1 Table of Contents

1 Table of Contents 1
1.1 Revision History 1
2 Central NAC Bring Your Own Certificate (BYOC) 2
2.1 Things you need 2
3 Central NAC and BYOC 3
Configure the 802.1.x WLAN in New Central 3
3.1 Existing User Certificate 5
3.2 BYO Server Certificate and Trusted CA Certificate Configuration 6
3.3 Converting Certificates 8
3.4 Authentication Profile 9
3.5 Central NAC Authorisation Policies 12
3.6 Client Testing 15

1.1 Revision History

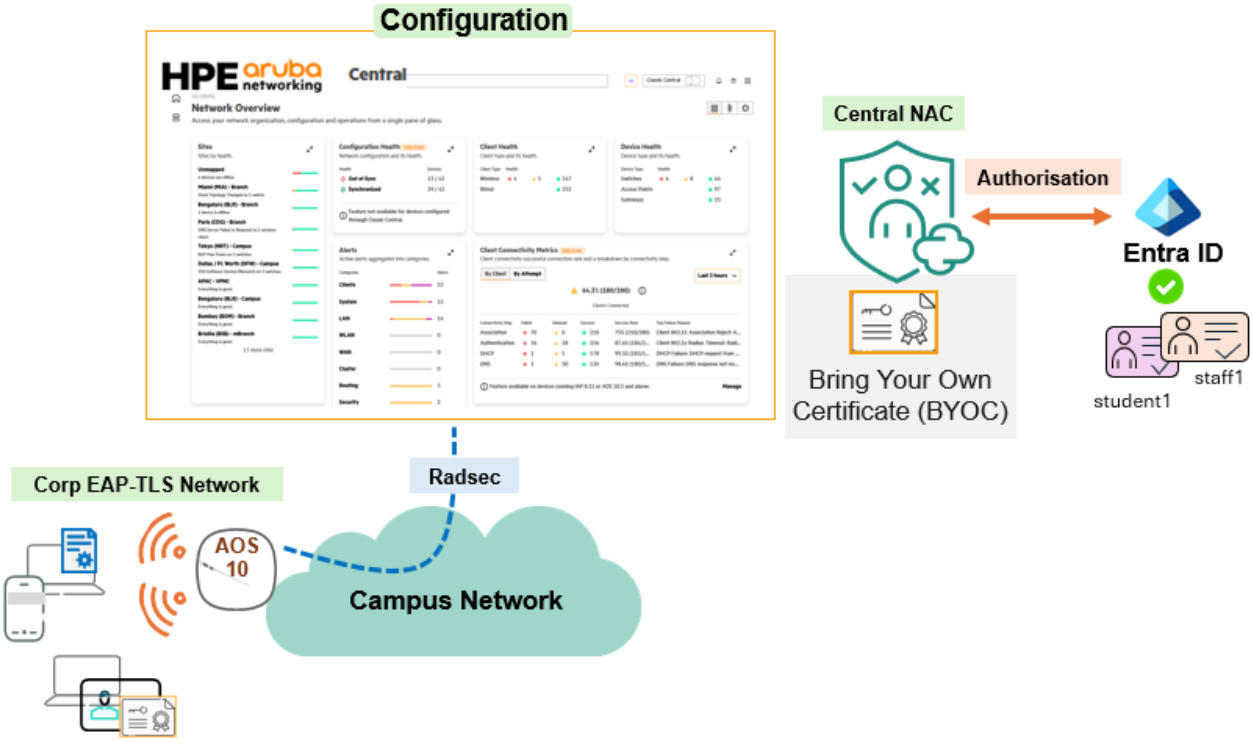
DATE	VERSION	EDITOR	CHANGES
10 Oct 2026	0.1	Ariya Parsamanesh	Initial creation
01 Nov 2026	0.2	Ariya Parsamanesh	Client Testing

2 Central NAC Bring Your Own Certificate (BYOC)

HPE Networking Aruba Central NAC (CNAC) brings network access control to the cloud. It authenticates users and devices, applies role-based access, and enforces policy across wired and wireless networks.

CNAC's Onboard App makes device onboarding easy, without the need to manage a PKI or device management setup. But what if your organisation already has its own PKI, or your devices have already been onboarded using your own root certificate? That's where Bring Your Own Certificate (BYOC) comes in. BYOC feature allows CNAC to work with an existing external PKI and is included with the CNAC Pro subscription.

To set this up, you upload a server certificate and trusted CA certificates for EAP-TLS authentication. CNAC can then trust client certificates issued by those external certificate authorities. You can also use Online Certificate Status Protocol (OCSP) to check the status of a certificate before allowing access.



In this technote, I'll use a scenario where the clients have already been onboarded using ClearPass Onboard. ClearPass Onboard is issuing user certificates to Entra ID users, and those certificates are already being used to connect to the wireless network.

If you'd like some background on that configuration, search my blog for the technote "Secure BYOD Access with ClearPass and Entra ID using SAML SSO".

The goal now is simple: move authentication to CNAC without onboarding those devices again. The clients will continue using their existing certificates issued by the ClearPass Onboard CA, while CNAC takes over the authentication.

For this setup, I'm using AOS10 APs deployed in bridge mode.

2.1 Things you need

- APs running AOS10 firmware version (I am using 10.8.1.1)
- Valid or evaluation HPE Aruba Central account and CNAC Pro subscriptions
- Existing user certificate that is issued by a Certificate Authority
- OpenSSL program to convert certificates.

3 Central NAC and BYOC

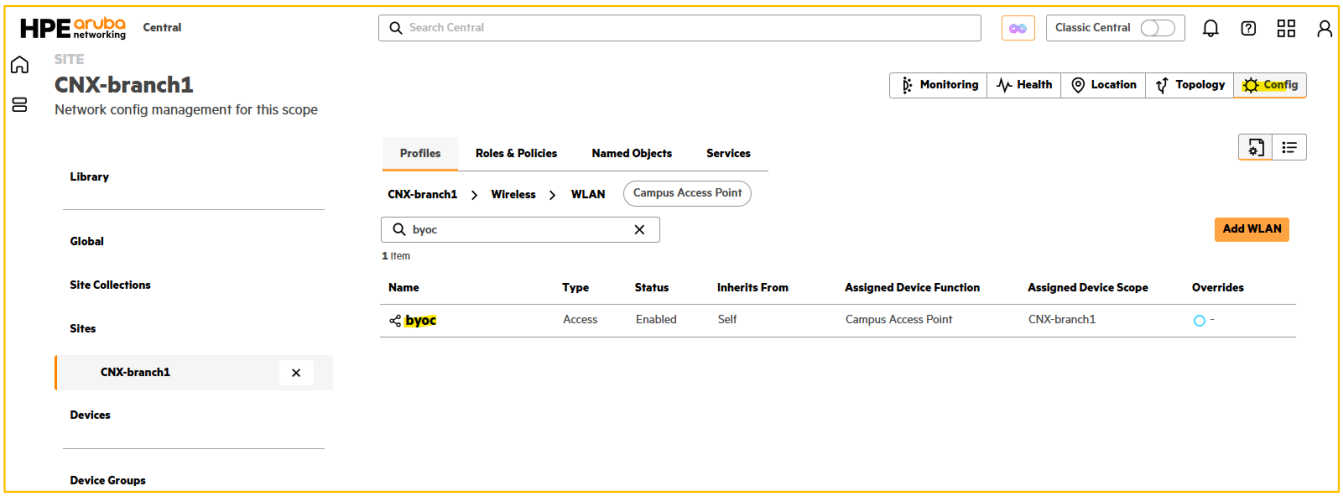
With the Central NAC & Entra ID Integration for Bridge Mode APs covered in the previous technote, let's configure BYOC. We'll start with the WLAN configuration, export the certificates from ClearPass, and then configure authentication and authorisation in CNAC. Finally, we'll test both a successful connection and a policy rejection.

Here's what we'll do:

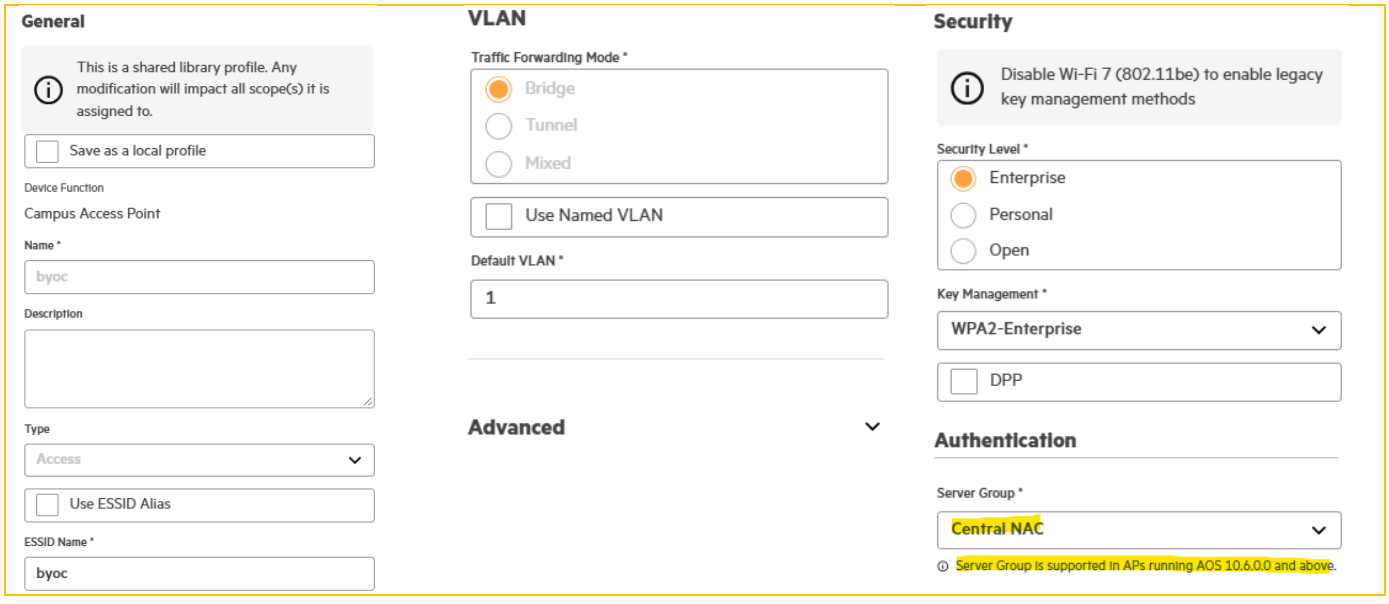
1. Configure the 802.1X WLAN and the associated user roles in New Central.
2. Export the server certificate and trusted CA certificate used for EAP-TLS authentication.
3. Convert the certificates to PEM format.
4. Configure the Authentication Profile in CNAC.
5. Configure the Authorisation policy in CNAC, optionally using the Entra ID identity store to authorise users.
6. Test the client connection.

Configure the 802.1.x WLAN in New Central

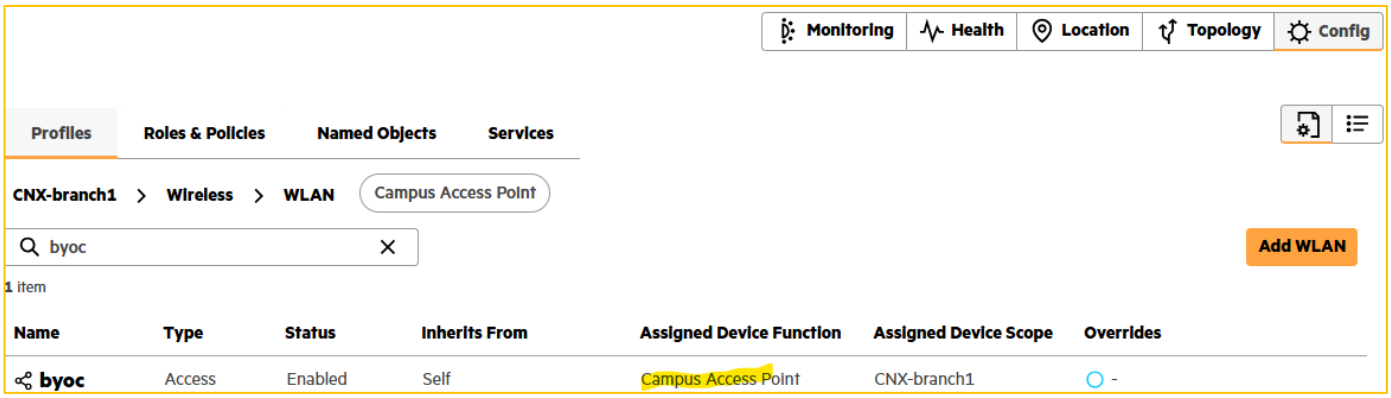
Here we'll configure a WLAN to be authenticated by CNAC. The name of the WLAN profile is byoc.



