hex string of 6 of lected Authorized (10052B (200527) able to associate di MAC OUI 100052B | characters Ex: 00052A DUIs fferent Client Group for each MAC OUI: Enabled CLIENT GROUP IT:Printer-1719776460 TO | |
| Ul is a hex string of 6 of lected Authorized (10052B (S) 000527 able to associate di MAC OUI 00052B | characters Ex: 00052A DUIs fferent Client Group for each MAC OUI: Enabled CLIENT GROUP IT:Printer-1719776460 CLIENT GROUP | |
| Ul is a hex string of 6 of lected Authorized (10052B (S) 00052A able to associate di 100052B 00052B | characters Ex: 00052A DUIs A S fferent Client Group for each MAC OUI: Enabled CLIENT GROUP IT:Printer-1719776460 | |

6. Click the Add Network or Update Network button to save the configuration. The created wired MAC authentication network is displayed (see sample image below).

Figure 6-15: MAC ByPass Authentication Configuration

| MONITORING | | |
|--|-------------------------|---|
| Dashboard Sessions | • | Update Network - Corporate MAC ByPass Authentication Wired Fill in the fields below to update the selected Network |
| Networks | Corp | orate MAC ByPass Authentication Wired |
| Identity Provider User Client | V Select | a bevice Group |
| Access Devices Certificates Administration Concourse | Auther | ntication reliation Type 2 Address Authentication |
| III Explore | MAC A MAC A Allow | Address Authentication Settings Address Authentication Settings w Registered Clients Only |

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 re-authentication 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. Under the Captive Portal settings:
 - 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 6-16: Figure: Captive Portal

| prive Portai | |
|---|--------------|
| nitial ACL For Portal Authentication | |
| guest-act | Show Domains |
| le-Authenticate Clients | |
| Always | * |
| Onfigure the following URL as captive portal in the initial role, to allow users sign in. | |
| https://do.adviana.pat/quastPortal/Eha61d180_0361_4837_o116-182575420cfh/optwork/136 | Сору |

Figure 6-17: Captive Portal (Re-authentication Option Periodic)

| Initial Role for Portal Authentication | |
|--|--|
| ACME-PREAUTH | |
| Authorized User Groups | |
| Re-Authenticate Registered Clients | |
| Periodic | |

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

Figure 6-18: Captive Portal URL

| Configure the below URL as captive portal in the initial role, to allow users sign in. | | |
|--|--------|---|
| ttps://qa.antaraops.net/captivePortal/Ec36fd356-3041-4fc1-98be-a83382522273/netv | work/6 | |
| | | C |

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 6-19: Guest Portal

| | • | | | | | | | | ь ø (|
|-------------------|-----|---------------------------------------|-------------------------|-----------|------|--|----------|------------------|------------------|
| MONITORING | = | Guest Portals Manage web portals a | nd UPSK portals for gue | st access | | | | + Add Web Portal | + Add UPSK Porta |
| ACCESS CONTROL | ٩ | Search by Name | er 2 | | | | | | |
| Als Segments | | | | ARIS | ТА | | V z | AR | |
| Identity Provider | a b | | | | 2 | internet and inter | 0 | | |
| Client | | | 0000 | | 0000 | | 000 | | 000 |
| CONFIGURATION | Der | rault | | Guestonly | 1 | Portal New | <u> </u> | | / 0 |

- 2. Click the + Add Web Portal button.
- In the Configuration tab, enter the portal name.
 Figure 6-20: Guest Web Portal Configuration

| | i. | ଓ ଡ଼ 💌 |
|---|--|--|
| MONITORING | Customize Guest Portal | ← Back |
| CCESS CONTROL | Configuration Customization | 🕓 Select an element to update it's appearance. |
| Networks | Porer Name New Guest Portal Athentication Types Clickthrough 20 X * | |
| Identity Provider User Client | Clickthrough Organizational User Login | |
| ff Guest · ff Users @ Portals | Guestbook | |
| Batches | Post-authentication Redirect URL | |
| Access Devices | Gancel Add Web Portal | |

4. Select the Authentication Types as Clickthrough.



Note: Based on the selections in the Authentication Types, the fields under Authentication section changes.

Figure 6-21: Configure Web Portal

| agni i ‱ | e test | | | G | 0 M |
|---|--------|---|---|---|--------|
| MONITORING | | Customize Guest Portal | | | ← Back |
| CESS CONTROL | | Configuration Customization | Select an element to update it's appearance. | | 2 |
| Networks 114 Segments | | New Guest Portal | | | |
| ACLS DENTITY | | Automotion Types Clickthrough 🔇 | ARISTA | | < |
| Identity Provider User | ~ | Authentication | Connect to enjoy free Wi-Fi Connect to enjoy free Wi-Fi Connect Research in allog do See Trail. | | ر |
| Client | ~ | Gleest User Pre-submittaate Guest Altware W | | 2 | 2 |
| Vsers Portals | | CAPTCHA Disabled | | | |
| Batches | | Post-authentication Redirect URL | | | |
| C Access Devices | ~ | Cancel Add Web Portal | | | |

- 5. Under the Authentication tab, select Always or Periodic for Guest User.
- 6. Enable CAPTCHA.
- 7. Enter the Post-authentication Redirect URL.
- 8. 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 6-22: Customize Portal

| | st | | | | ¢ | 0 м |
|---|--------|--|---------------|--|--------|---------------|
| MONITORING | | Customize Guest Portal | | | | € Back |
| COSS CONTROL | | Configuration Customization | | Select an element to update it's appearance. | | 2 |
| Networks ±I± Segments | | Theme temptate Default | • | | | |
| ACLS IDENTITY | | Finish demant | | Connectise enjoy free Wi-FI | | \prec |
| Identity Provider User | × | Global | Close | No Sector Contraction | | |
| Client | × • | Guest Login Toggle Login Form | | | \sim | \mathcal{S} |
| f Users Portals Batches | | Login Toggle Logo Page | | C | d | 20 |
| CONFIGURATION | | Terms of Use and Privacy Policy Guest | | | | |
| Access Devices Device Administration | ÿ | Guest CAPTCHA Guest Registration Confirmation | | | | |
| Certificates | × v | Guest Login Header | | | | |
| CONCOURSE | | | Cancel Update | | | |

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

Figure 6-23: Added Guest Portal

| | est | | | | | | | | | ୯ | 0 | 1 |
|---|------------|------------------------------------|--------------------|------------------|---------|-----------|------------------------------|------|----------------|-------------------------------|----------------|---|
| MONITORING | | Guest Portals Manage web portal | s and UPSK portals | for guest access | | | | (| + Add Web Port | al (+ / | udd UPSK Porta | |
| CESS CONTROL | _ ^ | Web UPSK | | | | | | | | | | |
| Networks 4 + Segments | | Q Search by Rame | | | | | | | | | | |
| ACLS | _ 1 | | 6 | - | | | ARISTA | | | ARISTA | | |
| Identity Provider User | | | | | | 7 | Connert in seign finn sich d | 0 | | | 0 | |
| Client | | | | | | | | 000 | | | 200 | |
| n Guest n dest | L | COMMERZEBANK | / 0 | Default | 10 | Employee | | / 0 | GuestOnly | | / 8 | Ì |
| Portals | | ARISTA | | | and the | | ARISTA | | | ARISTA | | 1 |
| III Batches | | Transmission | 1 | | | - 2 | National Science Standards | - | 1 6 | Millione is Sand Registration | | |
| CONFIGURATION | _ | (mainte | | 2 | | | | | 12 | | | |
| Access Devices | ~ | | | | C | 2 | - | 0 | 100 | 1 1 | 0 | |
| Device Administration | | | 000 | - | 00 | 2 | | 000 | 1 8 | | 00 | 1 |
| 🖶 Certificates | ~ | KK Guest Bestel Menu | 0000 | 100000 | 000 | Man Linek | 0 | cood | Test UDOK 1 | | 2000 | 4 |
| System | | KK Guest Portal New | | Minerator | / • | NEW UPSK | | - | rest-OPSK-1 | | / 0 | |

- 10. Navigate to Access Control > Network.
- **11.** 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 6-24: Network Settings

| ACME-wired-guest Provide the following details to update the selected Network | ← Back |
|--|--|
| Name ACME-wired-guest | |
| Connection Type: Wireless Wired | |
| Guest Switch | × ~ 🕀 |
| Select an Access Device Group to make this Network only applicable to a subs linked to the same Access Device Group. Status: Enabled | et of Access Devices. Multiple Networks can't be |
| Authentication | |
| Authentication Type | |
| Captive Portal Captive portal type: Internal Captive portal | <u>ح</u> |

Figure 6-25: Network Settings

| Captive portal type: Internal O External | |
|---|--------------|
| Select internal portal Default | Preview |
| | |
| | |
| aptive Portal | |
| Initial ACL For Portal Authentication | |
| | |
| guest-acl | Show Domains |
| guest-acl Authorized User Groups | Show Domains |
| guest-acl Authorized User Groups pplicable for organizational users only | Show Domains |
| guest-acl Authorized User Groups Applicable for organizational users only Re-Authenticate Clients | Show Domains |
| guest-acl Authorized User Groups pplicable for organizational users only Re-Authenticate Clients Periodic | Show Domains |

- 12. Click Add Network.
- 13. Edit the added network and Copy the portal URL.

Figure 6-26: 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

| escription | | |
|---------------------------|--|------------------|
| his is the segmentation p | olicy for employee access in the ACME corp | |
| atus: Enabled | | Disable Monito |
| Conditions MATCHES AI | L | |
| Network: Name is | ACME-CORP | × |
| User: Group is | imployees | × |
| | | ≓+ Add Condition |
| Actions | | |
| Assign VLAN Assign | /LAN through RADIUS response | × |
| VLAN | ACME-CORP-Access | |
| 0 | | |
| | | |

Sample Contractor Access Segment:

|--|

| ame | | |
|---------------------------|--|------------------|
| CME Corp Contractor Ac | Cess | |
| escription | | |
| his is the segmentation p | olicy for contractor access in the ACME corp | |
| atus: Enabled | | Disable Monito |
| Conditions MATCHES A | L | |
| User: Group is | Contractors | × |
| Access Device: Location | Arista Cognitive WiFi/North America/San Jose | × |
| | | ≡+ Add Condition |
| Actions | | |
| Assign VLAN Assign | VLAN through RADIUS response | × |
| VLAN | ACME-CONTR-Access | |
| 0 | | |
Sample BYOD Access Segment:

| Figuro | 7-3. | BYOD | Access | Seamont | Policy |
|--------|------|------|--------|---------|--------|
| гідиге | 7-3. | DIUD | Access | Segment | FOLICY |

| eccliption | | |
|---|--|------------------|
| is is the segmentation policy | for BYOD devices | |
| | | |
| atus: Enabled | | Disable Monito |
| onditions MATCHES ALL | | |
| Access Device: Location | Arista Cognitive WiFi/North America/San Jo | se |
| Network: Name is AC | ME-BYOD | × |
| User: Group in Employ | vees 📀 Contractors 📀 | > |
| | | EL Add Condition |
| | | |
| ctions | | |
| Assign VLAN Assign VLAN | through RADIUS response | × |
| Assign VLAN Assign VLAN | through RADIUS response | × |
| Assign VLAN Assign VLAN | through RADIUS response ACME-Internet | > |
| Assign VLAN Assign VLAN | through RADIUS response ACME-Internet ttributes | × |
| Ctions Assign VLAN Assign VLAN VLAN VLAN Radius: IETF Radius IETF a Filter-Id | through RADIUS response ACME-Internet ttributes 13 | × |

Sample IOT Access Segment:

Figure 7-4: IOT Access Segment Policy

| ACME Corp IOT Access | | |
|--|-----------------------------------|------------------|
| Service and the service and se | | |
| escription | | |
| his is the segmentation po | licy for IoT devices in ACME Corp | |
| tatus: Enabled | | Disable Monito |
| Conditions MATCHES ALL | | |
| Network: Name is | ACME-IOT | × |
| Client: Group is | DT Devices | × |
| | | ≡₊ Add Condition |
| Actions | | |
| Assign VLAN Assign V | LAN through RADIUS response | × |
| | ACME-IOT-Access | |
| 9 | | |

Configuring the Devices

Network Access Devices (NADs) connect with AGNI via RadSec and the devices are added to AGNI from the **Configuration** > **Access Devices** > **Devices** page of the portal.

You can add the devices to AGNI by:

- · Manually adding the devices.
- · Importing the devices using APIs.
- Devices managed by Arista CloudVision can be imported automatically into the system by installing Arista CloudVision or Arista CV-CUE concourse application.

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

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 RadSec protocol. The vendor list includes:

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

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

Figure 8-1: Adding a Device

| | | | ଓ ଡ 🕒 |
|--|--|-----------------|-------|
| MONITORING | Add or Import Access Devices Provide details to add a new device or import devices from a file Choose Action: Add Import | ← Back | |
| Networks | | | |
| IDENTITY (2) Identity Provider | MAG Adoress Vinto Arişta WiFi | | |
| Client Configuration | Savar Number | | |
| Access Devices Devices Devices | IP Address | | |
| Cloud Gateways Device Administration | Access Device Group Optional | - 🛞 | |
| Certificates v | Location Optional, example: Global/Americal/Galfornia/Site-1 | 0 | |
| Explore | Ca | ncel Add Device | |

8.2 Importing Devices in Bulk to AGNI

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

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

To bulk import devices to AGNI, perform the following steps:

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

| 000i I 1000 | ing . | | | | | | | | 6 O O |
|----------------------------|-------|----------------|--|--------------------|----------------|----------------------------------|---------------|-----------------------|-------------------------|
| terretinen 15 Destinant | | | Access Devices List of Access Devices allowed for Re- | first connections | | | | | + Add or Import Devices |
| Altersteres | | | | | | | | | |
| · Networks | | 9, | | | | | | Al Devices | |
| its Degenerite | | 14.1 | NAME | MAG ADDRESS | 189008 | LINEATION | RADGEC STATUS | UPDATE TIME | |
| REALTY. | | 1 | Merall 88 15 48 80 R 40 | 88/10 4X.0017.00 | (Clean Merger) | | | 1019/2023 02-44.48 | / 0 |
| (A) Mantity Provider | | | Munity AP | 10.01.24.12.77.4 | delate Will | Arres Cognitive WEUNorth America | | 1100/2023 23:10:33 | / 0 |
| A there | | | Aruba AP | 3817x1x5363638 | distant - | | | N7/2023 03:30141 | / 8 |
| ole. User Dringes | | 4 | - | 00 H x 9 26 05 05 | Ariana (MP) | Barta Clara | | 10/5/2123 03 03 03 08 | / 8 |
| Client | 124 | 1 | Cisco WLC | 18.5x8.9xe30.0xx20 | Churn | | | 10/17/2019 02:53:04 | / 0 |
| Citerra | | | ariste-710P | 2010/08/11/39/34 | Aritik Saritzh | Arists Couplinion/Tenen/San June | • 1 | 11/14/2023 10:32:00 | / 0 |
| Client Droupe | | 1. | topano.0-230 | 3046248276wl | Arona Witti | *North Americalian Jose | | 1014/2023 18:30:05 | / 0 |
| Concernation | | (\mathbf{x}) | suparus-w316 | 4430124100a.0f | Artsta Willi | More Americalian fan Jose | | TV14/3023 VE30:00 | / 8 |
| Devices | | 1.1 | Dente Anaba AP | 112233244-05-08 | (Analise | DidatAne/callanaCie/al-1 | | 1022/2023 43 49 58 | / 8 |
| 📄 Device Groups | | - 10 | Dens Cisco AP | an biographies # | Own | Barta Clara | | 15/23/2022 03 48 28 | / 0 |
| David Gatemays | | 11 | Demo Arlata AP | #162c3.04x5/6 | (Avena lands) | Santa Dana | | 11/23/2023 03:49:29 | / 0 |

Figure 8-2: Importing Devices

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

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

Figure 8-3: Add or Import Devices - Choose Action

| MONITORING Dashboard Sessions ACCESS CONTROL | Add or Import Access Devices Provide details to add a new device or import devices from a file Choose Action: O Ad Import | ← Back |
|---|--|-----------------|
| Networks *Is Segments ACLs DENTITY | Access Device Group Optional Captional Caption | - @ |
| Identity Provider User ~ | Columns: mac*, vendor*, name*, ipAddress, seriaNumber, location | Sampte 🛓 |
| Client CONFIGURATION Access Devices Devices | | Cancel Import - |

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

- MAC Address (mandatory)
- Vendor (Mandatory)
- Name (Mandatory)
- IP Address (Optional)
- Serial Number (Optional)
- Location (Optional)

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

| Figure 8-4: Add c | or Import Devices - S | Sample Button |
|-------------------|-----------------------|---------------|
|-------------------|-----------------------|---------------|

| | 9 | |
|---|--|---------------|
| MONITORING | Add or Import Access Devices Provide details to add a new device or import devices from a file Choose Action: Add Import | ← Back |
| Networks Ala Segments ACLS DENTITY | Access Device Droup Cotrona Upmar Civ File Device D | - 💿 |
| identity Provider User Client | Columns: mac*, vendor*, name*, ipAddress, serialNumber, location | Sample ± |
| CONFIGURATION Access Devices Devices Device Groups | | Cancel Import |

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

Figure 8-5: Add or Import Devices - Import Button

| MONITORING | Add or Import Access Devices Provide details to add a new device or import devices from a file | ← Back |
|--|--|----------|
| CCESS CONTROL | Choose Action: O Add Import | |
| Networks | Access Device Group | - 🕀 |
| C ACLS | Optional special COV for Drowse sample-devices.cov | |
| Identity Provider User | Columns: mac*, vendor*, name*, lpAddress, serialNumber, location | Sample 🛓 |
| Client ~ | | Cancel |
| Access Devices | | |

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

4. Click Import to import all the devices to AGNI.

Once the devices are successfully imported, they are displayed under the **Access Devices** > **Devices** tab (see image below).

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

Figure 8-6: Access Devices

王

| agni I Teet Org | | | | | | | | 6 0 I |
|---------------------------|------|--------------------------|------------------------|-----------------|-------------------------------------|---------------|---------------------|-------------------------|
| Coshboard | 6 | Access Devices | fiel consectors | | | | | + Add or Import Devices |
| A Seature Access control. | | | | | | | | |
| Networks | 9 | | | | | | At Devices | * |
| @ ACLS | | NAME | MAC ADDRESS | VINDOR | LOCATION | RADIAC STATUS | UPDATE TIME | |
| anner: | 1.0 | Merahi 88:15:48:60:17.48 | 88.15.44.6075.40 | Claud Merani | | | 11/16/2023 03:44.48 | / 8 |
| (A) Identity Provider | 1 | Mohit's All | 20.88.24.8277.41 | (Arata MPI) | Arista Cognitive WERborth America | | 11/0/2023 23:10:33 | / 0 |
| Clerit . | 1.8 | Andre AP | 2017(2)(6:3+58 | Angel | | | 8/7/2023 03:30:01 | / 0 |
| company | . 4 | alaca . | 99 Mu9 26 85 09 | (Answer) | Barta Clate | | 10/5/2029 1/2/22:90 | / * |
| Access Devices | | Cisco WLD | N 14 10 10 10 10 20 | Own | | | 10/7/2023 02/93/08 | / 0 |
| G2 Desires | ι., | arista-7109 | Sciencels III (Skinisk | (Avera Barrieta | Arista Cinadrigues/Terreri/Law Jaco | | V042023 16:0058 | 1.0 |
| Chaud Gateways | | ырата,0-339 | 30 mm 24 m2 7 m ar | durana (HERE) | Nevro America/Lan Jose | | 11/4/2023 10:00:00 | 1 . |
| 🗈 Davice Administration 🤟 | 1. | superio-w350 | w4xf124102a3d | Arieta MATI | "North America/Last San Jone | | 1014/2023 10:00-05 | / = |
| 😜 Certificates 🚽 | | Demo Arube AP | 112233-4435-69 | Anata | Orbia/America/GantaConalt.ale-1 | | 1123/2023 03:40:06 | |
| () System | . 10 | Cisco AP | an block of an if | Case | Barris Clara | | 1024/2022 15:28:35 | / 0 |
| E Explore | . 11 | Artata AP | watches with | Avera were | Danta Clara | | 11/24/2022 19:29:33 | / 0 |
| 😰 Installed Apps | - ir | Avista Switch | 22/33/44/33/08/77 | Aviata Bashch | last Jone | | 1104/2023 15:29(33) | / 8 |
| | 10 | Denso AP | #816514314211 | (Derett) | San Jone | | 1023/2023 03:49:39 | / = |
| | 34 | Demo Cisco Meraki | #8.00 c#.03.8272 | Ciscal Merani | Mountain View | | 1123/2023-03-48-26 | |
| | 18 | Arists 0-75 | 0011143546-81 | (Anata (MPI) | Global/America/BantaClara/Lab-1 | | 11,04/2023 15:3110 | / 8 |

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.

| agni | | | | | | | | C | 5 | 0 🕐 |
|---|-----|-----|--------------------------------------|-------------|----------|---------|--------------------|---------------|----|----------|
| MONITORING | | : | Users Manage the list of identity | uses | | | | | + | Add User |
| ACCESSIONS | | AUU | Sers Local Externa | | | | | | | |
| Networks Segments | | ٩ | Search by nema or email | | | | | Natur Arry | | * |
| ACL. | | | NAME | USER ID | TYPE | STATUS | UPDATE TIME | | | |
| KENTITY | | 1 | Steve Kratt | steve.kratt | External | Enabled | 7/10/2023 13:35:15 | | 11 | |
| Identity Provider User | | 2 | Mary Osborne | mary.osbome | External | Enabled | 7/10/2023 11:14:48 | | 11 | |
| 1 Users | - [| | | | | | | | | |
| 121 User Groups | | | | | | | | | | |

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.

| IONITORING | | Steve Kratt | | | |
|---|---|---|--------------------------------------|------------------------|------------------|
| Dashboard | | View user details and update | the selected user | | - Back |
| Sessions | | | | | |
| CCESS CONTROL | | Steve Kratt | | | |
| Networks | | | | | |
| sia Segments | | steve kratt | | | 2 |
| ACLs | | Contractor | | | |
| DENTITY | | Pesophiase | | | |
| (2) Identity Provider | | | | | |
| L User | ^ | Status: Enabled | | | |
| L Users | | | | | |
| 241 User Groups | | | | Ca | ncel Update User |
| | | | | | |
| Client | ~ | | | | |
| Client | ^ | User clients | | | Hide Clients |
| Client | ^ | User clients | | Stend | Hide Clients |
| Client | ^ | User clients | | Stand | + Hide Clients |
| Client Clients Client Groups | ^ | User clients Q Search by MAC address | REPRIOTION | STATUS | +lide Clients |
| Client Clients Client Groups | * | User clients Q. Search by MAC address. # MAC ADDRESS | DESCRIPTION | Stand Any STATUS | Hide Clients |
| Client Clients Client Groups Client Groups Chirauration Access Devices Certificates | * | User clients Q. Soarch by MAC address. # MAC ADDRESS 1. 70:1a:b8:82:10:31 | DESCRIPTION Steve Kratt's Windows | Status Enabled | Hide Clients |

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.

Note: The Login Invitation Email option is displayed only when the User ID is an email address.

=

| CloudVision agni | | |
|---|--|-----------------|
| MONITORING | Add Local User Fill in the fields below to add a new local User | ← Back |
| Networks ± ± Segments ACLs DENTITY | Use email address to get the credentials sent as an email to user. Name Test User Password | |
| Identity Provider User ^ Users user Groups | Status: Enabled User should change password at next login: Enabled | |
| Client ~ CONFIGURATION | Login Invitation Email | Disabled O |
| Certificates v System v | Enable to send notification with account details to user via email. | |
| << Collapse Sidebar | | Cancel Add User |

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) |
|----------------------------------|----------------|--------------------|-------------|
| | | | |

| QONI I set sev | ce Portal | | | | | | |
|--------------------|---|-----------------|----------------|----------|---------------------|------|---|
| Eb Marage Clients | Clients | | | | | | |
| 🕎 Wi-fi Pausphrase | Manage the list of clients as on 62/010 | 2024 13 55 67 | | | | | • |
| | | | | | | 1000 | |
| | Q Search by MAC without in description | | | | | Ary | • |
| | # WAC ADDRESS | DESCRIPTION | (MENER (1/583) | status | UPDATE THE | | |
| | 1 | Keen's Mac OS X | Kaurt | Bratived | e3je/j0004 11 53 61 | | • |
| | 2 Milancold an M | | Kenti | Entired | 01010304 22:30:35 | | 0 |
| | 3 44 51 33 75 76 64 | Kenn's Andruid | Kent | Statist | 21/06/2024 15 15:08 | | • |
| | | | | | | | |

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

| CloudVision 090i | | | | | | ୯ ଡ 💿 |
|-----------------------|---|--|---------------------------------------|----------|---------------------|------------------------|
| MONTOIRNO | | User Groups List of User Groups, include All Groups Local External G Bearch by Name p | s both local and external user groups | | | + Add Local User Group |
| ACLS | | # NAME | DESCRIPTION | TYPE | UPDATE TIME | |
| (A) Identity Provider | | 1 ACME Contractor | | External | 10/07/2023 21:05:38 | 0 8 |
| 1 User | • | 2 ACME Engineering | | External | 10/07/2023 21:05:38 | • |
| ± Users | | 3 ACME IT | | External | 10/07/2023 21:05:38 | 0 8 |
| ALL User Groups | 1 | | | | | |

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.

| IONITORING | Update Local User Group | |
|-----------------------|---|-------------|
| Dashboard | Fill in the fields below to update the Local User Group | ← Back |
| ✓ Sessions | | |
| CCESS CONTROL | Nome - | |
| Networks | Test User group | |
| La Segments | Description | |
| ACLs | local user group | |
| DENTITY | Type | |
| (4) Identity Provider | Local | |
| Luser ^ | | |
| * Unore | Users | |
| L Users | | |
| MA User Groups | Available Users Assigned Users | |
| Client ^ | | |
| Clients | Q Search by name or email | |
| Cient Groups | | |
| E chent oroups | | Selected: 1 |
| ONFIGURATION | Test User | - Remove |

Figure 9-6: Local User Groups

Client Configuration

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

| MONETORING Dashboard Sessions ACCESS CONTROL Networks ALA Segments ALLS DENTITY LIGENTITY LIGENTITY Provider | Test Client Group Add or Import Clients Back Fill in the fields below to update the Client Group Test Client Group Image: Client Group Test Client Group Test Client Group Image: Client Group Description The Client mapped to this group are test clients Image: Client Group User Ausotation Image: Client Group Image: Client Group |
|---|---|
| LUser ^ | Group U-PSK Enabled All Clients belonging to this group must use the below Group UPSK to connect to the network. |

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

| agni | | |
|------------------------------|---|----------|
| MONITORING | Add Client Group Fill in the fields below to add or import Clients to a Client Group | ← Back |
| Sessions COSS CONTROL | Test Client Group | |
| ACLs | Description | |
| () ROLS | Not user associated | * |
| LUser | Group U-PSK | Disabled |
| 224 User Groups | Allowed Networks | |
| Client Clients Client Groups | PUNE-WPA2 Select Networks | • |

• **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

| ngni | | | |
|--|--------|--|------------------------------|
| MONITORING Dashboard Sessions ACCESS CONTROL | | Test Client Group Fill in the fields below to update the Client Group Uter Association Not user associated | d or Import Clients 🔶 Back 🚦 |
| Networks ACLs | | Group U-PSK | Disabled Opp |
| L) Identity Provider | • | Allowed Networks | • |
| Client | • | Delegated Management In addition to AGNI admins, the selected User Groups will be allowed to add/remove Clients to this group. User Groups | Enabled |
| NFIGURATION | | Cloud Operations 😵 Select user_groups | * |
| Access Devices Certificates | * * | | Cancel Update Group |

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

| agni | | | | |
|---|---|---|--------|------------|
| MONITORING Dashboard Sessions | | Fill in the fields below to add a new Client or upload a file to import Clients | | ← Back |
| ACCESS CONTROL | | Client Group | | * ⊕ |
| ⊥i⊥ Segments | | Choose action: Add Import | | |
| Identity Provider User | | 00:11:74:12:ed:4f | | |
| LUSers | | Demorption Test Client | | |
| Client | ^ | | Cancel | Add Client |
| Client Groups | | | | |

Figure 10-5: Client Import

| Igni | | |
|-----------------------|---|---------------|
| MONITORING | Add or Import Clients Fill in the fields below to add a new Client or upload a file to import Clients | ← Bac |
| CCESS CONTROL | Client Group Test Client Group | - 🕀 |
| Networks Segments | Choose action: O Add Import | |
| DENTITY | United CSV File | |
| (1) Identity Provider | Browse | |
| Luser A | Columns: mac*, description | Sample 👲 |
| LUSERS | | Cancel Import |
| Client ^ | | |
| Clients | Clients in this group | Show Clients |
| ONFIGURATION | | |
| 🗟 Access Devices 🛛 🗸 | | |
| | | |

Note: AGNI enables you to add clients to the client group so as to apply segment rules using the client group.

