ARISTA

User Guide

AGNI (On Premises) Arista Guardian for Network Identity

Version P-2024.4.0



Arista.com

Arista Networks

DOC-07691-01

Headquarters	Support	Sales
5453 Great America Parkway Santa Clara, CA 95054 USA		
+1-408-547-5500	+1-408-547-5502	+1-408-547-5501
	+1-866-476-0000	+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 On-Prem Overview	
1.1 Prerequisites	
1.2 Accessing Launchpad App	
1.2.1 Adding Organizational Details	
1.2.2 Adding Account Details	
1.2.3 Adding API Tokens	7
1.2.4 Launch App from Dashboard	
1.2.5 Viewing Nodes in Cluster	
1.2.6 User Interface (UI) Theme	11
1.2.7 Viewing Licensing Details	
1.2.6 User Interface (UI) Theme	1

Chapter 2: Integrating with Concourse Applications (Internal)	13
2.1 Arista CV-CUE Integration	
2.2 Arista CloudVision Integration	
2.3 Arista CloudVision Portal (CVP) Integration	
2.4 Configuring CVaaS Instances.	18
2.5 Adding Multiple CVaaS Instances in AGNI	
2.6 Arista NDR Integration	20
2.6.1 Configuring Arista NDR	23
2.6.2 Configuring Segment Policies	27
2.6.3 Using Risk Action in Segment Policies	30

Chapter 3: Integrating with Concourse Applications (External)	32
3.1 Palo Alto Cortex XDR Integration	
3.2 Medigate Integration	
3.3 Microsoft Intune Integration	34
3.4 Jamf Integration	
3.5 ServiceNow CMDB Integration	37
3.6 Splunk Integration	
3.7 Sumo Logic Integration	40
3.8 CrowdStrike Integration	41
3.9 Workspace ONE Integration	42

Chapter 4: Configuring Identity Providers	45
4.1 Microsoft Entra ID 365 (Azure)	
4.2 OneLogin	
4.3 Okta	
4.4 Google Workspace	53
4.5 Local	

Chapter 5: Configuring the Networks	
5.1 Configuring Client Certificate Network	
5.1.1 Configuration Steps	
5.1.2 Authenticating Users with Email Codes (as against IDP)	59
5.1.3 Wireless Configuration on Devices	63

5.2 Configuring Unique PSK (UPSK) Network	82
5.2.1 Configuring the UPSK Settings	
5.2.2 Configuring the Device Count Limit for Authentication	
5.3 Configuring Wireless Captive Portal Network	
5.3.1 Configuration Steps	
5.4 Configuring Wireless MAC Authentication Network	
5.4.1 Configuration Steps	

Chapter 6: Configuring Wired 802.1X Network	91
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	104
7.1 Status	
7.2 Conditions	
7.3 Actions	
7.4 Configuration	
7.4.1 Sample Segments	

Chapter 8: Configuring the Devices in AGNI	109
8.1 Adding an Access Device	
8.2 Importing Devices into AGNI	

Chapter 9: User Configurations	
9.1 Users	
9.1.1 All Users	114
9.1.2 External Users	
9.1.3 Local User	
9.2 User Groups	
9.2.1 Local User Groups	117

Chapter 10: Client Configuration	118
10.1 Clients	
10.2 Client Details	
10.3 Creating Client Certificates Manually in AGNI	122

Chapter 11: Guest Onboarding Features	
11.1 Guest Onboarding Using AGNI	
11.1.1 Guest User in AGNI	
11.2 Guest Onboarding Offerings in AGNI	134
11.2.1 Portal Based Guest Onboarding	
11.2.2 Guestbook Based Onboarding	
11.2.3 UPSK Based Guest Onboarding	
11.3 Configuring UPSK for Onboarding Guest (Wireless)	

11.3.1 Configuring AGNI	146
11.3.2 Configuring CV-CUE	149
11.3.3 Onboarding the User	
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)	
11.5.1 Configurations on AGNI	
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)	
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	
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-Registration (Wired)	182

Chapter 12: G	enerating Client Certificates for RadSec	
12.1 Viewing t	the Certificates	
•	ring Device Groups	
5	5	

Chapter 13: Overview - TACACS Plus with AGNI	
13.1 Configuring TACACS Plus on Arista Switches	
13.2 Enabling Device Administration on AGNI	
13.3 Configuring TACACS Plus on AGNI	
13.4 Monitoring TACACS Plus on AGNI	
13.5 Accessing Device Admin Portal on AGNI	

Chapter 14: System	
14.1 Audit Viewer	
14.2 Self-Service Portal Settings	
14.3 RadSec Settings	
14.4 Support Logs	
14.5 System Events	
14.6 Notification Settings	
14.6.1 Configure Email Settings	
14.6.2 Configuring SMS Gateway	

Chapter 15: Sessions	214
15.1 On-Demand Disconnecting a Client from the Network	215

Chapter 16: Troubleshooting	

16.3 Sessions	
Appendix A: Appendix	
A.1 OIDC Vs SAML	
A.2 Identity Providers	
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 On-Prem Overview

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

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

The key features of CloudVision AGNI includes:

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

1.1 Prerequisites

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

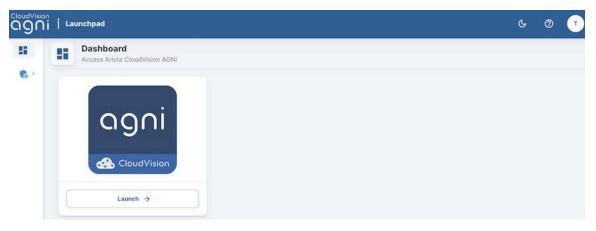
- · Release Notes for AGNI ON Premises available on Arista website:
- DCA-AGNI-100 Appliance Quick Start Guide available on Arista website: https://www.arista.com/en/ support/product-documentation/hardware.
- Setup and Access Guide for DCA-AGNI-100 appliance available on Arista website: https:// www.arista.com/en/support/product-documentation.

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

1.2 Accessing Launchpad App

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

Figure 1-1: AGNI On Prem Launchpad



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

Figure 1-2: On Prem Launchpad with Admin Tasks



1.2.1 Adding Organizational Details

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

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

Figure 1-3: Organization Details with Identity providers

Organization Details Manage organization name and identity provider	
Organization Name	
OnPrem-Pune	
Organization Domain	
mojonetworks.com	
Identity Provider	
G Google Workspace	
G Google Workspace	
Microsoft Entra ID	
O Okta	
1 OneLogin	

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



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

Figure 1-4: Organizational details on AGNI Launchpad

CloudVision	Launchpad	
	Organization Details Manage organization name and identity provider	
6 >	Organization Name OnPrem-Pune Organization Domain mojonetworks.com Identity Provider	
	G Google Workspace	•
	OIDC Client Secret	0
		Save

1.2.2 Adding Account Details

E,

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

Note: As part of the initial AGNI Appliance (DCA-AGNI-100) bring-up and setup, the following default accounts are created in the **Admin** > **Accounts** section.

- Organization Account An Organizational User account is created with the customer's registered email. This would be the same account used during the initial AGNI Appliance bring-up and registration.
- Local Account A Local User account is also created with the same name used in Organization User Account Name. This would be the primary account for users when they login to the AGNI GUI for the first time.

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

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

Figure 1-5: Admin User Accounts

Dashboard	Admin User A Manage the admin	Accounts n user accounts, who can access Arista CloudVision AGN	I, and their privileges.		+ Add Acc	count
Admin	All Users Super Adm	inistrator Administrator Operator			C	3 8
22 Accounts	Q Search by name or en	nail		An		÷
API Tokens						
Nodes	# NAME 个	USERNAME	ROLE	STATUS	ACTION	IS
	1 Tarun Khanna	shrirang.chikodikar@mojonetworks.com	Super Administrator	Enabled	1	0
	2 Tarun Khanna	shrirang.chikodikar	Super Administrator	Enabled		0

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

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

Figure 1-6: Update Accounts

Dashboard Admin ^	Fill in the following fields to update the selected Admin user details.
 Organization Accounts API Tokens Nodes 	Name Tarun Khanna User Type: Local username shrirang.chikodikar Email Address shrirang.chikodikar@mojonetworks.com Optional, use email address to get the credentials emailed to the user. User Role Super Role Super Administrator
	Status: Enabled

A local account with the specified privileges is created.

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

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

Figure 1-7: Card View of User Accounts

Dashboard	Admin User Accounts Manage the admin user account	its, who can access Arista C	loudVision AGNI, and their privileges.			+ Add Accor
Admin ^	All Users Super Administrator	Administrator Operat	or			C
# Accounts	Q. Search by name or empil				Any	
API Tokens						
Nodes		Invited	(E	inabled	D	Enabled
	Maya	Tan	un Khanna		arun Khanna	
	abc.xyz	shri	irang.chikodikar@mojonetworks.com		hrirang.chikodikar	
	Super Administrator	Su	per Administrator		Super Administrator	

1.2.3 Adding API Tokens

Ξ,

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

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

agn CloudVision	Launchpad	Add Admin API token	6 © T
	Admin API Toker Manage the admin use	Fill in the details to create a new API token to access Arista CloudVision AGNI	+ Add API Token
6 >	Q Search by name	Token Name operator	
		Read-Write	
	_	Allow read-write access to Arista CloudVision AGNI product	
		Token Validity (days)30	
		Cancel Add Token	

Figure 1-8: Add Admin API Tokens

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

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



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

Figure 1-9: API Token Details

Admin API T Manage the adm	okens In user API tokens to access Arista CloudVision AGNI product using APIs	+ Add API Token
Q. Search by name		
	Add Admin API token Fill in the details to create a new API token to access Arista CloudVision AGNI	
	Token Nime OnPrem-bir	
	Read-Write	
	Ticken Validity (days)	
	For security reasons, the token will NOT be shown after closing this window.	
	eyJhbGciOiJFUz11NilsInR5cCl6lkpXVCJ9.eyJvcmdJRCl6lk	
	Close	

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

Figure 1-10: API Documentation Access

Dashboard	Dashboard Access Arista CloudVision AGNI	Help
Admin ~	Access Aliste Cloudyision Acini	User Guide 🔀 Community Central 🗹
		API Documentation
	agni	Product Version P-2024.4.0
		Software Image Version 25.0115.0534

1.2.4 Launch App from Dashboard

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

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

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

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

Dashboard	Email Settings are not configured. Click here to configure.		
Sessions CESS CONTROL Networks	View Analytics		In-mh04-pl-agni-01 png.aristanetworks.c
Segments ACLs NTITY	users 2 5	CLINNTS 23	Accessbrvices
Identity Provider User Client	Sessions Trend	Click here to view Clients.	Click here to view Access Devices.
Guest Access Devices Device Administration Certificates System	2 2 3 3 3 3 3 3 3 3 3 3 3 3 3		
Explore	50 1000 0100 0100 0100 0100 0100 0100 1500 1600 1750 1890 1990 2000 2100 22	1999 0109 0110 0110 0110 0110 0110 0110	tino otrio otrio otrio otrio otrio otrio otrio otrio 730 0830 0930 1030 1130 1230 1330 1430 153
wcourse Explore Installed Apps	0109 0109 0109 0109 0109 0109 0109 01	230 23:30 00:30 01:30 02:30 03:30 04:30 05:30 06:30 0	730 0830 0930 1030 1130 1230 1330 1430 153

Figure 1-11: Dashboard

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

1.2.5 Viewing Nodes in Cluster

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

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

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



E

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

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

Figure 1-12: Nodes List and Status

oudVisio IGN		unch	npad				Ċ.	0	Ţ
5			odes t of Nodes and their	r details.					
G >	^		ADMIN IP	DATA IP	HOSTNAME	ROLE	HEALTH STATUS		
	~	1	10.87.128.200	10.87.129.200	in-mh04-pl-agni-01.pnq.aristanetworks.com	Principal	Healthy		
	~	2	10.87.128.201	10.87.129.201	in-mh04-pl-agni-02.pnq.aristanetworks.com	Standby	Healthy		Ø
	~	3	10.81.204.15	2	bm15.agni.sjc.aristanetworks.com	Auxiliary	Needs Attention		

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

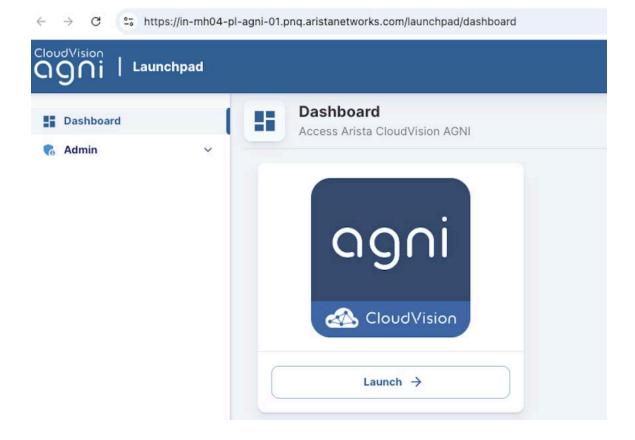
Note: Check the node separately if any node's health status displays the status as "Needs Attention".

Figure 1-13: Viewing Health Status of Nodes

	••	Nod List o	les f Nodes and their (details.				
	^	#	ADMIN IP	DATA IP	HOSTNAME	ROLE	HEALTH STATUS	
	^	1	10.87.128.200	10.87.129.200	in-mh04-pl-agni-01.pnq.aristanetworks.com	Principal	Healthy	
- 6	Gui	rent Not	de is healthy					
	~	2	10.87.128.201	10.87.129.201	in-mh04-pl-agni-02.pnq.aristanetworks.com	Standby	Healthy	
	^		10.87.128.201	10.87.129.201	in-mh04-pl-agni-02.pnq.aristanetworks.com	Standby	Healthy	
	^ Rea	2	10.87.128.201	10.87.129.201	in-mh04-pl-agni-02.pnq.aristanetworks.com	Standby	Healthy	
	A Rea He	2 chabilit	10.87.128.201 y		in-mh04-pl-agni-02.pnq.aristanetworks.com aristanetworks.com successful	Standby	Healthy	
	Rea He Rea	2 chabilit	10.87.128.201 y y check to https://in-			Standby	Healthy	

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

Figure 1-14: Launchpad for Nodes



1.2.6 User Interface (UI) Theme

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

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

agni I																								¢	, 0	•
MONITORING	1		ishboar w Analytic																į	ben19.ag	mi.ajc.aria	tanetworks		Navig	ation	
Sessions Access contract Networks sla Segments Acces		USERS Click here		ers.						Click	ers 4 here to vie	ew Clients.							Sec. Sec.	10	ccess Dev	ices.	19	Color Sc	hemes	
Sentity Provider		Sessions	Trend																							
Client	3 3	20 13																		\wedge						
Access Devices Device Administration	¥ ¥	47																								
Gertificates	*	01.06 10.30	01.06	01.06 12.30	01/06 13/30	01.06	01.06 15:00	0108 16:00	61.06 17.30	01.06 18:30	01.06 19:30	01.06 20:30	01.06 21.30	01.06 22.30	01.06 23:30	01.07 00:00	0107	01.07 02:30	61.67 63.30	01.07 04.30	01.07 05:30	01/07 06:30	01.07 07.30	01.07	01.07 09.30	01.07 10:30
concounts													• 1	tai efalu	*											

1.2.7 Viewing Licensing Details

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

Figure 1-16: AGNI License Details

ngni I			
MONITORING		License License Details	
Sessions ACCESS CONTROL		License Details	
Networks		Туре	Trial
l≐ Segments		License count	1000
IDENTITY		Valid until	03/01/2026 01:14:57
Identity Provider User Client Guest configuration	~		
Access Devices	~		
Device Administration	~		
Certificates	~		
System	~		
Audit Viewer			
License			

Chapter 2

Integrating with Concourse Applications (Internal)

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

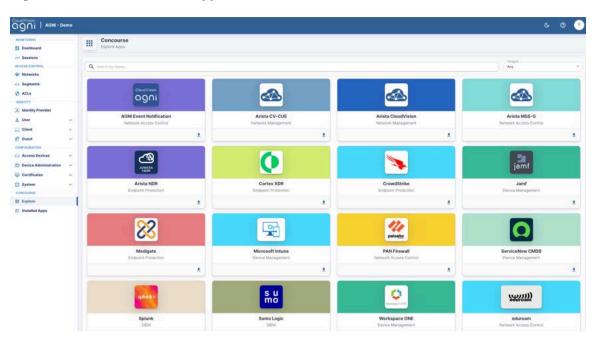


Figure 2-1: AGNI Concourse Applications

2.1 Arista CV-CUE Integration

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

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

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

c. CV-CUE Key Value

Figure 2-2: Verify CV-CUE Application

Maintown Maintown Maintown Sabbbaud Maintown Sabbbaud Maintown Sabbbaud Maintown Mainto	
Acts Control Acts Control Acts CUP-DUE Control 0 Acts Control 0 Acts Acts Control 0 Acts A	
Anisa CV-CUE P Networks Is segments Actiss CV-CUE // CV-CUE	
Is Segments (KEY-ATNS67556-1192-1 OCTOT YY Solentity Provider	
ACLs CV-OIX Fay Way Lisentity Provider	
DONTRY C C C C C C V C C V C V C C C C C C C C	
2) Identity Provider	
- identity Provider	
Landquad ARUR.	
L User Y https://aunchpad.wif.arista.com/api/v2	
Client Y District Control of Cont	

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

Figure 2-3: Installing CV-CUE Application

SUCANON I NONI-D	imó				
MONTORNE S Dashboard	3	Arista CV-CUE Enter the following fields to centigure the app.			+ Back
N Sessions					
ACCESS CONTROL		Anna CV-CUE			
Networks		Contract Name Of			
ALA Segments		KEY-ATN587856-2432			
ACL8		for Out my more			
REHTITY		c02828x008f8ac4cea863ce77b040223f			6
K Identity Provider		Lawrence Art UK			
I User	Y.	https://teurohpad.wth.ansta.com/epi/v2			
Client	*				_
# Guest	4		Cancel	Vertty	batal
CONTINUESTICIE					
Access Devices	81				
Device Administration	Ψ.				
G Contificates	10				
System	4				
CONCOURSE					
III Explore					
EF Installed Apps					

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

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

Figure 2-4: Synchronizing CV-CUE App

	Arista CV-CUE Enter the following fields to update the selected app.	← Ba
	Arisis CV-CUE Cr-Oc 49y 0 KEY+ATN567856-1192-1 CV-CUE 49y 0mr	
×	Launinger M1 UK. https://launchpad.wifi.arista.com/api/v2	
•		Cancel Verify Update
~ ~	Synchronization Details	
*	Location and Access Device information will be synced from CV-CUE.	
ី	Last Successful Sync At	16/07/2023 10:30:0
	Last Sync At	07/01/2025 11:30:04
	Syne Status	Partial Success Sync Now
	2 2 2 2	Anita CV-CUE V OI Ny 0 KCY-ATK65/858-1192-1 V OI Ny 50 KCY-ATK65/858-1192-1 V OI Ny 50 Synchronization Details Synchronization Details O Location and Access Device Information will be synced from CV-CUE. Last Successful Sync At Last Sync At

You can view the synchronized Access Points by navigating to:

Configuration > Access Devices > Devices (see image).

٩	Search by Name, MAC Addres	is, IP Address or Location					Arista WiFi	
	NAME	IP ADDRESS / SUBNET	MAC ADDRESS	VENDOR	LOCATION	UPDATE	TIME	
1	Arista_CA:9A:0F	10.81.204.94	30-86-2d:ca:9a:0f	Arista WiFi	*/North America/Bassett Lab	07/01/20	25 05 22 38	
2	Arista_B1:D0:3F		30:86-2d:b1:d0:3f	Arista WiFi	*/Boston/Boston-CustomCert	03/01/20	25 03:14:34	
3	Atul-C200	192.168.0.163	30:86:26:92:bd:9f	Arista WiFi	*/North America/Boston	03/01/20	25 03:14:34	
4	Arista-C200-9155df	172.211.58	30:86:2d:91:55:df	Arista WiFi	*/North America/Bassett Lab	03/01/20	25 03 14 34	
	# 1 2 3	# NAME 1 Arista_CA:9A:0F 2 Arista_B1:D0:3F 3 Atul-C200	1 Arista_CA:9A:OF 10.81.204.94 2 Arista_81:D0:3F 3 Atul-C200 192.168.0.163	# NAME IP ADDRESS / SUBNET MAC ADDRESS 1 Arista_CA:9A:0F 10.81204.94 30.86/2dxa9a:0f 2 Arista_B1D0:3F 30.86/2dxa9a:0f 30.86/2dxa9a:0f 3 Anul-C200 192168.0163 30.86/2d:92:09/2d:0f	# NAME IP ADDRESS / SUBNET MAC ADDRESS VENDOR 1 Arista_GA:9A:0F 10.81204.94 30.862dxa.9a:0f Arista_WFI 2 Arista_B1:00:3F 30.862dxb1:d0:3f Arista_WFI 3 Atul-C200 192:168.0163 30.862dxb1:d0:3f Arista_WFI	# NAME IP ADDRESS / SUBNET MAC ADDRESS VENDOR LOCATION 1 Arista_GA 9A:0F 10.81204.94 30.86.2d cc.92.01 Arista_WFi */North America/Bassett Lab 2 Arista_B100:3F 30.86.2d b1:d0:37 Arista WFi */Boston/Boston-CustomCert 3 ANI-C200 192.168.0163 20.86.2d 92.bd.9f Arista WFi */North America/Boston	# NAME IP ADDRESS / SUBNET MAC ADDRESS VENDOR LoCATION UPDATE 1 Arista_CA:9A:0F 10.81204.94 30.86/2d xb:a0.0f Arista W/Fi */North America/Bassett Lab 07/01/20 2 Arista_BI:00:3F 30.86/2d xb:a0.3f Arista W/Fi */Boston/Boston-CustomCert 03/01/20 3 Atu-C200 192.168.0163 30.86/2d:92:bd:9f Arista W/Fi */North America/Boston 03/01/20	# NAME IP ADDRESS / SUBNET MAC ADDRESS VENDOR LOCATION UPDATE TIME 1 Arista_GA:9A:0F 10.81204.94 30.862d:cx/9a:0f Arista_WFI */North America/Bassett Lab 07/01/2025 05:22:38 2 Arista_B1:00:3F 30.862d:b1:d0.3f Arista_WFI */Boston/Boston-CustomCert 03/01/2025 03:14:34 3 ANd-C200 192:168.0163 20.862d:92:bd.9f Arista_WFI */North America/Boston 03/01/2025 03:14:34

2.2 Arista CloudVision Integration

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

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

Prerequisites

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

Integrate CloudVision by installing the application as a Concourse App on the AGNI portal. To install CloudVision, perform the following steps:

- 1. Navigate to Concourse > Explore.
- 2. Install the Arista CloudVision application.
- 3. Enter the following parameters:
 - a. Arista CloudVision in the Name field.
 - **b.** The URL of the CloudVision application.
 - c. API Token value.

Figure 2-6: Installing Arista CloudVision Concourse Application

MONITORING		Arista CloudVision Enter the following fields to update the selected app.	← Back
CCESS CONTROL		Com	
Networks		Arista CloudVision	
ACLs		https://www.arista.io/	
IDENTITY (2) Identity Provider			
L User	×	To add secondary CloudVision Servers, click here	
Client	~		
Guest	~	Secondary Servers	
Access Devices	^	Secondary Server https://www.arista.io	/ 0
Devices		second	/ 0
Device Groups Cloud Gateways		http://www.arista.io/	
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).

2.3 Arista CloudVision Portal (CVP) Integration

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

CHECK THIS PAGE AFTER GETTING DETAILS FROM SHRIRANG/Venky

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

Prerequisites

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

Integrate CloudVision by installing the application as a Concourse App on the AGNI portal. To install Arista CloudVision Portal, perform the following steps:

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

Figure 2-7: Installing Arista CloudVision Portal Concourse Application

agni onPrem-			G	Q	T
Moterformo S Dashboard Sessions ACCES CONTROL Networks ACLS DONITY S Identity Provider		Arista CloudVision Portal Enter the following fields to configure the app.			
L User	× ×	• • • • • • • • • • • • • • • • • • •			
∱↑ Guest CONFIGURATION	ų.	Cancel Verify Install			
🖂 Access Devices	~				
Device Administration	×				
G Certificates	×				
System	Y				
III Explore					

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

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

2.4 Configuring CVaaS Instances

To configure CVaaS instances, perform the following steps:

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

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

ONITORINO		Arista CloudVision	← Ba
Dashboard	9	Arista Cloud Vision Enter the following fields to update the selected app.	(- b)
Sessions		where	
ESS CONTROL		Arista CloudVision	
Networks		- 101	
Segments		https://www.arista.io/	
ACLS		794	
Identity Provider			
User	v	To add secondary CloudVision Servers, click here	
Guest	÷	Secondary Servers	
FIGURATION		Secondary Server	/ 8
Access Devices	~	https://www.arista.io	
Devices		second	/ 0
A Device Groups		https://www.arista.io/	
Cloud Gateways			
Device Administration			Cancel Verify Update
Certificates System	×.	Synchronization Details	
Explore		Access Device information will be synced from Arista CloudVision	
installed Apps		Last Successful Sync At	31/03/2024 08:30:0
		Last Sync At	07/01/2025 12:30:0
		Sync Status	Partial Success
		Description	Failed to sync from servers Arista CloudVision, Secondary Serve
			Sync Now
		Application Logs	ShowLogs

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

Figure 2-9: Adding Secondary Servers

	dVision Server		1222		>
Provide the f	ollowing details to add a	new CloudVision Serv	ver		
> Name					
CV-test-doc					
CV-lest-doc					
URL					
	testlab.io/				
URL	testlab.io/				
	testlab.io/				
https://www.arista-	testlab.io/				0
https://www.arista-	testlab.io/				Ø
https://www.arista-	testlab.io/			Verify	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 2-10: CVaaS Synchronization

Arista CloudVision Enter the following fields to update the selected app.	← Bad
Secondary Server https://www.arista.io	/ 0
second https://www.arista.io/	/ 0
Cancel	Verify Update
Synchronization Details	
Access Device Information will be synced from Arista CloudVision	
Last Successful Sync At	31/03/2024 08:30:00
Lost Sync At	07/01/2025 12:30:02
	Partial Success
	Sync Now
Application Logs	ShowLegs
(Income ferrative (Local *) (Serving) *) (Sminutes) *)	
	Reset Refresh

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.

Dashboard				cess Devices of Access Devices allow	wed for RadSec connection	ons as on 07/01/2025	15:39:00			+ Add	or Import D	evices
 Sessions CCESS CONTROL 											° (88
P Networks		۹	Search	s by Name, MAC Address,	IP Address or Location					Arista Swite	ch	
ACLS				NAME	MAC ADDRESS	VENDOR	LOCATION	RADSEC STATUS	UPDATE TIM	ε		
ENTITY			1	arista-710P	2c:dd:e9.ff:39:d4	Arista Switch	second/Tenant/San Jose	۰	01/11/2024	11:30:01	1	
dentity Provider			2	agni-720xp-24-1	c0:d6:82:16:3f:59	Arista Switch	second/Tenant/Bassett	0	01/11/2024	11:30:01	1	
			3	agni-720dp-24-1	28:e7:1d:ca:0e:f1	Arista Switch	second/Tenant/Bassett		01/11/2024	11:30:01	1	
	~		4	at-arista720dp	28:e7:1d:ca:0f:4b	Arista Switch	second/Tenant/AGNI_HQ		01/11/2024	11:30:01	1	
Access Devices			\$	agni-722xpm-48	ac:3d:94:c8:27.9c	Arista Switch	second/Tenant/AGNI_HQ		01/11/2024	11:30:01	1	
Devices	1		6	CV-CUE-12P-1	2c:dd:e9:fe:0f:ea	Arista Switch	second/Tenant/Undefined	•	01/11/2024	11:30:01	1	
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	
Cloud Gateways			8	Arista Switch		Arista Switch		0	29/01/2024	11:04:49	/	

Figure 2-11: View Access Devices

2.5 Adding Multiple CVaaS Instances in AGNI

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

2.6 Arista NDR Integration

You can integrate Arista NDR version 5.1.0 or later with AGNI for post-authentication profiling. To integrate Arista NDR with AGNI, perform the following steps:

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

Figure 2-12: Arista NDR Integration

MONITORING	3	Arista N	DR					← Back
Dashboard	ARRETA	Fill in the fo	llowing fields to	configure the a	рр			Dack
Sessions		me						
ACCESS CONTROL		rista NDR						
Networks	C							
l≟ Segments		This app pro	vides updates fro	m Arista NDR ab	out clients' behav	iour to AGNI.		
ACLs								
IDENTITY	Pro	file Synchroniza	tion: Disabled					
ldentity Provider	C	200-200-200 - 50		an an an an	attar interior			_
Luser	~ (Enable to fet	ch profile informa	tion for clients fr	om Arista NDR.			