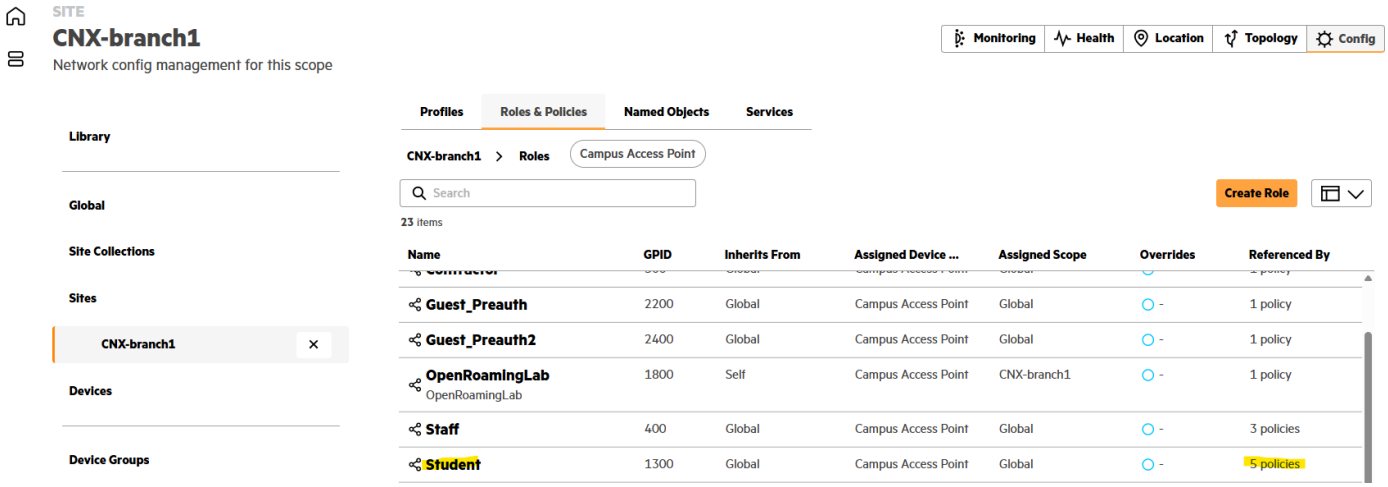
I'm creating the byoc WLAN at the site level, using the settings shown below. Everything else is left at its default. Before continuing, check the minimum AOS10 version shown beside the Central NAC server group.



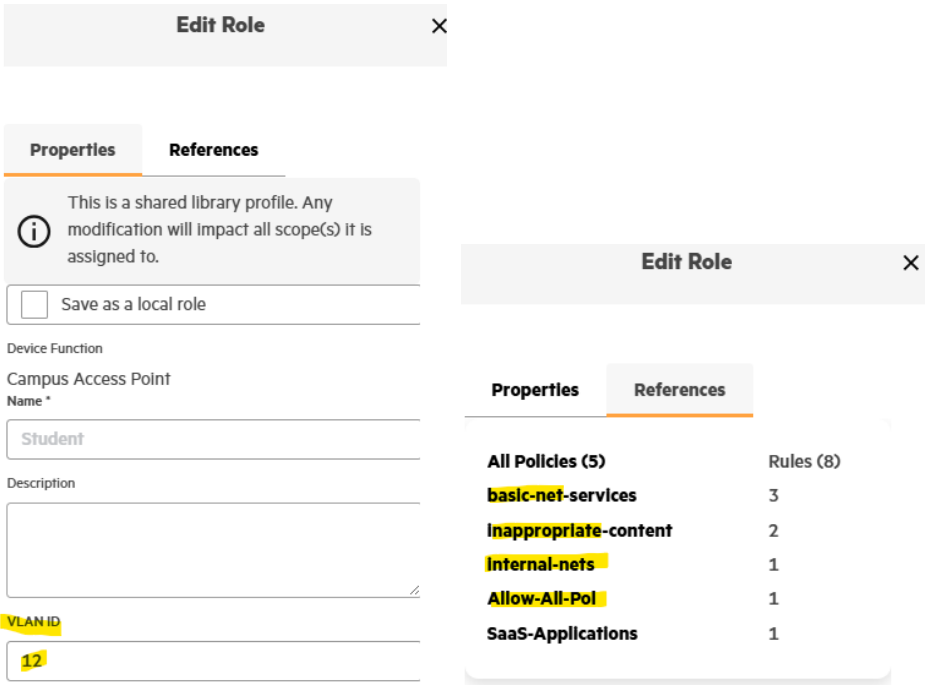
This WLAN previously used ClearPass as its authentication server group. I'm changing it to Central NAC. Once you've saved the profile, make sure it's assigned to the appropriate device function.



For this example, I'm using the existing Student role to assign VLAN 12 and apply the firewall policies shown below. I covered user-role configuration in the previous technote, so I'm including these screenshots for reference.

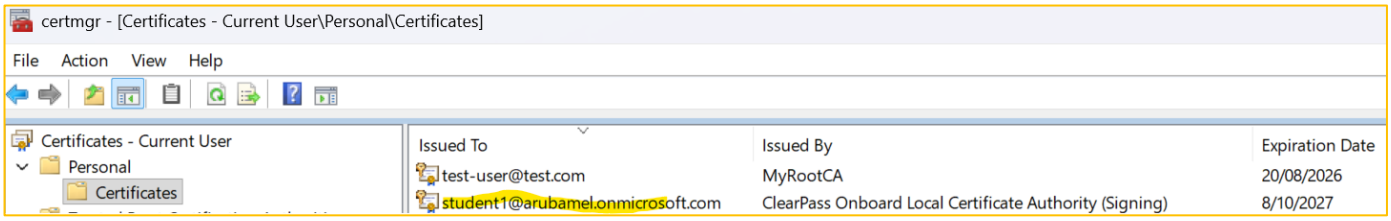


Since I have covered user-role configuration in my last technote, I am just showing Student role here for completeness.

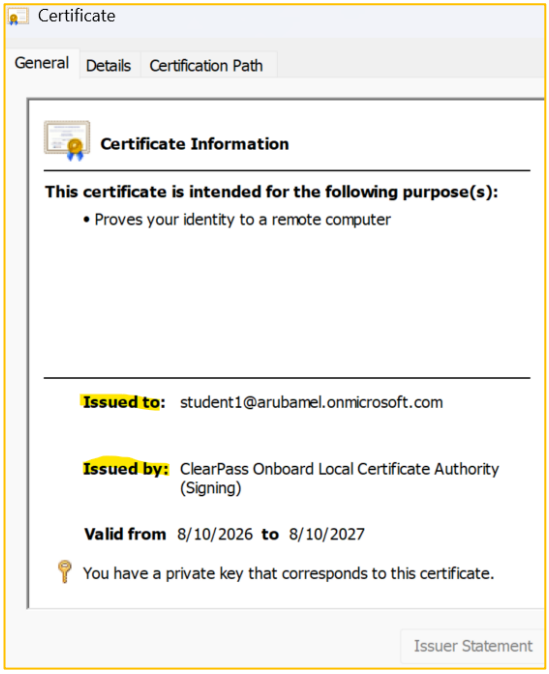


3.1 Existing User Certificate

Before changing authentication, let's check what's already on the client. This user has been onboarded through ClearPass Onboard and already has a certificate for EAP-TLS authentication. You can use certmgr and display the current user certificates on the windows laptop. Here we see that there is a certificate for student1 that is signed by ClearPass Onboard Local Certificate Authority with the displayed expiry date.

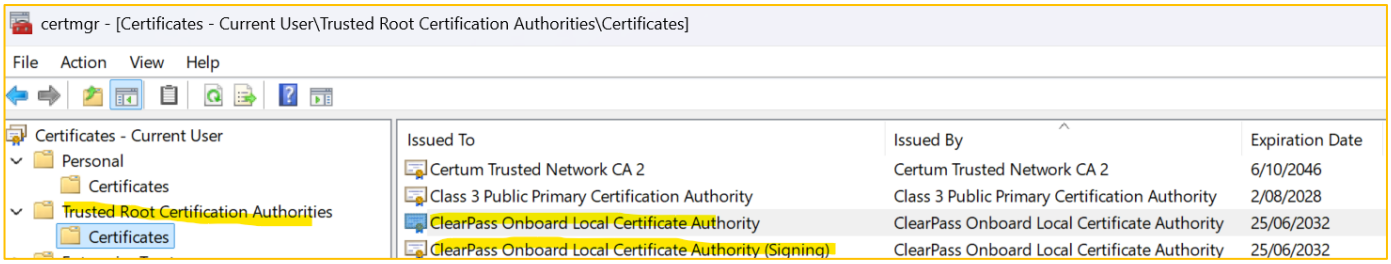


When I double click on it, I get the following details

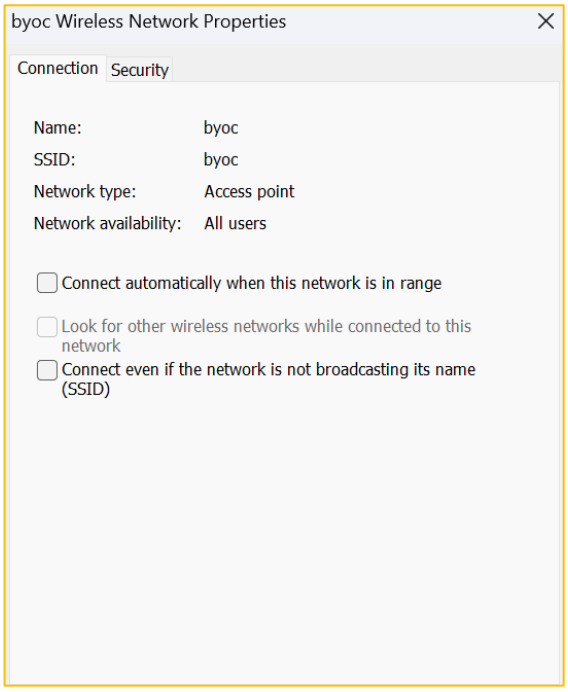


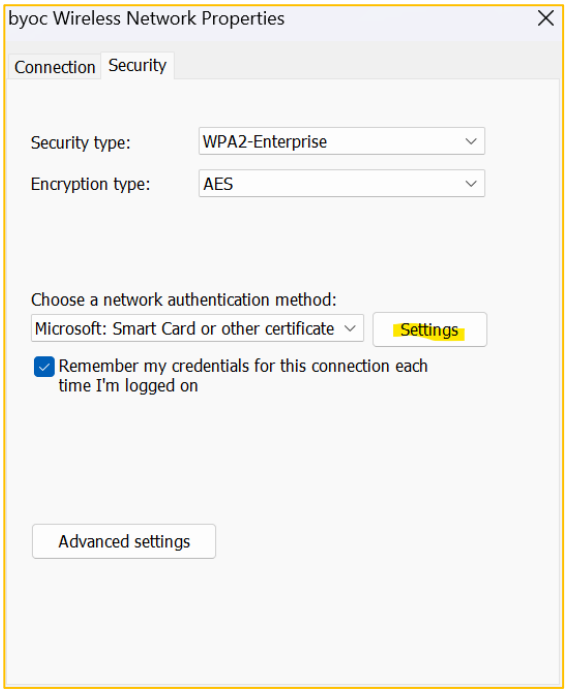


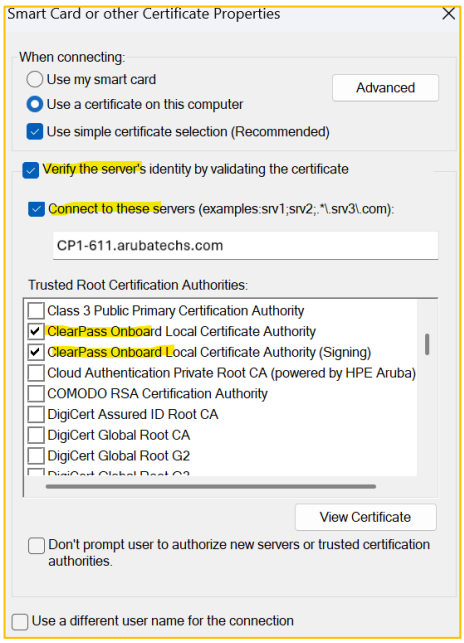
Now for all this to operate nicely, the two local CA and Local CA signing certificates should be listed in the trusted root certification folder. And the next thing we need to check is exactly that.

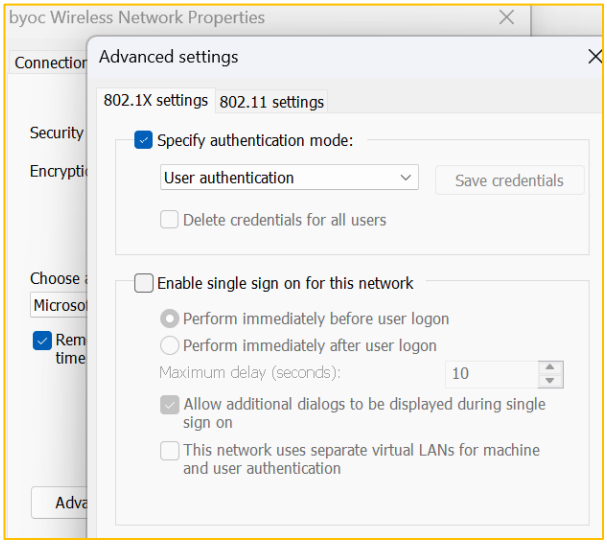


So now that the certificates are in order, let's check the existing wireless profile. The screenshots below show the authentication method, trusted CAs, server names and user-authentication settings used in this example.







