

1 Table of Contents

- 1 Table of Contents 1
 - 1.1 Revision History 1
- 2 Central NAC & Entra ID integration for Bridge Mode APs 2
 - 2.1 Things you need..... 2
- WLAN and User Role Configuration 3
 - 2.2 NAC-EAP WLAN..... 3
 - 2.3 User Role configuration 3
- Entra ID Configuration 7
- Central NAC..... 11
 - 2.4 Configuring Identity Store 11
 - 2.5 Authentication Profiles 13
 - 2.6 Authorisation Policies 14
- User Onboarding 17
 - 2.7 Staff1 Onboarding Using Onboarding App..... 17
 - 2.8 User Self-Service Option 21
- User Testing 23
 - 2.9 Audit Trail 23
 - 2.10 User Connectivity..... 23

1.1 Revision History

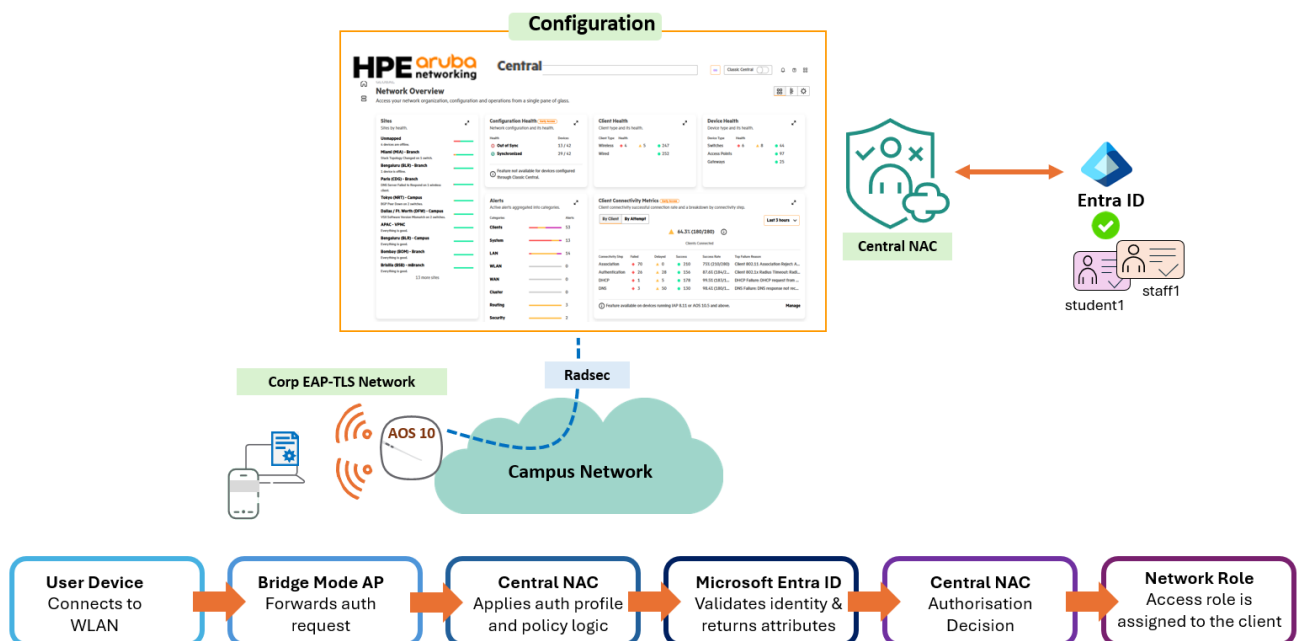
DATE	VERSION	EDITOR	CHANGES
10 Jul 2026	0.1	Ariya Parsamanesh	Initial creation
04 Aug 2026	0.2	Ariya Parsamanesh	Added the testing section
08 Aug 2026	0.3	Ariya Parsamanesh	Added the self-service option of the enrolment

2 Central NAC & Entra ID integration for Bridge Mode APs

HPE Networking Aruba Central NAC provides cloud-based network access control for authenticating users and devices, applying role-based access, and enforcing policy across wired and wireless networks. In this setup, Central NAC (CNAC) makes policy decisions for selected WLANs, while Microsoft Entra ID validates user identity and provides directory attributes such as group membership.

This lets Aruba Central use the organisation's existing identity framework for network access, reducing the need for separate user databases. When a client connects, Central NAC uses the authentication profile and policy rules to evaluate the user or device context and return the correct network role.

For bridge mode AOS10 AP deployments, this approach helps keep the access layer simple while still allowing centralised identity-based authentication, consistent role assignment, and easier operational visibility across corporate, guest, BYOD, and device-specific access scenarios.



Central NAC licensing has two options; see the details [here](#). Core features are included with the foundational subscription required for APs, switches, and gateways, while CNAC Pro adds advanced capabilities such as:

- Bring Your Own Certificate (BYOC)
- Integration with multiple IDPs
- Third party NAD support
- Support for unlimited MPK
- Robust authorization policy with more context parameters
- Portal Customisation, Override Profiles for multiple languages
- Support for Static Tags Limit per Tenant: 400 static tags

This technote covers:

- WLAN and user roles configuration
- Entra ID configuration
- CNAC Identity Stores configuration and its Authentication Profiles and Authorization Policy configuration

2.1 Things you need

- APs running AOS10 firmware version (I am using 10.7.2.1)
- Valid HPE Aruba Central account and subscriptions

WLAN and User Role Configuration

Here we'll cover configuration of a dot1x Authentication WLAN that uses Central NAC. It is basically configuring the WLAN that uses Central NAC for Authentication.

GLOBAL

Configuration Overview

Information about the Library

Library

Global

Site Collections 0 collection

Sites 13 sites

Devices 32 devices

Device Groups 1 group

Profiles

Roles & Policies

Named Objects

Services

Library > Wireless > WLAN

Search

Create Profile

Name	Type	Assigned Device Function	Assigned Device Scope	Status
CNX-guest	Access	Campus Access Point	Global	Enabled
byoc	Access	Campus Access Point	CNX-branch1	Enabled
cnx-psk	Access	Campus Access Point	CNX-branch1	Enabled
corp	Access	Campus Access Point	2 scopes	Enabled
corp-CP	Access	Campus Access Point	Global	Enabled
nac-eap	Access	Campus Access Point	CNX-branch1	Enabled
nac-mpsk	Access	Campus Access Point	Global	Enabled

2.2 NAC-EAP WLAN

This is to authenticate against Entra identity store. The WLAN is called “nac-eap” and it’s authentication server group will be Central NAC.

Update WLAN Profile

General

Name *

Description

Type

ESSID Name *

2.4 GHz

5 GHz

6 GHz

Disable Network

Network Configuration

Most Compatible

Balanced

High Density

Custom

VLAN

Traffic Forwarding Mode *

Bridge

Tunnel

Mixed

Use Named VLAN

Default VLAN *

1

Advanced

Security

Security Level *

Enterprise

Personal

Open

Key Management *

WPA2-Enterprise

Authentication

Server Group *

Central NAC

Air Pass

Reauthentication Interval

0

Minutes

Advanced

Access

Default Role -

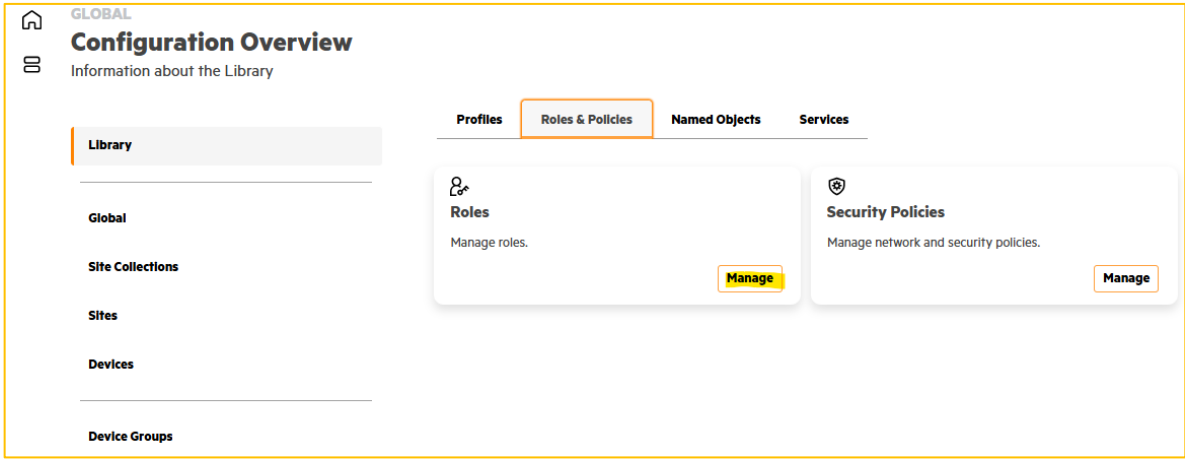
Override default role

Advanced

2.3 User Role configuration

When you configure a WLAN element profile, Aruba Central automatically creates a default role for that WLAN. It then assigns that role to both the campus AP and gateway device functions.

Here I'll go through the configuration of user roles and related policies. In most cases, you want to use the same user roles for your wired and wireless users. I'll start from the library level.



I'll create two roles, Staff and Student. Let's look the roles that I created before.

Profiles

Roles & Policies

Named Objects

Services

Library

>

Roles

Q

st

×

31 items

Create Role

▼

Name	GPID	Assigned Device Function	Assigned Scope	Referenced By
Staff	400	Mobility Gateway Access Switch Campus Access Point	Global	3 policies
Student	1300	Campus Access Point Access Switch Mobility Gateway	Global	5 policies

Here I am showing only what is relevant to the wireless users. You can also configure parameters that are specific to LAN switches. Also note the number of policies each of the roles have.

Edit Role

PropertiesReferences

Name *

Staff

Description

VLAN ID

11

Captive Portal Profile

Select

GPID *

400

☐ Dynamic Application Prioritization

Edit Role

PropertiesReferences

Name *

Student

Description

VLAN ID

12

Captive Portal Profile

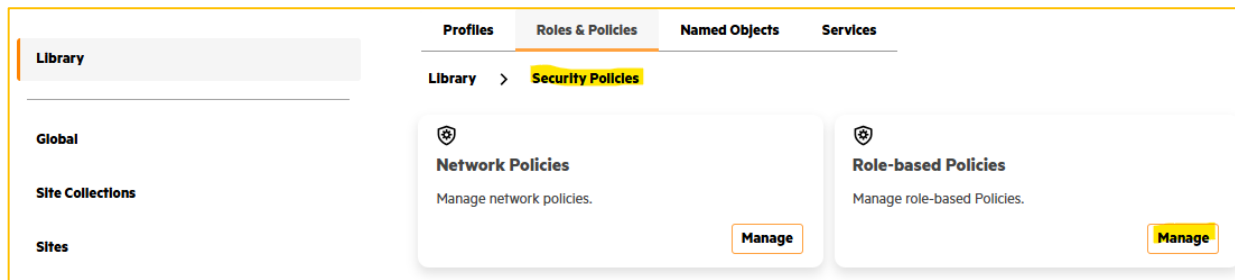
Select

GPID *

1300

☐ Dynamic Application Prioritization

Here for this role that we'll use for our bridge only WLAN, the VLAN id for Staff and Student are 11 and 12 respectively. Next, we go to the Security policies and choose Role-based Policies.