- 2. Click the Install button to Install the application. The AGNI API URL is displayed.
- 3. Click the Generate Token button to generate the API.

The API URL and API Token are used in the NDR solution to integrate with AGNI.

Note: The Token is displayed only once at the install time (see image).

Figure 2-13: Arista NDR Integration API Details

E,

MONITORING	Arista NDR	
Dashboard	Fill in the following fields to update the selected app	← Bac
Sessions CCESS CONTROL Networks Segments ACLs	Arista NDR This app provides updates from Arista NDR about clients' behaviour to AGNI.	
DENTITY Clientity Provider User Client Guest	Profile Synchronization: Disabled Disabled Disabled Disabled Disabled Disabled Notification API details	
ONFIGURATION Access Devices Device Administration Certificates System		NI.
Explore	Generate Token Application Logs	Show Logs

MONITORING	Arista NDR Fill in the following fields to update the selected app
V Sessions CCCESS CONTROL VIEWorks LA Segments CCLS	Arista NDR This app provides updates from Arista NDR about clients' behaviour to AGNI.
Identity Provider User Client Guest Configuration	Profile Synchronization: Disabled Disabled Enable to fetch profile information for clients from Arista NDR. Notification API details
Certificates	 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 For security reasons, API token is shown only once. Use the following token henceforth.
Explore	API Token Application Logs Show Log

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

2.6.1 Configuring Arista NDR

To configure Arista NDR, perform the following steps:

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

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

Figure 2-15: Arista NDR Settings Page

Click on the Add Service option to add a new connected service in NDR (see image below).
 Figure 2-16: Arista NDR Configuration - Add Service

Same A					D And, query		
Connected Services					٤	0 + AN 3	anata -
V Name	7.44	Prary	es. 1	Ordentals			
2 m		80	https://ga.agnieng.net/lapl	Header			

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

Figure 2-17: Arista NDR Configuration Details

Edit Service	
Name	
agni	
URL	
https://qa.agnieng.net	/api
Header Name	
Authorization	
* Header Value	
Bearer eyJhbGciOiJFU	zI1NiIsInR5cCl6lkpXVCJ9.eyJvcmdJRCl6lkU0NWZIZWNmMi040GNhLT
* Proxy	
Discard Changes	

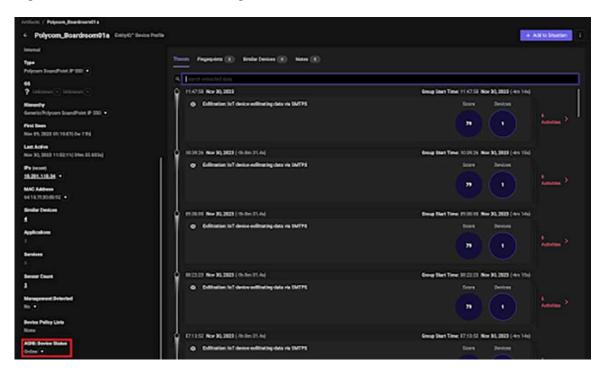
4. Click the **Save** button to add AGNI service to NDR.

Navigate to Investigations > Artifacts from the left panel.
 Figure 2-18: Arista NDR Configuration Artifacts Details

습	Home	Artifacts / Polycom_Boardroom01a	
8	Investigations	e Polycom_Boardroom01	EntityIQ [™] Device Profile
6-5	Situations	Internal	
	Artifacts	Type 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)	
\odot	Dashboards 🗸	Last Active Nov 30, 2023 11:52:11(-39m 33.833s)	
9	Manage Detections	IPs (recent) <u>10.201.110.34</u> ▼ 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 2-19: Arista NDR - AGNI Integration Status



2.6.2 Configuring Segment Policies

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

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

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

· Navigate to Sessions and select a device.

• Click the MAC address of the device.

IONITORINO	~		essions							
Dashboard		LH	st of Sessions as	on 27/06/2024 22:58:26						
/ Sessions	No	twork A	ccess Devi	ce Administration						CE
CCESS CONTROL	-									
P Networks	C	Sear	ch by Identity, MAI	Address, IP Address or Session	10 .			MAC	Authentication * Any	
± Segments									-	
ACLS	^		IDENTITY	TYPE	MAC ADDRESS	IP ADDRESS	STATUS		TIMESTAMP	
DENTITY	~		Laptops	MAC Authentication	38:ca:84:b4:d5:0b		Success	•	26/06/2024 06:37:49.810	
Identity Provider										
User	~	2	Laptops	MAC Authentication	38:ca:84:b4:d5:0b		Success	0	26/06/2024 05:37:49.540	<
Client	~	3	Laptops	MAC Authentication	38:ca:84:b4:d5:0b		Success	•	26/06/2024 04:37:49.267	<
Guest		1		MAC Authentication	38:ca:84:b4:d5:0b			-	26/06/2024 03:37:48.997	
ONFIGURATION	~	4	Laptops	MAC Authentication	38:ca.84:b4:d5:00		Success	0	26/06/2024 03:37:48.997	
Access Devices	× •	5	Laptops	MAC Authentication	38:ca:84:b4:d5:0b		Success		26/06/2024 02:37:48.725	
Device Administration	~	6	Laptops	MAC Authentication	38:ca:84:b4:d5:0b		Success		26/06/2024 01:37:48.455	
Certificates			coprope						10,00,000,000,000,000	
] System	~	7	Laptops	MAC Authentication	38:ca:84:b4:d5:0b		Success	0	26/06/2024 00:37:48.183	<
ONCOURSE	~	8	Laptops	MAC Authentication	38:ca:84:b4:d5:0b		Success		25/06/2024 23:37:47.912	
Explore										
Installed Apps	~	9	Laptops	MAC Authentication	38:ca:84:b4:d5:0b		Success		25/06/2024 22:37:47.630	•

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

Figure 2-21: Sessions Client Details

MONITORINO		Session Details - Rcptmjpdtlc4c72slam Details for Session	🔶 Back			
		Authentication Request	Success	Session Details	Close	
Networks	etworks Authentication Type		MAC Authentication	Client IP Address		
L Segments		Segment	Default	Session Start Time	26/06/2024 06:37:49.8	
ACLS		Location	Pune/ABZ	Session Stop Time	26/06/2024 06:47:36.0	
) Identity Provider	÷	L User	Client Enabled 38car84194.d5:0b WindowsLaptop Chaptops		Actions	
Client v Guest v ONFIGURATION		Not available			Allow Access	
Device Administration Certificates System System Explore		Access Device Arista Switch	Network	Enabled		
		fcbd 67.0e/8/5 PLM-Switch01-10.87.33.41 PLM-Switches	MAC-AUTH Wired MAC Authentication			
Installed Apps		Input Request Attributes	•	Output Response Attributes		

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

Figure 2-22: NDR Client Details

agni l					େ ଡ 💌
MONITORING		ient Details - WindowsLapto w client details and update the select			← Back :
CCESS CONTROL	38:ca:84:			Client Details	
Networks III Segments	Description Windows	Laptop		Device Type Machine Authenticated	Hardware Manufacturer:HP Inc.
C ACLS	Ctent Group Laptops			Added At	11/01/2024 17:54:27
(2) Identity Provider	, Status:	Enabled		Updated At	11/01/2024 17:54:27
	Client A			Client Fingerprint	×
CONFIGURATION	Arista N	DR:	×	Last Session Details	Closed
		Device Brand Device Hierarchy	Pe Add Attribute	IP Address	· · · · · · · · · · · · · · · · · · ·
Certificates		Device Type Risk Action	Cancel Update Client	Location	Pune/ABZ Default
CONCOURSE	·			Authentication Status	Success
III Explore	Netw	vork	MAC Authentication	Access Device	Arista Switch
	MAC-AUTH Wired			fc:bd:67:0e:f8:f5 PLM-Switch01-10.87:33:41	
	Sessions fo	or 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 2-23: Add Segment Details

agni I					ତ ଡ м
MONITORING		Segments Segmentation Policies			
Sessions ACCESS CONTROL P Networks		Q. Search by segment name or description	Add Segment Provide the follow	wing details to add a new segment	2 ×
±l± Segments			Name		
ACLs DENTITY Identity Provider		₩ Add Segment	 NDR Description AGNI NDR		
LUser	*	• Derault	 Status: Enable	d	Disable Monitor
* Guest			Conditions M	MATCHES ALL	
CONFIGURATION			Client: Arista	NDR:	×
Device Administration	•			Device Brand Device Hierarchy	P+ Add Condition
Certificates	×		Actions	Device Type Risk Action	
CONCOURSE					#+ Add Action
III Explore					Cancel Add Segment

2.6.3 Using Risk Action in Segment Policies

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

agni I				ତ ୬	M
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	2	×
111 Segments	1	₽+ Add Segment	Nore		
Identity Provider User Glient	× ×	✓ Default	AGNI NDR Status: Enabled	Disable Mo	nitor
R Guest	*		Conditions MATCHES ALL Client: Arista NDR: Risk Action is quarantine		×
Access Devices Device Administration	v			P+ Add Condit	sion
Certificates	* *		Actions		
Explore Installed Apps			Assign VLAN Assign VLAN through RADIUS response		×
				#, Add Acti	on
				Add Seg	ment

Figure 2-24: Add Segment Details for Risk Action

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

After a risk analysis, if the client is not *at risk*, then either the NDR admin or the AGNI admin can 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 2-25: Update Client Details for Risk

agni I					७ ७ 💿
NONTOEND		Polycom_Boardroom01a - Polycom SoundPoint IP View client details and update the selected client			(* tack
Sessions		64 16 77 10 000 BV		Client Details	
ACCESS CONTROL VIETWORKS		deseter		Device Type	Generic Polycom SoundPoint # 550
ila Segmenta		Polycom_Boardroom01a - Polycom SoundPoint IP 550		Machine Authenticated	No
@ ACLs		Sector 1			
(DENTITY		Home-I07s	*	Added At	04/07/2024 04:27:43
(1) Identity Provider		Util Tangtone		Updated At	09(07)2024-0115-16
± 0447	*	······	Cupy	Client Fingerprint	~
Client	•	Status Ender **		Concredenting	
Clents		Sana (Maria)		Last Session Details	Open
Client Groups		Client Attributes		# 409 mil	
E Guest	*	Arista NDR Device Herarchy . General	Polycom SoundPoin X		*
CONTIQUERTION		Arista NDR Device Type s Polyco	SoundPoint IP 550 X	Location	Arista Cloud Vision/Tenant/AGNUHQ
Access Devices	٠	Arista NDR Risk Action = BrQue		Segnera	NDR-Polycom
	^	Anita NUK Risk Action	All A	Authentication Status	Success
C Access Policy			Ps Add Attribute		
			(management)		
			Cancel Update Client		
CONCOLINE		9 Network	Client Certificate	Access Device	Arista Switch
III Explore					
10 Installed Apps		AT-WHED-EAP		ac3d94x8279c	
		Wred		agni-722xpm-48	
		Sessions 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

Contractor .		Contex XDH Fit is the Values of Auto to Configure the sup			* Not
12 Destinant		Ye in the following fields to configure the app			Colorado -
Sendore .					
CORD-CO-THE		form 40			
· Astanta					
the Degeneration		A11(R)			
a and a					
X Sherify Router		AP-0			
1.00	2				
C Owd	1	Alting			
and the second s	202	0.0			
Access for these	*	This approvides the ability to estimate the specularial status for sheets, provident by Series KSK.			
D Daries Adventitution			(west	(WHIN)	and a
Cardona					
D Ryman					
num n					
E Captorn					
E Installed Agen					

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

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

3.2 Medigate Integration

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

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

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

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

Figure 3-2: Installing Medigate Concourse Application

àgni I			6 0 📀
Control of the second of	Price XDI Price XDI Price XDI Price XDI Price Price	() bot	

- 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 E Dushbaard // Sessions Access controls P Nativashs III: Segments @ ACLs Destriny	Medigate Fit in the server fails to get in the server tag
X Identity Provider 1 User ~ 1 User ~ 1 User Groups . Client ~	Synchronization Details
Charts	Clerit Information Adli De Aptical from Ned gane Last Sync Ad Last Sync Ad Last Sync Ad Sync Ma Sync Ma Sync Ma Sync Ma Sync Ma Sync Ma
Contractors Contr	Application Logo (Boor Logo

Figure 3-3: Installed Medigate Concourse Application

3.3 Microsoft Intune Integration

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

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

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

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

1. Navigate to Concourse > Explore.

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

Figure 3-4: Installing Microsoft Intune Concourse Application

agni			
 Dashboard Sessions 		Microsoft Intune Enter the following fields to configure the app.	← Back
ACCESS CONTROL		, Name	
Networks		Microsoft Intune	
± ± Segments)
ACLs		Directory(tenant) ID	
IDENTITY			
😩 Identity Provider		Application(client) ID @arista.com	
🚨 User	~	Cient Secret	
🛄 Client	~		0
ff Guest	~		
CONFIGURATION		Azure Government: Disabled	
Access Devices	~		
Device Administration	~	① This app helps to provision AGNI issued EAP-TLS client certificates to managed devices through Microso	oft Intune
Certificates	~		
System	~	Cancel Verify	Install
CONCOURSE			

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

The Microsoft Intune application is displayed as an installed application on the Concourse page. Figure 3-5: Installed Microsoft Intune

MONITORING	Microsoft Intune	← Back
Dashboard	Details of the selected app	C Back
✓ Sessions		
ACCESS CONTROL	Name	Microsoft Intune
Networks	Directory(tenant) ID	b07f76f5-dca9-43d8-a2b4-b4ca914da8e1
l∸ Segments	Application(client) ID	240d3ea7-5e84-4a4a-85d1-d2db363b65c8
ACLS	Azure Government	Disabled
) Identity Provider	This app helps to provision AGNI issue Microsoft Intune	ued EAP-TLS client certificates to managed devices through
	Client Information Synchronization	
	Compliance Status Synchronization	Enabled
	Client Certificate Enrollment	Enabled
	Use the following SCEP server URL for	or creating a SCEP profile in Intune.
installed Apps	SCEP Server URL	enrollment/scep/E01907201-b42f-7

3.4 Jamf Integration

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

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

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

1. Navigate to Concourse > Explore.

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

Figure 3-6: Installing Jamf Concourse Application

agni I			6 Ø 🕒
MONITORING	Jamf Fill in the following fields to update the selected app	(+ Back	
 Networks als Segments ACLs 	Jamf O This app provides ability to provision AGNI issued EAP-TLS client certificate	s to managed devices through Jamf.	
(2) Identity Provider	Client Certificate Enrollment	Enabled	
L User ↔	Use the following SCEP challenge for creating SCEP profile in Jamf.		
CONFIGURATION Access Devices Control of the second secon	500P Datinge 729d90f8-8812-4475-85a6-dbc137e81eef Regenerate	C copy	
🖶 Certificates 🗸 🗸	Use the following SCEP server URL for creating a SCEP profile in Jamf.		
CONCOURSE III Explore IV Installed Apps	SCP Server VB, https://qa.agnieng.net/enrollment/scep/E45feecf2-88ca-413a-ac64-1cd299ff25	Re/scop-sen	
	Application Logs	ShowLogs	
		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.

3.5 ServiceNow CMDB Integration

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

This requires a configuration change in AGNI and ServiceNow CMDB.

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

1. Login to the ServiceNow CMDB portal.

2. Click the All tab and search for Application Registry Under the System OAuth option. Figure 3-7: Accessing ServiceNow Application Registry

servic	enow	II Favorites	History	Workspaces	Admin
- V	Application Re	\otimes	इ		
FAVO	ORITES				
I No R	esults				
ALL	RESULTS				
	System Applica	ations			
	Application Re	stricted Caller	<u>Acc</u>		
	System OAuth	Applicatio	on Registry		
	Application Re	g <u>istry</u>	″☆		

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

Figure 3-8: Create a new Application for AGNI

• 7	Application Registries Name -	Search			0	Actions or	selected	ows	~ Ne
l > Type	= OAuth Client .or. Type = OAuth Provider								
9	Name 🔺	Active	Туре	Client ID	Co	omments			
	Azure AD	true	OAuth Provider	Enter Client ID					
	Azure OAuth OIDC Entity	true	External OIDC Provider	<provide application="" azure="" id="" uri=""></provide>	Us	sed for Azure	to Service	now Integ	ration
	cmdb oauth provider	true	OAuth Client	90487a8324ce461090d01d6488ce1744					
	jwt_auth	true	OAuth Client	0698aa91cad242502139be8761d0f475					
	Mobile API	true	OAuth Client	ac0dd3408c1031006907010c2cc6ef6d	Us	sed by the mo	bile app to	allow acc	ess 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	Us	sed by the se	vice Webl	Kit HTML	to PDF

5. Select Create an OAuth API endpoint for external clients from the list of OAuth application types. Figure 3-9: Select OAuth API Endpoint for External Clients

servicenow	All	Favorites	History	Admin	1	OAuth application 😭	Q Search	•	Q	© 0	BN
< OAuth application										Edit Int	erceptor
What kind of OAuth	applica	ation?									
Create an OAuth API end	point for	r external clien	ts								
Create an OAuth JWT AP	I endpoi	nt for external	clients								
Connect to a third party C	Auth Pr	ovider									
Configure an OIDC provid	ler to ve	rify ID tokens.									
Connect to an OAuth Pro	vider (si	mplified)									

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

Figure 3-10: Provide CMDB OAuth details for AGNI

ervicenow All Favorites	History Workspaces Admin	Application Registries - New Record 😭	Q. Search 👻	• •	
Application Registries [View: Default*]					0 🔘 Sut
Refresh Token Lifespan Time in second Access Token Lifespan: Time in second Redirect URL: The rediect URLs author Enforce Token Restriction: Restricts ti	uth application. Leave it empty for auto-generati 5s the Refresh Token will be valid. is the Access Token will be valid. ization server redirect to. They must be absolute		across other REST APP's, Learn more.		
fore Info				-	
* Name	AGNI CMDB OAuth	Application	Global	O	
* Client ID	02dfdcefa04f4290206120bd3c179817	Accessible from	All application scopes		
Client Secret		Active			
Redirect URL		8 * Refresh Token Lifespar	8,640,000		
Logo URL		A * Refresh Token Lifespar A * Access Token Lifespar	1.800		
0.000					
Public Client		Login URL			
Comments					
Auth Scopes					⊚ -
Auth Scope					
+ Insert a new row					
Submit					

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

3.6 Splunk Integration

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

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

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

1. Navigate to Concourse > Explore .

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

Figure 3-11: Installing Splunk Concourse Application

agni I	i.		ଓ ଡ 🕒
MONITORING		Splunk Fill in the following fields to configure the app	
ACCESS CONTROL		Name Splank	
Networks			
ACLs		Splurk Hostname	
(1) Identity Provider		443	
	v v	Token	
CONFIGURATION		This app provides ability to push sessions information to Splunk	
Device Administration		Cancel Verify Install	
Certificates	÷		
CONCOURSE			
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.

3.7 Sumo Logic Integration

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

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

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

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

1. Navigate to Concourse > Explore.

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

Figure 3-12: Installing Sumo Logic Concourse Application

ngui I			¢.	0	B
MONITORING Dashboard Sessions	s u mo	Sumo Logic Fill in the following fields to configure the app			
VICCESS CONTROL		mo Lógie			
ACLs	Sur	mo Lógic UBL			
(2) Identity Provider	0) This app provides ability to push sessions information to Sumo Logic			
LUser	* L	Cancet Venify Install			
Access Devices	~				
Device Administration Certificates	• •				
System	*				
III Explore					

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

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

3.8 CrowdStrike Integration

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

For details on CrowdStrike, see the vendor documentation.

To install CrowdStrike on AGNI, perform the following steps:

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

For details, see the documentation here.

ITORING	CrowdStrike	← 84
Dashboard	Fill in the following fields to update the selected app	(B)
Sessions		
ESS CONTROL	CrowdStrike	
Networks	ATUR	
Segments	https://api.crowdstrike.com	
ACLs	API CENT D	
YTITY	4860/c67e66a40ba9d449b18aceb8ac8	
Identity Provider		
User v	AP Cleart Secret	0
Client 🗸		
Guest 🗸	This app provides updates from CrowdStrike about clients' behaviour to AGNI.	
FIGURATION		
Access Devices 🗸 🗸		
Device Administration 🗸 🗸	Event Notification	Disabled
Certificates 🗸 🗸	Enable to allow CrowdStrike to send notifications to AGNI for managed clients.	
System 🗸		
COURSE		

Figure 3-13: Installing CrowdStrike Concourse Application

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

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

Figure 3-14: Event Notification Configuration for CrowdStrike

Device Administration	~	Event Notification			Enabled	-0
Certificates	×	Use the following details in CrowdStrike to send notifications to AGNI.				
System CONCOURSE EXPlore IN Explore IN Installed Apps	v	NetReason slik. https://dev.agnieng.net/api/concourse.app.crowdstrike.notification/Eb9107b0d-c35f-42e8-ad1f-48f2c39f6686 NetReason Seoret XmRrvZ_CBxUlyqSdyL9rXC11qXXRDHF2	Copy	Regenerate		
		Application Logs			Show	Logs
				Cancel	Verify	pdate

3.9 Workspace ONE Integration

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

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

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

To install the Workspace ONE application, perform the following steps:

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

agni I				
MONITORING Dashboard Sessions ACCESS CONTROL Networks		Workspace ONE Fill in the following fields to configure the app me orkspace ONE		← Back
LIL Segments	0	This app provides the ability to provision client certificates and retrieve managed client information from Workspace ONE.	Cancel	Install
 Identity Provider User Client Guest CONFIGURATION Access Devices Device Administration Certificates System CONCOURSE 	* * *			
Explore III Explore IV Installed Apps				

Figure 3-15: 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>.

agni I O Workspace ONE + Back 1 Dashboard ~ Sessions Networks III Segments () This app provides the ability to provision client certificates and retrieve managed client info on from Workspace ONE ACLs mation Synchronizat Client Info (a) Identity Prov Client Information Synchronization: Enabled 1 User Client API URI * Guest Access Devices Client ID C Device Adminis 🖯 Certificates System Verity Explore Event Notification: Disabled IV Installed Apps Enable to allow Workspace ONE to send notifications to AGNI for managed **Client Certificate Enrollment** Disabled Application Logs Show Logs Cancel Update

Figure 3-16: Configuring Workspace ONE Parameters

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

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



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

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

Figure 3-17: Configuring Workspace ONE Parameters

agni I			¢	٥	۲
S Dashboard	Workspace ONE Fill in the following fields to update the selected app	4 Back			
A Sessions	Clerit D				
ACCESS CONTROL	Clerificati				
Y Networks					
ats Segments		Souty			
O ACLS		ready			
(A) Identity Provider	Event Notification Evalues =				
1 User ~	Use the following details in Workspace ONE to send notifications to AGNI.				
Client v	Nork-our UK				
🛒 Guest 🗸 🗸	https://qa.aprieng.net/api/concourse.app.workspaceone.notfication/Ex6131909-2x76-4453-ba16-2x274944e045	() cwy			
CONFIDURATION	Institution Linemand weds/2056-8afe-6430-acce7-8ares0fedc(79c	10 Copy			
Access Devices	46342339 5844 4430 4241 58480 890 LVK	() cas			
Device Administration · Gentificates ·	funds at the Factoread 729cG/bc-7c79-4801-8799-9e15c8303a14	D Copy Represente			
O System	778/050-7279-4601-6799-9411(3303314	C Copy Represente			
concounte	Note : Changes will be saved once you click on update.				
Explore	Client Certificate Enrollment	(nations) and			
IF Installed Apps					
	Use the following SCEP challenge for creating SCEP profile in Workspace ONE.				
	1027 Owenge 95004886-6051-4962-83ce +7877640c364	(D Copy) (Begenerate			
	O Use the following SCEP server URL for creating a SCEP profile in Workspace ONE.				
	100° (non-10) Miljis J./ga.agnieng.net/innet/nonp/f.ad1376rb-2a7N-44d3-ba16-2e27n644e045/scop-tenver/748/tasth-5e02-55e3	() copy			
	Note : Changes will be saved once you click on update.				
	Application Logs	(StonLogs)			
		Cancel Update			

Configuring Identity Providers

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

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

AGNI integration with IDPs requires:

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

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

4.1 Microsoft Entra ID 365 (Azure)

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

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

If you provide user authorization, perform the following steps:

- 1. Navigate to Identity > Identity Provider.
- 2. Click the Edit or Add button to edit an existing IDP or to add a new IDP.
- 3. Enter a Name and Domain Name in the respective fields.
- 4. Enable Identity information Synchronization.

5. Provide the identity provider details.

(Refer to Appendix section on how to configure the details in Microsoft Azure AD):

- a. Directory (tenant) ID
- b. Application (client) ID
- c. Client Secret
- d. Sync Interval (hours)
- 6. Click the **Verify** button. Once the operation is successful, the system fetches the list of groups from the IDP, which can be used in the policy creation.