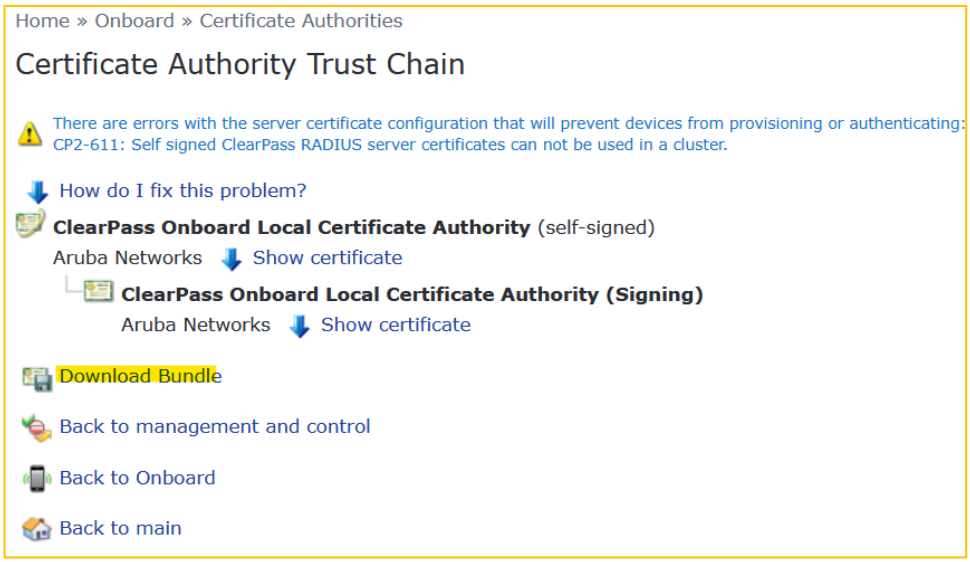


3.2 BYO Server Certificate and Trusted CA Certificate Configuration

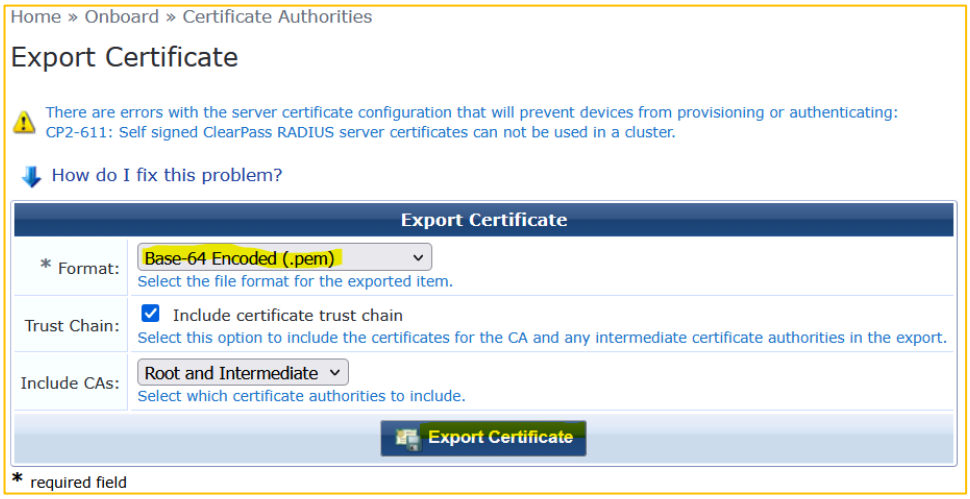
Since we are using ClearPass Onboard CA as our CA that has signed the BYO certificate and it was also confirmed in the previous section, first we have to export the onboard CA certificates. For that we navigate to the onboard section and then to Home » Onboard » Certificate Authorities to list the certificates.



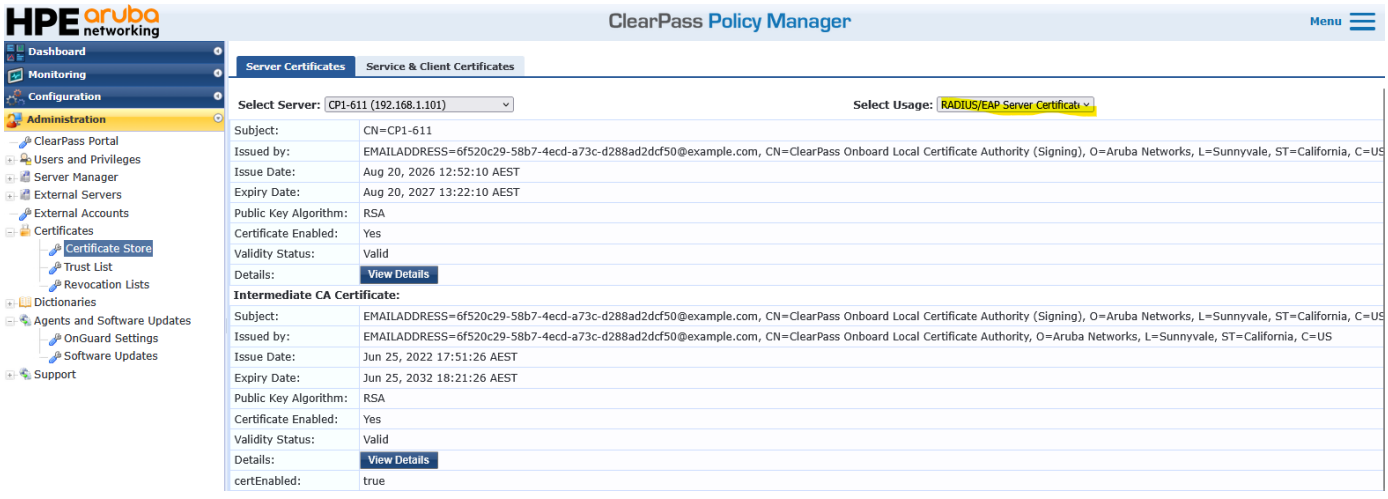
By clicking on the trust chain, we bring up the following where we can download the bundle.

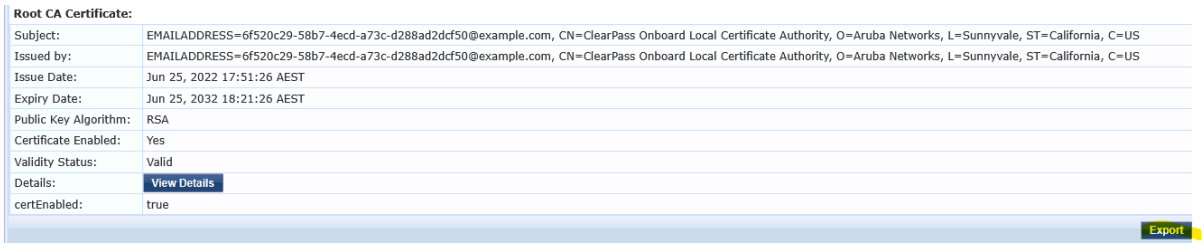


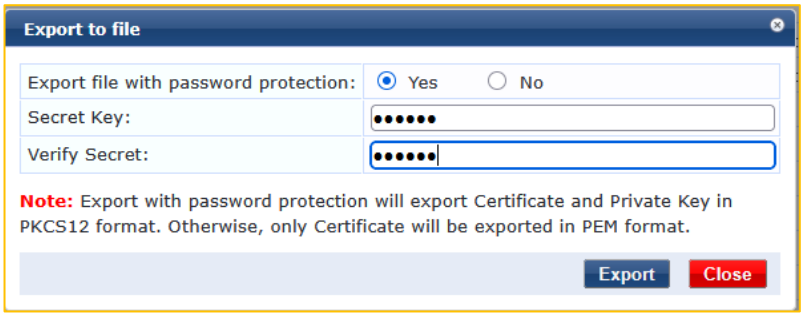
Make sure you change the format to PEM which automatically bring up the follwoinf and will inlcude the root andintermediate CAs.



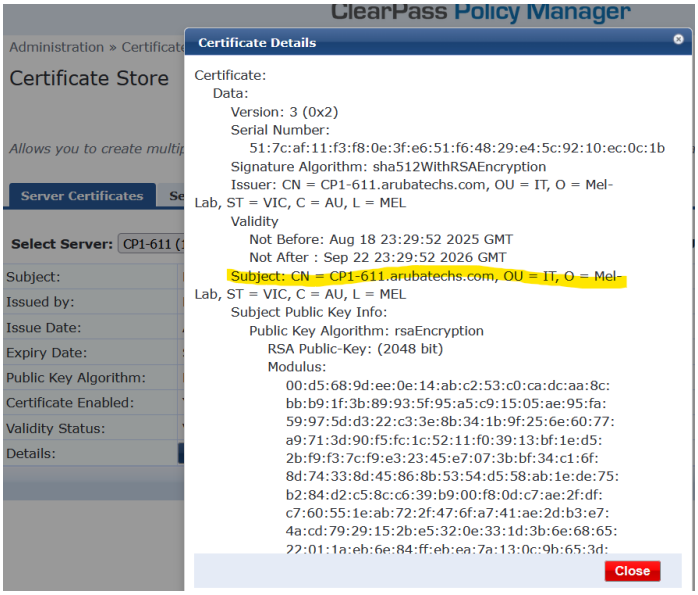
Next we'll export the EAP server certificate, for that we'll navigate to Administration » Certificates » Certificate Store

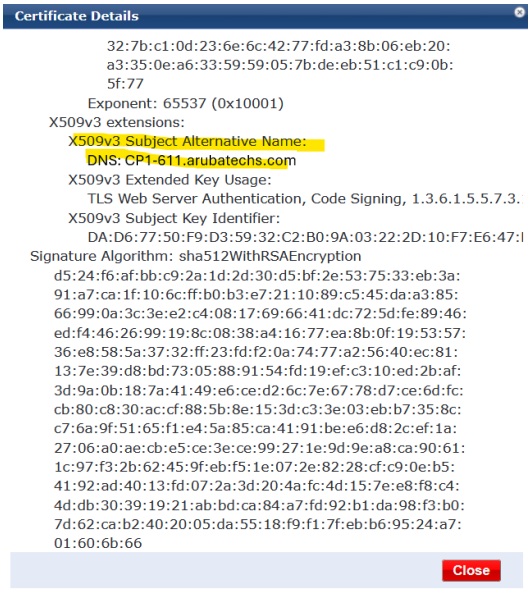






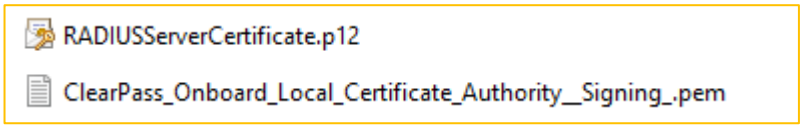
Note that the EAP server certificate should have a SAN field, if not, regenerate a self-signed certificate with SAN field.





3.3 Converting Certificates

Here we have two certificates as shown below. The first one is the radius server certificate as the name indicates and the other one is the trust chain for Onboard CA that has signed the RADIUS server certificate.



Starting with “RADIUSServerCertificate.p12”, a .p12 extensions indicates that the certificate is based on the PKCS #12 standard that bundles a private crypto key, an X.509 public key certificate, and often an intermediate trust chain into a single, password-protected binary file.

This radius server certificate needs to be in PEM format and should include server certificate, all the intermediate certificate and root certificate. It is often best practice to separate them into individual files for clarity and security.

So first we'll extract only the certificate(s). OpenSSL is one of the best tools to convert and extract private keys from certificates, so here we are using it for exactly that purpose.

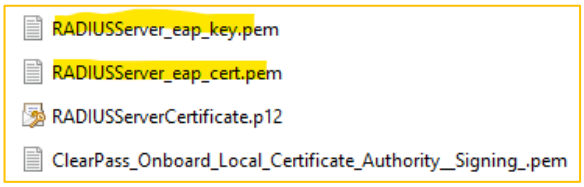
The following will extract the full trust chain without the private key.

```
openssl pkcs12 -in RADIUSServerCertificate.p12 -out RADIUSServer_eap_cert.pem -clcerts
-nokeys
```

and this command will only extract the private key.

```
openssl pkcs12 -in RADIUSServerCertificate.p12 -out RADIUSServer_eap_key.pem -nocerts
-nodes
```

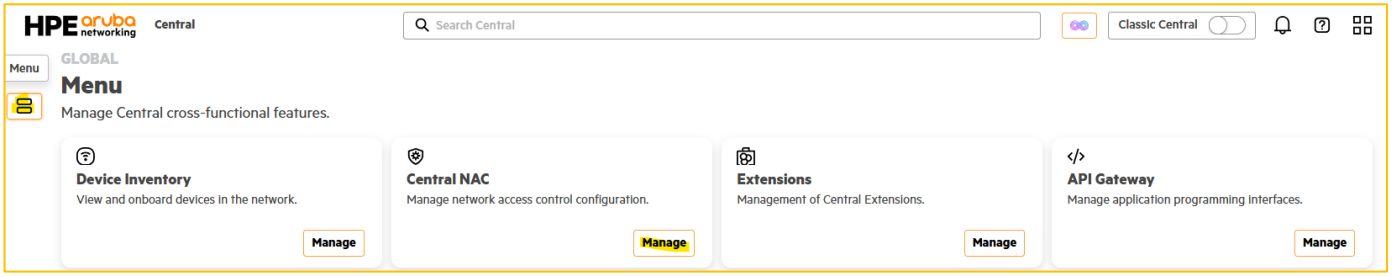
The two commands will create RADIUSServer_eap_cert.pem containing only the certificate(s) and RADIUSServer_eap_key.pem containing the unencrypted private key.



