

1 Table of Contents

1	Table of Contents	1
1.1	Revision History	1
2	Overview.....	2
2.1	Things you need.....	2
3	ClearPass SSO Integration with Entra ID	3
3.1	Entra ID Configuration	4
3.2	Adding Microsoft Azure federated SSO certificate in ClearPass.....	8
3.3	Policy Manager SSO Identity Configuration.....	9
3.4	Policy Manager SSO Service.....	10
3.5	Policy Manager Onboard Authorisation Service.....	11
3.6	Policy Manager EAP-TLS Service	12
3.7	ClearPass Onboard Configuration.....	13
3.7.1	Network Setting.....	13
3.7.2	Configuration Profile.....	14
3.7.3	Provisioning Setting	14
4	User Onboarding Test.....	16
4.1	ClearPass Onboard Certificate Management	20
4.2	WLAN Connectivity Test	21

1.1 Revision History

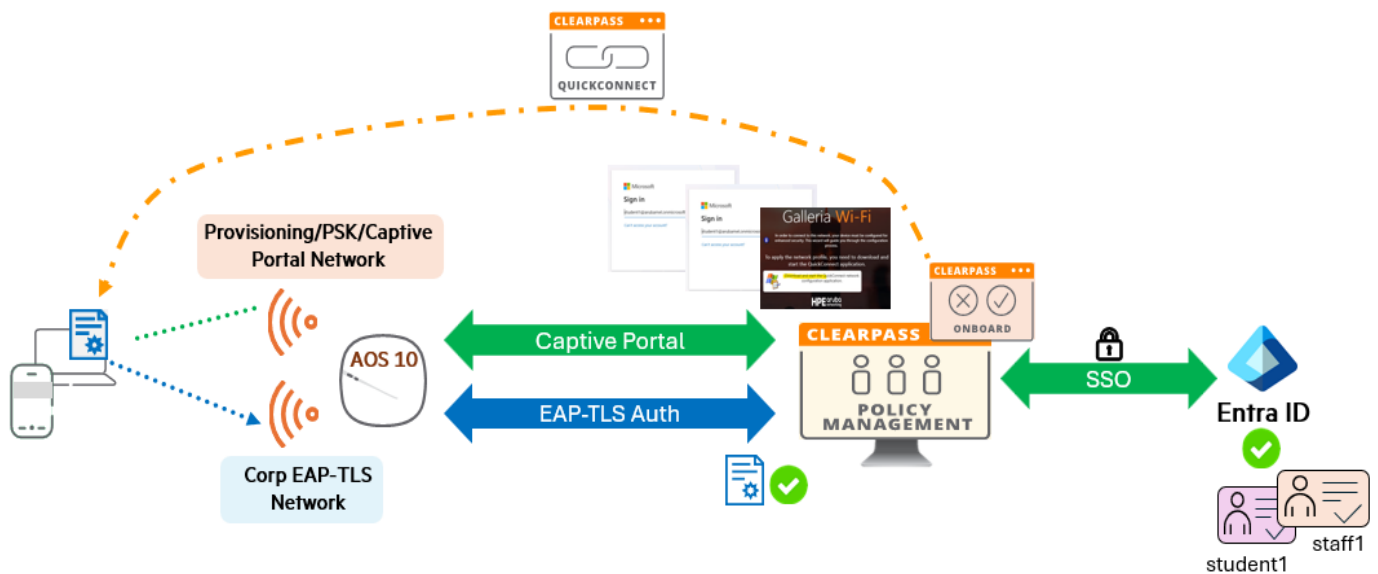
DATE	VERSION	EDITOR	CHANGES
09 Apr 2026	0.1	Ariya Parsamanesh	Initial creation
24 Apr 2026	0.2	Ariya Parsamanesh	Added the testing section

2 Overview

Here we'll configure ClearPass Onboard to create and issue user certificates for Entra ID users. This will use single sign-on (SSO) to authenticate Entra ID users and onboard new devices. This solution is well suited for Bring your own Device (BYOD) policy in which the Entra ID users can onboard their devices based on the policy of the organisation.

Most of today's organisations use some kind of SSO. Because SSO system allows the user to sign-on once and use all the applications and/or websites without reauthenticate again. If you like to access an application, the authentication is done in the background, and you have a seamless and uninterrupted workflow.