Figure 4-1: Adding Identity Provider

Dashboard		Add Identity Provider Provide the following details to add a new Identity Provider	← Ba
Sessions CCESS CONTROL Networks		Azure-test	
Segments ACLs ENTITY		antaraaleng.onmicrosoft.com	
Identity Provider User	~	Microsoft Entra ID	
Client Guest	* *	Identity Information Synchronization Directory(tenant) ID b07(76f5-dca9-43d8-a2b4-b4ca914da8e1	Enabled
Access Devices Device Administration	* *	Application(clent) ID	
Certificates System NCOURSE	~	Client Secret	0
Explore Installed Apps		24	
« Collapse Sidebar			Cancel Verify Ad

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 Management			
Sessions CCESS CONTROL	azure eng	Sync Enabled	agni365.net	Sync Enabled
P 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
ldentity Provider	Last Sync Scheduled At	08/01/2025 09:30:00	Last Sync Scheduled At	07/01/2025 21:30:00
Client V	Sync Status	Success	Sync Status	Success
Guest ~		/ 8		/ 0
Access Devices 🗸 🗸	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
INCOURSE	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 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 Administrat 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 G Finance Installed Apps - Remove TK-Devices TK-Devices - Renove 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

(2) Identity Provider			
💄 User	~		
Client	~		
f Guest CONFIGURATION	~	User Attributes	
Access Devices	~		
Device Administration	~	Synchronized Attributes Preview	
Gertificates	~	User Attributes Organization 8 Select User Attributes	Add
System	~		
CONCOURSE		Synchronized User Attributes	
Explore		Department 🔇 CostCenter 🔇	
Installed Apps			
≪ Collapse Sidebar			Cancel Verify Update

• **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 Fill in the fields below to update the selected Identity Provider	
Dashboard	Fill in the fields below to update the selected Identity Provider	€ 83
✓ Sessions		
CCESS CONTROL	Engineering	- Remove
Networks	Platform Engineering	- Remove
Li= Segments	Plation Engineering	
ACLs	5 Site Reliability Engineering (SRE)	- Remove
DENTITY		
Identity Provider		
 Identity Provider User 	User Attributes	
L User	_	
User A	Synchronized Attributes Preview	
L User	Synchronized Attributes Preview	Get
User A	Synchronized Attributes Preview	Get
User ^	Synchronized Attributes Preview	Cet
User ^ Users Users User Groups Client ^	Synchronized Attributes Preview User login name shane@systestpoc.onmicrosoft.com User Attributes	
User ^ Users 22: User Groups Client ^ Clients	Synchronized Attributes User login name shane@systestpoc.onmicrosoft.com User Attributes Email	shane@systestpoc.onmicrosoft.com
User ^ Users LUser Groups Client ^ Clients Client Groups	Synchronized Attributes Preview User login name shane@systestpoc.onmicrosoft.com User Attributes	
User ^ Users User Groups Client ^ Clients Client Groups ONFIGURATION	Synchronized Attributes User login name shane@systestpoc.onmicrosoft.com User Attributes Email	shane@systestpoc.onmicrosoft.com

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

ONITORING		Add Identity Provider Provide the following details to add a new Identity Provider	← Bi
Dashboard	1	Provide the following details to add a new Identity Provider	C Bi
Sessions			
CESS CONTROL		Name -	
Networks		OneLogin	
Segments		, Domain Nome	
ACLs		test.org	
ENTITY		Adentity Provider	
Identity Provider		O OneLogin	
User			
Client		Identity Information	
		_ OIDC Instant URL	
Guest	~	https://antara.onelogin.com/oldc/2	
Access Devices	~	_ DEC Client D	
		0oa4ltci6gV0fkQ8q5d0oa4ltci6gV0fkQ8q5d0oa4ltci6gV0fkQ8q5d	
Device Administration	~		
Certificates	~	Add the following URL in the redirect URI's for OIDC application.	
System	~		
NCOURSE		https://dev.agnieng.net/sso/login/callback	Copy
Explore			
Installed Apps			(2000)-
		Identity Information Synchronization	Enabled
		API Clent ID	
		API Client Secret	-
			©
		, Sync Interval Incurs)	

- 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).

gni		
Dashboard	Add Identity Provider Fill in the fields below to add a new Identity Provider	(← Back)
V Sessions CESS CONTROL Vetworks	24	
ACLs	User Groups	
ENTITY	Available Groups Synchronized Groups	
L User V	Q Search by proop name.	
Client V		(Selected: 3)
Access Devices V	CN=Executive,OU=Groups,OU=Employees,DC=myorg1,DC=com	- Renau
Certificates v	CN=IT,OU=Groups,OU=Employees,DC=myorg1,DC=com	- Reten
ONCOURSE	CN++R,OU=Groups,OU=Employees,DC+myorg1,DC+com	··· Server
Explore Installed Apps		
	User Attributes	
	Synchronized Altributes Proview	
	User Atributes	* Add
		Cancel Verify 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

agni I	
MONITORING	Update Identity Provider Exact Provide the following details to update the selected Identity Provider Exact
✓ Sessions	
ACCESS CONTROL	Name Okta-testorg1
≟l≞ Segments	Domain Name
ACLs	/ Identity Provider
Identity Provider	O Okta
💄 User 🗸 🗸	Identity Information
Client V	
Guest ~	dev-01259439.okta.com
Access Devices V	Application(client) ID 0oa4ltoi6gV0fkQ8q5d7
 Device Administration Certificates 	
System 🗸	Add the following URL in the sign-in redirect URI's for OIDC application.
CONCOURSE Explore	https://dev.agnieng.net/sso/login/callback
Installed Apps	

- 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).

MONITORINO Dashboard	Update Identity Provider Provide the following details to update the selected Identity Provider	← Back
Sessions		
ACCESS CONTROL	Identity Information Synchronization	Enabled
ACLS		
A Identity Provider	24	
L User	Synchronization Details	
Guest	, Last Sync Scheduled At	07/01/2025 21:30:00
Access Devices	Sync Status	Success
Device Administration		Syne Now
Certificates	User Groups	
CONCOURSE	Available Groups Synchronized Groups	
installed Apps	Q. Search by group name	
		Selected: 40
	largegrouptest.1	Remove
	targegrouptest_1000	Remove
	G largegrouptest,301	- Remove
	largegrouptest_302	- 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

Dashboard	Update Identity Provider Provide the following details to update the selected Identity Provider	← Bac
Sessions CCESS CONTROL Networks Segments ACLs	Antara Al Net Option Prane AntaraaLinet	
Jentity Jdentity Provider	G Google Workspace	*
User Client Guest	V V Identity Information Synchronization V Cogetime to Cogetime t	Enabled
Access Devices Device Administration Certificates	Account these alan@antaraai.net Update Service Account	
System DerCOURSE Explore Installed Apps	Upload the file in JSON format. Updating this will even write existing Service Account. Sectimenal Invite 24	

4.5 Local

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

Figure 4-11: Local IDP Configurations

CloudVision COONi			
MONITORING	8	Identity Provider Identity Access Management)
ACCESS CONTROL	Loca	al Users	
Networks	Ide	entity Provider	local
± ≛ Segments	Do	main	local
ACLS			
(1) Identity Provider			
Liser	×		
CONFIGURATION			/ 1
Access Devices	×		
Certificates	× .		
System	~		
CONCOURSE			
Explore			
Collapse Sideba			

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
Dashboard	Provide the following details to add a new Network
✓ Sessions	(Name -
ACCESS CONTROL	Arista-corp
♥ Networks ↓↓ Segments	Connection Type: Wireless Wired
	SSID
DENTITY	Arista-corp
ldentity Provider	Status: Enabled
💄 User	 Image: A start of the start of
Client	~ Authentication
📅 Guest	Authentication Type
CONFIGURATION	Client Certificate (EAP-TLS)
Access Devices	Domain Machine Authentication: Enabled
Device Administration	Allowed Machine Domains
Certificates	V domain.xyz & pepsico.com &
System	Optional, Press ENTER after each domain.
CONCOURSE	

- 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	
SSID NSE-CORP	
Status: Enabled	
Authentication	
Authentication Type Client Certificate (EAP-TLS)	•
Domain Machine Authentication: Enabled	
Allowed Machine Domains 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

- 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.

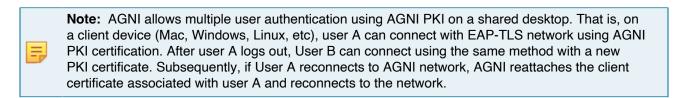
This process creates the network. It also creates an **Onboarding URL**, which should be set as a captive portal URL in the Wi-Fi configuration of your AP. Clients are redirected to this URL during the onboarding process.

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 client	ts.
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

low Local User Self Registration: Enabled		
 Users can onboard their clients using the below URL. 		
Casi a cari o nocara unan cinenta dang una beron onte:		
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 Provide the following details to update the selected Network	÷	Back
Dashboard				
' Sessions		Test-docs		
Networks				
Segments		Connection Type: Wireless Wireless		
		sso Test-docs		
ACLS		151-00-3		
Identity Provider		Status: Enabled		
User	~			
Client	~	Authentication		
Guest	~	, Authenticetion Type		
NFIGURATION		Client Certificate (EAP-TLS)		
Access Devices	~			
Device Administration	^	Domain Machine Authentication: Enabled		
C Access Policy		Enable to allow machine authentication with domain machine certificates.		
TACACS+ Profiles				
(Here I Mer J. M.				
Certificates	*	Trust External Certificates	Disab	oled O
System	*			
Explore		Enable this setting to accept client certificates issued by external CAs.		
Installed Apps				
Installed Apps		Onboarding	Enab	oled a
		Allow Email Code Login for IDP User: Enabled		
		Belect Authorized User Groups		
		Provense and a second s		
		Users can onboard their clients using the following URL.		
		https://dev.agnieng.net/onboard/Eb9107b0d-c35f-42e8-ad1f-48f2c39f66886/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

Sign In		
UserID or Email		
alan-test-docs(@arista.com	
1	Proceed	

Click the Proceed button and click the Use one-time password option.
 Figure 5-7: Use One-Time Password Option

Sign l	n	
UserID or Em		
alan-test-	docs@arista.com	
	Use one-time password	
6		

6. Check your registered email for OTP details:

Figure 5-8: AGNI Login

7.

Arista Guardian for Network Identity (AGNI)				
Hello	@arista.com			
You have requested for one-time passsord (OTP) to log in to AGNI Self-Service Portal.				
Login using the following details:				
Email:	@arista.com			
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: Verify OTP				

Verif	y one-time password	
	eck your email for one-time password.	
One-time pr	assword	
	Submit	

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 (Is Mac OS X	
	Registe

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

090i My Self Service Portal	
	Register Client
	Vour 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.

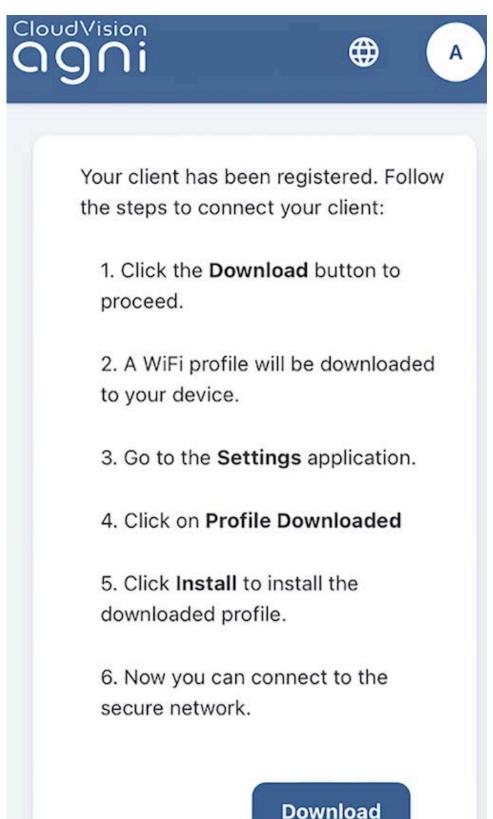
The profile installation process varies based on the client device operating system. AGNI supports the following devices and the instructions are provided:

- 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

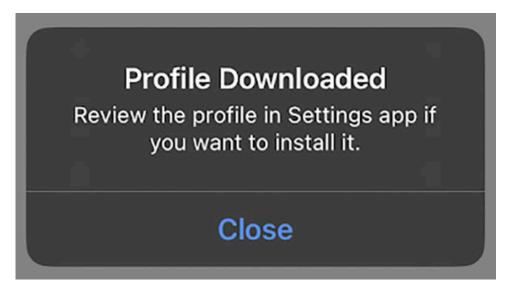


Figure 5-14: Profile Downloaded

Profi	le Downloaded	×
>	Airplane Mode	
?	Wi-Fi	TLS-TEST >
*	Bluetooth	On >
((†))	Mobile Data	>
ଡ	Personal Hotspot	>
VPN	VPN	
	Notifications	>

Figure 5-15: Profile Installed

Cancel	Install Profile	Install
	AGNI-Wifi Config	
Signed by	ANGI, Issuer CA Not Verified	
Description	Configure Wifi and SCEP	
Contains	Wi-Fi Network Device Identity Certificate Certificate	
More De	etails	>
Re	emove Downloaded Profile	

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**

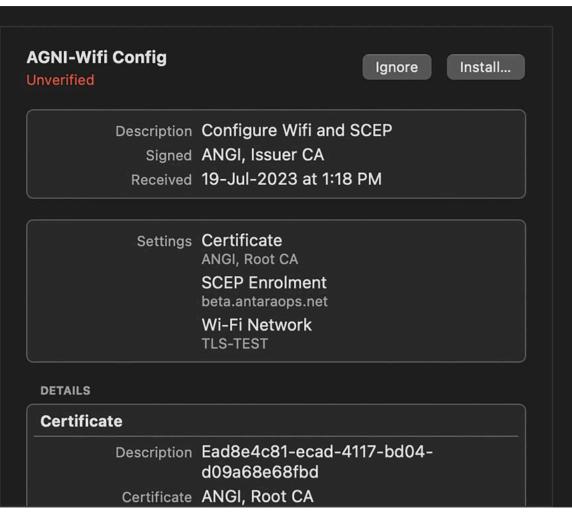


Figure 5-17: Unverified Profile

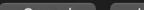
Profile "AGNI-Wifi Config"

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
--	--------	-------	----------	--------------

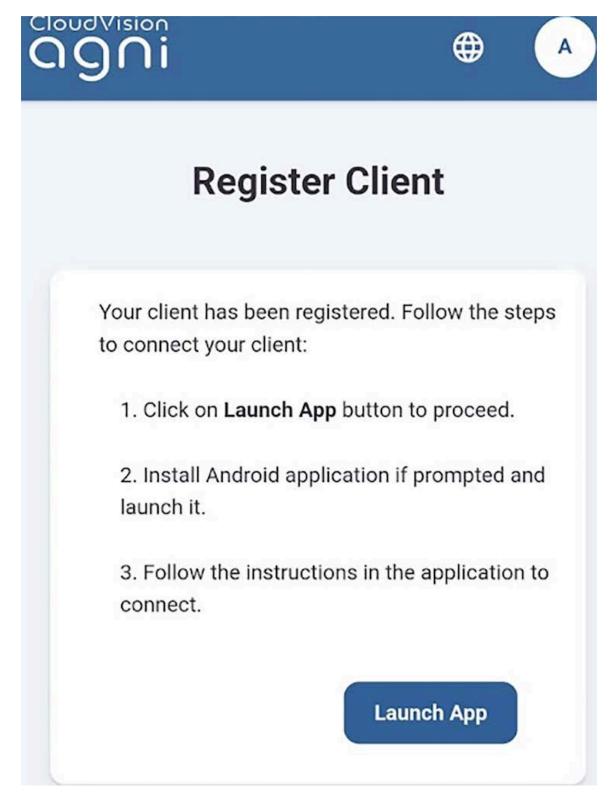
Keychain Access	[① ① ANGI		0
All Items Passwords Secure Notes My Certificates	Keys Certificates		
ANGI, Root CA Root certificate authority Expires: Sunday, 27 March 2033 at 10:17:39 This certificate is marked as trusted for t		Expires	Keychain
📑 ANGI, Root CA	certificate	27-Mar-2033 at 10:17:39	login

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

· · · · · · · · · · · · · · · · · · ·
nud

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

Start

Figure 5-26: Security Warning

Security Warning



You are about to install a certificate from a certification authority (CA) claiming to represent:

AGNI, Root CA

Windows cannot validate that the certificate is actually from "AGNI, Root CA". You should confirm its origin by contacting "AGNI, Root CA". The following number will assist you in this process:

Thumbprint (sha1): 672E7033 F800F345 91A25760 31730E05 899D07C0

Warning:

If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

Vec	No
ics	140

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.
- 2. Open the AGNI onboarding URL in the browser. You are redirected to the Self-Service Portal.

Figure 5-28: Register Client

	3
Register Client	
Provide the following details to register your client device. Description Shallendra'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

	\$
Register Client	
Your client is registered. To connect your client. I. Install CleardVision AOM on your Chromebook. After app is installated, Go to the bottom right, select the time. Select Settings ● I. In the "Appes" section, Select Manage your apps > CloudVision AONI. Lunder Opening Supported Links, Select Open in CloudVision AONI. C. Click Launch App button to proceed. Lunch 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

Settings	Q. Search settings	
Phone Hub, Quick Share		
Accounts 4 accounts	← cop CloudVision AGNI	Uninstall
Device	Pin to shelf	
Keyboard, touchpad, print	Allow notifications	
Wallpaper and style Dark theme, screen saver	Permissions	
Privacy and security	Cocation Denied	
	Manage permissions	
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	
	O Open in Chrome browser	
 About ChromeOS Updates, help, developer options 	App details	
	Andmini ann installed from Goonle Play Store 12	

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

Your client is registered. To connect your client	
3. Install GloudVision 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 AGNL	
5. Click Launch App Isation to proceed.	3

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

Figure 5-32: Onboarded Client

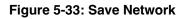


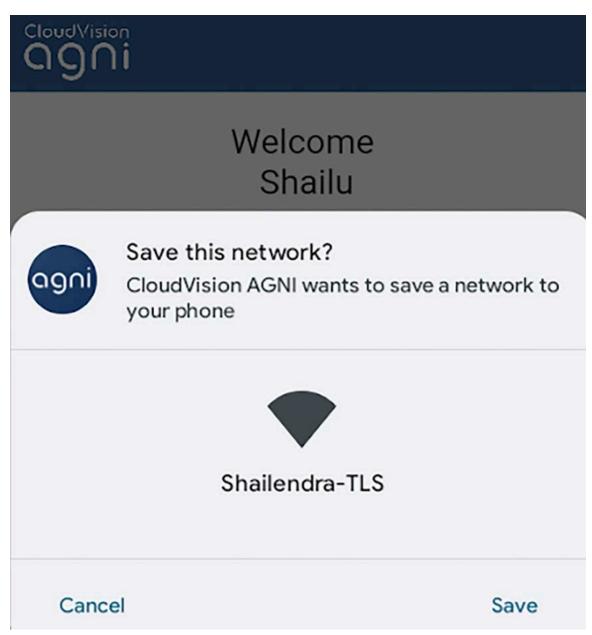
Welcome Shailu

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

Start

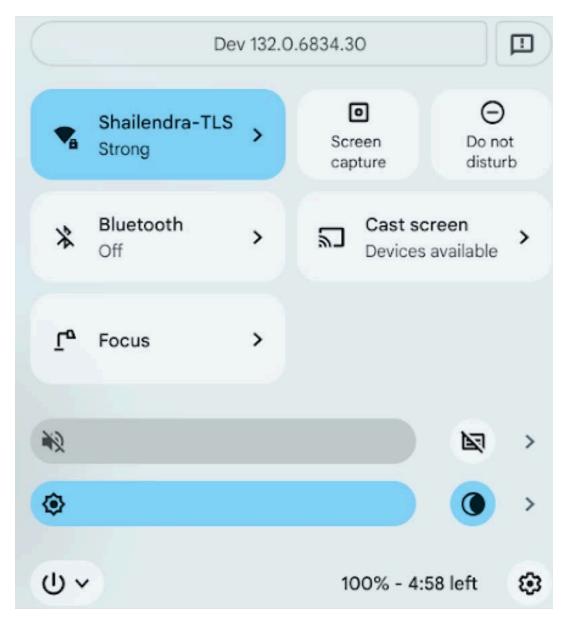
Allow the application to configure the wireless profile and install certificates.





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 ESS CONTROL	Session Details - Rct9d3a2g12 Details for Session	2qs72vtq5lg	6		🗧 🗧 Back
Networks Segments	Authentication Request		Success	Session Details	Closed
ACLS	Authentication Type		Client Certificate (EAP-TLS)	Client IP Address	192.168.1.9
NTITY Identity Provider	Segment		Default	Session Start Time	06/12/2024 15:57:52.192
User ~	Location			Session Stop Time	06/12/2024 15:13:26.090
Client v	1 User	Enabled	Client	Enabled	Actions
Access Devices ~ Device Administration ~	Shailu Shailendra		10:a0:54:b3:03:d1 Shailendra's Chrome OS		Allow Access PAN Firewall: Push User Information Target = PANFW 24316
Certificates v System v	Access Device	Arista Wifi	- Network	Enabled	
Explore Installed Apps	e4:d1:24:10:2a.8f Shailendra:2a:8f		Shailendra-TLS Shailendra-TLS Client Certificate (EAP-TLS)		

5.2 Configuring Unique PSK (UPSK) Network

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

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

Prerequisites :

- Wireless SSID should be configured on the APs to perform UPSK authentication.
- · Onboarding roles should be configured on the APs.
- Onboarding PSK passphrase should be configured on the SSID.
- Walled garden domain names are configured to allow access to the required domains (more details under the Show Domains section in Step 7c below).

5.2.1 Configuring the UPSK Settings

To configure the UPSK settings, perform the following steps:

1. Navigate to Access Control > Networks.

2. Click on the Add Networks button.

Figure 5-36: Configuring Wireless UPSK Network

IONITORING	ACME-BYOD	← Back
Dashboard	Fill in the fields below to update the selected Network	← Back
✓ Sessions	Charm -)
CESS CONTROL	ACME-BYOD	
P Networks	Connection Type: Wireless Wireless	
* Segments	, 590	
ACLS	ACME-Byod	
DENTITY		
Identity Provider	Status: Enabled	
L User		
Client ~	Authentication	
INFIGURATION	Authentication Type	
Access Devices 🗸 🗸	Unique PSK (UPSK)	*
Certificates ~		
System ~	User Private Networks	Enabled -
DNCOURSE		
Explore	Shared Clients: enabled	
P Installed Apps		
	Available Clients Shared Clients	
	Q. Search by mac address or description	
		(Shared 1)
	O0:23:68:0b:fc:1c Alaris Infusion Pumo Module (8300 FtCO2 Module)	+ Add
	Construction of the second second second second	
	Oa:65:bc:92:81:dd Maquet Ventilator (Servo)	+ Add
	00:23:68:31:d7:22 Alaris Influsion Pump Module (8110 Syringe Module)	+ Add
	00:17:23:21:c3:9a Alaris Infusion Pump Module (8110 Suringe Medule)	+ Add
<< Collapse Sidebar	Alaris Infusion Pump Module (8110 Syringe Module)	1. Same

- 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.
- Authentication The type of authentication should be set to Unique PSK (UPSK). This enables the system to honor UPSK authentication requests.
- 7. User Private Networks:
 - **a.** Enable this setting when interacting with Arista APs. This setting sends Arista VSAs for UPSK transactions.
 - **b.** Shared Clients (Optional). Enable the setting and choose the list of clients this connection can share from the configuration. This is specific to Arista APs.
- 8. Onboarding Enables the end user to self-register the devices.
 - a. Initial Passphrase for Onboarding Specify the initial passphrase that should be used by the clients to connect to the UPSK network. This passphrase should match with the one configured on the SSID of your APs.
 - **b.** Initial Role for Onboarding Specify the initial role to be associated with when the clients connect to the UPSK network. This role should be configured in the APs.
 - **c.** Show Domains Shows the list of walled garden domain names that need to be allow-listed in your network infrastructure (wired or wireless) to allow the onboarding process. Without this, the user authentication may be blocked by the network infrastructure.

- d. Allow Email Code Login for IDP User: Click the toggle button to enable email code login.
- e. Allow Local User Self Registration:
 - 1. **Disabled** Disallows local users to self-register into the system as part of the user onboarding process.
 - 2. Authorized User Group This setting is optional. Choose the names of the User Groups, if you want to allow onboarding to be permitted for the users belonging to these groups. When this setting is not provided the system honors onboarding requests from all the users of the organization.
 - 3. Enabled Users can self-register into the system as part of the user onboarding process.

Figure 5-37: Wireless UPSK Network User Onboarding

Initial Passphrase for Onboarding	
changeme123	
Initial Role for Orbioarding	
onboarding-psk	Show Domai
Ow Local User Self Registration: Enabled	
https://qa.antaraops.net/onboard/Ee8eb46d1-d266-460d-9b41-a904b655234b/network/4	Сору
Jsers can scan a WiFi QR code to connect to this SSID for onboarding.	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 Available Networks					+ Add Network	🌣 Set	tting
CCESS CONTROL		All N	tworks Wireless	Wired					E	3
Networks	- [Q	Search by Name or SSID					Authenticatio	on Type —	
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	Ō
 Identity Provider User 	•	2	AT-WIRED-MBA	Wired	MAC Authentication		Enabled	15/11/2023 04:46:37	1	đ
Client	•	3	agni-arista-Us	Wireless	Client Certificate	agni-arista-tis	Enabled	21/10/2023 00:38:14	1	0
ONFIGURATION	~	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	0
🖵 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	Ō
Installed Apps		9	AT-ARUBA-PSK	Wireless	MAC Authentication	AT-ARUBA-PSK	Enabled	19/07/2023 01:47:00	1	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				
Q	Search by Name	UPSK Settings		Authentication	n Type —	-
1	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
2	AT-WIRED-MB	Expires Periodically	Enabled	15/11/2023 04:46:37	1	Ô
ka:	agni-arista-tis	Personal Passphrase Validity Period (Days)	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	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
	AT-ARUBA-PSK	Wireless MAC Authentication AT-ARUBA-PSK	Enabled	19/07/2023 01:47:00		1

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 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* 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.

DNITORING	ACME-Guest	
Dashboard	Fill in the fields below to update the selected Network	← Back
Sessions	Y Norm	
CESS CONTROL	ACME-Guest	
P Networks	Connection Type: Wireless Wireless	
4 Segments	100	
ACLS	ACME-Guest	
ENTITY		
Identity Provider	Status: Enabled	
L User v		
Client V	Authentication	
INFIGURATION	Authentication Type	
Access Devices 🗸	Captive Portal	
Certificates ~	User Type: Organizational user O Guest user	
System V	User type: Organizational user Organizational user	
E Explore	Captive Portal	
installed Apps		
/ installed Apps	Initial Rule for Portal Automotication agni-guest	Show Domains
	มปัณ-ปัจตอง	snow Domains
	Authorized User Groups	
	Re-Authenticate Registered Clients	
	Periodic	*
	Re-Authentication Period (days)	

Figure 5-41: Wireless Captive Portal Network Page One

Figure 5-42: Wireless Captive Portal Network Page Two

ACME-Guest Fill in the fields below to update the selected Network ACME-Guest	- Back
Authentication	
Automatication Type Captive Portal	•
User Type: Organizational user Organizational user	
Default Portal ASU-GUEST-2023-01-31_12-01-17	
	Fill in the fields below to update the selected Network ACME-Guest Status: Enabled Authentication Authentication User Type: Organizational user Overfault Default Portal

- **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

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

5.4 Configuring Wireless MAC Authentication Network

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

Prerequisites

Wireless SSID should be configured on the AP to perform MAC Bypass Authentication.

Roles/VLANs used in the segmentation policies should be configured on the AP.

5.4.1 Configuration Steps

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

- 1. Navigate to Access Control > Networks and select the Add Networks button.
- 2. Enter the Network Name and choose Connection Type as Wireless.
- 3. Enter the SSID name. Ensure the name matches the SSID configured in the wireless APs
- 4. Set the Status value:
 - a. Enabled Enables this network to honor incoming requests.
 - b. Disabled Disables this network.
- 5. Authentication Type Authentication type should be set to MAC Authentication. This enables the system to honor MAC-based authentication requests.
- 6. MAC Authentication Settings:
 - Allow All Clients Allows MAC authentication to succeed for all the clients irrespective of registration status.
 - Add New Clients to Group Specify the client group to persist the newly authenticated MAC addresses.
 - **b.** Allow Registered Clients Only Allows MAC authentication to succeed for the clients that are registered in AGNI.

- **Disallow user-associated clients** When this option is enabled, the MAC authentication for the previously onboarded clients is rejected.
- c. Allow Authorized OUIs Only Allows MAC authentication to succeed for the listed OUIs only.
 - 1. Allow New Clients to Group Specify the client group to persist the newly authenticated MAC addresses.
 - 2. Allow Registered Clients and Authorized OUIs This option behaves similarly to Allow Registered Clients Only and Authorized OUIs Only combined.

Figure 5-44: Wireless MAC Authentication Network

)∩i		
Dashboard	ACME-MACAUTH Fill in the fields below to update the selected Network	- Back
Sessions SS CONTROL	ACME-MACAUTH	
Networks Segments	Connection Type: Wireless Wired	
ACLS	990 ACME-MacAuth	
Identity Provider	Status: Enobled	
Client	Authentication	
Access Devices ~	Advectation Type MAC Authentication	
System ~	MAC Authentication Settings	
Explore	MAG Authenticulari Type	
Installed Apps	Allow Registered Clients and Authorized OUIs Disallow user associated clients: Enabled The Disallow user associated clients on this network.	
	Authorized QUIs	Add
	OUI is a hex string of 6 characters el: 00052A, 00052D Selected Authorized OUIs	
	00052A 🛞 00052B 🔕	
	Add New Clienth To Droup	
	IOT-Segment	* 🕀

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	- 🕀
Select an Access Device Group to make this Network only applicable to a subset of Access Devices. Multiple Networks of Group. Status: Enabled	and a set resonance in a set of the filled of the filled of the
Authentication	
Authentication Authentication Type	
	•
	•

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 Ob
1	

- **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 Certific		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	v

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

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



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

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

Figure 6-7: Allow Authorized OUIs Only

MAC Address Authentication Settings	
Allow Authorized OUIs Only	
Authorized OUIs	Add
OUI is a hex string of 6 characters ex: 00052A, 00052D	
Selected Authorized OUIs	
00052A 🙁 00052B 🙁	

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

Figure 6-8: Onboarding

Dnboarding	Enabled
Allow Local User Self Registration: Disabled	
, Authorized User Groups	
Test 🔕 Select 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).