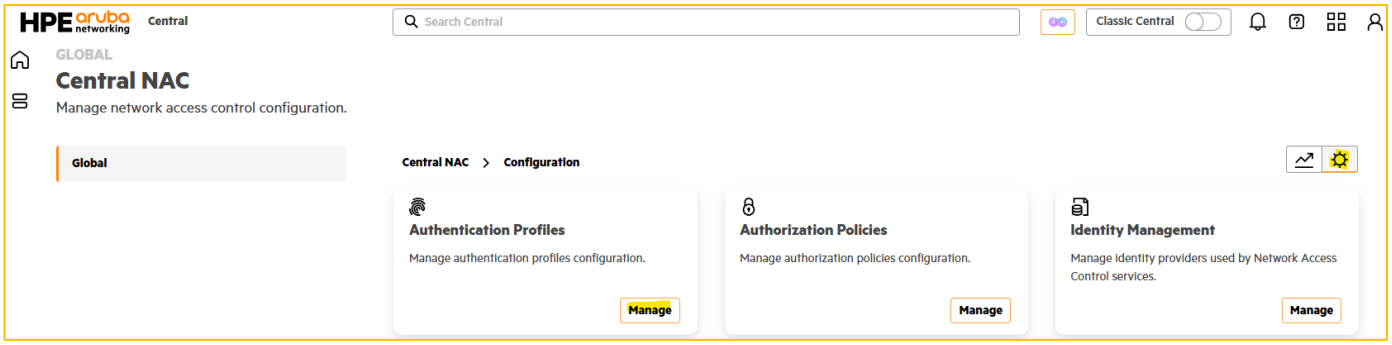
Now we have all our certificates which will be using in the next section.

3.4 Authentication Profile

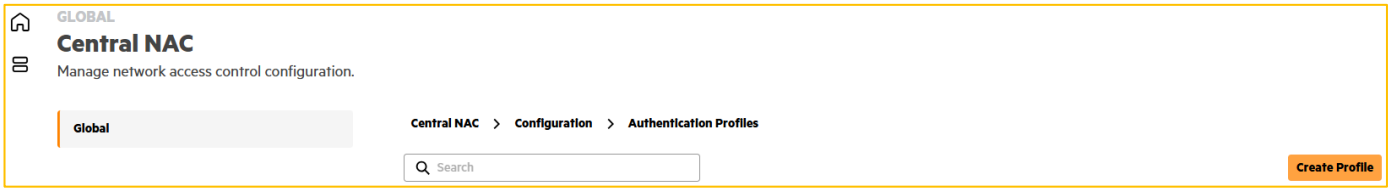
The next task is to configure CNAC Authentication profile, from the main page, you need to navigate to Manage Central NAC by click on the burger symbol.

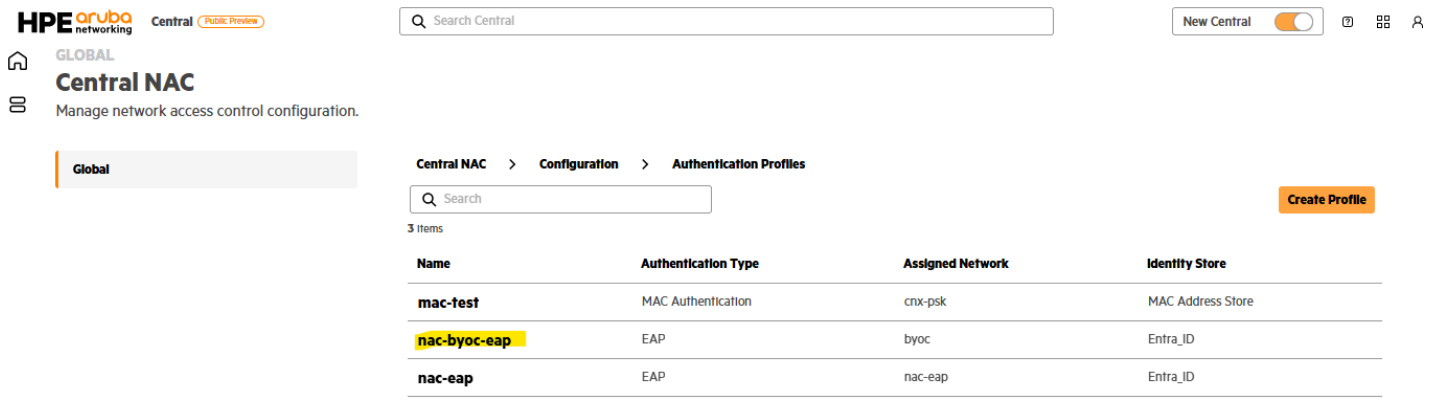


Then click on the gear icon and start with Manage Authentication Profile card.

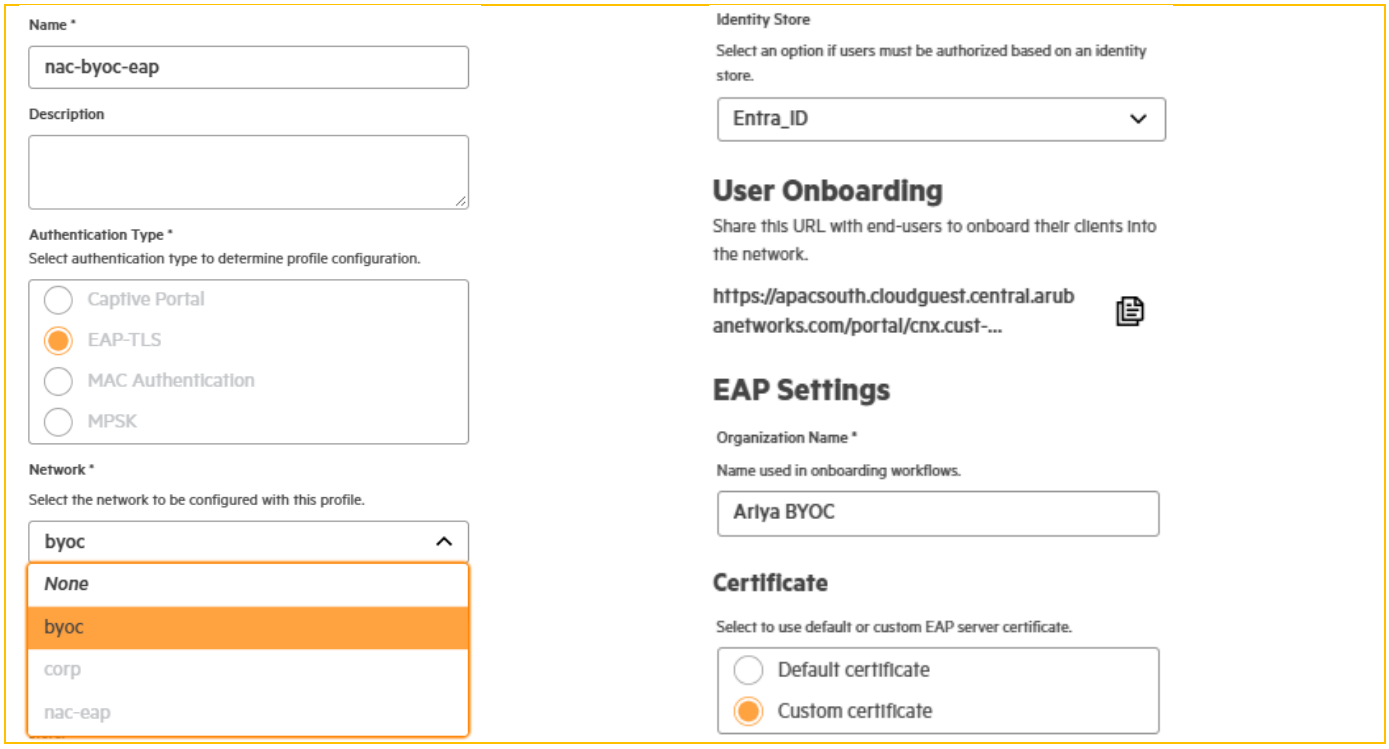


Here we'll create a new profile.

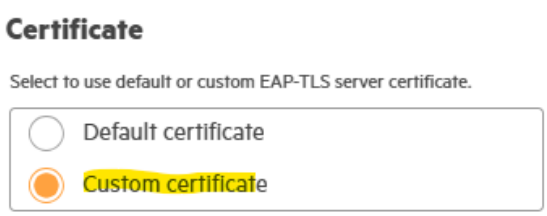




We'll start with the name and then select EAP-TLS as authentication type, followed by selecting the WLAN profile that we created earlier.



The next is the certificate section and for BYOC we have to use custom certificate



Now we get to upload our RADIUS server certificate we exported from ClearPass. There are 4x sections here

1. **EAP-TLS Server Certificate -** *Provide certificates as a sequence of PEM encoded X.509 certificates order from leaf server certificate, then signing intermediate CA's, finally root CA (if included).*

This is our "RADIUSServer_eap_cert.pem" file that we separated from its private keys. Note that you need open the file and then copy from the begin certificate to the end, exactly as shown below.

```
-----BEGIN CERTIFICATE-----
MIID7jCCAtagAwIBAgIBJDANBgkqhkiG9w0BAQ0FADCB0jELMAkGA1UEBhMCVVMx
EzARBgNVBAgMCkNhbGlmb3JuaWExEjAQBgNVBAcMCVN1bm55dmFsZTEXMBUGA1UE
<lines removed>
EDYVi7gx9BcJIba19mGcvbb0Lt7s/AWzZERYtgWUT97vmjebHtY4kOVvFVyGMUDL
lU5XjOGpKuVcd3ZVgQcad+ju1KqGEuOwML3sUNlRtky3THYGurTbA4VTH8u6ZRBH
zVw=
-----END CERTIFICATE-----
```

2. **EAP-TLS Server Key -** *Provide EAP-TLS server key as a PEM encoded private key.*

You need to do the same thing with the file "RADIUSServer_eap_key.pem" and copy from the begin private key to the end, exactly as shown below.

```
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQC6kVzFBxp3Tvp2
<lines removed>
gHJT7spXH9F9yCnsS+GmsRMvw6tymdLqEhLvQf9muOlVHqZcs+WpCgeUbJwacmVN
Sq634twkR2VCsSh/W5tjow==
-----END PRIVATE KEY-----
```

3. **EAP-TLS Server Key Passphrase -** *If EAP-TLS Server Key is encrypted, provide the corresponding decryption passphrase.*

Type in the key passphrase you used when you exported the server certificate from ClearPass.

4. EAP-TLS Client CA chain - *Provide the trust chain as a sequence of PEM encoded X.509 certificates.*

This is the file "ClearPass_Onboard_Local_Certificate_Authority__Signing_.pem" that we exported from ClearPass onboard CA which has the CA chain.

```
-----BEGIN CERTIFICATE-----
MIIEsDCCA5igAwIBAgIBAjANBgkqhkiG9w0BAQ0FADCByDELMAkGA1UEBhMCVVMx
EzARBgNVBAgMCkNhbGlmb3JuaWExEjAQBgNVBAcMCVN1bm55dmFsZTEXMBUGA1UE
<lines removed>
baew47Z1T7HfJmfpJEMOapPlWzftKQZy9l6WNZT67LewLYMhX5vhikVGj0mLIjcW
oJd893+wz9OkOjtTr/POZmWmhLxno2fRNFSNId07VqRoAuV7nLTSpR6CwZUoSyXI
9TX8RA==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEgzCCA2ugAwIBAgIBATANBgkqhkiG9w0BAQ0FADCByDELMAkGA1UEBhMCVVMx
EzARBgNVBAgMCkNhbGlmb3JuaWExEjAQBgNVBAcMCVN1bm55dmFsZTEXMBUGA1UE
<lines removed>
ytZp1t954RtXUIDIE5tJQtJtf8z9De4BHN4+2VHgiQ1QD6ko4f7Zn+UhGKokLR9t
dFrNkDmiClvwQNZnvMU+FyQp03OSRDhRKKY3ZybpP6hQITop1a8iMe19OwNSQ8XY
f7XFHedlXw==
-----END CERTIFICATE-----
```

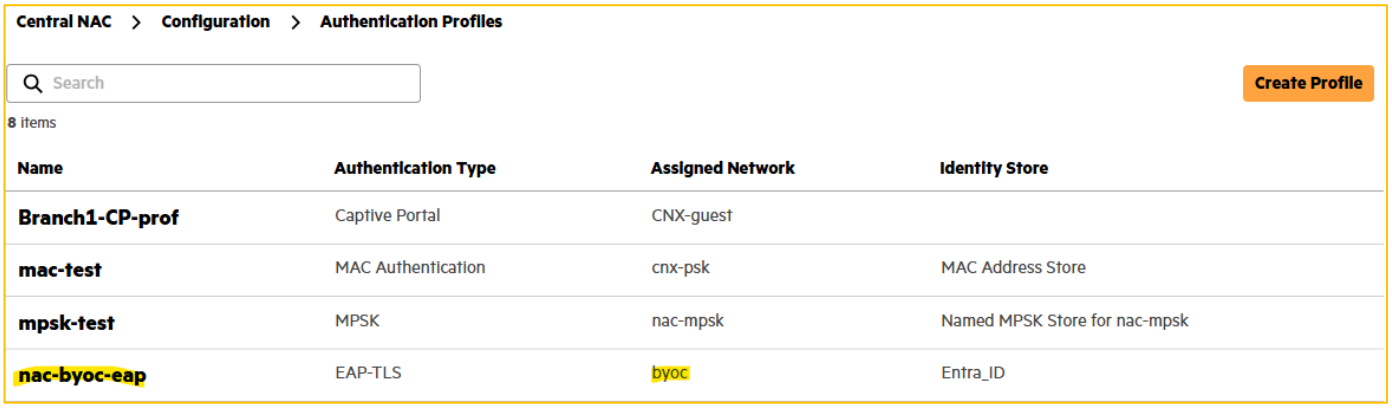
Now the next thing is to enable Online Certificate Status Protocol (OCSP). This is optional so you need to enable it if you require it. Note that when you enable this, CNAC would use the OCSP URL from the client certificate to validate the certificate. If client certificates do not have an OCSP URL or if you wish to override the OCSP URL specified in the certificate, there is option to provide a OCSP URL.

