1 Table of Contents

1.1 Revision History

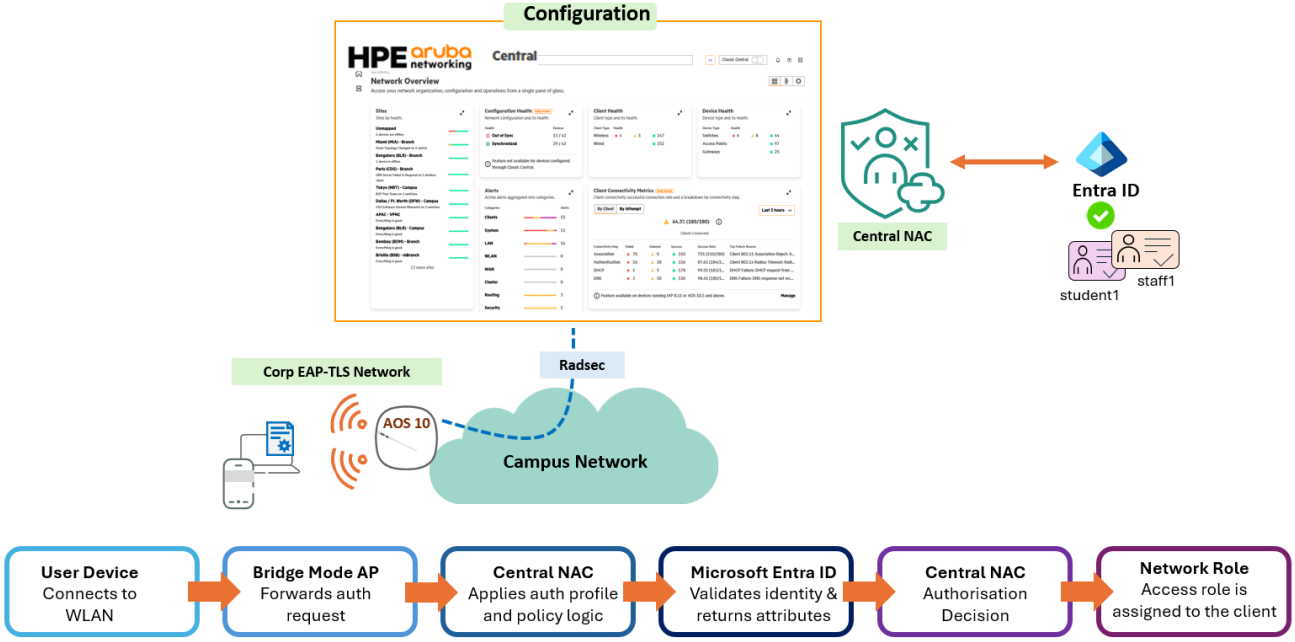
DATE	VERSION	EDITOR	CHANGES
10 Jul 2026	0.1	Ariya Parsamanesh	Initial creation
04 Aug 2026	0.2	Ariya Parsamanesh	Added the testing section
08 Aug 2026	0.3	Ariya Parsamanesh	Added the self-service option of the enrolment

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 Cenrtifcate (BYOC)
- Integration with multiple IDPs
- Third party NAD support
- Support for unlimited MPSK
- 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:

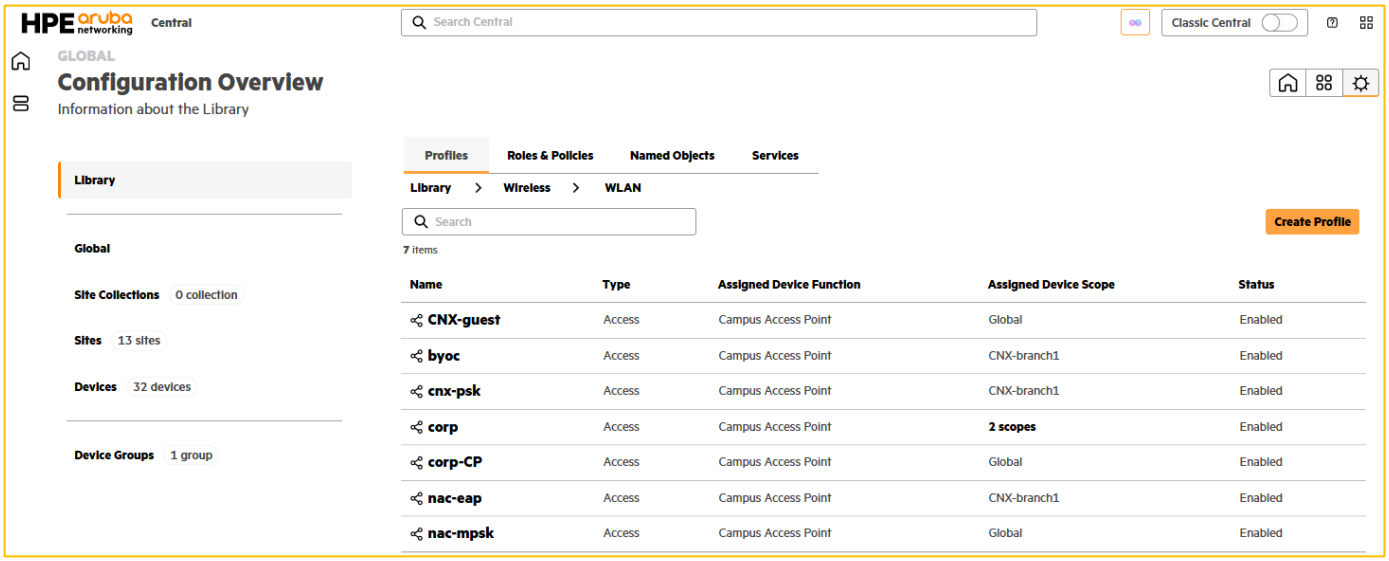
- WLAN and user roles configuration
- Entra ID configuration
- CNAC Identity Stores configuration and its Authentication Profiles and Authorization Policy configuration

2.1 Things you need

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

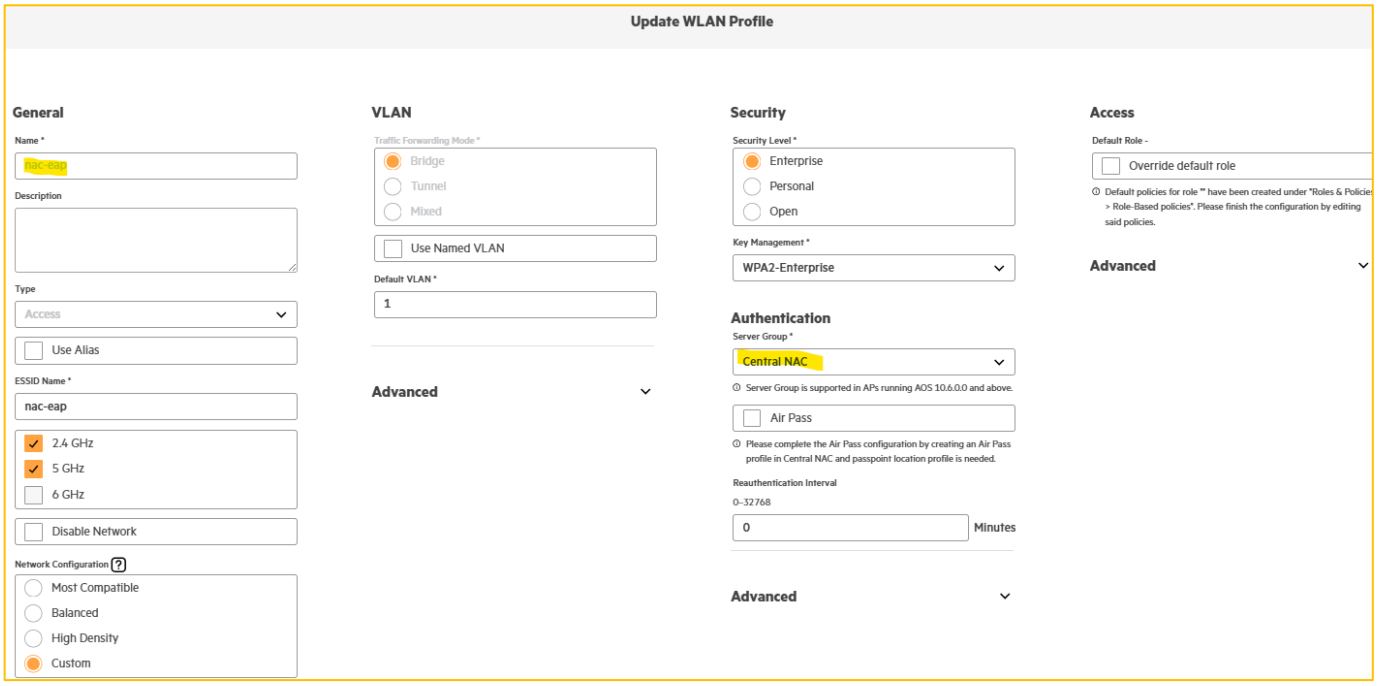
WLAN and User Role Configuration

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.



2.2 NAC-EAP WLAN

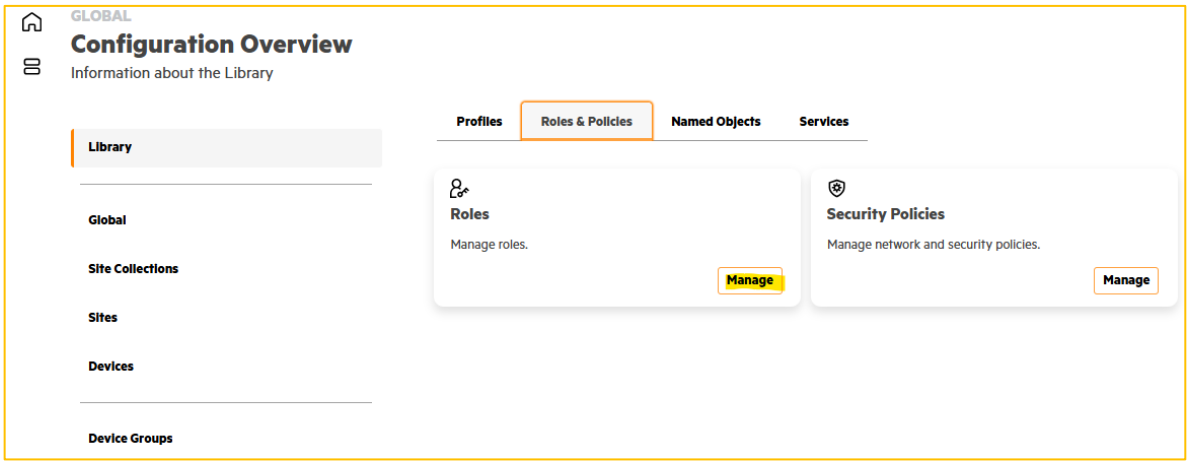
This is to authenticate against Entra identity store. The WLAN is called "nac-eap" and it's authentication server group will be Central NAC.



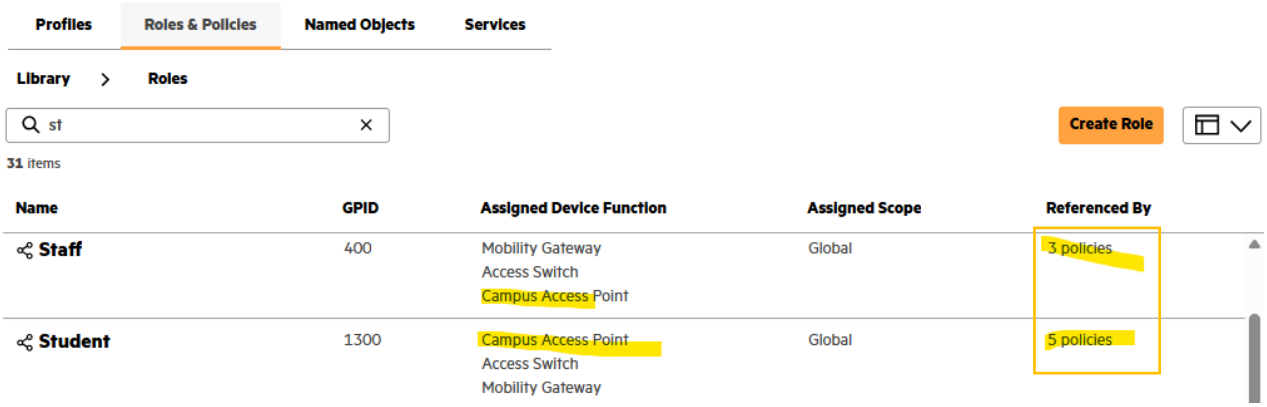
2.3 User Role configuration

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.

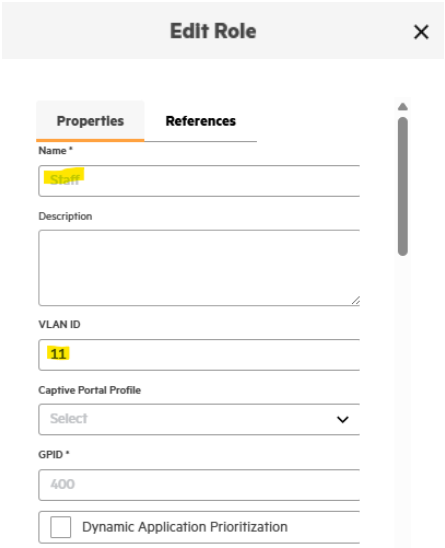
Here I'll go through the configuration of user roles and related policies. In most cases, you want to use the same user roles for your wired and wireless users. I'll start from the library level.

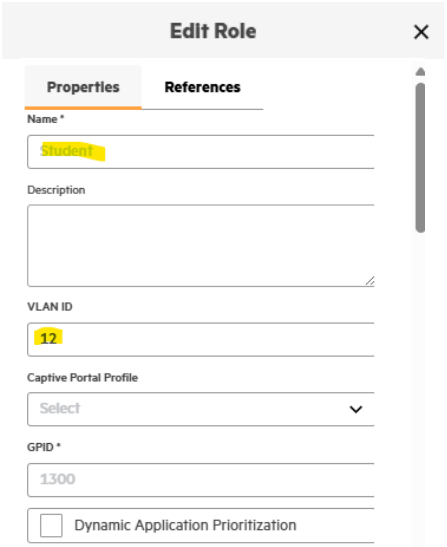


I'll create two roles, Staff and Student. Let's look the roles that I created before.

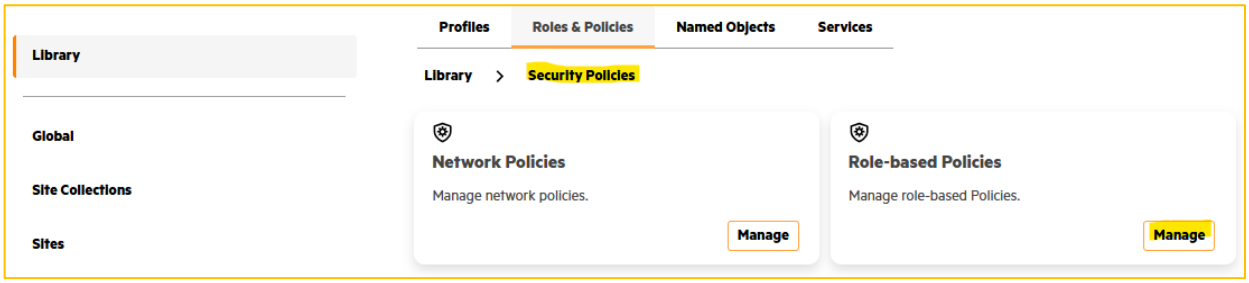


Here I am showing only what is relevant to the wireless users. You can also configure parameters that are specific to LAN switches. Also note the number of policies each of the roles have.