CONTORNO	Add Network Provide the following details to add a new Network	€ Bec
Sessions	Barlet an Access Davids Group is make this Nativon only applicable to a subset of Access Davides Multiple Networks can't be intend to the same Access Davids Group.	No. 1997
ESS CONTROL		
P Networks	Status Exceed •	
a Segments	Authentication	
acls		
DENTITY	Client Certificate ([AP-7]_5]	
L Identity Provider		
L User	Domain Machine Authentication: Enubled	
1 Users		
ALL User Groups	Enable to allow machine authentication with domain machine certificates.	
Client v		
OHFIDLIBATION	Trust External Certificates	Disatriest Q1
Access Devices v	0	
Gertificates	 Enable this setting to accept client certificates issued by external CAs. 	
System v		
ONCOURSE	Fallback To MAC Authentication	Enabled and
Explore	a list further stor for	
P Installed Apps	Allow Registered Clients Only	*
	Displow user associated clients Environ	
	Enable to disallow user associated clients on this network.	
	Onboarding	Disatived O

Figure 6-9: Sample Wired 802.1X configuration

6.2 Configuring Wired MAC Authentication Network

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

Prerequisites

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

6.2.1 Configuration Steps

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

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

- 5. MAC Authentication Settings Lists the available authentication settings, you can choose the one applicable to the network.
 - **a.** Allow All Clients When set, the MAC authentication admits all the clients that are attempting the wired authentication. Choose a client group to add the authenticated MAC addresses. This help to build an inventory of the client devices.

Figure 6-10: Add Network

C Authentication Settings	
VAC Authentication Type	
Allow All Clients	Ť
Add New Clients To Group	- ()

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

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

AC Authentication Type	
llow Registered Clients Only	
Disallow user associated clients: Enabled	
sallow user associated clients:	

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

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

Figure 6-12: Add Network (Authorized OUIs)

MAC Address Authentication Settings	
Allow Authorized OUIs Only	
Authorized OUIs	Add
OUI is a hex string of 6 characters ex: 00052A, 00052D	
elected Authorized OUIs	
elected Authorized OUIs 00052A 8 00052D 8	

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

ONITORING Dashboard Sessions	Update Network - Corporate MAC ByPass Authentication Wired Fill In the fields below to update the selected Network
CCESS CONTROL Networks La Segments	Corporate MAC ByPass Authentication Wired Connection Type: O Wireless O Wired
identity Provider	Access Device Groups are configured
Access Devices ~ Certificates ~ Administration ~	Authentication Authentication Type MAC Address Authentication
II Explore Installed Apps	MAC Address Authentication Settings MAC Address Authentication Settings Allow Registered Clients Only

Figure 6-13: MAC ByPass Authentication Configuration

6.3 Configuring Wired Captive Portal Network

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

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

Prerequisites

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

6.3.1 Configuration Steps

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

- 1. Navigate to Access Control > Networks. Click on the Add Networks button.
- 2. Enter the Network Name and choose Connection Type as Wired.
- 3. Authentication Choose the Authentication Type as Captive Portal.
- 4. Captive Portal:
 - a. Initial ACL for Portal Authentication Specify the initial ACL for Captive Portal authentication.

Note: This ACL should be configured on the switch and the user is forced to redirect to the captive portal by ACL applied on the switch port.

Figure 6-14: Figure: Captive Portal

aptive Portal	
Initial ACL For Portal Authentication	Show Domains
Re-Authenticate Clients	
Always	*
O Configure the following URL as captive portal in the initial role, to allow users sign in.	
https://qa.agnieng.net/guestPortal/Eba61d189-e361-4837-a116-182575420cfb/network/136	ру

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

https://qa.antaraops.net/captivePo	ortal/Ec36fd356-3041-4fc1-98be-a83382522273/network/6	Copy	
			~

6.4 Configuring Guest Portal Network

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

6.4.1 Configuring AGNI

Perform the following steps to configure AGNI.

- 1. Log in to AGNI and navigate to Identity > Guest > Portals.
 - Figure 6-17: Guest Portal



2. Click the Add Guest Portal button.

Figure 6-18: Add Guest Portal

agni AzureSys	stest-Q/			ଜ ଡ	•
	*	Portal Settings Self-service and Guest portal settings	Client Management Portal	+ Add Guest I	Portal
Access Devices	× .				
Device Administration	×	Q Search by Name			
Certificates	*				
System Audit Viewer Culture	^	ARISTA			
Portal Settings	1	000			
C RadSec Settings					
Support Logs		Default /			
E System Events					

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

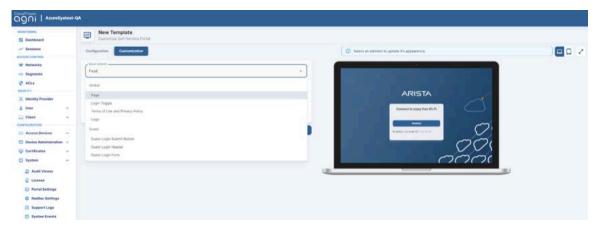
Figure 6-19: Configure Portal

Cilent	v	New Template Customize Self-Service Portal		G () (+ 114
Access Devices Device Administration	*	Configuration Customization	O . Select an element to update it's appearance.	
Certificates	~	AGNI Portal		
 System Audit Viewer License Portal Settings RadSec Settings Support Logs System Events 	×	Default Default Split Screen Cancel Add Guest Portal	Connect to enjoy free Wi-Fi Connect to enjoy free Wi-Fi Connect to enjoy free Wi-Fi Connect to enjoy free Wi-Fi	0
DINCOURSE				

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

- b. Login Toggle
- c. Terms of Use and Privacy Policy
- d. Logo
- e. Guest Login Submit Button

Figure 6-20: Customize Portal



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

Figure 6-21: Added Guest Portal

Dashboard	Portal Settings Self-service and Guest portal settings	Client Management Portal + Add Guest Portal
CCERS CONTROL	Q. Search by Name	
Networks Segments ACLs		
A Identity Provider		20
Access Devices		
Device Administration 👻		
Certificates 🗸 🗸		
System o		

- 7. Navigate to Access Control > Network.
- 8. Add a new network with following settings:
 - a. Network Name
 - b. Connection Type Wired
 - c. Access Device Group Switch Group
 - d. Authentication
 - 1. Authentication Type Captive Portal
 - 2. Captive portal type Internal for AGNI Hosted Captive Portal.
 - e. Captive Portal
 - 1. Initial ACL ACL Name
 - 2. Authorized user group if applicable

3. Re-Authentication Clients - per requirement

Figure 6-22: Network Settings

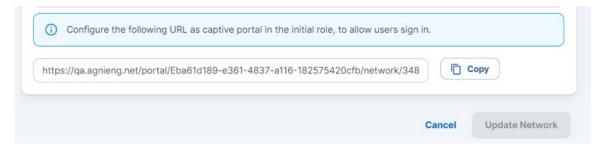
ACME-wired-guest Provide the following details to update the selected	ł Network
ACME-wired-guest	
Connection Type: Wireless Wired	
Guest Switch	× ~ 🕀
Select an Access Device Group to make this Network only applicate linked to the same Access Device Group. Status: Enabled	ile to a subset of Access Devices. Multiple Networks can't be
Authentication	
Authentication Type	
Captive Portal	
Captive portal type: 🔘 Internal 🔘 External	

Figure 6-23: Network Settings

Provide the following details to update the selected Network	← Back
Captive portal type: 💿 Internal 🔘 External	
Select internal portal	
Default	Preview
aptive Portal Initial ACL For Portal Authentication	
guest-acl	Show Domains
Authorized User Groups	•
Authorized User Groups Applicable for organizational users only	•
	•
Applicable for organizational users only	•
Applicable for organizational users only Re-Authenticate Clients	•

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

Figure 6-24: Portal URL



6.4.2 Configuring EOS

An administrator must also configure the Arista Switch for the guest workflow.

Log in to the switch and add the following commands:

```
dot1x
   aaa accounting update interval 60 seconds
   mac based authentication hold period 300 seconds
   radius av-pair service-type
   mac-based-auth radius av-pair user-name delimiter none
lowercase
   Captive-portal
!
ip access-list guest-acl
   10 permit udp any any eq bootps
   20 permit udp any any eq domain
   50 deny tcp any any copy captive-portal
   60 deny ip any any
!
```

Chapter 7

Configuring Segmentation Policies

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

7.1 Status

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

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

7.2 Conditions

Conditions define rules based on various attributes associated with:

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

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

7.3 Actions

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

- · VLAN assignment
- · Application of ACLs
- · Allow or deny helper access primitives

- Standard RADIUS attributes
- VSAs

7.4 Configuration

Perform the following steps to configure segmentation policies:

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

7.4.1 Sample Segments

The following samples are for reference.

Sample Employee Access Segment:

Figure 7-1: Employee Access Segment Policy

10 10 10 [2]]]				
escription	licy for employee access in the ACME corp			
his is the segmentation po	icy for employee access in the ACME corp			
atus: Enabled		Disable Monitor		
conditions MATCHES ALL				
Network: Name is	ACME-CORP	×		
User: Group is Er	nployees	×		
		≡ + Add Condition		
Actions				
Assign VLAN Assign V	LAN through RADIUS response	×		
O VLAN	ACME-CORP-Access			
0				

Sample Contractor Access Segment:

Figure 7-2: Contractor	Access	Segment	Policy
------------------------	--------	---------	--------

ame CME Corp Contractor Ac	22991	
2. 1939		
escription his is the segmentation p	policy for contractor access in the ACME corp	
atus: Enabled		Disable Monitor
Conditions MATCHES A	LL	
User: Group	Contractors	×
Access Device: Location	n Contains Arista Cognitive WiFi/North America/San Jose	×
		≡+ Add Condition
Actions		
Assign VLAN Assign	VLAN through RADIUS response	×
	ACME-CONTR-Access	

Sample BYOD Access Segment:

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

scription		
his is the segmentation polic	y for BYOD devices	
atus: Enabled		Disable Monito
onditions MATCHES ALL		
Access Device: Location	contains Arista Cognitive WiFi/North America/San Jose	>
Network: Name	CME-BYOD	×
User: Group in Empl	loyees 3 Contractors 3	>
		≓+ Add Condition
ctions		≓+ Add Condition
Assign VLAN Assign VLA	N through RADIUS response	≡ ₊ Add Condition
	N through RADIUS response	
Assign VLAN Assign VLA	ACME-Internet	
Assign VLAN Assign VLA	ACME-Internet	
Assign VLAN Assign VLA	ACME-Internet	

Sample IOT Access Segment:

Figure 7-4: IOT Access Segment Policy

ame		
CME Corp IOT Access		
escription		
his is the segmentation p	olicy for IoT devices in ACME Corp	
Enabled		Disable Monito
Conditions MATCHES AL	L.	
Network: Name is	ACME-IOT	×
Client: Group is	IOT Devices	×
		≡ ₊ Add Condition
Actions		
Assign VLAN Assign	VLAN through RADIUS response	×
	ACME-IOT-Access	
		≕+ Add Action

Configuring the Devices in AGNI

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

You can add the devices to AGNI by:

- · Manually add the devices.
- · Add a whole subnet
- · Import the devices using CSV file

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

8.1 Adding an Access Device

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

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

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

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

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

- f. Enter the RADIUS Shared Secret for the device.
- g. Enter the TACACS+ Shared Secret for the device.
- h. Enter the RADIUS CoA Port for the device. The default port is 3799.
- i. Enter the Access Device Group to which this new device is part of. You can also add a new device group by clicking the + icon.
- j. Enter the Location of the device.
- 3. Click the Add Device button.

Figure 8-1: Adding or Importing a Device

ONITORING Dashboard	Add or Import Access Devices Provide details to add a new device, subnet or import devices from a file	(← Ba
Sessions CESS CONTROL	Choose Action: Add Device Add Subnet Import	
Networks Segments	OnPrem	
ACLS	P Address 1011.24	
Identity Provider	Required for RADIUS / TACACS+	
User v		
Client v	Required for RadSec	
Guest 🗸	e Verda	
FIGURATION	Arista WiFi	-
Access Devices A	Servir Marther	
Device Administration V	- MAD SAME SHOW -	Ø
Certificates ~	/ MCAOS+ Started Secret	Ø
System 🗸	RADIUS GAN POT	•
NCOURSE Explore Installed Apps	3799	
Instaned Apps	Access Device Group	- 🕀
	Optional	
	Location	0
	Optional, example: Global/America/California/Site-1	

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

Figure 8-2: Adding a Subnet

agni onPrem			
		Add or Import Access Devices Provide details to add a new device, subnet or import devices from a file	← Back
Sessions		Choose Action: O Add Device Add Subnet O Import	
 Networks 2 2 Segments ACLs 		OnPrem	
IDENTITY		10.1.1.24/24	
 Identity Provider User 	~	Arista WiFi	-
□ Client ☆ Guest	ž	RADIUS Shared Secret	٥
CONFIGURATION		TACACS+ Shared Secret	
 Access Devices Devices Device Groups 	^	RADUS CoA Port	•
Device Administration	~	Access Device Group	* 🕀
System	~	Optional	
CONCOURSE ::: Explore ::: Installed Apps		Location Optional, example: Global/America/California/Site-1	0
			Cancel Add Device

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

8.2 Importing Devices into AGNI

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

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

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

Figure 8-3: Importing Access Devices

Destinant			Access Devices	fart summettions					Add or Import Devices
" Sessions									0
P Networks		9,						Al Devices	
ACLS			NAME	MAC ADDRESS	VINCOR	C LOCATION	840965 378705	UPGATE TIME	
altry.		2	Merall 8815-68180/K-e0	66/10 44.00 (Fail)	Chica Metani (10102023 024448	/ 0
Mantity Provider		\mathbf{x}	Munity AP	1010124.8277.4	Artista (MUT)	Anna Cognitive WPShorth America		110(202123 23:99:33)	10
1 Uners	8		Aruba AP	3817-01059-58	(Analog)			A/7/2023 03/20/41	1.
A. User Dringes		4	cites	00 11 (0 (0 (0 (0 (0 (0	Ariana Wilth	daeta Oara		10/5/2023 03:02:08	/ 8
Ciant	Sk .	10	Cisco WLC	14 to 2 the 90 day 20	(Dars)			10/17/2023 02:53-08	/ 0
Citerta		κ.	arista-710P	2010/07/3034	Aring Salari	Arista OsudiVision/Tenen/San Jone	• 1	11/14/2023 10:30:00	1 0
Client Groupe		1	suparsa,0-230	30/8624.8276.wf	Arona Well	"North Americalian Jose		1014/2023 18/30:06	/ 0
Access Devices		\mathbf{x}	suparus-sillő	44101-2410-2410	Arata Willi	Weisers America/East San Jose		1014/2023 1830:00	/ 8
Devices	1	1.	Dette Anaba AP	11223344.0548	Andre	DobathmentartianaClarabab 1		102202023-02-49-58	1 0
Device Groups		- 10	Dems Claco AP	automorphism 7	Chern	Barra Cara		19220202234334838	1 0
David Galeways			Dumo Ariata AP	al 62x3.04x5/6	(Arrang Marth)	Santa Dans		1025/0029 03 49 09	/ =

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

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

Figure 8-4: Choosing Import option

MONITORING Dashboard	Add or Import Access Devices Provide details to add a new device, subnet or import devices from a file	← Back
CCESS CONTROL	Choose Action: Add Device Add Subnet Import	
 ♥ Networks ⊨i= Segments ♥ ACLs 	Access Device Group Optional Upload 527 file	* ⊕
IDENTITY Client Client	Columns: name*, ipAddress, mac, vendor*, serialNumber, radiusSharedSecret, tacacsSharedSecret, tocaPort, location	Sample 🛓
Guest		Cancel Import
 Access Devices Devices Device Groups 		
Device Administration	S V	
Certificates	×	
System	×	
III Explore		

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

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

- · Radius Shared Secret (optional)
- TACACS+ Shared Secret (optional)
- CoA Port (optional)
- Location (optional)
- 3. To download a sample . CSV file, click the Sample button.
- 4. Click the **Browse** button and select the .CSV file that needs to be uploaded. The **Import** option gets enabled after the .CSV file is uploaded (see image below).

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

Dashboard	Add or Import Access Devices Provide details to add a new device or import devices from a file	← Back	
Sessions SS CONTROL	Choose Action: O Add import		
Segments	Access Device Group	- ④	
ACLs	Optional Userar Div Ne Browse sample-devices.csv		
Identity Provider User v	Columns: mact, vendort, namet, lpAddress, serialNumber, location	Sample 👲	
Client ~		Cancel	
Access Devices			

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

5. Click **Import** to import all the devices to AGNI.

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

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

Figure 8-6: Access Devices List

Ξ.

Destroyerd	6	Access Devices Use A Accessed to the Accessed							
· Senatura									=
Metworke	٩						At Devices		-
ACLS		NAME	MAC ADDRESS	VINCOR	LOCATION	SADIAC STATUS	UPDATE TIME		
maner -	1.80	Merani 88115-68.60.11+8	88.15.44.8075.40	Clause Menant		•	11/16/2023 03:88.48	1	8
C Identify Provider	1	Mobil's AP	20.00.2110.77.41	Areta MPL	Artela Cognitive Will/North America		FVW/2023 23-10.33	1	
Chevit v		Anuba AP	8917131453458	Angela			8/7/2023 08:00:04	1	
and a store	4	alacia	00 Mu9 20 05 00	Advect HINK	Danta Clara		10/5/2029 02/02/09	/	
Access Devices 1 / /		Cisco WLD	Tel Ing The 100-104-20	(Deck)			10/5/12/02 02:43:08	1	
Cl. Device Services		arista-210P	21.00540.0138.04	(Avista Balture)	Antesa Dasadvision/Tenent/Sav Joan		1114203310.0010	1	
Cloud Gateways	10	маратта, 0-239	30 mm 24 m 22 7 m ar	(Aviese Mill)	Nerts America/Las Jose		11/16/2023 10:00:08	1	
Device Administration 🚽	1.	auguarna-w258	wise(124102a))/	Artesa Milli	"North America/Last Law Jose	0	11/4/2023 16:00:45	1	
Certificates -		Demo Arube AP	112233-44.95.68	Avite	Optio/America/Ganaciaet 4		1123/2023 03:40:36	1	
3 System v	10	Cisco AP	an identification of	(Dect.)	Barta Cara		10242023162838	1	
Explore	п.	Artsta Alf	vision and a second second	Arista 2001	Garta Clara		11/24/2022 19:20:03	1	
Inshalled Apply	-tr	Arista Switch	22/33/44/31(08/77	Adata Darkers	Sam Jone		1124/2023 16/29(33)	1	8
	10	Denso AP	#81604031271	(Deven)	San Jone		17/23/2023 03:49:39	1	
	14	Demo Cisco Meraki	a6.05 c4:03:02:02	Crucit Mercard	Mountain View		11/23/2023 03:48:36	1	
	18	Arists C-75	001111418-44-45	Anata MEPL	Ocharik-nariva/famaCarat.ak-1		11.04/2023 15:3110	1	

Chapter 9

User Configurations

9.1 Users

9.1.1 All Users

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

9.1.2 External Users

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

agni								G	0 💽
MONITORING	-	Users Manage the list of identity	v users					6	+ Add User
CONTROL		Users Local Externa	1						
 Networks segments 		Control by news or evidet					Ary		
@ ACLS		NAME	USER ID	TYPE	STATUS	UPDATE TIME			
IDENTITY .	1	Steve Kratt	steve.kratt	External	Enabled	7/10/2023 13:35-15		1	
 (≥) Identity Provider ▲ User ~ 	2	Mary Osborne	mary onborne	External	Enabled	7/10/2022 11:14:48		1	
1 Users	1								
14. 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.

Dashboard	+	Steve Kratt View user details and update	the selected user		÷	Back :
Sessions SESS CONTROL Networks Segments ACLs	Uber	ve Kratt				
Identity Provider						
User ^	Statu	s: Enabled				
ALL User Groups				Cane	el Upda	te User
Client ^	User	clients			H	lide Clients
Client Groups	Q	Search by MAC address		Any		*
Access Devices		MAC ADDRESS	DESCRIPTION	STATUS		
Certificates ~	1.	70:1a:b8:82:10:31	Steve Kratt's Windows	Enabled	11	

pdated 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.

agni		
MONITORING	Add Local User Fill in the fields below to add a new local User	← Back
Sessions ACCESS CONTROL	User Id test@myorg1.com	
Networks + = Segments	Use email address to get the credentials sent as an email to user.	
ACLs	Test User	
IDENTITY	Password	
LUser ^	Status: Enabled .	
Users	User should change password at next login: Enabled	
Client ~	Login Invitation Email	Disabled Orm
Access Devices ~		
Certificates ~	Enable to send notification with account details to user via email.	
Collapse Sidebar		Cancel Add User

Figure 9-3: Add Local Users

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

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

Eb Marage Clients	Clients Manage the list of clients as on 62/010	224 13 14 07					
	Q Search by MAC address in party days.					Ary	
	# WAE ADDRESS	DESCRIPTION	(MINER (VILER)	\$127.45	VPDK78 TAVE		
	1	Keert's Mac OS X	Keert	Brathed	02/07/2024 11 53 51		•
	2 bleasticidd ee ff		Kents	Endowd	01012924 22:30:35		۰
	3 ++.5133.1526.04	Kent's Astroid	Kert	Enabled	21/04/2024 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

ngni					େ ୭
MONITORING Dashboard Sessions ACCESS CONTROL Notworks	All Groups Local Extern	udes both local and external user groups			+ Add Local User O
ALA Segments	Q. Smith by Nome				
ACLS	# NAME	DESCRIPTION	TYPE	UPDATE TIME	
(4) Identity Provider	1 ACME Contractor		External	10/07/2023 21:05:38	0 0
± 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.

Dashboard	Update Local User Group	← Back
Sessions	Fill in the fields below to update the Local User Group	
CESS CONTROL	None -	
Networks	Test User group	
- Segments	Description .	
ACLS	local user group	
ENTITY	Type	
C Identity Provider	Local	
User ^		
1 Users	Users	
🔐 User Groups	Available Users Assigned Users	
Client		
Clients	Q Search by name or email	
Client Groups		Selected: 1
NFIGURATION	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.

agni		
MONETORING Dashboard Sessions ACCESS CONTROL Networks ALA Segments CALS IDENTITY (2) Identity Provider		Test Client Group Add or Import Clients Ell In the fields below to update the Client Group Nume Test Client Group Escongton Description The client mapped to this group are test clients User Absolution *
 User Users User Groups 	•	Group U-PSK Enabled All Clients belonging to this group must use the below Group UPSK to connect to the network.
Client	^	Сору Сору

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

Fill in the fields below to add or import Clients to a Client Group	← Back
Test Client Group	
Description	
. User Association Not user associated	•
Group U-PSK	Disabled O
Allowed Networks	
Purte-wha Select Networks	*
	Fill in the fields below to add or import Clients to a Client Group Firme Test Client Group Description User Association Not user associated Group U-PSK Allowed Networks Filtrons

• **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		Fill in the fields below to update the Client Group	C Back
 Networks Segments ACLs 		Group U-PSK	Disabled Opp
L User	•	Allowed Networks	•
Lat User Groups	^	Delegated Management	Enabled
Clients		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

loudVision 290i				
MONITORING Dashboard Sessions		Add or Import Clients Fill in the fields below to add a new Client or upload a file to import Clients		← Back
CCESS CONTROL		Client Group		
Networks		Test Client Group		* 🕀
Li= Segments		Choose action: Add Import		
ACLs		chose action.		
DENTITY				
E Identity Provider		MAC Address 00:11:74:12:ed:4f		
Luser	^	Description		
2 Users		Test Client		
🕰 User Groups				
Client	^			
			Cancel	Add Client
Clients				
Client Groups				

Figure 10-5: Client Import

gni		
ONITORING	Add or Import Clients	← Back
Dashboard	Fill in the fields below to add a new Client or upload a file to import Clients	
V Sessions	Client Broup	
CESS CONTROL	Test Client Group	- 🕀
 Networks Segments ACLs 	Choose action: O Add tmport	
ENTITY	, Upload CSV File	
Continue	Browse	
User	Columns: mac*, description	Sample 🛓
LUSers		
Jan User Groups		
Client		Cancel Import
Clients	Clients in this group	Show Clients
NFIGURATION		
Access Devices 🗸 🗸		
Certificates		

10.2 Client Details

Click on the clients to display the client details:

• Client Information – Displays MAC address, description, client group, passphrase, and status.