And finally, you need to select an option for OCSP Check Failure Response.

Generally one would want OCSP checks to always be enforced but there are cases where one might want the devices to connect to the network to be able to get a new certificate.



Once you have saved it, it will be listed under the authentication profiles as shown below.

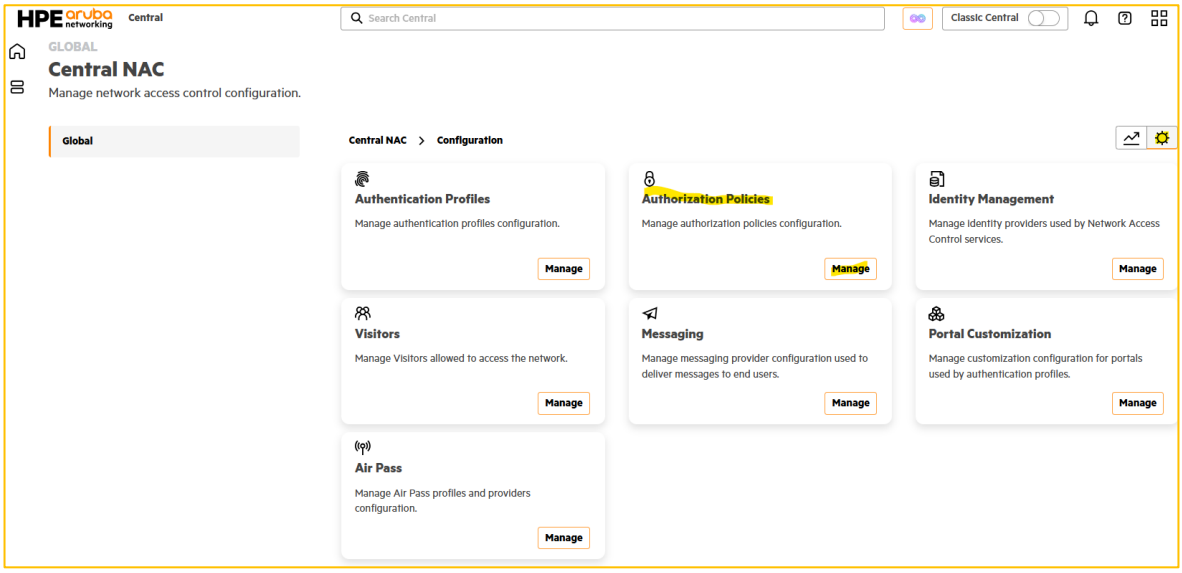


Name	Authentication Type	Assigned Network	Identity Store
Branch1-CP-prof	Captive Portal	CNX-guest	
mac-test	MAC Authentication	cnx-psk	MAC Address Store
mpsk-test	MPSK	nac-mpsk	Named MPSK Store for nac-mpsk
nac-byoc-eap	EAP-TLS	byoc	Entra_ID

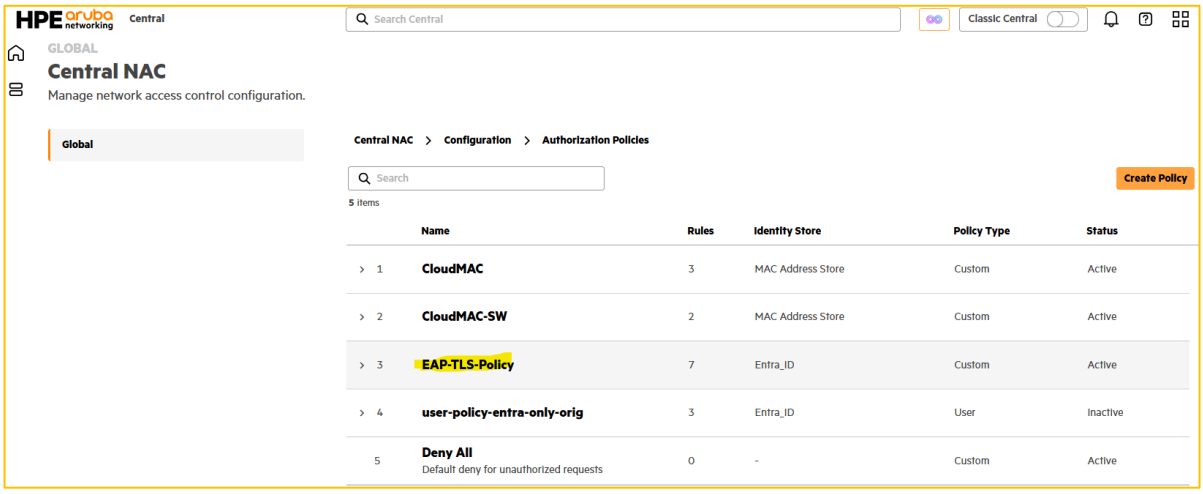
There are couple of things you need to know, the first one is that you can chain multiple PEM formatted x509 root CA certificates together under the field “EAP-TLS Client CA chain”. The other thing is that both ECC and RSA certificates are supported when you add the RADIUS server certificate.

3.5 Central NAC Authorisation Policies

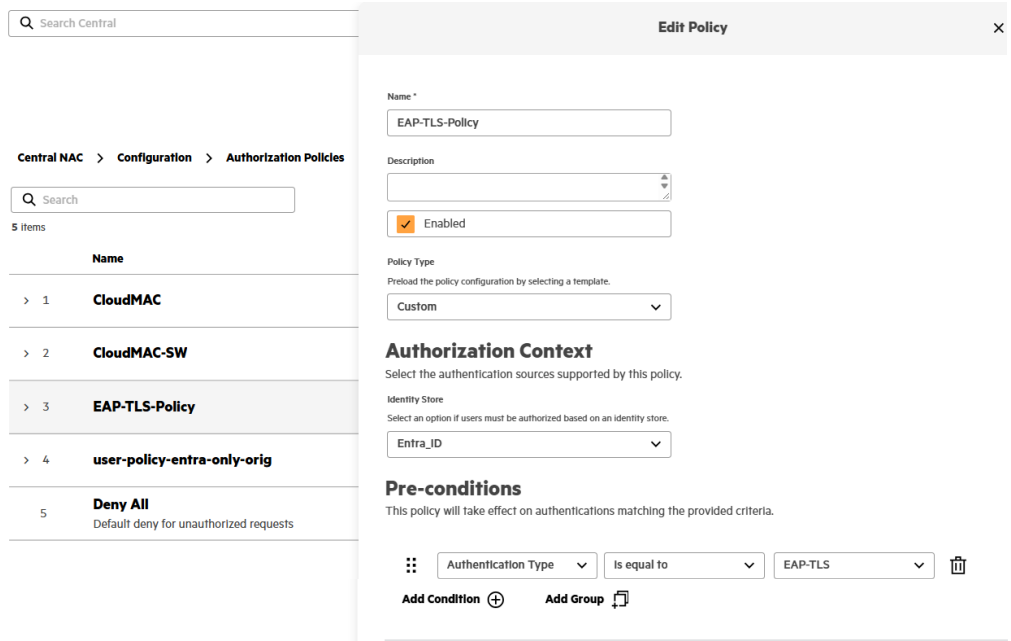
Once a user is authenticated it confirms user’s identity. The authorisation policy then determines the access they receive. This can be based on any user attribute and/or device context. So, the next step is for us to configure the authorisation policy, and we do that by navigating to Central NAC and configuration section and click on the Authorization card shown below.



Here I have already configured a few authorisation policies and currently it is applied globally. As you can see first couple are authorisation for MAC addresses and then the third one is our EAP-TLS-Policy that has a reference to our BYOC and then we have an inactive policy and finally a Deny All policy.



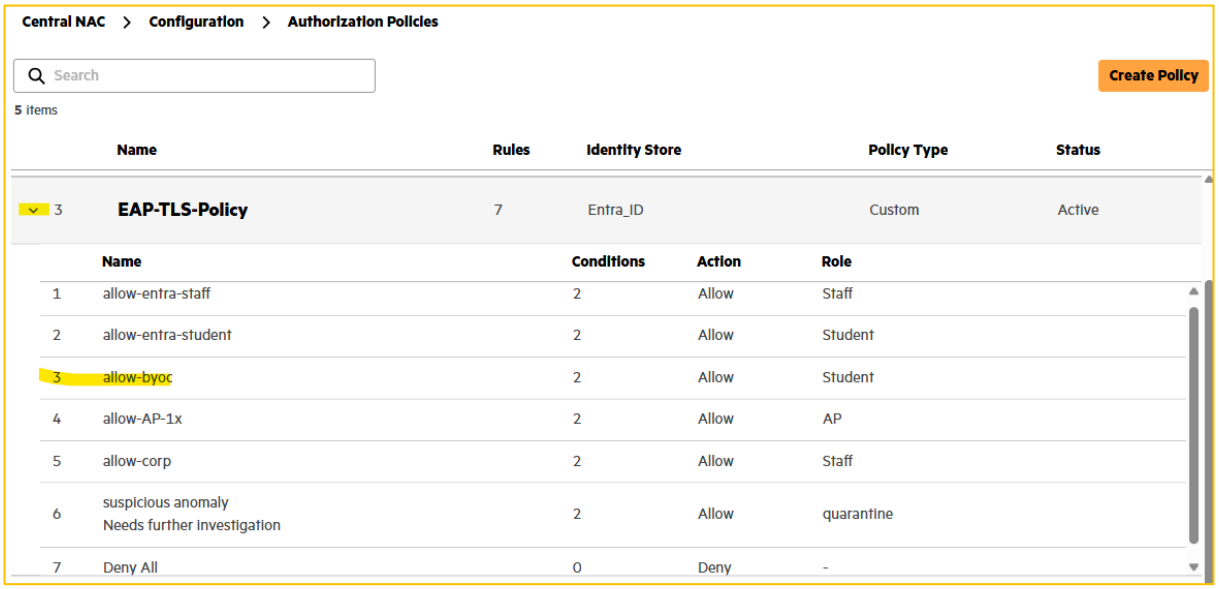
We can see that EAP-TLS-Policy has 7x rules and the status is active. But let's first click on the EAP-TLS-Policy



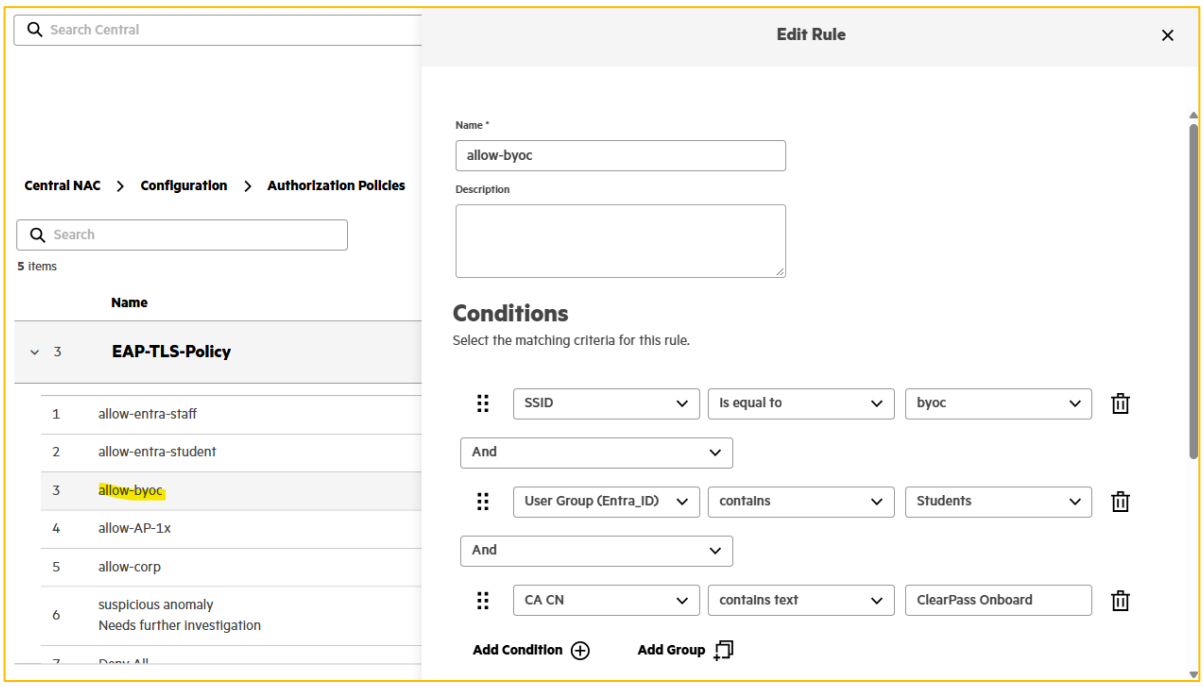
The policies have pre-conditions that determine which policy would be used. Here our precondition is authentication type being EAP-TLS. The Pre-condition options are

- Authentication type [Captive portal, MAC authentication, EAP-TLS, MPSK]
- Authentication source [Identity store like Entra ID]
- Connection type [wired or Wireless]
- NAD Vendor [HPE Aruba Networking, Cisco Meraki wired, Cisco Meraki Wireless, Cisco Wired, Cisco Wireless, AOS Switch, HPE Comware Wired, IETF, Juniper Mist Wireless and Juniper Wired]

When a policy is first created, it would only have the Deny All rule within it. We have to add rules to the policy based on our requirements to then assign user role, VLAN id and session timeout to be returned after a successful authentication.