Few points about security policies

- Security Policies are still applied to scopes and device functions.
- The security policies are processed in a top-down fashion until a match is found.
- Policies can be assigned to multiple roles.
- Anything that starts with “sys_” is system generated. Shown below we have two. The sys_allow_all is an explicit allow all rule, which means all wireless traffic that is bridged locally instead of tunnelled to a gateway, will match this policy if it hasn’t yet found a match.
- For “Deny all” policy, you need to explicitly create one.
- And if you decide to have “Deny all” policy then other policies with rules explicitly allowing certain traffic should be defined above it.
- The roles will only be sent to the APs, Switches and Gateways if they have at least one policy referencing it.

Profiles	Roles & Policies	Named Objects	Services
Library	Security Policies	Role-based Policies	Create Policy
Name	Rules	Assigned Device Function	Assigned Scope
> sys_central_nac This is a system generated configu...	3	Campus Access Point	Global
> basic-net-services	6	Mobility Gateway, Campus Access Point	Global
> Inappropriate-content	2	Campus Access Point, Mobility Gateway, Access Switch	Global
> Internal-nets	1	Campus Access Point, Mobility Gateway	Global
> Allow-All-Pol	1	Mobility Gateway, Campus Access Point, Access Switch	Global
> sys_allow_all Default policy to allow role to role...	8	Campus Access Point	Global

I have 4x policies that I created, and each policy consists of a set of rules and are assigned to multiple roles.

Policies	Purpose	Associated User role for most of the rules
Basic-net-services	Allow access to DHCP and DNS	Student, quarantine, Guest_Preauth
Inappropriate-content	Deny access to inappropriate web categories	Staff, Student
Internal-nets	Allow access to RFC 1918 networks	Student
Allow-All-Pol	Allow-all access	Staff, Students

Let’s expand the “basic-net-services” policy. Note that each rule can be assigned to multiple roles. I have just hovered my mouse over the roles and it displays all the roles that it is assigned to.

Profiles Roles & Policies Named Objects Services							
Library > Security Policies > Role-based Policies							
Create Policy							
Name	Rules	Assigned Device Function			Assigned Scope		
> sys_central_nac This is a system generated configu...	3	Campus Access Point			Global		
▼ basic-net-services	6	Mobility Gateway, Campus Access Point			Global		
IP Version	Role: quarantine, Student, Guest_Preauth	Service/Applic...	Category Type	Action	Description	DSCP	802.1P
IPv4	Role: quarantine	Any	svc-bootp	Net Service	Allow	-	-
IPv4	Role: quarantine	Any	svc-dhcp	Net Service	Allow	-	-
IPv4	Role: quarantine	Any	svc-dns	Net Service	Allow	-	-
IPv4	Role: quarantine	Any	svc-icmp	Net Service	Allow	-	-
IPv4	Role: quarantine	Net Destinati...	svc-https	Net Service	Allow	access to clea...	-
IPv4	Role: quarantine	Net Destinati...	svc-http	Net Service	Allow	access to clea...	-
> Inappropriate-content	2	Campus Access Point, Mobility Gateway, Access Switch			Global		

In another example, expanding the “inappropriate-content” policy, you see that I am denying access to Adult and Gambling sites. This policy is applied to most of my roles. So here you don’t need to duplicate the rule for each user role.

Profiles

Roles & Policies

Named Objects

Services

Library > Security Policies > Role-based Policies

Create Policy

Name	Rules	Assigned Device Function	Assigned Scope			
> sys_central_nac This is a system generated...	3	Campus Access Point	Global			
> basic-net-services	3	Campus Access Point	Global			
▼ Inappropriate-content	2	Campus Access Point, Access Switch	Global			
Source	Destination	Service/Application	Action	Description	DSCP	802.1P
Role: Staff, Student	Any	Adult and pornogra...	Deny	-	-	-
Role: Staff, Student, ...	Any	Gambling	Deny	-	-	-
> Internal-nets	1	Campus Access Point				
> staff-pol	1	Access Switch, Campus Access Point				
> student-pol	1	Access Switch, Campus Access Point				

Add Rule Above

Add Rule Below

Move Down

Clone Rule Above

Clone Rule Below

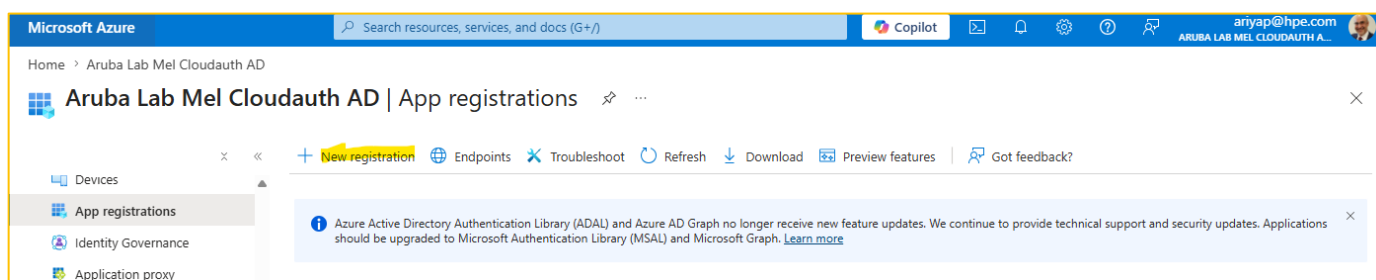
When you hover your mouse over a rule, “...” appears and by clicking on it you can bring up the rule ordering cloning pop-up. As you are reordering the policies, the order gets synced to the devices that are associated to the user-role. You can check the rules that were pushed down to the gateways with “show right <user-role-name>” as shown below for Staff role where I am showing a part of the output that refers to the access policies.

Entra ID Configuration

The main configuration components on Entra Id are:

1. Register an application
2. Configure API permissions for the Application
3. Grant admin consent
4. Create the secret password for it.

Here we'll start with the creating an application that we'll use for New Central integration. Navigate to your Entra ID service >> Manage >> App Registrations



Create a new App and give it a name and leave the “Redirection URI (optional)” empty for the time being. We'll add it later once we have the URL from Aruba Central. A redirect URI is where the Microsoft identity platform sends security tokens after authentication.

Home > Aruba Lab Mel Cloudauth AD | App registrations

Register an application

*** Name**

The user-facing display name for this application (this can be changed later).

NewCentral NAC ✓

Supported account types

Choose the account types that can use this application or access this API

Single tenant only - Aruba Lab Mel Cloudauth AD Help me choose

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

Once you register it, the application will have a tenant and Application ID.

Home > Aruba Lab Mel Cloudauth AD | App registrations

NewCentral NAC

Search

Deactivate Delete Endpoints Preview features

Overview

- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
 - Branding & properties
 - Authentication (Preview)
 - Certificates & secrets
 - Token configuration
 - API permissions
 - Expose an API

Essentials

Display name : [NewCentral NAC](#)

Application (client) ID : 2eb9f2a4-
Object ID : 5817201d
Directory (tenant) ID : 0391024d

Client credentials : [0 certificate, 1 secret](#)

Redirect URIs : [1 web, 0 spa, 0 public client](#)

Application ID URI : [Add an Application ID URI](#)

Managed application in L... : [NewCentral NAC](#)

Supported account types : [My organization only](#)

State : Activated

Azure Active Directory Authentication Library (ADAL) and Azure AD Graph no longer receive new feature updates. We continue to provide technical support and security updates. Applications should be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

[Get Started](#) [Documentation](#)

We need these IDs when we'll be configuring Central. For time being just copy it.

Application (client) ID = 2eb9f2a4-b
Tenant ID = 0391024d

After registering the application, configure the following API permissions:

- Directory.Read.All
- Group.Read.All
- IdentityProvider.Read.All
- People.Read.All
- User.Read
- User.Read.All

Here I am showing how to set those up.

Home > Aruba Lab Mel Cloudauth AD | App registrations > NewCentral NAC

NewCentral NAC | API permissions

Search

Refresh Got feedback?

Granting tenant-wide consent may revoke affected. [Learn more](#)

The "Admin consent required" column shows whether the application needs admin consent in your organization, or in organizations with which your application is federated.

Configured permissions

Applications are authorized to call APIs when all the permissions the application needs. [Learn more](#)

+ Add a permission ✓ Grant admin consent

API / Permissions name Type

> Microsoft Graph (6)

To view and manage consented permissions for your application, click on the permission name.

Request API permissions

Microsoft Graph
<https://graph.microsoft.com/> Docs

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.

Select permissions [expand all](#)

direct

Permission	Admin consent required
Directory (1)	
☒ Directory.Read.All ○ Read directory data	Yes
☐ Directory.ReadWrite.All ○ Read and write directory data	Yes

Request API permissions

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.

Select permissions

Group

Permission	Admin consent required
Group.Create	Yes
Group.Read.All	Yes
Group.ReadWrite.All	Yes

Request API permissions

signed-in user.

Select permissions

Identity

Permission	Admin consent required
AgentIdentity	
AgentIdentityBlueprint	
AgentIdentityBlueprintPrincipal	
AgentIdUser	
Group-XTenantIdentitySync	
IdentityNotifications	
IdentityProvider.Read.All	Yes

Request API permissions

Microsoft Graph
https://graph.microsoft.com/ Docs

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.

Select permissions

people

Permission	Admin consent required
People.Read.All	Yes

Request API permissions

TeamsAppInstallation

TeamsTab

UserAuthenticationMethod

UserNotification

UserShiftPreferences

User

Permission	Admin consent required
User.Export.All	Yes
User.Invite.All	Yes
User.ManageIdentities.All	Yes
User.Read.All	Yes
User.ReadWrite.All	Yes

Then click on “Update Permissions”. Next we need to “Grant admin Consent” for them.

Home > Aruba Lab Mel Cloudauth AD | App registrations > NewCentral NAC

NewCentral NAC | API permissions

Search

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication (Preview)

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already granted on their own behalf are not shown.