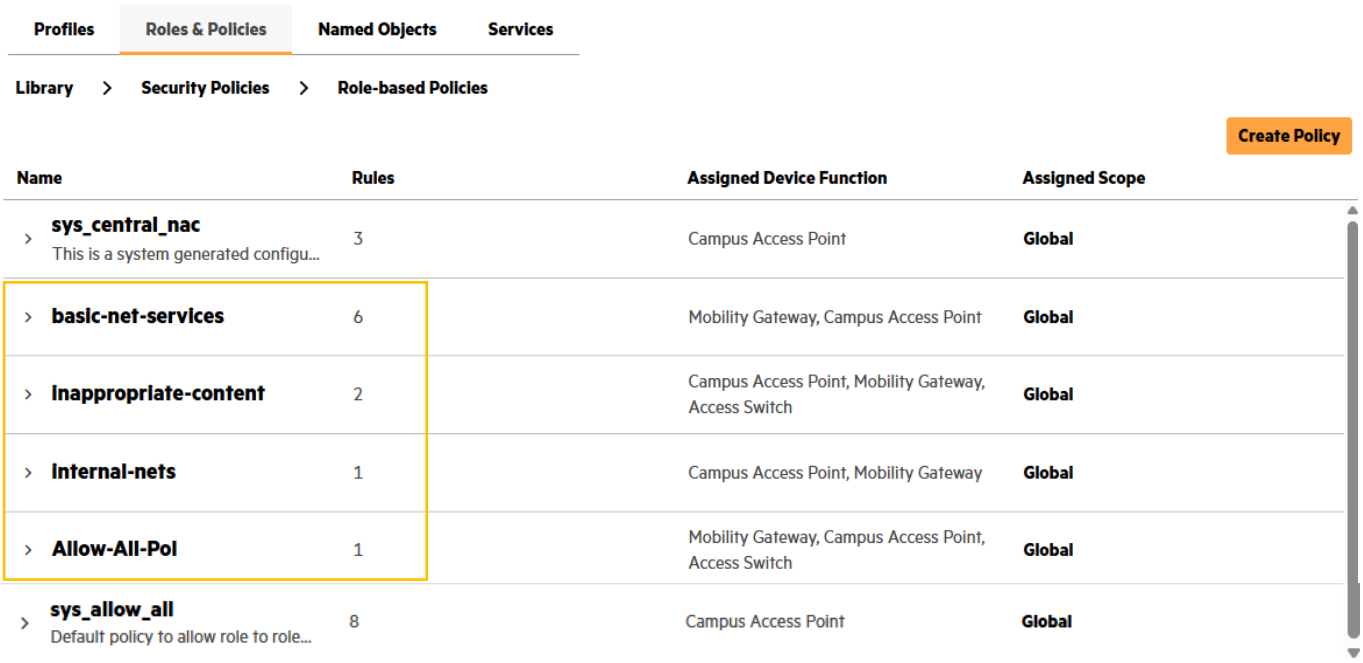


Here for this role that we'll use for our bridge only WLAN, the VLAN id for Staff and Student are 11 and 12 respectively. Next, we go to the Security policies and choose Role-based Policies.



Few points about security policies

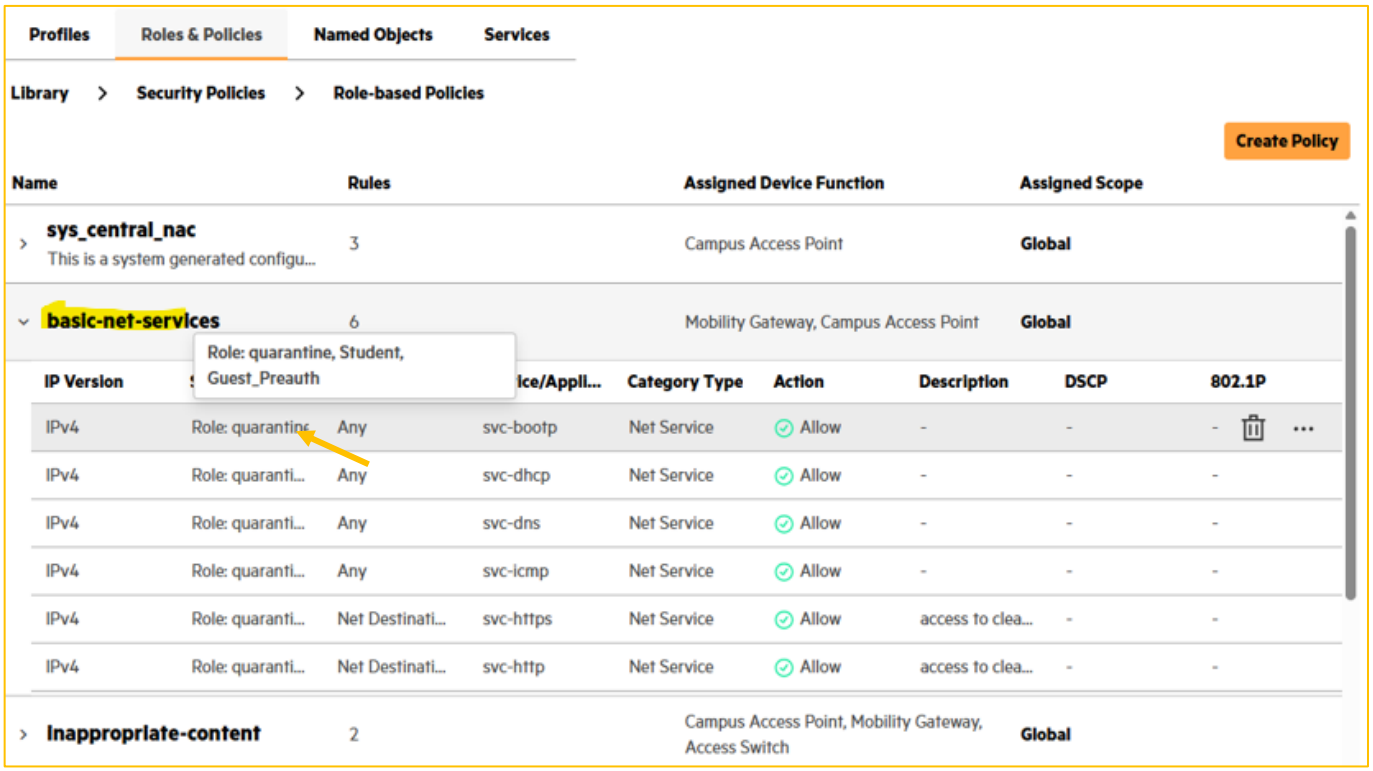
- Security Policies are still applied to scopes and device functions.
- The security policies are processed in a top-down fashion until a match is found.
- Policies can be assigned to multiple roles.
- Anything that starts with "sys_" is system generated. Shown below we have two. The sys_allow_all is 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 polices 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.



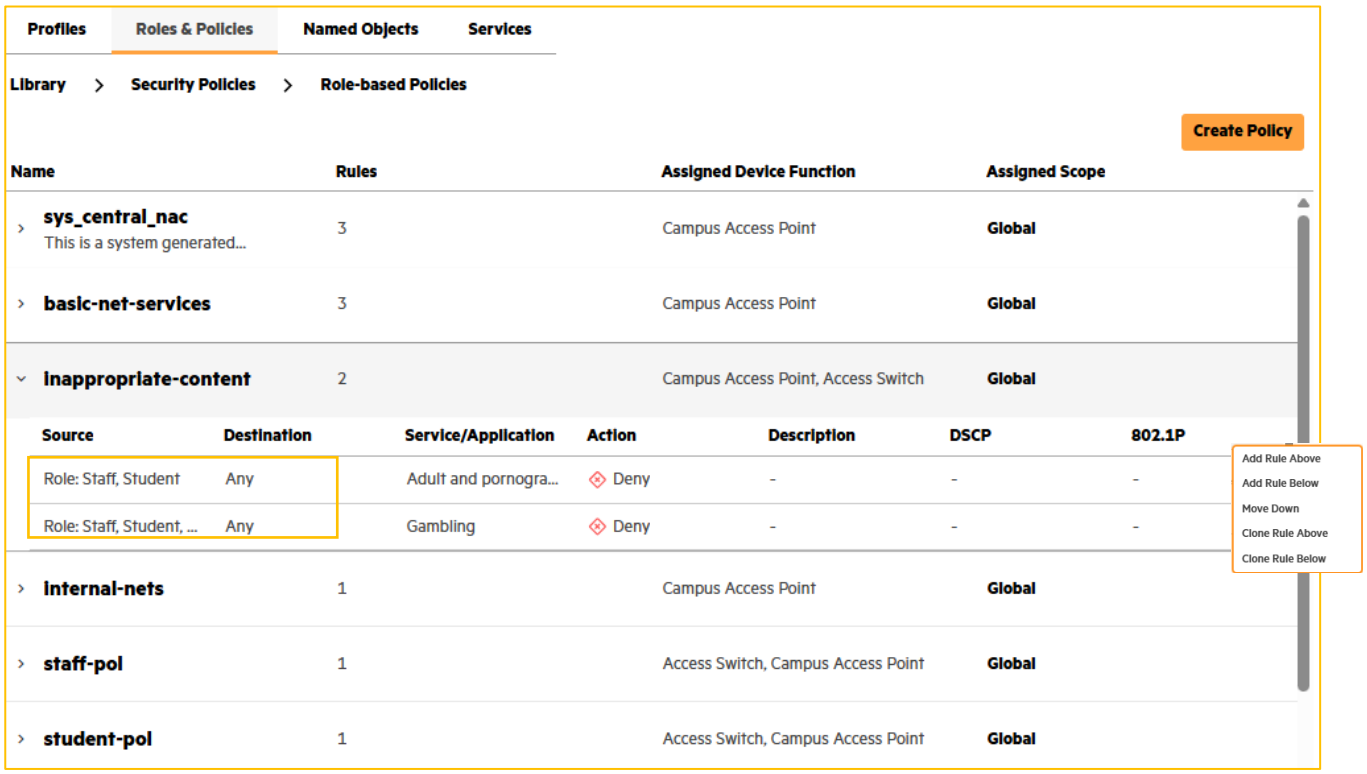
I have 4x policies that I created, and each policy consists of a set of rules and are assigned to multiple roles.

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.



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.



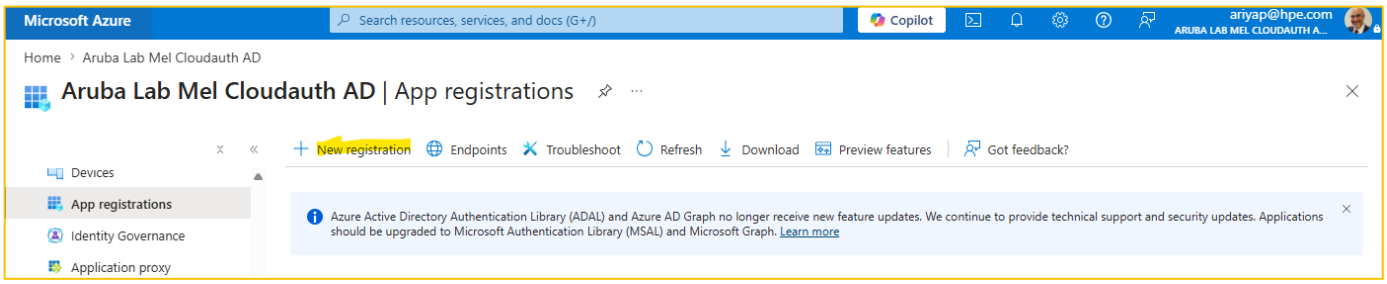
When you hover your mouse over a rule, "**...**" appears and by clicking on it you can bring up the rule ordering cloning pop-up. As you are reordering the policies, the order gets synced to the devices that are associated to the user-role. You can check the rules that were pushed down to the gateways 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

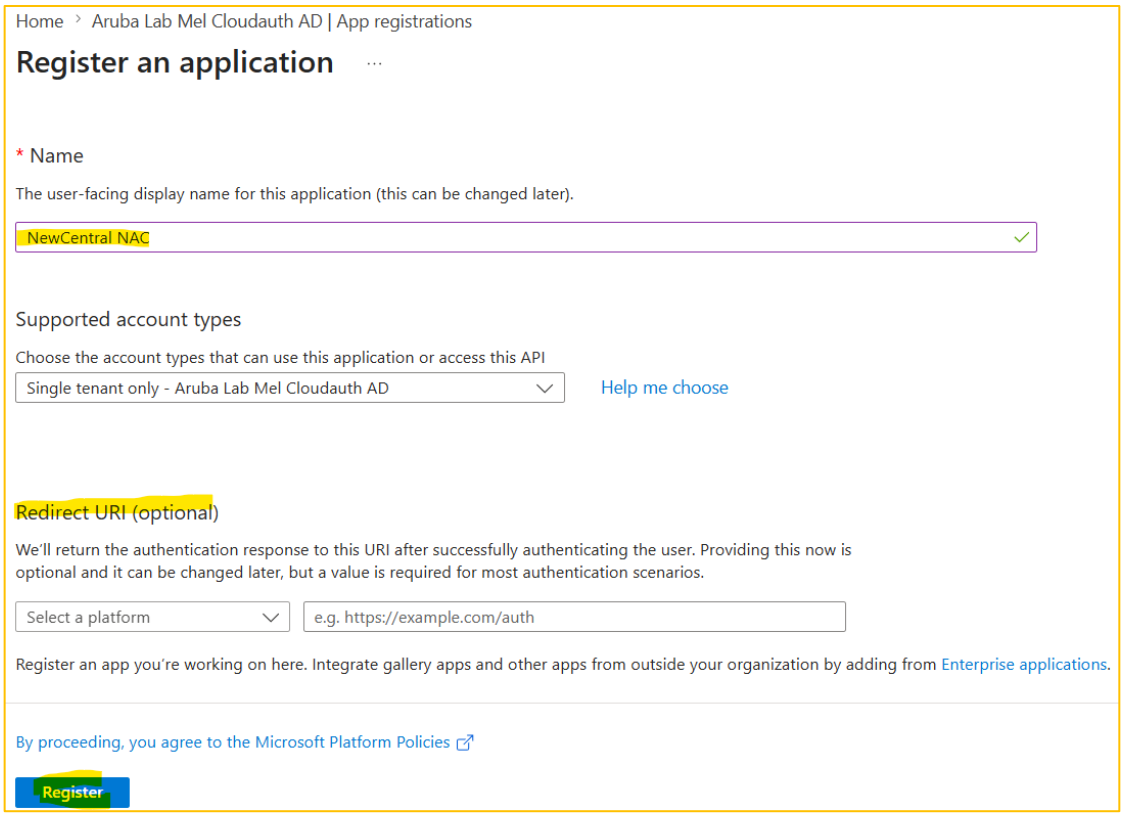
The main configuration components on Entra Id are:

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

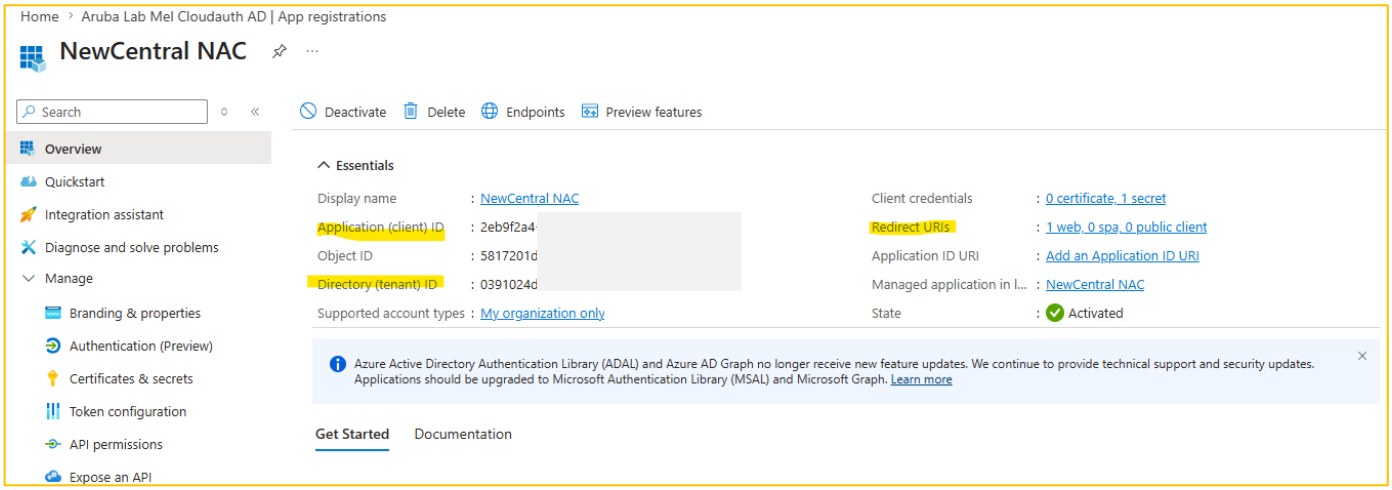
Here we'll start with the creating an application that we'll use for New Central integration. Navigate to your Entra ID service >> Manage >> App Registrations



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.