=

10.2 Client Details

Click on the clients to display the client details:

- Client Information Displays MAC address, description, client group, passphrase, and status.
- Description Displays the description of the client machine.
- Client Group Displays the groups this client is associated with.
- Status Status of the client (enabled or disabled).
- 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 - Sample 1

| MONITORING | tarun's Android Details of selected client | | | | | é Back |
|---|---|---------|-----------------|-----------------------|--|--------------------|
| ≁ Sessions | Description | | tarun's Android | Client Details | | |
| CCESS CONTROL | Client Group | | 2.5 | Device Type | 5 | martOevice:Android |
| *[# Segments | Status | | Enabled | Machine Authenticated | | No |
| ACLs | | | | Added At | 2 | 4/04/2025 00:37:05 |
| Identity Provider | | | | Updated At | 3 | 4/04/2025 00:37:11 |
| LUser v Client A | | | | Client Fingerprint | | ~ |
| Clients | Client Certificate (EAP-TLS) | | | | | Good |
| 📌 Guest 🗸 🗸 | Subject DN | | | | | CN=tarun, O=local |
| | Issuer DN | | | CN#AGNI, Is | suer CA, O=Google test (E0e0f7309-24f8-4986-88 | db-33976263384a) |
| Device Administration | Expiry Date | | | | 84 | 4/04/2026 00:37:11 |
| Gertificates ~ | | | | | | |
| System ^ | | | | | | |
| Audit Viewer | L User | Enabled | Network | | Access Device | |
| License Self-service Portal RadSec Settings | tarun tarun | | Not available | | Not available | |
| Cupport Long | | | | | | |

Figure 10-7: Client Details - Sample 2

| agni I | | | | 6 O | ۲ |
|-----------------------|---------------------|-----------------|------------------------------|---|-----------|
| TS Permant | chandron's Mac OS X | | | (+ ma | |
| - Deserved | 4 10 40 10 10 10 | | Classificate Distant Span | The second se | - 21 A |
| on Ingenera | Chardren Mar 192. B | | Second Information | | |
| A NO. | here . | - 😔 | John R | Richard In | righted . |
| X ments haven | | • D fee | Chert Programs | | |
| E Clerk | 10x (100) • | | | | |
| Chert Droppe | Chard Rothadas | | | | |
| Internation | | 5. Aprillion | | | |
| E farma Adventision - | | face (provident | | | |
| Distributes - | 1 too (1001) | · Actest | | C. Annes berie | |
| 2 Auto Vener | | Notices | | Net postdite | |
| O Radias Invitega | | | | | |

Figure 10-8: Client Sessions

| agni I | - | | | | lana lang lang lang lang lang lang l | وما مرما مرما مرما | والمرجا ورجا | e her her her her her her | | 6 9 | | • |
|--------------------|---|----|---|------------------|--------------------------------------|--------------------|--------------|---------------------------|---|-----|---|----|
| Ti lamani | | | 0 | lands. | e terreizzis delle pr | | | 0. | int Management and | | | - |
| | | | | | | | | | | | | = |
| - | | ą | | | | | | | (build | | | ÷. |
| C ALL | | | + | 1441.4034032 | And and the second | - | 10004 | index beauty | UPDATE TAK | | | |
| abarrer . | | | | And an Advantage | 404.000 | | frank. | 14p12 | Marking Column | | 1 | |
| A specify binetize | | 0 | ٠ | | | | and. | C 10000 (******** | 11040000-010000 | | 1 | |
| L Cherry | 1 | .0 | 4 | 001x2h3x4411 | | | (Dares) | and a | In the later of the Pe | | 1 | |
| C Tare | 1 | 0 | 4 | 001+20.384639 | | | (rest) | A-012 | 100000000000000000000000000000000000000 | | 1 | • |
| 2 the base | | α. | | 91143434-4622 | | | (based) | and a | | | 1 | |
| T front | • | Π | | 00142424-0454 | 0.0001 | | 2444 | And is | 100000000000000000000000000000000000000 | | 1 | |
| Accession | | 0 | 1 | 414141414141 | | | (based) | | NUMBER OF STREET | | 1 | |
| C Decis American | | 12 | | ISSUERA. | | | 1.011 | | - | | 1 | |

Click the update icon (pen icon) on the far right of the client to edit and update the client details.

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:

Ξ.

- · 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 10-9: Clients Dashboard

| ထိရိုဂ်၊ ၊ | | | | | | | | | | | 5 O | • |
|---|--------|---|--------|----------------------------------|----------------------------------|--------------|---------|--------------|------------------|--------------|-----------------|--------|
| Moletoinus E Dashboard | | | Cli | ents hage the list of Clients | | | | Client M | anagement Portal | + Add Clie | nt or Import Cl | lients |
| ACCESS CONTROL | | | | | | | | | | | E | 88 |
| Vetworks | | ٩ | Searce | N by MAC address or owner(| vser) | | | | | torus Any | | • |
| ACLs | | | | MAC ADORESS | DESCRIPTION | OWNER (USER) | STATUS | CLIENT GROUP | UPDATE TIME | | | |
| DENTITY | | | 1 | | Shailu's Linux | Shallu | Enabled | | 20/03/2024 13 | :36:31 | 1 | |
| Identity Provider User | 0 | | 2 | 5c:e9:1e:87:e5:a1 | Shaik/'s Mac OS X | Shallu | Enabled | | 20/03/2024 13 | :31:39 | 1 | 0 |
| Ctient | ~ | | 3 | 88:b1:e1:13:3d:12 | test | | Enabled | venky | 18/03/2024 11 | 47:48 | 1 | 0 |
| 📌 Guest | * | | 4 | 88:b1:e1:13:3d:1f | test | | Enabled | venky | 18/03/2024 11 | 45:04 | 1 | 0 |
| CONFIGURATION | ÷ | 0 | 5 | 16:6b:3e:d3:7e:c4 | Auto-registered using Eduroam | | Enabled | | 18/03/2024 03 | 01:42 | 1 | ٥ |
| Device Administration | * | | 6 | bc:d0:74:01:d9:33 | Auto-registered using Eduroam | | Enabled | | 17/03/2024 00 | 40:19 | 1 | 0 |
| Certificates | × , | | 7 | | Auto registered by Workspa | Atul Tambe | Enabled | | 16/03/2024 05 | 40:09 | 1 | 8 |
| CONCOURSE | | | 8 | | Auto registered by Workspa | Atul Tambe | Enabled | | 15/03/2024 08 | 48:46 | 1 | 0 |
| III Explore | | | 9 | | Auto registered by Workspa | Atul Tambe | Enabled | | 15/03/2024 08 | 39-35 | 1 | 0 |
| 19 Instance Apps | | | 10 | be:0f:65:37:e8:8c | Auto-registered using Eduroam | | Enabled | | 15/03/2024 05 | 08-02 | 1 | 0 |
| | | | 11 | 11:11:11:11:11:19 | Atharva Test Client 1 | | Enabled | test4 | 14/03/2024 13 | 41.23 | 1 | ٥ |
| | | | 12 | | Auto registered by Workspa | Atul Tambe | Enabled | | 12/03/2024 06 | 07:07 | 1 | 8 |
| | | | 13 | | Auto registered by Workspa | Mohit Goyal | Enabled | | 12/03/2024 06 | 00:48 | 1 | 0 |

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 10-10: Select Client

| ရီရီဂါ၊ ၊ | | | | ७ ७ 😐 |
|-----------------------|--|---|-----------------------|----------------------------------|
| MONTORNO | Shailu's Mac OS X View client details and update the selected | client. | | ← Back |
| 🛷 Sessions | With Address A | | Client Dotails | |
| ACCESS CONTROL | - Description - | | Device Type | Computer/Mac OS X |
| Ala Segments | Shailu's Mac OS X | | Machine Authenticated | No |
| The ACLS | Status: Enabled = | | Added At | 12/03/2024 12:11:45 |
| A Identity Provider | | | Updated At | 14/03/2024 10:53:12 |
| ± User v | Client Attributes | | | |
| 🛄 Client 🗠 | Arista NDR: Risk Action | quarantine X | Client Fingerprint | v |
| Clients | Device Manager | - Janf X | Last Session Details | Closed |
| Client Groups | Workspace ONE: Compliance Status | * Compliant X | IP Address | 192.168.0.101 |
| 🕺 Guest 🗸 | | Pe Add Attribute | Location | */india/Uttarakhand |
| Access Devices ~ | | | Segment | |
| Device Administration | | Cancel Update Client | Authentication Status | Success |
| Certificates v | (| | | |
| CONCOURSE | Client Certificate (EAP-TLS) | | | Good |
| III Explore | Subject DN | | | CN+Shailu, O+local |
| IV Installed Apps | Issuer DN | | | CN+AGNI, Issuer CA, O+arista-dev |
| | Expiry Date | | | 12/03/2025 12:12:40 |
| | | | | ± |
| | | | | Download Certificate |

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 10-11: Download Certificate**

| Dashboard | | Shailu's Mac OS X View client details and update the selected | client | | | | ← Back |
|-------------------|------|--|--------|------------|---------------|-----------------------|----------------------------------|
| ' Sessions | C | we notice | | | | Client Details | |
| Networks | | notoxe | | | | Device Type | Computer:Mac OS) |
| Segments | s | haik/s Mac OS X | | | | Machine Authenticated | No |
| ACLS | Sta | itus: Enablea =0 | | | | Added At | 12/03/2024 12:11:45 |
| Identity Provider | | Canal Attributer | | | | Updated At | 14/03/2024 10:53-13 |
| . User 🗸 🗸 | | Adapt Mining Contract Annual | | a constant | | Client Fingerprint | |
| Client | | Device Manager | | quarantine | Ĵ | | |
| Clients | | Workspace ONE: Compliance Status | | Compliant | ŷ | Last Session Details | Close |
| Guest v | | | | | | IP Address | 192.168.0.10 |
| ONFIGURATION | | | | 76 A | dd Amribute | Location | */India/Uttarakhan |
| Access Devices ~ | | | | Cancel | Update Client | Segment | |
| Certificates | | | | | | Authentication Status | Success |
|) System 🗸 | Clie | ent Certificate (EAP-TLS) | | | | | 6000 |
| Explore | Si | ubject DN | | | | | CN+Shailu, O+loca |
| Installed Apps | 19 | suer DN | | | | | CN+AGNI, Issuer CA, O+arista-dev |
| | Ð | spiry Date | | | | | 12/03/2025 12:12:40 |

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

Figure 10-12: Generate Certificate

| agni I | L. | | େ ଡ м |
|-----------------------|---|-----------------------|----------------------|
| MONITORING | Shailu's Mac OS X View client details and update the selected client | | (- Back |
| × Sessions | SenditedTecas | Client Details | Ca Reprofile |
| Networks | Description | Device Type | Generate Certificate |
| ili Segments | Shalu's Mac OS X | Machine Authenticated | E Delete |
| O ACLS | Status: Enabled | Added At | 12/03/2024 12:11:45 |
| (2) Identity Provider | | Updated At | 14/03/2024 10:53:12 |

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 10-13: Certificate - Generate Radio Button

| GoodVision GG∩i I | | | | G | 0 | M |
|-----------------------------------|---|--|----------------------------------|---|---|---|
| Monstoning | | Generate Client Certificate Fill in the details to generate client certificate for the selected client | é Back | | | |
| ACCESS CONTROL | | Generate Certificate: Generate Use CSR | | | | |
| Vetworks | | See See Street See See State Shaku's Mac OS XI | | | | |
| ACLs | | | | | | |
| IDENTITY (2) Identity Provider | | A certificate already exists for the selected client. Generate only if required. | | | | |
| 1 User | | 🖶 Shally | Expires on 12/03/2025 | | | |
| Client | ^ | Subject DN | CN+Shallu, O+local | | | |
| Clients | | Issuer DN | CN+AGNI, Issuer CA, O+arista-dev | | | |
| A Guest | | | <u>.</u> | | | |
| | | Faiterd | | | | |
| Device Administration | | Specify the password to generate the client certificate | | | | |
| Gertificates | ~ | | | | | |
| System | * | | Cancel Generate Certificate | | | |
| Explore Installed Apps | | | | | | |

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 10-14: Certificate Added

| agni I | ł | | | 1c4d70b3b997.p 2,559 8 - Done | 512 | © 💌 |
|--|---------|---|------|----------------------------------|-----|-----|
| MONITORING | | Generate Client Certificate € в Fill in the details to generate client certificate for the selected client € в | ek . | | | |
| Networks Is Segments AcLs DOMITY | | Generata Certificate: Generate Use CSR Corr te:4d 70 b3 b997 (Sheki/s Linux) | | | | |
| Identity Provider User Client Clients Client Clients Client Client Client Client | • | Shahu Expires on 21/03/2022 Subject DN CN+Shahu, O+local Issuer DN CN+AGN, Issuer CA, O+anista-dev | | | | |
| AT Guest | ÷ | | J | | | |
| Access Devices Device Administration Certificates System | > > > > | Password Specify the password to generate the client certificate Cancel Generate Certificate |] | | | |
| CONCOURSE III Explore IV Installed Apps | | | | | | |

 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 10-15: Certificate - Use CSR Radio Button

| MONITORING | | Generate Client Certificate | |
|-----------------------|---|--|-----------------------------------|
| Dashboard | | Fill in the details to generate client certificate for the selected client | ← Back |
| ✓ Sessions | | | |
| ACCESS CONTROL | | Generate Certificate: O Generate I Use CSR | |
| Networks | | | |
| La Segments | | 1c:4d:70:b3:b9:97 (Shailu's Linux) | |
| ACLs | | | |
| IDENTITY | | A certificate already exists for the selected client. Generate only if required. | |
| (1) Identity Provider | | | |
| Luser | ~ | 😝 Shailu | Expires on 27/03/2025 |
| Client | ^ | Subject DN | CN=Shailu, O=local |
| Clients | | Terring (M) | CNI-ACAN Jacobs CA. O-prints. dau |
| Client Groups | | ISSUEL DIV | CIN-NOIN, ISSUELCA, O=alista-dev |
| 9 Guest | | | ± |
| CONFIGURATION | | | |
| Access Devices | | Select Action: O Upload CSR File Paste CSR | |
| Device Administration | ~ | Poste CSR | |
| Gertificates | ~ | Sample CSR text | |
| System | ~ | | |
| CONCOURSE | | | |
| Explore | | | |
| Installed Apps | | | E |

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:

- Guest Onboarding using AGNI
- Guest Onboarding Offerings in AGNI
- <u>Configuring UPSK for Guest Onboarding (Wireless)</u>
- <u>Configuring Guest Portal Using Guestbook (Wireless)</u>
- <u>Configuring Guest Portal Using Guestbook-Host Approval (Wireless)</u>
- <u>Configuring Guest Portal Using Self-Registration (Wireless)</u>
- Configuring Guest Portal in AGNI for Wired Clients
- <u>Configuring Guest Portal Using Guestbook (Wired)</u>
- <u>Configuring Guest Portal Using Guestbook-Host Approval (Wired)</u>
- <u>Configuring Guest Portal Using Self-Registration (Wired)</u>

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

| 桁 | Ou Mar | est Users | Quest Users | | | | + Add Darest | r legert Quests | 0 Bettings |
|------|-----------|---|---|---|--|--|--|--|---|
| AFUN | vers | Pertal | UPSK | | | | | | • |
| ٩ | Short | ty Containing (| real, Agentive, Name or Company | | | | | Any | |
| 0 | • | USERNAME | CMAL | GUEST APPROVER | TYPE | \$14115 | ACTINATION DATE | EXPIRATION DATE | |
| D | ×. | (Dei | entergetikelikentestjøpslesen | shirangchhadha@ensizcon | Portal | Endled | 29/03/2024 11:10:57 | 06/04/2024 3319-57 | |
| | 7 | Series | sivangchicolian@gnal.com | | Note | Fadded | 20/03/0024 14 55 47 | 05/04/2024 14:55:47 | - |
| | 5 | guestasert | рыторнытри.com | | Portel | Entited | 20/13/2024 11:28:00 | 0%/34/2224 11/28/00 | 1 |
| | | Mill Out Altitutes Image: Constraint of the second | Couldst Users Managet the last of Managet the last of | Cuest Users Manage the list of Cuest Users At Users Until USER Q. Search by Usersens, Dreat, Approve, Name of Company, Cuest Usersens, Dreat, Approve, Name of Company, Image the list of Cuest Users Original Company, Dreat, Approve, Name of Company, Cuest, Cue | Cuest Users Manage the list of Cuest Users Killers Partial USER Quest Users Guest Users Guest Users Quest Users Guest Users < | Cuest Users Manage the list of Quest Users Killers Imma UPSK Q Search by Userses UPSK Q Search by Userses DMAL Guest Admonute 1 Search UMAL Guest Admonute Profile 2 String Stringphatediae/gradicers stringphatediae/gradicers Profile 2 Stringphatediae/gradicers puest/gradicers Profile 3 guest/generation puest/generation Profile | Cuest Users Manage the list of Quest Users Killers Partial UTSK Q Samuel the list of Quest Users OutSC Q Samuel the list of Quest Users OutSC Q Samuel the list of Quest Users OutSC Q Samuel the list of Quest Advances for Questers OutSC OutSC Q Samuel the list of Quest Advances for Questers OutSC Trace Samuel Island Q 1 Samuel the list of Quest Advances Islands Samuel Islands Samuel Islands Instance Q 2 Orreany Samuel Islands Samuel Islands Instance Instance Q 3 Quest Islands Duest Islands Instance Instance | Cubert Users Cubert Users Cubert Users Kitture Immediate Durate Users Immediate Durate Users Immediate Durate Users Kitture Immediate Durate Users UPSK Immediate Durate Users Immediate Durate Users Immediate Durate Users UPSK Immediate Durate Users Immediate Durate Users Immediate Durate Users Immediate Durate Users UPSK Immediate Durate Users Immediate Durate Users Immediate Durate Users Immediate Durate Users UPSK UPSK Immediate Durate Users Immediate Durate Users Immediate Durate Users Immediate Durate Users UPSK UPSK Immediate Durate Users Immediate User | Cuest Users Manage the list of Quest Users + Add Quest Users Killer Partial UTSX Q Search by Userse Quest Agreement Name of Company Partial Q Search by Userse Quest Agreement Name of Company Partial Add Duest Agreement Name of Company Partial Q Search by Userse Construct Name of Company Partial Add Duest Name Despension Q Search by Userse Construct Agreement Name of Company Partial Status Add Duest Name Despension Q Search Construct Agreement Name of Company Partial Status Add Duest Name Despension Q Search Construct Agreement Name of Company Partial Status Add Duest Name Despension Despensintet the status Despension |

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.

| uniture1 | | | |
|--------------------------------|---------------------|---------------|--|
| astýcorçie.com | | | |
| w. | | | |
| guers | | | |
| 004/2024 08:32 PM | 10/54/2024 05 52 PM | Veloty 8 Days | |
| en l'est | | | |
| | | | |
| itional guest user information | | | |

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

| agni I | - | -1 | | | | | | | | | 6 0 0 |
|-----------------|---|----|-----|-----------------------|---|-------------|----------|----------|--------------------------------|------------------------|------------------|
| B Indianal | | 17 | 540 | et Users | and the second se | | | | | 9 Additional as the | attests 0 hilles |
| er tessen | | | - 1 | NM VIX | | | | | | | • |
| W Arturnta | | 9 | | | and here many | | | | | 100 | |
| d and | | | | and the second second | 1946 | NAU ATTRING | 1100 | 1000 | and the local diversion of the | CONSTRUCTION DOCUMENTS | |
| (dartie | | 0 | 1 | (himp | and any built of participation. | | (Marine) | (marked) | 10/14/2014 (1401-14 | Andrew States that and | 11 |
| A manta frantar | | | ĸ. | petad | permanent. | | (term) | (sense | 10.744 (10.94 (0.75) 10 | 10104/2014 (2110) | 11 |
| C mark | | | | | | | | | | | |
| C. town | | | | | | | | | | | |
| £ | 1 | | | | | | | | | | |
| C monate | | | | | | | | | | | |

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

| eose Action 🔘 A33 🔘 Inport | | | |
|--|----------------------|--------------------|--------|
| herad Drig usams | | | |
| 50/54/0004 08:33 PM | 100 0 00 00 00 33 FM | Validity: (# Days) | |
| heine Land. | | | 8 |
| Broke Stampe-gard-using dis | | | |
| runne warramet emailt rame, company, phone, ad | tress, riches | | Sample |

The imported users are listed in the portal user listing.

Figure 11-6: Portal User List

| 19 5 | Auest Users | inere. | | | | | + Add Devil a larger | |
|------|-----------------------------|---|----------------|--------|----------|-----------------------|----------------------|-----|
| *** | | | | | | | | |
| q | of the concernance of the l | | | | | |) (11 | |
| 0 . | summe | 2440, | 0.427 #7952108 | 745 | 19598 | ACTIVITIES DATE | EXPRATO-CASE | |
| | 100 | and any features of the part of | | And | (Bunket) | \$1754276762764418 | NUMBER OF A DISANCE | 1.1 |
| 0 1 | anarit? | the second second second produces to | | (Anna) | Banker | N2104020(16:07:44-07) | 1004.0014.0144.00 | / 1 |
| a • | ata#11 | an any tender conjugations | | (Area) | (based) | 67067679774418 | Notacidate Pressille | / 1 |
| α. | and a | entergretoritar (Appendican | | (here) | (bunne) | Refs (254) (2.4) (8 | No. 1014 (1994) 10 | / 1 |
| 0 1 | | and any structure of speed care | | (here) | (1000) | 10110304214248 | 101040518214214218 | / * |
| 0 . | - | the any Marine Constraint | | (mer | and a | \$215x232x25x25x23 | 10/04/0124 21:42:02 | |
| 0 : | Driven | this angle March angle and some | | (2004) | (bolted) | 10161010121010 | NO43034210930 | / 1 |
| 0 * | gentant | Presidente de la constitución de la | | (mean) | (Deshed) | REPORTED ADDRESS | 1004.0034.00.0210 | |

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 Batch Users

Batch users are created when the administrators have to pre-generate guest user accounts

Keerti Keshav Lingala then introduced the "guest batches" feature, designed for events where administrators want to pre-generate guest user accounts for any events. This feature enables the admins to distribute the login information directly to attendees, bypassing the need for self-registration at a kiosk or portal.

Note: Once the event is over, the batch of accounts expire and is automatically deleted.

Figure 11-7: Guest Batch List

Ξ.

| MONITORING | | - | Batches | | | | | | | - | Add |
|---|----|----|--------------------------------|-----------------|-----------------|-------------|------------|---------------|-----|---|-----|
| Sashboard | | - | Manage the list of Guest Ba | tches | | | | | | - | |
| ACCESS CONTROL | | | | | | | | | | C | |
| Networks Segments | | ٩ | Search by Name, Description of | Usemanie Prefix | | | | | Any | | Ψ. |
| ACLs | | | BATCH NAME | USER COUNT | USERNAME PREFIX | DESCRIPTION | BATCH TYPE | EXPIRES IN | | | |
| IDENTITY | | 3 | Copy of Copy of abc | 200 | abcde- | ~ | Increment | Expired | | 1 | 8 |
| Identity Provider User | | 2 | Copy of abc | 200 | abc- | 82 | Increment | Expires Today | | 1 | 0 |
| Client | 40 | 3 | Copy of abc new | 200 | abc- | 8 | Increment | Expired | | 1 | 8 |
| 🚏 Guest | | э. | Copy of abod | 200 | abcd- | 6 | Increment | Expired | | 1 | |
| 📌 Users | | 5 | Copy of xyz | 100 | xyz- | P | Increment | Expired | | 1 | |
| Portals Ratches | | 6 | abc | 200 | abe- | | Increment | Expired | | 1 | |
| CONFIGURATION | | 7 | xyz | 100 | xyz- | 8 | Increment | Expired | | 1 | |

Note: The batch users list created using this process will not be displayed in the normal Guest Users list of AGNI as the batch users are temporary user accounts created for a specific event for the duration of the event.

11.1.1.2.1 Adding Batch Users

Ξ.

To add batch users, perform the following steps:

- 1. Navigate to Identity > Guest > Batches on the AGNI portal.
- 2. Click +Add button at the top of the screen.
- 3. Enter the following details:
 - a. Batch Name
 - b. Description
 - c. Username Prefix
 - **d.** Batch Type as Random (to generate random guest user accounts) or Increment (to generate incremental user accounts).
 - e. Username Length
 - f. Password Length
 - g. User Count

h.