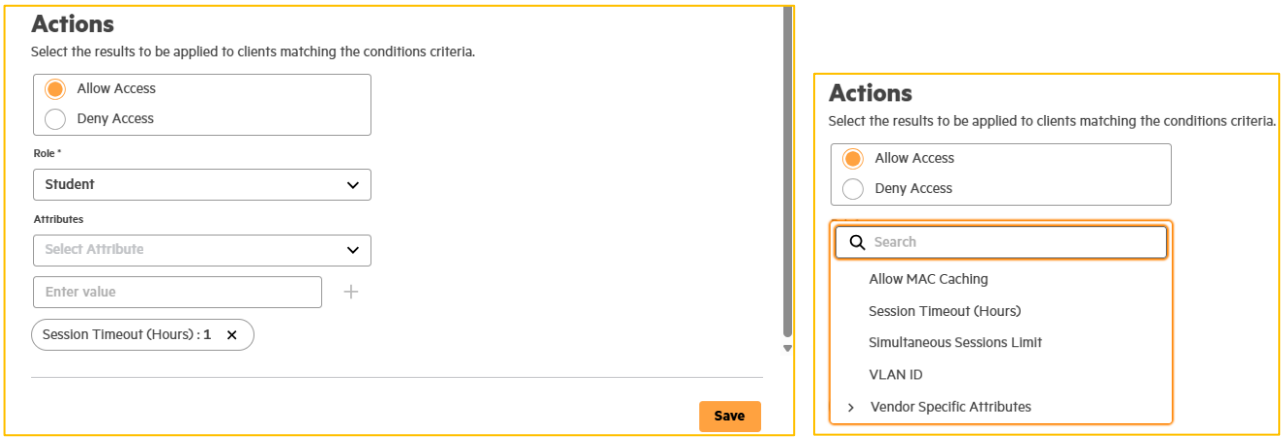


This authorisation policy includes rules for the pre-condition of EAP-TLS authentication, the first two rules are for authorisation directly for Entra users that are using the CNAC onboarding and CA Certificate, and the third one is for our BYOC use case. Let's look at it in more details by clicking on the allow-byoc policy.

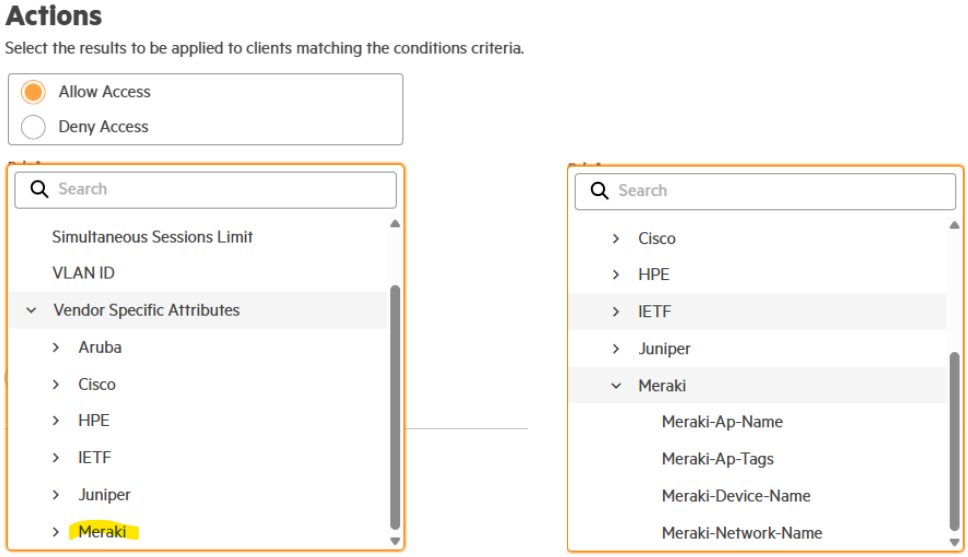


Here I am just showing that we can have several conditions, and it can be both AND/OR operations even though I am just using AND as shown above.

The sale rule does also have the Action section. You can also send back more than one attributes.



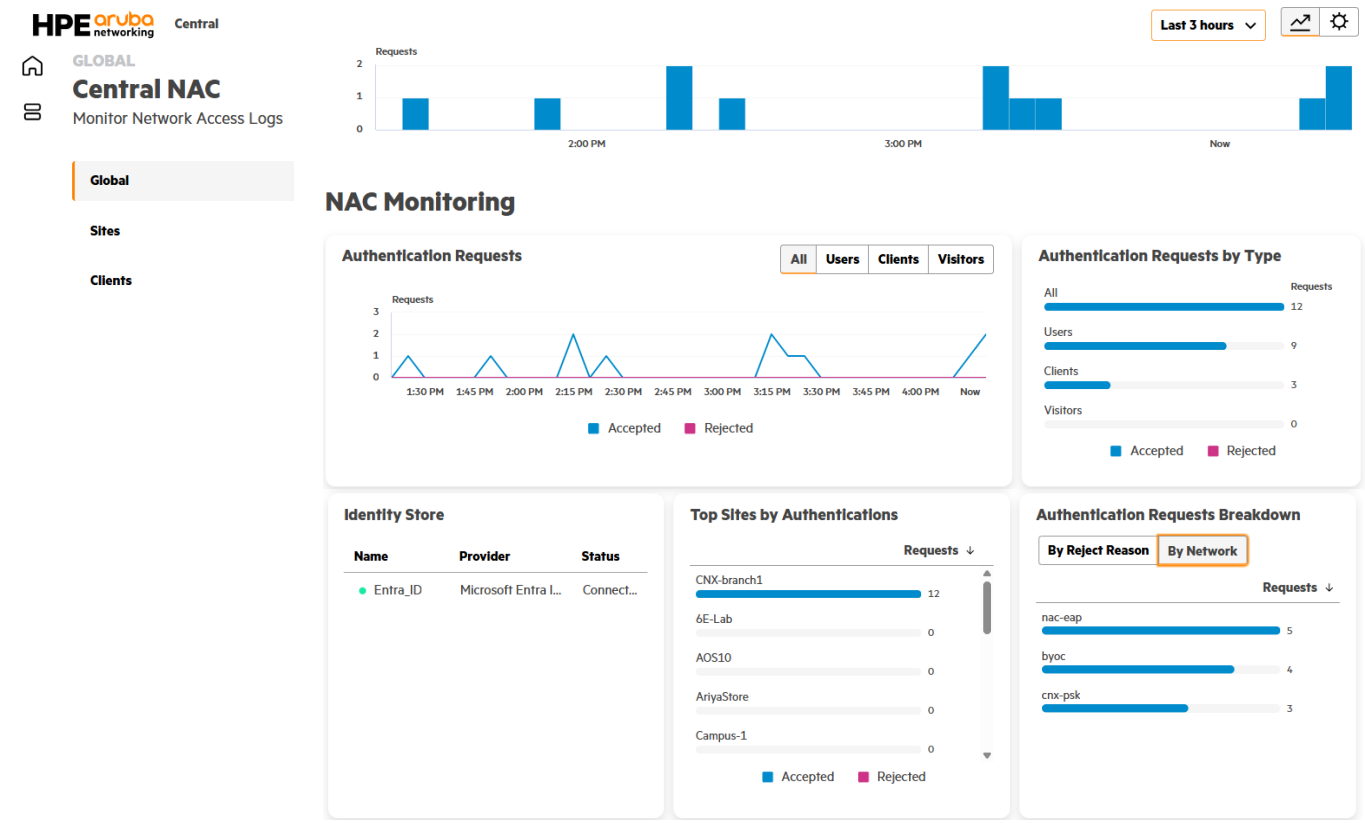
Here I am just using a user role that is already preconfigured to assign and session Timeout of one hour. But you can also add other attributes like Simultaneous session limits and even Vendor Specific Attributes (VSA).



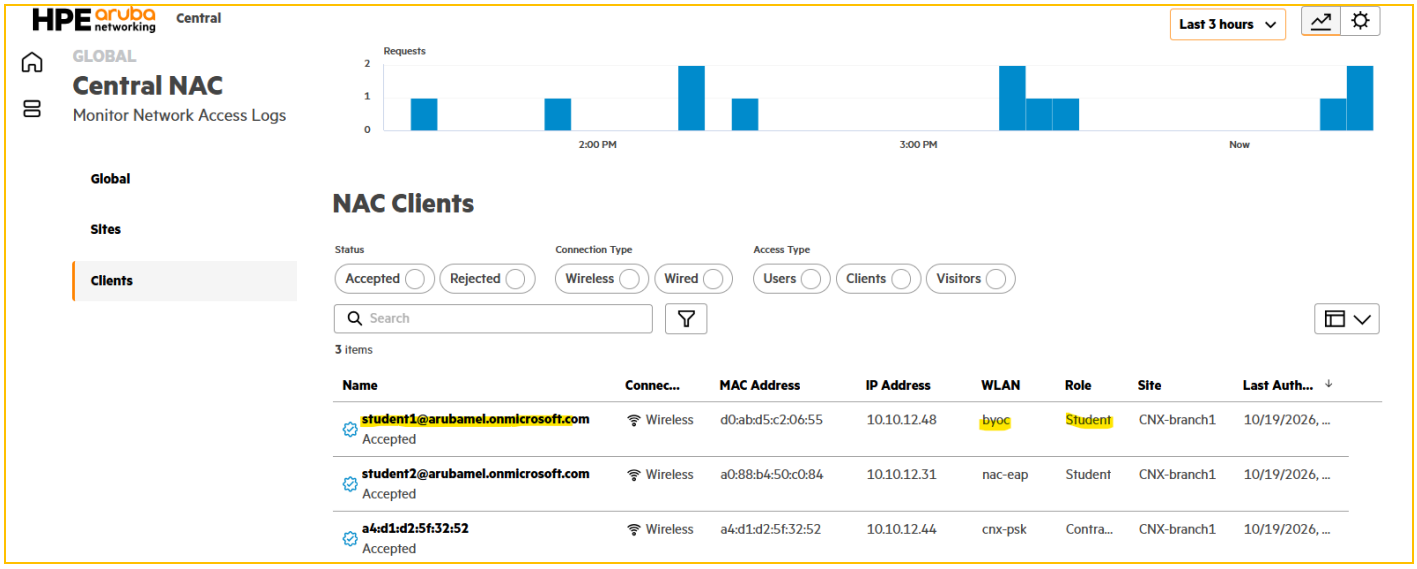
In the above diagram we are showing Meraki VSAs.