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



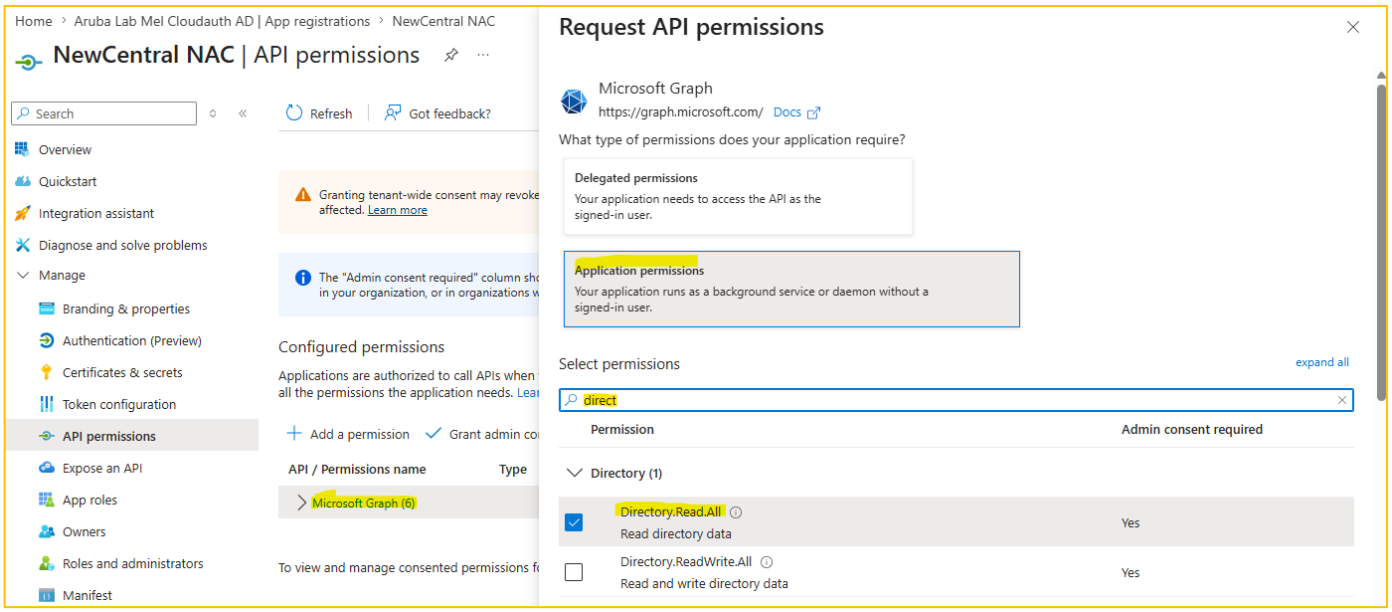
We need these IDs when we'll be configuring Central. For time being just copy it.

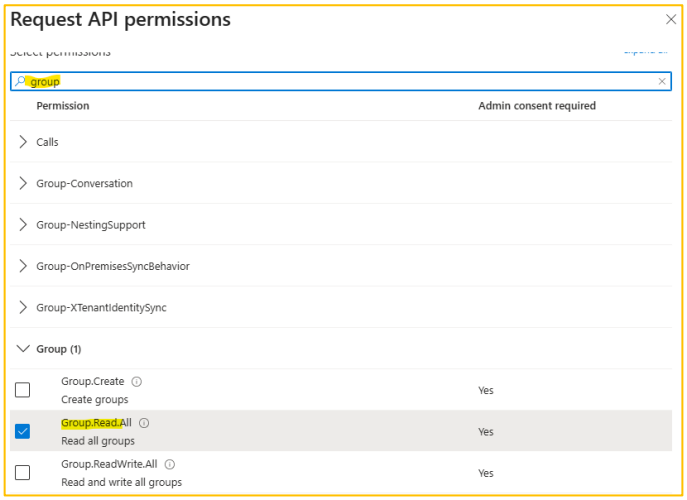
```
Application (client) ID = 2eb9f2a4-b
Tenant ID = 0391024d
```

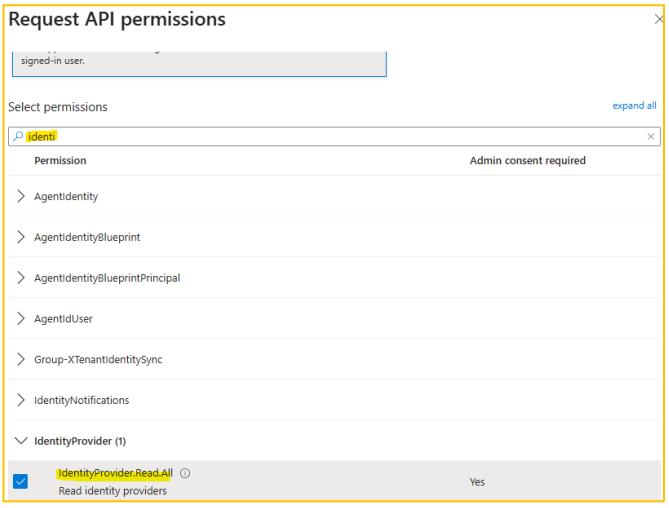
After registering the application, configure the following API permissions:

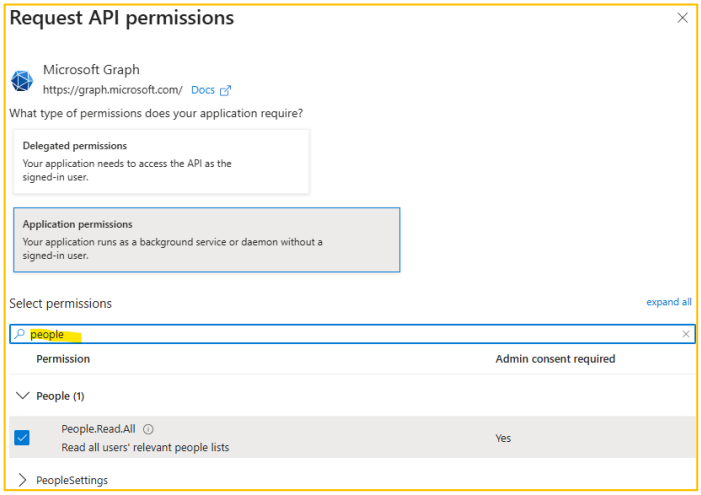
- Directory.Read.All
- Group.Read.All
- IdentityProvider.Read.All
- People.Read.All
- User.Read
- User.Read.All

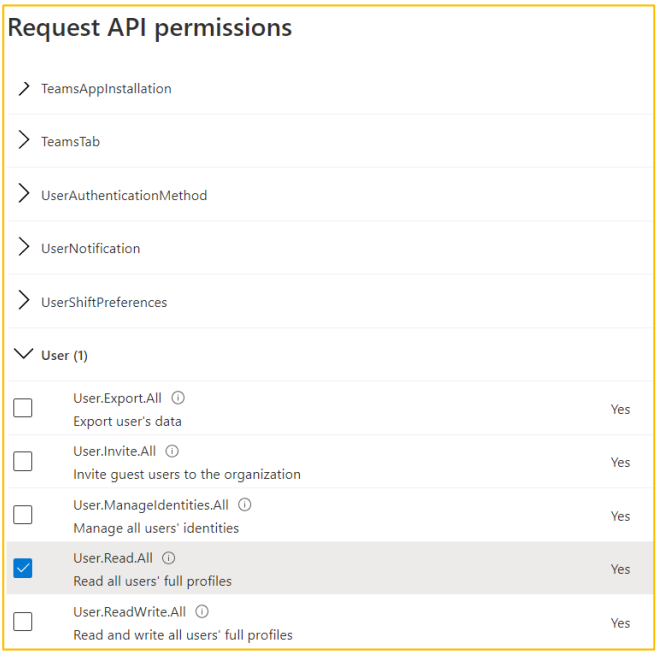
Here I am showing how to set those up.



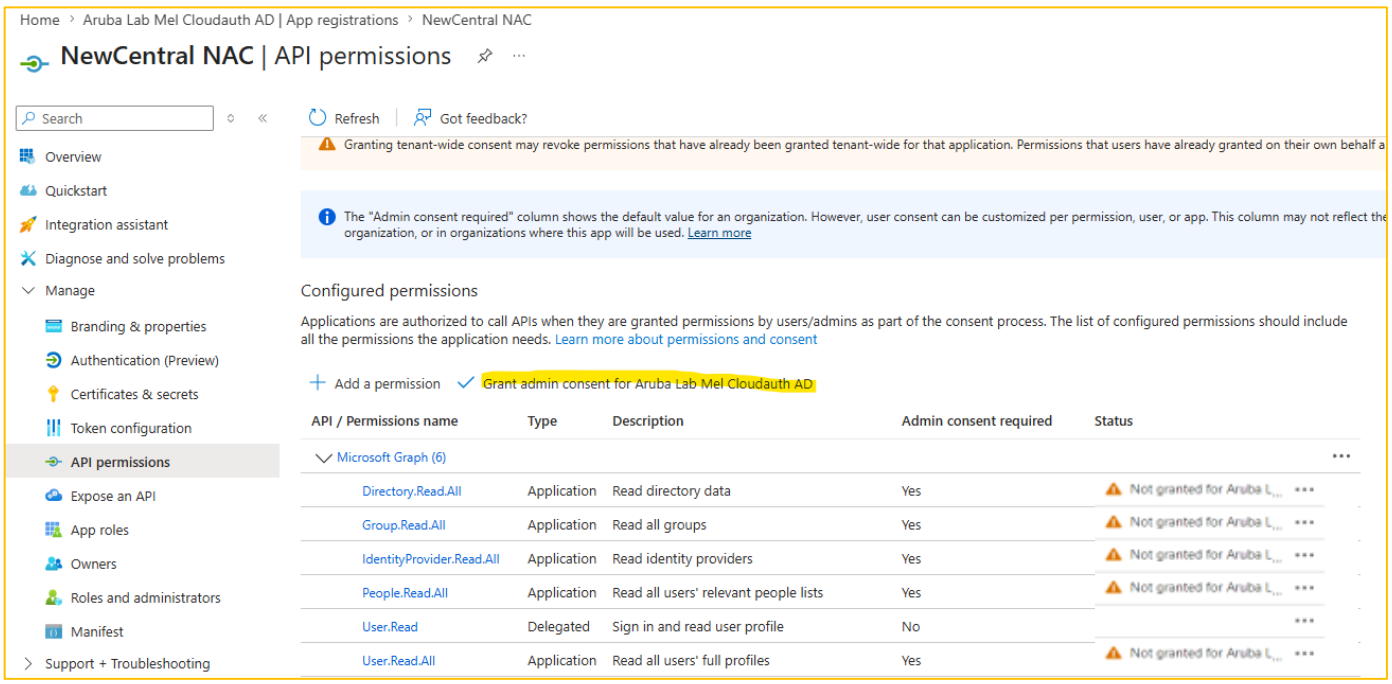




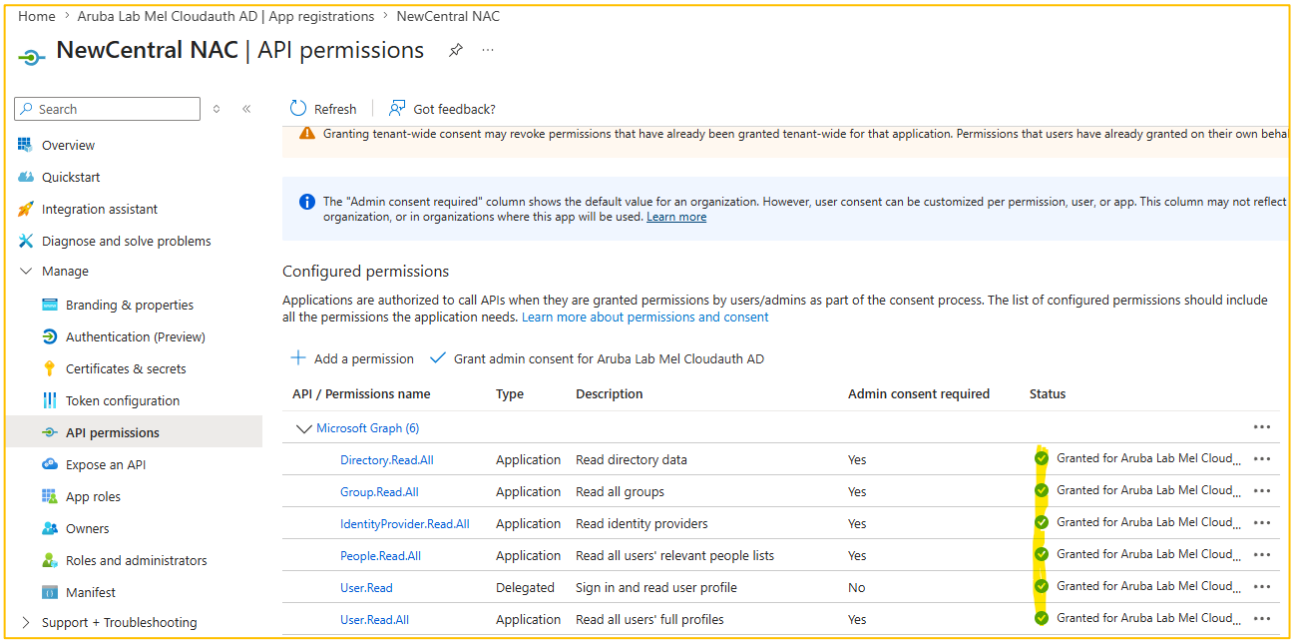




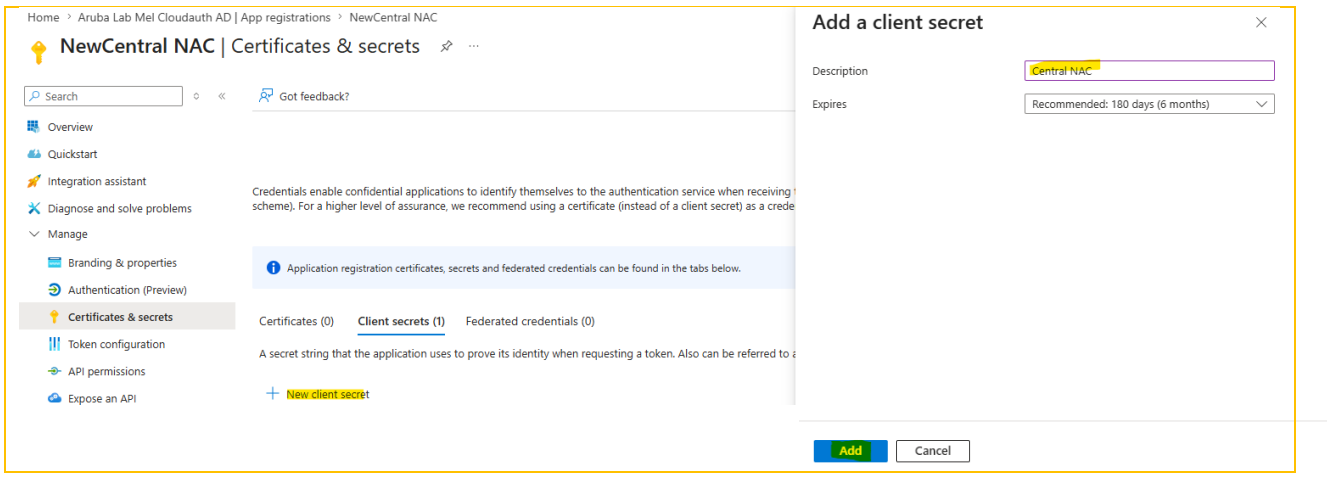
Then click on “Update Permissions”. Next we need to “Grant admin Consent” for them.