- i. Portal to which Portal this batch of users will be associated with.
- j. Valid From and Valid To time.

k. Device Limit

Figure 11-8: Adding Batch Users

| ← → 0 0 | 合 ## 0+ https://qa.agnieng.net/agni/identity/guests/batches/new | ☆ | ල 🗄 🕼 ච 📑 |
|--|---|---|-----------|
| Import bookmarka. Getting Started . CloudVision CloudVision myorg1.com | 🛛 A free online intood. 🛛 🔲 Data Generator (CS 👌 Online Data Generat | | ୯ ଡ м |
| MONITORNO Dashbaard Sessions ACCESS CONTROL NACCESS CONTROL NACCESS CONTROL NACCESS CONTROL NACCESS CONTROL NACCESS ACLE DENTITY CALL LUSER LUSER LUSER LUSER CEIENTS | Add Batch Provide the following details to add a new Batch | | |
| Device Administration v | Cancel Add Batch | | 0 |

4. Click the Add Batch button to add the batch users to the selected guest portal network.

The guest user (batch) list is displayed (in this sample image a random list of users are generated):

| IONITORING | | | Empl | oyee Event | | | | 6 800 | |
|--|----------|-----------------|-----------------------|---|-------------------------------|---|--|--------------|----------|
| Dashboard | | | Provide | the following details to update the sele- | cted Batch | | | C Bac | |
| Sessions | | Batch | Name | | | | | Employe | e Even |
| CCESS CONTROL | | | | | | | | | |
| Networks | | Desci | ription | | | | | | |
| - Segments | | Usern | ame pre | fix | | | employe | e-onboarding | -event |
| ACLS | | Batch | Turne | | | | | | andom |
| DENTITY | | Daten | type | | | | | | Property |
| Jdentity Provider | | Usern | ame Len | gth | | | | | |
| User | ^ | Password Length | | | | | | | |
| L Users | | User (| Count | | | | | | 10 |
| 241 User Groups | | Portal | | | | | | kk-guest-por | tal-ne |
| Client | ~ | - Velist Pr | | | y Valid Te | | | | |
| Clients | | 6/9/2 | 025 05- | 42.PM | 6/10/2025 01:42 AM | | Validity: 7 Hours 59 Minutes | | |
| Client Groups | | | | | | | | | |
| at) enem ereeps | | Device 2 | Linit | | | | | | |
| Guest | ^ | | | | | | | | |
| 常 Users | | | | | | | | | |
| Portals | | | | | | | Cancel | Update | EBatci |
| Batches | | Active | Guest | lears for this hatch | | | | Mide Gue | + 11++ |
| INFIGURATION | | Active | oueste | vaera for this batch | | | | Hide oue. | n ose |
| Access Devices | ×. | 0 | | Pul Uniorminum | | | Stat | a - | |
| and a second second | × | 9 | and the second second | by Oseronine | | | 1. Com | | |
| Device Administration | ~ | | # | USERNAME | STATUS | ACTIVATION DATE | EXPIRATION DATE | | |
| Certificates | | - | 1 | employee-onboarding-event-v23hz | Enabled | 6/9/2025 17:42:24 | 6/10/2025 01:42:24 | 1 | 0 |
| Certificates System | ^ | | | | | | | | |
| Certificates System | ^ | | 2 | employee-ophoarding-event-ryk91 | Enabled | 6/9/2025 17:42:24 | 6/10/2025 01:42:24 | 1 | |
| Certificates System Audit Viewer | <u>^</u> | | 2 | employee-onboarding-event-rxk91 | Enabled | 6/9/2025 17:42:24 | 6/10/2025 01:42:24 | 1 | 8 |
| Certificates System Audit Viewer Cicense Self-service Portal | ~ | | 2 3 | employee-onboarding-event-rxk91 employee-onboarding-event-74tku | Enabled | 6/9/2025 17:42:24 | 6/10/2025 01:42:24 | 1 | 8 |
| Certificates System Audit Viewer Cicense Self-service Portal | è | | 2 3 4 | employee-onboarding-event-rxk91 employee-onboarding-event-74tku employee-onboarding-event-f1f3c | Enabled Enabled Enabled | 6/9/2025 17:42:24 6/9/2025 17:42:24 6/9/2025 17:42:24 | 6/10/2025 01:42:24 6/10/2025 01:42:24 6/10/2025 01:42:24 | 1 | 0 |

Figure 11-9: Batch User List

5. Admin can save this list as a PDF file and hand over each user account slip to the guest users as and when the guests arrive for the event.

| | := | Corp | porate Event de the following details to update the | selected Batch | | | | | ← Back | |
|------------------------------|----------|---------------------------|--|----------------|--------|-------------------|----------------------------|---------------|--------------|-----------|
| Sessions | | Batch Name | | | | | | () c | lone | |
| CCESS CONTROL | | Description | | | | | | - | cint all que | et us are |
| > Networks | | Corporate E | vent | | | | | 0.1 | rint all gue | st users |
| Segments ACLs | | Username pr | efix | | | | c | ilo. | elete | |
| ENTITY | | Batch Type | | | | | | | Incre | ement |
| Identity Provider | | Start Index | | | | | | | | 100 |
| User | ~ | Password Ler | ngth | | | | | | | 6 |
| Lusers | | User Count | | | | | | 200 | | |
| zat User Groups | | | | | | | | 1.22 | | |
| | | Portal | | | | | | ki | -guest-port | al-new |
| Client | ^ | Valid From 6/9/2025 05 | 546 PM | 6/11/2025 01:3 | 0 AM | | Validity: 1 Day 7 Hours 43 | Minutes | | |
| Client Groups | | Desire Limit | | | | | | | | |
| Guest | | No Limit | | | | | | | | |
| ouest | | | | | | | | | | |
| * Users | | | | | | | | Cancel | Update | Batch |
| E Portals | | | | | | | | Gunteer | opunt | Daton |
| Batches | A | ctive Guest | Users for this batch | | | | | | Hide Gues | t Users |
| INFIGURATION | | | | | | | | | | |
| Access Devices | × | Q Searc | h by Username | | | | | Status Any | | * |
| Device Administration | ~ | - | | | | | | | | |
| Certificates | Ÿ | | USERNAME | ST | ATUS | ACTIVATION DATE | EXPIRATION DATE | | | |
| System | ^ | 1 | Global-Corporate-Event-User-29 | 19 E | nabled | 6/9/2025 17:46:56 | 6/11/2025 01:30:56 | | 1 | ٥ |
| Audit Viewer | | 2 | Global-Corporate-Event-User-29 | 18 E | nabled | 6/9/2025 17:46:56 | 6/11/2025 01:30:56 | | 1 | ٥ |
| W License | | 3 | Global-Corporate-Event-User-29 | 17 E | nabled | 6/9/2025 17:46:56 | 6/11/2025 01:30:56 | | 1 | 0 |

Figure 11-10: How to Print the Guest List

Figure 11-11: Creating Batch Users from Self-Service Portal

| Manage Clients | | Batches | Internal | | | | | | + | Add |
|------------------|-----|-------------------------------|---------------------|------------------------------|-----------------|------------|---------------------|-------------|---|-----|
| Register Client | | intersept one rector during t | | | | | | | | |
| Wi-Fi Passphrase | | | | | | | | | | |
| QUEST | | | | | | | | Table Table | | |
| Users | Q | Swarth by Name, Description | or Weiernerm Prefix | | | | | Any | | |
| Batches | | | | | | | | | | |
| | 100 | BATCH NAME | USER COUNT | USERNAME PREFIX | DESCRIPTION | BATCH TYPE | EXPILES IN | | | |
| | | Corporate Event | 200 | Global-Corporate-Event-User- | Corporate Event | increment | Expires in T day(s) | | 1 | |
| | 2 | Employee Event | 100 | employee-onboarding-event- | | Random | Expines in 1 day(s) | | 1 | 0 |
| | . 4 | keerthi-batch-1 | 100 | kserthi-event-1 | | Raygort | Express in T-day(s) | | 1 | 0 |
| | 140 | keerthi-batch-2 | 200 | koerthi-event-2 | | Increment | Expires Today | | 1 | |



Note: If you do not have Guest Operator permissions, you will get the following error when you login:

"You are not a Guest Operator. Not authorized for Guest UPSK portal. Contact your administrator for details"

11.1.1.3 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 11-12: Add or Import UPSK Users

| Add or Import Guests Provide the fallowing details to add a new guest user or upliced a file to import guest users. | 4- Book |
|--|-------------------------|
| Choose Action: O Add pomerceer I ActoUPSK user O Import | |
| shrivingchkodkur-usik@gnul.com | |
| 8 Haus | |
| A A A A A A A A A A A A A A A A A A A | •) |
| Additional guest user information | |
| , ma | |
| Testilian | |
| (tereses | |
| Example LLC | |
| Prese | |
| A53916 | |
| (***** <u>-</u> | |
| Test account | |
| | Cancel Add Add and Emul |
| | |

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 11-13: UPSK User Details

| 1 Update Outed User | t abort | | | |
|-----------------------------------|---------|---------------|---------------------------------|----|
| energi tiszbangoszbyrók son | | | Parlaugh (M sode for Title unit | |
| and a second second second second | | | Vitere, brank (Wumber) | |
| O This is a later based good one. | | | ■200 | |
| | | • 0 iw | | ř. |
| (management of the state | 1 | THE PERMIT | 16773第44 | 6 |
| * | | | EIF 2.3 | f |
| Bea (100) | | | | |
| Additional guard user information | | | | |
| Net | | | | |
| teries Demonstat | | | | |
| | | | | |
| Notice 1 | | | | |
| nne Ned actived | | | | |
| | | And Departure | (account) | |

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 11-14: Guest User Registered Successfully



11.1.1.4 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.

| ngni I | E | | | <mark>७ ०</mark> (|
|-------------------------|---|---|---|---|
| MONTORNE | | Guest Users Manage the list of Quest Users as on 09/07/2024 22:50:32 | | C Self-service Portal + Add or Import \$\$ Settin |
| ~ Sessions | | All Dairs Portal UPIX | | |
| Potworks is Segments | | Q. Sauch by Username, Small, Approve, Name or Company . | |) (Any |
| 8 ACLS | | | No data to display | |
| A) Identity Provider | | | | |
| 1 User | | | Manage Guest Settings | |
| Client | * | | | |
| f Guest | | | Ouest Sponsors | |
| t Users | 1 | | Selected user groups can manage only their guest users, | |
| Portals | | | User Droops + | |
| COMPIGURATION | | | | |
| Access Devices | | | Quest Operators | |
| Device Administration | | | Relative to an annual sea annual sea annual sean includes Cast 100% | |
| Certificates | * | | law then | |
| System | 4 | | Overst Sponsors 🧿 Overst Operations 🥥 Service Uniter Concest | |
| CONCOURSE | | | | |
| III Explore | | | These users can use Self-service Portal to manage guests. | |
| C Installed Apps | | | Cancel Update | |

Figure 11-15: Manage Operator Settings

11.1.1.5 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 portalbased 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 11-16: Enable CAPTCHA

| | - New Template | |
|--|---|--|
| E Dashboard | Custerize Guest Portal | + Task |
| A Sessiona | Configuration Dustomization | 💿 Suriett an eximment to update it's appearance. |
| Networks Segments | Portal Name | ARISTA |
| Ø ACLA | Extremente frant Dicktorrung 🙆 Organizational Unar Login 🥥 - | |
| (2) Islantity Provider | Authentication | |
| Continues | Over User to consider the constant of the cons | |
| 🕞 Access Devises 🔗 🛩 | CAPICIA Reality | C)()()() |
| Certificates - | Peer and the telephone terms to UK. | |
| III Explore F Installed Apps | Anogy * Instruction No Limit * | |
| | Astersed User Groups * | |
| | Post-authentication Redirect URL | |
| | Eancel Add Owest Partal | |

Figure 11-17: Guest Login

| ARISTA | 205 |
|---|-------|
| EMPLOYEE OUEST Connect to enjoy free Wi-Fi Enter username Enter password | |
| E M9 T H7 C Enter CAPTCHA Connect By signing in you accept the Terms Of Use, | 0000 |
| | 00000 |

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 11-18: Redirect URL

| agni I AGNI-D | emo | | <u>د</u> (|
|--|-------|--|------------|
| Mourtilies S Dashbeard Sessione ACOTS CONTROL W Networks | | Arista CloudVision Prove Arista CloudVision Prove Arista CloudVision Arista CloudVision | (* fax |
| ACLA | | ver Moschleeversentation/ | • |
| L User | х - х | Canar 🔤 | Verify |
| Access Devices | 4 | | |
| Certificates | * | | |
| Explore Installed Apps | | | |

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 their 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 authorized user groups are allowed to onboard and the rest of the users are rejected access. The admin can configure the re-authentication method and device limit for the guest users.

Additionally, to ensure that an employee do not use any unauthenticated clients for onboarding, the admins can configure the **Authorised Client Groups** feature, wherein only authorized clients are redirected to the captive portal for an organizational user (employee) login and non-authorized clients get rejected



Note: The **Authorized Client Groups** option is compatible only with organizational user login. If you select guest authentication options, AGNI displays an error message: "*Authentication types other than Organizational User Login are not supported when selecting one or more client groups*".

The sample configuration for this portal-based onboarding method is as follows:

Figure 11-19: Organizational User Login

| agni coogle to | əst | | | <u>د</u> و و |
|--|--------|---|---------------|--|
| MONITORING | | Default Customize Guest Portal | € Back | |
| C Sessions | | Configuration | | 💿 Select an element to update it's appearance. |
| Networks Segments ACLs | | Vina Nere Default Annexector Type Operational Table I com | | ARISTA |
| L) Identity Provider | 3 | Authentication | | Organization Legin |
| Client Guest | y y | Organizational User In althemican Over Always ~ | | |
| Access Devices Device Administration | e e | a * | | ୶୶୶ |
| Certificates | > > | Advected User Orouge OperCroup 🔞 Select Authorized User Groups_ | | |
| CONCOURSE | | Autosted Client Orsage ThiComputer (3) Select Authorized Client Occups | • | |
| Installed Apps | | Post-authentication Redirect URL | | |
| Installed Apps | | Post-authentication Redirect URL | Cancel Update | |

You can customize the portal settings such as the background image and color using the Customization tab:

| | | Default | | | | | | 6 | |
|---|---|-----------------------------|-----------------|---------------|----------------------------|-------------------------|------|----|---|
| Dashboard | | Customize Guest Portal | | | | | | | ¢ |
| Sessions CCESS CONTROL | | Configuration Customization | | | Select an element to updat | it's appearance. | | 2 | |
| Networks | | Theme template | | | | | | _ | 1 |
| Segments | | Default | | * | | ARISTA | | | L |
| ACLS | | failed about | | | | | | | L |
| ENTITY | | Page | | | Con | ect to anjoy free Wi-Fi | | | l |
| User | ~ | Background Tunar | mana Color | | | | | | |
| LUSers | | Background Image | | | | land have at an order | | 2 | |
| Client | ~ | Theme Color | #F5A823 | | | | | 2 | l |
| Clients | | Text Color | #4A4AAA | | | (| / /(| 20 | l |
| Client Groups | | Form Color | afffff | | | | | | Ī |
| Guest | ^ | Link Color | #125500 | | | | | | |
| Portals | | Button Text Color | meeree | | | | | | |
| Batches | | Button Border Radius | | | | | | | |
| VEGURATION | | | | _ | | | | | |
| Access Devices | Ŷ | | | Cancel Update | | | | | |
| Device Administration | 8 | | | | | | | | |
| Certificates | * | | | | | | | | |

Figure 11-20: Portal Customization
Below is a sample portal after desired customization is made:

Figure 11-21: Organizational User Login

| ARI | STA | |
|-----------------------------|------------------|--------|
| | | \sim |
| Organiza | tion Login | |
| Enter email address | | |
| Enter password | • | \sim |
| Sut | bmit | |
| By signing in you accept th | he Terms Of Use. | |
| | | C/() |
| | | |

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.



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

Figure 11-22: Guestbook Configuration

| agni myorg1.c | om | | & @ 💌 |
|---|--------|-------------------------------------|--|
| MONITORING | | Customize Guest Portal | (+ Back |
| ACCESS CONTROL | | Configuration | 🕜 Select an element to update it's appearance. |
| Networks ± ± Segments | | Portal Name | ARISTA |
| ACLS | | Guestbook 🔇 | Contract to enjoy free Wir-Fi |
| Identity Provider User | * | Authentication Guestbook | |
| Client | * • | Guest User Re-authenticate Guest | |
| CONFIGURATION | ÷ | Device Limit | ന്ന്ന |
| Device Administration | ~ | CAPTCHA Enabled | |
| System | Ŷ | Post-authentication Redirect URL | |
| « Collapse Sidebar | | Cancel | Add Guest Portal |

The sample portal is as follows:



| ARISTA | 200 |
|---|-----|
| EMPLOYEE QUEST Connect to enjoy free Wi-Fi Enter utername | |
| Enter password | |
| | |
| | |

11.2.2.2 Self-Registration

In this method, the admin can allow the guest users to enroll themselves into the system using the portalbased 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 11-24: | Enable Self | Registration |
|---------------|-------------|--------------|
|---------------|-------------|--------------|

| Customize Guest Portal | |
|---|------------------|
| Configuration Customization | |
| Portal Name | |
| AGNI Guestbook | |
| Authentication Types | |
| Guestbook 🛞 | • |
| | |
| Authentication Guestbook | |
| Authentication Guestbook Default Validity 8 Hours |) |
| Authentication Guestbook Default Validity 8 8 Hours ♥ | Enabled |
| Authentication Guestbook Default Validity 8 Hours Allow Self Registration Approval required for guest access | Enabled Disabled |

Below is a sample portal:

Figure 11-25: Self Registration Login Portal

| Connect to enjoy | / free Wi-Fi |
|---|-----------------------------|
| Enter user name | |
| Enter password | |
| Connect | t |
| Don't have an ac By signing in you accept th | ccount? he Terms Of Use. |

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



| Create An Account | | |
|-------------------|--------|----------|
| User Name | | |
| Email | | |
| Name | | |
| Company | | |
| | Cancel | Register |

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 11-27. HOSt Approval configuration | Figure | 11-27: | Host A | pproval | Configu | iration |
|---|--------|--------|--------|---------|---------|---------|
|---|--------|--------|--------|---------|---------|---------|

| AGNI Gues Customize Gue | tbook est Portal | | |
|----------------------------|---------------------|----------------------|---|
| Authentication Types | | | |
| Guestbook 🚫 | | | |
| Authentication | Guestbook | | |
| Default Validity | | | |
| 8 | Hours 👻 | | |
| Allow Self Registration | | Enabled | |
| Approval required for g | est access | Enabled | |
| Add approvers by: | User Groups | Email Domains | |
| Authorized User Groups | | | |
| Engineering 😣 ap | prover 🛞 Select Au | thorized User Groups | • |
| Quetomize Quest Lie | Fielde | | |
| Customize Guest Os | rielus | | • |

Below is a sample portal:

Figure 11-28: Host Login Portal

| ARISTA | |
|--|--|
| Connect to enjoy free Wi-Fi | |
| Enter user name | |
| Enter password | |
| Connect | |
| Don't have an account? By signing in you accept the Terms Of Use. | |
| | |

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

Following is a sample form:

| Figure | 11-29: | Create a | n Account |
|--------|--------|----------|-----------|
|--------|--------|----------|-----------|

| User Name | |
|----------------|--|
| Email | |
| Name | |
| Company | |
| Approver Email | |
| | |

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

Figure 11-30: Approve Guest

| | Guest User Registration Approval (Dome) > Head | |
|------|--|---|
| NE'M | Arista Cloud Vision AGNI 🔮 -monohydrayn artes Io- Io ne • | |
| | | Guest User approval request |
| | | A quant account is created with the following details: |
| | | Name: Shrirang |
| | | Username: Shri |
| | | Email: shriranqchikodikar+test@umail.com |
| | | Company: shritanuthikodikar@gmail.com |
| | | Notes: shrirangchikodikar@gmail.com |
| | | Device limit: 4 clients |
| | | Valid from: 29 Mar 24 05:49 UIC |
| | | Valid until: 06 Apr 24 05:49 UTC |
| | | To approve the great account, click the following button: |
| | | Approve Guest |

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

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

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

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 Lookup 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

To configure AGNI for UPSK onboarding, 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 11-31: Add Network

| MONITORING | Add Network | |
|---|--|----------|
| Dashboard | Provide the following details to add a new Network | e Baci |
| Sessions | UPSK for Guest | |
| Networks 12 Segments | Connection Type: Wireless Wired | |
| ACLS | upskGuest | |
| L) Identity Provider | Status: Enabled | |
| User | | |
| Client | Authentication | |
| Guest CONFIGURATION | Authentication Type Unique PSK (UPSK) | - |
| Access Devices Device Administration | Allowed Users: O Organizational users only Guest users only | |
| Certificates | The wireless SSID type must be configured as WPA2 only for guest access. Applicable for Arista Wi- | Fi only. |
| CONCOURSE | | |
| Explore | User Private Networks | Enabled |
| Installed Apps | Shared Clients: Disabled | |
| | Enable to make a set of clients accessible to all users. | |

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.

E,

6. Click the Add or Import Guest option to add a UPSK guest.

7. Select the Add UPSK user option.

Figure 11-32: Add UPSK User

| Manage Clients Register Client | Add or Import Guests Provide the following details to add a new guest user or upload a file to import guest users. | ← Back |
|---|---|--------|
| : Wi-Fi Passphrase UESTS ³ Users | Choose Action: O Add portal user O Add UPSK user O Import | |
| | Veldity 8 Hours | |
| | No Limit | |
| | Additional guest user information | ~ |

8. Add the user's email address and click the Add and Email option.

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.

| Co Manage Clients | Update Guest User View guest user details and update the selected guest user | et Back |
|--------------------------------------|---|-----------------|
| USFFI Passphrase OUESTS OUESTS | Energy Mergansk-rupskiguest (#gemail.com Annumer Mergansk-rupskiguest (#gemail.com) OT Tris is a LPSx based guest user. Drupsker Other H Drupsker Drupsker Drupsker B Hours Valid writh: 120/2024 04:36 PM B Hours Valid writh: 120/2024 04:36 PM B Hours Valid writh: 120/2024 04:36 PM B Hours Valid writh: 120/2024 04:36 PM | Verbers lateral |
| | Additional guest user information | |

Figure 11-33: Update Guest User

The following is an example of the email received:

Figure 11-34: Guest Account Registration Success

| Guest User Add Confirmation D Heart | | | | 9 | ß |
|---|------------------------------|--|---------------------------|-----------|---|
| Arista CloudVision AGNI «noreptythagei arista ki» to keenthikenkev-upskguentitigmel.com. + | | | III a 367M (I minute app) | \$ 3 " | I |
| | Guest Accoun | t registered successfully. | | | |
| | Hello keerthik | eshav+upskguest@gmail.com | | | |
| | A unique WI-FI passphrase h | as been created for you. | | | |
| | Use the following passphrase | to connect your client devices. | | | |
| | Wi-Fi Passphrase: p7u | aj7v24e | | | |
| | Device limit: No Limit | | | | |
| | Valid from Date: 03 De | ac 24 16:36 +0530 | | | |
| | Valid until Date: 04 De | ac 24 00:34 +0530 | | | |
| | WiFi Network xyz | QR code file abc | | | |
| | kk-upsk-guest-ssid | kk-upsk-guest-said.png | | | |
| | Scan the network QR code a | nd connect to the wireless network. | | | |
| | This is an automated email | notification. Please do not reply to this message. | | | |
| One attachment + Scanned by Gmail () | | | | | æ |
| | | | | | |

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 RadSec enabled
 - 2. Authentication Server
 - 3. Accounting Server

4. CoA - Enable

Figure 11-35: Configure WIFI UPSK Guest

| * | WiFi ~ | s | SID | | · | | | | |
|--------------|--------------|--------|----------|---------|----------------------|-----------|---------------|--------------|------|
| DASHBOARD | | | | Ch. | nges will restart th | e SSID If | it is on. The | changes will | affi |
| MONITOR | ← upsk | Guest | | | | | | | |
| CONFIGURE | WLAN 🗸 | Basic | Security | Network | Access Control | : | | | |
| TROUBLESHOOT | Name | | | | | | | | |
| FLOOR PLANS | SSID Name * | | | |] | | | | |
| REPORTS | Profile Name | | | | | | | | |
| SYSTEM | upskGuest | | | | | | | | |
| Services | Select SSI | D Type | | | | | | | |

Figure 11-36: WIFI Security

| * | WIFI - SSID |
|--------------|--|
| - | And Grant Obarges will restart the SSO if it is an. The changes will affect all groups and folders using this SSO. |
| | ← upskGuest |
| CONFIGURE | WLAN - Basic Security Network Access Control 1 |
| TROOMLESHOOT | Select Security Level for Associations In the 6 Ord band, will 62 does not support security methods older than WRA2 (WRA2, Open, etc.), Hence, this SSID will not be activated on 6 Ord radios. |
| FLOCE FLARS | WFA2 • O PIX ③ UPIX ① N02.1X |
| REPORTS | UFSK User Frivate Networks. Arr a radio with multiple SDDs to the same VGAR if UPSN Cher Private Networks is enubled for any SSD, the first configured SSD Lakes preference. |
| EVETEM | UTSUSEE (By Lookup) This setting is not estuable because of LiPSK Liner Private Networks is enabled. |
| Sevice | Mitigate WPA/WPA2 Key Reinstallation Vulnerabilities in Clients |

Figure 11-37: WIFI Access Control

| | WiFi ~ | 5 | SID | | | | | | |
|-----------|-----------|---------|----------|---------|-----------------------|----------------|---------------|-----------------|------------------|
| DASHBOARD | | | | Ch | anges will restart th | e SSID if it i | s on. The cha | nges will affec | t all groups and |
| MONITOR | ← upsk | Guest | | | | | | | |
| CONFIGURE | WLAN ~ | Basic | Security | Network | Access Control | : | | | |
| | RADIUS Se | ettings | | | | | | | |

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.

11.3.4 Onboarding the Guest User Using UPSK (QR Code)

This functionality enables guest users to self-register using a guest portal and connect to the Guest network using a QR code or Unique Personal Shared Key (UPSK). For example, users can securely register at the reception or kiosk using a common Tablet device and upon successful registration, a unique QR Code or UPSK is generated, which the users can scan to connect to the Guest Wi-Fi network.

This onboarding process includes the following steps:

- 1. AGNI Admin: Adds a new UPSK portal, customizes the portal as desired, and associate the portal to a UPSK network for guest users.
- **2.** Login: On the day of the event, Guest Operator logs in to the tablet which is provisioned for guest registration and makes it ready for the guests.
- 3. Guest Arrival: The guest arrives at the reception area.
- **4.** Operator Guidance: The receptionist directs the guest to use the provided tablet device for self-registration.
- 5. Registration Information: The guest enters the required registration information on the tablet. The information to be filled is pre-configured by the AGNI admin.
- 6. QR Code Generation: Upon successful registration, the system generates a unique QR code on the tablet's screen.
- 7. QR Code Scanning: The guest scans the QR code using their mobile device.
- 8. Wi-Fi Access: The guest's device is automatically connected to the facility's Wi-Fi network.

11.3.4.1 Adding the UPSK Portal

To add a UPSK portal to AGNI, perform the following stpes:

1. On AGNI dashboard, navigate to Identity > Guest > Portals.

2. Click the +Add UPSK Portal button (highlighted in red).

Figure 11-38: Guest Portal Page

| MONITORING | | Guest Portals | | | | | | + Add Web Port | Add LIPSK Port |
|--------------------------|------|------------------|----------------------------|-------------------------|----|------------|--------|----------------|----------------|
| Dashboard | - | Manage web porta | is and UPSK portals for gu | est access | | | | Contraction | |
| Sessions | | | | | | | | | |
| ACCESS CONTROL | Q | Search by Name | | | | | | | |
| Networks | | | | 2 | | | | <i>2</i> . | |
| ala Segments | | | | | | ARISTA | | | |
| ACLs | | ANS | | ARIS | TA | Tapatan ap | | | ARISTA |
| IDENTITY | | | | (and the second | | in second | \Box | | |
| Identity Provider | | | · 0 | Corporation Corporation | | | 0 | | - · · |
| L User | | | 00 | | | | 00 | <u>a</u> | - |
| Client | ~ 6 | | 0000 | | | | 2000 | - | 200 |
| 🖗 Guest | × De | fault | | GuestOnly | | Portal New | | | |
| CONTRACTOR IN CONTRACTOR | | | · · | TOCYCS. | | 1000.000 | | | |

- 3. Enter the required details and customize the portal settings (See the sample screenshot here):
 - a. Default Validity (in hours or days): time for which the user remains connected to the Wi-Fi network.



- b. Device Limit: number of clients or devices that can simultaneously connect to the network
- **c.** SMS Gateway (optional): configure if you want to receive the passphrase over SMS to the user's mobile device.

| | | | | | | | с (| 9 | - |
|------------------------|--------|--------------------|---------------------------|-----------------------------|---|--------|----------------|------|-----|
| MONTORNO | | | Test-UPSk Customize UP | (SK Guest Portal | | | (| ← Bi | acl |
| CESS CONTROL | | Configur | ation C. | ustomization | Select an element to update it's appearance | | 2 | | |
| Networks | | Test-U | ns PSK | | < Welcome Page | | | | |
| ACLS | | Detaur V 8 | wary . | Hours • | ARISTA | | | | |
| A) Identity Provider | ~ | Deveration 10 | M | * | Webows to Govern Registration | ~ | < | | |
| Client Guest | * | SMS Ger Twillio | sms GW QA ti | at * | A space on and M long in the | | ر س | | |
| ft Users | | Custo | mize Guest Us | er Fields | • | \sim | 2 | | |
| Batches | | | Display | Field Label | Mandatory | 200 | 20 | | |
| Access Devices | 2 | н | | Usemame | | | _ | - | |
| Device Administration | ~ ~ | 8 | | Name | | | | | |
| System | × | | | Company | | | | | |
| Explore Installed Apps | | н | | Address | | | | | |
| | | н | | Notes | | | | | |

Figure 11-39: Adding UPSK Portal

4. Customize the look and feel of the portal using the Customization tab, if required.



Note: The AGNI admin can select a UI element displayed in the preview on the right side and update. The preview is available on both laptop and tablet devices.

Figure 11-40: Adding UPSK Portal-Customize page

| | ost | | G @ 🕒 |
|--------------------------|---------|---------------------------------|--|
| MONITORING | | Customize UPSK Guest Portal | € Back |
| ACCESS CONTROL | | Configuration Customization | 💿 Select an element to update it's appearance. |
| Networks #1= Segments | | Default | C Display OR Page > |
| ACLS IDENTITY | | Salati demant | ARISTA |
| Identity Provider | | rage | Scal QR to connect to WPI |
| LUSET | | Global | |
| Client | * | Logo | |
| R Guest | | Page | |
| 1 Users | | Terms of Use and Privacy Policy | |
| Portals | | Guest | |
| Batches | | Additional Instructions | They all states with the |
| CONSIGNIBLATION | | Finish Button | |
| Access Devices | | Page Close Message | |
| Device Administration | 100 | Scan QR code instruction | |
| Certificates | | Self Registration | |
| Rustam | 52545 C | Start Button | |
| CONCOURSE | set. | | |
| III Explore | | | Cancel Update |
| Installed Apps | | | |

Figure 11-41: Adding UPSK Portal - Customization

| 090i ‱ | st | | | େ ଡି |
|-----------------------|----|-----------------------------|------------------|--|
| Dashboard | | Customize UPSK Guest Port | at | |
| Sessions CONTROL | | Configuration Customization | | 🔘 Select an element to update it's appearance. |
| Networks | | Default | | C Display OR Page > |
| ACLS | | Select element | | ARISTA |
| Identity Provider | | Page | | Scan QR to connect to W/Fi |
| User | | Background Type: | Image O Color | |
| Guest | | Background Image | - | |
| 📌 Users | | Theme Color | #B8E588 📕 | |
| Portals Batches | | Text Color | #000000 i | |
| ONFIGURATION | | Form Color | HEREFEF 📋 | |
| Access Devices | * | Link Color | #2174E9 | |
| Device Administration | * | Button Text Color | #000000 iii | |
| System | × | Button Border Radius | | |
| Explore | | | Cancel | pdate |

11.3.4.2 Adding a Wi-Fi Network

To add a Wi-Fi network to the UPSK portal, perform the following steps:

- 1. On AGNI portal, navigate to **Access Control** > **Networks**.
- 2. Add or edit a network.