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

Figure 10-6: Client Details

Steve Kratt's Windows Vere client dectais and update the selected client		(* Bask)
	Client Details	
	Device Type	Computer/Windows
Inne Kart's Woopes	Machine Authenticated	(8)
State (Least) +	Added At	7/10/2023 13 49 20
	Upplaned An	7/10/2023 13:49:36
Cancel Update Office		
	Clast Fingerprint	<u>^</u>
	DHCP Option 66	1.3.6.95.31.33.43.44.46.47110.121.349.252
	DHCP Options	55
	ARAC Venator	Initial Componishin
	10170 User Agent	Missilia/5.0 (Western NT 10.0; WestA; e64) Approximits(2)(5)7.30 341/746; mar
	HTTP User Agent	Microsoft NCS
	Last Session Details	Ound
	IF Andress	10.86-50.226
	Location	
	Septert	Default
	Authentication Status	(Satass
Client Cortificate (IAP-TLB)		(Beat)
Guipeen Dis		Chi-steve avest, O-myong1.com
huar (N		CN+404, usuar CA, O+7x0ne-Beta (C1eH256c-ex15-4ee3-93b7-c2ab4872b4sc)
Expery Data		7/9/2024 13-49-36

Figure 10-7: Client Sessions

								G	
۹	Search	by Identity, MAC Address, IP Addres	is or Session ID			Auth Type Any	•	Any	
~	#	IDENTITY	ТҮРЕ	MAC ADDRESS	IP ADDRESS	STATUS	TIMESTAN	лр	
~	17	steve.kratt@myorg1.com	Client Certificate	70:1a:b8:82:10:31		Falled	7/10/2023	3 13:51:20.425	0
	18	steve.kratt@myorg1.com	Client Certificate	70:1a:b8:82:10:31	10.86.60.226	Success	7/10/2023	3 13:49:40.005	0
	19	steve.kratt@myorg1.com	Client Certificate	70:1a:b8:82:10:31		Failed	7/10/2023	3 13:36:30.225	0
	20	steve.kratt@myorg1.com	Client Certificate	70:1a:b8:82:10:31		Falled	7/10/2023	3 13:36:19.984	o
	21	steve.kratt@myorg1.com	Client Certificate	70:1a:b8:82:10:31	10.86.60.226	Success	7/10/2023	3 13:36:02.830	0
	22	mary.osborne@myorg1.com	Client Certificate	e4:a4:71:26:2a:b4	192.168.1.14	Success	7/10/2023	3 11:19:11.704	ø
ŝ	23	mary.osborne@myorg1.com	Client Certificate	e4:a4:71:26:2a:b4	192.168.1.14	Success	7/10/2023	3 11:18:36.506	0
,	24		Client Certificate	e4:a4:71:26:2a:b4		Failed	7/10/2023	3 11:18:25.244	0

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:

특

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

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

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

To generate the Client certificate, perform the following steps:

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

Figure 10-8: Clients Dashboard

Dashboard			Clients Manage the list of Clients				Client M	anagement Portal + Add Clie	it or Import C	lienti
Sessions									C	3
Networks		Q	learch by MAC address or owner	(used)				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	
dentity Provider			2 5c:e0:1e:87:e5:a1	Shailu's Mac OS X	Shallu	Enabled		20/03/2024 13:31:39	1	0
Client	÷.		3 88:b1:e1:13:3d:12	test		Enabled	venky	18/03/2024 11:47:48	1	
Guest	•		4 88:b1:e1:13:3d:1f	test		Enabled	venky	18/03/2024 11:45:04	1	
Access Devices			5 16:6b:3e:d3:7e:c4	Auto-registered using Eduroam		Enabled		18/03/2024 03:01:42	1	0
Device Administration	~		6 bc:d0:74:01:d9:33	Auto-registered using Eduroam		Enabled		17/03/2024 00:40:19	1	0
Certificates	ž		7	Auto registered by Workspa	Atul Tambe	Enabled		16/03/2024 05:40:09	1	0
ONCOURSE			8	Auto registered by Workspa	Abul Tambe	Enabled		15/03/2024 08:48:46	1	0
Explore			9	Auto registered by Workspa	Abul Tambe	Enabled		15/03/2024 08:39:35	1	
Installed Apps			10 be:0f:65:37:e8:8c	Auto-registered using Eduroam		Enabled		15/03/2024 05:08:02	1	0
			11 11:11:11:11:19	Atharva Test Client 1		Enabled	test4	14/03/2024 13:41:23	1	
			12	Auto registered by Workspa	Atul Tambe	Enabled		12/03/2024 06:07:07	1	
			13	Auto registered by Workspa	Mohit Goyal	Enabled		12/03/2024 05:00:48		

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



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

Figure 10-9: Select Client

agni I					ତ ଡ 😐
MONITORNO	Shailu's Mac OS X View client details and update the selecter	d client			🔶 Back
~ Sessions	WC A39111 50:09.10:37:05:33			Client Details	
Ketworks	Service And And			Device Type	Computer/Mac OS X
ALA Segments	Shailu's Mac OS X			Machine Authenticated	No
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 	×	Client Fingerprint	×
Clients	Device Manager	- Jand	×	Last Session Details	Closed
Client Groups	Workspace ONE: Compliance Status	Compliant	×	IP Address	192.168.0.101
Guest v		**	Add Attribute	Location	*/India/Uttarakhand
Access Devices		1. C. C.		Segment	
Device Administration		Cancel Update Client		Authentication Status	Success
☐ Certificates ∨ ○ System ∨	Client Certificate (EAP-TLS)				Good
CONCOURSE III Explore	Subject DN				CN+Shailu, O+local
I Installed Apps	Issuer DN				CN+AGNI, Issuer CA, O+arista-dev
	Expiry Date				12/03/2025 12:12:40
					1

3. Download the certificate by clicking the **Download** button (arrow).

The X509 certificate (.pem file) is saved to the download folder. You can open the file to verify the details. Figure 10-10: Download Certificate

Dashboard		Shailu's Mac OS X View client details and update the selected	d client				🔶 Back	
 Sessions SCESS CONTROL Networks 		ScrothersPosat				Client Details Device Type	Computer Mac OS X	
A Segments		Shalt/s Mac OS X Status: Enabled =				Machine Authenticated Added At	No 12/03/2024 12:11:45	
C Identity Provider	2	Client Attributes				Updated At	14/03/2024 10:53:12	
Client ^	•	Arista NDR: Risk Action Device Manager Workspace ONE: Compliance Status	•	quarantine Jamt	×××××××××××××××××××××××××××××××××××××××	Client Fingerprint	Cose	
Client Groups	•	Wonspace one: Compliance Status		Compliant	IP Address 19236 Location */India/Uttar			
Access Devices	-	Cancel Update Client				Segment Authentication Status		
System		Client Certificate (EAP-TLS)	Good					
Explore Installed Apps		Subject DN Issuer DN					CN+Shailu, O+loca CN+AGNI, Issuer CA, O+arista-de	
instance apps		Expiry Date					12/03/2025 12:12:4	

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

Figure 10-11: Generate Certificate

MONITORING	Shailu's Mac OS X View client details and update the selected client		- Back		
🗸 Sessions	Scredite 87/e5/at	Client Details	Co Reprofile		
Networks	Description	Device Type	🤤 Generate Certifica		
Segments	Shailu's Mac OS X	Machine Authenticated	E Delete		
ACLS	Status: Enabled	Added At	12/03/2024 12:11:45		
1) 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 10-12: Certificate - Generate Radio Button

agni I					6	0	M
Monstolens		Generate Client Certificate Fill in the details to generate client certificate for the selected client	é Beck	8			
ACCESS CONTROL		Generate Certificate: Generate Use CSR					
Networks 4/4 Segments		Over Screitte 87:45:41 (Sheku's Mac OS X)					
@ ACLs							
EDENTITY (2) Identity Provider		A certificate already exists for the selected client. Generate only if required.					
± User	~	🖶 Shally	Expires on 12/03/2025				
🛄 Client	^	Subject DN	CN+Shallu, O+local				
Clients		Issuer DN	CN+AGNI, Issuer CA, O+arista-dev				
* Guest	~		<u>*</u>				
CONFIGURATION		charact					
Access Devices							
Device Administration	~	Specify the password to generate the client certificate					
Gertificates	~						
System concounts	*		Cancel Generate Certificate				
Explore							

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

Figure 10-13: Certificate Added

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 Groups 	•	Shahu Expires on 21/03/2022 Subject DN CN+Shahu, O+local Issuer DN CN+AGN, Issuer CA, O+anista-dev				
AT Guest	÷		J			
 Device Administration Certificates 	> > > >	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 10-14: Certificate - Use CSR Radio Button

		Generate Client Certificate Fill in the details to generate client certificate for the selected client	← Bac
V Sessions			
ACCESS CONTROL		Generate Certificate: O Generate 💿 Use CSR	
Networks		Clert	
1± Segments		1c:4d:70:b3:b9:97 (Shailu's Linux)	
ACLS			
IDENTITY		A certificate already exists for the selected client. Generate only if required.	
Identity Provider			
Luser	~	📮 Shailu	Expires on 27/03/2025
Client	^	Subject DN	CN=Shailu, O=local
Clients		Issuer DN	CN=AGNI, Issuer CA, O=arista-dev
Client Groups		ISSUE DIN	GREACH, ISSUELON, C-SISTE-DEP
Guest	v		*
CONFIGURATION		0	
Access Devices	~	Select Action: O Upload CSR File Paste CSR	
Device Administration	~	Sample CSR text	
Certificates	~	Sample USK text	
System	~		
CONCOURSE			
Explore		C	

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

Contractor		桁		rest Users	Quest Users				+ Add Duest	r legert Quests	O lettings
// Sessions		A810	sers	Pertol	ursk						
· Networks		٩	Sheed	t by Chernister, B	rval, Agenties, Name or Company					Any	
& ACLA		0	•	USERNAME	(MAL	GUEST AFPROVER	TYPE	\$14115	ACTINATION GATE	EXPRATION DATE	
X Meetily Presider	4	D	1	(2wi	етофлюваннорумски	shrang chiedla gerstacen	Porter	Indied	29/03/9024 11/10/57	00/34/2224 1119-57	
Cient Gunt		٥	7	Ortang	skingchicela@pailcon		Porte	Endled	20/03/2024 14 55 47	05/04/2024 14:55/47	-
🕺 Users 🕞 Partala			5	guestasort	рыктрыцтри.com		Portel	Entited	21/03/2024 11:28:00	05/34/2224 11/28/00	-
04/00/00											

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.

oose Actor: Ass Import			
sentzser1			
andjenne je com			
w.			
guers			
004/2024 08:32 PM	10/54/2024 05 52 PM	Veloty 8 Days	
en l'est			
Rional 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

B Partneri	1 Event Users	and the second sec					* Add Denite New	them: 0 hille
* Sealars								
W Martantia	4. (and a second second second	and here i serve i					100	
a lagrante P mon		1946	NAU ATTRING	1100	1000	and the local diversion of the	CONSTRUCTION DOCUMENTS	
(And I all a second sec	() I prime	and a gradient state of the sta		(Marine)	(marked)	10/14/2014 (1401-14	Referigible Delle Mi	
Cauriy Poundar Line -	D r permit	pediespecie		(100)	Tame:	30/10/2010 01/10/10	10140 (1014 (015) 101	
2 mail in								
form -								

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

cose Action 🔘 A33 🛞 Inport			
urur Dig usens			
antran Distriction contas Par	10/04/2020 09:33 PM	Value of A Days	
wine land			
Browne Lamps-guest-conv.com			
unic useriamet estalit name, company, phone, ad	3945, 00396		Sample

The imported users are listed in the portal user listing.

Figure 11-6: Portal User List

f? 0	west Users	nen.					· Add Daniel in Surger	riberta 🖉 bellege

۹	1 by Concerns, 5 bot, 4) (m)	
0 .	stante	2545.	0.417 #740743	7/5	1949A	ACTIVITIE 2475	EXPRATORIZATI	
a '		and any features of the grade and		And	(Bunker)	400x0000 2144 00	NUMBER OF A DESCRIPTION	1.1
	ana iti	an ang Marilan Ang grain at		(Renal	(Bushed)	NO10400000 (** 444.00)	1004,0014 (144.00	1.1
a •	ana 11	an approximation projection		(Area)	(based)	Sciences in second	Notacidita Prantili	/ 1
a •	and it.	and any development out		(here)	(butter)	K015-C2524-21-62-08	No. 1014 (1984) (1982) (19	/ 1
0.1	100	an any Montha Object on		(here)	(100)	10110301214210	10/04/0014 (P-42-00	/ *
0 •	and the	an any Marine Condison		(mer	(beater)	1011-010427-018	10/04/0124 21:42:00	/ 1
a +	Details	erine prinche dans for		(2004)	(based)	824632421018	NO43034210508	/ 1
0 .	period	participation and		(Area)	(Darbert)	\$20% (20) × 20 (20) (20)	1004.0034.00400	

If the admin or guest operator uses the **Import and Email** option, an email (similar to previous image) is sent to the email address mentioned in the CSV file.

Guest users added using self-registration and host approval portal methods are also listed here. In the case of the Host-Approval method, the guest sponsor username is listed in the Guest Approver column.

11.1.1.2 UPSK Users

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

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

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

3. Select the Add UPSK user option, and add email, user validity, and device limit (mandatory fields). You can also add optional guest information, including name, company, phone number, address, and notes.

Figure 11-7: Add or Import UPSK Users

Add or Import Guests Provide the following details to add a new guest user or uplated a file to import guest users.	+ Beck
Chrosse Actions O Add pomariseer I Add UPSK user O Import	
shrivangchkodkur-upsk@gnul.com	
8 Hurs	
_ (worket	
Additional guest user information	
TestUser	
Oneny	
Example LLC	
I'rone :	
Astres	
(****	
Test account	
	Cancel AM Add and Envel

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

Figure 11-8: UPSK User Details

1 Update Ganet User	nd good and		(in the second s
nor anna gcliochangosógraí con			Telesyst (M sole for the use
			Vieters, brawie 🖤 with law
O The Lat Product part and			■270
And an and a second sec		O Corr	
Annenin Print II	a man	THE OF CONTRACTOR OF T	前發揮
Bana (Seate) 🐢			
Additional guard user information			
No.			
areas -			
bargarist			
-			
METHOD .			
ten Nel scinet			
			(annual)

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

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

Figure 11-9: Guest User Registered Successfully

	Guest user registered successfully. Helis Testicue A unique 1019 parquirant has been unualed for you. One the following parquirant to sometry your client devices. Hill F3 Pesspherese: 3xe574mar6 Device Tandii: 4 clientis Valid france: 05 Apr 24 15: 15: +0535
	A ungen With peopleses has been unaled for you. Une the following peopleses to convert your client devices. With FS People reset: 1 we57 device Device Tandy: 4 clients
	une the following paraphrane to convert your client devices. Will PS Paraphranes: JaceS74ena18 Device Tandy: 4 clients
	une the following paraphrane to convert your client devices. Will PS Paraphranes: JaceS74ena18 Device Tandy: 4 clients
	Device limit: 4 climits
	Valid from: 05 Apr 24 15 15 +0530
	Valid webit: 03 Apr 24 21:58 +0530
	MPI Notwork upshiGuest
	QR mole file: uppinGuest pro
	Boart the nationals QR state and served to the scheles, reduces.
	Fits is an automated shall sufficience. Research wat tuply in this teamoup.
exactment - Sorvetty Snal Q	
BC5376	

11.1.1.3 Guest Operator

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

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

agni I				७ ७ 😐
MONTORNE		Manage the list of Guest Users as on 09/07/2024 22:50:32		🖹 Self-service Portal + Add or Import 🗘 Settings
Sessions		All Users Portal USER		E =
 Networks Ale Segments 		Q Starch by Username, Small, Approver, Name or Company .		Avy *
@ ACLS			No data to driplay	
(2) Identity Provider				1
1 User	*		Manage Quest Settings	
f Guest			Ourst Sponsors	
# Users	1		Selected user groups can manage only their guest users,	
Portals			User Groups +	
CONTIQUEATION				
Access Devices	*		Quest Operators	
Device Administration	*		Selected user groups can manage all guest users including Guest UPSK.	
Gertificates	*		Guest Sponses O Guest Operators O Select User Groups	
Concounse			(was sporter) (was spectra of section (color	
III Explore			These users can use Self-service Portal to manage guests.	
By Installed Apps			Cancel	

Figure 11-10: Manage Operator Settings

11.1.1.4 Guest Sponsor

Guest sponsors are users who belong to a specified user group and have the right to add portal users. Guest Sponsors can only manage the portal users they add. The admin can configure particular user groups as guest sponsors by selecting the **Identity** > **Guest** > **Users** > **Settings** option.

11.2 Guest Onboarding Offerings in AGNI

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

11.2.1 Portal Based Guest Onboarding

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

The AGNI admin can add a portal with multiple customization options and modify every field on it. The 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 11-11: Enable CAPTCHA

Dashboard	New Template Customize Guest Portal		€ Bac
Sessions	Configuration Customization	💿 Swiect an eliment to update It's appearance.	
P Networks Segments 3 ACLs Deentry	Perter Name Minimum Part Distances (a) Organizational Mark Login ()		
A) Identity Provider L User v Client v () Guest v Contrastantion v Device Administration v	Authentication		
Cartificates System Controlled System Controlled Explore Solution The System Solution	Promodenentialism Redenest UR. Organizational User In transmission Providence Inter User Inter User Inter User Inter User Inter User Inter User Inter User I		
	Autorized Liker Conge +		

Figure 11-12: Guest Login

ARISTA	200
EMPLOYEE GUEST Connect to enjoy free Wi-Fi Enter username	
E M9 I H 7 G Enter CAPTCIA Connect By signing in you accept the Terms Of Use.	-
	$\partial \partial \partial \nabla$
	VVVVV

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 \rightarrow Guest \rightarrow Portals.

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

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

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

Figure 11-13: Redirect URL

튭

agni I ADNI-DI	imo			G	(2	Ð
Cashbeard	d	Arista CloudVision Enter the following fields to configure the app.	(dr Back				
Sessions CESS CONTROL		New Arrest Control of					
Networks		Anata ChaudWania					
Segments		un, Mitpic/Jewww.anista.is/					
ACLA		- New					
ENTOY			0				
Identity Provider							
User	<u> </u>		Control Verify Install				
Client	* -						
Guest	~						
Access Devices	φ.						
Device Administration	<u></u>						
Certificates	0						
System	0						
HCOURSE							
Explore							
Installed Apps							

11.2.1.3 Organizational User Login

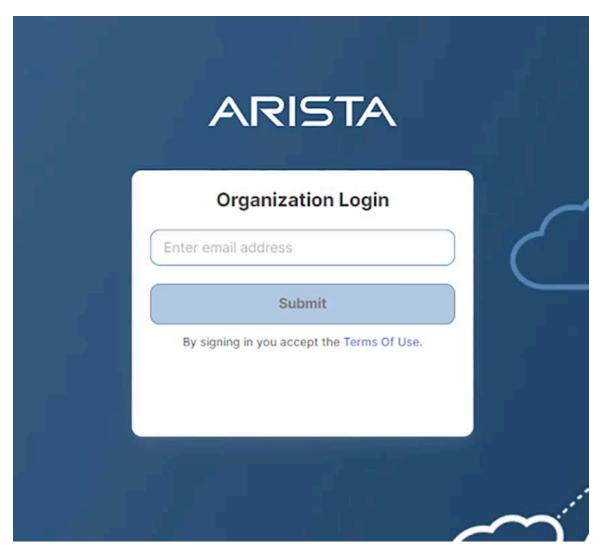
This guest onboarding method is mainly used to onboard organizational user devices onto the network. This method requires an **Identity Provider**. In this method, a portal is presented to the user; the user must provide his domain credentials that are verified against the configured identity Provider. If the user gets authenticated successfully then the device gets onboarded onto the network. Admin can restrict the user onboardings using the **Authorised User Groups** feature. Users belonging to these user groups are allowed to onboard the

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

Org User Portal		
Authentication Types		
Organizational User Login 😣		
Authentication		
ganizational User		
	Re-Authentic	cation Period
e-authenticate User	 Re-Authentic 12 	Hours -
te-authenticate User		
te-authenticate User Periodic Device Limit		
te-authenticate User		
te-authenticate User Periodic Device Limit		

See the sample portal below:

Figure 11-15: Organizational User Login Portal



11.2.2 Guestbook Based Onboarding

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

11.2.2.1 Guestbook Method

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

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

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

Figure 11-16: Guestbook Configuration

Ę

agni myorg1.com		ଓ ଡି 🕓
MONITORING	Customize Guest Portal	← Back
ACCESS CONTROL	Configuration Customization	💿 Select an element to update it's appearance.
Networks ± ± Segments	Portal Name	ARISTA
C ACLS	Guestbook 😵	Contract to enging free Wi-Fi
 Identity Provider User 	Authentication Guestbook	Diament Oliver
드 Client ~ 作 Guest ~	Guest User In-anthriticate Guest Always	tere statistics
CONFIGURATION	Device Limit ~	<i>₼₼₼</i> (
Device Administration	CAPTCHA Enabled	
CONCOURSE	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 username Enter password	\sim
E M9 1 H7 5 Enter CAPTCIA Connect By signing in you accept the Terms Of Use.	0000
	00000

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	11-18:	Enable Se	elf Registratio	'n
--------	--------	-----------	-----------------	----

Configuration Customization		
. Portal Name		
AGNI Guestbook		
, Authentication Types		
Guestbook 🛞		•
Authentication Guestbook		
Authentication Guestbook		
- Default Validity	Enabled	

Below is a sample portal:

Figure 11-19: Self Registration Login Portal

	e Wi-Fi
nter user name	
nter password	
Connect	
Don't have an account By signing in you accept the Term	

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:



	An Account			
Use	r Name			
Ema	iu (
Nan	ie			
Con	npany			
			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	11-21:	Host A	Approval	Configu	iration

Guestbook 😵				¥
Authentication C	uestbook			
. Default Validity		~		
8	Hours 👻			
Allow Self Registration		Enabled	-	
Approval required for gu	est access	Enabled	-	
Add approvers by:) User Groups (C Email Domain	ns	
Authorized User Groups	· · · · · · · · · · · · · · · · · · ·			
Engineering 🚱 and	rover 🙁 Select	Authorized User	Groups	*

Below is a sample portal:

Figure 11-22: Host Login Portal

Connect to enjoy	free Wi-Fi
Enter user name	
Enter password	
Connect	
Don't have an ac By signing in you accept the	

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

Following is a sample form:

Figure	11-23:	Create	an	Account
--------	--------	--------	----	---------

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 11-24: Approve Guest

	Guest User Registration Approval (Comp) > Here	
ACM.	Arista Cloud Vision AGNI 🔹	
		Guest User approval request
		A quest account is created with the following details:
		Name: Shrirang
		Username: Shri
		Email: shrirangchikodikar:ttest@gmail.com
		Company: shrirangchikodikar@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

Perform the following steps:

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

- 4. Shared Clients Disabled
- 3. Click the Add Network button.
 - Figure 11-25: Add Network

MONITORING	Add Network	
Dashboard	Provide the following details to add a new Network	- Baci
Sessions	UPSK for Guest	
 Networks Segments 	Connection Type: Wireless Wired SSD	
ACLS	upskGuest	
Identity Provider	Status: Enabled	
Client	Authentication	
Guest	Authentication Type Unique PSK (UPSK)	-
Access Devices	Allowed Users: O Organizational users only O Guest users only	
Certificates	The wireless SSID type must be configured as WPA2 only for guest access.	Applicable for Arista Wi-Fi only.
ONCOURSE 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 11-26: 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 OUESTS ポ ⁹ Users	Choose Action: Add portal user Add UPSK user Import Email Validity	
	8 Hours Device Limit No Limit	•
	Additional guest user information	~

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

Figure 11-27: Update Guest User

Manage Clients Register Client	View guest user details and update the selected guest user	🔶 Back 🔋
*** Wi-Fi Passphrase OUESTS 所 Users	Kerr Annum Annum Marrier Marrie	Network QR code for this use: Wreless Network: C that-paret-sale
	Additional guest user information	

The following is an example of the email received:

Figure 11-28: Guest Account Registration Success

Guest User Add Confirmation D Max *				8	2
Arista CloudVision AGNI «noreply@agei.atista.ks» to keerthkenher-opdguret@gmal.com. *			III a 36.7M (1 minute ago)	\$ 3 4	I
	Guest Account	t registered successfully.			
	Hello keerthike	shav+upskguestØgmail.com			
	A unique Wi-Fi passphrase ha	is 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	c 24 16:36 +0530			
	Valid until Date: 04 De	c 24 00:34 +0530			
	WiFi Network xyz	QR code file abc			
	kk-upsk-guest-said	kk-upsk-guest-said.png			
	Scan the network QR code an	d connect to the wireless network.			
	This is an automated email	notification. Peace 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 RADIUS or RadSec enabled
 - 2. Authentication Server
 - 3. Accounting Server
 - 4. CoA Enable

Figure 11-29: Configure WiFi UPSK Guest

1	Search Falders / Pases	Search for MACK IP Address / Uper Namer Device Namer. 🛛 🖾 0 🛛 📲 1 👘 🔟 0 👘 16 🔹 🛆 104 🖉 🚺
	• 🗀 Arista Cognitive WiFi	WiFi ~ SSID More :
DASHBOARD	CEI Staging Area	Changes will restart the SSID if it is on. The changes will affect all groups and folders using this SSID.
MONITOR	* 🗀 india	← UPSK-Guests
CONFIGURE	• 🗁 Bengaluru • 🗀 Bannerghatta	WLAN - Basic Security Hetwork Access Control :
ROUBLESHOOT	🗀 Brookefield	Name
INGAGE	• 🗀 Hennur	SSID Name *
	🗀 Horamawu	UPSH Guests
MAPS	🗀 Jayanagar	Profile Name *
REPORTS	🗄 🖾 Marathahalli	UPSK Guests
SYSTEM 🔍	C TC	Select SSID Type
	 Cochin Co Dehi 	Private Guett
	🗀 GGN	Hide SSID
	Pov Pane Pune Pune Pune Pune Pune Pune Pune P	Include AP Name in Beacon
wascript volge	Groups (2)	Cancel Save & Turn SSID On

Figure 11-30: WiFi Security

DASHBOARD DASHBOARD MONITOR CONFIGURE TROUBLISHOOT ENGAGE	Seirih folders / Roon Arista Cognitive Wifi Staging Area C India C India C Inegabru C Itengabru	WiFi ~ SSID Changes will restart the SSID If it is on: The changes will affect all groups and folders using this SSID.	() [®]
MAPS	Horamanu Horamanu Jayonagar D Marathahali	WPA2 PISK UPSK 822.13 UPSK User Private Networks For a table with multiple SDDx on the same VLAX, if UPSK User Private Networks is enabled for any SSID, the first configured SSID takes preference. UPSK User Private Networks This setting is not editable because of UPSK User Private Networks is enabled.	
575TEM 8	TC Whitefield Cookin Cookin	Deny Locally-Administered MAC Addresses Mitigate WPA/WPA2 Key Reinstallation Vulnerabilities in Clients	
	C Pune Pute-rew Uttarakhand North America	, 802.11w	
Keerti Keshav	Groups (2)	Cancel Save & Turn SSID On	

Figure 11-31: WiFi Access Control

1	E Search Folders / Roons	Sepersificar AMACUIR Addressif Uper Namme Device Namme
	▼ □ Arista Cognitive WFi	WiFi ~ SSID
DASHBOARD	E Stagng Area	Changes will restart the 5500 if it is on. The changes will affect all groups and folders using this 3500.
	▼ C3 India	← UPSK-Guests
CONFIGURE	• 🗀 Bengaluru	WLAN V Ibase. Security Network Access Control 1
	🔸 🖾 Bannerghatta	
OUBLESHOOT	🗀 Brookefield	RADIUS Settings
ENGAGE	🕴 🎦 Hennur	RADIUS Pooling
MAPS	C Horamavu	Radiec
1444-1420-00	🗀 Jayanagar	Primary Secondary
REPORTS	: 🖾 Marathahalli	
SYSTEM 🔍	C TC	Authentication Server* Accounting Server*
	Cochin	agri-onprem-pune-02 🔹
		None Add/Tot
	• 🗅 Delhi	agni-onprem-pune-02
	D POY	Send DHCP Options and HTTP User Agent
	+ D Pune	
		Retry Parameters
	Uttarakhand	Attempts* Timeout*
	North America	4 C [1-10] 2 C seconds [1-10]
		Username and Password
leerti Keshav	Groups (2)	Cancel Save & Turn SSID On

-	Search folders / Floors		Search for MMZ2 IP Addresse User Namer Device Name	💷 0 📾 1 📖 0 😻 16 🙆 104 🚺
	 Arista Cognitive WIR 	WiFi ~ SSID		More 🗄
DASHBOARD	El Staging Area	Changes will restart the	SID if it is on. The changes will affect all groups and folders a	sing this \$\$i0
MONITOR	• 🗀 India	← UPSK-Guests		
and the second s	• 🖾 Bengaluru	WLAN - Basic Security Network Access Control		
CONFIGURE	+ 🗀 Bannerghatta			
TROUBLESHOOT	🗀 Brookefield	RADIUS Settings		
INGAGE	+ 🗀 Hennur	RADIUS Pooling		
MAPS	🗁 Horamavu	🖉 RadSec		
REPORTS	🗄 🖾 Marathahalli	Primary Secondary		
SYSTEM 🖷	C3 YC	Authentication Server* Accounting Server*		
	• 🗁 Cochin	AGNI QA Cluster AGNI QA Cluster Additide	~	
	• 🖾 Dethi	AGNI Dev Cluster		
	GGN	AGNI Beta Cluster		
	C3 POY	AGNI QA Cluster ad HTTP User Agent		
	+ 🖾 Pune	KK, AGNI, QA, RADSEC		
	D PONE-HIN	WK System		
	🗀 Uttarakhand	*X Agni Dev Attempts* Timeout *		
	D North America		ands [1 - 10]	
		Username and Password		
Keerti Keshav	Groups (2)			Cancel Save Save & Turn SSID On

Figure 11-32: WiFi Access Control

3. Save and Turn ON the SSID Profile.

11.3.3 Onboarding the User

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

• The guest user scans the UPSK QR code and onboard to the AGNI network.

OR

· The guest user can use the UPSK received in the email.

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

11.4 Configuring Guest Portal Using Guestbook (Wireless)

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

11.4.1 Configuring the Portal on AGNI

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

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

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

Figure 11-33: Identity Guest Portals

ngni I					ତ ୭
MONITORNO		Guest Portals Manage the list of Quest Portals			+ Add Guest Portal
ACCESS CONTROL		Q Search by Name			
Networks Segments ACLs CENTRY Identity Provider User Clent Clent	*	ARISTA Outline on Internet Lagrande hard	0000		
ff Guest ff Users 문 Portais	Î	Default			
CONTIGURATION					
Access Devices Device Administration	*				
Certificates	*				
System	*				
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**.
- 4. Select Guestbook as the Authentication Type.