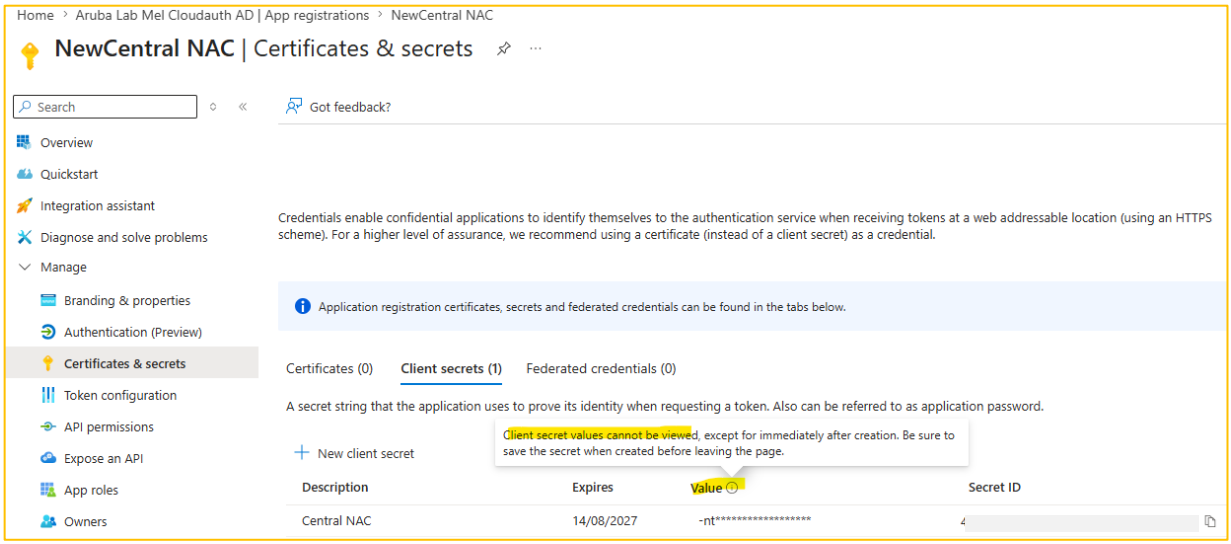
Once we have done that, you should see the following status for the Microsoft graph APIs you had selected.



Finally, we need to create client secret ID



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.



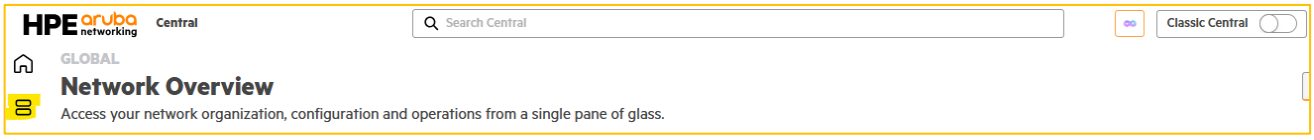
Even if you forgot to copy the secret value, you could delete it and create new secret password.

Central NAC

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

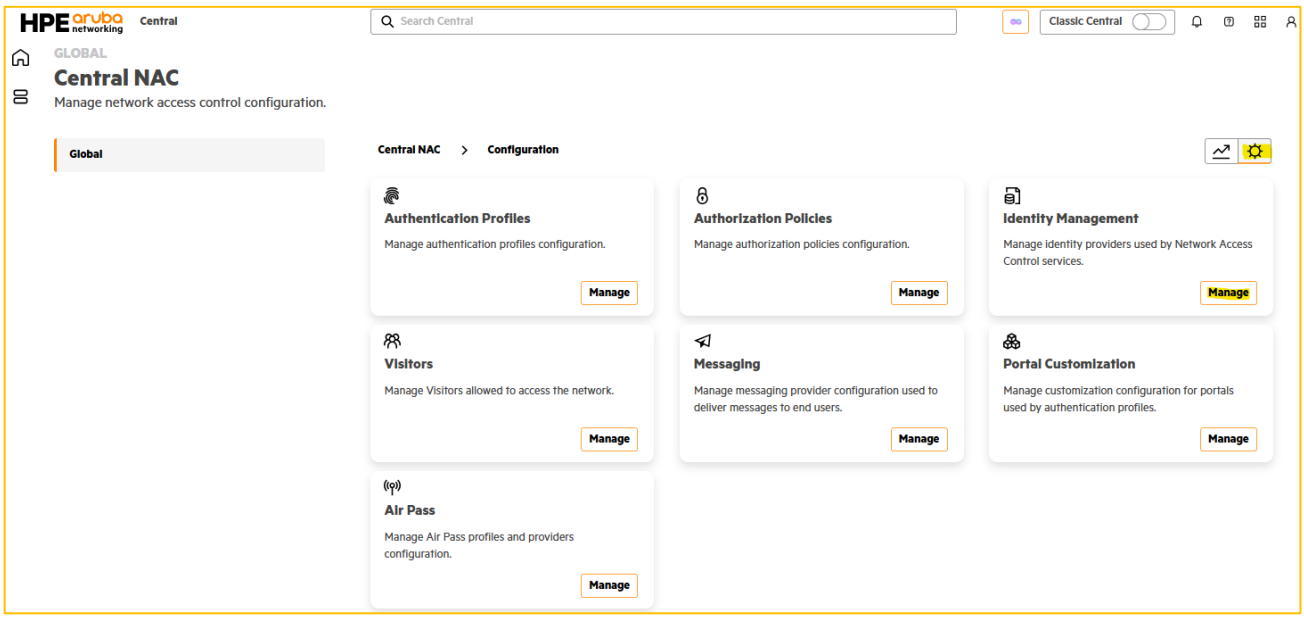
Central NAC Identity Management	Central NAC Authentication Profile	Central NAC Authorisation Policy

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

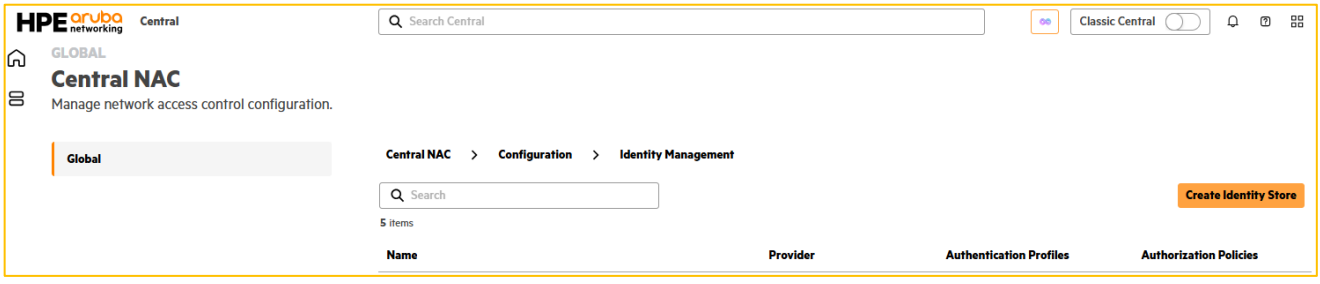


2.4 Configuring Identity Store

Starting with adding Entra as an Identity store.

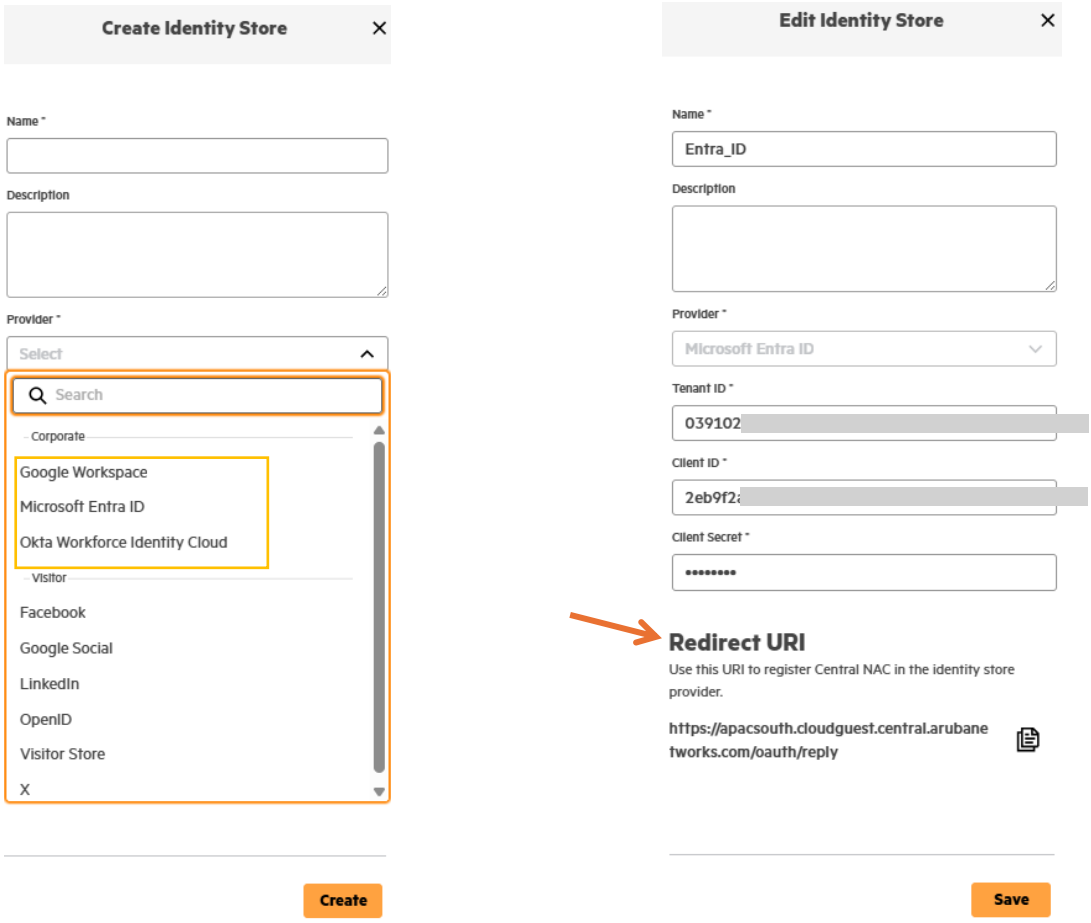


Once you click on the gear icon to get the following screen, here I'll create our first identity store.



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

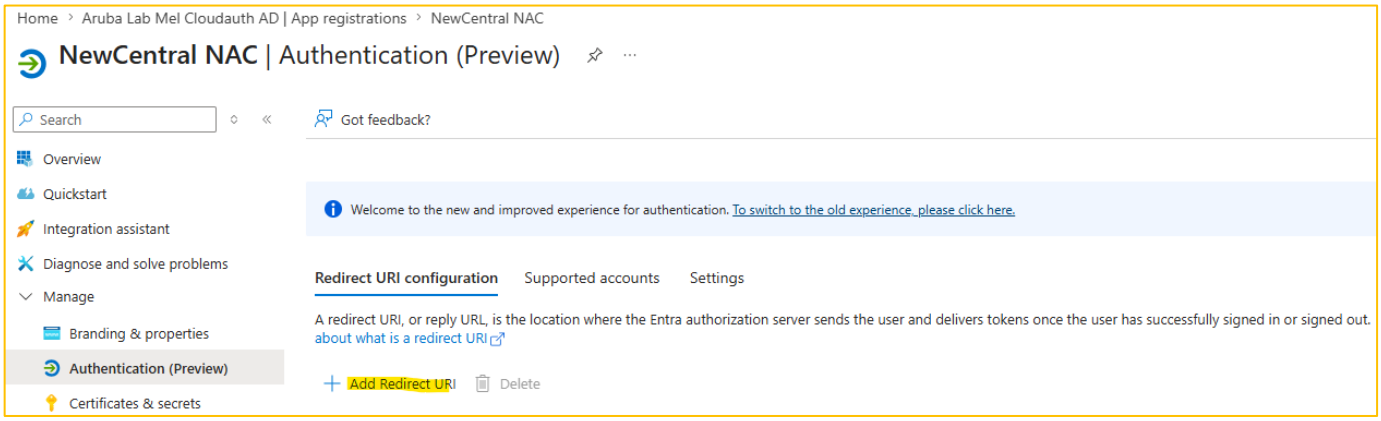
```
Application (client) ID = 468415c0-1e
Directory (tenant) ID = 0391024d-
Secret Value = QE-8Q~
```



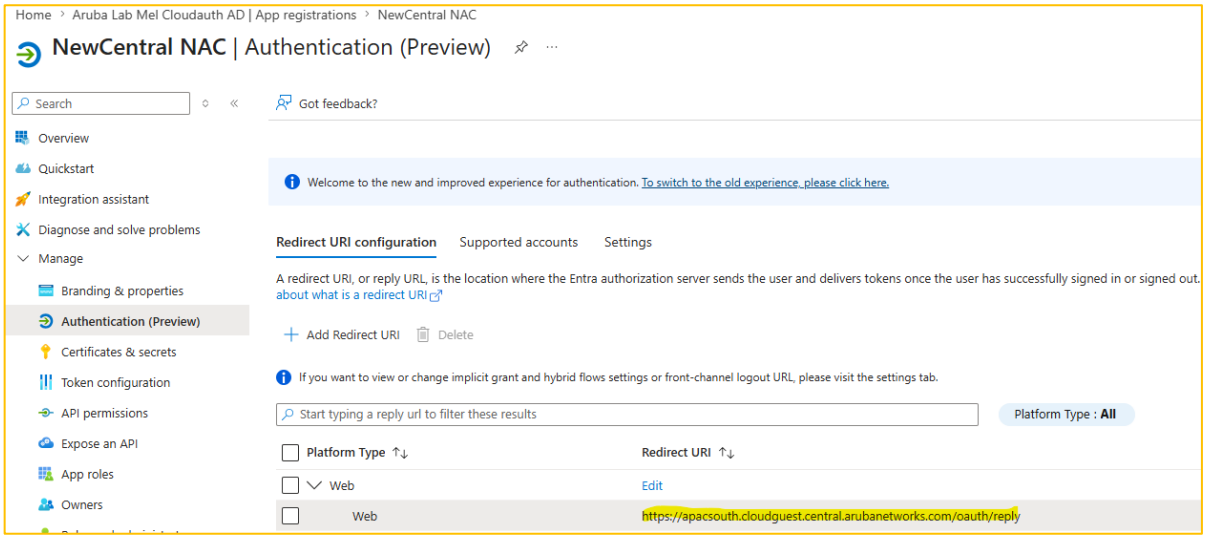
Here you'll see the Redirect URI, copy it as we need to add it to our Entra Id application.

```
https://apacsouth.cloudguest.central.arubanetworks.com/oauth/reply
```

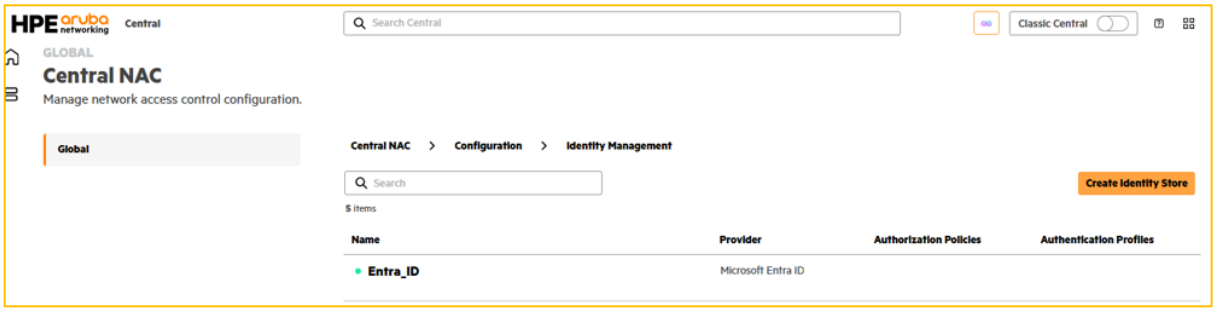
You can navigate back to the Entra Id application you just configured and add Redirect URI for Web.



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



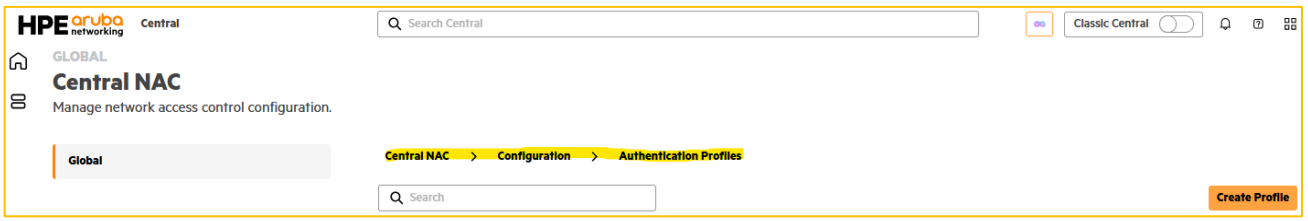
Now back in Central NAC, save the Identity store configuration and after a while you should see a green status next to it.