The “Admin consent required” column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the organization, or in organizations where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission

Grant admin consent for Aruba Lab Mel Cloudauth AD

API / Permissions name	Type	Description	Admin consent required	Status
Microsoft Graph (6)				
Directory.Read.All	Application	Read directory data	Yes	Not granted for Aruba Lab Mel Cloudauth AD
Group.Read.All	Application	Read all groups	Yes	Not granted for Aruba Lab Mel Cloudauth AD
IdentityProvider.Read.All	Application	Read identity providers	Yes	Not granted for Aruba Lab Mel Cloudauth AD
People.Read.All	Application	Read all users' relevant people lists	Yes	Not granted for Aruba Lab Mel Cloudauth AD
User.Read	Delegated	Sign in and read user profile	No	
User.Read.All	Application	Read all users' full profiles	Yes	Not granted for Aruba Lab Mel Cloudauth AD

Once we have done that, you should see the following status for the Microsoft graph APIs you had selected.

Home > Aruba Lab Mel Cloudauth AD | App registrations > NewCentral NAC

NewCentral NAC | API permissions

Search Refresh Got feedback?

Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already granted on their own behalf are not affected.

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect organization, or in organizations where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for Aruba Lab Mel Cloudauth AD

API / Permissions name	Type	Description	Admin consent required	Status
▼ Microsoft Graph (6)				
Directory.Read.All	Application	Read directory data	Yes	Granted for Aruba Lab Mel Cloud...
Group.Read.All	Application	Read all groups	Yes	Granted for Aruba Lab Mel Cloud...
IdentityProvider.Read.All	Application	Read identity providers	Yes	Granted for Aruba Lab Mel Cloud...
People.Read.All	Application	Read all users' relevant people lists	Yes	Granted for Aruba Lab Mel Cloud...
User.Read	Delegated	Sign in and read user profile	No	Granted for Aruba Lab Mel Cloud...
User.Read.All	Application	Read all users' full profiles	Yes	Granted for Aruba Lab Mel Cloud...

Finally, we need to create client secret ID

Home > Aruba Lab Mel Cloudauth AD | App registrations > NewCentral NAC

NewCentral NAC | Certificates & secrets

Search Got feedback?

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (1)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Add a client secret

Description: Central NAC

Expires: Recommended: 180 days (6 months)

Add Cancel

When you have added the client secret you should get this screen, note that you need to copy the secret value when you create it as we need it when we configure the Entra integration on New Central.

Home > Aruba Lab Mel Cloudauth AD | App registrations > NewCentral NAC

NewCentral NAC | Certificates & secrets

Search Got feedback?

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (1)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Client secret values cannot be viewed, except for immediately after creation. Be sure to save the secret when created before leaving the page.

Description	Expires	Value	Secret ID
Central NAC	14/08/2027	-rt*****	4

Even if you forgot to copy the secret value, you could delete it and create new secret password.

Central NAC

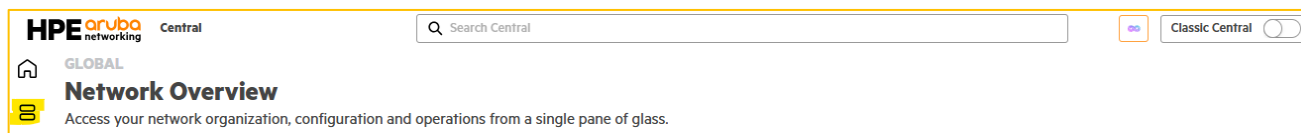
In this section I'll cover the Central NAC configuration and here are the main components that needs to be configured.

Central NAC Identity Management

Central NAC Authentication Profile

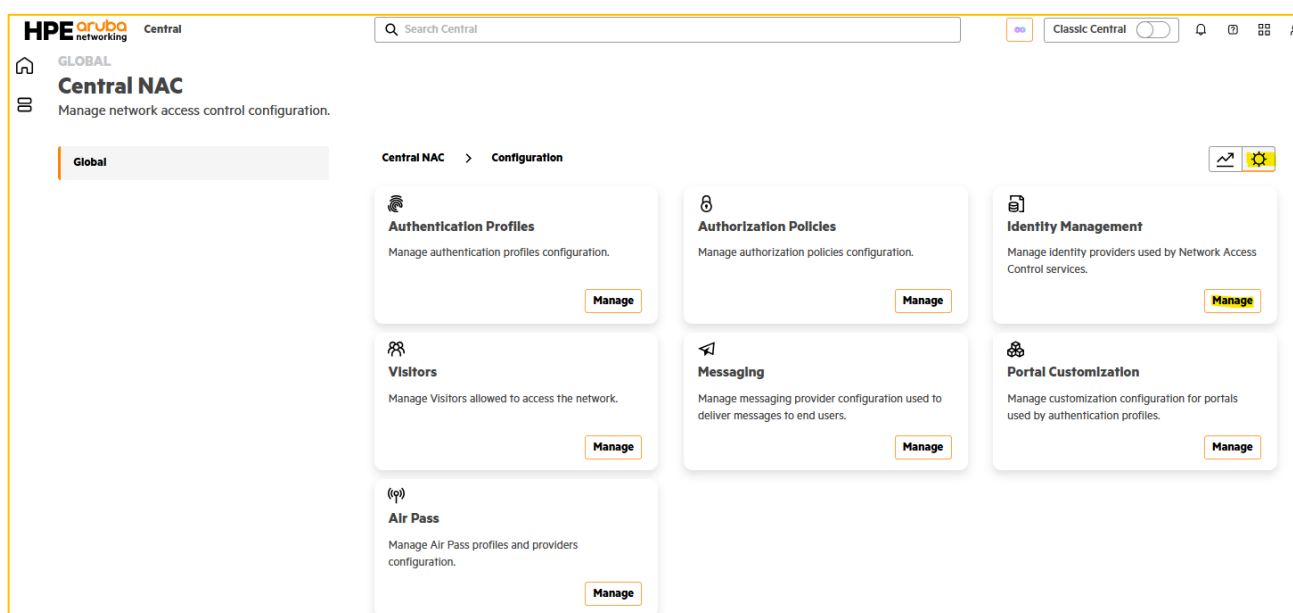
Central NAC Authorisation Policy

Navigate to Central NAC section by Clicking on the highlight icon and then selecting "Manage" Central NAC card.

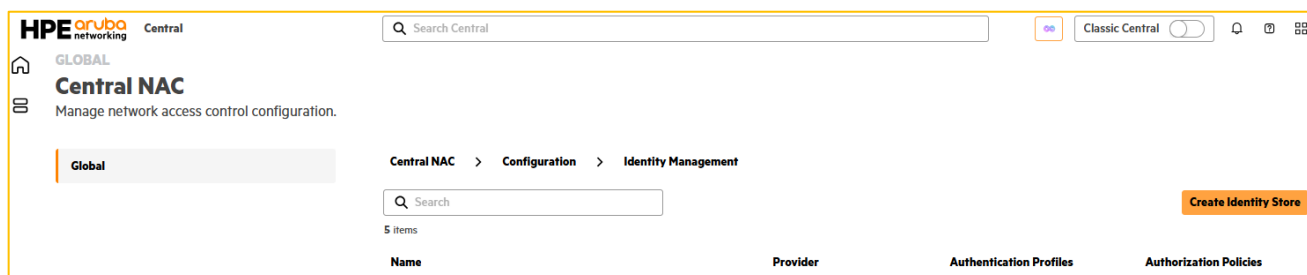


2.4 Configuring Identity Store

Starting with adding Entra as an Identity store.



Once you click on the gear icon to get the following screen, here I'll create our first identity store.



We'll choose Microsoft Entra ID from the drop-down menu. And add the three values we had from Entra Id

Application (client) ID = 468415c0-1e
Directory (tenant) ID = 0391024d-
Secret Value = QE-8Q~

Create Identity Store

Name *

Description

Provider *

Select

Search

Corporate

Google Workspace

Microsoft Entra ID

Okta Workforce Identity Cloud

Visitor

Facebook

Google Social

LinkedIn

OpenID

Visitor Store

X

Create

Edit Identity Store

Name *

Description

Provider *

Tenant ID *

Client ID *

Client Secret *

Redirect URI

Use this URI to register Central NAC in the identity store provider.

<https://apacsouth.cloudguest.central.arubanetworks.com/oauth/reply>

Save

Here you'll see the Redirect URI, copy it as we need to add it to our Entra Id application.

<https://apacsouth.cloudguest.central.arubanetworks.com/oauth/reply>

You can navigate back to the Entra Id application you just configured and add Redirect URI for Web.

Home > Aruba Lab Mel Cloudauth AD | App registrations > NewCentral NAC

NewCentral NAC | Authentication (Preview)

Search Got feedback?

- Overview
- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
 - Branding & properties
 - Authentication (Preview)**
 - Certificates & secrets

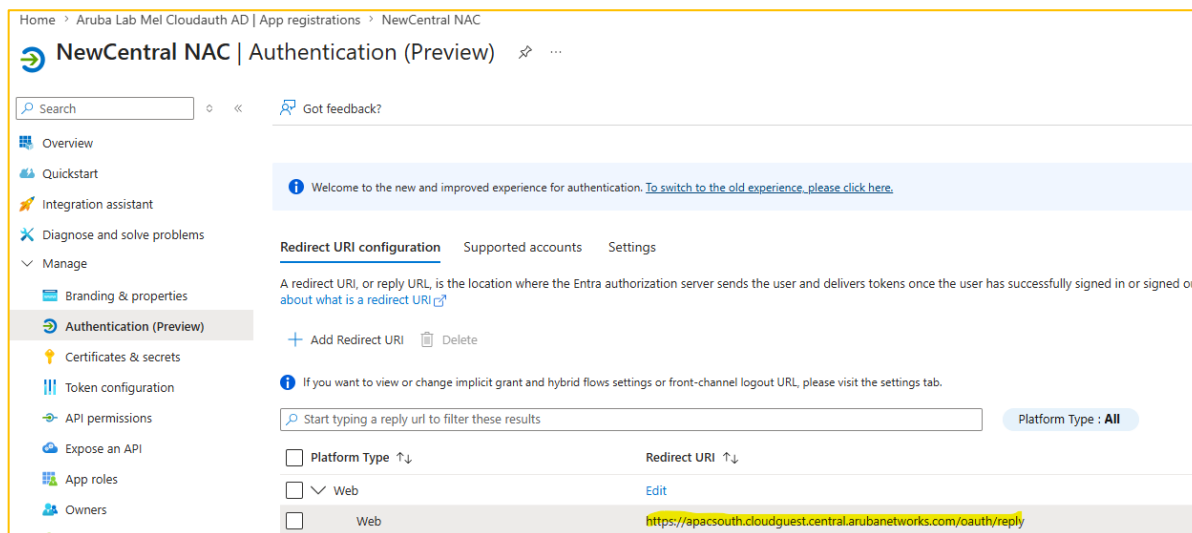
Welcome to the new and improved experience for authentication. [To switch to the old experience, please click here.](#)