Figure 11-34: Configure Guest Portal - Guestbook

Ceshboard	New Template Outperior Genet Portal	(+ Bar
501 004740,	Configuration Customization	💿 Senect an element to update it's appendices.
Nelverks Engrants	Pers Nata	
ACLA	(Suntation Volt	
ldertity Novider	Cionage	
Chief v	Crgastanions/User Legis	
Guest	Cuerton	
t' Users	(hearpe	
Detais	No Linit *	(E)

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

• Device Limit - 4

Figure 11-35: Re-authenticate Guest Periodic

agni I	
MONITORING	Customize Guest Portal
V Sessions	Configuration Customization
Networks + + Segments	Portal Name
C ACLS	Cuestbook 🔕
 A Identity Provider User 	Authentication Guestbook
Client ~	Guest User Re Authentication Pariod
ff Guest ^	Periodic • 12 Hours •
Portals	4
CONFIGURATION	Cancel Add Quest Portal
<< Collapse Sidebar	

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

Figure 11-36: Device Validity

	Customize Guest Portal
CCESS CONTROL	Configuration Customization
Vetworks	Portal Name
ACLS	Authentication Types Ouestbook 😒
 Identity Provider User 	Authentication Guestbook
	8 Days •
* Users	Allow Self Registration Disabled
	Cancel Add Guest Portal

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 11-37: Customization Settings

Overtownes Dashboard		E New Te	mplate : Own! Portal		(+ I
Sessions		Configuration	Customization	O Select an element to update it's appearance.	
Networks Segments ACLs CNITY		Default		ARISTA	
Identity Provider User Client Count If Users Portals	5 5 6 6	Pagel Background Typ Background Imu Themis Color Text Color	Goobal Page Logo Togge Logo Form Terms Of Use and Privacy Policy Logo		
Access Devices Device Administration Certificates System El Audit Viewer Q License	* * *		Guest Overt Logis Somt Button Overnane Textos Parasoal Textos Overt Logis Italia Self Registration Self Registration	_	

Figure 11-38: Additional Customization Settings

igni I							
ONTORNS		New Template Customize Guest Portal					+
Dashboard		- Contrainty Construction					
· Sessions		Configuration Customization			Select an element to update it's appearance.		4
CESS CONTROL		Nete seguiri			See a second		
Networks		Default			No. of Concession, Name of		
Segments							
ACLS		based answerd			ARISTA		
ENDTY .		Page			Contrast Is any fee 20 A		
Identity Provider							
User	*	Background Type.	triage Color		taningkings	5	
Client	¥						
Guest	•	Background Image			00	<u>(</u>	
17 Users					000	C	
E Portals		Thome Color	#417980			100 C	
enoueation		Test Color	PEALACA				
Access Devices							
Device Administration		Form Color	x				
Certificates	2	Link Color	#125500				
System		Button Text Color	#77555				
E Audit Viewer		Button Border Radius					
C License							
Self-service Portal			Cancel	Add Guest Portal			
C RadSec Settings							
Support Logs							
System Events							

8. When done, click Add Guest Portal.

The portal gets listed in the portal listing.

Figure 11-39: Add Guest Portal

LATIT?	-	Guest Portals	
Savetity Provider		Manage the list of Guest Portain	+ Add Quest Partial Q Enail Settings
User			
Clevel	~ 9	Seach by Name	
Guest			
T Users		ARISTA	
D Portes			
Access Devices	× .		
Device Administration	. w	Portinet / 6 Ovied / 6	
	· .		
Certificates			
Certificates System	*		

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

Figure 11-40: Add or Import Guest

ດັງກິເ ເ			6 Ø 🕚
Sentend	-	Const Users Manage the fail of Genit Users	+ Add Owned or Import Owneds
A Brasilies		Althes Puter LPSK	
V Notworks		Q. Story (1 by Disersport, Engl., Approver, News or Diseasery	(
Contro Contro X Montry Provider		No dela to display	
1 User	~		
Ciert	8		
AT Guest	×1		
ft Users	1		
D Partals			

- **11.** Add a Guest user with the following settings:
 - Username guestuser1
 - Email guest@example.com
 - Portal AGNI Guestbook
 - Validity 8 Days
 - Device Limit 4



Figure 11-41: Guest User Settings

ONTORNO	Provide the following details to add a new guest user or upload a file to import guest users.	
Dashboard	- Back	
COSTS CONTROL	guestuser1	
Networks	Crist guest@example.com	
44 Segments	Anadronikeren	
ACLS SENTITY	AONI Questbook	*
A) Identity Provider	Valid Trans 28/03/2024 11:28 AM G 05/04/2024 11:28 AM G Valid ty: 8 Days	
Client V	Owner Live	
Guest ^	14	•
the Users		
Portals	Additional guest user information	~
ONFIGURATION		

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

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

The guest user is listed in the Portal User listing.

Figure 11-42: Added Guest

Desiderand		ħĩ		est Users age the list of O	wet Users				+ AN	i Guessi ar Import Guessi		O Seri	ángs
A Sessions		ALU	bers	Press	IP5K								1
• Networks		٩	Search	by therease, it	na), Azorowi, Naviw ar Car	sang							
ACLA				USERNAME	DMAL	QUEST APPROVER	TYPE	STATUS	ACTINATION DATE	EXPRATION DATE			
DENTEY			3	guestasert	ристроляри соп		Porol	English	20/03/0024 11:08:00	05/04/2024 11:201	20	1	0
A klentity Previder													
1 User	v												
Client													
ft Quest													
# Users	- 1												
18 Partala	- 1												

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

Figure 11-43: Edit System Generated Password

ONTORNO	Update Guest User				
Dashboard	NI View guest user details and update the selected guest user				
~ Sessions	, Unitare -				
CESS CONTROL	guestusert				
Networks					
4 Segments	Passet				
	••••••••••••••••••••••••••••••••••••••				
O ACLS	tra .				
INTER	guest@example.com				
 Identity Provider 					
User v	KAN Quertonia				
Client v	AND STOLENSON				
P Ouest	Changing portal will updated validity and device limit.				
	Vale from Vale for				
R Users	28/03/2024 11:28 AM				
1 Portals					
	Device land -				
FIGURATION	- <u>4</u> . *				

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

Figure 11-44: Export User Details

ດັ່ງົກຳ ເ										G	Ø	
Client	^	ħ		est Users	Svest Users				+ 444	Guest or Import Guests	0 See	ings
🛄 Clients		ALU		Pertor	ursk						C	
# Garat	•	212	Actions	Deter	Report				One Duest Part of	with current filter is selected.	Care	
ft them	1			USERNAME	EMAL	DUEST APPROVER	TYPE	STATUS	ACTIVATION DATE	EXPRATION DATE		
D Periols		-	5	(sestase)	propromption		Porte	Ensted	20/23/2024 11 28:00	05/54/2024 11.28:00	1	٥.

11.4.2 Configuring the Network

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

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

- 3. Select internal portal AGNI Guestbook
- f. Captive Portal
 - Internal Role for Portal Authentication portal-role

Figure 11-45: Add Network

S Contant	Add Network Product the following default to add a new following	1 ma
A Beating	and an and a second sec	
· Ingeneta	Conserve type (a) Women (C) West	
P Alla	Loss 100	
Card To	Data (Sect) .	
X sharing Provider	100 C C C C C C C C C C C C C C C C C C	
1 (her -		
Clerk 1	Admittatio	
C Dead	A Markator Tay	
(windows how	Cashin Nerie	
Access Institute 1	tamegotrijos 😸 Hane 🔘 briene	
Device Manimization -	Stratter for	
Cambuten V	#P#3seffex	· Pester
D Farture -		
(maxing)		
E Bullet	Capita Pana	
T Installed Agen	A Market State Advanced	
	para	

11.4.3 Configuring CV-CUE

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

11.4.3.1 Configuring Role Profile

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

- 1. Log in to CV-CUE and navigate to Configure > Network Profiles > Role Profile.
- 2. Add a Role Profile.
- 3. Add the Role Name as portal-role.
- 4. Click the Redirection check box and select Dynamic Redirection.

5. Keep other settings to default values.

Figure 11-46: Co	onfiguring	Role	Profile
------------------	------------	------	---------

Network Profiles - Role Profile
← portal-role
portal role
Role Specific Settings
2 VLAN ·
 ♥ VLAN ID ○ VLAN Name 0 - 40541
• Firewall
User Bandwidth Control
 Unit the maximum upited bandwidth per user to
C MBps V [1-1024]
Redirection
State Redirection
HTTPS Redirection
Certificate Information
Common Name Organization Organization Unit
www.arista.com Arista Networks Arista Networks
Websites That Can Be Accessed Before Authorization *
(lagiunicate/lexamilit,40 X) (askatura/astront/85.40 X)
autochinesaudiviet.85,443 X loginitier.com 83,443 X
spinetagring.net81.443 X

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 11-47: Guest SSID

WiFi ~	s	SID			
← Gues	t SSID				
WLAN ~	Basic	Security	Network	:	
Name					
SSID Name *					
Guest SSID					
Profile Name	e				
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 if required. Uncheck this option to use RADIUS.
- 7. Select the Authentication and Accounting servers.

```
Figure 11-48: Authentication and Accounting Servers
```

/iFi ∽ ssio	
Guest SSID	
LAN - Basic Security Network Access Control	
> Firewall	
Client Authentication	
Google imegration ③ RADIUS MAC Authentication	
ADIUS Settings	
) Radiec	
Primary Addisonal	
ithentication Server *	Accounting Server
radiez.iyontagnerg.net 🐱	radsecsystem.agnieng.ret 🗸
Send DHCP Options and HTTP User Agent	
tempts.*	Timoput *
4 C [1 - 10]	2 C seconds [1 - 10]
sername and Password	
Isername and Password	

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

You have created the **portal-role** role profile while configuring the Role Profile in the previous section. **Figure 11-49: Portal Role**

WiFi ~	1	SID									
← Gues	t SSID										
WLAN V	Basic	Security	Network	Access Control	:						
Accour	ting Sto	op Delay									
If Clent Autho			i.								
Role Ba											
INACIUS VS	4	Desigle OU	This setting	tis not editable beca	vse Olera	Austens	itation sia (Goople A	togration (s	disidika.	Charge Settings?
Rule Type *											
	elauk VSA		~							•	
Operand *				Assign Role *	Leones	~					
			- S]		24.7253.						
DHCP F	ingerpr	inting bas	sed Access	Control							
🗆 Bonjou	r Gatev	ray									
Redire	tion										
🗆 Wifi Cl	ients in	Allow List	t or Deny I	list							
Client	solation	n									

9. Save the settings and turn ON the SSID.

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

11.5 Configuring Guest Portal Using Guestbook-Host Approval (Wireless)

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

11.5.1 Configurations on AGNI

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

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

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

Figure 11-50: Identity Guest Portal

agni I							S	۲	•
MONTORNO		Guest Portals Manage the list of Quest Portals				+ Add Guest Portal)•	Email Se	ttings
ACCESS CONTROL	Q	L Search by Name .							
👳 Networks									
alla Segmenta									
@ ACLs			ARISTA						
XONTITY	_	ARISTA	Constant No angles Non MER						
(2) Identity Previder		transmin lain	(10.000)	$ \simeq$					
1 User	- 11 C	The red state	(terment	~					
Client	4			\mathcal{O}					
1 Overt		000	And in case of the second s	000					
T Users			0	2000					
🕀 Portals	De	etaat 🖉 🖉	test	/ 0					
CONTIQUEATION									
Access Devices	*								
C Device Administration	-								
Gertificates									
System									
CONCOURSE									
Explore									
😰 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 11-51: Configure Portal

agni I		Customize Guest Par	au)						s	(Back
Coshboard Sessions		Configuration Customic					Select an element to update it's appearance.		0 2)
P Networks • Segments • ACLs • ACLS		Parta hane Test-AGNI Automotion Types Overstook					ARISTA			
C Identity Provider	5 - 5	Authentication Oceant	000k					\bigcirc		
f Overs ff Users © Portals	*	Periodic Deveryori 4	-	No Authoritantian Parla 12	Hours •					
Access Devices	2				Cancel	Add Quest Portal				
Certificates System OnCOURSE	3 3									
Explore Distalled Apps										

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

7. Click the Update button.

Figure 11-52: Update Portal

agni				
MONITORING	4	st-AGNI tomize Guest Portal		
Sessions ACCESS CONTROL Networks	Portal Name Test-AGNI			
±∣± Segments	Authentication			*
E Identity Provider	Authentica	tion Guestbook		
Luser	v Default Validit	Days 🕶		
榾 Guest 榾 Users	Allow Self Re Approval req	gistration uired for guest access	Enabled =	
Portais	Authorized	ers by: 💿 User Groups 🔿 Email Domair	15	•]
Access Devices Device Administration Certificates	Customiz	e Guest User Fields		^
Concourse	Display	Field Label User Name		Mandatory
Installed Apps		Email		
	S S	Company		•
		Phone		0-
		Address		•
		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 11-53: Customize Portal

MONITORING	Customize Guest Portal	
CESS CONTROL	Configuration Customization	
Networks ± ± Segments	Default	*
O ACLS	Select element	
 Identity Provider User 	✓ Global	
Client	Y Login Form	
们 Guest 们 Users	 Login Toggle Logo Page 	
Portals CONFIGURATION	Terms of Use and Privacy Policy	
Access Devices	✓ Guest Guest Login Header	
 Device Administration Certificates 	Guest Login Submit Button	
CONCOURSE	User Name Textbox	
Explore Installed Apps	Self Registration Clickthrough	

9. When done, click Add Guest Portal.

The portal gets listed in the portal listing.

Figure 11-54: Guest Portal Added

ATTE	-	Guest Portals	
Martity Provider		Manage the list of Guest Portain	+ Add Guest Partial D Envel Settings
User	*		
Clevel	~ Q	Seach by Name	
Cornt			
T Users		ARITA	
D Portes			
PELANTON		0	2
Access Devices	× 1		23
Device Administration	·	Porestant / B	
Certificates	- LE		
System	*		

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 11-55: User Onboarding

At Institute State - Booligh (Bablic Tagling)					
New York State	i territori Territoria	Kasar Intel			
April .		Institution	Automatic and an		
seen.	100000000000000000000000000000000000000	i laurini la			
1 ~~	12 mil		-		
Minute Contract of	brankin.		No years		
• marine (1997)	a				
n Mar Frider Sang Palati	etter Santani ♥ Lucit Hitt Diploc Salt				
Nyak Research Mindowski	*	Intel Reports Articles			
		Specific and a service of the	ingen/woord. An experience of Laboration (State Config of The Source of Viewards) and the second second second		
		Annual Trickey Annual Trickey and a	Autoreactives 1		
Internative Neural Neural Networks			(****		

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

Figure	11-56:	Loain	Portal -	- Reaui	re Account
iguic		Login	i oitai	nequi	C AUGUUIII

ARISTA	\sim
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.	
	()

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

Figure 11-57: Create an Account

User Name	
Email	
Name	
Company	
Address	
Optional	
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	11-58:	Onboarded	User	Details
--------	--------	-----------	------	---------

An and a second s			have been		-
service for		Latertera	Loss & Autom	No. 404	
(agreen)		Sec	here but her	5440-104 P 10.014	
Laurent .		La anivelana de taxas	No. of Concession, Name		
8 teatras)	D	-	1 mm	
and the second se		Re-bein		1.000	
•	(Analy)	4	1.00	8 II.	
end (mine) A bene, since A		the basis ● basisti basisting			
hard Barren Strations			Start Ingene Statem		
			Name Of Trans		Automotive Strength Contraction and Automatics of
			Note 27 Second on Adams		
hand has in more . Balling to Band					(Berry)

11.6 Configuring Guest Portal Using Self Registration (Wireless)

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

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

11.6.1 Configuring the Portal on AGNI

To configure the portal, perform the following steps:

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



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

Figure 11-59: Guest Portal

agni I									¢	0	•
MONITORINO		Guest Por Manage the I	rtals list of Guest Portals					+ Add Guest Portal) 💿	Email Set	tings
ACCESS CONTROL V Networks 4/4 Segments ACLS DENTRY C Identity Provider		(Q. Search by Name	ARISTA Operators see	6							
± User ☐ Client AT Ouest AT Users ☐ Portais	~ ~	Default									
CONTIDURATION Access Devices Device Administration Continue Administration Continue Administration	* * *										
System Concounce 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**. Select **Guestbook** as the Authentication Type.
- 4. From the Authentication section, select the following settings for the guest user:
 - a. Re-authenticate Guest Periodic
 - b. Re-authentication Period 12 Hours

c. Device Limit - 4

Figure 11-60: Guest Portal Settings

09ni I		s o 🔹
Martana Santaset M Session	New Template Outprice Count Portal Outprice Count Portal Outprice Count Portal Outprice Count Portal Outprice Counterportage	🖉 Beneti O Senect an element to update its appearance.
X Notuentes X Unor Chors ✓ Chors ✓ Chors	Porte Nore Gambox © 1 × • Costrouge Costrouge Costrouge	
Poetas Coneccaston (Coneccaston Coneccaston	Nota (Jor Notalinit * Carcol Add Quark Particle	

Figure 11-61: Guest Portal Settings

Dashboard	Customize Guest Portal
Sessions	Configuration Customization
Networks I Segments	Portal Name
ACLS	Authentication Types Guestbook 3
 A) Identity Provider LUser 	Authentication Guestbook
🗋 Client 🗸 🗸	Guest User Re-authenticate Guest Re-Authentication Period
에 Guest ^	Periodic * 12 Hours *
Portals	4 *

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

- e. Address
- f. Notes

Figure 11-62: Guest Portal User Fields

àgni				
E Destinord	Cashorder D			
~ Sessions	Configuration	Sustantiaetion		
ACCASE CONTROL	- Portal factor			
· Activistia	ASN Exection			
via Segnents	Automaticana Span			
A AGLA	Querticos O			•]
Control Previder				
1 Unit A	Autoritation	Garothers		
	Delice Server			
± vers	1	Days •		
site User Droups	Alon Self Reponsion		Entrol	
Cieri *	Approver Insurant for		(burned O-	
Clarks	ADDARE INCOME.	per scen	(and C	
Chert Druge	Customize Quest &	har Ficility		^
C Out -	Distant	Ferziste		Mandatory
	22	Quer Norte		-•
S. Creek		200		
C Portica		Crost		
CONTRACTOR		Farte		-•
Access Devices				
Device Administration 🗸	-	Conquiry		
Certificates V	0	Pore		
C] System				
II Capitore		Abbens		
	•	Pacies		
[7 Installed Appn				

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

- 6. Click the **Customization** tab to customize the portal settings:
 - a. Theme template
 - 1. Default
 - 2. Split Screen
 - b. Select element
 - 1. Global
 - a. Page
 - b. Login Toggle
 - c. Terms of Use and Privacy Policy
 - d. Logo
 - 2. Guest
 - a. Guest Login Submit Button
 - b. User Name Text box
 - c. Password Text box
 - d. Guest Login Header
 - e. Guest Login Form
 - f. Self Registration

g. Clickthrough

Figure	11-63:	Guest	Portal	Customize
--------	--------	-------	--------	-----------

agni I		
MONITORING	Configuration	
 Networks Lis Segments ACLs 	Default	•
IDENTITY (2) Identity Provider 2 User	Page Global	<u>`</u>
Client ff Guest	Login Toggle Logo	-11
☆ Users ② Portals	Page Terms of Use and Privacy Policy Guest	
CONFIGURATION	Guest Login Form Cuest Login Visador	

Figure 11-64: Guest Portal Customize

agni I	
DENTITY (*) Identity Provider * User Client 했 Guest 양 Users (*) Portals	AGNI Guestbook Customize Guest Portal Configuration Theme template Default
CONFIGURATION Access Devices Device Administration Certificates System CONCOURSE Explore Explore System Concourse Concourse Conc	 Guest Guest Login Form Guest Login Header Guest Login Submit Button Password Textbox User Name Textbox Self Registration Clickthrough

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

Figure 11-65: Guest Portal Added

ngni I				& @ 🤇
X Savetty Provider		۲	Guest Portals Marage the list of Guest Portals	+ Add Guest Partial (Creal Settings
1 User				
Circl	-	9	earch by Name	
ST Cornt	~			
T Users			AMINTA	
Directors	1			
Access Devices	÷.		00	
Device Administration	÷.	4.14		
Cartificates	*		Desiliant 10	
G System	4			
00400.#38				
II Capiere				
17 Installed Apps				

11.6.2 Configuring the Network

For details, see the <u>Configuring the Network</u> 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 11-66: Identity Guest Portals

agni I				6	0	-
MONTOING		Guest Portals Manage the fat of Guest Portals	+ Add Overst Po	•	Q Enails	ettings
Sessions Access control Networks	٩	Stephing Stephing -				
Lis Segments ACLs DENTITY (2) Identity Provider 1 User Client						
ff Guest ff Users © Portals	A De					
CONTINUEATION Access Devices Device Administration	•					
Concounts Explore Exp	•					

2. Click the Add Guest Portal button.

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

Figure 11-67: Configure Portal

agni I						6	0
MONITORING		New Te Customize	mplate • Guest Portal				(* Back
CONSTRUCTION		Configuration	Customization		Select an element to update it's oppearance.		
P Networks		forst term Ounst-wired			ARISTA	1	
DENTITY		Cickthrough ()	6	× *	Canadi tu appo faz (6.6)		
L'Identity Provider	•	Authentication	ClickStrough Organizational User Logn				
Client Client Guest	*	Always	Guestibook		00		
17 Users				Cancel Add Guest Portal	<i>∩∩∩</i>		
Access Devices							
Device Administration							
Certificates							
3 System	аў.						
Explore Distalled Apps							

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

Figure 11-68: Customize Portal

agni I						(6	0 🕑	
MONTOINS		Customize Overst Portal						(* Back	D
ACCESS CONTROL		Configuration Outcomization			Select an element to update its appearance.		Z		
V Networks		Default		*					
O ACLS		have even							
 Adentity Provider User Client 	× ,	Background Type:	🛞 smaga 🔘 Color						
f Guest	~	Background Image			001				
🕂 Users 🔁 Portais		Theme Color Text Color	#417900 #44.64.64			μ			
Access Devices		Form Color	ariiiii						
Device Administration Gertificates	*	Link Color							
System concourse	. w	Button Text Color Button Border Radius		<u></u>					
Explore B Installed Apps				Cancel Add Ouest Portal					

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

Figure 11-69: Add Guest Portal

MONITORING	2	Guest Portals Manage the list of Guest Portals			
✓ Sessions					
ACCESS CONTROL	٩	Search by Name			
Networks					
: Segments					
ACLS		ARISTA			ARISTA
L) Identity Provider		Organization Login			Connect to enjoy free Wi-Fi
User	~	true and attres	~		Convert An appropriate and and the forme Of Line.
Client	×	Re repting in you arrange the Terrer CP case.	\mathcal{S}		\mathcal{C}
P Guest	^		000		00
分 Users			7000		$- \alpha \alpha \alpha$
Portals	Def:	ault	10	Guest-wired	10

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

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

Figure 11-70: Copy URL

agni I		
MONITORING	Suest-wired Provide the following details to update the selected Network	← Back :
CESS CONTROL	Guest-wired	
Networks als Segments	Connection Type: O Wireless Wired	
ACLS	Access Device Group	- 🕀
 identity Provider User 	Select an Access Device Droup to make this Network applicable only to a subset of Access Devices. Multiple Networks can't be linked to the same Al Status: Enabled end	cess Device Group.
Client	Authentication	
ff Guest ff Users 回 Portals	Automotive Portal	•
CONFIGURATION	Captive portal type: internal External Select Internal	
Access Devices Device Administration	Test-AGNI-Docs	Preview
 Certificates System 	Captive Portal	
CONCOURSE	initial ACL For Fortal Authentication . guest-act	Show Domains
88 - COM	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	Copy
		Cancel Update Network

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 <u>document</u>.

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 CONDOURATION () 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 l			ଓ ଡ 🕒
ACLS	at-aruba-ap Provide the following details to update the selected Device	← Back	
(2) Identity Provider	At-aruba-ap		
1 User			
	Mic Assess a6:bd/27:c5:a8:a2		
Access Devices	Verdor		
Devices	Aruba	*]	
🗁 Device Groups	C Seriel Number		
Cloud Gateways			
Device Administration	IP Address		
E 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		
System Events			
CONCOURSE	You can generate a RadSec client certificate for this Access Device.	Client Certificate	
III 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		ଓ 💿 🕒
O ACLS	Generate RadSec Client Certificate Fill in the details to generate RadSec client certificate for the Access Device	
 identity Provider User ~ Client ~ 	Generate Certificate: Generate Generate Generate Guse CSR (Single Device) Upload Zip with multiple CSRs Access Device	
CONSIDURATION Access Devices Devices	Password	
Device Groups Cloud Gateways Device Administration ~	DNS Names	
Certificates System Audit Viewer	Cptional, specify DNS Names one per line Cancel Generate Certificate	
License 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

		¢	0	
ACLs DENTITY	at-aruba-ap Provide the following details to update the selected Device			
 Identity Provider User 	Arranda			
	also			
 Access Devices ^ Devices Device Groups Cloud Gateways 	Anba v			
Device Administration Access Policy	PASSess			
TACACS+ Profiles	Access Device Group - 💿			
🖶 Certificates 🗸 👻	Outonal			
System ^	Location			
Audit Viewer Q License Portal Settings	Optional, example: OutbatthemicalCalifornia/Stan1 RadSec Connection Status: Not Connected			
RadSec Settings Support Logs	You can generate a RadSec client certificate for this Access Device. Get Client Certificate			
CONCOURSE	Cancel Update Device			
Explore	RadSec Connection Logs Show Lops			

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.