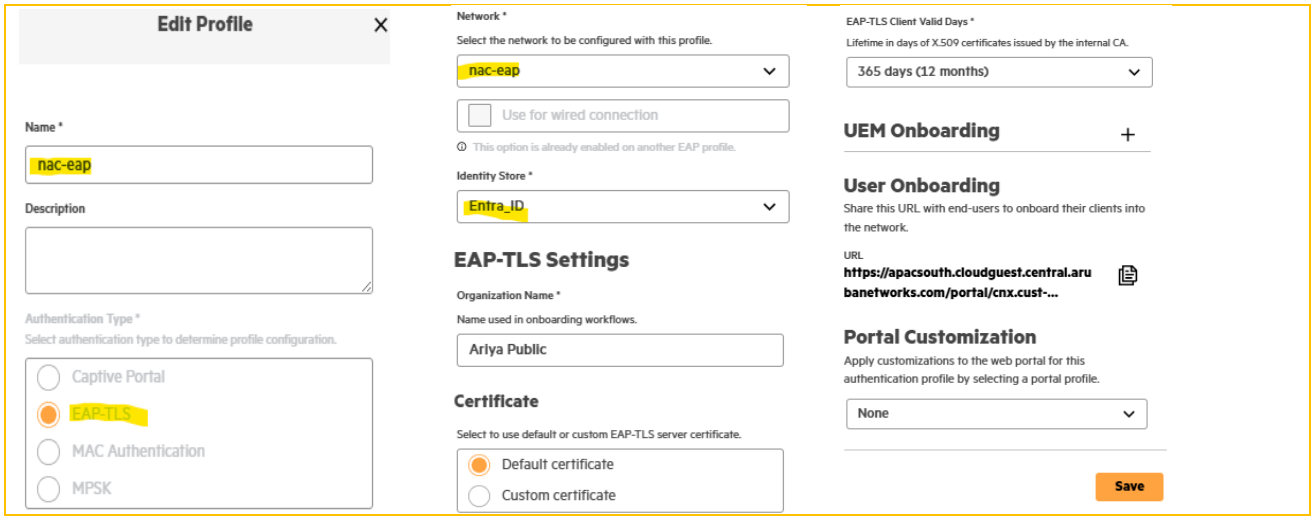


2.5 Authentication Profiles

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.



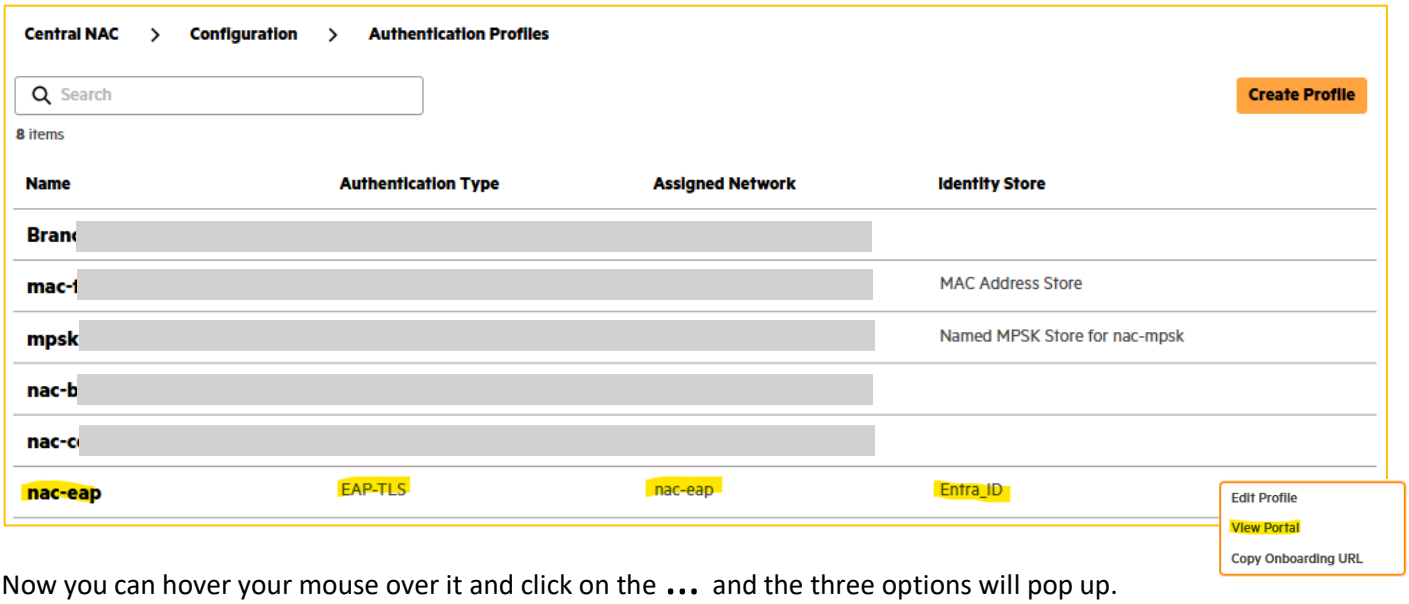


The UEM onboarding you see in the above screen shot, is if you have Intune or JAMF extension integration, here I don't have that setup, so we skip it.

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

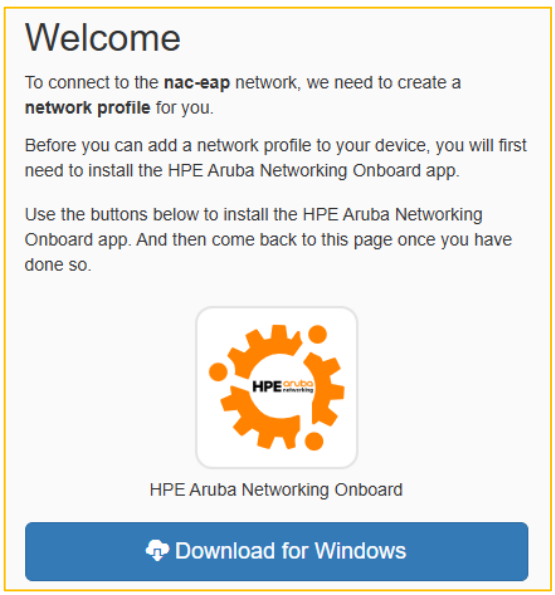
```
https://apacsouth.cloudguest.central.arubanetworks.com/portal/cnx.cust-
46efde6c02                                                    :9f/passpoint
```

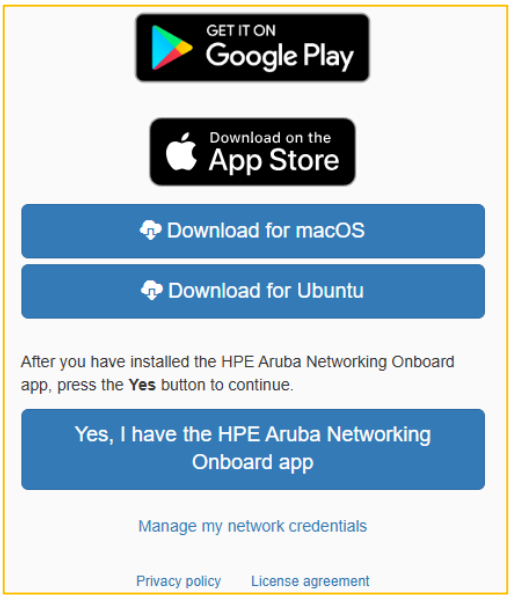
Lastly you can customise the onboarding portal as well. Here I have chosen not to customise it. And once you save it, the authentication profile will be as shown below.



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.





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.

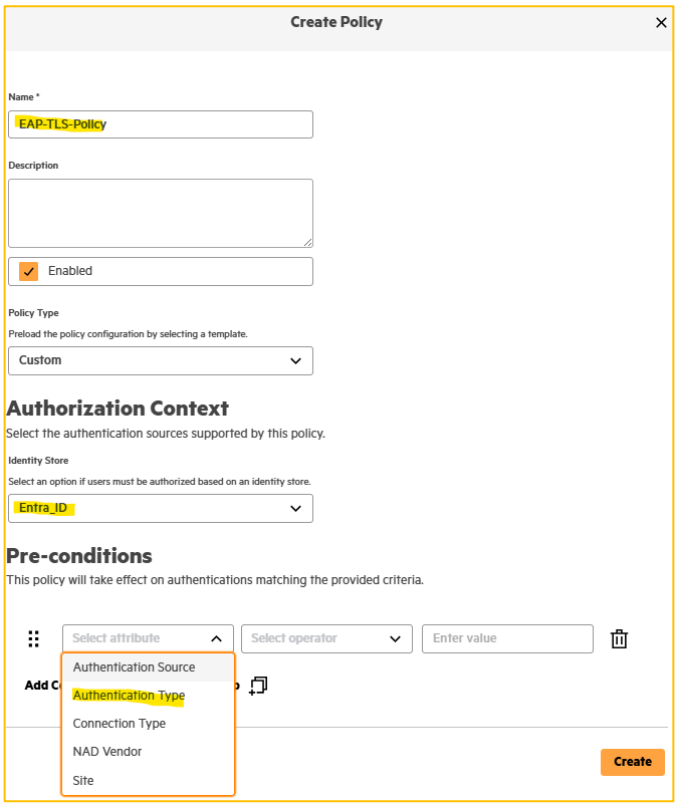
These rules allow Central NAC to apply different enforcement actions based on user, device, group, or identity-store attributes, providing flexible and consistent access control across WLANs.

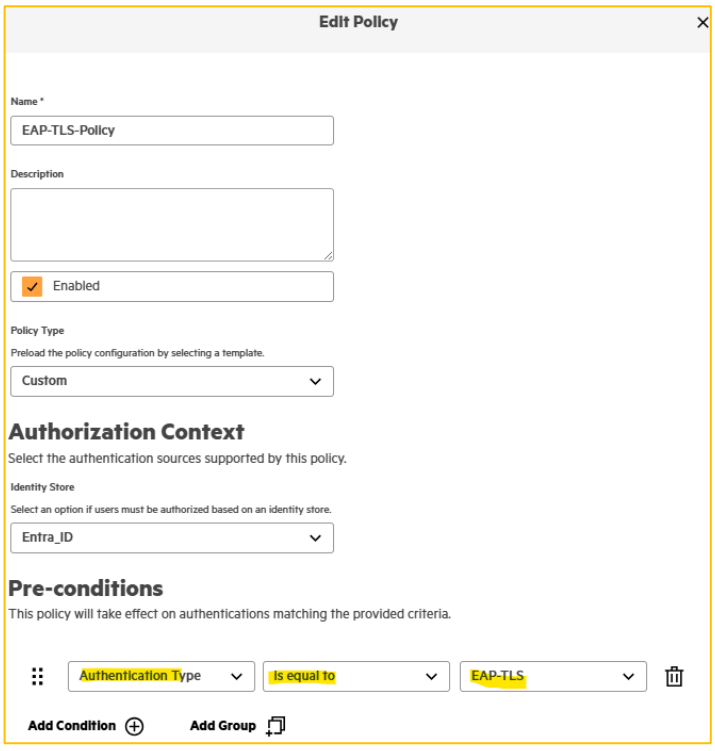
Now I'll navigate to the authorisation policies and create a new one.

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.

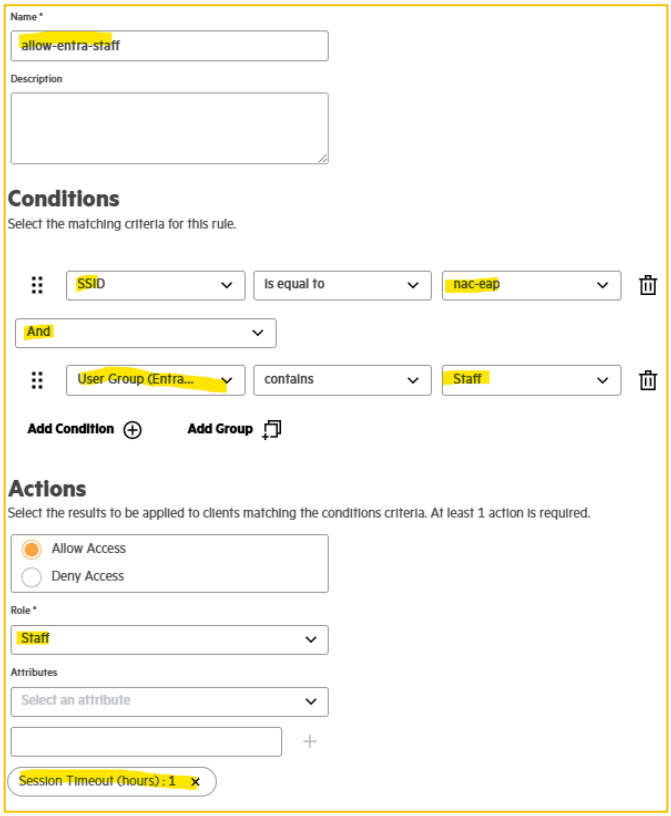
Here are the other preconditions that can be added as well.

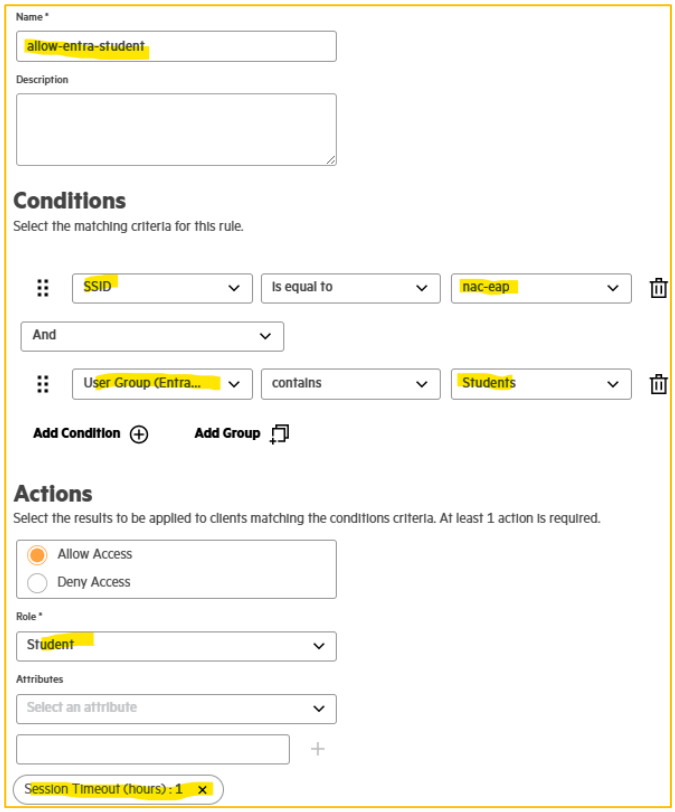
- Authentication Source = based on the configured Identity stores
- Authentication Type = MPSK, EAP-TLS, MAC Authentication Bypass (MAB), Captive Portal (CP)
- Connection Type = Wired or wireless
- NAD Vendor = AOS-Switch, Cisco/Meraki wired, Cisco/Meraki Wireless, HPE Comware wired, IETF, Juniper Mist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



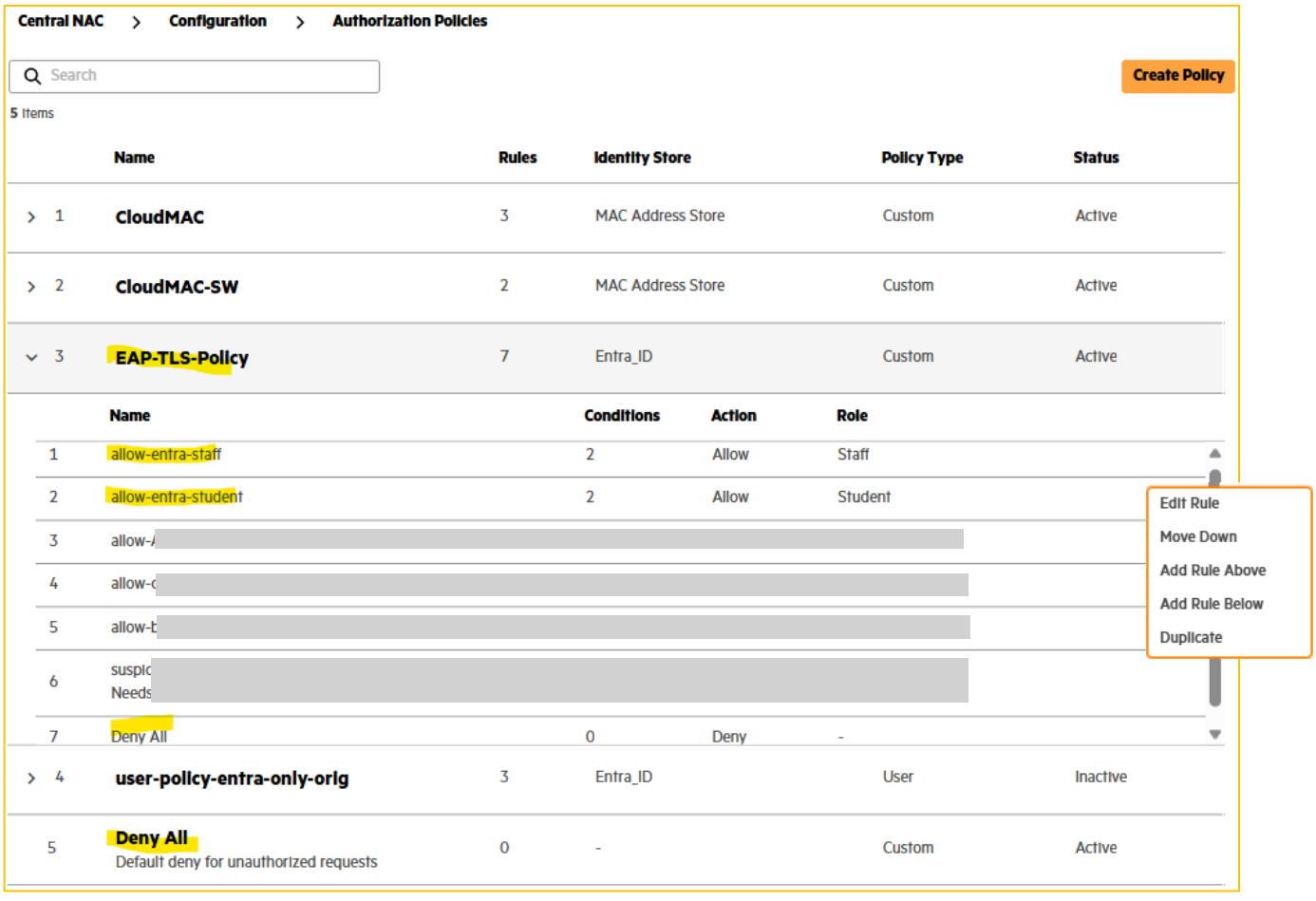


Next, I need to add the rules under this policy. Here are my two simple rules.