Redirect URI configuration
Supported accounts
Settings

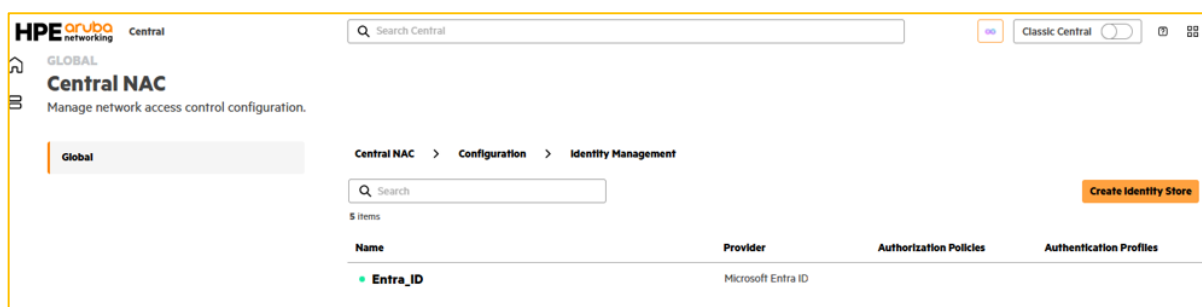
A redirect URI, or reply URL, is the location where the Entra authorization server sends the user and delivers tokens once the user has successfully signed in or signed out. [about what is a redirect URI](#)

+ Add Redirect URI
Delete

Once you save it, you'll see it listed as shown below.



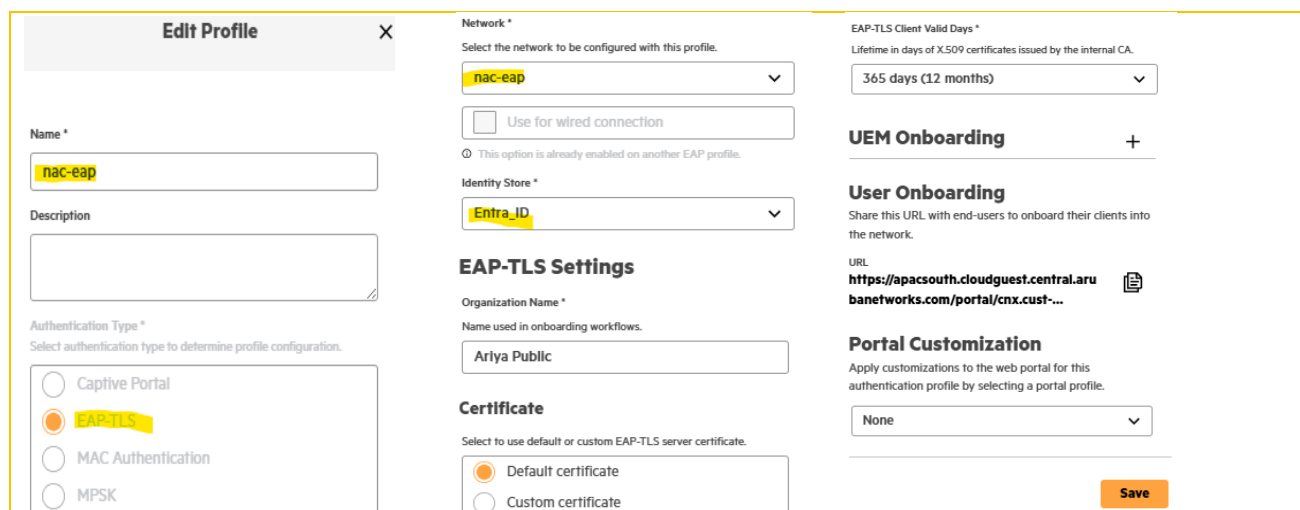
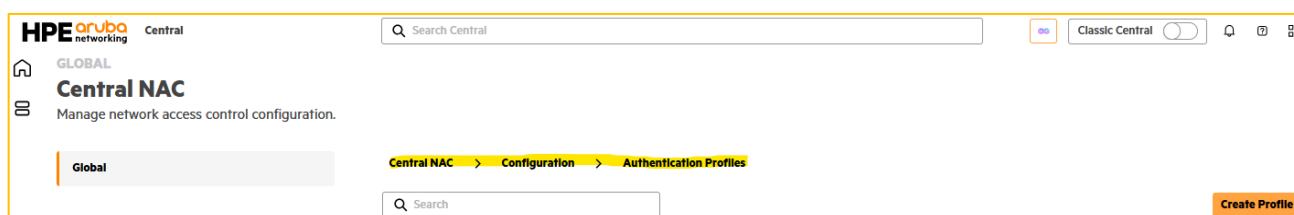
Now back in Central NAC, save the Identity store configuration and after a while you should see a green status next to it.



2.5 Authentication Profiles

The next thing we need to configure is the authentication profile where we specify how which WLANs should be authenticated and what identity store to use.

So, we navigate to Authentication Profile and create a new profile.



The UEM onboarding you see in the above screen shot, is if you have Intune or JAMF extension integration, here I don't have that setup, so we skip it.

The Onboarding URL is as pasted below and is used for client onboarding.

```
https://apacsouth.cloudquest.central.arubanetworks.com/portal/cnx.cust-46efde6c02...9f/passpoint
```

Lastly you can customise the onboarding portal as well. Here I have chosen not to customise it. And once you save it, the authentication profile will be as shown below.

Central NAC > Configuration > Authentication Profiles

Create Profile

8 items

Name	Authentication Type	Assigned Network	Identity Store
Branch			
mac-t			MAC Address Store
mpsk			Named MPSK Store for nac-mpsk
nac-b			
nac-c			
nac-eap	EAP-TLS	nac-eap	Entra_ID

Edit Profile

View Portal

Copy Onboarding URL

Now you can hover your mouse over it and click on the ... and the three options will pop up.

Here is how the onboarding portal looks.

Welcome

To connect to the **nac-eap** network, we need to create a **network profile** for you.

Before you can add a network profile to your device, you will first need to install the HPE Aruba Networking Onboard app.

Use the buttons below to install the HPE Aruba Networking Onboard app. And then come back to this page once you have done so.



HPE Aruba Networking Onboard

Download for Windows

GET IT ON Google Play

Download on the App Store

Download for macOS

Download for Ubuntu

After you have installed the HPE Aruba Networking Onboard app, press the **Yes** button to continue.

Yes, I have the HPE Aruba Networking Onboard app

Manage my network credentials

Privacy policy License agreement

2.6 Authorisation Policies

An authorisation policy defines the sources and rules used to determine which policy rules is assigned to a user or device after successful authentication. In Central NAC, the policy is built around the following key components:

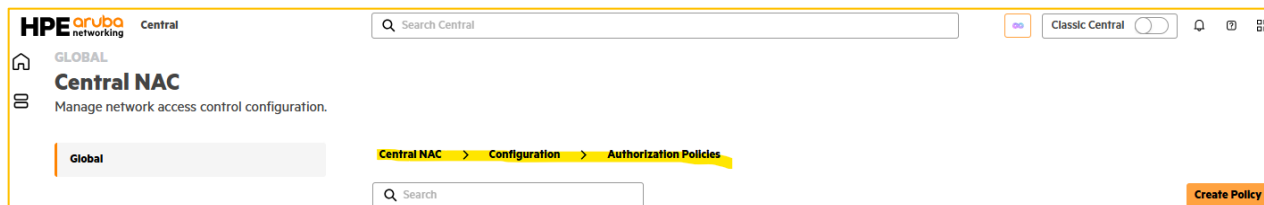
- Authorisation context
- Pre-conditions and authentication matching criteria

The authorisation context is based on the identity stores configured in Central NAC. These may include Microsoft Entra ID, Google Workspace, Okta, or the MAC address table, depending on the authentication method and deployment requirements.

Pre-conditions determine which policy is evaluated for a given authentication request. When a new policy is created, it includes only a default Deny All rule. Additional rules must be added to define the enforcement outcome, such as the user role, VLAN ID, or session timeout returned after successful authentication.

These rules allow Central NAC to apply different enforcement actions based on user, device, group, or identity-store attributes, providing flexible and consistent access control across WLANs.

Now I'll navigate to the authorisation policies and create a new one.



I'll call it EAP-TLS Policy, and I select the Entra Id identity store, and the precondition will be Authentication type equal to EAP-TLS.

Here are the other preconditions that can be added as well.

- Authentication Source = based on the configured Identity stores
- Authentication Type = MPSK, EAP-TLS, MAC Authentication Bypass (MAB), Captive Portal (CP)
- Connection Type = Wired or wireless
- NAD Vendor = AOS-Switch, Cisco/Meraki wired, Cisco/Meraki Wireless, HPE Comware wired, IETF, Juniper Mist Wireless, Juniper wired.

The image contains two side-by-side screenshots of the policy configuration forms. The left screenshot is the 'Create Policy' form, and the right is the 'Edit Policy' form. Both forms have a 'Name' field with 'EAP-TLS-Policy' entered. The 'Description' field is empty. The 'Enabled' checkbox is checked. The 'Policy Type' dropdown is set to 'Custom'. Under 'Authorization Context', the 'Identity Store' dropdown is set to 'Entra_ID'. The 'Pre-conditions' section shows a list of attributes: 'Authentication Source', 'Authentication Type', 'Connection Type', 'NAD Vendor', and 'Site'. In the 'Create Policy' form, 'Authentication Type' is highlighted. In the 'Edit Policy' form, a condition is added: 'Authentication Type' is equal to 'EAP-TLS'. The 'Add Condition' and 'Add Group' buttons are visible at the bottom of the 'Edit Policy' form.

Next, I need to add the rules under this policy. Here are my two simple rules.

Name *
allow-entra-staff

Description

Conditions
Select the matching criteria for this rule.

SSID Is equal to nac-eap

And

User Group (Entra... contains Staff

Add Condition + Add Group

Actions
Select the results to be applied to clients matching the conditions criteria. At least 1 action is required.

☒ Allow Access
☐ Deny Access

Role *
Staff

Attributes
Select an attribute

Session Timeout (hours): 1

Name *
allow-entra-student

Description

Conditions
Select the matching criteria for this rule.

SSID Is equal to nac-eap

And

User Group (Entra... contains Students

Add Condition + Add Group

Actions
Select the results to be applied to clients matching the conditions criteria. At least 1 action is required.