- 3. Enter details as described in the Configuring AGNI sub-section under the Configuring UPSK for Onboarding Guest section.
- 4. Select Guest Users only under Allowed Users and select the guest UPSK portal that you created in the previous section.

| | | | ୯ ଡ 🍝 |
|-----------------------------|--|--------------|-------|
| MONTORNG | 🔷 test-upsk-qa-nw | ← Back | |
| Dashboard | Provide the following details to update the selected Network | | |
| ✓ Sessions | Connection Type: Writers | | |
| ACCESS CONTROL | 100 | | |
| Networks | test-upsk-qa | | |
| 414 Segments | | | |
| CLs CLs | Status: Enabled | | |
| IDENTITY | | | |
| 3 Identity Provider | Authentication | | |
| 🚨 User 🗸 🗸 | , American Tpe | | |
| 🛄 Client 👻 | Unique PSK (UPSK) | * | |
| 📌 Guest 🛩 | | | |
| CONFIGURATION | Allowed Users: O Organizational users only Guest users only | | |
| Access Devices 🗸 🗸 | Construction of the second sec | | |
| 🖸 Device Administration 🗸 🗸 | Compare the writers solo type as write only to guest access. Application for Artiste Write only. | | |
| Gertificates 🗸 🗸 | Select Own UPSC pints | | |
| System v | Luan Dran | | |
| CONCOURSE | | | |
| III Explore | User Private Networks | Disabled Orm | |
| Installed Apps | | | |
| | O Enable to prevent clients belonging to different users from communicating with each other. | | |
| | Guest UPSK Portal | | |
| | O Use the following URI: to allow guests to self-register for UPSK-based network access. | | |
| | https://hext.agnieng.net/onboard/ | Сору | 0 |

Figure 11-42: Add UPSK Network

- 5. Copy the Guest UPSK Portal URL and paste it to another browser window.
- 6. Login with your Guest Operator credentials.



Note: If you do not have Guest Operator permissions, you will get the following error when you login:

"You are not a Guest Operator. Not authorized for Guest UPSK portal. Contact your administrator for details."

Figure 11-43: Self Service Portal Login Page

| n In | | | | |
|----------|---------------|---------------------------------------|-----------------------|-----------------------|
| or Email | | | | |
| | Procee | d | | |
| | | | | |
|) | J n In | J n In D or Email Procee | o or Email Proceed | D or Email Proceed |

After successful registration, the following window is displayed:

Figure 11-44: Click to Register Now



11.3.4.3 Registering Guest Users (Self-Register)

To self-register (Guest users), perform the following steps :

- 1. Click the **Register Now** button on the Welcome to Guest Registration window.
- 2. Enter the required details, such the email address, phone number (optional) and click the Register button.

Note: You receive an email with the passphrase to connect to the network (see sample image below). If you had added the phone number, you receive an SMS with the passphrase.

AGNI also displays a QR code indicating that the registration is complete.

- 3. Using your mobile device, scan the QR code to connect to the Wi-Fi network.
- 4. Click the Finish button.

| - |
|---|
| - |
| |

Note: The QR code remain visible for 60 seconds if you do not click the Finish button and after which the screen changes to the Registration page for next user.

Figure 11-45: Self Registration Email Sample

| Guest user updated successfully. | | | |
|----------------------------------|---|--|--|
| | Hello | | |
| | Your account is updated with the following credentials: | | |
| | Username: agni-interview-we9ib | | |
| | Password: | | |
| | Device limit: 3 | | |
| | Valid from: 06 May 25 09:00 +0530 | | |
| | Valid until: 08 May 25 17:00 +0530 | | |

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

After all registrations are completed, the Guest Operator or an authorized person can logout (using the icon on the far right top corner) from the page to ensure network security access.

11.3.5 Authenticating Guests via SMS Auth

In the SMS-based authentication process, a guest's identity is verified by AGNI sending a one-time password (OTP) to their mobile phone via SMS. Guest can enter the received OTP to complete the login process.

Pre-requisite:

- · Configure at least one SMS gateway.
- AGNI admin should configure the OTP requirements such as number of digits, OTP expiry interval.

To configure SMS gateway, perform the following steps:

- 1. On AGNI dashboard, navigate to Identity > Guest > Portal.
- 2. Click the +Add Web Portal button.
- 3. Add a Portal Name.
- 4. Select SMS Auth for Authentication Types and enter the relevant details.

Figure 11-46: Configuring SMS Gateway

| ONITORINO | | New Template | (t Ba |
|--------------------------|----------|-------------------------------|---|
| Dashboard | | Customize Guest Portal | |
| Sessions CESS CONTROL | | Configuration | 💿 Select an element to update it's appearance. |
| Networks | | Portal Name | |
| Segments | | SMS-Auth | |
| 401+ | | Authentication Types | ARISTA |
| ACLS . | | SMS Auth 🙁 | |
| Identity Provider | | | Connect to unjoy free WI-FI |
| | | Authentication SMS Auth | |
| User | Č. | INS Getawar | in the second |
| Client | × . | MSG Test-1 * | |
| Guest | | | |
| t Users | | Default Country Code | |
| Portais | | | 0000 |
| - Batchice | | Optioner | |
| date batteries | | 5 | |
| NEIGURATION | | | |
| Access Devices | × . | Logn Code Validity Period | |
| Device Administration | × | 5 Minutes | |
| Certificates | . | Max Attempts to Senared IME | |
| System | | 5 | |
| ONCOURSE | | Mic. Interval to Reserve 3MIS | |
| | | 30 Seconds | |

5. Click the Add Web Portal button.



Figure 11-47: Error Message to Configure Guest OTP

| agni Google te | st | | O Guest OTP template is not configured for the selected SMS Gateway. To configure it, <u>click herce</u> X |
|---|-----------------------------------|-------------------------------|--|
| MONITORNO | - | Customize Guest Portal | (€ Back |
| ACCESS CONTROL | | Configuration Customization | 💿 Select an element to update it's appearance. |
| Networks Alla Segments | | SMS-Auth | |
| C ACLS | | Authentication Types SMS Auth | ARISTA |
| (A) Identity Provider | | | |
| 1 User | v | Authentication SMS Auth | |
| Client | ~ | IMS Getwee | |
| 📌 Guest | | M5G-105(-1 | |
| 📌 Users | | Default Country Code * | |
| Portais | | Optional | |
| = Batches | | Login Code Langth | |
| CONFIGURATION | | 5 | |
| Access Devices | ~ | Logn Code Validity Period | |
| Device Administration | Υ. | 5 Minutes | |
| Gertificates | арын (С. 1997) Солон (С. 1997) | Max Attempts to Sesand SMD | |
| System | | 5 | |
| CONCOURSE | | Mrc. Interval to Resard SMS | |
| III Explore | | 30 Seconds | |
| III Installed Apps | | | Cancel Add Web Portal |

- 6. On the right side of the page, click an element. The relevant details are displayed on the left side of the page. Update the details as desired.
- 7. Click the **Update** button after entering required all details.

11.3.5.1 Registering Guest Users

To self-register (Guest Users), perform the following steps:

When a guest user clicks on the **Register** button on the **Welcome Guest Portal** page, the OTP page is displayed.



| Conne | ect to enjoy free \ | Vi-Fi |
|----------------|----------------------------|-------|
| ≭ +91 ▼ | Enter phone number | × |
| | Send OTP | |
| / signing in y | ou accept the Terms Of Use |). |

- 1. Enter the mobile number and click the **Send OTP** button.
- 2. Enter the received OTP.

The guest gets connected to the Wi-Fi network.

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 11-49: Identity Guest Portals

| ရီရိုဂ်၊ ၊ | | | | | | | & Ø | - |
|-----------------------|-----|---|---|--|--|--------------------|----------|----------|
| MONITORINO | | Guest Portals Manage the list of Gue | at Portais | | | + Add Guest Portal | ¢ Emails | Settings |
| ACCESS CONTROL | | Q Search by Name | | | | | | |
| Networks | | | | | | | | |
| 4)1 Segments | | | and the second se | | | | | |
| O ACL | | ARIS | TA | | | | | |
| IDENTITY | | | | | | | | |
| (4) Identity Provider | | | | | | | | |
| 1 User | * | · · · · · · · · · · · · · · · · · · · | | | | | | |
| Client | ~ | * | 00 | | | | | |
| ft Guest | ^ | | 0000 | | | | | |
| ft Users | | Default | 10 | | | | | |
| Portals | 1 | - | | | | | | |
| CONTIQUEATION | | | | | | | | |
| Access Devices | | | | | | | | |
| Device Administration | . w | | | | | | | |
| 🕞 Certificates | | | | | | | | |
| System | | | | | | | | |
| CONCOURSE | | | | | | | | |
| Explore | | | | | | | | |
| F Installed Apps | | | | | | | | |

- 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 11-50: Configure Guest Portal - Guestbook

| 000i I | - | s @ 🔹 |
|--|--|---|
| Montenen 11 Decklaure 24 Sections | New Template Dustanize Genet Partal Orefigenetian Custanization | 🖉 Serect an element to update its appearance. |
| Actuality Webuchs Bagewebs ACLs Gentry | Partit Norta Nettoria Nort Gambox Qui X • | ARISTA |
| ★ Manetzy Provider ↓ Unor v Gener v ∰ Genert n | Charrouge Charrouge Cognitional Charloge Charlos | |
| 1 Overs | As Lint * Carcel Add David Parts | |

- 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 11-51: Re-authenticate Guest Periodic

| ũg∩i I | |
|--|---|
| MONITORING Dashboard Sessions ACCESS CONTROL | Customize Guest Portal Configuration Customization |
| Networks If Segments ACLs | Portal Name Authentication Types Cuestbook |
| Aldentity Provider ▲ User ✓ Client ✓ ✓ | Authentication Guestbook Guest User Ite Authenticates Paried Periodic * Onvice Line * |
| CONFIGURATION | Cancel Add Ouest Portal |

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

Figure 11-52: Device Validity

| | Customize Guest Portal |
|---|-------------------------------------|
| Sessions | Configuration Customization |
| Networks | Portal Name |
| ACLS | Authentication Types Guestbook 😒 |
| Identity Provider User | Authentication Guestbook |
| Client | × B Days ▼ |
| ∰ Users | Allow Self Registration Disabled |
| Portals | Cancel Add Guest Porta |

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

E,

- 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 11-53: Customization Settings

| agni I | | | 6 Ø 😬 |
|--|---|---|--------|
| MONTORNS | Rew Template Customize Guest Portal | | é liek |
| ** Sessions Accessions Accessions Segments Segments Contry Sessions Sensity Provider Cont Cont for Osers Overs Pretais | Configuration Configu | Seter an element to update it's appearance. | |
| Controutstrion Access Devices Device Administration Certificates System Audit Viewer C Loonse Self-service Pertal | Thet Color Cong C | | |

Figure 11-54: Additional Customization Settings

| agni I | | | | | | s | 0 (|
|---|---|-----------------------------|-----------------|------------------|--|---|-----|
| MONTRENS | - | Customize Guest Portal | | | | | (B |
| Ar Sessions | | Configuration Customization | | | Select an element to update it's appearance. | | č. |
| Networks Segments | | Trains require Default | | | | | |
| @ ACLs | | Mad general | | | ARISTA | | |
| A Identity Provider | | Page | | | Consect Vi signs file 30.6 | | |
| 1 000 | ٣ | Background Type. | mage Color | | O | | |
| Client ff Guest | × | Background Image | · · | | 00 | | |
| 🖅 Users | | Theme Color | #417980 | | ନନ୍ନ | u | |
| CONTIQUEATION | | Text Color | #AAAAA | | | | |
| Access Devices | * | Form Color | #171012 | | | | |
| Device Administration Certificates | ž | Link Color | #125900 | | | | |
| O System | | Button Text Color | | | | | |
| B Audit Viewer | | Button Border Radius | | - | | | |
| License Self-service Portal | | | Cancel | Add Guest Portal | | | |
| C RadSec Settings | | | | | | | |
| U Support Logs | | | | | | | |
| System Events | | | | | | | |

8. When done, click Add Guest Portal.

The portal gets listed in the portal listing.

Figure 11-55: Add Guest Portal

| õğni I | | | | 6 Ø 🕚 |
|--------------------------------|-----|------|---|--------------------------------------|
| saverer 🗶 saverity Provider | | ۲ | Cuest Portals Manage the list of Guest Portals | + Add Quest Partial Q Email Settings |
| 1 User | | | | |
| Circl | - | Q | earch by Name | |
| ST Corret | ^ | | ANISTA | |
| D Portais | - 1 | | | |
| CONTEURATON | | | | |
| Access Devices | * | | 00 | |
| Device Administration | ÷. | 1.11 | | |
| Certificates | * | | | |
| C System | * | | | |
| 00400.838 | | | | |
| E Capiere | | | | |
| 📅 Installed Apps | | | | |

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

Figure 11-56: Add or Import Guest

| Construction Const Users Const Us | 5 |
|---|---|
| Al Dians | - |
| Polyands Q. Spech to Dimension, Unal, Approve, Name of Dimanry, Any | |
| C. Acia | • |
| Restore No defaits display | |
| A sately reveale | |
| Clear v A Goust A | |
| f Usen | |

- **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 11-57: Guest User Settings

=

| လီရီက်၊ ၊ | | | |
|--|------|---|-----------|
| MONITORINO Dashboard Sessions ACCESS CONTROL Networks ACLS CONTROL ACLS CONTRY ACLS CONTRY CONTRY Contry Client | * * | Provide the following details to add a new guest user or upload a file to import guest users. | |
| ff Guest 위 Users 回 Portals | ^ | 4 Additional guest user information | • |
| CONFIGURATION | ebar | Cancel Add Add | and Email |

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 11-58: Added Guest

| agni I | | | | | | | | | \$ | ۲ | 3 |
|--|------------|--------|----------------------------------|-----------------------------|----------------|-------|---------|---------------------|------------------------|-------|--------|
| Mawrooms Desidecard | 1 1 | Gu | vest Users mage the list of O | uest Users | | | | + 444 | Quest or Import Quests | 0 let | inga (|
| ACCESS CONTROL | ABS | 26era | | IPSK | | | | | | | 18 |
| Networks Segments | ٩ | Search | n by shorname, Br | nal, Azərbəri, Nəmə a' Cəri | sang | | | | Alv | | • |
| O ACLA | | | LISCENAME | DMAIL | QUEST APPROVER | TYPE | STATUS | ACTINATION DATE | EXPRATION DATE | | |
| Klentity Provider User | • | 3 | questusert | perdeurps con | | Porst | Entited | 20/23/2024 11:28:00 | 85/04/2024 11/28/00 | / | • |
| Client f [*] Guest | ž | | | | | | | | | | |
| ff Users 18 Fartula | 1 | | | | | | | | | | |

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

Figure 11-59: Edit System Generated Password

| ONITORING | Update Guest User View guest user details and update the selected guest user | ← Back | | | |
|------------------------------|---|-----------------|--|--|--|
| | | | | | |
| Sessions | Union - | | | | |
| ISS CONTROL | guestuser1 | | | | |
| P Networks | | | | | |
| Segments | Puter - | | | | |
| ACLA | | (] Ceby | | | |
| | first . | | | | |
| | guest@example.com | | | | |
| , Identity Provider | Area - | | | | |
| User | | | | | |
| Client | AUNI OVESTOOR | | | | |
| Cuest o | Changing partial will updated validity and device limit. | | | | |
| | Vertices | | | | |
| R Users | 28/03/2024 11:28 AM | Valcity: B Days | | | |
| 10 Portals | | | | | |
| 22 | Device Lind | | | | |
| FIGURATION | 6 | | | | |

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 11-60: Export User Details

| agni I | - | | | | | | | | | G | • | 3 |
|-----------|---|-----|---------|--------------------------------|--------------|----------------|--------|---------|---------------------|----------------------------------|----------|----|
| Cient | ^ | 稻 | Gue | est Users ope the list of C | luest Users | | | | + | Guest or Import Guests | Ø Sertin | 91 |
| Clevis | | ALU | - | Pertal | UPSK | | | | | | | 18 |
| # Guest | ~ | | Actions | Contra | Report | | | | One Duest Parts | with current filter is selected. | Carect | |
| g Dars | 1 | 2 | | USERSAME | EMAL | DUEST APPROVER | 1115 | STATUS | ACTIVATION DATE | EXPERITION DATE | | |
| D Periodo | | 8 | 1 | (sestant) | pengeunpicon | | Porter | Ensteed | 20/23/2024 11 28:00 | 05/54/2024 11 28:00 | 1 | • |

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 11-61: Add Network

| S Carbort | Add Stelwork Protect the following default is well a new following | (* Text |
|---|--|----------|
| W beating | for any harmon | |
| · Inconte | Constants Type () Works () West | |
| P Alla | Los 108 | |
| V Marries Provider | Data (Sent) . | |
| 1 100 - | | |
| Class v | American | |
| C track | , tester la | |
| (window) with the second se | Lasterbein | |
| Denta Merinaturian - | Californi (Lor Sarrisona 🖉 Internel 🔘 Enternel | |
| Cambune v | #P#Sarbox | · Perior |
| D Fysteen | | |
| (m), so and | | |
| E Eulers | Capital Parta | |
| 17 Installed Apart | No for the interview | |
| | hua car | |
| | | |

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 11-62: Configuring | Role Profile |
|---------------------------|--------------|
|---------------------------|--------------|

| Network Profiles ~ Role Profile |
|---|
| |
| ← portal-role |
| Profile Nerre* Specific Settings |
| Role Specific Settings |
| VLAN 0 VLAN Name (0 → 4094) (0 - 4094) |
| + Firewall |
| User Bandwidth Control |
| Unit the maximum upitad bandwidth per user to |
| C Mbps V [1-1024] |
| Redirection |
| 🔿 Static Redirection 💿 Dynamic Redirection |
| HTTPS Redirection |
| Certificate Information |
| Common Name Organization Organization Unit |
| www.arista.com Arista Networks Arista Networks |
| Websites That Can Be Accessed Before Authorization * |
| (Infrumoniationine.com/8240 X) (askidronitastront/8240 X) |
| androhmsevtynet.80,443 X kgin.for.com.80,443 X |
| nprest.sgriorg.ret.\$3,443 🗙 |

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.

Provide the SSID Name - Guest SSID.
 Figure 11-63: Guest SSID

| WiFi ~ | s | SID | | | | |
|----------------|--------|----------|---------|---|--|--|
| ← Gues | t SSID | | | | | |
| WLAN ~ | Basic | Security | Network | : | | |
| Name | | | | | | |
| SSID Name * | | | | | | |
| Guest SSID | | | | | | |
| Profile Name * | (| | | | | |
| Guest SSID | | | | | | |
| | | | | | | |

Select SSID Type

Private
 Guest

Hide SSID

Include AP Name in Beacon

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

- 6. Select RadSec.
- 7. Select the Authentication and Accounting servers.

Figure 11-64: Authentication and Accounting Servers

| WiFi ~ SSID | |
|--|--|
| Guest SSID | |
| NLAN - Basic Security Network Access Control : | |
| > Firewall | |
| Olient Authentication | |
| Google Imegration ③ RADIUS MAC Authentication | |
| ADIUS Settings | |
|) RadSec | |
| Primary Addisonal | |
| | |
| rhertikation Server * | Accounting Server |
| unar synam agreeg an | About Value of About Abo |
| Send DHCP Options and HTTP User Agent | |
| etry Parameters | |
| 4 C [1 - 10] | 2 Seconds [1 - 10] |
| Isername and Password | |
| NCT-14714 | |
| MAC Address without Delimiter | |

- 8. Select the Role-Based Control checkbox and configure the following settings:
 - a. Rule Type 802.1X Default VSA
 - **b.** Operand Match
 - c. Role Portal.

You have created the **portal-role** role profile while configuring the Role Profile in the previous section. **Figure 11-65: Portal Role**

| WAN • Basic Security Network Access Control Accounting Stop Delay Ident Authorization Fab. Desconnect Stay connected Role Based Control Basic Spa* 402 XX Defsu2 YSA Couple CO This setting in not extrable because Clere Authenotation sur Google imagration is distabled Courge Set Basic Spa* Axingn Role * • 402 XX Defsu2 YSA Couple CO This setting in not extrable because Clere Authenotation sur Google imagration is distabled Courge Set But provide Table pertail-role (portal role) • • DHCP Fingerprinting based Access Control • • Bonjour Gateway • Redirection • | | | | | |
|---|--|----------------------------|----------------------------|--------------------------------|----------------|
| Accounting Stop Delay Clerit Authorization Fab. Obscorrect Stay corrected Role Based Control Datauts VSA Couple CO This setting is not editable because Over Authorization site Google importation is disabled Owage Set Role Type * | AN V Basic Security Netwo | Access Control | • | | |
| Start Authoritation Fab Disconrect Stay connected RADIUS VSA Couple CO This setting is not edivable because Cherr Authoritation we Google integration is disabled. Charge Set Radio Type * #00_1X Default VSA Operand * Match State State * DHCP Fingerprinting based Access Control Bonjour Gateway Redirection | Accounting Stop Delay | | | | |
| Role Based Control BADRUS VSA Couple CO This setting is not editable because Client Authensization six Google integration is disabled. Charge Set But type * | Isent Authorization Fails Disconnect O Stay connected | | | | |
| RADIUS VIA Completion This setting is not editable because Cliere Authentication site Google integration is disabled. Charge Setting is a construction in the Google integration is disabled. Rule type * #02.1X DetauX VSA • • • Month • persul cole (portal cole) • • DHCP Fingerprinting based Access Control • • • • Bonjour Gateway Redirection • • • • | Role Based Control | | | | |
| Rule Type* 402.1X.Oetsuk VSA Operand * Assign Role * Mittch DHCP Fingerprinting based Access Control Bonjour Gateway Redirection | RADRUS VSA Oscipli DU TNS M | tting is not editable beca | use Olere Authensization W | Google integration is disabled | Change Setting |
| Access Control Bonjour Gateway | Aule Type * | | | | |
| Operand * Axign Role * Match DHCP Fingerprinting based Access Control Bonjour Gateway Redirection | R02.1X Debuit VSA | | | | |
| Math | Operand * | Assign Role * | | \odot | |
| DHCP Fingerprinting based Access Control Bonjour Gateway Redirection | Match 👻 | portal-role (porta | l ruie) 🗸 🗸 | | |
| Redirection | DHCP Fingerprinting based Acc Bonjour Gateway | ess Control | | | |
| | Redirection | | | | |
| WiFi Clients in Allow List or Deny List | WiFi Clients in Allow List or De | ny List | | | |

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 11-66: Identity Guest Portal

| agni I | | | | | | | | ¢ | ۲ | ۲ |
|-------------------------|-----------|---|-----------------------------|----------------|--|--|--------------------|-----|---------|---------|
| MONTORNO | | Guest Portals Manage the first of Overst Portals | | | | | + Add Guest Portal |)(• | Email S | rttings |
| ACCESS CONTROL | Q | Search by Name | | | | | | | | |
| · Notworks | - Chanter | | | | | | | | | |
| ala Segmenta | | | | | | | | | | |
| O ACL | | | ARISTA | 7.5 | | | | | | |
| KORNTITY | _ | ARISIA | Connect In action has NO P. | | | | | | | |
| 😩 Identity Previder | | ityenster team | (***** | | | | | | | |
| 1 User | - 10 C | (the red data | (fermal) | ~ | | | | | | |
| Client | 4 | | | \mathcal{O} | | | | | | |
| f Overt | A | 000 | And and and a second second | 000 | | | | | | |
| ST Users | | | \sim | $n - \alpha c$ | | | | | | |
| 🕀 Portala | De | daut / 0 | test | 10 | | | | | | |
| CONFIDURATION | | | | | | | | | | |
| Access Devices | w | | | | | | | | | |
| C Device Administration | ÷ | | | | | | | | | |
| E Certificates | | | | | | | | | | |
| C System | | | | | | | | | | |
| CONCOURSE | | | | | | | | | | |
| Explore | | | | | | | | | | |
| IP Installed Apps | | | | | | | | | | |

- 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 11-67: Configure Portal

| agni I | | | େ ୭ 😬 |
|---|--|--|---------|
| MONTORNO | New Template Customize Curst Portal | | (· Back |
| - Sessions | Configuration Customization | Select an element to update it's appearance. | |
| Notworks Segments Acts Acts | Answer Tach ADN Answerschen Generace () | ARISTA | |
| ☆ Identity Provider ⊥ User □ Client ☆ Guest ☆ Users ⊕ Portails | Authentication Overthook Authentication Verthook Authentication Authentication Authentication Authentication | | |
| Colencousantox Access Devices Centice Administration Centificates Controlouse Controlouse Equire Finitatied Apps | Cancel Add Guest Purter | | |

- 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 11-68: Update Portal

| agni | | | | |
|-----------------------|-----------------|-------------------------------------|---------|----------|
| MONITORING | Cu | est-AGNI stomize Guest Portal | | |
| ✓ Sessions | | | | |
| ACCESS CONTROL | Portal Name | | | |
| Networks | Test-AGN | 21 | | |
| ⊥ ⊥ Segments | Authenticati | on Types | | |
| ACLS | Guestbo | ok 🔞 | | × |
| IDENTITY | | | | |
| (2) Identity Provider | Authentic | cation Guestbook | | |
| 🚊 User | V Default Valid | Ry | | |
| Client | ~ 8 | Days 👻 | | |
| 49 Guest | | | | |
| N1 Guest | Allow Self F | registration | Enabled | |
| ☆위 Users | Approval re | quired for guest access | Enabled | |
| Portais | Add appro | vers by: 💿 User Groups 🔘 Email Doma | ns | |
| CONFIGURATION | | | | |
| Access Devices | ~ Authorize | d User Groups | | * |
| Device Administration | ~ | | | |
| Cartificates | Customi | ze Guest User Fields | | ^ |
| | Display | Field Label | Ma | andatory |
| System | × | User Name | | - |
| CONCOURSE | | | | |
| :::: Explore | | Email | | - |
| Installed Apps | - | | | |
| | | Name | | |
| | | Company | | • |
| | | Phone | | ò= |
| | | Address | | |
| | | Notes | | • |
| | | Approver Email | | 0- |

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 11-69: Customize Portal

| agni I | |
|--|---|
| MONITORING | Test-AGNI Customize Guest Portal |
| Sessions ACCESS CONTROL | Configuration Customization |
| Networks ± ± Segments | Default ~ |
| ACLS | Select element |
| (a) Identity Provider | Page |
| Oser Oser | Global Login Form |
| 祝 Guest | Login Toggle |
| 州 Users 回 Portals | Logo Page Terms of Use and Privacy Policy |
| CONFIGURATION | Guest |
| Device Administration ~ | Guest Login Header |
| Certificates | Password Textbox |
| CONCOURSE | User Name Textbox Self Registration |
| iii Explore | Clickthrough |
| :> instance Apps | |

9. When done, click Add Guest Portal.

The portal gets listed in the portal listing.

Figure 11-70: Guest Portal Added

| agni I | | | | | | | | | ¢. | 0 | |
|---------------------------------|----|------|--|-------------|--------|--------|---|---------------|-----|---------------|---|
| Kalenter 🗶 Malenter Provider | | ۲ | Guest Portals Manage the list of Guest Portal | | | | E | Add Coast Par | • • | Erail Setting | • |
| 1 User | | | | | | | | | | | |
| Circl | ÷ | 9 | bearshity Norse | | | | | | | | |
| f Comt | ^ | | ARISTA | | ARISTA | | | | | | |
| D Portes | | | | | - | 0 | | | | | |
| Access Devices | ×. | | 00 | | | 00 | | | | | |
| Device Administration | ÷. | 4114 | | 24 Declared | 0 | 167670 | | | | | |
| Certificates | * | | / 0 | | | · •) | | | | | |
| C System | ÷. | | | | | | | | | | |
| 00400.038 | | | | | | | | | | | |
| II Capitre | | | | | | | | | | | |
| 📅 Installed Apps | | | | | | | | | | | |

11.5.2 Configuring the Network

For details, see the <u>Configuring the Network</u> section above.