	Trusted Certificates							
Dashboard	Details of the Certificate Authorities trust	d by Arista CloudVision AGNI			+ Add Certificate		Set	ttings
Sessions ACCESS CONTROL	All Certificates Internal External						C	3 28
Networks Ali Segments	Q Search by Subject or Issuer details							
@ ACLs	# SUBJECT			TYPE	VALIDITY			
IDENTITY	1 CN+AONI, Issuer CA, O+atulacme			Internal	30/06/2026	*	0	0
 A Identity Provider User ~ 	2 CN=AGNI, Root CA, O=atulacme	Certificate Settings		Internal	30/06/2033	ŧ	0	0
🛄 Client 🗸	3 CN=AntaraAl Intermediate CA, OU=Antara	View expiry settings for all Internal certificates,		External	20/03/2032	<u>+</u>	1	8
CONFIGURATION	4 CN=AntaraAl Root CA, OU=AntaraAl Certif	Client Certificate (EAP-TLS) Validity:	1 year	External	17/03/2042	ŧ	1	8
Device Administration	5 CN=Example Certificate Authority, O=Exar	Server Certificate Validity:	3 years	External	26/04/2024	*	1	
Certificates ^	6 CN+External Certificate Authority, O+Exan	Issuer Certificate Validity:	5 years	External	23/06/2024	±	1	٥
Trusted	7 CN=External1 Certificate Authority, O=Exa	Root Certificate Validity:	10 years	External	15/07/2024	*	1	٥
System ~ CONCOURSE	8 CN+agni_scale_ca, O=Arista Networks, L=	_	Close	External	16/07/2033	ŧ	1	0
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						6 Ø (
MONITORING			Access Device Grou			+ Add Access Device Grou
CCESS CONTROL						
Vetworks		٩	Search by Name			
ACLS		*	NAME	DESCRIPTION	UPDATE TIME	
DENTITY		1	AT-WIRED-CP		10/09/2023 22:58:59	/ 1
 Identity Provider User 		2	AT-WIRED-EAP		17/11/2023 01:12:57	/ 0
	~	3	AT-WIRED-MBA	AT-WIRED-MBA	12/09/2023 23:10:24	/ 0
ONFIGURATION		4	Imported	Imported	06/12/2023 05:33:55	/ (
Access Devices	^	5	Systest-Kaveen	LLDP VSA in Accounting	14/09/2023 21:50:06	/ 0
📄 Device Groups	1					
Cloud Gateways						
Device Administration	~					
Gertificates	~					
	×					
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

			د. د	0	
AcLs Control Contro Control Control Control Control Contr	Add Access Device Group Provide the following details to add a new Access Device Group Test Test Test Test Test Test Test Test	e bok			
Controlation C	Access Devices Available Devices Assigned Devices Q: Greach by Name, MAC Address or Location				
 Access Policy TACACS* Profiles Certificates System 	 a8bd22c45a8a2 a1-arcbi-ap d420cb831b8f d420cb831b8f 	(Reference () + Ann + Ann			
 Audit Viewer License Portal Settings RadSec Settings 	d420b041879f Jun-AP-Office 30x82x402bb49f Aut-C200 28x714cxx0f4b	+ AM + AM			
SupportLogs System Events CONCOURSE Explore	at-arista2006 arbbice different arbbice different constraints constraint	+ A65			
Installed Apps		Cancel Add Access Device Group			

Overview - TACACS Plus with AGNI

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

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

13.1 Configuring TACACS Plus on Arista Switches

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

```
conf terminal
tacacs-server policy unknown-mandatory-attribute ignore
tacacs-server host <IP ACG> key <shared secret>
```



튭

Note: The shared_secret should be the same shared secret provided while adding the Arista Cloud Gateway on AGNI.

```
aaa group server tacacs+ agni-tacacs
server <IP ACG>
```

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

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

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

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

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

13.2 Enabling Device Administration on AGNI

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

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

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



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

Figure 13-1: Device Administration Enabled with Passphrase Validity

ni l			6 Ø 🖉
MONITORING		Device Administration Device Administration Policies using RADIUS / TACACS+	Device Administration Portal
ACCESS CONTROL		Enable device administration: Enabled	
Networks Lis Segments ACLs		Amount for an and the second s	-
(1) Identity Provider			
LUser Client	> > >	Q. Soarch by policy warms or description	
CONFIGURATION			
Access Devices Device Administration	~	Te Add Policy	
🐔 Access Policy			
C TACACS+ Profiles		II v TacacsProfile-PaloAtto	1
System	~	II v agnipim TACACS+ 🖌 🖸	1
Ⅲ Explore Ⅳ Installed Apps		Allow Access	I

13.3 Configuring TACACS Plus on AGNI

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

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

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

Figure 13-2:	TACACS+	Profile	Creation
--------------	---------	---------	----------

Provide the following details to update the selected TACACS+ Profile			+ Back
Tacacsiyofie			
Description			
Printip last			
Mow Enable (Privileged Shell Access): Traitied			
ervices and Attributes			
ust of selected Services and its Attributes.			Add Service Attribute
# NAME			
1 shall			1 1
ou may add a new TACACS+ Service dictionary, if needed.			Add TACACS+ Service Dictionary
ommands			0
ction for unmatched commands.			Add Command
# DOMMAND			
1 show			/ 1
Deny Arguments neming-contg	Permit Arguments:	Unmatched Arguments: Dany	
Note : Changes will be saved once you click on update.			
			Cancel Update TACACS+ Profile

Figure 13-3: Adding TACACS+ Access Policy

Device Administration Device Administration Policies using RADIUS / TACACS+			Device Administration Portal
Packing checke administration Packing campaigned Packing campai	Update	Add Policy Provide the following details to add a new policy New Access Policy Description Policy Type:	× ×
 Sauch sy body have an electropic By, Add Publicy CVP Admin 	TACACS+	Statur (Inside) e Conditions Unitoritis Aut User: Onco is Switch Admin Local	X Pa. Add Condition
Switch Admin TACACS	TACACS+	Actions	-+ Apa Usharuun
Switch Admin TK Switch Operator TACACS	TACACS+	TACACS+ TACACS profile O TACACSHotile Teacofhotile O	×
✓ Switch Admin Radius	RADUS /		The Add Action
✓ Swicth Operator Radius	RADIUS /		Cancel Add Pelicy
✓ Default			

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

Figure 13-4: Creating TACACS+ Policy Details

vide the following details to add a new policy	2 ×
me . ccessPolicy	
escription	
olicy Type: TACACS+ RADIUS	
tatus: Enabled	
onditions MATCHES ALL	
Access Device: IP in 10.81.204.0/26	×
	≓+ Add Condition
ctions	
TACACS+ TACACS profile	×
TACACSProfile TacacsProfile	×
TACACS+ TACACS profile	× ≡+ Add Action

	v policy	×
ame accessPolicy		
escription		
Policy Type: 🔘 TACACS+ 🔘 RAD	olus	
Unoy type. Inchost O Mil	200	
Status: Enabled		
onditions MATCHES ALL		
onditions monority are		
CloudGateway: Location contains	1	×
	HQ	=+ Add Condition
	San Jose 🗸	-+ Add condition
Actions		
Actions		
Actions TACACS+ TACACS profile		×
TACACS+ TACACS profile	TacacsProfile	×
TACACS+ TACACS profile	TacacsProfile	×
TACACS+ TACACS profile	TacacsProfile	×
TACACS+ TACACS profile	TacacsProfile	≍ ∓+ Add Action

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

13.4 Monitoring TACACS Plus on AGNI

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

Figure 13-6: Monitoring Session Details

Session Details - TcInm60c88nsc72qekc50 Details for Session				← Back	ē
Authentication Request	Success	Request Details			
Authentication Type	TACACS+	NAS IP Address		10.81.204.5	
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 - 10.81.204.7 San Jose		
Input Request Attributes	×	Output Response Attributes		v	
TACACS+ Activity				Show Activity	
Session logs for request: TcInm60c88nsc72qekc50				Show Logs	

Figure 13-7: Monitoring TACACS+ Session Details

User	Enabled	Access Device		Cloud Gateway	Connected
un run		Not available		CloudGateway - 10.81.204.7 San Jose	
aut Request Attributes			Output Response Attribu	stes	~
ACACS:AuthnPrivLevel		1			
ACACS:AuthnService		Login			
ACACS: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	
¥ 3		Permit		05/12/2023 23-20-59	

13.5 Accessing Device Admin Portal on AGNI

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

Figure 13-8: Device Admin Portal

Dashboard		Your trial license will expire in 251 day(s).		
 Sessions CESS CONTROL 		C Device Administration Device Administration Policies using RADIUS / TACACS+		Device Administration Poe
P Networks				
segments		Enable device administration: Enabled		
ACLS		Automatitier Solas Pattorn Engineering 🔕 Switch Admin Local 🚱 +2 Solect Authorized User Groups		
Identity Provider				
User	*		Update	
Client	~			
NEIGURATION		Q Search by policy name or description		
Access Devices	1	assects by banch use at description		
Devices				

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 Device OS				
Apple Mac				r
Follow the given steps to in	stall the DeviceAdmin	application:		
1. Download the DeviceA	dmin application for yo	ur client.		
2. Install the application	and allow it to run in the	e background.		
3. When prompted, give	permissions for the app	plication to accept incoming	connections.	
4. In the Self-Service Po	rtal, add the Access De	vice in the Devices UI.		
5. Click the 'Connect' ice	on for the device to laur	ich the SSH session.		

Figure 13-9: Device Admin Application for Mac OS

Figure 13-10: Device Admin Application for Windows

Your Client Device OS Microsoft Window	S			*	
and at 199					
Apple Mac					
Microsoft Windo	9WS				
2. Install the appl	cation and allow it to ru	in in the background.			
3. When prompte	d, give permissions for	the application to accept	incoming connections.		
4. In the Self-Ser	vice Portal, add the Acc	ess Device in the Devices	s UI.		
5. Click the 'Conr	ect' icon for the device	to launch the SSH sessio	on.		

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

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

=

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

Note: The Device Login Credentials work for days or even months without expiry as determined by the duration allowed by the administrator.

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

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

Figure 13-11: Device Admin Portal

Ξ,

pe Portal	•
Device Login Credentials	
View device login credentials	
Use device login credentials in external terminals to access	
devices securely.	
Login Username	
operated	
Click to generate a device login password.	
	Device Login Credentials View device login credentials Use device login credentials in external terminals to access devices securely. Login Usemane operatol

Figure 13-12: Device Login Credentials

agni Self-Service	e Portal	•
D Manage Clients	Device Login Credentials	
19 Register Client	View device login credentials	
😐 Wi-Fi Passphrase		
DEVICE ADMINISTRATION	Use device login credentials in external terminals to access	
Devices	devices securely.	
🗘 Setup	Login Usemane	
😐 Login Credentials	operator	
GUESTS		
∱ [™] Users	Your device login password will expire on 06/02/2025 14:59. Copy and Save the generated password; it will not be displayed later. Login Password Copy Password Copy Copy and Save the generated password; it will not be displayed later. Copy Password Copy Password <td></td>	

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

Figure 13-13: TACACS+ Authorization Allowed and Denied Output

🚰 login as: shrirang@agniplm.onmicrosoft.com Keyboard-interactive authentication prompts from server: | Password: End of keyboard-interactive prompts from server Last login: Tue Feb 6 16:56:22 2024 from 10.86.28.96 IN-MH04-PL-SW04#show interfaces status % Authorization denied for command 'show interfaces status' IN-MH04-PL-SW04#show running-config % Authorization denied for command 'show running-config' IN-MH04-PL-SW04#show version Arista CCS-710P-16P Hardware version: 11.04 Serial number: WTW23230216 Hardware MAC address: 2cdd.e9f6.cd13 System MAC address: 2cdd.e9f6.cd13 Software image version: 4.30.4M Architecture: 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#

System

This section captures the administrative tasks at the system level.

14.1 Audit Viewer

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

Very trial license will every in 254 dayle)				
Tour that icense will expire in 354 day(s).				
List of audit records				
All Actions Insert Update Delete				
Q Search by Name or User				Type Any
A # NAME	TYPE	ACTION	USER / API TOKEN	DATE & TIME
∧ 1 Mac auth clients	Client Group	Update	bobby.flay@testorg1.com	7/24/2023 13:37:25
Details				
Name	Description	Group U-PS	ĸ	Allowed Networks
Mac auth clients		Disabled	Enabled	All Networks
1				
A 2 ACME-CORP	Network	Update	bobby.flay@testorg1.com	7/24/2023 11:22:11
Details				
Name	Connection Type	SSID		Authentication Type
ACME-CORP	Wireless	ACME-Corp		Client Certificate
Trust External Certificates	Onboarding	Status		
Enabled	Enabled	Enabled		
✓ 3 test	Client Group	Insert	bobby.flay@testorg1.com	7/24/2023 09:16:4
	List of sudit records All Actions Insert Update Delete Q. Stearch by Name or User A # NAME A 1 Mac auth clients Details Name Mac auth clients Add Actions Add Acti	Audit Viewer Ust of audit records Al Action Insert Update Delete Search by Name or User Image: Search by Name or User Image: NAME TVPE Image: Name Description Mace auth clients Client Group Details Description Mace auth clients Description Mace auth clients Description Mare Connection Type ACME-CORP Wineless Trust External Certificates Onbearding	Audit Viewer List of audit records All Actions Insert Update Delete Search by Name or User Image: Search by Name or User	Audit Viewer List of audit records Af Actions Insert Update Delete Search by Name or User * NAME TYPE * NAME TYPE * NAME TYPE * NAME TYPE * NAME Client Group Update bobby/fay@testorg1.com Details DisabledEnabled * 2 ACME-CORP Network Update bobby/fay@testorg1.com Details Connection Type SSID ACME-CORP Wireless ACME-Corp Trust External Certificates Onboarding Status

14.2 Self-Service Portal Settings

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

ngni I	j,								¢.	େ ଡ
Dashboard		Customize Self-service P						🔘 Salt-service	Salf-service Portal	🕑 Self-Service Portal 🖉 🗘 Se
Sessions		Theme Settings			ſ	CON PAGE LANDING PAGE				
P Networks		Parts News Self Service Portal								
ACLS		Header Background	#326297				agni i setsevertere			
1) Identity Provider		Thome	#326297				Signin Garti d Inal			
Client	*	Logo	Add				C round	Prosent Control of Con	Prosent	Head and a second se
	*	Login Page Settings								
Access Devices Device Administration	> >	Background Image Form Color	Add #F30000							
Certificates	× <	Userserv Later UserID or Email								
Audit Viewer		Terms of Use								
Self-service Portal RadSec Settings	1	Additional Information for Users		Disables						
 Support Logs System Events 			al information for Self-service Portal users.							
CONCOURSE Explore			Default	Reset						

Figure 14-1: Self-Service Portal

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

• Click the **Settings** button at the top right of the Self-Service Portal screen.

• In the Manage Self-service Portal Settings pop-up window, add the user groups that you want to provide with read-only access. By default, all user groups have read-write access to the portal.

Figure 14-2: Manage Self-Service Portal Settings

Dashboard	Your trial license expires in 11 day(s).				×
Sessions CESS CONTROL	Self-service Portal Customize Self-service Portal				C Self-service Portal
Networks Segments	Theme Settings		LOGIN PAGE LANDING PAG	O 0	
CLS ITTY	Pora Fane Self Service Portal			QQAI : setSenseAura	
Identity Provider User ~	Header Background	#326297 Manage Self-service Portal Settings		Spain	
ient v	Theme	Read-only User Groups		Gard a Dea	
CONTRACTION CONTRACTION	Logo	Add These uses will not be allowed to register clients. However, they will be	allowed to onboard their clients,	- Passed	
Device Administration 🔍 Certificates 🗸	Background Image	Add Restricted Onboard Users () Scient			
ystem v	Form Color Unemana Label				
plore stalled Apps	UserID or Email		Cancel Update		
	Terms of Use				
	Additional Information for Users	(Dashled)			
	Enable to include additional informat	tion for Self-service Portal users.			
		Default Reset Update			

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

portal or APIs (see image).

E

Manage Clients Wi-Fi Passphrase	Clients Manage the lat of clients as on 62,07(2	024 13 IN OF					
							a :
	Q. Search by MAC address or participants					Ary	
	* WAC ADDRESS	DESCRIPTION	(MINER (1/518)	\$127.45	VPOATS TIME		
	1	Keert's Mac OS X	Kaw1	Brathed	02/07/0524 11 53 51		•
	2 bleasticidd ee ff		Kawis	Enabled	010339234 22:30:35		
	3 ++ 5133.1576.M	Kent's Andruid	Ket	Enabled	2504/2024 15 15:58		•

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

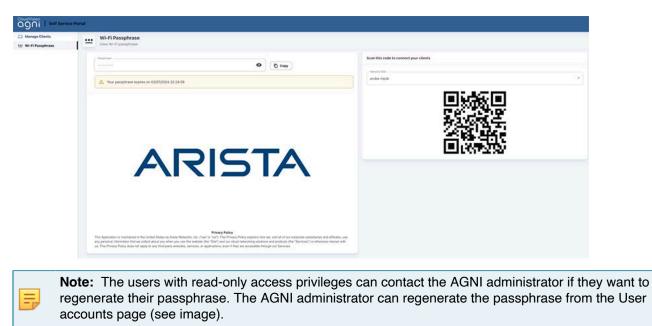


Figure 14-4: Self-Service Portal WiFi Passphrase (client with Read-only access)

Figure 14-5: User Account Details with Regenerate Passphrase option

agni I					6 0 C
Scontonie 11 Centreard		Keerti Vern vaar ohdals and optide the selected vaer		é fack I	
ACCESS CONTROL		(1999)			
V Networks		Aut			
als Segments		The first of the second			
DENTITY .		, the feature			
(i) identity Provider			C Copy Regarante		
1. When	12				
± Users		New paragetrase is generated. EXX Update to use this paraghtesis for any future regionations.			
III. User Drouds		Status (Facine)			
Ciere					
Clienta		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					
Q Radioc Settings					
Support Lega					
E Fystern Events					
CONCOURSE					
II Explore					
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).

ର୍ଗ୍ୱମାଁ ।		
MONTORNS	Self-service Portal Outformize Self-service Portal	
ACCESS CONTROL	Theme Settings	
P Networks	Ford Name Self Service Portal	
@ ACLS	Header Background #326297	
 Meetiky Provider User 	Theme #326207	
Client v Guest v	Login Page Settings	
Access Devices	Background Image Add	
Device Administration V Certificates V System A	Form Color User/Doc Provide User/D or Emel	
Audit Viewer License	Terms of Use	
Salf-service Portal		
RadSec Settings SupportLogs	Additional Information for Users The following details will be displayed after onboarding is successful.	Enabled
E System Events		
DACOURSE	ARISTA	
Explore Filestalled Apps	Procedure and the control of the con	ed about you when you use this invite interact with us. This Privacy.
	Additionally, show in user's W-FI Passphrace page Trusted	
		Default Reset Update

Figure 14-6: Self-Service Portal Settings – Additional Details

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

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

Manage Clients		Wi-Fi Passphrase				
Register Client Wi-fi Passphrase Out 515	1	Der Desp	-		Scan this code to connect your clients	
Users		Paragress	۲	Copy	terun till Minagskauth	-
		This is your passphrase. Click Regenerate to create a new passphrase.	ne passpfirase if needed.			
		ARISTA Privey Policy This Application is mantained in the United States by Arata Tatworks, in				
		This Application is manifested in the United States by Annia Networks, to baced annia and attainate, use why personal information that are collect at solutions and products (the "Services") or otherwise interact with us. This applications, even if they are accessible through our Services.	bout you when you use this w	eballe (the "Site") and our cloud releasing		



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

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



14.3 RadSec Settings

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

Figure 14-10: RadSec Settings

			6 Ø
Dashboard	٥	RadSec Settings View RadSec Settings	📮 Get Client Certificat
CESS CONTROL	RadS	ec Server	
Networks	RadSec Server Historiame		radsec.ga.agnieng.net
ACLS	0	Use the above server as RadSec(TLS) RADIUS server in your Network Access Devices.	
Identity Provider	RadS	re CA Certificate	Expires on 6/4/203
LUser v	Sub	eet DN	CNHISRG Root X1, Owinternet Security Research Group, CHUS
NEIGURATION	Issu	er DN	CN#ISRG Root X1, OwInternet Security Research Group, C#US
Access Devices v Certificates	0	Use this CA certificate to validate the RadSec(TLS) server certificate.	
🖵 Trusted			
System ^	-		
Audit Viewer			
Q License			
Portal Settings			
C RadSec Settings	1		

14.4 Support Logs

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

Ogni | Testorg . 11 Support Logs 1 Dashbo ~ Sessions - Debug Local ACCESS CONTRO P Networks Reset Refresh Lis Segments ACLs Support log entries Des 7/24/2023 17:02:04.356 DENTITY 0 (1) Identity Provider 7/24/2023 17:02:04.351 INTO {t=Rbs61d189=s361-4837-a116-182575420cfb api8eq13=APICIVEIV542GL572G04580} /api/session.actions.get [8.118634ms] 7/24/2023 17:02:04.378 INFO [t=%De61d199=#361=4837=#116=182575420cfb spiRegID=APICIV#1V5426L87204N6V0] /spi/se saion.get [35.729421ma] 1 User 7/24/2023 17:02:04.477 INFO [t=Ebs61d189=e)61-4837=a116-182575420eFb apilegID=APICTYRIV5Q25/2708F30] /api/session.details.get [16.618934es] Client 0 7/14/2011 17:07:04.479 ERROR (ap)Reg15-APICIVE/V52007172998710 t-Ehadid195-e041-4837-e116-192575420ctb) /api/identity.client.opt err=0bject.not.found (5.647852ee) 7/24/2023 17102104.480 1900 [t=Rba61d189=m361=4837=s116=182575420ctb api8egID=APICTV81V5420L672004586] /api/contig.mad.get [5.537296ms] Access Devices 7/24/2023 17:02:04.481 INFO [t=Rba61d189-e361-4837-e116-182575420cfb apiRegID=APICTV81V5420L57204N705] /api/config.metwork.get [6.85240]ms G Certificates 7/24/2023 17102:04.481 INTO [t=Rba51d189=e361=4837=a114=182575420eTb apiXegID=APICTVMIV5420L072268700] /api/session.actions.get [7.068959ns] System 7/24/2023 17:02:06.495 1900 (t+Ebs61d189-e361-4837-a116-182575420cfb apiReg1D+AFICIV81V0g79.1572F88F40) /api/session.log (795.043774ms) 7/24/2023 17:02:22.454 1800 (apiReg10+ADICIVH2350382972058940 t=Eba61d189-e361-4837-a116-182575420cfb) /api/config.network.list [7.884107ms] E Audit Viewer 7/24/2023 17:02:22.945 1HF0 [apiReqID+AFICIVH23L42015720048C0 t=Eba61d189-e361-4837-a116-182575420cfb] /api/config.network.list [9.106400 Q License 7/24/2023 17102:29.182 INFO [apiRegID=APICIV8250420L522088710 t=Eba61d189=e341-4837-a114-182575520cfb] /api/config.entity.refer es.get [13.164089ms] Portal Settings 7/24/2023 17:02:30.376 INPO (t=Rbe61d189=e361=4037=a116=182575420cfb) config = delete network[id=172 name= suid=] A RadSec Settings 7/24/2023 17:02:30.374 INFO (t=Rbaild189=e361=4837=e116=182575420efb apiRegID=AFFCIV8251Q78251Q782572F88750) /api/config.metwork.delete (29:401428ms) Support Logs 3/24/2023 17102:30.498 INPO [t=Eba61d189=e361=4837=s116=18257542/bcfb apiXed1D=APICTV825LQJRJ572P88F5G] /api/config.network.list [11.235125ms] 7/24/2031 17:02:02.00 TESSE [apling19-03101V028L20L372004000 t=fhaild18-e361-0031-0114-105754306(h) /apl/metvice.log er=math_failed: 1 arror occurrent + invalid_input_or validate mession for appLMDI1] [1:04017mm] System Events 0 7/24/2023 17(02)55.546 INPO [issReqID=IAMcivh2bt42gis72g44egg t=Ebat1d189-e161-4837-a116-1825754200fb] iss[iogin] - prelogin completed for appURL=/launchpad done 7/24/2023 17102156.210 INFO [ianheqID=TAMeivh2bs42g1#72qd4egg t=Eba61d189=#361=4837=#116=182575420erb] ian(login) = init 830 III Explore

Figure 14-11: Support Logs

14.5 System Events

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

Dashboard		O Your trial license will expire in 354 day(s).						
Sessions	F	System Events List of system events						
Networks Segments	-	Error Warning Info						
ACLS	٩	Search			(^T ipe			
Identity Provider		TYPE	MESSAGE	LEVEL	DATE			
User v	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			
Access Devices	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 v	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	Info	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			
C 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	into	7/24/2023 18:01:00			
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			
NCOURSE	12	Identity Provider Sync	onelogin(onelogin) - starting IDP Sync	Info	7/24/2023 17:29:00			

Figure 14-12: System Events

14.6 Notification Settings

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

14.6.1 Configure Email Settings

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

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

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

- d. Password
- e. From email
- f. Choose the Connection Security as None, SSL, or Start TLS.
- g. Enter the Port number
- h. Enter the Connection Timeout in seconds.
- 4. Click the Add button to add the SMTP server.

Figure 14-13: Notification Settings- Email Settings

agni onPrem-		ଓ ଡ 💽
ACCESS CONTROL Networks	Notification Settings Choose the type of notification you want to update. Email Templates	
-II Segments		
ACLS	Email Settings SMS Gateways	
IDENTITY	Sender Name	
(a) Identity Provider	AGNI	
💄 User 🗸 🗸	SMIP Server	
🛄 Client 🗸 🗸	smtp.abc.com	
* Guest v		
CONFIGURATION	Username IT@abc.com	
Access Devices	11@abc.com	
Device Administration	Patiword	
Certificates	From email	
System ^	no-reply@abc.com	
Audit Viewer	Connection Security	
Q License	SSL *	
Self-service Portal	Port	
RadSec Settings	465	
Support Logs	Connection Timeout (second)	
System Events	15	
A Notification Settings	Update	
🛠 Collapse Sidebar		

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

- 5. Click the Send Test Email down-arrow and enter the following details:
 - a. Email address of the recipient.
 - **b.** Subject of the email.
 - c. Email message.
 - **d.** Click **Send Email** button to send the email. An email sent successfully message is displayed at the top right corner of the page.

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

Figure 14-14: Email Settings - Global Settings

	& @ <u>*</u>
Email Templates Customizable email templates to streamline your communication needs.	← Back
Global Templates	
Theme Colors	Sample Email of Add Guest User
Background Color #326297	Select Email Type Send with Password
leader Content	Subject: Guest User Add Confirmation
B I U % ⊠ Hs Hz ▲ 网 ≞ ⊟ Tx	Guest Account registered successfully.
	Hello Alex
	Your account is created with the following credentials -
ooter Content	Username: alex@acme.org
B I U % H₁ H₂ A K ⊨ ⊟ T _x This is an automated email notification. Please do not reply to this message.	User Password: 12345678
tana any any amang ang ang ang ang ang ang ang ang ang	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.

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

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

myorg1.com agni MONITORING **Email Templates** Customizable email templates to streamline your communication needs. Dashboard → Sessions Global Templates ACCESS CONTROL Select Email Template Networks Add Guest User × ±|± Segments ACLs Er Guest G Add Guest User IDENTITY (2) Identity Provider Guest User Updated Em; Guest User Approval 💄 User V Guest User Approved Client V A Organization User 💏 Guest V CONFIGURATION Add Organization User Access Devices v Y **Onboard Client** Onboard OTP Login Device Administration V User Password Update D 📮 Certificates ~ Wi-Fi Passphrase System ~

Figure 14-15: 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 14-16: Email Templates Example**

Email Templates Customizable email templates to streamline your communication needs.	← Bac
Seec Enst tespine	Sample Email of Add Guest User
	/ Select Email Type
Inal Labor	Send with Password
Guest User Add Confirmation	Subject: Guest User Add Confirmation
all Placeholders	
Account created with Pasignrase	Guest Account registered successfully.
A unique Wi-Fi passphrase has been created for you.	Hello Alex
Recourt created with Papersid -	Helio Alex.
Your account is created with the following credentials -	Your account is created with the following credentials -
Device limit Device limit	Username: alex@acme.org
5474	User Password: 12345678
Hello	
Header Text	Device limit: 2
Guest Account registered successfully.	Valid from Date: 22 Jul 24 16:59 +0530
Fergevala matuction	Valid until Date: 23 Jul 24 00:59 +0530
Use the following passphrase to connect your client devices.	
Prineet	This is an automated email notification. Hease do not reply to this message.
User Password	
DPC code file	
QR code file abc	
28 scal instruction	
Scan the network QR code and connect to the wireless network.	
Network .	
Username	
with the second s	
Valid from Date	
vala unit	
Valid until Date	
Ad Intera	
WiFi Network xyz	
MT FT Pessaltrase	
Wi-Fi Passphrase	

14.6.2 Configuring SMS Gateway

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

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

To configure the SMS Gateway, log in as an admin and perform the following steps:

Navigate to Configuration > System > Notification Settings > SMS Gateways

Figure 14-17: Notification Settings - SMS Gateways

MONITORING	Notification Settings Choose the type of notification you want to update.	🖻 Email Templates
Dashboard	Choose the type of notification you want to update.	
V Sessions	Email Settings SMS Gateways	
Networks is Segments.	SMS Gateway Settings	
ACLS	To add another SMS Gateway, click here	
(2) Identity Provider	Test MSG91 QA d MS091	/ 0
LUser	Y Y	· •
Client	Test twillo ga 🔞 Twillo	
f Guest	v lest twillo da 😈 iweo	/ 0
CONFIGURATION		
Access Devices	×	
Device Administration	×	
Certificates	•	
System	*	
Audit Viewer		
License		
Self-service Portal		
RadSec Settings		
Support Logs		
System Events		
Notification Settings		

14.6.2.1 Configuring the Twilio SMS Gateway

To configure the Twilio SMS gateway:

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

Figure 14-18: SMS Gateway - Twilio Settings

			6 0
Contrations	Choose the type of notification you want to update.	in treat Templanes	
CESS CONTROL Networks	Email Settings EMS Galeways		
Segments	SMS Gateway Settings		
ACLA	Child Samou For		
Identity Provider			
User X	🛞 Twite		
Class v	d utoer		
Quest ^	Twilio SMS Account Settings		
🕂 Users 💷 Portals	Account SID		
Access Devices	Auth Token	0	
Device Administration 🗠	Tablo Nuester		
lystem .	Text Proce Number		
Audit Viewer	Task phone burdler is required for coefficiency		
 License Self-service Portal 		- Uniting -	
RadSec Settings Support Logs		Satura Add	
System Events			
0. Notification Settings	1		
« Collapse Sidebar			

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

- b. Auth Token
- c. Twilio Number
- d. Test Phone Number

Figure 14-19: SMS Gateway - Twilio Settings Details

	11		6 0 N
MONTONING Dashboard Stations Access controls	Notification Settings Crosses the type of extification year want to update. Ensat Settings Std Serversys	Cal Translation	
 Networks Segments ACLs 	SMS Gateway Settings		
Ance Dentry (2) Identity Provider	Mil Sarang Yan Tana Tana Sara Sara	<u> </u>	
1 User	Y Tello HO Sut		
f Guest Guest Duers	Tuilis SMS Account Settings Tourise SMS Account Settings Tourise SMS Account Settings Society/WY/122222		
Communitation		•	
Certificates	- +124/6/19		
E Audit Viewer	Test phone mention is required for sectionaries	wety	
 SeiT-service Portal RadSec Settings Support Logs 		Delete Add	
System Events	s.1		
(K Cultapue Sidebar			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

14.6.2.2 Configuring the MSG91 SMS Gateway

To configure MSG91 SMS gateway:

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

- a. Guest user add content
- **b.** Guest user update content
- **c.** Guest disabled content
- 6. Click the **Add** button to add the details.