☒ Allow Access
☐ Deny Access

Role *
Student

Attributes
Select an attribute

Session Timeout (hours): 1

And the whole thing is as shown below. The key thing is that there is a deny All rule at the end of every policy and a Deny all policy at the end. Of course, you can hover you mouse over a rule and there will be pop-up menu where you can edit the rule, duplicate it, move the rule up and down, etc.

Central NAC > Configuration > Authorization Policies

Search

Create Policy

5 Items

	Name	Rules	Identity Store	Policy Type	Status
> 1	CloudMAC	3	MAC Address Store	Custom	Active
> 2	CloudMAC-SW	2	MAC Address Store	Custom	Active
∨ 3	EAP-TLS-Policy	7	Entra_ID	Custom	Active
	Name	Conditions	Action	Role	
1	allow-entra-staff	2	Allow	Staff	
2	allow-entra-student	2	Allow	Student	
3	allow-/				
4	allow-c				
5	allow-t				
6	suspicious Needs				
7	Deny All	0	Deny	-	
> 4	user-policy-entra-only-orig	3	Entra_ID	User	Inactive
5	Deny All Default deny for unauthorized requests	0	-	Custom	Active

Edit Rule
Move Down
Add Rule Above
Add Rule Below
Duplicate

User Onboarding

Central NAC makes secure device onboarding easier with the Aruba Onboard App. It is a good option for organisations that do not want to manage their own PKI or device management platform. If an organisation already uses PKI or device management tools, it should keep using those tools to provision devices.

Note that Central NAC also supports Bring Your Own Certificate (BYOC), which allows external PKI to be used during authentication. I'll cover in the next technote.

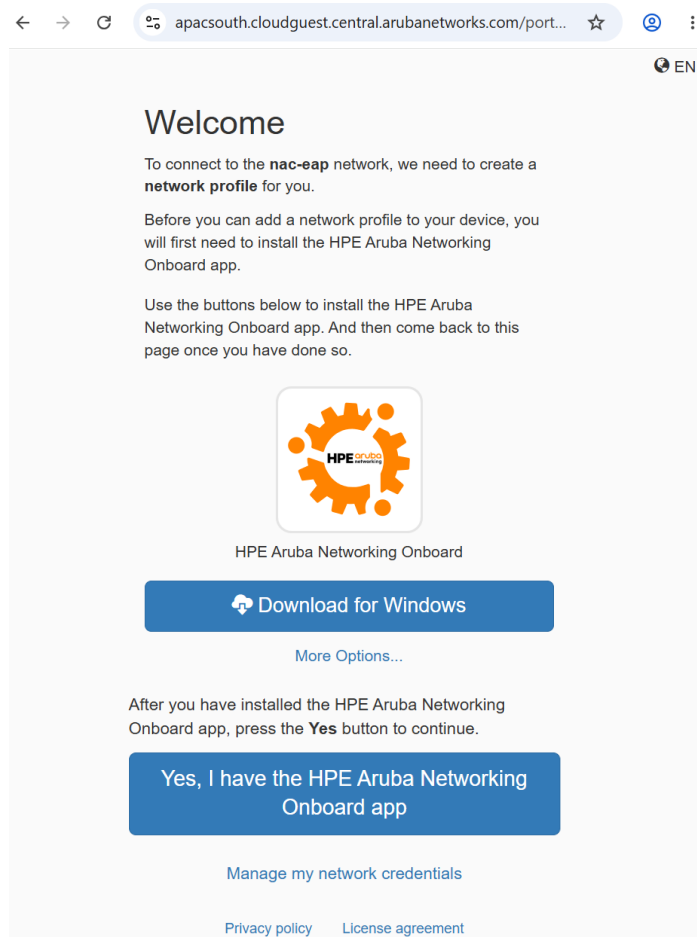
The requirements for Central NAC onboarding are

1. Sharing the onboarding URL with the users
2. The users should know their Entra credentials
3. Ensuring the user devices support the following operating systems
 - Windows 10 version 1803 or later versions
 - Windows Server 2016 or later versions
 - Android 9 or later versions
 - macOS 10.13 or later versions
 - iOS 12.1 or later versions

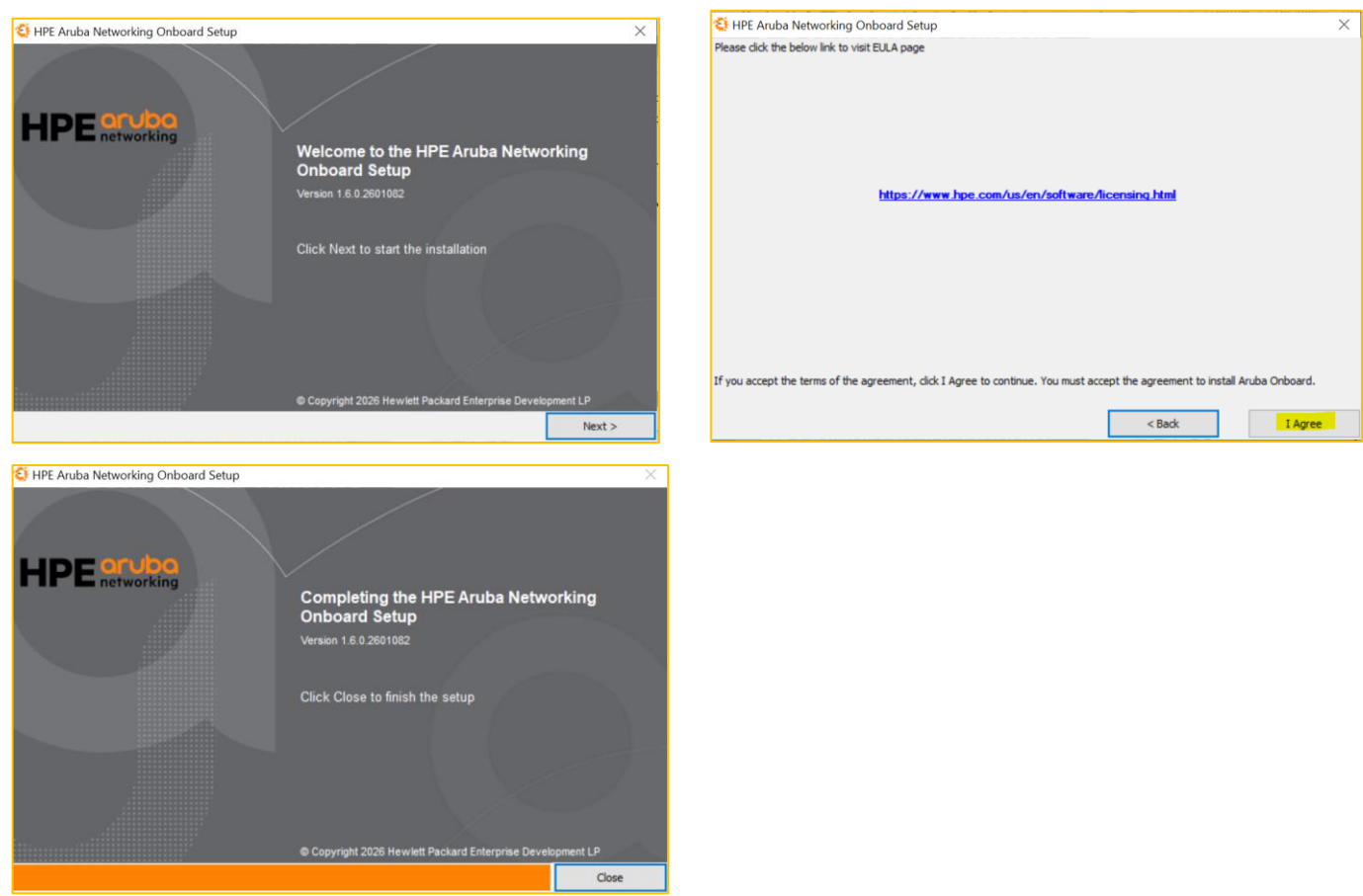
Aruba Central NAC uses Passpoint to provide ease of access. The idea here is that we can send this onboarding URL to the users so they can get connected to this WLAN which is being authenticated with Central NAC.

2.7 Staff1 Onboarding Using Onboarding App

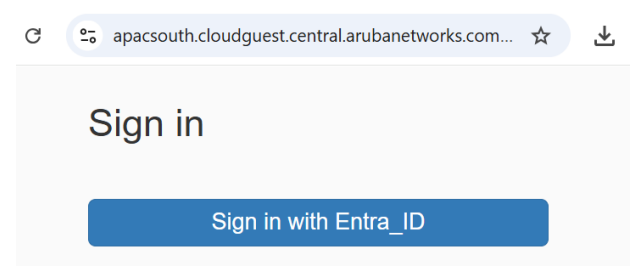
Remember the onboarding URL is under Central NAC >> Authentication profile. Now the staff1 user browses to the onboarding URL, and this is their workflow.



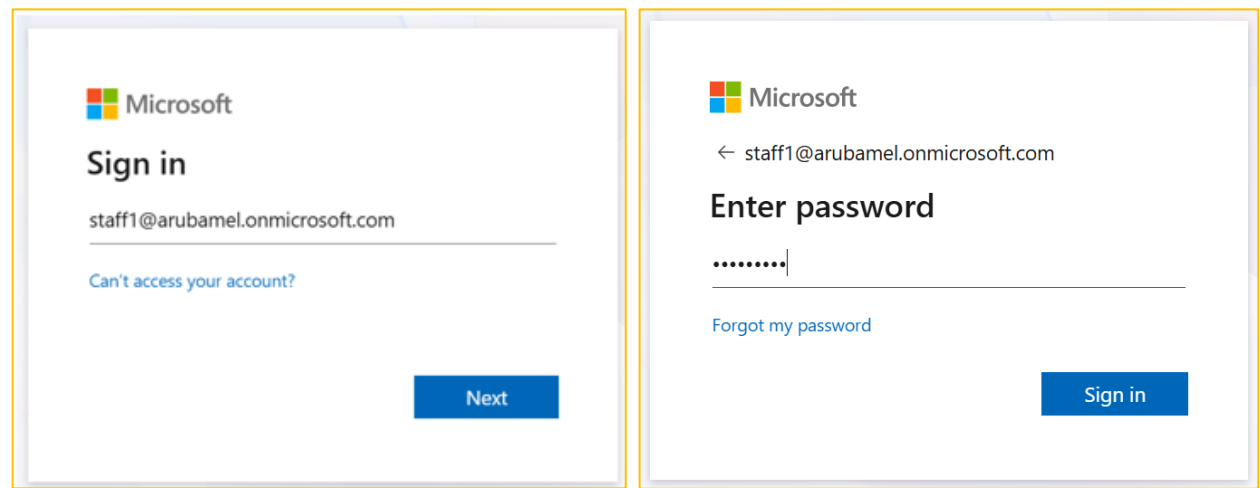
Since this is the first time the user is onboarding, they need to download HPE Aruba Networking Onboard App. Because I am using a windows laptop, it is automatically showing the windows options. So now I have downloaded it and will install it.