11.5.3 Configuring CV-CUE

For details, see the <u>Configuring CV-CUE</u> 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 11-71: User Onboarding

| er Innere brack - Booligh Balder Taglings | | | | | |
|--|---------------------------------------|--|--|--|--|
| Notes that the second sec | - Second Second | News New Control Contr | | | |
| Signal. | | Seat Service | artyria (Lanca) | | |
| Gaussi . | - constitution from the | Strain Intel Total | 3819304 p.m. 447 | | |
| 1 ~·· | 12 mil | | hee | | |
| Missee | Accession . | | No annual | | |
| • market (1997) | a week | . Tana | | | |
| A Real Print Sea (Print | ette hannen • hannen hydrachete | | | | |
| Tayat Respirat Aminose | ×. | Intel Report Holder | | | |
| | | Second Conference of the second of the | maniferent averagen er antannin inn hill die Solast Norson (19 maar. | | |
| | | Name of Party and Party an | Automaticate | | |
| | | Nexa CP Technical Adver | | | |
| Internation Statements | | | (| | |
| | | | | | |

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.

| ARISTA | |
|--|--------|
| Connect to enjoy free Wi-Fi | |
| Enter user name | |
| Enter password | |
| Connect | |
| Don't have an account? By signing in you accept the Terms Of Use. | |
| | |
| | |
| | \sim |

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

Figure 11-73: Create an Account

| User Name | |
|----------------|--|
| Email | |
| Name | |
| Company | |
| Address | |
| Notes | |
| Optional | |
| Approver Email | |

- 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 11-74: Onboarded User Details

| M Institut Infalls - Bacillitation/Devilent | | | • |
|---|--|---|--|
| Antoninaan sananaan jaj Sagani Sasan | interna Jacobie Maria | Search Room Specific Assess Search Technic Technic Technic | andra 1 Andra 1 Andra 1 |
| k Sectors (1997) | D Sectors S | | Anne |
| Age Bages (reduce) | | Sept September March 1996 March 1996 Natural 1997 Sept 1 | n bester begetet net en an en de menser be |

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 11-75: Guest Portal

| ရီရီဂ်၊ ၊ | | | | | | | | େ ଡ | - |
|---|-------|------------------------------------|---------------|-----|--|--|--------------------|---------|----------|
| MONITORINO | | Guest Portal Manage the list of | Guest Portals | | | | + Add Guest Portal | ¢ Email | Settings |
| ACCESS CONTROL | | Q Search by Name | | | | | | | |
| Networks Segments AcLs Control Sedentity Provider User Client Client Guest Y' Users | * * * | Default | | 007 | | | | | |
| Portals | 1 | - | | | | | | | |
| CONTIQUEATION | | | | | | | | | |
| Access Devices | * | | | | | | | | |
| Device Administration | | | | | | | | | |
| Gentificates | * | | | | | | | | |
| System concourse | ~ | | | | | | | | |
| Explore | | | | | | | | | |

- 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 11-76: Guest Portal Settings

| àgni I | - | s @ 💿 |
|---|---|-------|
| Montpano El Centaned M Sensions | New Template Contantee Geest Partia Orfigentian Custanteadon | 🖉 🔤 🖉 |
| Norbuchs Supremb Als Descript Desc Clost Ver Clost Ver Clost v ff Gast n ff Users Postala | Perta Nore Ametodor Nor Gamtook 1 | |
| ccanocaanoa cc Collepse Salebar | Cancel Add Queet Partial | 0 |

Figure 11-77: Guest Portal Settings

| Dashboard | | lew Template | tal | | |
|--|------------|------------------------|-------|----------------------------|---------|
| Sessions | Configura | ation Customiza | ation | | |
| Networks Segments | Portal N | lame | | | |
| ACLS | Authentic | stion Types XXXXX 😵 | | | ÷ |
| Jdentity Provider | Authent | cication Guestb | ook | | |
| Client | Guest Use | Bf Hicate Quest | | , Re-Authentication Period | |
| Guest | Periodic | 1 | * | 12 | Hours 👻 |
| 帮 Users | Device Lin | ÷. | | | |
| Portals | 4 | | • | | |

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

Note: The **Allow Auto Login** option is displayed only if the **Allow Self Registration** option is enabled.

For additional details, see the Configuring Guest Portal Using Self-Registration (Wireless) document.

- a. User Name
- **b.** Email
- c. Name
- d. Company
- e. Address
- f. Notes

Figure 11-78: Guest Portal User Fields

| ← → C O | Ef Or https://jaa.agnieng.net/agni/identity/puests/portals/280 Anter onlore introd. Data Generator (CS | ☆ © ± @ £ ≅ |
|---|---|--|
| agni myorg1.com | | & @ 😖 |
| MONITORING | Customize Guest Portal | ← Back |
| ACCESS CONTROL | Configuration Customization | Select an element to update it's appearance. |
| Networks La Segments AcLs IDENTITY | Perial Name Kk-guest-portal-new Authentication Types Clickthrough O Organizational User Login O Guestbook O SMS Auth O * | |
| Identity Provider User ^ Users User Groups | Authentication Ouestbook SMS Auth | |
| Client ^ | Twillo SMS GW QA | - de de |
| 橋 Guest へ 州 Users ■ Portals | Allow Auto Login Enabled Approval required for guest access Disabled | |
| Batches | Cancel Update | |
| Access Devices V Device Administration V | | |

Figure 11-79: Sample Screen for Guest Auto-Login

| Customize Quest | I User Fields | | ^ | | Gelect an eleme | ent to update it's app | earance. | | <u> </u> |
|--|-----------------|------------|-----------|---|-------------------------------------|------------------------|-------------|-----------------------|-----------|
| Display | Field Label | | Mandatory | 1 | | | | | |
| 8 | Ernolt | | -0 | | 1.11 | ARIS | TA | | |
| H 🛂 | Usemane | | | | | Connect to and | o the Wi-fi | | 6 |
| II 🖬 | Name | | 0- | | | (100.0000 | | | \supset |
| II 🖬 | Company | | | | | | <u> </u> | | 0 |
| H 🖬 | Phone | | | | | A special in second 1 | and an | 0 | Ő. |
| H 🖬 | Address | | | | | | C | $\delta \hat{\sigma}$ | ->0 |
| H 🖬 | Notes | | | | | | | | |
| low Self Registrati | ion. | Enabled - | | | | | | | |
| low Auto Login | | Grabled -0 | | | | | | | |
| llow Auto Login pproval required fo | or quest access | Grabled - | | | | | | | |



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:
 - 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 Textbox
 - c. Password Textbox
 - d. Guest Login Header
 - e. Guest Login Form
 - f. Self Registration

g. Clickthrough

Figure 11-80: Guest Portal Customize

| 9 | | |
|--|---|---|
| Dashboard | Customize Guest Portal | |
| Sessions ACCESS CONTROL | Configuration Customization | |
| Networks 414 Segments | Default | • |
| ACLS | Select element | |
| (Identity Provider | Page | |
| 🛓 User | ✓ Global | |
| Client | ✓ Login Toggle | |
| ∱ Guest | Logo | |
| f Users | Page Terms of Use and Privacy Policy | |
| Portals | Guest | |
| CONFIGURATION | Guest Login Form | |

Figure 11-81: Guest Portal Customize

| ENTITY | Customize Guest Portal | |
|---|--|---|
| L User | Configuration Customization | |
| P Guest | Default | Ť |
| Portals | Select element | * |
| Access Devices Device Administration Certificates | Guest Guest Login Form Guest Login Header | Î |
| System V ONCOURSE | Guest Login Submit Button Password Textbox User Name Textbox | |
| installed Apps | Self Registration Clickthrough | |

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

Figure 11-82: Guest Portal Added

| 000 i | | | | | | | 6 Ø O |
|---|---|--------|--|--------|---------------|--------------------|-------------------|
| Control (2) Sources Provider | | C | uest Portals arage the list of Guest Port | 44 | | + Add Overal Parts | d 🗘 Enal Settings |
| Clevel | 1 | Q, 144 | th by Name | | | | |
| f Comt | ^ | | ARISTA | 5 | | | |
| | | | | 3 🗖 | - 22 | | |
| Device Administration Certificates | - | AON DA | es/box | Owland | - 0000 / 8 | | |
| C) System | • | | | | | | |
| II Capitore | | | | | | | |

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 <u>Configuring CV-CUE</u> 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 11-83: Identity Guest Portals

| agni I | | େ ୭ 🕑 |
|---|--|---------------------------------------|
| MONTORNO Controlend Sessions | Cuest Portals Manage the list of Guest Portals | + Add Ovest Portal 🗘 C Email Settings |
| Access Control. | | |
| Vises Vises Vises Vertals Ver | | |

- 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 11-84: Configure Portal

| ରଗୁଁମାଁ । | | | 6 Ø (|
|--|-------|--|--|
| MONTORNO | | New Template Customize Guest Portal | (e) had |
| ACCESS CONTROL | | Configuration Contamization | 💿 Select an element to update it's appearance. |
| Networks Segments ACLS EXECUTY | | Australian | |
| Weentity Provider User Client Guest | , c e | Authentication Overst User Organizational User Logn Anneys Overstition Overst User Overst User Overstition Oversti | |
| Portals | | | Cancel Add Genet Partal |
| Access Devices | * | | |
| Certificates | ÷ | | |
| System CONCOLINE | а. | | |
| Explore | | | |

- 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 11-85: Customize Portal

| agni I | | | | | 6 | 0 😬 |
|-----------------------|--|----------------|----------------------|---|-------------|--------|
| MONTORNS | Customize Guest Portal | | | | | é Back |
| 💉 Sessions | Configuration Contomization | | | Select an element to update it's appearance. | PO Z | |
| ACCESS CONTROL | Contraction of the local division of the loc | | | | Seal of the | |
| V Networks | Prana templana | | | | | |
| Ja Segments | Default | | * | the second se | | |
| ACL. | | | | ARISTA | | |
| DENTITY | hind served | | | | | |
| (2) Identity Provider | Page | | | Contract to adapt free 28.0 | | |
| ± User | The second second second | 0 mm | | A Maria and A Maria and A Maria | | |
| Client | eacepound type. | C maps () coos | | | | |
| f Guest | Background Image | | | 001 | | |
| 17 Users | Theme Color | #417980 | | 0000 | | |
| E Portais | | | | | | |
| CONTIQUEATION | Text Color | | | | | |
| Access Devices | Form Color | writter | | | | |
| Device Administration | Tink Color | applied | | | | |
| G Certificates | | | | | | |
| System | Button Text Color | wiiiiii | | | | |
| concounte | Button Border Radius | | | | | |
| Explore | | | | | | |
| IF Installed Apps | | Can | cel Add Quest Portal | | | |

When done, click Add Guest Portal. The portal gets listed in the portal listing.
 Figure 11-86: Add Guest Portal

| agni | | | | | |
|---|---------|---|-----|-------------|--|
| MONITORING Dashboard Sessions | | uest Portals anage the list of Guest Portals | | | |
| ACCESS CONTROL Powerks 2 2 Segments ACLS | Q Sea | ch by Name | | | ARISTA |
| IDENTITY (2) Identity Provider (2) User | | Organization Login Trior end states | 0 | | Connect to enjoy free Wi-Fi Count Drages in su many in laws (File. |
| 🛄 Client 桁 Guest | * | National Reporting in particular from 20 cm | 000 | | |
| ☆ Users | Default | (| | Guest-wired | |

- 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 11-87: Copy URL

| | | Guest-wired Provide the following details to update the selected Network | ← Back |
|-----------------------|---|--|-------------|
| ~ Sessions | | , Kane | |
| CCESS CONTROL | | Guest-wired | |
| Networks Segments | | Connection Type: O Wireless Wired | |
| ACLS | | Access Device Group | - @ |
| JENTITY | | Select an Access Device Group to make this Network applicable only to a subset of Access Devices, Multiple Networks can't be linked to the same Access Device Group. | |
| User | ~ | Status: Enabled Control Status | |
| Client | v | | |
| Guest | ^ | Authentication | |
| 招 Users | | Automotication Type Captive Portal | 1 |
| INFIGURATION | | Captive portal type: Internal External | |
| Access Devices | ~ | Test-AGNI-Docs | - Preview |
| Device Administration | ~ | | |
| Certificates | ~ | | |
| System | * | Captive Portal | |
| DNCOURSE | | West ACL For Forty Authentication | |
| Explore | | guest-acl | Show Domain |
| Installed Apps | | Configure the following URL as captive portal in the initial role, to allow users sign in. | |
| | | https://qa.agnieng.net/portal/Ea613f9d9-2a76-44d3-ba16-2e27e944e045/network/810 | |

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.

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).

agni I G 0 **RadSec Settings** ACLs \$. (1) Identity Provider RadSec Server 1 User RadSec Server Hostname radsec.qa.agnieng.net Client CON () Use the above server as RadSec(TLS) RADIUS server in your Network Access Devices 🚍 Access Devices Devices RadSec CA Certificate Expires on 04/06/2035 🗁 Device Groups Subject DN CN=ISRG Root X1, O=Internet Security Research Group, C=US Cloud Gateways Issuer DN CN×ISRG Root X1, O=Internet Security Research Group, C=US Device Administration ~ 🖶 Certificates () Use this CA certificate to validate the RadSec(TLS) server certificate System <u>*</u> Audit Viewer Q License Portal Settings RadSec Settings Support Logs C System Events

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)

| agni I | | | ଓ ୭ 🕒 |
|-----------------------------|--|------------|-------|
| C ACLS | Provide the following details to update the selected Device | ← Back | |
| (a) Identity Provider | Chane | | |
| 1 User | at-aruba-ap | | |
| | MAC Assess a8:bd 37:c5:a8:a2 | | |
| Access Devices | , Wedar | | |
| Devices | Aruba | * | |
| 📄 Device Groups | Carlar Number | | |
| Cloud Gateways | | | |
| Device Administration | IP Address | | |
| 🖶 Certificates | | | |
| System | Access Device Group | - 🛞 | |
| Audit Viewer | Optional | | |
| License Portal Settings | Location | 0 | |
| RadSec Settings | Optional, example: Global/America/California/Site-1 | | |
| Support Logs | RadSec Connection Status: Not Connected | | |
| CONCOURSE | You can generate a RadSec client certificate for this Access Device. | ertificate | |
| Explore | | | |

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

| agni I | | د. د | 0 | в |
|---|---|---------|---|---|
| AcLs DEXITY Identity Provider User Client Constouration Access Devices Devices Devices Devices Devices Devices Cloud Gateways | Cenerate RadSec Client Certificate Cenerate RadSec Client certificate for the Access Device Fill in the details to generate RadSec client certificate for the Access Device Cenerate Certificate: Generate Certificate: Cenerate Outpload Zip with multiple CSRs Access Device Password DNS Names | | | |
| Device Administration Certificates System Audit Viewer CLicense | Optional, specify DNS Names one per line Cancel Generate Certificate | | | |
| Portal Settings RadSec Settings Support Logs System Events | | | | |

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 |
|--------|-------|--------|---------|
| | | | |

| Coopril I | | ୯ ଡ 💿 |
|--|--|-------|
| ALL Segments | at-aruba-ap Provide the following details to update the selected Device | |
| Client Y | VHC ANYH | |
| Access Devices ^ Devices Device Groups Cloud Gateways | Veda Auba * | |
| Device Administration Access Policy | (P-Address | |
| TACACS+ Profiles | Access Device Group * 💿 | |
| System ^ | Location | |
| Audit Viewer Q License Portal Settings | Optional, mample: Obtablickensroal/California/Star-1 Rad/Sec Connection Status: Not Connected | |
| RadSec Settings SupportLogs System Events | You can generate a RadSec client certificate for this Access Device. Get Client Certificate | |
| CONCOURSE | Cancel Update Device | |
| Explore | RadSec Connection Logs Show Logs | |

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** \rightarrow **Certificates** \rightarrow **Trusted**. Then, click on **Settings** to view the details of AGNI certificates.

| agni I | | | | | હ | ¢ | 0 | |
|---|---|---|----------|----------|-------------------|----------|------|-------|
| MONITORINO | Trusted Certificates Details of the Certificate Authorities trusted | by Arista CloudVision AGNI | | | + Add Certificate | • | Sett | lings |
| ACCESS CONTROL | All Certificates Internal External | | | | | | | 88 |
| Networks | Q. Search by Subject or insuer details | | | | | | | |
| ACLS | # SUBJECT | | | TYPE | VALIDITY | | | |
| IDENTITY | 1 CN+AGNI, Issuer CA, O+atulacme | | | Internal | 30/06/2026 | ± | • | 0 |
| Identity Provider User | 2 CN=AGNI, Root CA, Osatulacme | Certificate Settings | | Internal | 30/06/2033 | <u>+</u> | • | D |
| 🖵 Client 🗸 | 3 CN=AntaraAl Intermediate CA, OU=Antara | View expiry settings for all Internal certificates. | | External | 20/03/2032 | <u>*</u> | 1 | 8 |
| | 4 CN=AntaraAl Root CA, OU=AntaraAl Certif | Client Certificate (EAP-TLS) Validity: | 1 year | External | 17/03/2042 | ± | 1 | 8 |
| Access Devices | 5 CN+Example Certificate Authority, O+Exam | Server Certificate Validity: | 3 years | External | 26/04/2024 | <u>*</u> | 1 | |
| Certificates | 6 CN+External Certificate Authority, O+Exan | ssuer Certificate Validity: | 5 years | External | 23/06/2024 | | 1 | 8 |
| Trusted | 7 CN=External1 Certificate Authority, O=Exa | Root Certificate Validity: | 10 years | External | 15/07/2024 | * | 1 | 8 |
| 🖸 System 🗸 🗸 | 8 CN+agni_scale_ca, O+Arista Networks, L+ | | Close | External | 16/07/2033 | ŧ | 1 | 8 |
| III Explore | | | | | | | | |

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

| agni I | | | | | | ତ ଡ |
|---|-----|---|---------------------|------------------------|---------------------|---------------------------|
| MONITORING | | | Access Device Group | ps ^{IS} | | + Add Access Device Group |
| ✓ Sessions | | | | | | |
| Networks Alls Segments | | ٩ | Search by Name | | | |
| ACLS | | | NAME | DESCRIPTION | UPDATE TIME | |
| IDENTITY | | 1 | AT-WIRED-CP | | 10/09/2023 22:58:59 | / 8 |
| Identity Provider User | ÷ | 2 | AT-WIRED-EAP | | 17/11/2023 01:12:57 | / 0 |
| Client | ~ | 3 | AT-WIRED-MBA | AT-WIRED-MBA | 12/09/2023 23:10:24 | / 0 |
| CONFIGURATION | | 4 | Imported | Imported | 06/12/2023 05:33:55 | / 8 |
| Access Devices | ^ | 5 | Systest-Kaveen | LLDP VSA in Accounting | 14/09/2023 21:50:06 | / 0 |
| 📄 Device Groups | 1 | | | | | |
| Cloud Gateways | | | | | | |
| Device Administration | 1 v | | | | | |
| 🖶 Certificates | • | | | | | |
| CONCOURSE | | | | | | |
| III Explore | | | | | | |

• 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

| | | | G | , (0) | |
|---|--|--------------------------------|---|-------|--|
| Segments AcLs DONTRY Control Contro Control Control Contr | Add Access Device Group Provide the following details to add a new Access Device Group New | (+ Back | | | |
| ± User ~ | Test | | | | |
| Client Y | Description Test | | | | |
| Access Devices | | | | | |
| Devices Device Groups Cioud Gateways | Access Devices Available Devices Assigned Devices | | | | |
| Device Administration | Q Bearch by Name, MAC Address or Location | | | | |
| C Access Policy | | (Selected 0) | | | |
| TACACS+ Profiles | a8.bd:27.c5:a8:a2 at-aruba-ap | + A65 | | | |
| Certificates ~ | 0 44-20-30-83-18-6f Jun-AP-Home | + 444 | | | |
| Audit Viewer | 0 44.20.50/41.87.9f Jun-AP-Office | + AM | | | |
| License Portal Settings | 0 30:86:24:92:54:91 Abu-C200 | (+ 444 | | | |
| C RadSec Settings | 28:e7:1d:ca:01:4b at-arista720dp | + Add | | | |
| Support Logs | axbbcc:ddee:76 | (+ Ass | | | |
| CONCOURSE | Access Devices belonging to other groups will be reassigned to this Device Group, if selected. | | | | |
| Installed Apps | | Cancel Add Access Device Group | | | |

Chapter 13

Overview - TACACS Plus with AGNI

This section explains the process of configuring TACACS+ with AGNI. Before configuring TACACS+ with AGNI the administrator should first configure the Arista Cloud Gateway (ACG) solution, which provides greater security in accessing the public internet. The Arista Cloud Gateway solution integrates with AGNI over secure web sockets.

The following image illustrates that Arista Cloud Gateway enables the TACACS+ proxy implementation to terminate the TACACS+ protocol on-premise and transport the TACACS+ information as HTTPS payload to AGNI cloud.

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

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





Any Vendor Switch/Router

13.1 Configuring Arista Cloud Gateway on Arista Switches

Get the latest version of the SWIX extension from Arista Software Download page. On the Software Download page, navigate to EOS (Tab), scroll down to Extensions --> AGNI \rightarrow latest version and download the SWIX extension

Follow the CLI configurations below to install Arista Cloud Gateway on EOS switches:

```
Copy the Arista Cloud Gateway file to the system flash:
scp .\AristaCloudGateway-1.0.2-1.swix
admin@192.168.1.10:/mnt/flash
copy flash:AristaCloudGateway-1.0.2-1.swix extension:
extension AristaCloudGateway-1.0.2-1.swix
show extensions
daemon AristaCloudGateway
exec /usr/bin/acg
option AGNI_API_TOKEN value <token from AGNI>
no shutdown
```

| _ | - 1 |
|---|-----|
| _ | _ |
| - | - |
| | 10 |

Note: If you reload the switch, the SWIX extension gets uninstalled unless you copy the extension to the boot-extension using the command:

```
copy installed-extension boot-extension
```

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

Figure 13-2: Installing SWIX extension on EOS Switch

| IN-MH04-PL-SW02 (config) #daemon Ari | staCloudGateway | | | | | | |
|--|--|---------------------------|--|--------------------------------------|--|--|--|
| IN-MH04-PL-SW02 (config-daemon-Aris | taCloudGateway) #exec | /usr/bin/act | a . | | | | |
| IN-MH04-PL-SW02(config-daemon-Aris ExNi0xODI1NzU0MjBj2mIiLCJ0b2t1bk1E | taCloudGateway)#optic IjoiRURDTFMwU0JTSVFNV | n AGNI API KM3M1MISKNO | TOKEN value eyJhbG MCIsImlzcyI6IkFHTk | GCIOIJFUZIINIISI KKILCJhdWQIOIJBC | InR5cC161kpXVCJ9.ey Q0cgRGV2aWN11FRva2V | JvcmdJRCI6IkViYTYx: uliwi2XhwIjoiMjEyMi | ZDE40S11MZYxLTQ4MzctY1 10xMS0xOFQwNzozOToyNy4 (XR1 |
| | | | | | | | M08 |
| youzxoirx0.JjtBvkrFnikg/iLuetiNF-V | nsmsP21pAzQym0L3FT_Fq | R/bcyt9as5B. | 104FnkPJeBx8JESrT/ | TUFASLYL_18PW | | | |
| This is an Reedly application | cacioudsaceway) eno sn | lucdown | | | | | |
| Full agent name is 'acq-AristaClou | dGateway! | | | | | | |
| IN-MH04-PL-SW02 (config-daemon-Aris | taCloudGateway) | | | | | | |
| IN-MH04-PL-SW02 (config) #show exten | sions | | | | | | |
| ! No extensions are available | | | | | | | |
| The extensions are stored on inter | nal flash (flash:) | | | | | | |
| IN-MH04-PL-SW02(config)#copy flash | :AristaCloudGateway-1 | .0.0-1.swix | extension: | | | | |
| Copy completed successfully. | | | | | | | |
| IN-MH04-PL-SW02 (config) extension | AristacloudGateway-1. | 0.0-1.SW1X | | | | | |
| IN-MNU4-PL-SWU2 (CONIIG) #Show exten | Varsion/Palassa | SFATUR | Extension | | | | |
| | | | | | | | |
| AristaCloudGateway-1.0.0-1.swix | 1.0.0/1 | A, I | | | | | |
| A surflikle i MA, and surflikle i | | | and a second | | | | |
| C. valid eignature NC. invalid e | in instanted Fi to | TOAG D: TI | ibtail at boot | | | | |
| The extensions are stored on inter | nal flash (flash:) | | | | | | |
| | | | | | | | |

Figure 13-3: Installing Arista Cloud Gateway on EOS Switch



The below snapshot displays the logs indicating that the daemon is listening on port 49:

Figure 13-4: Arista Cloud Gateway Daemon Listening on Port 49

| agni-720dp48-1(config-daemon-AristaCloudGateway)#no_shutdown |
|---|
| This is an EosSdk application |
| Full agent name is 'acg-AristaCloudGateway' |
| agni-720dp48-1(config-daemon-AristaCloudGateway)#trace monitor acg |
| Monitoring /var/log/agents/acg-AristaCloudGateway-8965 |
| 2023/12/06 08:21:22 DEBUG [swix] acg service started |
| 2023/12/06 08:21:22 DEBUG [swix] AGNI_API_TOKEN(md5sum) : 19c3f3b4136e7919ca126b7158aaeb40 |
| 2023/12/06 08:21:22 DEBUG [swix] ENABLE_DEBUG_LOG : false |
| 2023/12/06 08:21:22 DEBUG [swix] AGNI_ACG_TACACS_PORT : 49 |
| 2023/12/06 08:21:22 DEBUG [swix] AGNI_ACG_ENABLE_DHCP : false |
| 2023/12/06 08:21:22 DEBUG [swix] AGNI_ACG_VRF : default |
| 2023/12/06 08:21:22 DEBUG [swix] acg service started [pid=8989] |
| 2023/12/06 08:21:24 INFO acg - dhcp module is disabled |
| 2023/12/06 08:21:24 INFO tacacs - started gateway at 0.0.0.0:49 |
| 2023/12/06 08:21:24 INFO websocket - connected successfully to wss://qa.agnieng.net/acg/connect |

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

option AGNI_ACG_TACACS_PORT value <port_no>

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

Figure 13-5: Running TACACS+ on non-standard Port

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

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

option AGNI ACG VRF value <vrf name>

Figure 13-6: CLI - Non Default VRF

Ξ.

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

Figure 13-7: CLI - Trace Monitor ACG

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

13.2 Configuring Arista Cloud Gateway on AGNI

To configure Arista Cloud Gateway on AGNI:

1. Navigate to Configuration > Access Devices > Cloud Gateways.

2. Click +Add Cloud Gateway button to add a new cloud gateway to AGNI.

Figure 13-8: Adding a New Cloud Gateway

| Cloud Gateway-1 | | |
|--|--|---------|
| Location San Jose | | 0 |
| ptional, example: Global/America/California/Site- | 4. | |
| CACS+ Termination | | Enabled |
| evices must use any of the TACACS+ shared so help manage shared secrets, provide a name SHARED SECRET NAME | ecrets added here to connect to the Cloud Gateway. along with its value. VALUE | |
| | ······· • | × |
| AristaSwitch | | |

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

5. Click Update Cloud Gateway.

Figure 13-9: Updating the Cloud Gateway

| loud Gateway-1 | | | | |
|--|---|------------|-----|--------------|
| ocation | | | | |
| an Jose | | | | 0 |
| otional, example: Global/America/California/Site-1 | | | | |
| Not Connected | | | | |
| incetion status. | | | | |
| Copy the generated token into the Cloud | Gateway. | | | |
| sken | | | | |
| | | | | 1011 |
| 4 | | | | V4 |
| y. | | | | VH. |
| y. CACS+ Termination | | | | Enabled |
| y. CACS+ Termination | | | | Enabled |
| y. CACS+ Termination vices must use any of the TACACS+ shared set | crets added here to connect to the Clou | d Gateway. | | Enabled |
| y. CACS+ Termination vices must use any of the TACACS+ shared set help manage shared secrets, provide a name a | crets added here to connect to the Clou long with its value. | d Gateway. | | Enabled |
| y. CACS+ Termination vices must use any of the TACACS+ shared set help manage shared secrets, provide a name a SHARED SECRET NAME | crets added here to connect to the Clou long with its value. VALUE | d Gateway. | | Enabled |
| y. CACS+ Termination vices must use any of the TACACS+ shared set help manage shared secrets, provide a name a SHARED SECRET NAME | crets added here to connect to the Clou long with its value. VALUE | d Gateway. | | Enabled |
| y. CACS+ Termination rices must use any of the TACACS+ shared set help manage shared secrets, provide a name a SHARED SECRET NAME AristaSwitch | crets added here to connect to the Clou- long with its value. VALUE | d Gateway. | 0 | Enabled |
| y. CACS+ Termination rices must use any of the TACACS+ shared ser- help manage shared secrets, provide a name a SHARED SECRET NAME AristaSwitch | crets added here to connect to the Clou- long with its value. VALUE | d Gateway. |) © | Enabled X |
| X- XACS+ Termination ices must use any of the TACACS+ shared set telp manage shared secrets, provide a name a HARED SECRET NAME AristaSwitch | crets added here to connect to the Clou long with its value. VALUE | d Gateway. | | Enabled |
| ACS+ Termination ices must use any of the TACACS+ shared served melp manage shared secrets, provide a name a HARED SECRET NAME AristaSwitch | crets added here to connect to the Clou- long with its value. VALUE | d Gateway. |) © | Enabled |

For security reasons, the generated token is visible only for the first time on AGNI portal. NC Ensure to copy and save the token when it is generated.