For this post, I will use ClearPass SSO with Entra ID, which uses Security Assertion Markup Language (SAML) in the background to exchange the authentication data and then it uses ClearPass Onboard Certificate authority to issue a user certificate and installs it on the device along with the necessary wireless profile.



ClearPass can leverage either SAML or OAuth 2.0 to authorise against cloud identity providers. Here we'll be using SAML to authorise against Entra ID and the use ClearPass Onboard to issue user certificates and onboard the clients to use EAP-TLS authentication to connect to the organisation's secure WLAN.

2.1 Things you need

- APs running AOS10 firmware version (I am using 10.7.1.1)
- Valid HPE Aruba Central account and subscriptions
- ClearPass 6.11.x with Access and Onboard licenses. (I am using 6.11.14)
- ClearPass requires a valid public server certificate for HTTPS and an FQDN matching the certificate CN that clients can resolve via DNS.
- Entra ID administrator access
- ClearPass date and time are synched with NTP
- User has permission to access Entra Cloud services for SSO authentication.

3 ClearPass SSO Integration with Entra ID

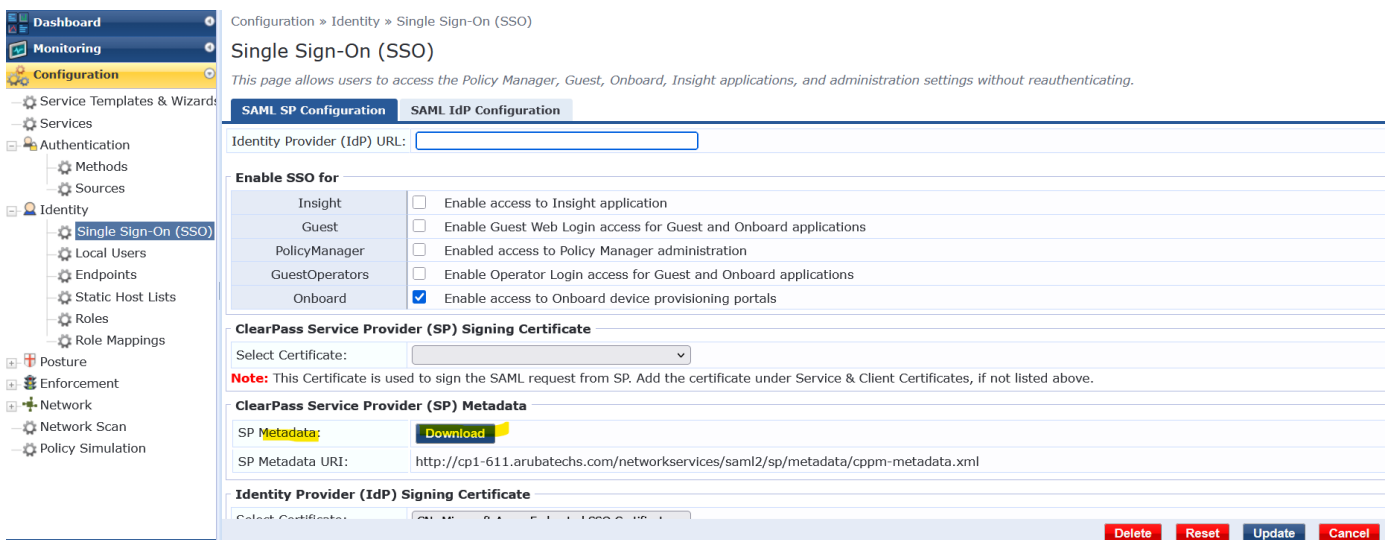
Here are the main tasks:

1. Configure Identity SSO in ClearPass Policy Manager.
2. Configure SSO application service in ClearPass Policy Manager.
3. Configure Entra’s corresponding Enterprise app to use SAML with ClearPass as SP.
4. Assigning user group to use this Entra SAML app (to be done in Entra).
5. Download the Microsoft SSO federated certificate (to be done in Entra).
6. Adding Entra’s Federated SSO certificate to the Certificate Trust list on Policy Manager.
7. Adding Entra as IdP on ClearPass SSO and selecting Onboard for device provisioning.
8. Configuring the onboard provisioning in ClearPass Onboard side of things.
9. Modify the existing EAP-TLS service to allow and different access for the BYODs with Onboard certificate.