3.6 Client Testing

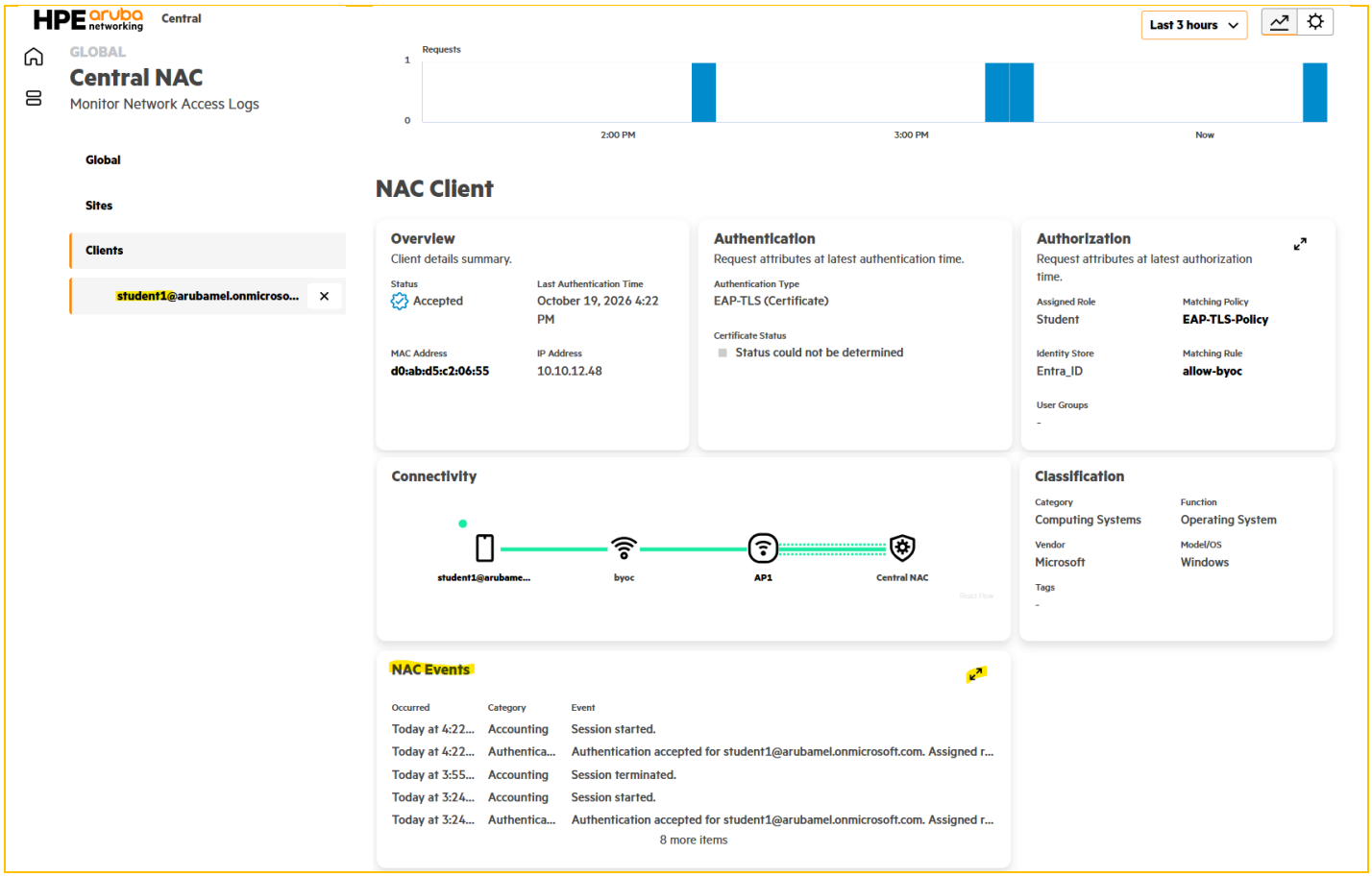
Now we have configured everything as outlines in the start of the technote and are ready to test. Let's navigate to Central NAC. Here we can see the overview of all the authentication at Global, Site level and at client level.



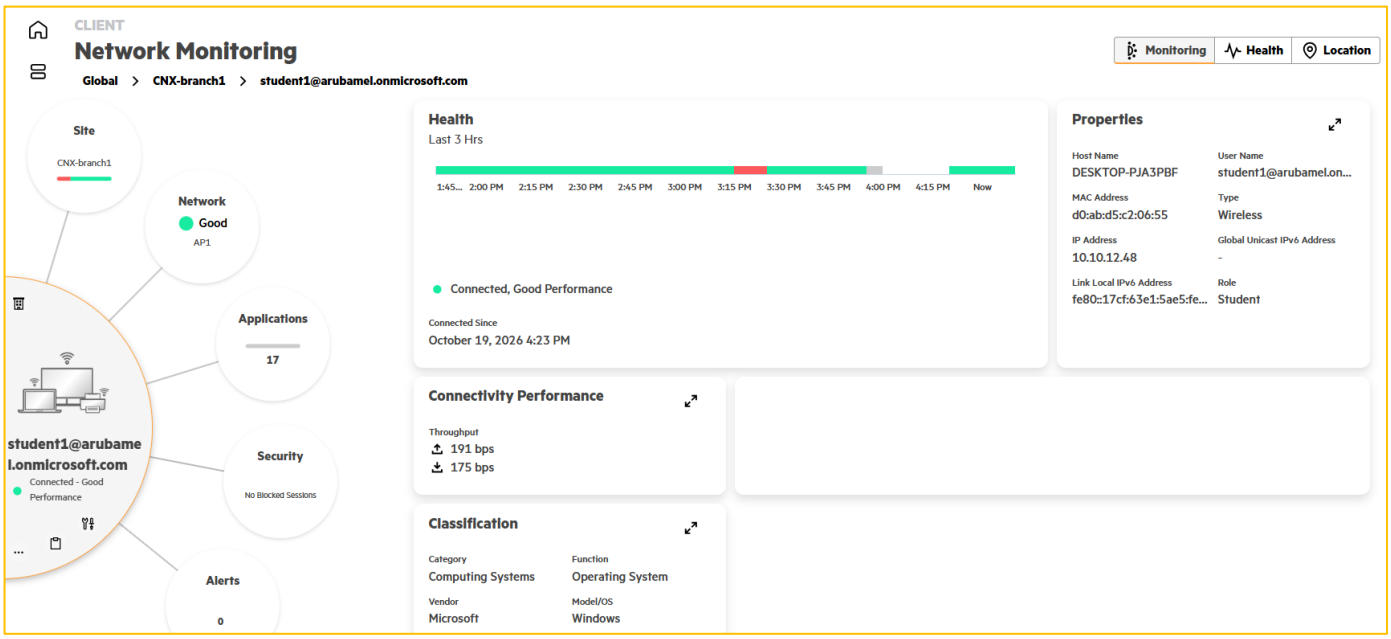
First we get a student1 that had been onboarded by ClearPass to connect to the BYOC wireless network and then we'll go to the client level CNAC monitoring.



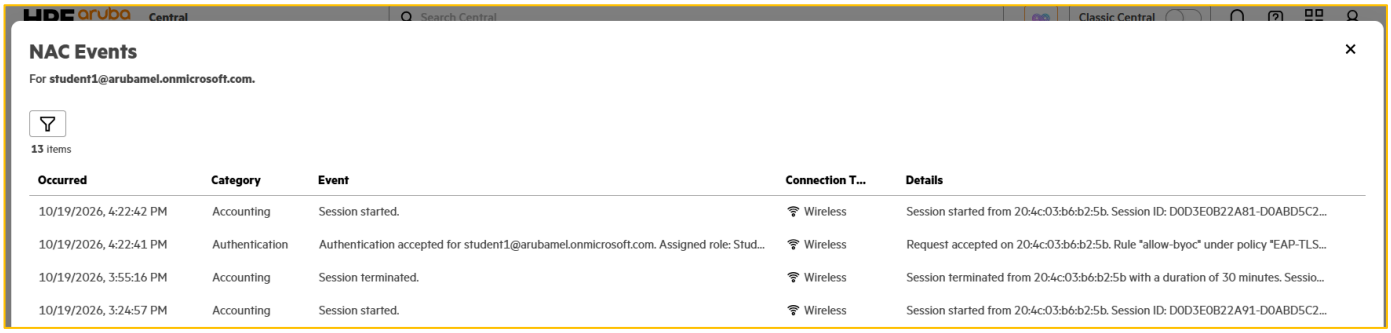
Note that in the above screenshot student2 was onboarded with CNAC. Now lts click on the Strudnet1 to get the authentication details.



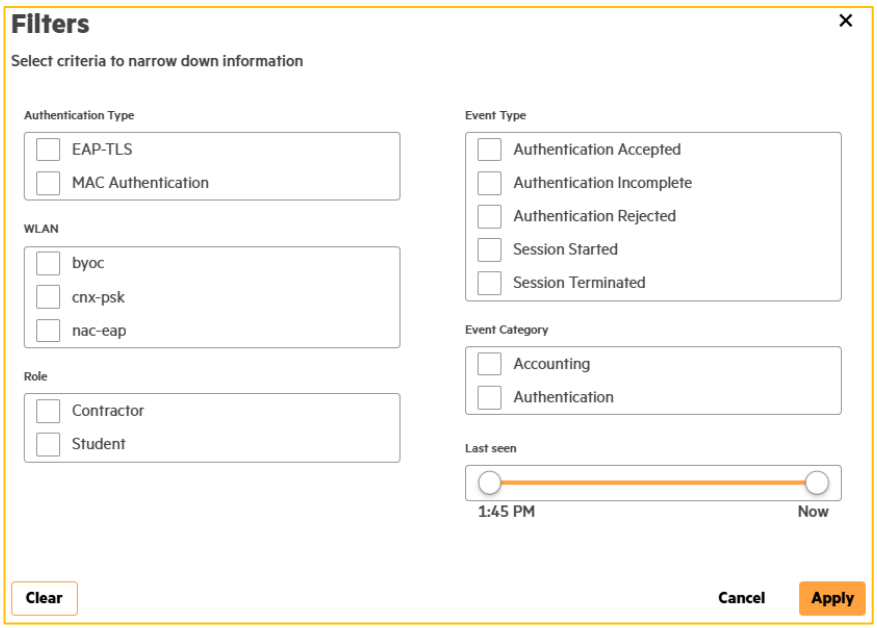
As shown above you can all the important information about the client and its authentication type that was used, the authorisation policy and its matching rule. You can also click on the Matching Rule allow-byoc, Matching Policy EAP-TLS-Policy or the MAC address to go to that specific attribute. For example, if you click on the MAC address, it will take you to client monitoring for it where you can also inspect all the other user context like application experience, etc.



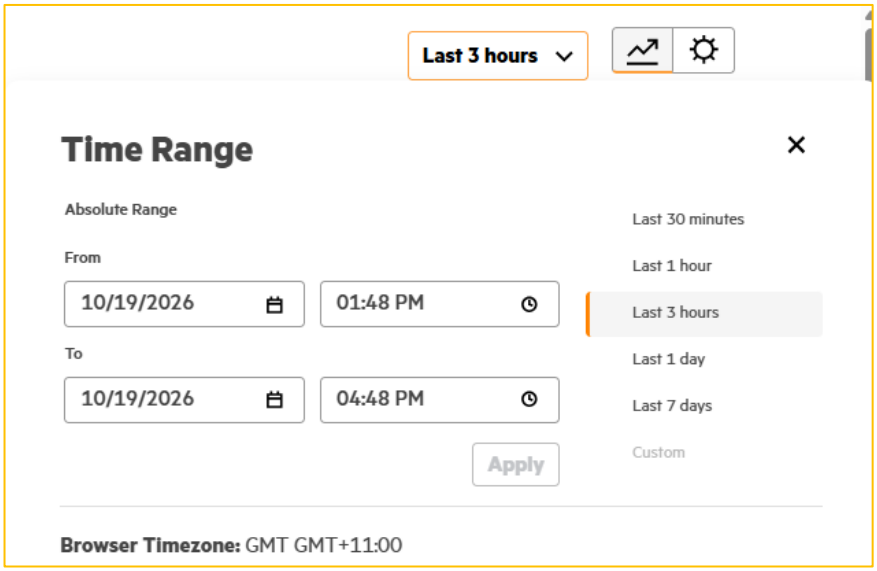
But coming back to the CNAC client monitoring, expanding the “NAC events” we get all the NAC evets for that user where we can filter and search for specific event.



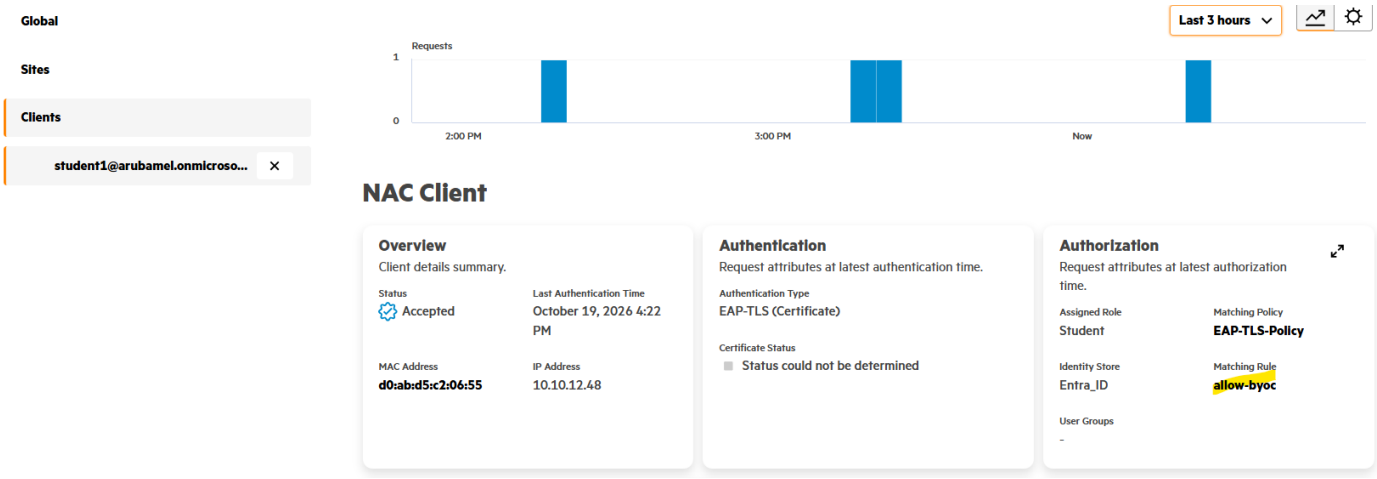
These are the available filters. The last seen is based on default the time filter (3 hours).