6. Click the **Regenerate** button to generate a new Token (see image):

Figure 13-10: Regenerate Token

| Name | | | |
|--|--|-------|---------------|
| Cloud Gateway-1 | | | |
| Location - | | | ٥ |
| ptional, example: Global/America/California/Site-1 | | | |
| nnection Status: Not Connected | | | |
| To change the token used by the Cloud Gateway cu | urrently, click the 'Regenerate' butto | n.s | |
| Regenerate | | | |
| ACACS+ Termination | | | Enabled |
| vices must use any of the TACACS+ shared secrets adde | ed here to connect to the Cloud Gat | eway. | |
| help manage shared secrets, provide a name along with | its value. | | |
| SHARED SECRET NAME | VALUE | | |
| AristaSwitch | | • | × |
| | | | ≓+ Add Secret |
| | | | |

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

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

Figure 13-11: Regenerate Token Process

| Cloud Gateway-1 Provide the following details to update the selected Cloud Gateway | ← Back : |
|---|----------|
| Cloud Gateway-1 | |
| Location | 0 |
| Optional, example: Global/America/California/Site-1 Connection Status: | |
| To change the token used by the Cloud Gateway currently, click the 'Regenerate' button. | |
| Regenerate | |

Figure 13-12: List of Cloud Gateways

| | Cloud Gateways | | | | + Add Cloud Gateway |
|---|-----------------|----------|--------|---------------------|---------------------|
| | | | | | |
| ٩ | Search by name | | | | |
| | NAME | LOCATION | STATUS | UPDATE TIME | |
| 1 | Cloud Gateway-1 | | • | 01/12/2023 23:05:38 | / 8 |
| 2 | Cloud Gateway-2 | San Jose | ٠ | 01/12/2023 23:05:20 | / 0 |
| з | Home ACG | | • | 01/12/2023 00:51:50 | / 0 |

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

13.3 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

13.4 Debug commands on Arista Cloud Gateway

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

| agni-720dp48-1(conf | ig-daemon-AristaCloudGateway)#trace monitor acg |
|---------------------|---|
| Monitoring /var | /log/agents/acg-AristaCloudGateway-26882 |
| 2023/12/01 16:53:47 | INFO websocket - connected successfully to wss://qa.agnieng.net/acg/connect |
| 2023/12/01 17:13:35 | DEBUG [swix] handling agent shutdown/no shutdown: False |
| 2023/12/01 17:13:35 | DEBUG [swix] stopping acg service |
| 2023/12/01 17:13:35 | DEBUG [swix] restricting port : 49 |
| 2023/12/01 17:13:35 | DEBUG [swix] restricted port : 49 |
| 2023/12/01 17:13:35 | DEBUG [swix] acg service stopped |
| 2023/12/01 17:14:12 | DEBUG [swix] handling agent shutdown/no shutdown: True |
| 2023/12/01 17:14:12 | DEBUG [swix] allowing port : 49 |
| 2023/12/01 17:14:12 | DEBUG [swix] allowed port : 49 |
| 2023/12/01 17:14:12 | DEBUG [swix] setting-up acg service. wait for 10s |
| 2023/12/01 17:14:22 | DEBUG [swix] starting acg service |
| 2023/12/01 17:14:22 | DEBUG [swix] acg service started |
| 2023/12/01 17:14:22 | DEBUG [swix] AGNI API TOKEN(md5sum) : 831ca11c87f65ae90764c1ddf07e8e29 |
| 2023/12/01 17:14:22 | DEBUG [swix] ENABLE DEBUG LOG : false |
| 2023/12/01 17:14:22 | DEBUG [swix] AGNI ACG TACACS PORT : 49 |
| 2023/12/01 17:14:22 | DEBUG [swix] AGNI ACG ENABLE DHCP : false |
| 2023/12/01 17:14:22 | DEBUG [swix] AGNI ACG VRF : default |
| 2023/12/01 17:14:22 | DEBUG [swix] acg service started [pid=32154] |
| 2023/12/01 17:14:23 | INFO acg - dhcp module is disabled |
| 2023/12/01 17:14:23 | INFO tacacs - started gateway at 0.0.0.0:49 |
| 2023/12/01 17:14:23 | INFO websocket - connected successfully to wss://qa.agnieng.net/acg/connect |

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

Ξ.

Figure 13-13: Show Daemon ACG

| IN-MH04-PL-SW02 (con Agent: AristaCloudG Uptime: 0:02:23 (St Configuration: Option | fig)#show daemon AristaCloudGateway ateway (running with PID 6987) art time: Tue Dec 12 07:41:15 2023) Value |
|--|--|
| AGNI_API_TOKEN | eyd haafal marfind far fel gened. TQ4 1Sk jZy zoT iwi jZ0 2x1 .JjtBvKrFnlkg7iLuet1NF-Vnsm8PzipAzQymUL3fT_FqR7bcyt9as5BIO4FnkPJeBx8JZ\ SrT71uFAsLyL_18Pw |
| Status: | |
| Data | Value |
| Agent status | enabled |
| IN-MH04-PL-SW02 (con | fig) t |

Figure 13-14: Show Extension Command

| IN-MH04-PL-SW02(config)#show extensio Name | ons Version/Release | Status | Extension |
|---|--|---------------|-------------|
| AristaCloudGateway-1.0.0-1.swix | 1.0.0/1 | A, I | 1 |
| A: available NA: not available I: S: valid signature NS: invalid sign The extensions are stored on internal IN-MH04-PL-SW02(config)# | : installed F: force hature flash (flash:) | ed B: insta | all at boot |

13.5 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 13-15: Device Administration Enabled with Passphrase Validity

| | est | | | | | | ୯ ଡ 🔎 |
|---|------|--|---------|---|------|----|------------------------------|
| MONITORINO | 6 | Device Administration Device Administration Policies using RADIUS / TACACS+ | | | | | Device Administration Portal |
| ACCESS CONTROL | En | able device administration: Enabled | | | | | |
| Networks Segments | Č | unorised User Groups Device Admins 👩 System Administrator 👩 Select Authorized User Groups | | | | • | |
| C ACLS | 3 | white Login Pasaword Validity (Says) 100 | | | | | |
| Identity Provider User | Alle | ow user to specify Device Login Password: Enabled | | | | | |
| Client | | When disabled, the user's Device Login Password will be system generated. | | | | | |
| CONFIGURATION | | | | 1 | Upda | te | |
| Device Administration | - | Q Search by policy name or description | | | | | |
| TACACS+ Profiles | | | | | | | |
| Certificates System | | ₹+ Add | | | | | |
| CONCOURSE | | Tacacs-Device-Policy | TACACS+ | 1 | 8 | : | |
| 野 Installed Apps | н | ✓ Tacacs-Testing | TACACS+ | 1 | 0 | I. | |

13.6 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 13-10. TACACST Frome creation | Figure | 13-16: | TACACS+ | Profile | Creation |
|--------------------------------------|--------|--------|----------------|---------|----------|
|--------------------------------------|--------|--------|----------------|---------|----------|

| TacacsProfile Provide the following details to update the selected TACACS+ Profile | | | + Back |
|--|------------------------------|----------------------|--------------------------------|
| TacacsProfile | | | |
| Description | | | |
| Prohips load 15 | | | |
| Alow Erable (Privileged Shell Access) | | | |
| ervices and Attributes | | | |
| List of selected Services and its Attributes; | | | Add Service Attribute |
| × ∉ NAME | | | |
| r 1 shet | | | / 0 |
| ou may add a new TACACS+ Service dictionary, if needed. | | | Add TACACS+ Service Dictionary |
| ommands | | | 0 |
| ction for unmatched commanda. | | | Add Command |
| a command | | | |
| 1 show | | | × 0 |
| Deny Arguments wening-config | Permit Arguments (wroter) | Unmatched Arguments: | |
| tote : Changes will be saved once you click on update. | | | |
| | | | Cancel Update TACACS+ Profile |

Figure 13-17: Adding TACACS+ Access Policy

| Device Administration Device Administration Policies using RADUS / TACACS+ | | | Device Administration Portal |
|--|---------|--|------------------------------|
| Enable device administration: Example | Update | Add Policy Provide the following lists to add a new policy New AccessPolicy Description Policy Type: | × × |
| Q, Search by policy name an description Pr. Add Policy Y CVP Admin | TACACS+ | Status Enabled Conditions MitTovetS ALL User: Onco 8 Switch Admin Local | × |
| Switch Admin TACACS | TACACS+ | Actions | II+ Add Condition |
| Switch Admin TK Switch Operator TACACS | TACACS+ | TACKS+ TACACS profile TACACS/Puble Tacashrdfe | × |
| Switch Admin Radius | ADUS / | | The Add Action |
| ✓ Switch Operator Radius | NOUS / | | Cancel Add Pelicy |
| ✓ Default | / | | |

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

Figure 13-18: Creating TACACS+ Policy Details

| wide the following details to add a new policy | 2 × |
|--|--------------------|
| iame AccessPolicy | |
| Description | |
| olicy Type: TACACS+ RADIUS Status: Enabled | |
| Access Device: IP in 10.81.204.0/26 | × |
| | =+ Add Condition |
| | |
| Actions | |
| Actions TACACS+ TACACS profile TACACSProfile TacacsProfile TacacsProfile TacacsProfile | × |
| Actions TACACS+ TACACS profile TacacsProfile TacacsProfile TacacsProfile | × ≅+ Add Action |
| ame | | |
|--|---------------|------------------|
| ccessPolicy | | |
| escription | | |
| Policy Type: () TACACS+ () RAE | DIUS | |
| | | |
| itatus: Enabled | | |
| | | |
| onditions MATCHES ALL | | |
| CloudGateway: Location contains | | ~ |
| contains | HQ | ~ |
| | San Jose | =+ Add Condition |
| | | |
| | | |
| Actions | | |
| Actions TACACS+ TACACS profile | | × |
| Actions TACACS+ TACACS profile | TacacsProfile | × |
| Actions TACACS+ TACACS profile I TACACSProfile I | TacacsProfile | × |
| Actions TACACS+ TACACS profile TACACSProfile | TacacsProfile | × |

Figure 13-19: Creating TACACS+ Policy Details-Conditions

13.7 Monitoring TACACS Plus on AGNI

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

Figure 13-20: Monitoring Session Details

| Session Details - TcInm60c88nsc72qekc50 Details for Session | | | | ← Back | ē |
|--|----------------------|---------------------------------------|---------------|-------------------------|---|
| Authentication Request | Success | Request Details | | | |
| Authentication Type | NAS IP Address 10.81 | | | | |
| Policy | Switch Admin TACACS | Request Time | | 05/12/2023 23:20:57.448 | |
| Location | San Jose | TACACS+ Profile Name | | TacacsProfile | |
| L User Enabled | Access Device | | Cloud Gateway | Connected | |
| tarun tarun | - Not available | CloudGateway - 10.81204.7 San Jose | | | |
| Input Request Attributes | × | Output Response Attributes | | ~ | |
| TACACS+ Activity | | | | Show Activity | |
| Session logs for request: Tcinm60c88nsc72qekc50 | | | | Show Logs | |

Figure 13-21: Monitoring TACACS+ Session Details

| User | Enabled | Access Device | | Cloud Gateway | Connected |
|---|---------|----------------|------------------------|--|---------------|
| run run | | Not available | | CloudGateway - 10.81.204.7 San Jose | |
| put Request Attributes | | ^ | Output Response Attrib | utes | ~ |
| fACACS:AuthnPrivLevel | | 1 | | | |
| ACACS:AuthnService | | Login | | | |
| fACACS:AuthnType | | AuthnTypeASCII | | | |
| CACS+ Activity | | | | | Hide Activity |
| ▲ # COMMAND | | STATUS ER | ROR REASON | UPDATE TIME | |
| 1 show running-config | | Deny De | nied by Policy | 05/12/2023 23-21-05 | |
| ✓ 2 show version | | Permit | | 05/12/2023 23-21:02 | |
| v 3 | | Permit | | 05/12/2023 23-20-59 | |

13.8 Accessing Self Service Portal on AGNI

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

| 1901 Google to | est | | <u> </u> |
|--|---------|--|------------------------------|
| MONITORING | | Device Administration Device Administration Policies using RADIUS / TACACS+ | Device Administration Portal |
| Sessions Access contract Networks Ital Segments Accs | | Enable device administration: Enabled Amortast liser Ones Device Administration: Solarct Authorized User Groups | |
| Identity Provider User | ~ | Allow user to specify Device Login Password: Enabled | |
| Client 招 Guest CONFIGURATION | | When disabled, the user's Device Login Password will be system generated. Update | |
| Access Devices Device Administration | | Q. Search by policy name or description | |
| C Access Policy | | | |
| Certificates | • | ≅e Add | |
| CONCOURSE | <u></u> | II V TACACS+ V 🖥 I | |
| Installed Apps | | II Tacacs-Testing | |

Figure 13-22: 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.



| Your Client Devi | ce OS | | | | - |
|------------------|-------------------------|-------------------------|-----------------------|--------------|-----|
| Арріе мас | | | | | · _ |
| Follow the giv | en steps to install the | DeviceAdmin applic | ation: | | |
| 1. Downloa | d the DeviceAdmin ap | plication for your clie | ent. | | |
| 2. Install th | e application and allow | w it to run in the back | kground. | | |
| 3. When pr | ompted, give permiss | ions for the applicati | on to accept incoming | connections. | |
| 4. In the Se | lf-Service Portal, add | the Access Device in | n the Devices UI. | | |
| 5. Click the | 'Connect' icon for the | e device to launch th | e SSH session. | | |

Figure 13-24: Self-Service Portal for Windows

| our Client Device OS /icrosoft Windows | | | * | |
|---|-------------------------------|--------------------------------|------------|--|
| | | |) | |
| Apple Mac | | | | |
| Microsoft Windows | | | | |
| 2. Install the applicati | on and allow it to run in the | background. | | |
| 3. When prompted, g | ve permissions for the appl | ication to accept incoming cor | nnections. | |
| 4. In the Self-Service | Portal, add the Access Dev | ice in the Devices UI. | | |
| 5. Click the 'Connect' | icon for the device to laund | h the SSH session. | | |

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.

Apart from generating the system generated password, users can generate the device login password using the Self-Service portal.

Figure 13-25: Device Login Credentials on Self-service Portal

E,

| e Portal | V |
|---|----------|
| Period Login Credentials Ver device login credentials in external terminals to access devices securely: Image: Im | |
| | e Portal |

Enter the desired password and click the **Update** button.

Figure 13-26: Device Login-Update Password

| Use device login credentials in external terminals to access devices securely. | |
|--|------|
| Login Username | |
| config | |
| Login Password | Θ |
| | 10-2 |

If you want to regenerate the password, click the **Regenerate** button.

Figure 13-27: User Password Regenerate

| ** | Device Login Credentials View device login credentials | |
|-------|---|------------|
| G |) Use device login credentials in external terminals to access devices secure | ly. |
| Cor | in Username nfig | |
| | Your device login password will expire on 15/03/2028 21:01 | |
| Click | to regenerate a new device login password. | Regenerate |
| Click | to manually update a new device login password. | Update |

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

Figure 13-28: Self-Service Portal SSH Credentials

| | vice Partal | 0 |
|-----------------------------------|---|---|
| D Hange Clerk S Register Clerk | SSH Credentials View Series art credentials | |
| CEVICE ADAMADYSATION | 🔘 Use 50H credentials it external terninuls to access devices security. | |
| Q Setup 100 1000 Conductivity | alla con | |
| ff there | Chih ta prevulte a SSH Revultician. | |

Figure 13-29: SSH Credentials

| | vice Partal | 0 |
|--|---|---|
| CE HassgeClerts Degister Clert Well Resolution | SSH Credentials View device sch Credentials | |
| Device Active rear to | Une SSH trademises in extented herminals to access devices security. Une ssecure January January | |
| PATTI PATTI P [®] Users | Your Stirl Presightness will regime on 01/E4/2828 11.64. Copy and New The generated SSH Desightness, it will not be shown here. | |

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

Figure 13-30: 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: 1686 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#

Configuring DHCP Containers

This section describes how a local container service (the Cloud Gateway) can send IP addresses and other DHCP information to AGNI. To successfully send the IP addresses and DHCP information to AGNI, install a DHCP relay container in your docker environment, preferably on a Linux platform.

Prerequisites for the local container service or Cloud Gateway:

- · Must have Internet access to communicate with AGNI.
- · Must communicate with the network infrastructure to relay the client's IP addresses to AGNI.

The container listens on port 67 to get DHCP information from clients and sends it to AGNI. The container then establishes a secure web socket connection with AGNI over HTTPS.

Network administrators must configure AGNI and the docker to establish a connection between AGNI and the Cloud Gateway.

To configure cloud gateway on AGNI, see the Configuring Arista Cloud Gateway on AGNI section.

14.1 Installing Docker Container

To install the Docker Container, perform the following steps:

- 1. Choose a client (host machine) system (for example, Mac OS) where you want to install the docker container.
- Install Docker Utility on your host Machine. Use any easier method of installation. For example, the Docker Desktop is installed on the Host machine in this scenario. For more on Docker installation and Dockerrelated commands, see the documentation at: https://docs.docker.com/get-docker/.
- **3.** Start the Docker container:

```
docker run --rm --name acg-dhcp
-p 67:67/udp -p 49:49 --env AGNI_ACG_ENABLE_DHCP=true --env ENABLE_DEBUG_LOG=true --env
AGNI_API_TOKEN=<your token here> us-central1-docker.pkg.dev/agni-eng-common/agni-public/
acg:1.3
```

4. Validate Port 67 is running on the client machine where you have installed the Docker.

Figure 14-1: Docker- CLI Output

```
      Icoct@atult=ubuntu=001:/home/atult#
      sudo
      lsof -i -P
      grep
      docker

      docker-pr
      709711
      root
      4u
      IPv4
      3523058
      0t0
      UDP *:67

      docker-pr
      709717
      root
      4u
      IPv6
      3523601
      0t0
      UDP *:67

      docker-pr
      709729
      root
      4u
      IPv6
      3513327
      0t0
      TCP *:49
      (LISTEN)

      docker-pr
      709736
      root
      4u
      IPv6
      3523070
      0t0
      TCP *:49
      (LISTEN)

      root@atult=ubuntu=001:/home/atult#
      Image: tabular interval
      Image: tabular interval
      Image: tabular interval
```

Figure 14-2: Docker - CLI Output (page2)

```
root@atult=ubuntu=001:/home/atult#
root@atult=ubuntu=001:/home/atult# docker ps
CONTAINER ID IMAGE COMMAND CREATED STATUS
PORTS NAMES
71b2441dbbbd us-centrall-docker.pkg.dev/agni-eng-common/agni-public/acg:1.3 "./acg_go" 2 days ago Up 2 days
0.0.0.0149->49/tcp, 1::49->49/tcp, 0.0.0.0:67->67/udp, :::67->67/udp acg-dhcp
root@atult=ubuntu=001:/home/atult#
```

14.2 Configuring Arista Switch for DHCP Messaging

To receive DHCP messaging by AGNI, add the Docker Containers' IP address as the DHCP relay. For example, below is a sample gateway configuration on an Arista EOS switch where *10.81.204.14* is the Container IP address:

```
interface Vlan4003
no autostate
ip address 10.81.204.130/26
ip helper-address 10.81.178.70
ip helper-address 10.81.204.14 source-address 10.81.204.129
```

Authenticating the Client

Authenticate a client on the switch and ensure the DHCP workflow is working well for the client so that AGNI receives the client IP address.

Figure 14-3: Show Output

```
agni-720dp48-1#

agni-720dp48-1#show dot1x hosts

Port Supplicant MAC Auth State Fallback VLAN

Etl1 a0ce.c889.69ff EAPOL SUCCESS NONE

agni-720dp48-1#
```

14.3 Debugging Workflow

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

Figure 14-4: Debug Workflow - CLI Output

Iroot@atult=ubuntu=001:/home/atult# docker logs 71b2441dbbbd 2023/12/01 12:54:00 INFO Starting dhcp service port=67 2023/12/01 12:54:00 INFO tacacs - started gateway at 0.0.0.0:49 2023/12/01 12:54:00 INFO websocket - connected successfully to wss://qa.agnieng.net/acg/connect 2023/12/01 13:02:45 INFO dhcp - mac=f8e43bc00cld send packet(size=1400) to cloud in 123.893522ms 2023/12/01 13:02:45 INFO dhcp - mac=f8e43bc00cld send packet(size=1400) to cloud in 129.377742ms 2023/12/01 13:31:44 INFO dhcp - mac=14ebb6222659 send packet(size=1400) to cloud in 207.460354ms

Figure 14-5: Debug Workflow - CLI Output (continuation)

```
root@atult-ubuntu-001:/home/atult#
root@atult-ubuntu-001:/home/atult# sudo tcpdump -i any port 67 -n
tcpdump: verbose output Suppressed, use -v[v]... for full protocol decode
listening on any, link-type LINUX_SLL2
(Linux_cooked v2), snapshot length 262144 bytes
07:41:16.170766 enxa0cec88a2831 In IP 10.81.204.129.67 > 10.81.204.14.67: BOOTP/DHCP, Request from f8:e4:3b:c0:0c:1d, length 300
07:41:16.170817 docker0 Out IP 10.81.204.129.67 > 172.17.02.67: BOOTP/DHCP, Request from f8:e4:3b:c0:0c:1d, length 300
07:41:16.170823 verbfs10372 Out IP 10.81.204.129.67 > 172.17.02.67: BOOTP/DHCP, Request from f8:e4:3b:c0:0c:1d, length 300
07:41:16.173434 enxa0cec88a2831 In IP 10.81.204.129.67 > 172.17.02.67: BOOTP/DHCP, Request from f8:e4:3b:c0:0c:1d, length 300
07:41:16.173434 verbfs10372 Out IP 10.81.204.129.67 > 172.17.02.67: BOOTP/DHCP, Request from f8:e4:3b:c0:0c:1d, length 304
07:41:16.173444 verbfs10372 Out IP 10.81.204.129.67 > 172.17.02.67: BOOTP/DHCP, Request from f8:e4:3b:c0:0c:1d, length 304
07:41:16.173444 verbfs10372 Out IP 10.81.204.129.67 > 172.17.02.67: BOOTP/DHCP, Request from f8:e4:3b:c0:0c:1d, length 304
07:41:16.173444 verbfs10372 Out IP 10.81.204.129.67 > 172.17.02.67: BOOTP/DHCP, Request from f8:e4:3b:c0:0c:1d, length 304
07:41:16.173444 verbfs10372 Out IP 10.81.204.129.67 > 172.17.02.67: BOOTP/DHCP, Request from f8:e4:3b:c0:0c:1d, length 304
07:41:16.17344 verbfs10372 Out IP 10.81.204.129.67 > 172.17.02.67: BOOTP/DHCP, Request from f8:e4:3b:c0:0c:1d, length 304
07:41:16.17344 verbfs10372 Out IP 10.81.204.129.67 > 172.17.02.67: BOOTP/DHCP, Request from f8:e4:3b:c0:0c:1d, length 304
07:41:16.17344 verbfs10372 Out IP 10.81.204.129.67 > 172.17.02.67: BOOTP/DHCP, Request from f8:e4:3b:c0:0c:1d, length 304
07:41:16.17344 verbfs10372 Out IP 10.81.204.129.67 > 172.17.02.67: BOOTP/DHCP, Request from f8:e4:3b:c0:0c:1d, length 304
07:41:16.17344 verbfs10372 Out IP 10.81.204.129.67 > 172.17.02.67: BOOTP/DHCP, Request from f8:e4:3b:c0:0c:1d, length 304
07
0 packets coeptiend by kernel
0 packets dropped by ker
```

System

This section captures the administrative tasks at the system level.

15.1 Audit Viewer

The Audit Viewer page captures the details about system configuration modifications such as additions, deletions, and modifications. This page helps to track any changes performed on the system along with the owner details, modification details, and the time-stamp.

You can view the audit records for added configurations, updated configurations, deleted configurations, or all configuration changes.

| | 791 | E | Audit Viewer | | | | | |
|---|-----|------|------------------------|-----------------------|---------|------------------|------------------------------------|----------------|
| Sessions | | A11/ | Actions Added Up | dated Deleted | | | | C |
| Networks ± ± Segments | | ٩ | Search by Name or User | | | | Type Any C | onfig Entity 🔻 |
| ACLS | | # | NAME Arista CV-CUE | TYPE Concourse App | ACTION | USER / API TOKEN | DATE & TIME 13/05/2025 14:00:07 | Ø |
| Identity Provider User | ~ | 2 | ServiceNow CMDB | Concourse App | Updated | system | 13/05/2025 14:00:04 | 0 |
| Client | Ų | 3 | Arista MSS-G | Concourse App | Updated | system | 13/05/2025 14:00:02 | 0 |
| H Guest | × | 4 | Arista MSS-G | Concourse App | Updated | system | 13/05/2025 14:00:01 | ø |
| Access Devices | ~ | 5 | ServiceNow CMDB | Concourse App | Updated | system | 13/05/2025 14:00:01 | 0 |
| Device Administration | ~ | 6 | Arista CV-CUE | Concourse App | Updated | system | 13/05/2025 14:00:00 | O |
| Certificates | ~ | 7 | Arista CV-CUE | Concourse App | Updated | system | 13/05/2025 13:00:08 | 0 |
| Audit Viewer | - 1 | 8 | ServiceNow CMDB | Concourse App | Updated | system | 13/05/2025 13:00:03 | ٥ |
| C License | | 9 | Arista MSS-G | Concourse App | Updated | system | 13/05/2025 13:00:02 | O |

To view the details of each audit record, click the eye icon towards the end of the row for the selected record (see images):

| MONITORING | | | Auc | lit Details for A y Type: Concourse A | rista CV-CUE | | | ← Ba |
|--|---|----|-----------|---|-------------------|----------------|-------------------------------|----------------|
| Sessions ACCESS CONTROL | | Au | dit Activ | ity | Last 3 days 👻 | Entity Details | | Diff Fu |
| Networks Segments | | • | Updated | by system | 9 minutes ago | User system | Timestamp 13/05/2025 14:00 | |
| ACLS | | 0 | Updated | by system | 10 minutes ago | Name | | Arista CV-CU |
| Identity Provider | | 0 | Updated | by system | about 1 hour ago | Category | Net | work Managemen |
| User Client | 2 | 0 | Updated | by system | about 1 hour ago | | | |
| Guest | ~ | 0 | Updated | by system | about 2 hours ago | | | |
| Access Devices | ~ | 0 | Updated | by system | about 2 hours ago | | | |
| Device Administration | č | 0 | Updated | by system | about 3 hours ago | | | |
| System | ~ | 0 | Updated | by system | about 3 hours ago | | | |
| Audit Viewer | | 0 | Updated | by system | about 4 hours ago | | | |

| agni I 🏎 | | | | | 6 | 0 😁 |
|---------------------|---|--|------------------------------|----------------------------|------------------------------------|------------|
| E Instituted | - | Audit Details for Detty Type Device A | r test12 | | | 6- Back |
| And Basedore | | Audit Activity | Last 3 days * | Entity Details | | (Internet) |
| V Autorita | | by | adam allocat 11 hours age | | Fernanderige Thirds/PGTS III AD | |
| C ROLA | - | Acad by | | - Same | | seef 0. |
| 2 Sheriffy Provider | | | | linter | | Staatena. |
| - Cliwit | - | | | Description Police Term | | TACACIE: |
| ET Guess | - | | | For Dens | | 1 |
| Access Devices | - | | | Conditions | | |
| Carificates | | | | User Droug is not 112 | | |
| 13 Typiam | - | | | | | |
| I fagtere | | | | Dens Access | | |

15.2 License

This page displays the licensing information about the type, count, and validity period. Additionally, the license usage details are displayed on a monthly and weekly basis.