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.



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.

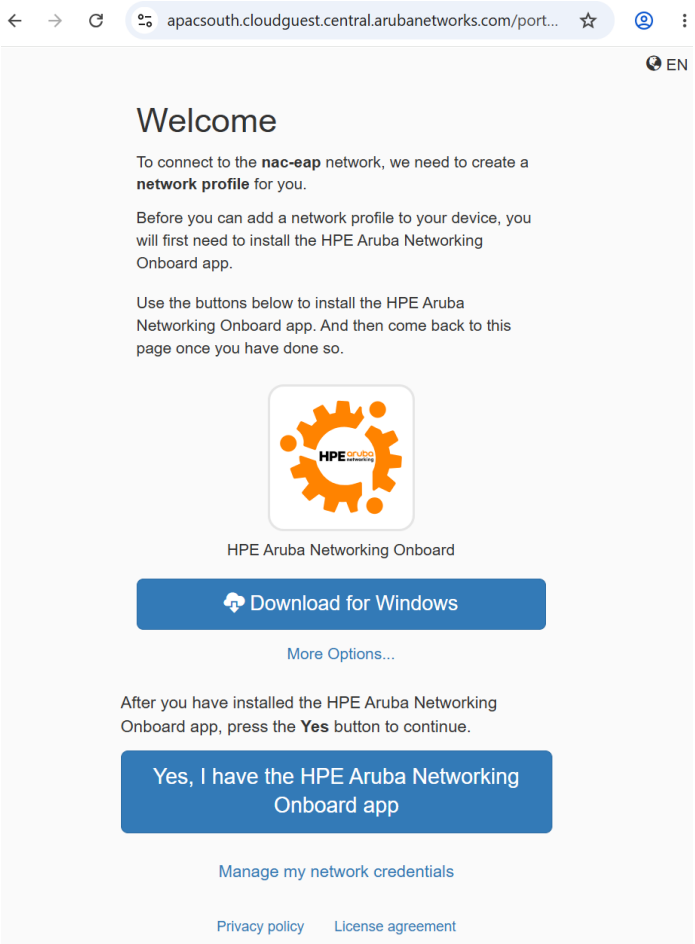
The requirements for Central NAC onboarding are

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

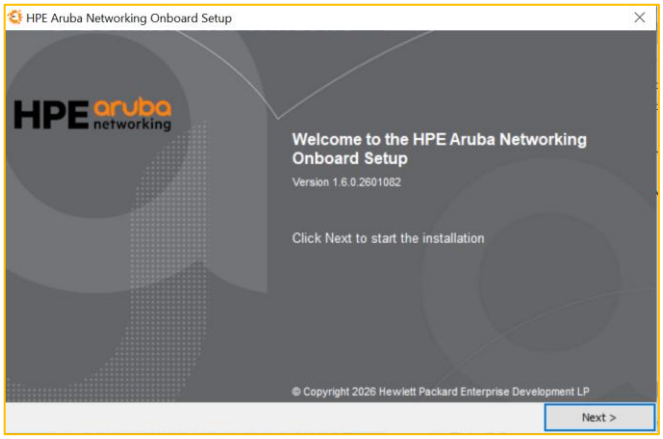
Aruba Central NAC uses Passpoint to provide ease of access. The idea here is that we can send this onboarding URL to the users so they can get connected to this WLAN which is being authenticated with Central NAC.

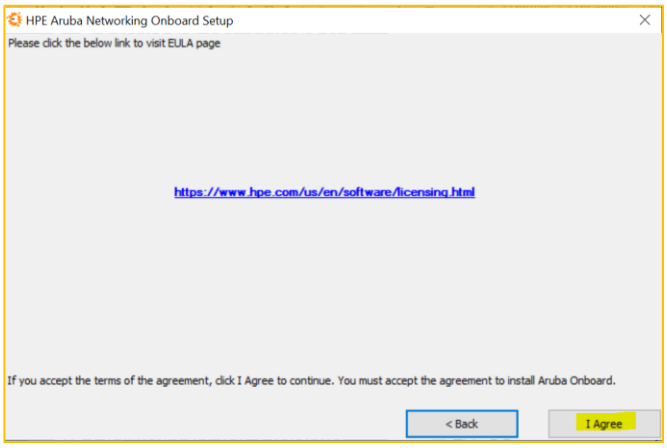
2.7 Staff1 Onboarding Using Onboarding App

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

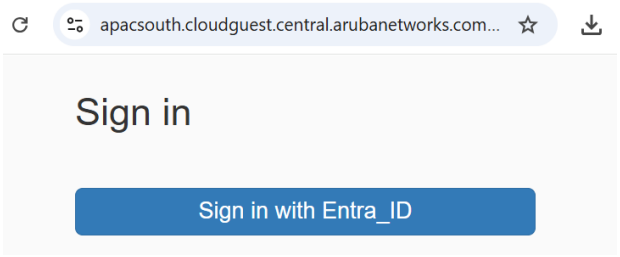


Since this is the first time the user is onboarding, they need to download HPE Aruba Networking Onboard App. Because I am using a windows laptop, it is automatically showing the windows options. So now I have downloaded it and will install it.

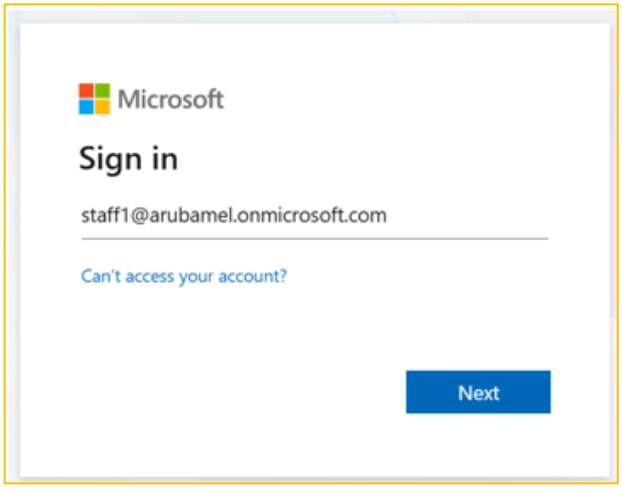


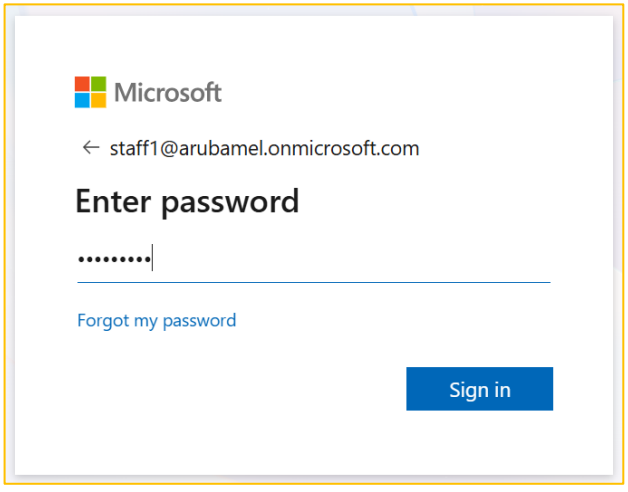


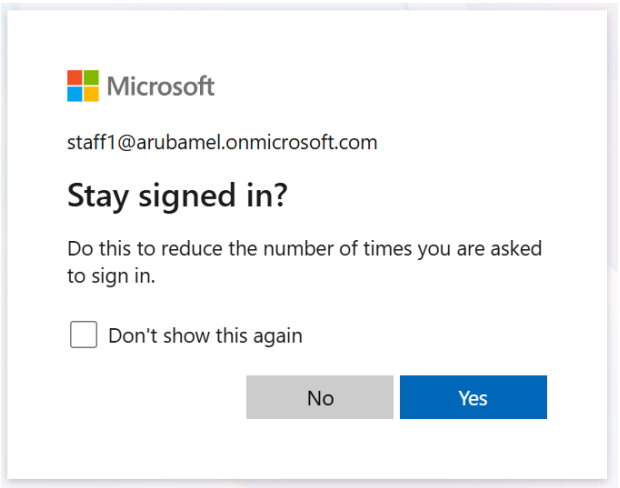
Once it is installed from the browser, click on the "Yes I have the Onboard App" button. This will start the Entra ID authentication.

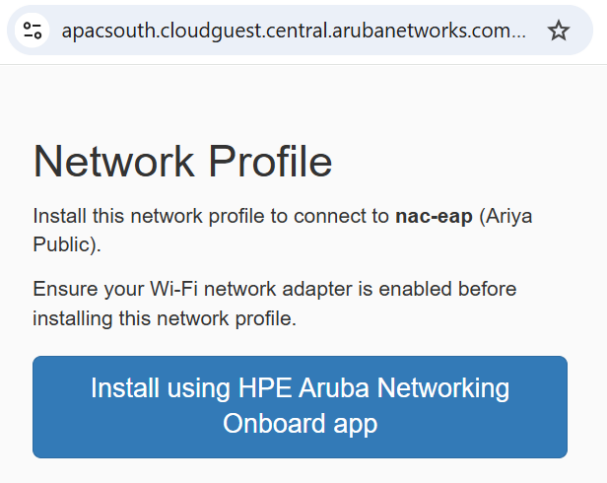


after which the user gets presented with the following

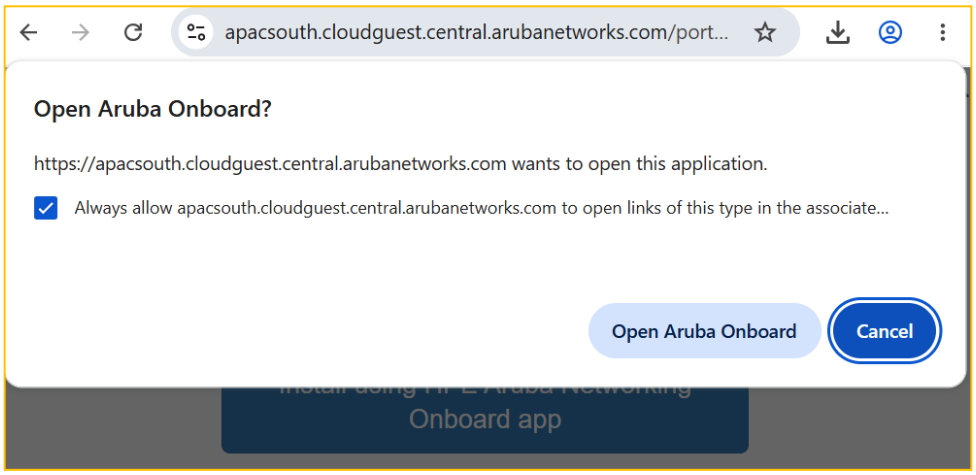




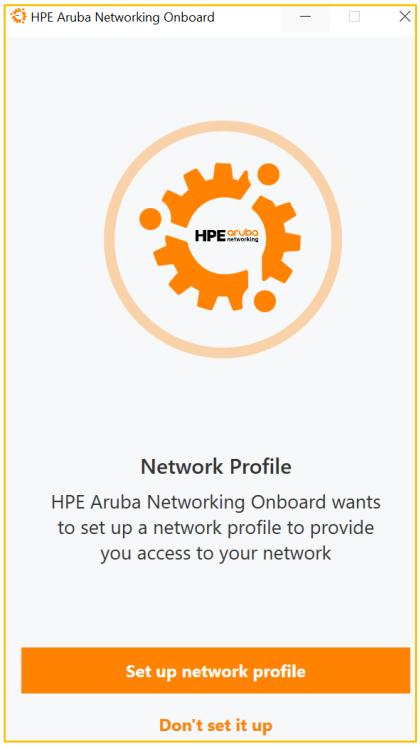


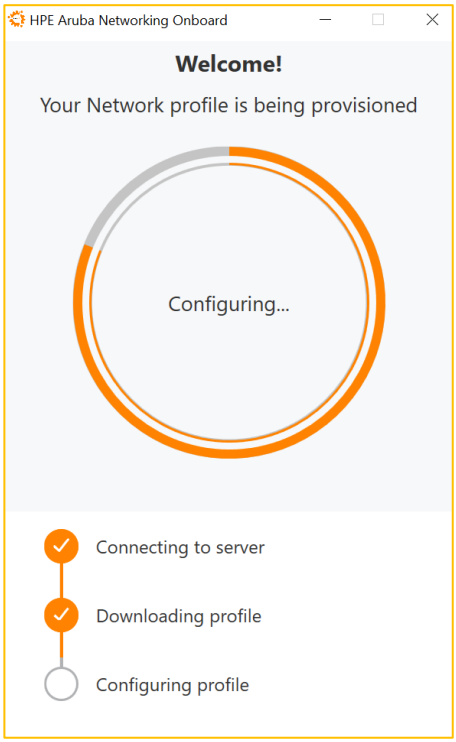


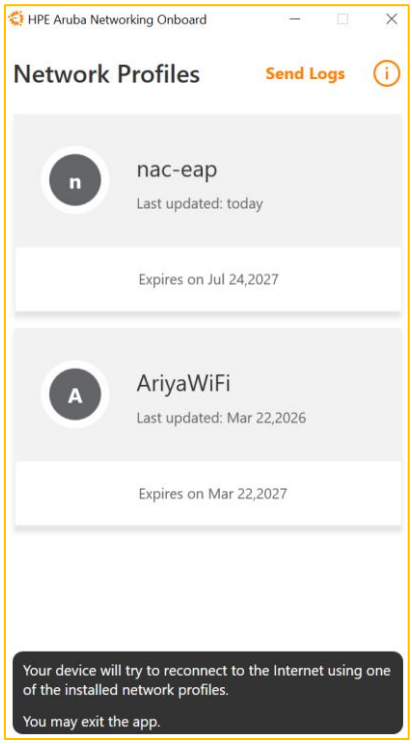
Now after successful authentication, Onboard App will install the Network Profile.



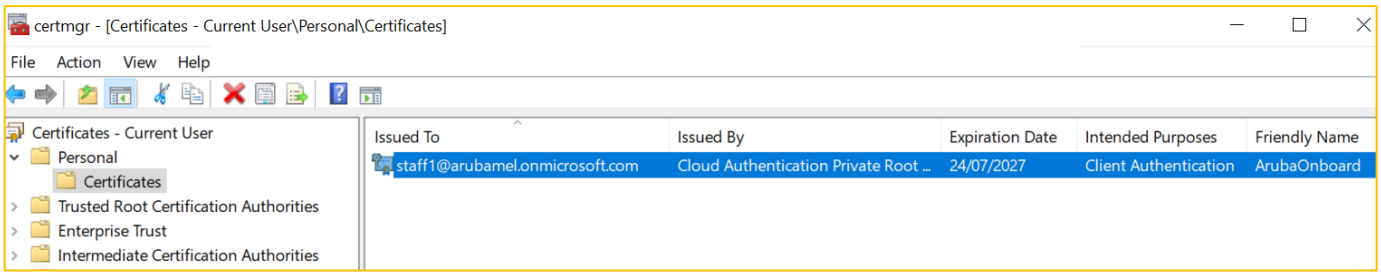
And here are the exact steps which is basically clicking on set up network profile and then waiting for it to finish.