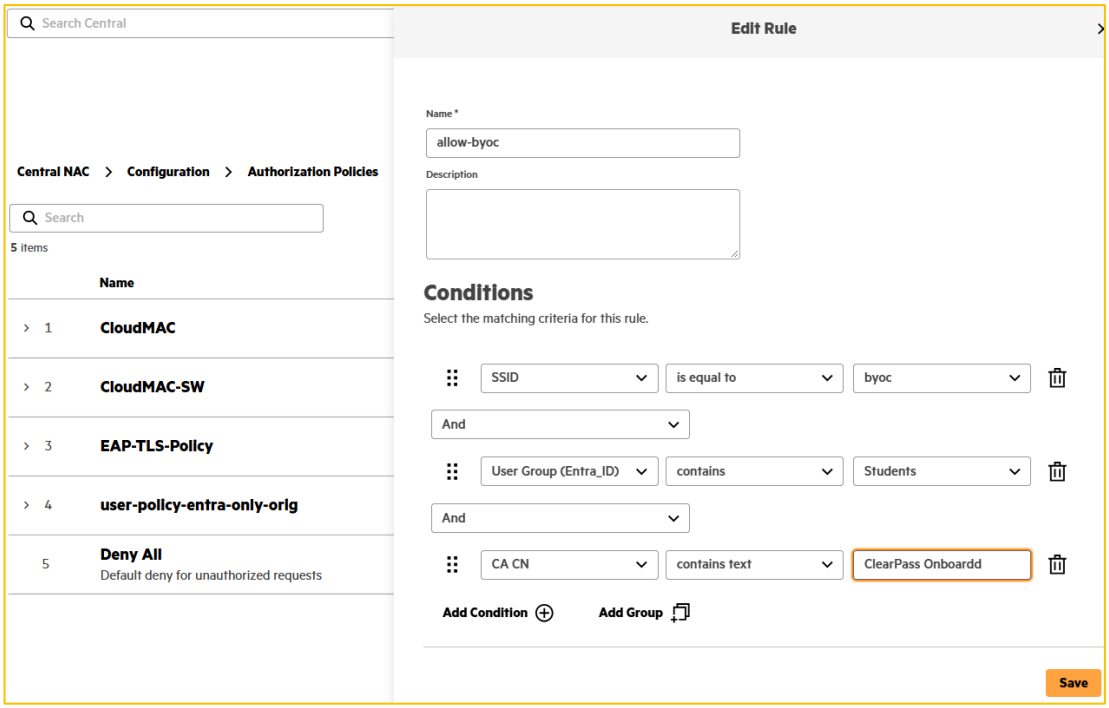
The time filter can be changed to 1 hour, 3 hours, 1 day, 7 days or a custom range.



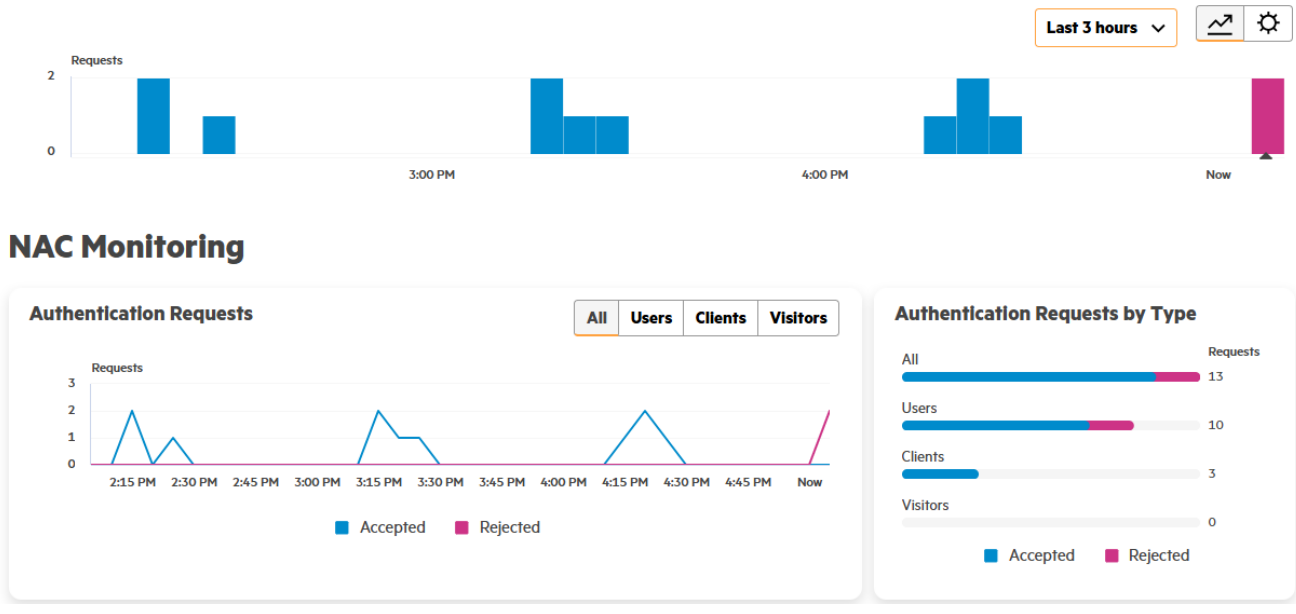
For our final test, I'll make a change to the authorisation policy rule to demonstrate that the CA certificate is being checked. As shown from the screenshot below, I click the "allow-byoc" matching rule from the CNAC client monitoring.

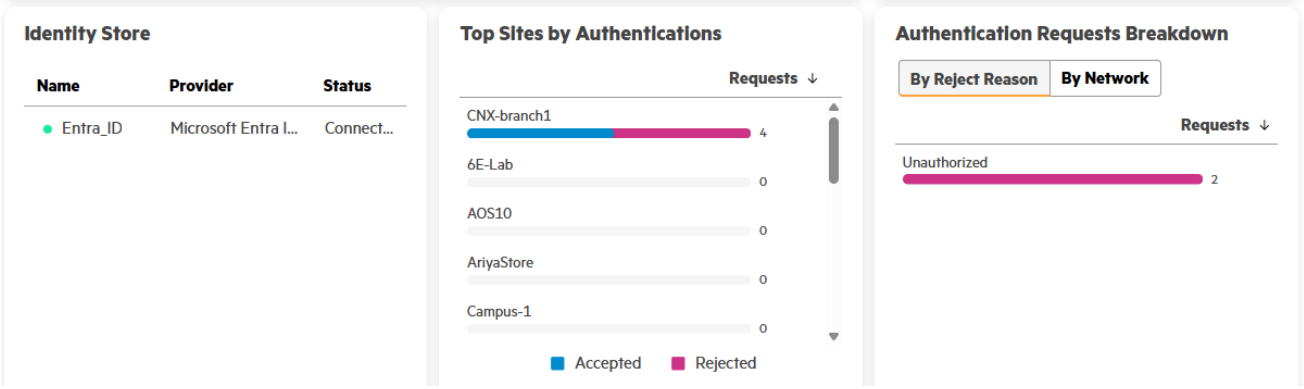


And it takes me to the exact rule. And here I'll deliberately change CA CN to "ClearPass Onboardd."

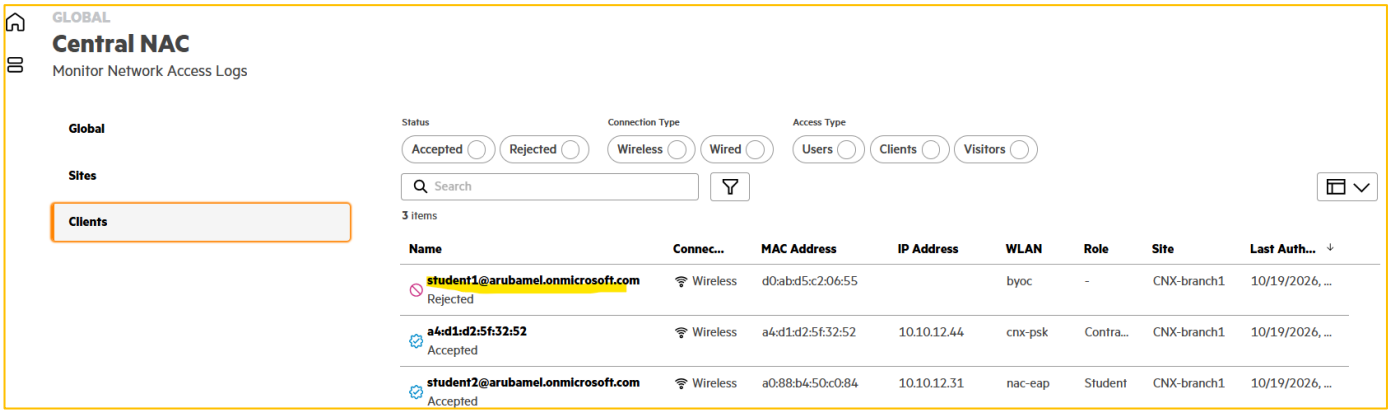


This will cause the client not to be able to connect anymore. Let's check the CNAC monitoring page. Note the triangle below the rejected bar which indicates a configuration change to gives you a quick reference point.

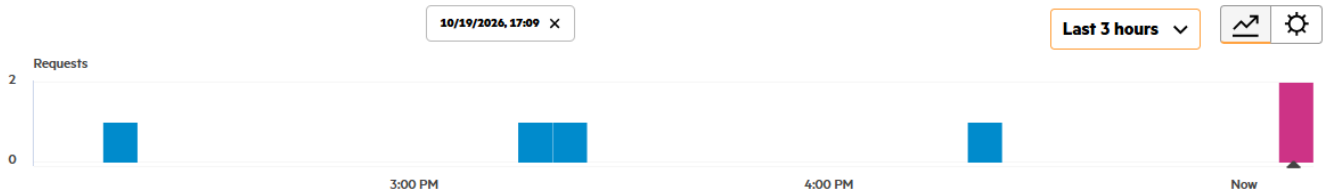




Now checking the CNAC Client monitoring, it displays that it was rejected .



Now clicking on the username, it takes us to CNAC view of that user that displays which rule in the authorisation policy caused the reject. So in our case it was the “Deny All “ rule because it did not match the earlier rule because we changed the CA CN to “ClearPass Onboardd.”



NAC Client

Overview

Client details summary.

Status: Rejected
Unauthorized

Last Authentication Time: October 19, 2026 5:07 PM

MAC Address: d0:ab:d5:c2:06:55

IP Address: -

Authentication

Request attributes at latest authentication time.

Authentication Type: EAP-TLS (Certificate)

Certificate Status: Status could not be determined

Status as of 19 October 2026, 17:13, not based on the selected time window

Authorization

Request attributes at latest authorization time.

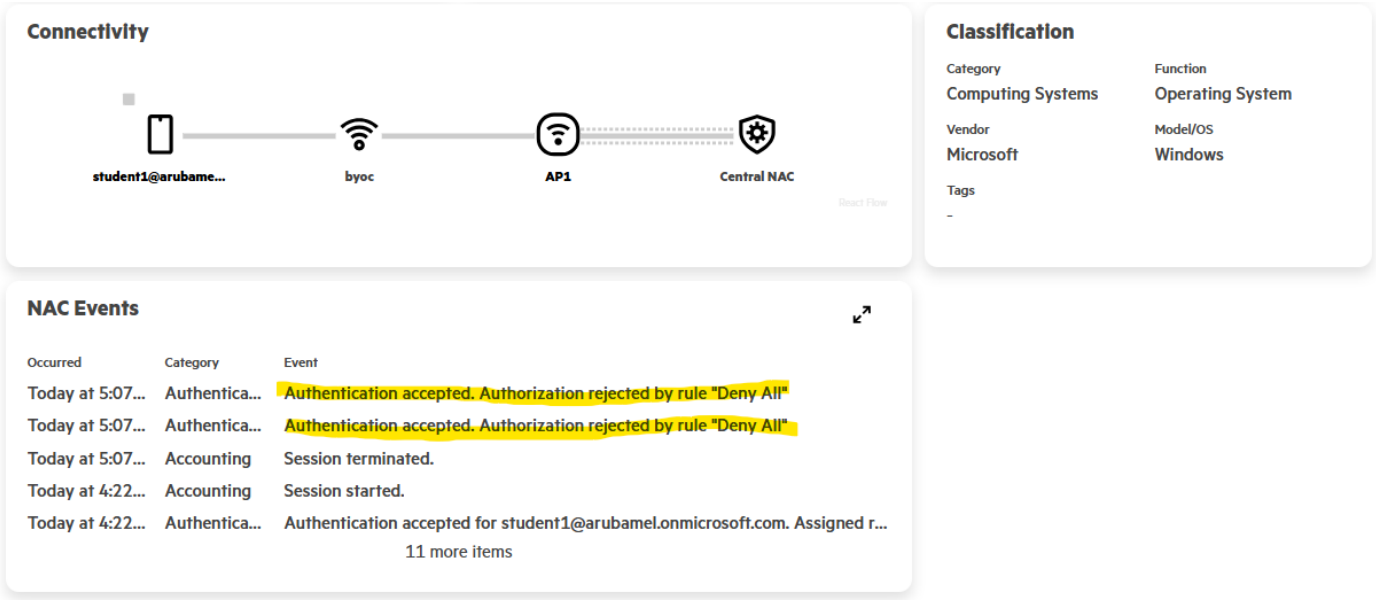
Assigned Role: -

Matching Policy: EAP-TLS-Policy

Identity Store: Entra_ID

Matching Rule: Deny All

User Groups: -



This concludes this technote, remember to restore the original CA CN back to “ClearPass Onboard.”