- License usage is displayed for the current month and the previous month.
- · License usage is displayed on a weekly basis for the current month.

• When usage exceeds the licensed count, the details are highlighted in red .

Figure 15-1: License Usage Details

| License Details | |
|--|---|
| Туре | Subscription |
| License count | 100 |
| Valid until | 18/07/2030 19:11:15 |
| Monthly License Usage Count for Jan 2025 | 190 |
| License usage is calculated based on the numb identified by client MAC addresses, over a rollin monthly average of weekly counts is computed | er of unique successful authentications, g 7-day period. To ensure stability, a to determine overall license utilization. |
| License usage is calculated based on the numb identified by client MAC addresses, over a rollin monthly average of weekly counts is computed | er of unique successful authentications, ig 7-day period. To ensure stability, a to determine overall license utilization. |
| License usage is calculated based on the numb identified by client MAC addresses, over a rollin monthly average of weekly counts is computed Weekly count of unique successful authentication | er of unique successful authentications, g 7-day period. To ensure stability, a to determine overall license utilization. s for current month |
| License usage is calculated based on the numb identified by client MAC addresses, over a rollin monthly average of weekly counts is computed Weekly count of unique successful authentication Week 1 (1st to 7th) | er of unique successful authentications, 1g 7-day period. To ensure stability, a 1o determine overall license utilization. 1s for current month Feb 2025 91 |
| License usage is calculated based on the numb identified by client MAC addresses, over a rollin monthly average of weekly counts is computed Weekly count of unique successful authentication Week 1 (1st to 7th) Week 2 (8th to 15th) | er of unique successful authentications, 1g 7-day period. To ensure stability, a to determine overall license utilization. Its for current month 91 91 |
| License usage is calculated based on the numb identified by client MAC addresses, over a rollin monthly average of weekly counts is computed Weekly count of unique successful authentication Week 1 (1st to 7th) Week 2 (8th to 15th) Week 3 (16th to 23rd) | er of unique successful authentications, 1g 7-day period. To ensure stability, a to determine overall license utilization. The Solution Solution Soluti |

15.3 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.

| | | | | | | | (| 9 C | D. |
|---|---|-----------------------------------|--|-------------|-------------------------|---------------------------|--------------------|-----|-----|
| Monitolisio | | Customize Self-service Portal | 4 ⁻ | | | | Self-service Porta | • | Set |
| CCESS CONTROL | | Theme Settings | | | LOGIN PAGE LANDING PAGE | | | | |
| P Networks | | Porta fami Self Service Portal | | | | - | | | |
| ACLS | | Header Background | #326297 | | | OGNI tert Service Parte | | | |
| Identity Provider | | Theme | #326297 | | | Sign in | | | |
| Client | 2 | Logo | Add | | | - | | | |
| Guest | * | Login Page Settings | | | | | _ | | |
| Access Devices | ~ | Background Image | Add | | | | | | |
| Device Administration | ř | Form Color | #F30000 | | | | | | |
| System | | UserID or Email | | | | | | | |
| Audit Viewer | | Terms of Use | | | | | | | |
| E Self-service Portal | 1 | | | | | | | | |
| 1 RadSec Settings | | Additional Information for Users | | Disabled 0= | | | | | |
| Support Logs System Events | | Enable to include additional in | formation for Self-service Portal users. | | | | | | |
| oncourse Explore | | | Default | Resol | | | | | |

Figure 15-2: 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 15-3: Manage Self-Service Portal Settings

| agni I | Ì., | | | ७ ७ 😬 |
|-----------------------------|-----|---|---|-----------------------|
| Nonstoness Dashboard | | O Your trial license expires in 11 day(s). | | × |
| ✓ Sessions | | Self-service Portal | | C Self-service Portal |
| Networks | | | | |
| Alla Segments | | Theme Settings | LOOIN PAGE LANDING PAGE | |
| ACLS | | | | |
| KOENTITY | | Self Service Portal | | |
| Identity Provider User | | Header Background | ogn / | Tel Banka Punz |
| Client | ~ | Theme | Manage Self-service Portal Settings Signin | |
| | ~ | Logo | Add Read-only User Groups | Record |
| Access Devices | 2 2 | Login Page Settings | register clients. However, they will be allowed to conboard their clients, access Device Administration features and manage guests, if applicable. | |
| Certificates | v | Background Image | Add Restricted Onboard Users 🔕 Snight User Croups | |
| System | ~ | Form Color | | |
| concourse | | Ourselve Label | | |
| III Explore | | UserID or Email | Cancel Update | |
| Installed Apps | | Terms of Use | | |
| | | Additional Information for Users | Duabled Ora | |
| | | Enable to include additional information for Se | ef-service Portal users. | |
| | | | Default Reset Update | |
| | | | | |

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

Figure 15-4: Self-Service Portal Clients with Read-only Access

| | vice Portal | | | | | | |
|--------------------|---|-----------------------------------|-------------------------|-------------------------------|--|-----|-------------|
| Eb Manage Clients | Clients | | | | | | |
| 😳 Wi-fi Pausphrase | Manage the list of clients as on 62/01 | (2024 13 51 07 | | | | | a :: |
| | | | | | | | |
| | Q Search by KAC address of description. | | | | | Ary | • |
| | # WAE ADDRESS | DESCRIPTION . | (Securit (VIII) | KTATUS | UPDATE TIME | | |
| | 1 | Keert's Mac OS X | Xaw1 | Brated | e3/01/2024 11 53 51 | | • |
| | 2 bleasticidd ee ff | | Kenti | Enational | 0103/2024 22:30:35 | | • |
| | 3 +4 51 33 15 76 M | Keent's Andruid | Keets | Bratiled | 25/06/2024 15 15:08 | | • |
| | 1 2 86-3400-082 ee/ff 3 ee/61332/629-64 | Kant's Mac DS X Kant's Andruid | Kauti Kauti Kauti | Evalued Evalued Evalued | 039070024 11 53 51 91(01/2024 22 30 35 21(06/2024 15 15/06 | | |

E

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

| Manage Clients Wi-Fi Passphrase | 1 == | Wi-Fi Passphrase View W-R possphrase | |
|------------------------------------|--------------|--|--|
| | | Automation | Scan this code to connect your clients |
| | | A Your passphrase expires on 02(01/0024 32:24:08 | make egal |
| | | | |
| | | AICISIA | |
| | | Next Naty The Approxime is marked at the United Tables by Antia Selections, the Confer of Way Then Stream Public optimes have as, and at if our composite administration are previous of interaction factor as and a global processing in the antiation (by Then Stream) and antia and public at a selection of the Stream Public optimes and public at a public optimes and public op | el añose, var el resource en |
| N | oto | The users with read-only access privile | ages can contact the AGNI administrator if they wa |
| N I re | ote: egen | I he users with read-only access privile erate their passphrase. The AGNI admi | eges can contact the AGNI administrator if they wa nistrator can regenerate the passphrase from the L |

Figure 15-5: Self-Service Portal WiFi Passphrase (client with Read-only access)

Figure 15-6: User Account Details with Regenerate Passphrase option

| agni I | | | | | 6 0 C |
|------------------------------|------|--|------------------|--------------|-------|
| Montoune | | Keerti Vern vaar ohdals and optide the selected vaer | | é fack I | |
| And the second second second | | (1999) | | | |
| · Networks | | -Out | | | |
| its Segments | | The first of the second | | | |
| CONTRA - | | , the feature | | | |
| 1 Identity Provider | | | C Copy Regarante | | |
| 1 there | 0.21 | | | | |
| 1 Users | | New paragetrase is generated. EXX Update to use this paraghtesis for any future regionations. | | | |
| III. User Drouds | | Status Budiet | | | |
| Ciert | | | | | |
| Cherta | | User status is managed by the Identity Provider. | | | |
| Client Groups | | Local User Groups | | | |
| ff Overst | 1.4 | H-gant user group (H-rs-group) | | | |
| St Users | | Estamat Quer Groups Name douver | | | |
| D Portala | | | | | |
| connounction | | | Carce | Opdate User | |
| Access Devices | * | | | | |
| Certificates | 1 | User clients | | Sive Clearly | |
| C) System | | | | | |
| 2 Auto Viewer | | | | | |
| Q License | | | | | |
| D Sett-service Pertal | | | | | |
| C Raffer Settings | | | | | |
| TI Supportions | | | | | |
| | | | | | |
| D System Lynnik | | | | | |
| CONCOLINE | | | | | |
| E Espices | | | | | |
| 10 Installed Appa | | | | | |

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).

| agni I | | | | |
|---------------------------------|---|--|--------------------------|---------------|
| Monttoend | Customize Self-service Portal | | | D Set-service |
| V Sessions | Theme Settings | | | |
| Networks | Fore same Set Service Portal | | | |
| ACLA | Header Background | *326297 | O'G'ni tel terser tend | |
| Mentity Provider | Theme | #3262987 | See Section 2010 | |
| tuar v | Logo | Ass | | |
| kent v | Login Page Settings | | | |
| Access Devices | Background Image | A44 | | |
| Device Administration 🔍 | Form Color | *870009 | | |
| Certificates v | UserD or Ernel | | | |
| Audit Viewer | Series of Use | | | |
| License Salf-service Portal | | | | |
| © RadSec Settings | Additional Information for Users | Enabled = | | |
| 1 SupportLogs | The following details will be displayed after onboarding a | successful. | | |
| 🔁 System Events | 8 J V & G H H I I I I I | A # 1: Z | | |
| Explore I Explore | ARISTA | | | |
| | The Application is maintained in the Linked States by Ands Ib and all of our corporate subsidiaries and affiliates, use any per- wobsite (the "Stat") and our cloud heteracting solutions and pr Policy does not apply to any third party websites, sortices, or | neona, Inc. ("we" of "ue"). This Privacy Policy explains how we, cond internation that we colled about you when you use the ducts (the "Services") or otherwise interact with us. This Privacy splications, even if they are accessible through our Services. | | |
| | Additionally, show in user's W-FI Passphrase page. | (Insted) -0 | | |
| 10001-000 | | Default Reset Update | | |



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 15-8: Self-Service Portal Wi-Fi-Passphrase

| ci gi i i | | | | | | |
|-------------------|---|--|--|--|--|---|
| C Manage Clients | | Wi-Fi Passphrase | | | | |
| 📅 Register Client | | View Wi-Fi passphrase | | | | |
| W-FiPassphrase | 1 | Detters | | | Scan this code to connect your clients | |
| QUESTS | | My Devices | | | | |
| AT Users | | Facebook | | | Server 100 | |
| | | | 0 | Copy | kk-spsk-auth | - |
| | | | | | C | |
| | | This is your passphrase. Click Regenerate to | create a new passphrase if needed. | | 电流常电 | |
| | | ARIST | ٩ | | | |
| | | Privacy Policy | | | 401억억건 | |
| | | This Application is insurtained in the United Status by Anata autoclanes and attiliates, use any personal internation that scalutions and products (the "Services") or otherwas interact applications, even it hey are accessable through our Service | Networks, Inc. ("we" or "us"). This Privacy (we collect about you when you use this w rwth us. This Privacy Policy does not appr ps. | Policy explains how we, and all of our corporate ibele (the "Sne") and our coud releasing (to any third-party websites, services, or | | |



Figure 15-9: Self-Service Portal Wi-Fi/UPSK-Passphrase

Figure 15-10: Self-Service Portal Registering a Client in the Native Onboarding page



15.4 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 15-11: RadSec Settings

| | | & @ _ |
|----------------------------------|---|---|
| MONITORING | RadSec Settings View RadSec Settings | 💭 Get Client Certificate |
| ACCESS CONTROL | RadSec Server | |
| Networks Il: Segments | RadSec Server Hostname | radsec.qu.agnieng.net |
| C ACLS | Use the above server as RadSec(TL5) RADIUS server in your Network Access Devices. | |
| (a) Identity Provider | RadSec CA Certificate | Expires on 6/4/2035 |
| LUser V | Subject DN | CNwISRG Root X1, Owinternet Security Research Group, CwUS |
| ONFIGURATION | Issuer DN | CNwISRG Root X1, Owinternet Security Research Group, CwUS |
| Access Devices Certificates | Use this CA certificate to validate the RadSec(TLS) server certificate. | |
| Trusted | | ± |
| System | | |
| Audit Viewer | | |
| Q License | | |
| Portal Settings | | |
| 1 RadSec Settings | | |

15.5 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 15-12: Support Logs

| | 9 | | | | | | | | S | 0 |
|--|-----|---|--|---|---|--|--|------------------------------------|-------------|-------------|
| MONITORINO | | | Support Logs Search support logs | | | | | | | |
| V Sessions Access control Networks | | Lo | al | *) Debug | •) | 5 minutes | | J | Resat | Refresh |
| ACLs | | Supp | ort log entries | | | | | | | Download |
| (A) Identity Provider | | • | 7/24/2023 13:02:04.350 BR80 7/24/2023 17:02:04.351 INPO | 98 (5=85a61d189-m361-4837-m116-1825754 9 (5=85a61d189-m361-4837-m116-18257542 | Dorfb spikeg10+APICIVELV502 | ajs72988920] /api/id LS72Q04580] /api/se | entity.client.get erreabj sion.actions.get (0.1106) | ect_not_found (6.309134mm) 4mm) | | |
| 1 User | × × | | 7/24/2023 17:02:04.378 INFO 7/24/2023 17:02:04.477 INFO | 0 [t=%De61d189-e361-4837-e116-18257342 0 [t=%De61d189-e361-4837-e116-18257542 | lbefb apiReqID=APICIV81V5426 Nefb apiReqID=APICIV81V503R | LS72Q6N6V0] /api/ses | sion.get [35.729421ms] sion.detsils.get [16.6169 | J4ms) | | |
| Access Devices | | | 7/24/2023 17102104.480 INFO 7/24/2023 17102104.481 INFO | <pre>(t=Eba61d189-m)61-4837-m116-18257542 0 (t=Eba61d189-m)61-4837-m116-18257542</pre> | terta apikaqID=APICIV81V5420 Seth apikaqID=APICIV81V5420 | LS72QD4586) /api/com | fig.nad.get [5.937296ms] fig.network.get [6.85240] | naj | | |
| Certificates | > < | | 7/24/2023 17:02:04.481 INPO 7/24/2023 17:02:06.495 INPO | [t=Rba51d189-e361-4837-a116-18257542 0 (t=Rba61d189-e361-4837-a116-18257542 | Oefb apiReqID+APICIV81V5426 | LS72Q6N700) /api/ses JS72F88F40) /api/ses | sion.actions.get [7.06895 sion.log [795.043774ms] | 5ma] | | |
| Audit Viewer | | | 7/24/2023 17:02:20.454 INPO 7/24/2023 17:02:22.945 INPO |) (apiReqID+ADICIVH235Q3AJS120B8P4G t=) (apiReqID+ADICIVH23L42CL672QD4SCG t= | Eba61d189-e361-4837-a116-18 Eba61d189-e361-4837-a116-18 | 2575420cfb) /api/con 2575420cfb) /api/con | fig.network.list (7.88410 fig.network.list (9.10680 | 7ma j 6ma j | | |
| Portal Settings | | | 7/24/2023 17:02:29.102 INPO 7/24/2023 17:02:30.376 INPO | 0 [apiReqID=APICIVH25D42GL672Q4H710 t= 0 [t=Ebe61d189=e361=4037=a116=18257542 | (Da61d109-e)61-6837-a116-18 (Ocfb] config - delete netwo | 2575420cfb] /api/con ck[id=172 name= suic | fig.entity.references.get | [13.184089ms] | | |
| U Support Logs | - | 7/24/2023 37:02:20.376 INFO [t=Rhos61d187=e361=437=e114=182574426cHb apimeg1b=AFE 7/24/2023 17:02:30.498 INFO [t=Rhos61d189=e361=4837=e116=182575426cHb apiMeg12=AFE | | | | iRegID=AFICIVE25LQ7H2512788f50] /api/config.network.delete [29.801628ms] iRegID=AFICIVE25LQ7H2522F88f50] /api/config.network.list [11.235125ms] | | | | |
| System Events | | 0 | 7/24/2013 17:02:02.047 ER80 validate excelos for app[AC | 00. [api8eq10=APICIVE2014201420147004800 1 ml] [1.844073ms] 2 [[appentDe1AMs(vb2b14201872044800 1 | *Ebx61d183-e361-4837-6116-1 | 257542Defb1 (api/ar | rvice.log erreath_failed | a I error occurred: * invalid_ | Linguat_And | IN LOW JOIL |
| III Explore | | | 7/24/2023 17:02:56.210 INPO | 0 [iamBegID=IAMcivh2bt42g1a72qd4egg t= | E2a61d189-e361-6837-a116-18 | 2575420cfb] iam(log) | n) - init 530 | or other complete and | | |

15.6 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.

| IONITORING | | 0 | Your trial license will expire in 354 da | y(s). | | |
|--|----|-----|--|---|-------|--------------------|
| Dashboard Sessions CCESS CONTROL | | E | System Events List of system events | | | |
| ACLs | | A . | Error Warning Info | | | |
| A) Identity Provider | | | TYPE | MESSAGE | LEVEL | DATE |
| User | ~ | 1 | Identity Provider Sync | AGNI Global(azure) - finished IDP sync job for 2 user(s), users updated 0 | Info | 7/24/2023 18:13:01 |
| Client | ~ | 2 | Identity Provider Sync | AGNI Global(azure) - starting IDP Sync | Info | 7/24/2023 18:13:00 |
| FIGURATION | 22 | 3 | Identity Provider Sync | SYStest POC(azure) - finished IDP sync job for 1 user(s), users updated:0 | Info | 7/24/2023 18:09:00 |
| Certificates | ~ | 4 | Identity Provider Sync | SYStest POC(azure) - starting IDP Sync | Info | 7/24/2023 18:09:00 |
| System | ^ | 5 | Identity Provider Sync | Antara Eng(azure) - finished IDP sync job for 1 user(s), users updated:0 | Into | 7/24/2023 18:08:00 |
| Audit Viewer | | 6 | Identity Provider Sync | Antara Eng(azure) - starting IDP Sync | Info | 7/24/2023 18:08:00 |
| Q License | | 7 | Identity Provider Sync | onelogin(onelogin) - finished IDP sync job for 1 user(s), users updated:0 | Info | 7/24/2023 18:07:01 |
| Portal Settings | | 8 | Identity Provider Sync | onelogin(onelogin) - starting IDP Sync | Info | 7/24/2023 18:07:00 |
| RadSec Settings | | 9 | Identity Provider Sync | AntaraAl(google) - finished IDP sync job for 1 user(s), users updated:0 | Info | 7/24/2023 18:01:01 |
| Support Logs | | 10 | Identity Provider Sync | AntaraAl(google) - starting IDP Sync | info | 7/24/2023 18:01:00 |
| E System Events | | 11 | Identity Provider Sync | onelogin(onelogin) - finished IDP sync job for 1 user(s), users updated:0 | Info | 7/24/2023 17:29:01 |
| NUSUNDE | | 12 | Identity Provider Sync | onelogin(onelogin) - starting IDP Sync | Info | 7/24/2023 17:29:00 |

Figure 15-13: System Events

15.7 Notification Settings

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

15.7.1 Configuring Email Settings on AGNI Cloud

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. Navigate to Configuration > System > Notification Settings > Email Settings.

Customize the Sender Name and the Reply Email and click the Email Templates button (see image).
 Figure 15-14: Notification Settings- Email Settings

| agni I coople te | ns. | | 6 Ø 📀 |
|------------------------|------|---|-------------|
| Bowrtossag | | True that Reame anythin in 205 day(h) | × |
| A Session | | Notification Settings Crosser the type of notification you want to update. | 7 Pemplates |
| Vietworks | | Envil Settions SHE German | |
| Ch artes | | | |
| DENTT: | | Answer Konstein | |
| (4) identity Provider | | that that | |
| 1 User | | pritantaichaidaidaista.com | |
| Client | ÷ | | |
| Unest | 94 L | 8 | Upstaha |
| T Users | | | |
| E Portala | | | |
| CONFIDURATION | | | |
| Access Devices | Se | | |
| Device Administration | | | |
| Certificates | | | |
| D Bystem | | | |
| E Audit Viewer | | | |
| 2 License | | | |
| Self-service Portal | | | |
| O RadSec Settings | | | |
| Bupport Logs | | | |
| D System Events | | | |
| O Notification Setting | | | |
| Collapse Sideber | | | 0 |

3. 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 15-15: Email Settings - Global Settings

| | ଓ ଡି 💌 |
|--|---|
| Customizable email templates to streamline your communication needs. | ← Back |
| Global Templates | |
| Theme Colors | Sample Email of Add Guest User |
| Background Color #326297 | Select Ereal Type Send with Password |
| Header Content | Subject: Guest User Add Confirmation |
| B I U % ⊠ Hs Hz ▲ ⊠ ≞ ⊟ T _x | Guest Account registered successfully. |
| | Hello Alex |
| | Your account is created with the following credentials - |
| Footer Content | Username: alex@acme.org |
| B I U % Hi Hz A M E ⊟ Z. | User Password: 12345678 |
| This is an advantation where reactions of these we first typy of the interaction | Device limit: 2 |
| | Valid from Date: 22 Jul 24 16:59 +0530 |
| Default Cancel Update | Valid until Date: 23 Jul 24 00:59 +0530 |
| | This is an automated email notification. Please do not reply to this message. |
| | (Q) |

- 4. Select the Templates tab in the Email Templates page (see image).
- 5. 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).

| MONITORING | Customizable email templates to streamline your communication needs. | |
|-------------------------|--|-----|
| Sessions | Global Templates | |
| Networks :- Segments | Select Email Template | × • |
| ACLS | Er Guest G Add Guest User | 1 |
| ldentity Provider | Guest User Updated | |
| User | Em: Guest User Approval | |
| Client | Guest User Approved | |
| Guest 🗸 | A Organization User | |
| ONFIGURATION | Add Organization User | |
| Access Devices | Y Onboard Client | |
|] Device Administration | Onboard OTP Login | |
| Certificates | D User Password Update | |
| - System | Wi-Fi Passphrase Greeting | |

Figure 15-16: Email Template Settings

b. Enter the Email Subject.

Ξ.

- 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 15-17: Email Templates Example**

| Email Templates Customizable email templates to streamline your communication needs. | ← Bas |
|--|--|
| Select Linut Tempera Add Guest User | Sample Email of Add Guest User |
| | / biettimai type |
| Insi bigar | Send with Password |
| Guest User Add Contemption | Subject: Guest User Add Confirmation |
| nail Placeholders | |
| Account created with Pasignnase | Guest Account registered successfully. |
| A unique Wi-Fi passphrase has been created for you. | Hello Alex |
| Account cleaned with Password | |
| Your account is created with the following credentials - | Your account is created with the following credentials - |
| Divice Unit | Username: alex@acme.org |
| Research Control Contr | User Password: 12345678 |
| Hello | |
| Header Taxt | Device limit: 2 |
| Guest Account registered successfully. | Valid from Date: 22 Jul 24 16:59 +0530 |
| Factorial mathematical | Valid until Date: 23 Jul 24 00:59 +0530 |
| Use the following passphrase to connect your client devices. | |
| Patient | This is an automated email notification. Hease do not reply to this message. |
| User Password | |
| QR code fire | |
| QR code file abc | |
| OR scale instruction | |
| Scan the network QR code and connect to the wireless network. | |
| literare . | |
| Username | |
| Wild from - | |
| Valid from Date | |
| Valid unit | |
| Valid until Date | |
| white a | |
| WiFi Network xyz | |
| Wir Fi Pessaltrase | |
| Wi-Fi Passphrase | |
| | |

15.7.2 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 15-18: Notification Settings - SMS Gateways

| ONITORING | Notification Settings | 🖻 Email Templat |
|---------------------------------------|--|-----------------|
| Dashboard Sessions CESS CONTROL | Email Settings SMS Gateways | |
| Networks Segments | SMS Gateway Settings | |
| ACLS | To add another SMS Gateway, click here | |
|) Identity Provider | Test MSG91 QA d MSG91 | / 8 |
| Client ~ Guest ~ | Test twillio qa 🔞 Twilio | / 0 |
| Access Devices ~ | | |
| Device Administration ~ | | |
| Certificates ~ | | |
| Audit Viewer | | |
| Q License | | |
| Self-service Portal | | |
| C RadSec Settings | | |
| Sustem Events | | |
| Natification Settings | | |

15.7.2.1 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 15-19: SMS Gateway - Twilio Settings

| | | | & Ø 📀 |
|---------------------------------------|--|-------------------|-------|
| scources E Cashdoard ~ Sessions | Notification Settings Choose the type of notification you want to update. | i Email Templates | |
| ACCESS CONTROL Wetworks | Email Settings SMS Galeways | | |
| Alla Segments | SMS Gateway Settings | | |
| Ø ACLA | r tid tarms for S Tailo | | |
| 🛞 identity Provider | (i) Twile | | |
| Clast v | al woost | | |
| ff Guest | Twillo SMS Account Settings | | |
| 🕂 Users 🕕 Portals | Account 50 | | |
| Contributantion Access Devices | Aun taun | ۲ | |
| Device Administration | Sello Netter | | |
| D System | Test Phone Number | | |
| E Audit Viewer | Their physics (Section 16 included for inclusion) | | |
| Elicense | | Verify | |
| Q RadSec Settings | | | |
| E Support Loga | | Destrie Add | |
| 🔃 System Events | | | |
| O Notification Settlegs | | | |
| K Collepse Sidebar | | | 0 |

- 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 15-20: SMS Gateway - Twilio Settings Details

| | last | 6 | ۲ | 8 |
|---|---|---|---|---|
| sepectorises Dashbeard M beasions Access contrac. | Notification Settings Crosse the type of extitcation year wate to update. Insult Sensity Subscription | | | |
| Networks Segments ACLs | SMS Gatewy Settings | | | |
| (2) Identity Provider 1 User | v Telle · · | | | |
| f Guest f Guest | Twillo SMS Account Settings | | | |
| Connounation Access Devices Device Administration | Image: Contract of the second secon | | | |
| Certificates | A Statistical | | | |
| License SeiT-service Portal RadSec Settings | nd (www) | | | |
| System Events Notification Setting | | | | |
| | | | | 0 |

- 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

15.7.2.2 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 15-21: SMS Gateway - MSG91 Settings

| | | s 🛛 📀 |
|---|--|--|
| MONITORINE 11 Deshiboard | Notification Settings Choose the type of restlication you want to update. | MS001 SMS Account Settings |
| -/* Sessions Access cowreck Asteocks | Ernel Sertings BMS Generality Accelerate/ch460c/7540c016425-2500.cd1a | |
| tis Segments Ø ACLA sobitty | And New Concerned | Create SMS simplifies in MSDB1 and provide their Cts below Sear out of veryors 0 HAXSEN |
| 2 User · □ Client · | + risketwine. | Europe service value Mananagen A, Province Measure VA |
| ff Overs * | See phone increase to required for sectorization. | Large called "Alle Research Re |
| Communition | Template Configuration | Weby |
| Device Administration V Certificates V System A | Gover account is added. Username ((username)) Pessenort ((passmort)) | Template Configuration |
| E Audit Vanner Q License E Self-service Portal | Guert account is updated. Usersament (<u>Learnament</u>) Paramotol (<u>Learnament</u>) team many function | Tells Maxemental per Januard (in Majaniard (in Majaniar |
| O Radiec Settings | Cont account Soublet. Username ((seename)) O To add another SMS Games, clock bag. | r Sant Alakter unter Heldy attalanterinate, your passion file attglassion fakt to high to deblag timely (n. |
| A Notification Settings 44 Collapse Sidebar | | Canol Met |