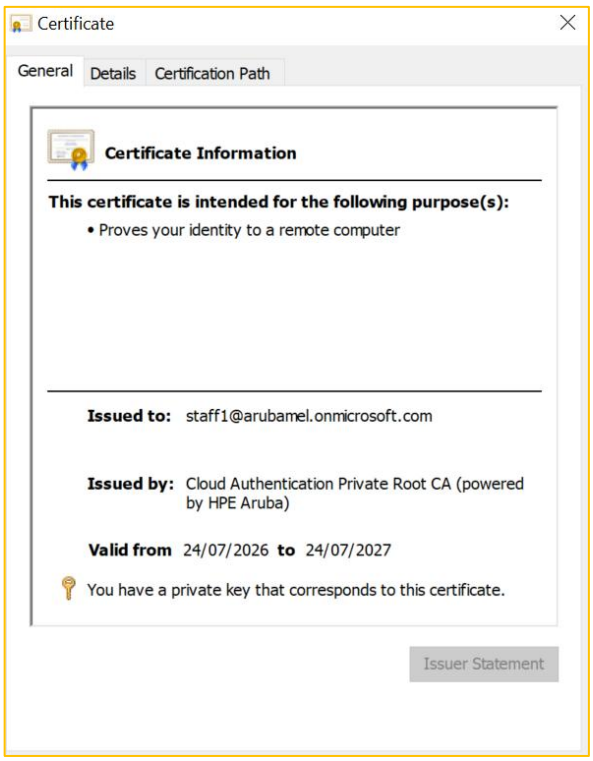


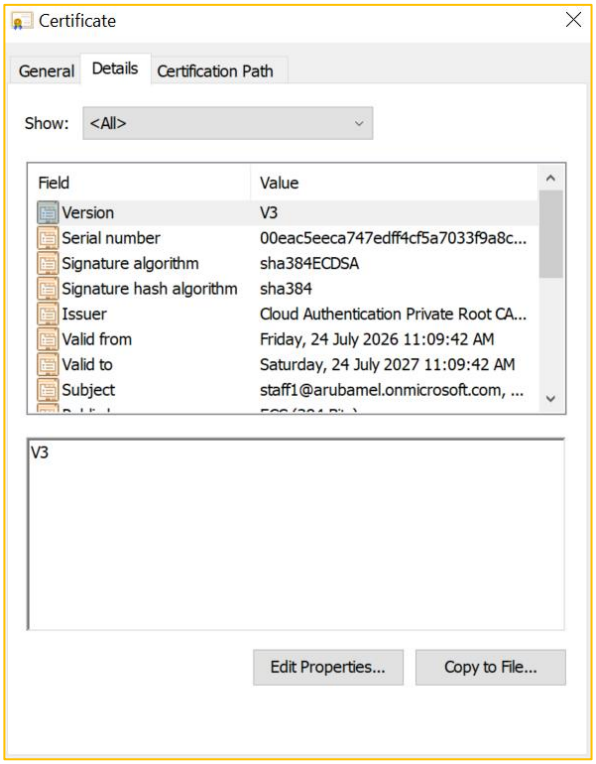


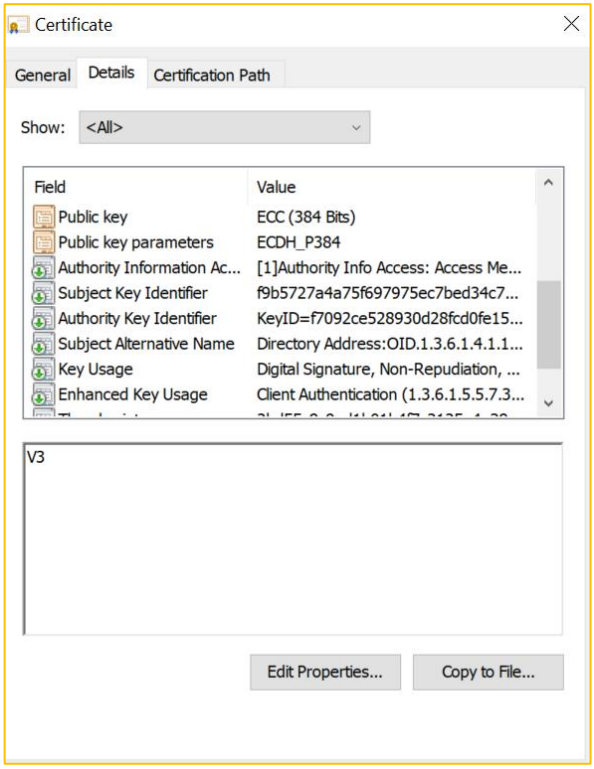
For the curious, you can check the user certificates to see the certificate that Central NAC just installed.

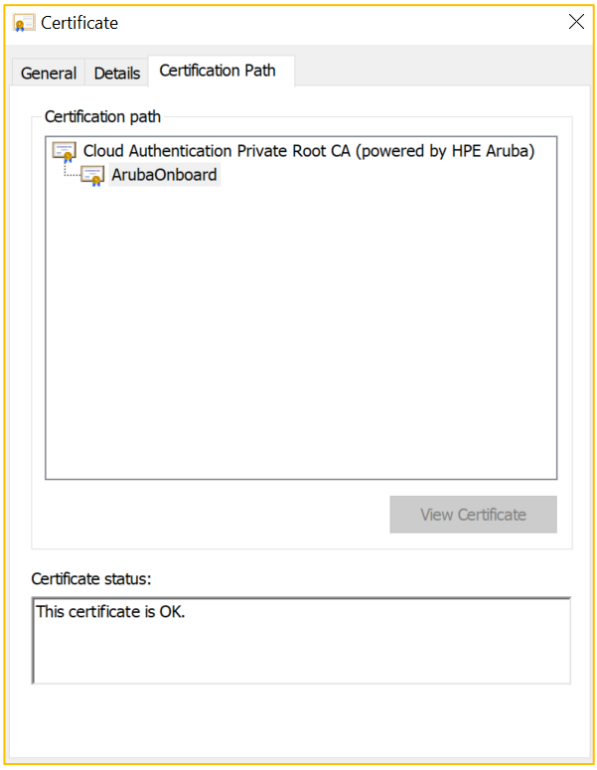


As you can see it is installed and issued by Cloud Authentication from HPE Aruba.

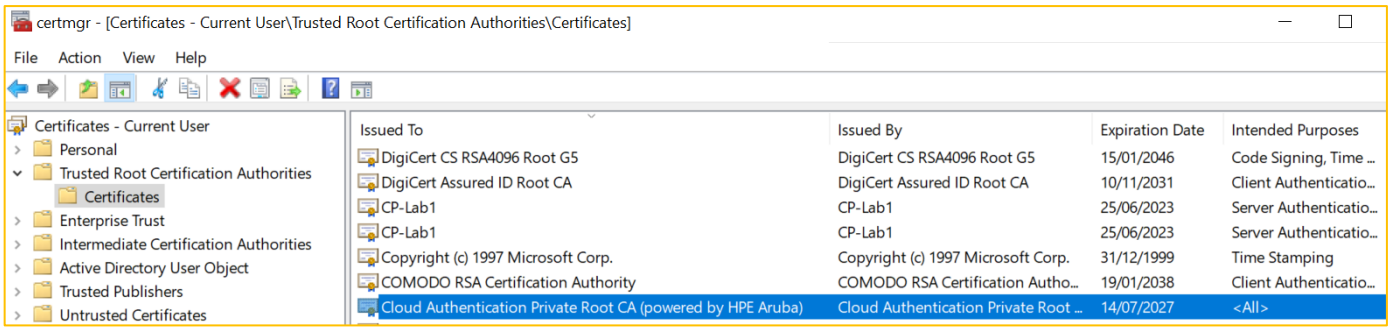








And here is trusted root CA certificate.



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.

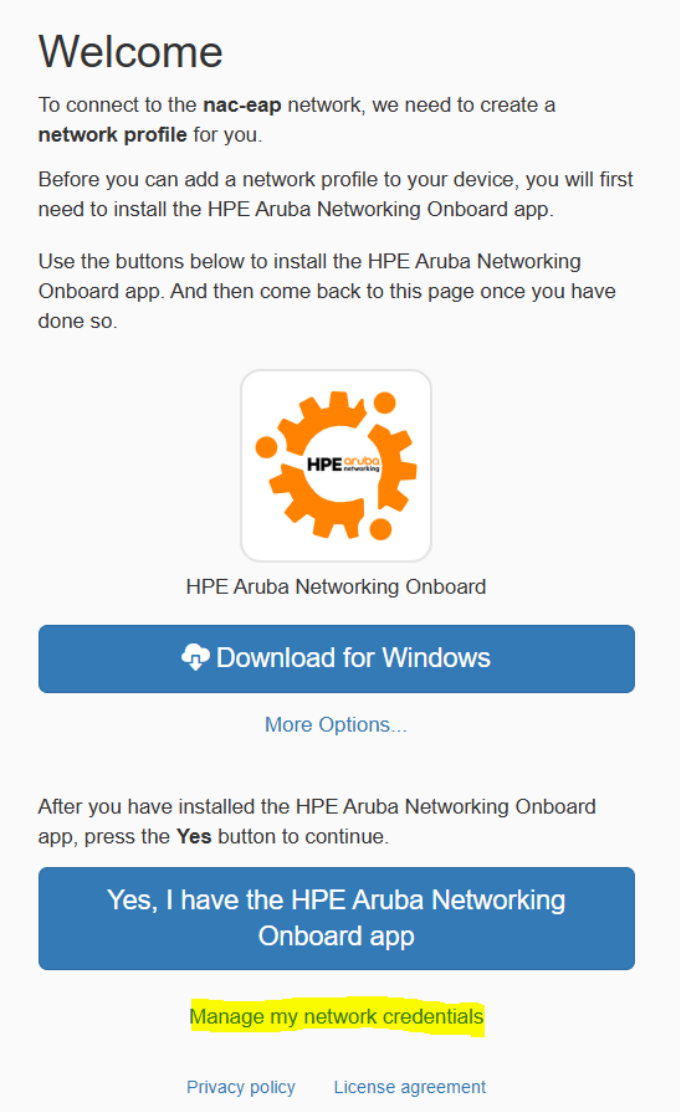
2.8 User Self-Service Option

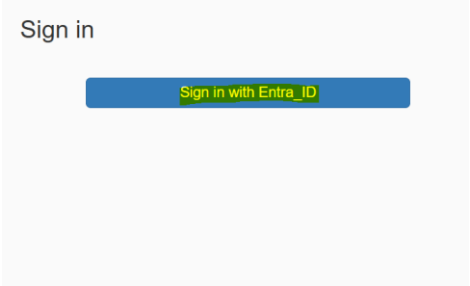
Central NAC also includes a user self-service option that allows users to view the network credentials issued to them, including credentials linked to their individual devices.

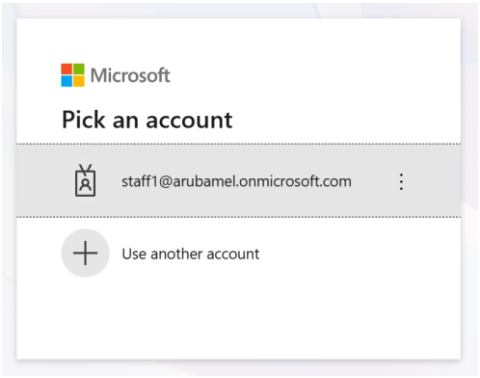
This improves the user experience by reducing reliance on IT for basic certificate management tasks. For example, if a device is lost, replaced, or potentially compromised, the user can access the self-service portal and revoke the relevant certificate directly.

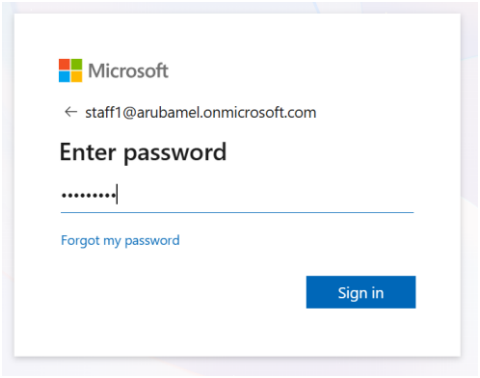
The screenshots below show how users can select “Manage my network credentials” at the bottom of the onboarding page. The onboarding URLs are available under Central NAC >> Authentication profile.

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

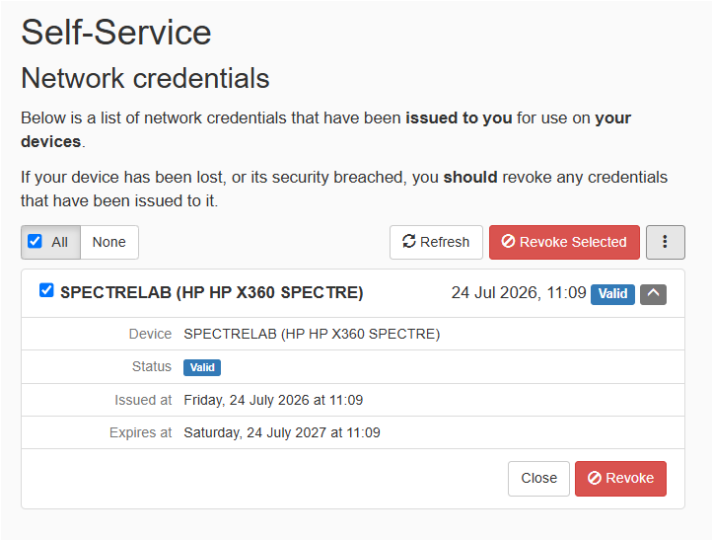


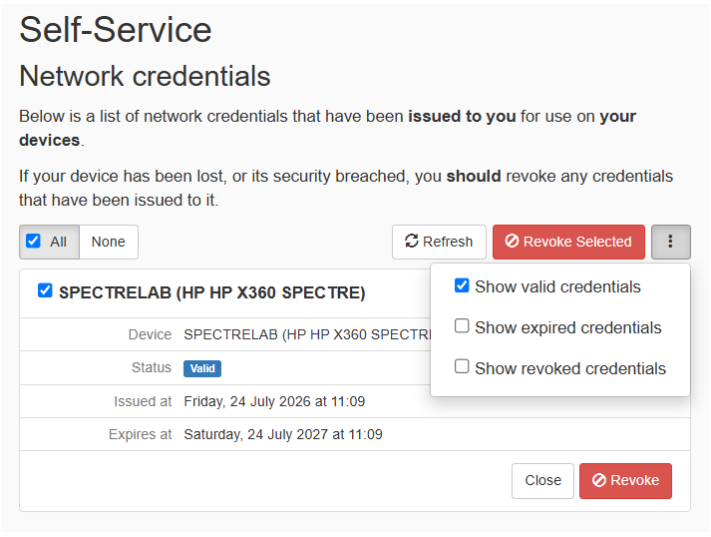






They will then be presented with the credential management page, where they can review the network credentials associated with their account and devices. From here, users can easily see which credentials are currently valid, which ones have expired, and which ones have already been revoked. This gives 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.