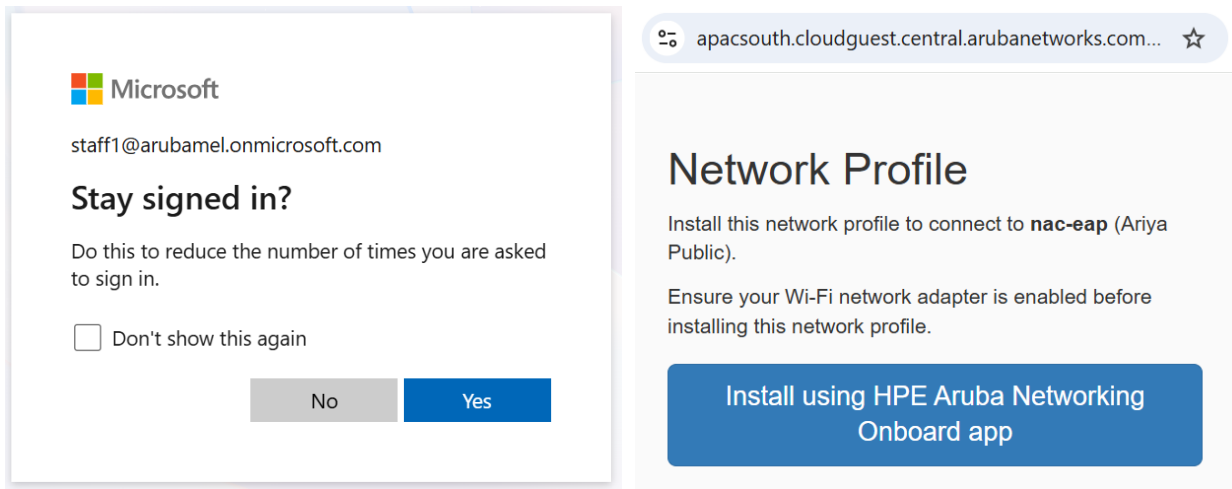


Once it is installed from the browser, click on the “Yes I have the Onboard App” button. This will start the Entra ID authentication.

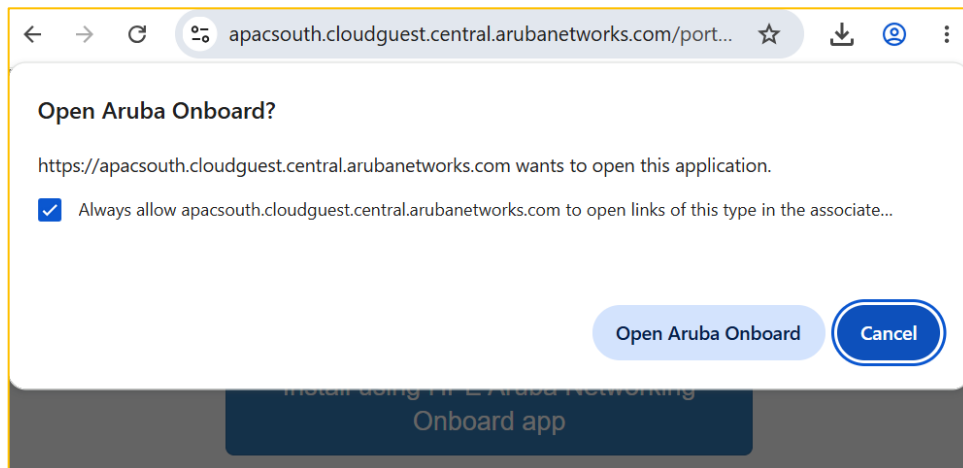


after which the user gets presented with the following

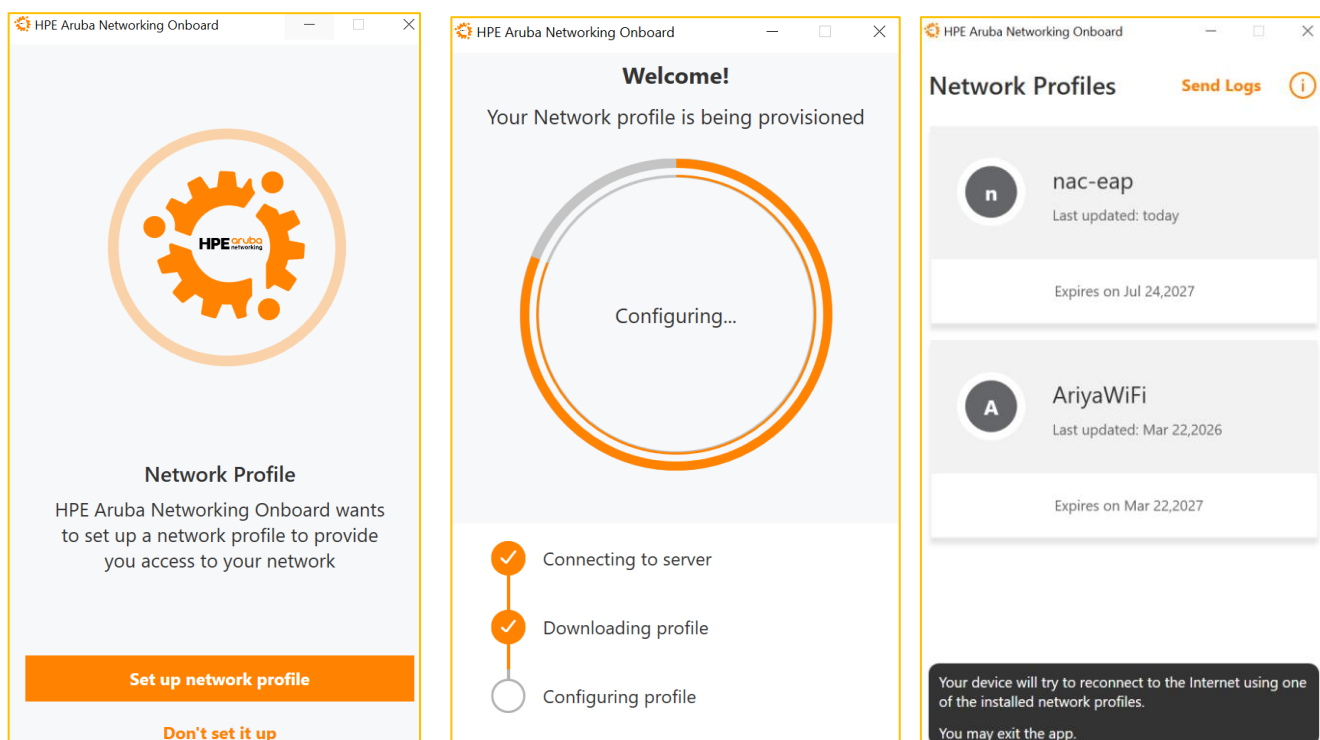




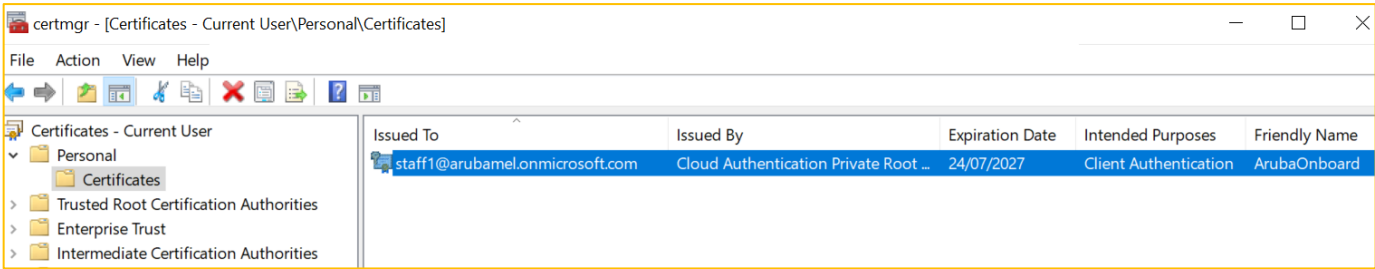
Now after successful authentication, Onboard App will install the Network Profile.