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

Sessions - AGNI Cloud

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

| õğni I | | | | | | | | | | | ७ ७ 💿 |
|--------------------------|---|--|----|---|--------------------|-------------------|---------------|----------------|---|-------------------------|-------|
| MONTORNO | I | ~ | Se | essions t of Sessions as on 07/12/20 | 23 13:09:13 | | | | | | |
| A Sessions | 1 | | | | | | | | | | C 目 🛙 |
| Networks Is Segments | | Q. Search by Identity, MAC Address, IP Address or Session ID . | | | | | |) (Any *) (Any | | | |
| @ ACLS | | ^ | | IDENTITY | TYPE | MAC ADDRESS | IP ADDRESS | STATUS | | TIMESTAMP | |
| (A) Identity Provider | | × | 5 | Home-IOTs | MAC Authentication | 0013/01/00/00/01 | 10.10.30.2 | Success | • | 08/12/2023 14:07:37148 | 0 |
| ± User v | | • | 2 | Home-IOTs | MAC Authentication | 0013/01/00/00/02 | 10.10.30.3 | Success | • | 08/12/2023 13:54:16.193 | 0 |
| Client v | | × | 3 | Home-IOTs | MAC Authentication | 00.11.d9.5e.3d.44 | 10 201110 50 | Success | • | 08/12/2023 13:48:42:317 | ø |
| 🖾 Access Devices 🗸 🗸 | | * | 4 | Home-IOTs | MAC Authentication | 00:13:01:00:00:01 | 10.10.30.2 | Success | • | 08/12/2023 13:07:37:065 | 0 |
| Device Administration | | ~ | 5 | Home-IOTs | MAC Authentication | 00-13-01-00-00-02 | 10.10.30.3 | Success | • | 08/12/2023 12:54 16:075 | Θ |
| Continuates o | | • | 6 | Home-IOTs | MAC Authentication | 00:11:d9:5e:3d:44 | 10.201.110.50 | Success | | 08/12/2023 12:48:42:236 | 0 |
| CONCOURSE | | × | 7 | CAMERA_GROUP | MAC Authentication | 18:e4:3b:c0:0c:1d | 192.168.1.12 | Success | • | 08/12/2023 12:32:24.121 | ٥ |
| Explore | | * | 8 | CAMERA_GROUP | MAC Authentication | 18:#4:3b:c0:0c:1d | | Success | • | 08/12/2023 12:31:47.824 | 0 |
| | | ~ | 9 | Home-IOTs | MAC Authentication | 00:13:01:00:00:01 | 10.10.30.2 | Success | • | 08/12/2023 12:07:36:985 | 0 |
| | | ~ | 10 | Home-IOTs | MAC Authentication | 00:13:01:00:00:02 | 10.10.30.3 | Success | | 08/12/2023 11 54 15.993 | 0 |
| | | * | 11 | Polycom Phones | MAC Authentication | f8:e4-36:c0:0c:1d | 192.168.1.12 | Success | • | 08/12/2023 11:50:47.419 | ۵ |
| | | ~ | 12 | Home-IOTs | MAC Authentication | 00.11:d9:5e:3d:44 | 10.201110.50 | Success | • | 08/12/2023 11:48:42:102 | 0 |

Figure 16-1: Monitoring Sessions

Figure 16-2: Monitor Session Details

| Dashboard | Session Details - Rclpdbk84n37c72vIs7v0 Details for Session | | | 🗞 Disconnect 🧹 🗧 | ick- |
|--|--|---|----------------------------|------------------|---------|
| Sessions | Authentication Request | Success | Session Details | | Open |
| Networks | Authentication Type | MAC Authentication | Client IP Address | 10. | 10.30.2 |
| & Segments | Segment | Home-IOTs | Session Start Time | 08/12/2023 14:07 | 37.148 |
| ACLS | Location | Arista CloudVision/Tenant/AGNL_HQ | Session Stop Time | | 12 |
| C Identity Provider | 1 User | Client | Enabled | Actions | |
| Client v Reformation Access Devices v Device Administration v | Not available | 00.13.01.00.00.01 Auto registered with MAC Authenti D Home-IOTs | cation | ⊘ Allow Access | |
| i Certificates v | Access Device Arista Switch | Network | Enabled | | |
| NCOURSE Explore S Installed Apps | и: 34594.c8.27.9: адл:722хрт-48 Ө лт-WRED-САР | AT-WRED-EAP Wired MAC Authentication | | | |
| | Input Request Attributes | Q -) | Output Response Attributes | | Ş |

16.1 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 16-3: Client Session Details

| ~ | Ser | ssions of Beautore as on 11/27/2023 12:19:32 | | | | | | |
|------|--------|---|--------------------|----------------------|-------------|-----------|-------------------------|-------|
| Netw | uri Ac | Device Administration | | | | | | c 🔳 🖩 |
| ٩ | | the Annual State Address of Antonia or Sevence II | | | | Ary | *) (Any | * |
| ~ | ۰. | ADDINTITY | TYPE | MAC ADDRESS | IP ADDRESS | STATUS | TIMESTAMP | |
| . • | 1 | isho@xystextpoc.comicrussft.com | Clarit Certificate | 30.141.70.41.01.40 | 192.108.118 | Sutten . | 11027/2023 12:02:34:321 | |
| | 2 | POTO | MAC Author/Heation | 18.01 die die Jurdie | | Datres . | 11/24/2023 12:08 24:025 | |
| * | 3 | P010 | MAC Automitication | 28/110e:08/30/0e | | (heren) @ | 1024/2025 12:04:14:826 | |
| | 4 | 0104 | MAC Automatication | 28/10/08/36/04 | | Falmet | 1024/2023 12/02/27/967 | |
| ¥ | 5 | isha@systestpic.onnicrosoft.com | Client Certificate | 10.16:7d-4t-01.4d | 192,166.131 | Second D | 11/73/2023 22:29:39.358 | |
| ٠ | 0.1 | Isha@xystestpac.onnicrosoft.com | Chert Certificate | 30.86/30.46/01.46 | 192,168,131 | Second 0 | 11/23/2023 22:20:12.585 | |

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

Figure 16-4: Client Session Details Page 2

| Details for Section | | | | | by Disconnet + Each |
|--|------------|--|----------------------------|----------------|-------------------------|
| Authentication Request | | decree. | Session Details | | Open |
| Authentication Type | | Client Certificate (EAP-TLS) | Client IP Appress | | 192.156.1.10 |
| legnent | | Defaum | Session Start Take | | 11/27/2023 12:02:04:321 |
| Location | | Media/Deh/DL-1 | Session Stop Time | | |
| A User | Frather | Ctern | Endied | Actions | |
| urhağlaşatestçec annikorasoft kinn taha | | 50.sm 7il 4lb 0f 4d Tarun Khanna's Android | | C Allow Access | |
| Access Device | Ariata WPI | 🖬 Network | Enabled | | |
| 94 ut 24. 10.00 of Tarun, Arista, w318,30.00 CF | | Centerna Canterna Client Centificate (EAP-TLS) | | | |
| Input Request Attributes | | · · | Output Response Attributes | | |
| Section loss for reducent Rel Milliology? (Thirty) | | | | | Show Loop |

3. Click the **Disconnect** button.

Figure 16-5: Client Session Details Page 3

| uthentication Request | | Success | Session Details | | Cover |
|--|------------|---|--|--------------|------------------------|
| Autoentication Type | | Client CentFcate (EAP-TLS) | Client IP Address | | 192,358.13 |
| Segment | | Default | Session Start Time | | 11/27/2023 12:02:34:32 |
| Location: " | | *Jindia/Dem/OL-1 | Session Stop Time | | |
| L User | Brabed | Client | Insted | Actions | |
| ha@aystestpoc.comicrosoft.com ha | | 30 bei 70 4b 0f 4d Tarun Khanna's Android | | Allow Access | |
| Access Device | Arista WP1 | - Hetwork | Endied | | |
| 1412410060 mm,Arista, x018,10.08-05 | | Canberta Canberta Cient Centificate (EAP-TLS) | Canterns © Canterns Chern Centificans (EAP-1)_55 | | |
| ut Becaret Attributes | | | Contrast Benarrows Attributes | | |

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

Figure 16-6: Client Sessions Details Page 4

| Session Details - Rcli3g0g4n37c72tsrtv0 Detaits for Session | | | b): Disconnect 4- Back |
|--|---|----------------------------|-------------------------|
| Authentication Request | Sutres | Session Details | Open |
| Authentication Type | Client Certificate (EAP-TLS) | Client IP Address | 192,566,516 |
| Teginert | Detaut | Session Start Time | 19/27/2023 12:02:34:321 |
| Location | */vita/Derv/DL-f | Season Stag Time | 15 |
| L User Butter | Client | Insided | Actions |
| Infragily procession and Learn Infra | 30 Star 70 40 TE-40 Tanun Khanne's Androist | | C Aron Access |
| Access Device Access | Disconnect An you sure you earl to disconnect Roldyby4x32x22mm Ca | Dessard Construct | |
| Input Request Attributes | * | Output Response Attributes | |
| Session logs for request: Bold3g0g4v33v72turtv0 | | | Bearings |

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

| and the second second | A | | | | |
|-----------------------|--|---|----------------------------|----------------|-------------------------|
| | Session Details - Rcli42t84n37c72tsrui0 Details for Session | | | | (class) |
| | Authentication Request | lucoma | Session Details | | Cper |
| | Automication Type | Clerk Certificate (EAP-TLS) | Ciert P Address | | 192.166.1.16 |
| | Segnet | Default | Session Start Time | | 11/27/2023 12:42:53.044 |
| | Located | *India/Deh//DL-1 | Session Stop Time | | |
| wider | 1 Uner | Clare | Entrat | Actions | |
| v dces v | Inhadpenteespec annicepsoft con- | 30 tb/7d 40.0% Ad Tarun Khanna's Android | | 😥 Allow Access | |
| | Access Device Andre W | a Network | Paint | | |
| 394 | Tarun, Arista, w318,10.08.CF | Centerna Crient CentRicate (EAP-TLS) | | | |
| | Inget Request Attributes | | Output Response Attributes | | * |
| | Provide last in second . But THE & TO THE OF | | | | (Phone and) |

Figure 16-7: Client Session Details Page 5

Now the client session status changes from Open to Closed.

Figure 16-8: Client Session Details Page 6

| Session Details - Rcli40gg4n37c72tsru90 Cotails für Session | | | | + Rock 🖶 |
|---|---|----------------------------|--------------|-------------------------|
| Authentication Request | Succese | Session Details | | Closed |
| Authentication Type | Client Certificate (EAP-TLS) | Client @ Address | | 192.168.118 |
| Sogreen | Default | Session Start Time | | 11/27/2023 12:37:46:145 |
| Location | *Andia/Dem/DL-1 | Session Stop Time | | 11/27/2023 12:39:42:152 |
| 1 User (Fuller) | Clean | Enabled | Actions | |
| Minalpepteopus anterminist com Note | 30 be /tg is (FA4 Tanus Khanna's Android | | Allow Access | |
| Access Davies Anits W/N el d1 24 100 pd Tranc, Arista, w318, 30 08 cd | Antosox Conterns Conterns Class Controlster (CAP 7(3)) | (fruitest | | |
| Input Request Attributes | × | Output Response Attributes | | * |
| Session logs for request: INIM40gg4x37x721xxx80 | | | | (Show Logs) |

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

Figure 16-9: Disconnect Debug Logs

E,



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

Figure 16-10: CoA Action Status

| | | | 6 6 |
|--|--|---------------------|---------------|
| Client Details - Aut View client details and up | to registered with UPSK adate the selected client | | e Back |
| | | | |
| Sessions for this client | | | Show Sessions |
| Client Activity | | | Hide Activity |
| Q Search by Activity type and | f status | | |
| ∧ # TYPE | STATUS | DATE & TIME | |
| ∧ 1 coa | Success | 12/1/2023 12:50:35 | |
| Details Access Device 30862dd07e8f | | | |
| ✓ 2 coa | Success | 11/28/2023 11:15:42 | |

Troubleshooting

17.1 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.

17.2 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 17-1: 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 17-2: AGNI Dashboard and charts

| CloudVision COGNi | | | | | • | <u>с</u> (|
|--|-------|------------------------------------|---|---|------------------|--------------|
| MONITORING | 1 | Dashboard View analytics | | | | ± Downlos |
| C Sessions | | 18:30 19:30 20:30 21:30 22:30 23:3 | 00 00 00 01 00 02 00 00 00 00 04 00 06 00 00 00 00 00 00 00 00 00 00 00 | 06:30 07:30 08:30 09:30 10:30 11:30 12:30 13:30 re 🗧 Total | 14:30 15:30 16:3 | / 17:30 18:3 |
| ACLs | | Top Failure Reasons | Today 🔂 Custom | Top Locations Affected By Failures | Today | tij 07/03 |
| Identity Provider User Glient Complementation | 2 | | • 768 TLS read failed | Man Office/Sound | | |
| Access Devices Certificates Administration Concourse | > > > | - | 3 Radius received timeout | 0 2 | 4 | Pérantérosé |
| Explore Installed Apps Collapse Sidebar | | Time is in UTC from 00:00 to 23:59 | | C Time is in UTC from 00-00 to 23-59 | ount | |

17.3 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 17-3: Monitoring Current Sessions

| | rg | | | | | | | | | | ତ ୭ 🖲 |
|-----------------------|----|---|--------|--|--------------------|-------------------|---------------|---------|---|------------------------|-------|
| MONITORING | | ~ | Ses | ssions of Sessions as on 7/24/2023 21:43:36 | | | | | | | |
| | | | | | | | | | | | |
| ACCESS CONTROL | | ٩ | Search | by Identify, MAC Address, IP Address or Session ID . | | | | Any | | * Success | • |
| ACLS | | ^ | | IDENTITY | TYPE | MAC ADDRESS | IP ADDRESS | STATUS | | TIMESTAMP | |
| (A) Identity Provider | | * | 128 | rachael.ray@testorg1.com | Captive Portal | ba:ba:d2:15:b9:bc | 192.168.1.102 | Success | • | 7/20/2023 18:59:16.781 | ۲ |
| L User | ~ | ~ | 129 | rachael.ray@testorg1.com | Captive Portal | baibaid2:15.b9:bc | 192.168.1.102 | Success | | 7/20/2023 18:59:08.167 | 0 |
| | ۷ | ~ | 130 | rachael.ray@testorg1.com | Captive Portal | ba:ba:d2:15:b9:bc | 192.168.1.102 | Success | • | 7/20/2023 18:58:47.539 | 0 |
| Access Devices | ~ | ~ | 131 | rachael.ray@testorg1.com | Captive Portal | ba.ba.d2:15:b9:bc | 192.168.1.102 | Success | | 7/20/2023 18:56:33.477 | ø |
| Certificates | Y | ~ | 132 | alice@agniglobal.onmicrosoft.com | Client Certificate | 0a.89.fd:e0:29:07 | | Success | | 7/20/2023 18:47:15.895 | 0 |
| System | ~ | ~ | 133 | rachael.ray@testorg1.com | Captive Portal | babad2:15:b9:bc | 192.168.1.102 | Success | | 7/20/2023 17:55:17:188 | • |
| Explore | | ~ | 134 | soham⊜xyz.com | Unique PSK (UPSK) | 98:60:ca:34:7c:ad | 192.168.1.138 | Success | • | 7/20/2023 17:54:19.136 | 0 |
| Installed Apps | | ~ | 135 | soham@xyz.com | Unique PSK (UPSK) | 98:60:ca:34:7c:ad | 192.168.1.138 | Success | | 7/20/2023 17:51:18.691 | • |
| | | ~ | 136 | soham@xyz.com | Unique PSK (UPSK) | 98:60:ca:34:7c:ad | 192.168.1.138 | Success | | 7/20/2023 17:51:13.129 | 0 |
| | | ~ | 137 | bill.gates@testorg1.com | Captive Portal | c4:75:ab:f5:e1:00 | 192.168.1.105 | Success | | 7/20/2023 17:41:50.735 | 0 |
| | | ~ | 138 | richard@antaraai.net | Captive Portal | c4:75:ab:15:e1:00 | 192.168.1.105 | Success | • | 7/20/2023 17:41:20.771 | 0 |
| | | | 100 | 2.5 | (m. 10 m. 10) | | 400 400 4 407 | Galance | | | |

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

| CloudVision QQ∩i | | | | | | 6 Ø 💽 |
|--|---|-------------|--|----------------------------|--------------|------------------------|
| MONITORNO | Session Details - Roils9e5j0h1 Details for Session | s72sc27mg | | | | (* Botk) 👼 |
| ACCESS CONTROL | Authentication Request | | Success | Session Details | | Cosed |
| 🐨 Networks | Authentication Type | | Client Certificate (EAP-TLS) | Client IP Address | | 10.86.60.228 |
| 411 Segments | Segment | | Default | Session Start Time | | 7/10/2023 14:13:36.305 |
| CLS IDENTITY | Location | | | Session Stop Time | | 7/10/2023 14:13:46.924 |
| A Identity Provider User | L User | Enabled | Client | (Frabled | Actions | |
| Client v Controlitation Controlitati | steve kratt Steve Kratt | | 70:1a b8 82 10 31 Steve Kratt's Windows | | Allow Access | |
| System v | Access Device | Arista WIFI | a Network | Enabled | | |
| Explore | 30.86.24.00.07.af Pune-C235AP | | PUNE-WIVA2 PUNE-WIVA2 Client Certificate (EAP-TLS) | | | |
| K Collapse Sidebar | Input Request Attributes | | • | Output Response Attributes | | •) |

Figure 17-4: Session Details

Figure 17-5: Session Details page 2

| and designed | | Session Details - Rolls9x5j0h1s72sc27mg | | | | * bes |
|---|------|---|--------------------|---|--|---|
| é chétén, | | · Ausses Trains | Anna APT | a notes | (hand) | |
| elacity agrocits dLa | | 20 Marce et et al Press (23344) | | Hand white Transit animal Chart Careform Gall (1,0) | | |
| antity Provider | | | | | | |
| | 8 | Trated Responsed determination | | ÷ | Original Perspirates Addributes | |
| and the second se | .e., | Carolicate D1 | | Disa Liki | Refeat & P. Clevil | initeratiji/statisi/200g/dantis/16.nemi ili42.412n-britaitato |
| rent Doubes | 14 | Carlfront DecCalipry | | 81 | Sudici (177-147-Herrige | |
| otherses . | ÷. | Carthine hine | Universe, hour DAD | CTR2+a Rana d'AMTERIA anti-anni-anti-anti-athantetanàs | Destroy 2017 (Second Paramet | 7.464 |
| abain | іж | Card State (State | | more confidential con- | Reduct 117 Terrenamen Arten | |
| | | Cardfoole Sullier | | Una constant, Daning Com | Reduct Managert (4), Wing data (a) | |
| and a second second | | Radius & TP-Rook, Salaman, ca | | 1114401/10110011/101011/10100 | C Replie Million Phys. (PTTE 1949) 761 | |
| and Appa | | Radius (17-Laber Darten id | | TO BE TO DO IN WORKS WINT | | |
| | | satured to camp orders of | | 10.00.00.00.00.00 | | |
| | | Reducid In Connect only | | CONNECT DIMAGN \$12.79 | | |
| | | Testucid IT 11P concept | | | | |
| | | Refueld IT fremed WTV | | 1418 | | |
| | | Rafterit IT Inside a forterit for | | | | |
| | | Autor (1996) - Autors | | | | |
| | | | | | | |
| | | Rear IV and the fun | | | | |
| | | And and the second second second | | | | |
| | | Balance Witness Alerea | | (hote) | | |
| | | Instruct The New Address of the | | automa a | | |
| | | Bashon R.W.W. Als Droug Carrier | | 1000 | | |
| | | Radius (117-06, Ale-Factoria-Capital | | 1027074 | | |
| | | | | | | |

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 17-6: Sessions and Show Logs

| าเ | | | | | | ~ O | | | | | |
|--|---|--|--|---|---|--------------------------|--|--|--|--|--|
| need to be a company of the second se | Session Details - Rolls9e5j0h1s72sc27mg Tetats to Texas | | | | | - 8ml | | | | | |
| instant | input | | | water fair the | | interaction of the party | | | | | |
| Converses. | and a second sec | | | Income from Time | | Stations to mark | | | | | |
| riserite | | | | | | | | | | | |
| apresenta. | 1 | (Doman) | D and | (Instant) | 11 cannot | | | | | | |
| dia . | | | 1 TO 1 TO 1 | | and the second se | | | | | | |
| | 1000 A 21 21 - | | 70 teld 60 10 11 | | (i) Alson Access | | | | | | |
| and by Provident | Dave want | | Stood Woald's Westpare | | | | | | | | |
| | | | | | | | | | | | |
| and in the second | | | | | | | | | | | |
| a.Af scim | Accession | (Annu MAT) | d attest | (Anations) | | | | | | | |
| man Devices - | | | | | | | | | | | |
| outputters | 10.000.200 of 107 of | | PL/M W192 | | | | | | | | |
| 200 Store 1 | Pure C231AP | | All All All All All All All All All All | | | | | | | | |
| | | | Steet Dentricate (GAP, TL31 | | | | | | | | |
| | | | | | | | | | | | |
| al all and the second | Incluing American A American American Ame | | | | | | | | | | |
| Process (Addres) | Negative Antonia Allanda Allanda A | | | | | | | | | | |
| | Contraction of the second second second | | | | | (here) (state | | | | | |
| | and the relation of the second second second | | | | | Channel Channel | | | | | |
| | (inter | | | | | | | | | | |
| | | | | | | | | | | | |
| | TYDE 2022 18-12 (no. 201 DFD) [pt:ED-05 tyDE)[transaction of Experimental DFD and the DFD and the Advance of the DFD Experimental CPUES, Restrict (ED7) and the Advance DFD (1), Restrict (ED7)[1], Rest | Trigger 14 (3.5.8) (M) (M) (M) (M) (M) (M) (M) (M) (M) (M | | | | | | | | | |
| | 198(00) IA-02/0.401 MPT (C-09970) C-0011-0404704C (C-04110-02001/10-050) - 00000 C-04001 C-04000-04020100-04021 C-04000-04021 C-040016 | | | | | | | | | | |
| | Transient is 10.3.3. Net ()-Prefine coll-and-Web-disadframe, industrie/particultury/antitury/agi (mono)(ments) - education (ments) - and mental (mental (ments)) - and mental (mental (men | | | | | | | | | | |
| | 1/38/2802 34 25 26 297 2972 [1-07471256-5402-641-0 | A (19/201) IN TO 20/20 A (19/20) AND AND AND A COMPLEMENT POLITICAL AND | | | | | | | | | |
| | Aranyanan kalan ini ana amir (sumerniko-nami-neo) en | thermostronic science(procedurity) corts | a - build was server sert chain in 4.6681000 | | | | | | | | |
| | True (mill 40-40-16-201 2000) (1)-(Torritor - add-446)-0 | an anaantiisen is holootaljanastielijng) onsi | ai(sag) : (sad select[com]ac106-00-00001, Hood CA.0-7000 | u-Arta (47647314; seit ess) 4367-4736487364813 | | | | | | | |
| | Transmit in to to the test of the proof that we have | or analytical indiation(montalized) on | orings) - ling rates[ink]eritSki9k#00[1, linee CB.0/91 | Ne bria (ESERVIEL-ext) Anni-1007-258487368013 | | | | | | | |
| | 1/26/28/2 18 11:16:111 2011 [1.179*1784-9421-864119 | (1-(74048720401 10-0)(1/10-[]0010/10-(2042] *4010 | alant) - prot finite-see together with convergencembersee | Childre endlightStreet#111110-54114 andthelltite:#1 | constants and constants of a second second | < | | | | | |
| | Tratigital to 11.16.101 (MPD [1-07071056-0101-0001-00 | a street in a second provided second | is satisfied a state. "It's farefully here one a consent closed | permitty-stew-bratt; be seen aloust belie | | | | | | | |
| | 1/0+/24/2 1a 1/ 14 /4/ 14/2 14/2 14/2 14/2 | r-chasting prophetical (main the | la-server) - plprl heidydde | | | | | | | | |
| | Transmission of the local state of the second | and an appropriate the state of | the second a state 755 heatingth and reasons a | on closed to Tol | | | | | | | |
| | side bill be in to be state that it distant and which a | en a mendente in antitue (mendenter ball alle | The second s | | | | | | | | |
| | topicarity to the lot of the state of the Parities, and the state | and shareful and supplications for the state | The second of the "The manufacture" and income in | () has | | | | | | | |
| | | and a second second second second | | | | | | | | | |
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 industrystandard 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.
- 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

| Microsoft Azure | P Search resources, services, and docs (G+/) | | 🖂 🛱 🖉 🛞 🕐 🦗 зирагла@agniglobal.on 🛔 | |
|--|--|---|---|--|
| Home > AGNI Demo Org App reg | gistrations ≥ AGNI Demo I permissions 🖉 … | Request API permissions | × | |
| Search Overview Ouckstart | O Refresh R Got feedback? A You are editing permission(s) to your application, users will have to consent even if they've | Microsoft Graph http://graph.microsoft.com/ Docs ©* What type of permissions does your application require? | | |
| Arberation assistant Manage Branding & properties Authentication Certificates & secrets Token configuration AP permissions Approxies Approxies | Configured permissions Applications are authorized to call APs when they are granted permissions by users/admin: all the permissions the application needs. Learn more about permissions and consent | Delegated permissions Your application needs to access the API as the signed-in user. | Application permissions Your application runs as a background service or daemon without a signed-in user. | |
| | + Add a permission 🗸 Grant admin consent for AGNI Demo Org | Select permissions P user read all | equad all X | |
| | Monsoft Graph (4) Directory Read All Application Read directory data | Permission > IdentityRiskyUser | Admin consent required | |
| | Group Read All Application Read all groups Group Member Read All Application Read all group memberships User Read Delegated Sign in and read user profile | User (t) User Read.All ⊙ | Yes | |
| Owners Owners Roles and administrators Manifest Support + Troubleshooting | Other permissions granted for AGNI Demo Org These permissions have been granted for AGNI Demo Org but aren't in the configured per adding them to the configured permission is fat Lemm more | Read an user' ful profiles | | |
| Troubleshooting New support request | API / Permissions name Type Description | | | |
| | User Read All Application Read all users' full profiles | | | |
| | To view and manage consented permissions for individual apps, as well as your tenant's cor | Add permissions Discard | | |

Table 1: API Permissions table

| API Permission | Туре | Admin Consent | Status |
|----------------------|-------------|------------------------|---------------------|
| Directory.Read.All | Application | Grant admin consent | |
| Group.Read.All | Application | es 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 <u>EAP-TLS based Enterprise SSID using CV-CUE and</u> <u>AGNI: Configuration and Onboarding</u> article.

See the following tables 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 | |

Table 3: URLs, Ports, Protocols, IP Address

| AGNI Cluster - DNS Name | Port | Protocol | IP Address | Usage | | | | |
|---|---------|----------|----------------|-------------------|--|--|--|--|
| BETA (Region - us-central1, Location - Council Bluffs, Iowa, North America) | | | | | | | | |
| beta.agni.arista.io | 443 | https | 34.36.123.182 | Launchpad UI, API | | | | |
| radsec.beta.agni.arista.io | 2083 | tcp | 34.121.180.70 | RadSec | | | | |
| US (Region - us-central1, Location - Council Bluffs, Iowa, North America) | | | | | | | | |
| ag01c01.agni.arista.io | 443 | https | 34.107.152.8 | Launchpad UI, API | | | | |
| radsec.ag01c01.agni.arista | a.20083 | tcp | 35.202.91.175 | RadSec | | | | |
| EUROPE (Region - europe-west3, Location - Frankfurt, Germany, Europe) | | | | | | | | |
| ag02w03.agni.arista.io | 443 | https | 34.160.66.7 | Launchpad UI, API | | | | |
| radsec.ag02w03.agni.arist | a2083 | tcp | 34.107.34.202 | RadSec | | | | |
| ASIA (Region - asia-south1, Location - Mumbai, India, APAC) | | | | | | | | |
| ag03s01.agni.arista.io | 443 | https | 34.36.152.229 | Launchpad UI, API | | | | |
| radsec.ag03s01.agni.arista | a.20083 | tcp | 34.100.196.137 | RadSec | | | | |
| Australia (Region - australia-southeast1, Location - Sydney, Australia, APAC) | | | | | | | | |
| ag04s01.agni.arista.io | 443 | https | 34.54.24.124 | Launchpad UI, API | | | | |
| radsec.ag04s01.agni.arista | a 20083 | tcp | 35.189.21.239 | RadSec | | | | |