SSO involves two main components: one is an Identity Provider (IdP) that authenticates users and manages identities (e.g., Okta, Entra ID), and the other is a Service Provider (SP) that provides the apps/services the user wants to access. Here Entra ID will be IdP and ClearPass will be SP.

For SAML federation a unique URI and often a URL is used that acts as the official, permanent name for an application. In our case ClearPass is SP and we need the entity ID. We can get this from SSO Identity page.

Navigate to the path shown and download the metadata.



We’ll open it and copy the URL with the FQDN of your ClearPass. When we configure Entra ID for SSO, it will require two pieces of information one is the Entity ID and the other is the “Reply URL” (Assertion Consumer Service URL).

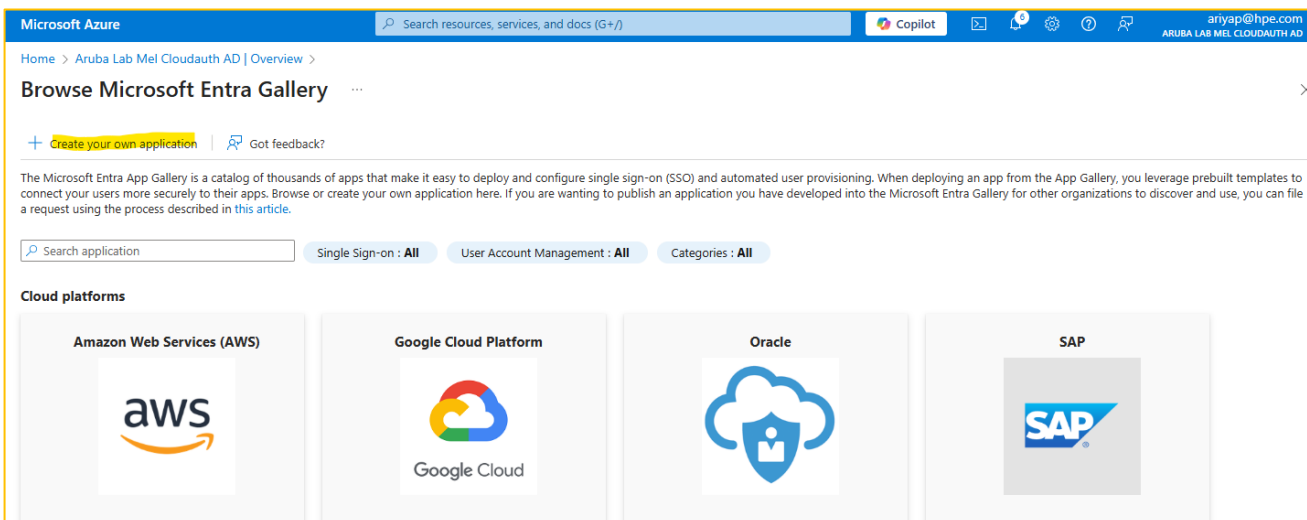
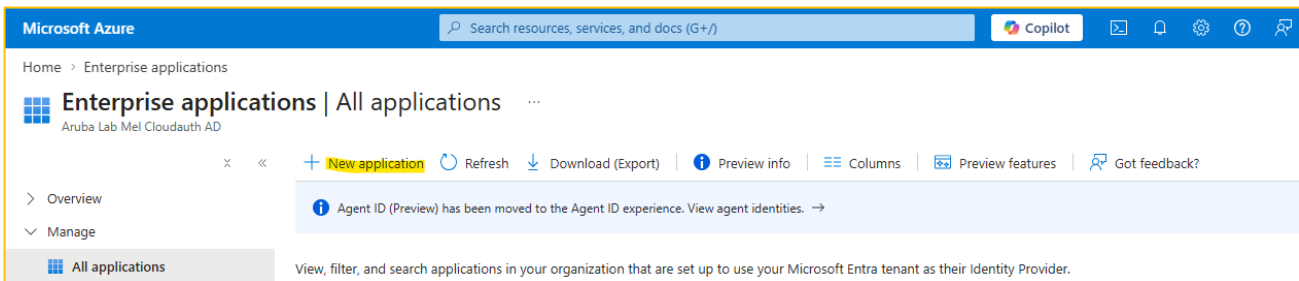
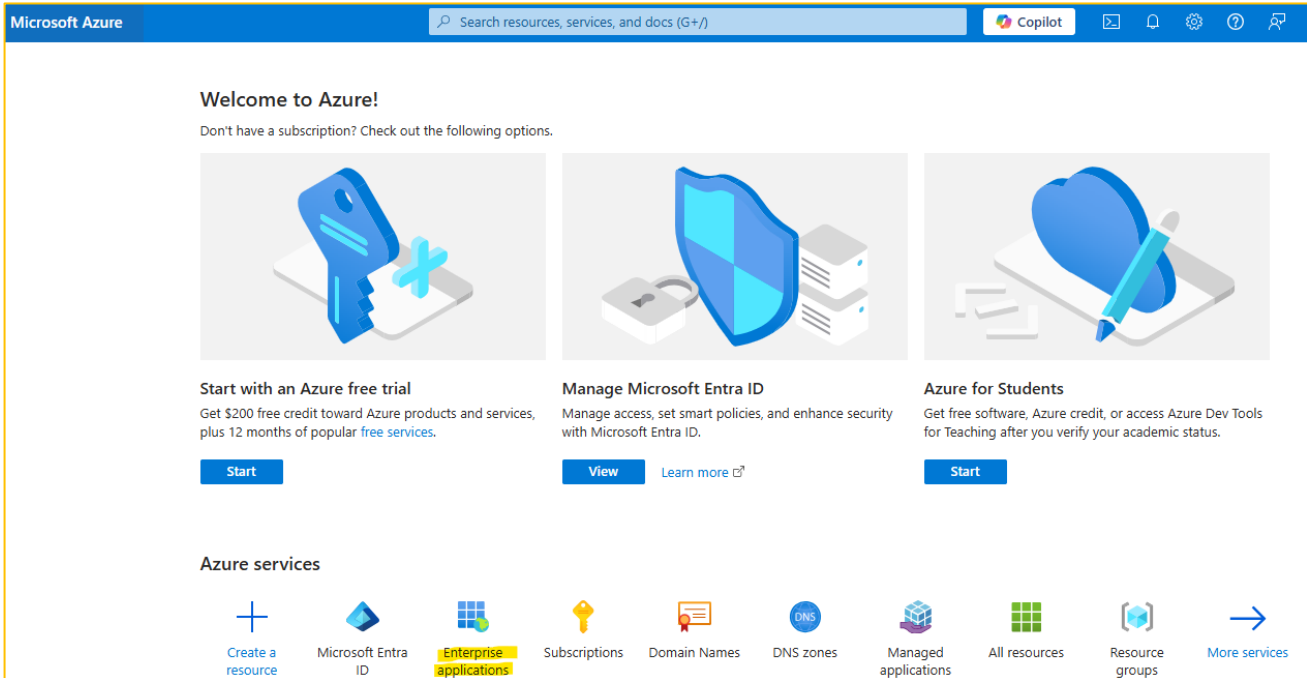
```
<?xml version="1.0" encoding="UTF-8"?><EntitiesDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"><EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" entityID="https://cp1-611.arubatechs.com/networkservices/saml2/sp"><SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"><NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified/><AssertionConsumerService index="1" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://cp1-611.arubatechs.com/networkservices/saml2/sp/acs" /><AttributeConsumingService index="1"><ServiceName xml:lang="en">ClearPass Policy Manager</ServiceName><ServiceDescription xml:lang="en">ClearPass Policy Manager as service provider</ServiceDescription><RequestedAttribute xml:lang="en" Name="SAMLResponse"/></AttributeConsumingService></SPSSODescriptor></EntityDescriptor></EntitiesDescriptor>
```

```
https://cp1-611.arubatechs.com/networkservices/saml2/sp
https://cp1-611.arubatechs.com/networkservices/saml2/sp/acs index = 1
```

Note that ACS is Assertion Consumer Service, that is part of SAML authentication process.