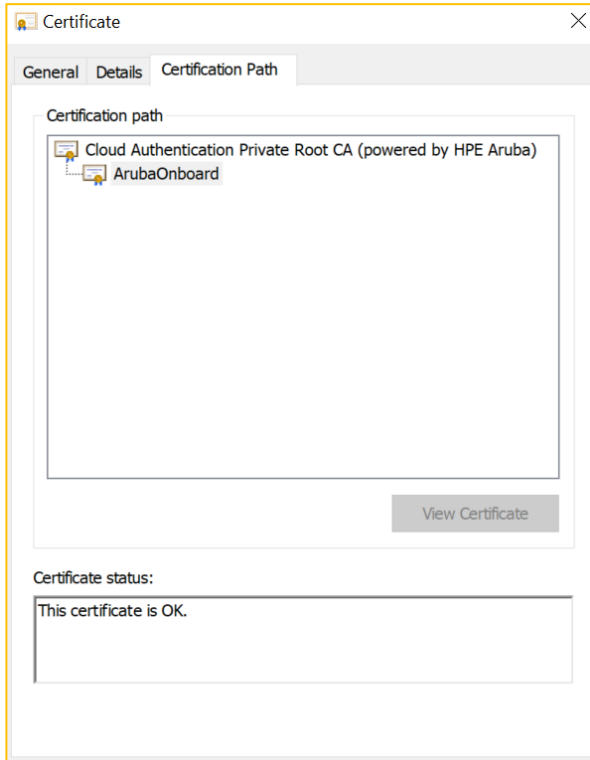
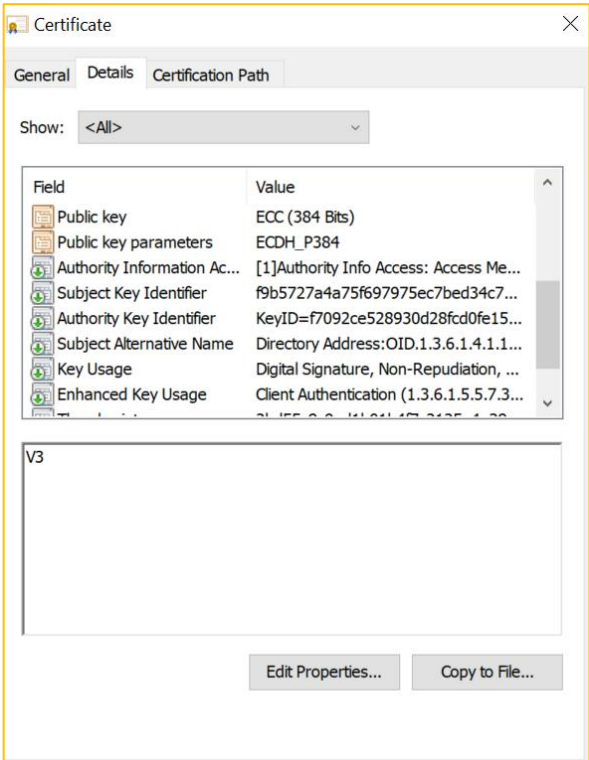
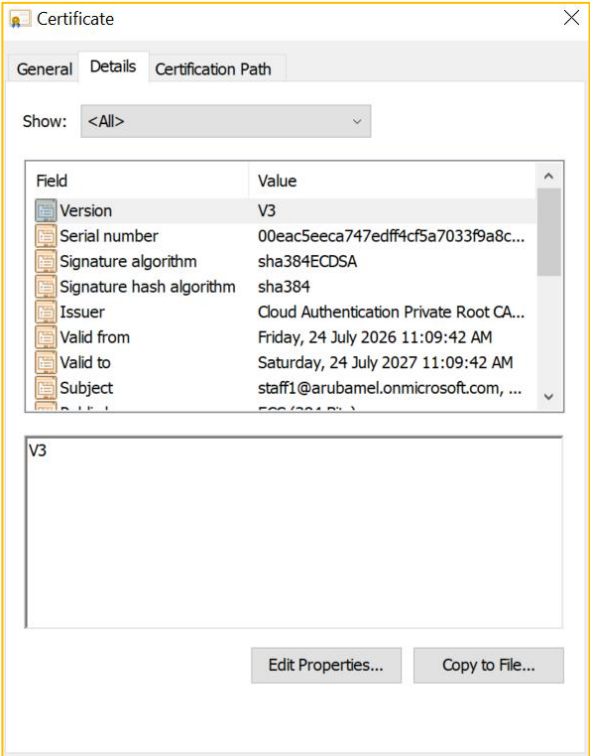
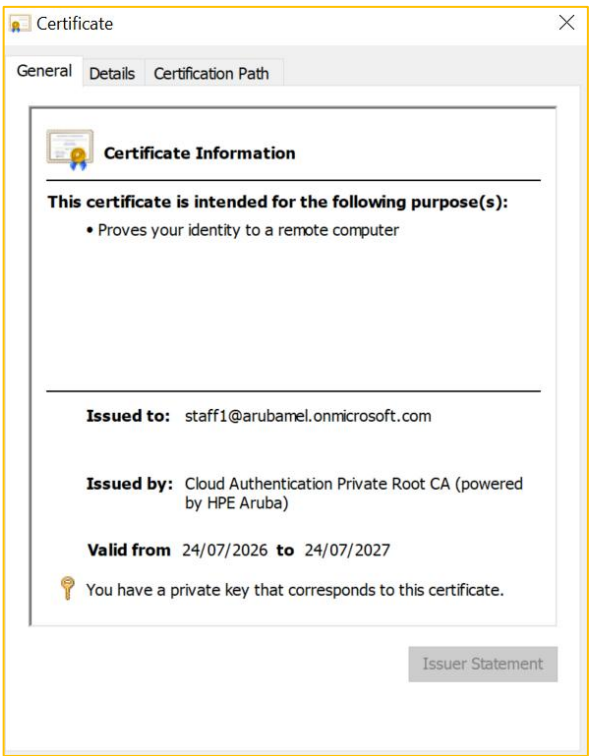
And here are the exact steps which is basically clicking on set up network profile and then waiting for it to finish.



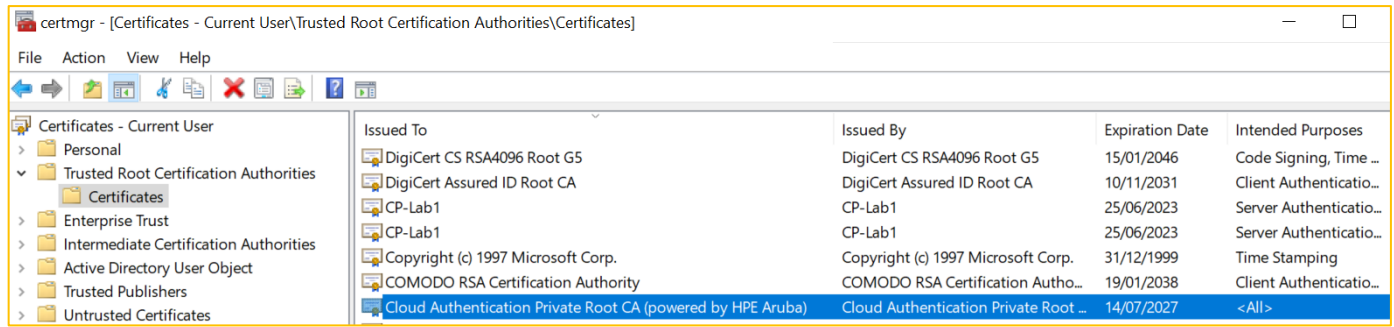
For the curious, you can check the user certificates to see the certificate that Central NAC just installed.



As you can see it is installed and issued by Cloud Authentication from HPE Aruba.



And here is trusted root CA certificate.



Note that not all older devices support hotspot 2.0. The way to find that out is by using this command and checking for Access Network Query Protocol (ANQP) support.

```
C:\>netsh wlan show wirelesscapabilities
```

Wireless System Capabilities

```
-----
Number of antennas connected to the 802.11 radio (value not available)
Max number of channels the device can operate on, simultaneously (value not available)
Co-existence Support : Unknown
```

Wireless Device Capabilities

```
-----
Interface name: Wi-Fi
                <other lines removed>

Wi-Fi Direct Client : Supported
Protected Management Frames : Supported
DOT11k neighbor report : Supported
ANQP Service Information Discovery : Supported
Action Frame : Supported
Diversity Antenna : Supported
IBSS : Not Supported
                <other lines removed>
```

```
C:\>
```

Hotspot 2.0 is a Wi-Fi Alliance specification based on the 802.11u protocol, which allows wireless clients to discover hotspots using management frames (such as beacon, association request and association response), connect to networks, and roam between networks without additional authentication.

ANQP provides a range of information, such as IP address type and availability, roaming partners accessible through a hotspot, and the Extensible Authentication Protocol (EAP) method supported for authentication, for a query and response protocol. The ANQP Information Elements (IEs) provide additional data that can be sent from an AP to the client to identify the AP's network and service provider.

2.8 User Self-Service Option

Central NAC also includes a user self-service option that allows users to view the network credentials issued to them, including credentials linked to their individual devices.

This improves the user experience by reducing reliance on IT for basic certificate management tasks. For example, if a device is lost, replaced, or potentially compromised, the user can access the self-service portal and revoke the relevant certificate directly.

The screenshots below show how users can select “Manage my network credentials” at the bottom of the onboarding page. The onboarding URLs are available under Central NAC >> Authentication profile.

After opening the URL and selecting Manage my network credentials, the user is prompted to sign in with their Entra credentials.

Welcome

To connect to the **nac-eap** network, we need to create a **network profile** for you.

Before you can add a network profile to your device, you will first need to install the HPE Aruba Networking Onboard app.

Use the buttons below to install the HPE Aruba Networking Onboard app. And then come back to this page once you have done so.



HPE Aruba Networking Onboard

 **Download for Windows**

[More Options...](#)

After you have installed the HPE Aruba Networking Onboard app, press the **Yes** button to continue.

Yes, I have the HPE Aruba Networking Onboard app

Manage my network credentials

[Privacy policy](#) [License agreement](#)

Sign in

Sign in with Entra_ID

 Microsoft

Pick an account

 staff1@arubamel.onmicrosoft.com

Use another account

 Microsoft

← staff1@arubamel.onmicrosoft.com

Enter password

.....

[Forgot my password](#)

Sign in

They will then be presented with the credential management page, where they can review the network credentials associated with their account and devices. From here, users can easily see which credentials are currently valid, which ones have expired, and which ones have already been revoked. This gives them better visibility into their own network access and makes it easier to manage common scenarios such as replacing a device, retiring an old device, or removing access for a device they no longer use.

Self-Service

Network credentials

Below is a list of network credentials that have been **issued to you** for use on **your devices**.

If your device has been lost, or its security breached, you **should** revoke any credentials that have been issued to it.

☒ All ☐ None

 Refresh

 Revoke Selected



☒ SPECTRELAB (HP HP X360 SPECTRE)	24 Jul 2026, 11:09	Valid	
Device SPECTRELAB (HP HP X360 SPECTRE)			
Status Valid			
Issued at Friday, 24 July 2026 at 11:09			
Expires at Saturday, 24 July 2027 at 11:09			
		Close  Revoke	

Self-Service

Network credentials

Below is a list of network credentials that have been **issued to you** for use on **your devices**.

If your device has been lost, or its security breached, you **should** revoke any credentials that have been issued to it.

☒ All ☐ None

 Refresh

 Revoke Selected



☒ SPECTRELAB (HP HP X360 SPECTRE)	24 Jul 2026, 11:09	Valid	
Device SPECTRELAB (HP HP X360 SPECTRE)			
Status Valid			
Issued at Friday, 24 July 2026 at 11:09			
Expires at Saturday, 24 July 2027 at 11:09			
		Close  Revoke	

☒ Show valid credentials
☐ Show expired credentials
☐ Show revoked credentials

User Testing

2.9 Audit Trail

Let's have a quick look at the audit trail to see some of the changes we have made. To navigate to it, you need to click on the burger icon  and then choose **Audit Trail**. There you can change the duration and also search for specific strings.

Here you can see who has made the changes and the details of the changes.

Classic Central
☒

Audit Trail

View the activities that impact the network.