Figure 14-20: SMS Gateway - MSG91 Settings

NETOWNE		
Dashboard	Notification Settings Choose the type of notification you want to update.	MS001 SMS Account Settings
Sessions		and the second se
CERE CONTROL	Ereal Serrings SMS Category	0
Networks	ACc48a8c4248607754657842527846878	
Segments		Create SMS semplates in MSGR1 and provide their IDs below
ACLA		- frame and and temperate the
1117		Normal Statement -
Identity Provider	+17542801198	Tarran control relic (Paper giver), Paper of Manuacriffe
User v		
Client v	Test Phone Number	noyy
Ouest o		Sample united State (Renationed Repairson)
		Card management #
T Users		in the second se
S Portale		Exercise prevent Selbs (receipt name) 45, accord to alloanted,
ensusation	Template Configuration	
Access Devices	the manual lenses	
Device Administration v	Guest account is added.	
Certificates v	Username: ((username)) Pessword: ((password))	Template Configuration
bystem A		Charter of the second sec
	Coert account is updated.	And a Reconstruction provides your parameter in Reparameter and the logis to determine the in-
Audit Viewer	Userrane (Luserrane)	1
C License	Passori ((passori)	v Start or option senses Tank of advancement of a programmer is adjunctionality to book to detaily similar by
Self-service Portal	See the of here	
RedSec Settings	Guert account disabled. Username: ((username))	Shreen and Shreen Sh
InsportLogs		Malls ##approximate_poor parametrical#_poor parametrical#_inclusion_dat#_inclusion_da
🖾 System Events	To add another SMS Gateway, click here	
A Notification Settings		

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

Related information

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

Sessions

This section provides details on how to access and view the session details in AGNI. To access the Session details, navigate to **Monitoring** > **Sessions**. The Sessions page displays a table with the list of devices and the corresponding session details.

F

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

Figure 15-1: Monitoring Sessions

NTORNO	N	Sessions							
Dashboard	~	List of Sessions as on 13/01/2025 16:21:01							
Sessions	1								C 🔳
ESS CONTROL									
Networks	Q	Search by Identity, MAC Address, IP Address or	Setsion ID	Any Any	•	Any		*) (Any	
ACLs	~	# IDENTITY	TYPE	MAC ADDRESS	IP ADDRESS	STATUS	TIME	STAMP	
NTITY							2 000		
Identity Provider	Y	1 Lindsay@agnipim.onmicrosoft.com	Unique PSK (UPSK)	96:01;e5:b7:36:b1	10.87130.53	Success	13/01	/2025 12:35:24.252	8
User ~	~	2 Lindsay@agniplm.onmicrosoft.com	Unique PSK (UPSK)	96:01:e5:b7:36:b1	10.87130.53	Success	12/01	/2025 18:27:07:331	
Client	~	3 Tarun@antaraaleng.onmicrosoft.com	Client Certificate	0a:73:e5:21:3b:27		Success	13/01	/2025 02:34:01.461	
Guest ~	~	4 Tarun@antaraaleng.onmicrosoft.com	Client Certificate	0a73;e5:2f3b:27		Faled	12/01	/2025 22:39:19.668	
Access Devices ~	v	5 Lindsay@agnipim.onmicrosoft.com	Unique PSK (UPSK)	96:01:e5:b7:36:b1		Faled	12/01	/2025 18:27:03:112	
Device Administration v Certificates v	~	6 Lindsay@agniplm.onmicrosoft.com	Unique PSK (UPSK)	96-01-e5-b7-36-b1	10.87130.53	Success	• 11/01	/2025 18:27:03.030	
System	v	7 Lindsay@agniplm.onmicrosoft.com	Unique PSK (UPSK)	96:01:e5:b7:36:b1		Faled	11/01	2025 18:26:58:368	
E Audit Viewer	~	8 Lindsay@agniplm.onmicrosoft.com	Unique PSK (UPSK)	06-01:e5:b7:36:b1	10.87130.53	Success	0 10/01	/2025 18:26:58:184	
License Self-service Portal	*	9 Tarun@antarasieng.onmicrosoft.com	Client Certificate	0a 73 e5 2f 3b 27	10.87130.221	Success	 10/01 	/2025 12:38:35:512	
RadSec Settings	~	10 Tarun@antaraaleng.onmicrosoft.com	Client Certificate	0a:73:e5:21:35:27	10.87130.221	Success	09/01	1/2025 12:53:07.976	
Support Logs	~	11 Tarun@antaraaleng.onmicrosoft.com	Client Certificate	0a:73:e5:2f:3b:27	10.87130.221	Success	0.09/01	1/2025 12:38:32:533	
System Events	~	12 agni-local	Client Certificate	3c#9.f7c2#813	10.87130.248	Success	1	1/2025 10:56:28.428	

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

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

Figure 15-2: Session Details

ONITORINO	N	Set	ssions								
Dashboard	~	Ust	of Sessions as on 13/01/2025 18:21:01								
Sessions	1										c 🔳
CESS CONTROL											
Networks	Q		by Identity, MAC Address, IP Address or Sess			Any		Any		+ Any	
Segments											
ACLS	^		IDENTITY	TYPE	MAC ADDRE	IS IP ADDA	RESS	STATUS		TIMESTAMP	
INTITY		- 28	Lindsay@agniplm.onmicrosoft.com	Unique PSK (UPSK)		10.8713		Success			
Identity Provider	×	10	Lindsay@agnipim.onmicrosoft.com	Unique PSK (UPSK)	96.01;e5:b7	36:61 10.8713	10.53			13/01/2025 12:35:24.252	
User	~	2	Lindsay@agniplm.onmicrosoft.com	Unique PSK (UPSK)	96:01:e5:b7	36.61 10.8713	10.53	Success	0	12/01/2025 18:27:07.331	0
Client	~	- 22	Tarun@antaraaieng.onmicrosoft.com	Client Certificate	0a/73/e5/2f	1-77		Success		13/01/2025 02:34:01.461	0
Guest		- 55			08.70.8278.0			Contraction	-	13/00/012/01/34/01/407	
PIDURATION	Det	ails									
Access Devices	5	Request	1D	AGNI Server		Access Device			20	etwork	
Device Administration		R ON019	Nide84-cc9e-79da-8ea9- I8fe80:cu22cg9po4us72nivnu0	in-mh04-pl-agni-01.pnq.aristanetwor	ks.com	AP-NEW				RUM	
Certificates v		500000	ereevicexxegepowers krawne								
System		Segmen	đ	Session Start Time		Session Stop Time					
E Audit Viewer		Defaolt		13/01/2025 02:34:01							

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

Figure 15-3: Monitor Session Details

agni onPrem-Pune				G 0			
MONITORING	Session Details Session 10 + R-ON01934bb0-0b1f-74c2-8c92-05f8908cf828 cu2bmd1po4us72ovv240						
ACCESS CONTROL	Authentication Request	Success	Session Details	Closed			
Networks	Authentication Type	Unique PSK (UPSK)	Client IP Address	10.87130.53			
+ + Segments Segment		Default	Session Start Time	13/01/2025 12:35:24.252			
ACLs	Location		Session Stop Time	13/01/2025 13:09:24.218			
 Identity Provider User 	Luser (Enabled	Client	Enabled	Actions			
Client ∽ ∰ Guest ∽ contributiantion	Lindsay@agniptm.onmicrosoft.com Lindsay	96.01.eS.b7:36.b1 Auto registered with UPSK		Allow Access PAN Firewall Push User Information Target = PANFW1			
Access Devices · Device Administration · Certificates ·	Access Device Arista WVF	eñ Network	Enabled	Target = DANSW2			
System ^ Audit Viewer License	10.87/130.244 Pune-Radsec-AP	DOGUPSK DOGUPSK Unique PSK (UPSK)					
 Self-service Portal RadSec Settings Support Logs 	Input Request Attributes	×)	Output Response Attributes	*			
System Events	Session logs for request: R 0N0193deb0-0b1f-74c2-8c92-05f6908cf828	cu2bmd1po4us72ovv240		ShowLogs			

15.1 On-Demand Disconnecting a Client from the Network

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

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

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

Figure 15-4: Client Session Details

	Sessions At af Sessions as an 11/27/2023 12:15:32						
Network	Access Device Administration						C 🔳 🖩
Q					Ary Ary	*) (Any	×.
* *	IOBMITY	TYPE	MAC ADDRESS	IP ADDRESS	STATUS	TIMESTAMP	
. v . 1	Isha@xystextpoc.onmicrussft.com	Clauri Certificate	30.86/76.46/01.40	192.108.1.10	Betreta .	15027/2023 12:02:34-321	0
w 3	P0T0	MAC Automatication	38.01.0x.06.36.0x		heren 🖷	11/24/2023 12:08 26:025	
¥ 3	P010	MAG Authentication	28/11/0e/08/20/0e		(heren) @	1024/2025 12/04/14 826	0
v 4	P010	AMC Automation	20/10k08/36/0a		4 wind	1024/2023 12:02:27:967	
¥ 5	isha@eystestpoc.onsicrosoft.com	Client Certificate	30.56:74-45:01-4d	192,166.131	Decress @	11/23/2023 22:29:39.358	0
w 0	Isha@xystestpac.onmicrosoft.com	Charit Certificate	30.86/30.48/0F.4d	192.168.1.11	Second O	11/23/2023 32:20:12.385	

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

Figure 15-5: Client Session Details Page 2

Session Details - Rcli3g0g4n37c72tsrtv0 Details for Session				by Disconnect + Each
urthentication Request	decree.	Session Details		Open
Authentication Type	Client Certificate (EAPITLS)	Client IP Actress		192.168.110
legnert	Dession Start Time		11/27/2023 12:02:04:321	
Location	*JedaiDehi(DL-1	Session Stop Time		
L User English	Client	Endows	Actions	
hadjuptestpol, environett com ha	30.382 76 49:09 44 Tanun Khanna's Anthroid		Allow Access	
Access Device Aruss With	al Hetwork	Entirel		
uni 24.10.00 eff arun, Arisida, w318,10.08 CF	Canterra Conterna Client Certificate (EAP-TUS)			
put Request Attributes		Output Response Attributes		÷
ession logs for request Roll3g0p8rd7c72tarte0				Show Logs

3. Click the **Disconnect** button.

Figure 15-6: Client Session Details Page 3

Session Details - Roll3g0g4n37c72tsrtv0 Details for Session				N Disconnect 🔶 Kack 🖶
Authentication Request	Success	Session Details		Oper
Authentication Type	Client Certificate (EAP-TLS)	Client IP Address		992,968.136
Segment	Default	Session Start Time		11/27/2023 12:02:34:321
Location	*Jindia/Deh/DL-1	Session Stop Time		
1 User (Fratuer)	Cient	Insted	Actions	
innegisy prestors, constrained, com table	30 bb: 70 4b:07 4d Tarun Khanna's Android		Allow Access	
Access Device Anits W7 ek d1 24 10 00 cf Tarun, Anits, w116, 30 08 CF	Hetwork Carborns Centerns Centro CentRoom (EAP-112)	Crutive		
Input Request Attributes	*	Output Response Attributes		•]
Session logs for request: Rollsgögdn37/72hartv0				Show Loge

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

Figure 15-7: Client Sessions Details Page 4

Session Details - Rcli3g0g4n37c72tsrtv0 Details for Session			by Disconnect C+ Back
Authentication Request	Success	Session Details	Open
Authentication Type	Client Certificate (EAP-TLS)	Client IF Address	192,566,316
Begraet	Default	Bession Start Time	11/27/2023 12:02:34:321
Location	*/mta/Den/DL-1	Session Stop Time	
L User (Tradies	Client	Trained	Actions
Infragiveneopos construction (const factor	30 Sti 70 Ab (1748) Tarun Khanna's Androst		💮 Atos Acces
Access Device Access of 31(24:50 Oct of Tanue, Africa, w218, 30 Oct Of	Disconnect Are you sure you earl to disconnect RoSSyDg4c32c72birth	Sessions December 1	
Input Request Athributes	•	Output Response Attributes	, e
Session logs for request: 8x83g/bg/x37x72mm/b			(Beelage)

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

	Session Details - Roll-42t84n37c72tsrul0 Details for Session					(+ Back
	Authentication Request		Recent	Session Details		Oper
	Automication Type		Client Certificate (EAP-TLS)	Ciert P Astress		192,168.3.9
	Beginet Default			Session Start Time		11/27/2023 12:42:53.04
	Location		*Andia/Deh/JU-1	Session Stop Time		
•	1 Uner	Insteel	Class	Engine	Asters	
v tration v	Inhage-steeport annitration con-		30 bb/7540 07.64 Tarun Rhanna's Android		S Allow Access	
*	Arrest Device Hind 12 (10 Ded) Tanut, Arrisa, w211, Jo 08 CF	(Arista 1071)	Meteore Meteore Conterns Conterns Conterns Contexts ISAV-11_31	(based		
	Ingut Request Altributes		· ·	Output Response Attributes		
	Session logs for request: Rt842184x37x721sru0					Show Ling

Figure 15-8: Client Session Details Page 5

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

Figure 15-9: Client Session Details Page 6

Session Details - Rcli40gg4n37c72tsru90 Details für Session				e fact e
Authentication Request	Succes	Session Details		(Cosed)
Authentication Type	Client Certificate (EAP-TLS)	Client @ Address		192 158.118
Sogname	Default	Session Start Time		11/27/2023 12:32:46:145
Location	*Andia/Dem/DL-1	Session Stop Time		1//2//2020 12:39:42:152
1 Uver Toulout	Cient	Fruitdent	Actions	
White Day standard, constrained from the second standard second	30 bb-78-8c 07-48 Tanun Khanna's Android		Allow Access.	
Access Davice	- Hetwork	(Resident		
el d1 24 1006 of Terun, Aristo, w318,30 08 CF	Carbers Carbers Cient Carbicate (EAP-TLS)			
Input Request Attributes	*	Output Response Attributes		•]
Session logs for request: IREADgg4x37r72tav400				(thew Logs)

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

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

Figure 15-10: Disconnect Debug Logs

=

ion logs for request.	Roli3vill-Indi7c721sru5g						Download	Hide Log
aler al	7.							
disconsistense, t	arminatelasier#, attrontation 1879-545-19-545	**************************************	A:18:08:07-Canterva) attempting Con					•
Nurme+Ls7a, Reflig: 88-70-48-07-40, Re Da+30%070400740279 Redlig:12877(4007-0	1877/NAS-IP-Address+192.168.1.2, Radius:1877 Hdus:1877/Connect-Info-COMUCT 5476ps B02.11 12868765, Radius:1877/ClasseRclibv184437472155	24875 (dekr115/j8407/22trukg multidesise20-000) 083-Inentifier-04-03-26-18-00-07-Lenserva, Ratios IB Ratios III: Ratios-18-18-18-00-34049640401000071 alg(CCDImeLE-1740-AMD-0740-122777Feast, Ratios-18 stalBAM, Radios:1877/Ac(3-Input-digmondsed, Ratios-	77/Called-Station-Id+D+-01-24-10-08-07-0 702008757, Radius-2877/SLAN-Pelr-dise-Cis 77/Event-Yimestamp-2023-11-27 07/07/38 -	enterna, Radius 18 Narw1927070, Radius 2000 UTC, Radius 2	TF:NAS-Port-Type=10, RedLus:IETF:Ser s:IETF:NLAN-Oroup-Cipher=L027070, Re ETF:Actt-Delay-Time=0, RedLus:IETF:A	vice-Type+2, Redius IETF/AAS-Por dian:IET7:NLAN-AAM-Suite-D027073 Ant-Section-Time+D3, Redius:DET7	t+1, Radius:1877(Callin), Radius:1877(Acct-Mult)Acct-Input-Packatu+91,	-Station-J
\$1/27/2813 \$2:37:	19.227 25/0 [\$10.0444304/4322-4824-8710-Fe79a	14837: Ld+Rell3-184+37072tor-chg multilassio+20+3050	anofestitesestite) ratios(ecct) - enque	ed ClientDissonner	10-4-10-10-10-10-10-10-10-10-10-10-10-10-10-	1.18]		
11/17/1913 11:17: 7.54548541	09.257 3570 [4+800a520a0-6212-4820-8750-Fa79a	14837: Ldomelliv/Imin37c72tarw5g multitession23+3000	WANNETARLINEARENS) Fadius(acct) - de von	iete ecct(utne) mei	1+105578488#fad, scrt5essior1D+105676	00FAEL812008CF174L818757 #111761	11154:010030007040840	4179196879
\$1/27/2825 12:57:	39.257 35PU [t=tdda410ed-62c2-482d-8710-fa79a	14897c 10-Roll3v184r37c72turv8g multiSessior30+3800	debefedi701000705] renius[ecct] - sessio	n completed in 7.8	113366ms			
		314837: 10-8:113/104+37:72tar/5g] w/wrtfrocessor(cl) 000fed","10":"192.148.1.16"}] # 3023-11-27 07:07:39		undversfroducer) e	ev disconnect[("org10":"Edda41#ed-62	12 (402d - 8733)-		
		d14837c ld+Rc113v184+37c72tsrvfg] eventProcessor[c1 Ho#4er,~1p*:*192.168.1.16*}] # 2823-11-27 87:87:38		itatafroducar] er d	flaconnect[{"arg20":"Roda418ed-62c2-	4820-8710-		
11/27/2823 12:37:	39.520 15/0 [t+Edds410ed-62c2-402d-8715-fa79a	14837c id+8cli3v184n37c72tsru5g] radius(cos) = adde	activity record for mac+3866754689744 in	2.923272ms				
	39,528 2370 [tvinnaki0as-63c2-6835-8735-fa79a arminataCassa+0, attravEadius 1875 506-19-805	14837: idem:likvl84ex37c72tsruig] radius + ssae[org]			00-88-70-48-8F-40, natCornID+6481380	Warf/12110030403727210-10.0, 0.1	Mag20+%c113v184r37c72ts	relige

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

Figure 15-11: CoA Action Status

Client Details - Aut View client details and up	to registered with UPSK adate the selected client		← Back
Sessions for this client			Show Sessions
Client Activity			Hide Activity
Q Search by Activity type and	d 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

16.1 Monitoring

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

16.2 Dashboards

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

To access dashboards, navigate to Monitoring > Dashboard



Figure 16-1: AGNI Dashboard and Session Trend

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

Figure 16-2: AGNI Dashboard and charts

ngni		⊕ 6
MONITORING	Dashboard View analytics	± Downloa
Sessions COESS CONTROL Networks	18:30 19:30 20:30 21:30 22:30 21:50 00:50 01:50 02:30 00:30 04:30 05:30	0630 0730 0830 0830 1030 1130 1230 1330 1430 1550 1630 1730 1830
#I# Segments	Top Failure Reasons 🔀 Custom	Top Locations Affected By Failures Today 😨 07/03
ACLS		
(1) Identity Provider		
土 User 🗸 🗸		
Client ~	768 TLS read failed 3 Radius received timeout	*Main Office/Ground
🖵 Certificates 🗸 🗸	91.6%	
Certificates ~ Administration ~	11.5%	
🖵 Certificates 🗸 🗸	99.5%	0 2 4 6 1 Count

16.3 Sessions

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

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

- MAC address
- · Identity
- · IP address
- · Session Identifier

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

Figure 16-3: Monitoring Current Sessions

Dashboard		~		rssions t of Sessions as on 07	201/2025 11:00:29						
Y Sessions	1										C 目
P Networks		٩	54970	h by Ioensty, MAC Aus	eni, P. Addenia et Senivo XV.))(Any	1) (Ary	+)(²⁰⁰⁰ / _{AU}	
ACLO		^		IDENTITY	TYPE	MAC ADDRESS	IP ADDRESS	STATUS		TIMESTAMP	
Utentity Provider		*	52	quarantine	MAC Authentication	00.0129.65.14.81	10.81.204.184	Success	•	07/01/2025 10 51 46.009	4
	4	*	2	quarantine	MAC Authentication	00.0e2945.e4.8c	10.81.204.184	Success	0	07/01/2025 10:31:45.958	
	*	~	a'	quarantine	MAG Authentication	00-0c:29-85.c4-8c	10.81.204.184	Success	0	07/01/2025 10 11 45 952	
Guest NITOURATION	* 3	v	4	quarantine	MAC Authentication	00.0c.29.65.c4.8c	10.81.204.184	Success		07/01/2025 09:51:45:925	
	*	*	5	quarantine	MAC Authentication	00-0c-29-65-c4-8c	10.81.204.184	Success	•	07/01/2025 09:31:45.893	
	÷.	~	à:	quarantine	MAC Autoentication	00.0c29.65:c4.8c	10.81.204.184	Success	•	07/01/2025 09/11:45.883	
System	*	×	2	quarantine	MAC Authentication	00.0c.29.65:c4.8c	10.81.204184	Success	•	07/01/2025 08:51:45:856	
Installed Apps		-	÷.	quarantine	MAC Autoentication	00.0129.6514.84	10.81204184	Success	•	07/01/2025 08:31:45.840	
		~	0	guarantine	MAC Authentication	00.01:29.65:14.81	10.01.204184	Success		07/01/2025 08:11:45.798	

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

Figure 16-4: Session Details

agni					େ ଡ 🔻
MONITORING	Session Details - Rcils9e5j0h1s72sc27mg Details for Session	1			e Book 👼
ACCESS CONTROL	Authentication Request	(Success)	Session Details		Closed
Networks	Authentication Type	Client Cestificate (EAP-TLS)	Client IP Address		10.86.60.228
411 Segments	Segment	Default	Session Start Time		7/10/2023 14:13:36:306
CENTITY ACLS	Location		Session Stop Time		7/10/2023 14:13:46.924
 Identity Provider User ~ 	L User	Client	(Enabled	Actions	
Client ~ CONFIGURATION Access Devices ~ Certificates ~	steve kratt Steve Kratt	70-1a b8 82-10-31 Steve Kratt's Windows			
System ~	Access Device	Network	Erabed		
III Explore	30.86.24.60.07 at Pune-C235AP	PUNE-WPA2 PUNE-WPA2 Cilent Certificate (EAP-TLS)			
(Collapse Sidebar	Input Request Attributes	~	Output Response Attributes		~

Figure 16-5: Session Details page 2

1 Aut			72sc27mg	Session Details - Rolls/9x5j0h1s72sc22	
					-
	(hoted)	- Naturn	Adda Addi	· Aucora Banica	-
		have write		100 MA 200 40 107 se	
		🕈 rusi aini		Pure-02154P	
		Chart Datellaum (Lat. 7,4)			
					President
	Original Bergiorean Altolisation	(e.)		Ingent Response Attributes	
international programmer and and an and an and an and an an and an an and an an and an and an and an and an and	Name 219 Class	1944 2 M		Cambrane D1	
	Tester CTT 247 Testage			Cardford Including y	
	Institut 2019 (assessed - Paramat	Tribe tes d'Attitus arts sais aux abandunas	Daradon, hazar Da.D	Carolisation	Doubes .
	Partice (CTF Terroramen, extens	THE REPORT OF		Cardinas See	
5 gi	Restau Managert 482 APPE data vier	(Process and domain) and		Carthony Sutient	
	Tagaid Minister Mart Arrist Anna Pag	The second s		National Trideon Streams on	
				Radius (177-Label Option 18	d Appen
		10-10-00-02-02-02		National Trianing station of	
		CONVERT ANNAL BUILDS		Reduct CP Connect only	
				Reduct (1.5.1) - Hereige	
		Peter .		Radue ETF France NTV	
				Nation (17) Transage - Fullyants per	
		No.44.44.253		Andrew (19-16), - Address	
		in the product of the data of		Tables (177 rate) constitue	
				Andrew (The state desce	
				Balloy (\$17.002-01) + Type	
		÷		Andrea ETF Carlos Appa	
		show in other		halor(17-cost-fame	
		N2TOTA		Bankup (1010), Ale Arité Auto	
		http://w		Padeor/ETF-WcAlls Orcup Capitor	
		NOTION .		Radiate (1978), Ale-Factoria - Califar	

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

Figure 16-6: Sessions and Show Logs

ni						6 O				
passa .	Session Details - Rolls9e5j0h1s72sc27mg Tetati for Texase					+ Bot				
anstani	(ingenere		server a	within the one		1114 AUG 10 10 10 10 10 10 10 10 10 10 10 10 10				
Carried .	Location			Salary Dep Time		NACES IN CONTRACT				
arisasika.										
-greata	A year	(frame)	Contract Contract	(Instant)	Actors					
62.e										
**	100.04.31920		PD 1a k0 62 10 31		(i) Align Access					
antity Prevident	Eteres 4/141		Shoon Would a Wendperg							
war										
Sent										
in African	Access Dentre	(Anna MPE)	a notest	(dearmer)						
unes Devices -										
enformer -	10 00 20 40 07 al		Print winz) Print winz)							
	Pure C231AP		Court Countrate (SAP-PL)							
LANS .			Contraction and the second second							
allers .										
whether Agen	Nand Request Rectings			Durput Responses Attributes						
	Bassier Lage for resumer Buildelightin familier					(Prosterior) (Marian				
	(inst									
	Through Lin D. St. W. (publick) of https://www.information.com/and/publicly									
	Transmission (and the first of the second seco									
		Transmit 14:13:14:19:14:19:14:19:14:14:14:14:14:14:14:14:14:14:14:14:14:								
	Alternal in the part of the state and approximation instituted instituted instituted instituted instituted in the state and approximately and approximately and approximately and approximately and approximately appr									
		Tributo as a set of province end only other strategies (as a set of province of of prov								
			ering) - Deer recerting erich Changel, weer 12,0 meer							
					monthly and an himself the anterphantle hours					
			is output) - state-"EX Electrodecomment classi;							
	Type paint to the size and two productions well-deep-the	-cheathings and distriction in a series	(a-server) - start haundale							
	Transmis in all in our attent protocoline and don't the	constraint (sector) and provide the provident	(hourses) - states "NA handstatellart" real regence &	the slaves '						
	7/96/2013 64-03-16-084-00368 [5-479/4708c-exd2-4ec]-03	not description and calendary resulting and	()- server) - plate-753 hetdytals/lary* and respecte fr	on clinet to Thi						
	The set is a set in the line set in the set of the set	(lle-orrese) - status/916 Baseniatellart* read response #	ve 7.1						
	frailaith to at highlight to at highlight to be	read and the statement of the second second second	the entropy of a shallow "Will be address at the the second second at the							

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+/)	1	🖂 🛱 🔎 💿 🖗 🖉 зирагла@agniglobal.on
Home > AGNI Demo Org [App regi 		Request API permissions	x
Overview Quickstant Integration assistant Manage	You are editing permission(s) to your application, users will have to consent even if they've Configured permissions Applications are authorized to call APs when they are granted permissions by users/admire all the permissions the application needs. Learn more about permissions and consent	What type of permissions does your application require? Delegated permissions Your application needs to access the API as the signed-in user.	Application permissions Your application runs as a background service or daemon without a signed in user.
Branding & properties Authentication Certificates & secrets If Token configuration	Add a permission same Type Description Moreoof Gaph (4)	Select permissions P user read all Permission	expand all (*) Admin consent required
API permissions Expose an API App roles Owners	Directory/Read All Application Read directory data 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	> IdentityRiskyUser ✓ User (1) User Read All ⊙ Read all user's full profiles	Yes
 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 permission Site. Learn more		
 Troubleshooting New support request 	API / Permissions name Type Description → Microsoft Graph (1) User Sea (A) Application Read all users' full profiles		
	User/Read All Application Read all users' full profiles To view and manage consented permissions for individual apps, as well as your tenant's corr Individual apps, as well as your tenant's corr	Add permissions Discard	

Table 1: API Permissions table

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

A.2.2 Google Workspace

- 1. Log in to Google Workspace.
- 2. Take note of the following entities from Google Console:
 - a. Customer ID
 - b. Domain
 - **c.** Account Email The username of the Google Workspace account that has minimum permissions to read the User and Group objects. Normally, this is the account that is used to configure or manage the GWS configuration objects.

d. Service Account

3. To read Customer ID and Domain:

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

A.2.3 OneLogin

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

A.2.4 Okta

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

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

A.2.5 URLs and Open Ports in Firewall

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

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

See table for the URLs and open ports:

Table 2: URLs and Open Ports in Firewall

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