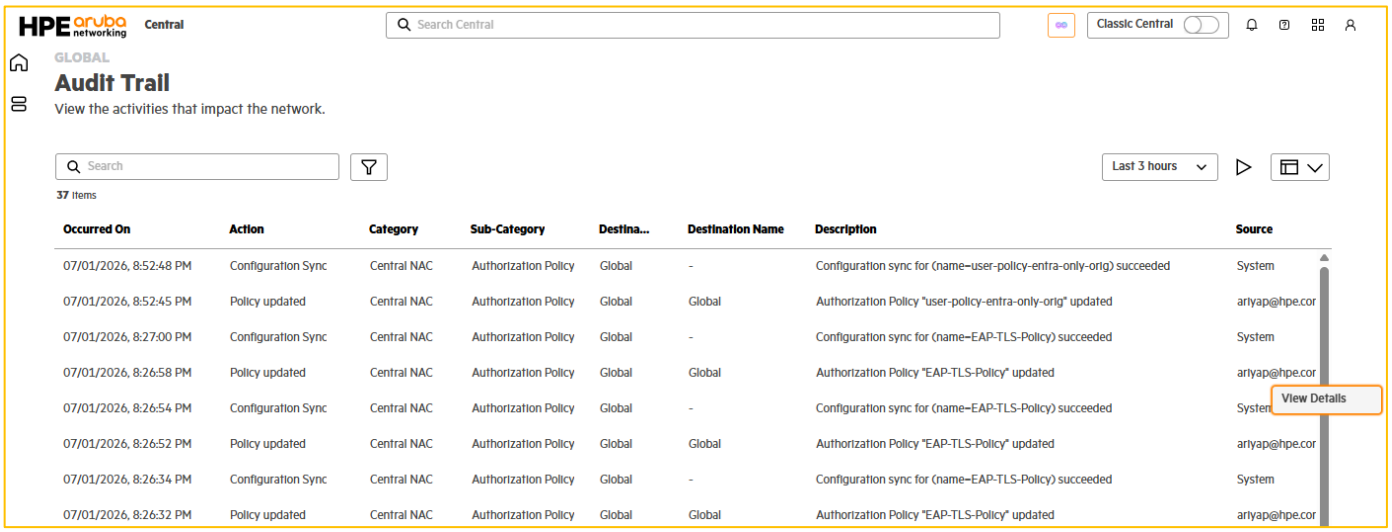


User Testing

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.



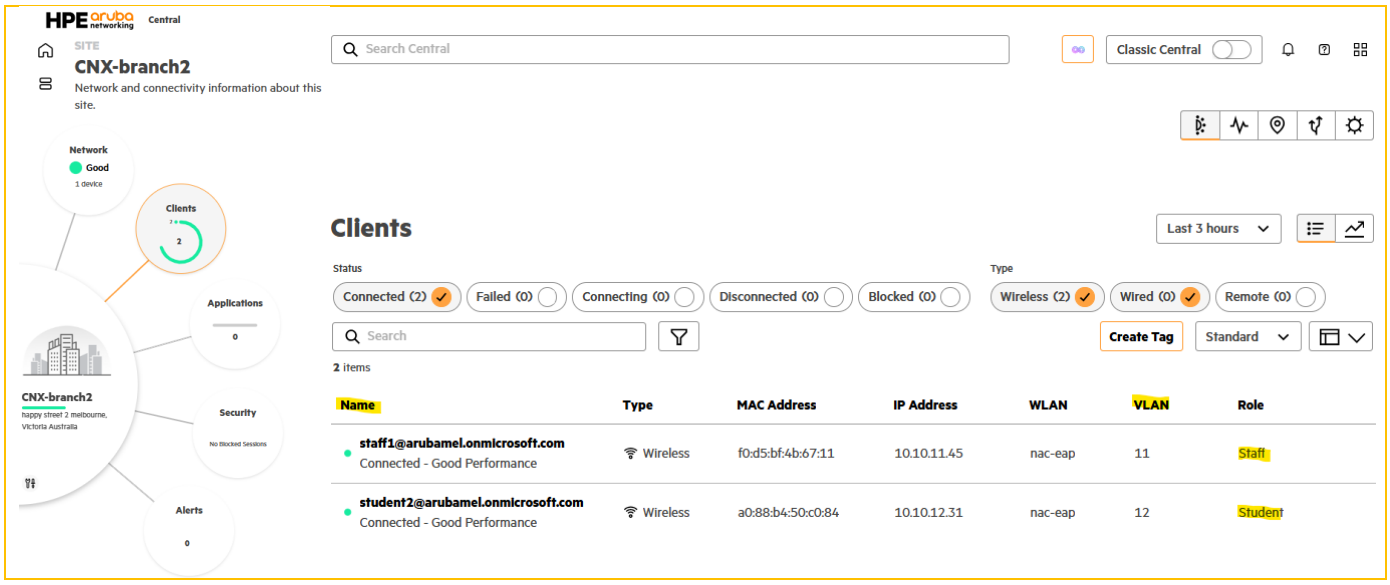
And here is the audit trail for some of the policies that I was updating

2.10 User Connectivity

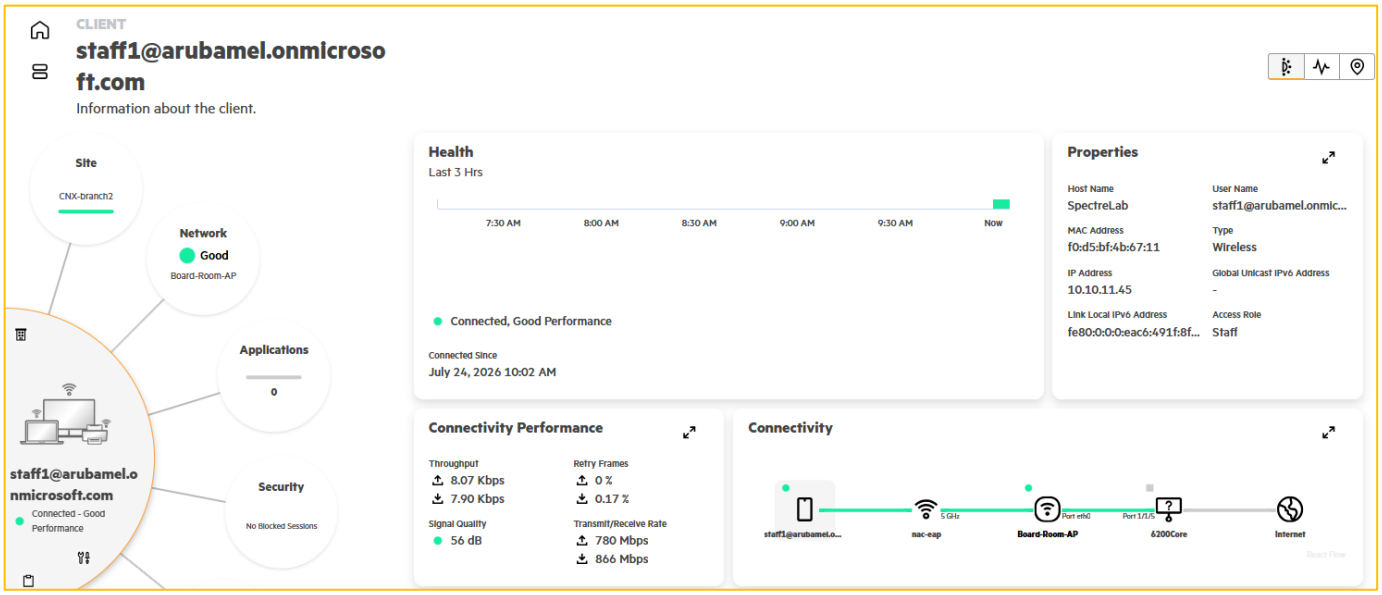
Now we get two clients to connect to the nac-eap WLAN, and the authentication flow will be as follows

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

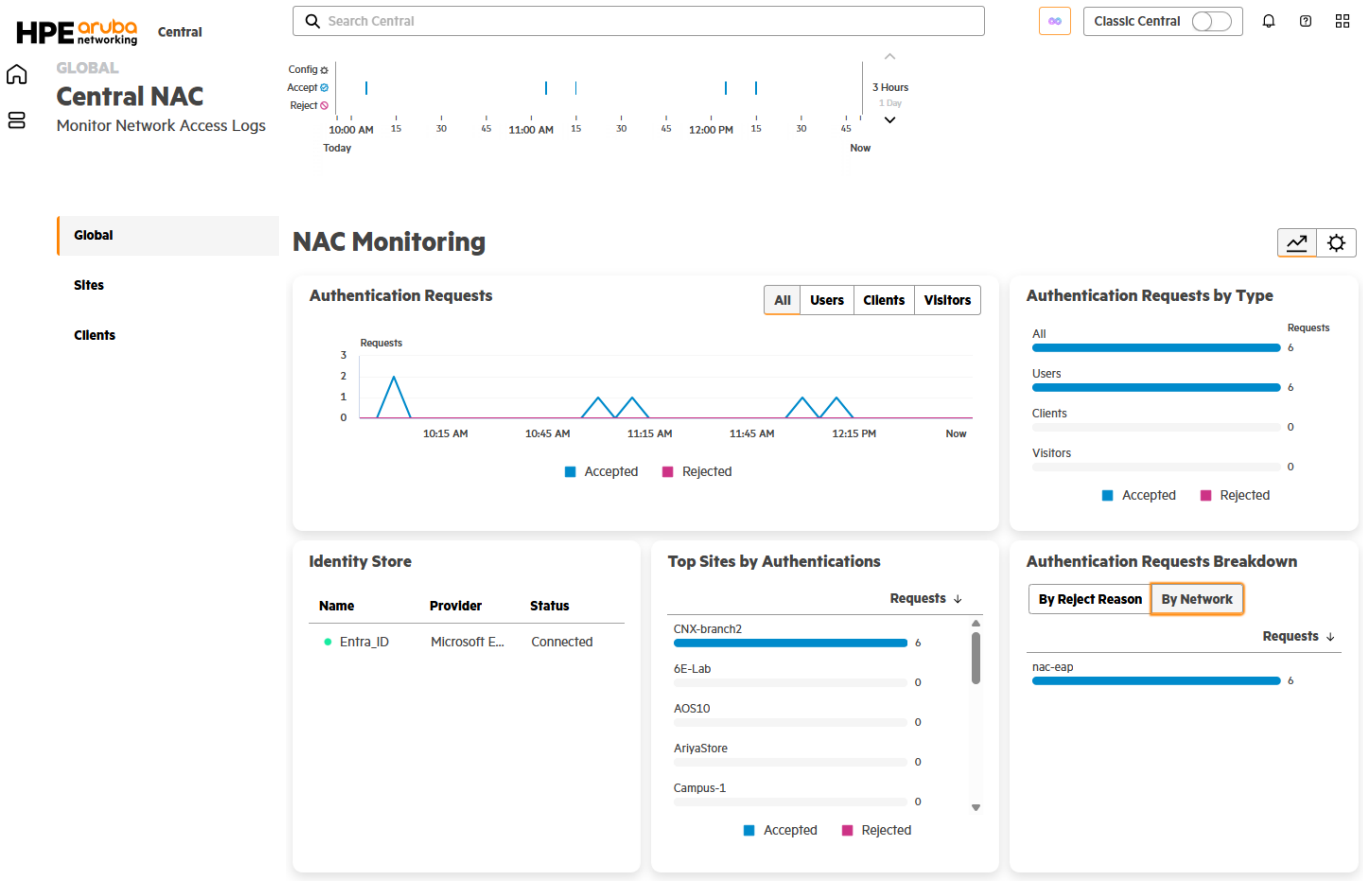
The two users onboarded as Staff and Student. Based on our authorisation policies they should be put into different roles. Here is the view of New Central.



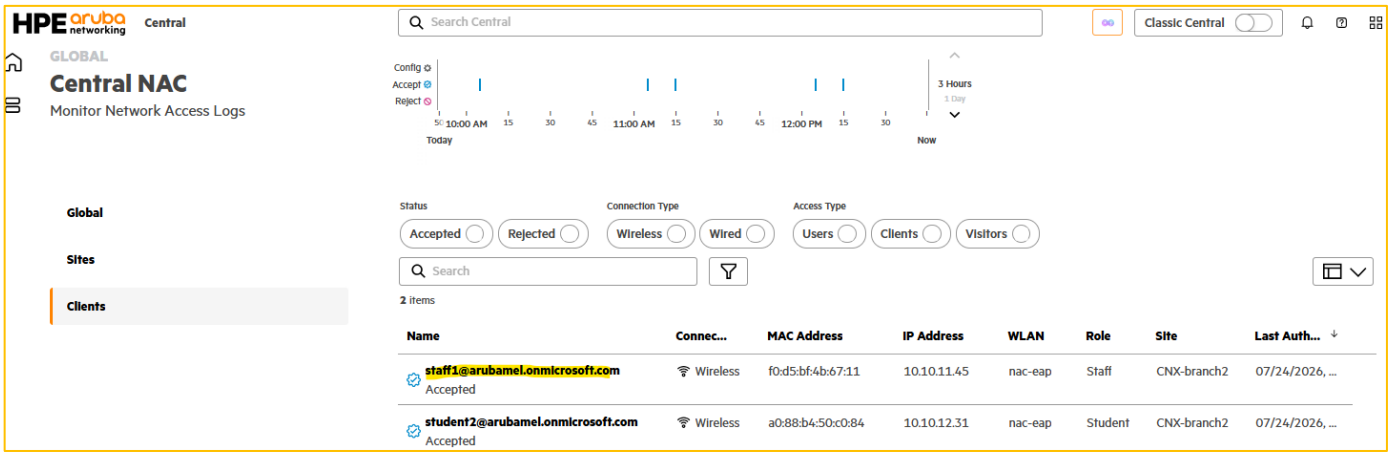
As shown above you can see the two users are in different user roles with the correct VLAN assignments. In the below screenshot you can see that details of staff1 user.



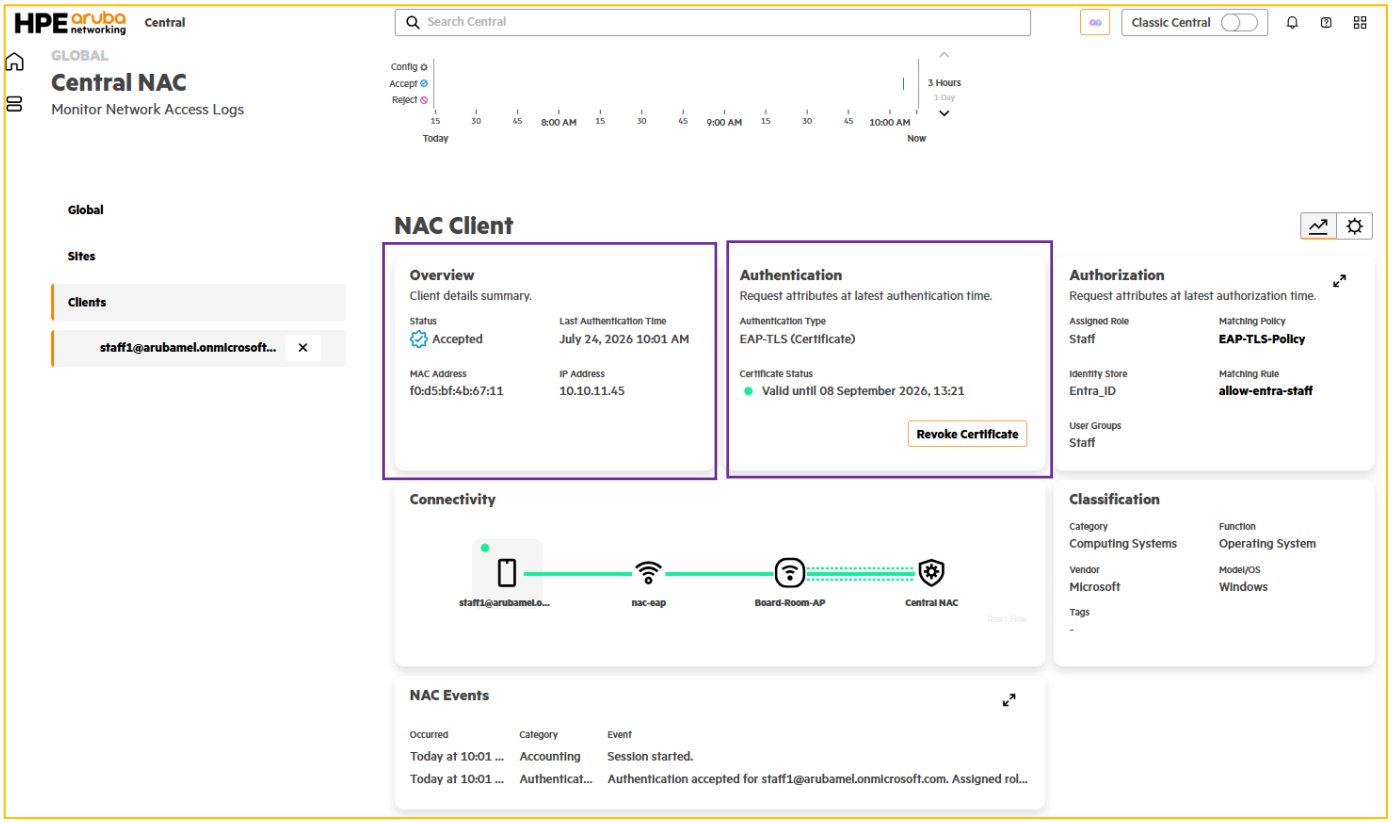
Now here is the Central NAC view that shows the authentication requests over the period and authentication breakdown by site clients and networks.



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



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.