Last 3 hours
▼

Occurred On	Action	Category	Sub-Category	Destina...	Destination Name	Description	Source
07/01/2026, 8:52:48 PM	Configuration Sync	Central NAC	Authorization Policy	Global	-	Configuration sync for (name=user-policy-entra-only-orig) succeeded	System
07/01/2026, 8:52:45 PM	Policy updated	Central NAC	Authorization Policy	Global	Global	Authorization Policy "user-policy-entra-only-orig" updated	ariyap@hpe.cor
07/01/2026, 8:27:00 PM	Configuration Sync	Central NAC	Authorization Policy	Global	-	Configuration sync for (name=EAP-TLS-Policy) succeeded	System
07/01/2026, 8:26:58 PM	Policy updated	Central NAC	Authorization Policy	Global	Global	Authorization Policy "EAP-TLS-Policy" updated	ariyap@hpe.cor
07/01/2026, 8:26:54 PM	Configuration Sync	Central NAC	Authorization Policy	Global	-	Configuration sync for (name=EAP-TLS-Policy) succeeded	System
07/01/2026, 8:26:52 PM	Policy updated	Central NAC	Authorization Policy	Global	Global	Authorization Policy "EAP-TLS-Policy" updated	ariyap@hpe.cor
07/01/2026, 8:26:34 PM	Configuration Sync	Central NAC	Authorization Policy	Global	-	Configuration sync for (name=EAP-TLS-Policy) succeeded	System
07/01/2026, 8:26:32 PM	Policy updated	Central NAC	Authorization Policy	Global	Global	Authorization Policy "EAP-TLS-Policy" updated	ariyap@hpe.cor

And here is the audit trail for some of the policies that I was updating

Configuration Update

Policy updated

Occurred On

07/01/2026, 8:52:45 PM

Category

Central NAC

Sub-Category

Authorization Policy

Destination

Global

Destination Name

Global

Source

arfyap@hpe.com

Description

Authorization Policy "user-policy-entra-only-orig" updated

Before

1

policy:

2

-

3

policy-id: 2491b9a5-a054-4b4b-8923-5a3680be587c

4

-

enable: true

After

1

policy:

2

-

3

policy-id: 2491b9a5-a054-4b4b-8923-5a3680be587c

4

+

enable: false

Impact Radius

i

Devices with local overrides for this change will not be affected.

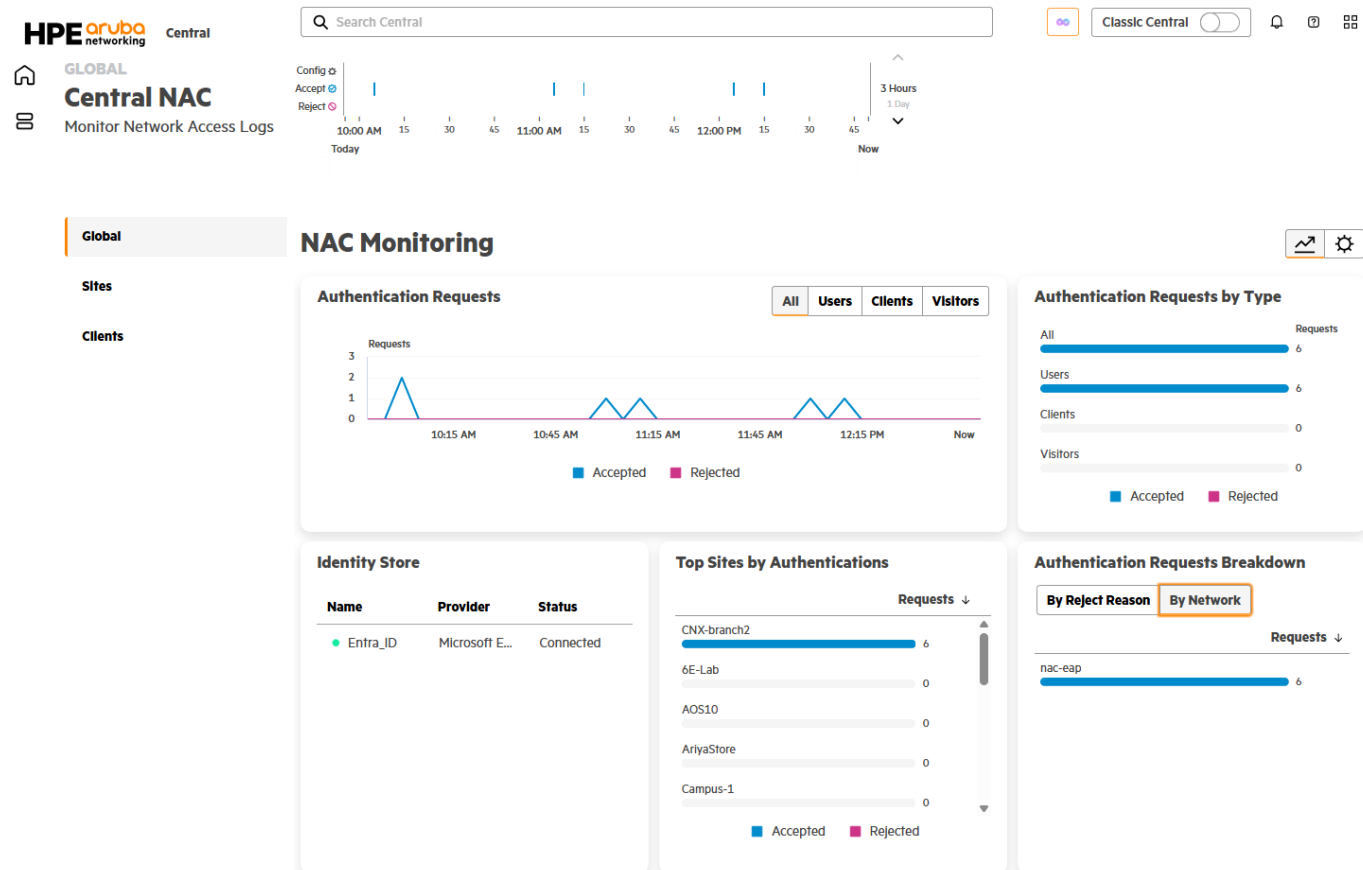
Applies to all devices under global.

2.10 User Connectivity

Now we get two clients to connect to the nac-eap WLAN, and the authentication flow will be as follows

Central NAC and Entra ID Authentication Flow				
1. User Device Connects to WLAN	2. Bridge Mode AP Forwards auth request	3. Central NAC Applies authentication profile and policy logic	4. Microsoft Entra ID Validates identity and returns attributes	5. Network Role Access role is assigned to the client

The two users onboarded as Staff and Student. Based on our authorisation policies they should be put into different roles. Here is the view of New Central.



You can look at the break down of clients and you can further customise the columns that are shown.

GLOBAL Central NAC
Monitor Network Access Logs

Clients

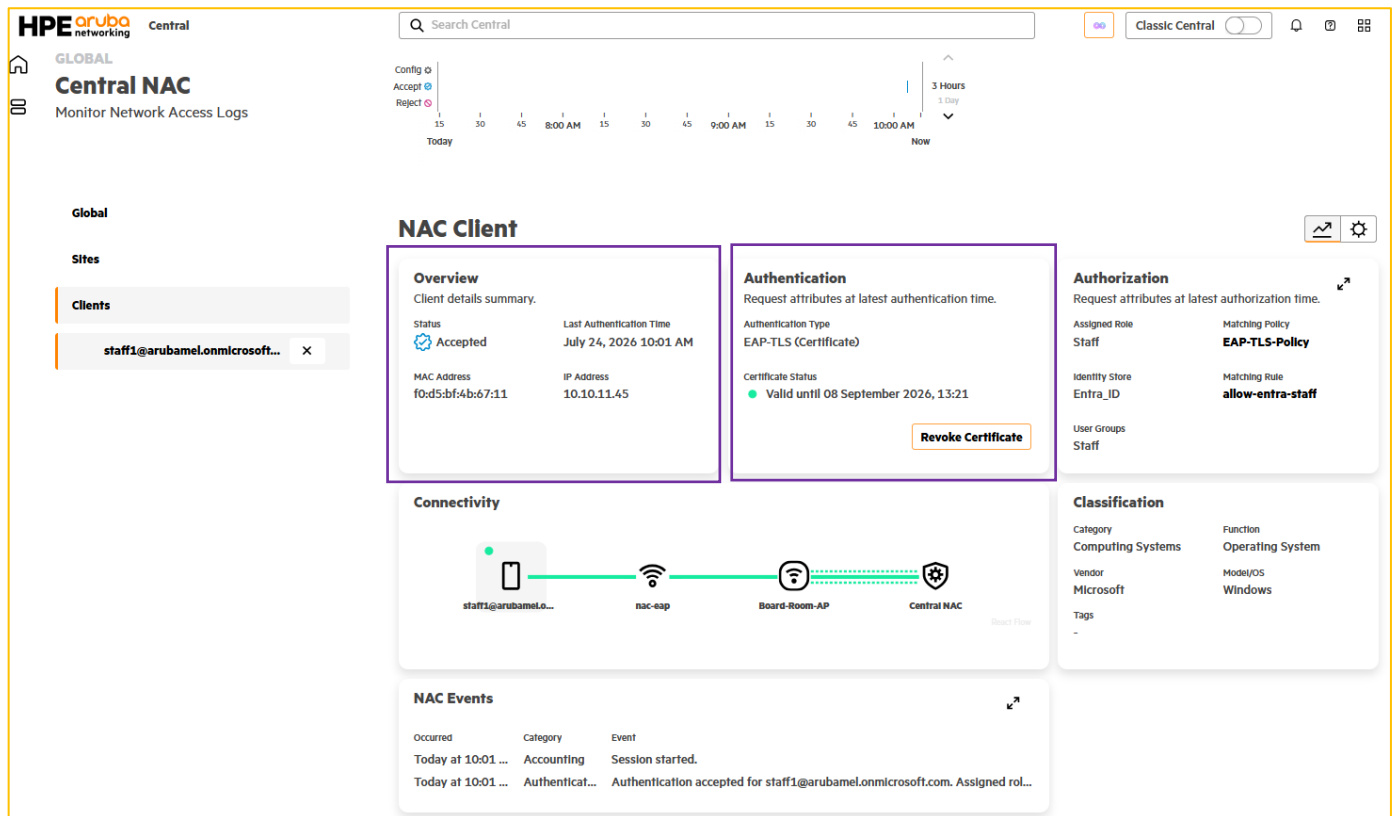
Status: Accepted Rejected Connection Type: Wireless Wired Access Type: Users Clients Visitors

Search

2 items

Name	Connec...	MAC Address	IP Address	WLAN	Role	Site	Last Auth...
staff1@arubamel.onmicrosoft.com Accepted	Wireless	f0d5:bf4b:67:11	10.10.11.45	nac-eap	Staff	CNX-branch2	07/24/2026, ...
student2@arubamel.onmicrosoft.com Accepted	Wireless	a088:b4:50:c0:84	10.10.12.31	nac-eap	Student	CNX-branch2	07/24/2026, ...

Clicking on the client's name will provide the details of that specific authentication as shown below.



This concludes our technote.

For comprehensive configuration detail for Central NAC can refer to [TechDocs-NAC](#)

You can also refer to the [Central NAC Overview documentation](#).