3.1 Entra ID Configuration

You need to go to Enterprise Application and create a new Application. That we'll use to interact with ClearPass and interchange the entity ID, etc.



Home > Aruba Lab Mel Cloudauth AD | Enterprise applications > Enterprise applications | All applications >

Browse Microsoft Entra Gallery

+ Create your own application | Got feedback?


The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. We users more securely to their apps. Browse or create your own application here. If you are wanting to publish an application you have developed into the Microsoft Entra described in [this article](#).

Search application


Single Sign-on: All | User Account Management: All | Categories: All

Cloud platforms


Amazon Web Services (AWS)



Google Cloud Platform



Oracle



On-premises applications

[Add an on-premises application](#) | [Learn about Application Proxy](#) | [On-premises applications](#) | [Create](#)

Create your own application

Got feedback?




If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

What are you looking to do with your application?

Configure Application Proxy for secure remote access to an on-premises application
 Register an application to integrate with Microsoft Entra ID (App you're developing)
 Integrate any other application you don't find in the gallery (Non-gallery)

We found the following applications that may match your entry
We recommend using gallery applications when possible.

-  ClearIP
-  ClearCompany
-  Peripass

[Create](#)

Once you have added a new application, continue with SSO setup.

Home > Aruba Lab Mel Cloudauth AD | Enterprise applications > Enterprise applications | All applications >

ClearPass | Overview

Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
 - Properties
 - Owners
 - Roles and administrators
 - Users and groups
 - Single sign-on
 - Provisioning
 - Application proxy
 - Self-service
 - Custom security




Properties

Name: ClearPass

Application ID: ff6b97e1-2059-48fe-8ec7-a...

Object ID: 476a2ba5-c571-4ad2-b6a8-...

Getting Started

- 
1. Assign users and groups
 Provide specific users and groups access to the applications
[Assign users and groups](#)
- 
2. Set up single sign on
 Enable users to sign into their application using their Microsoft Entra credentials
[Get started](#)
- 
3. Provision User Accounts
 Automatically create and delete user accounts in the application
[Get started](#)

Home > Aruba Lab Mel Cloudauth AD | Enterprise applications > Enterprise applications | All applications > Browse Microsoft Entra Gallery > ClearPass2


ClearPass | Single sign-on

Enterprise Application


- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
 - Properties
 - Owners
 - Roles and administrators
 - Users and groups
 - Single sign-on
 - Provisioning

Single sign-on (SSO) adds security and convenience when users sign on to applications in Microsoft Entra ID by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. [Learn more](#).


Select a single sign-on method [Help me decide](#)

 **Disabled**

Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

 **SAML**

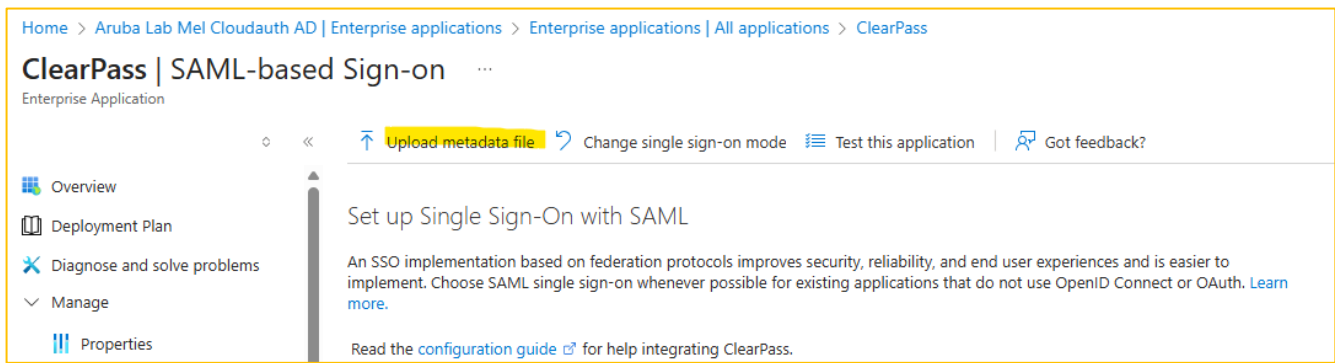
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

 **Password-based**

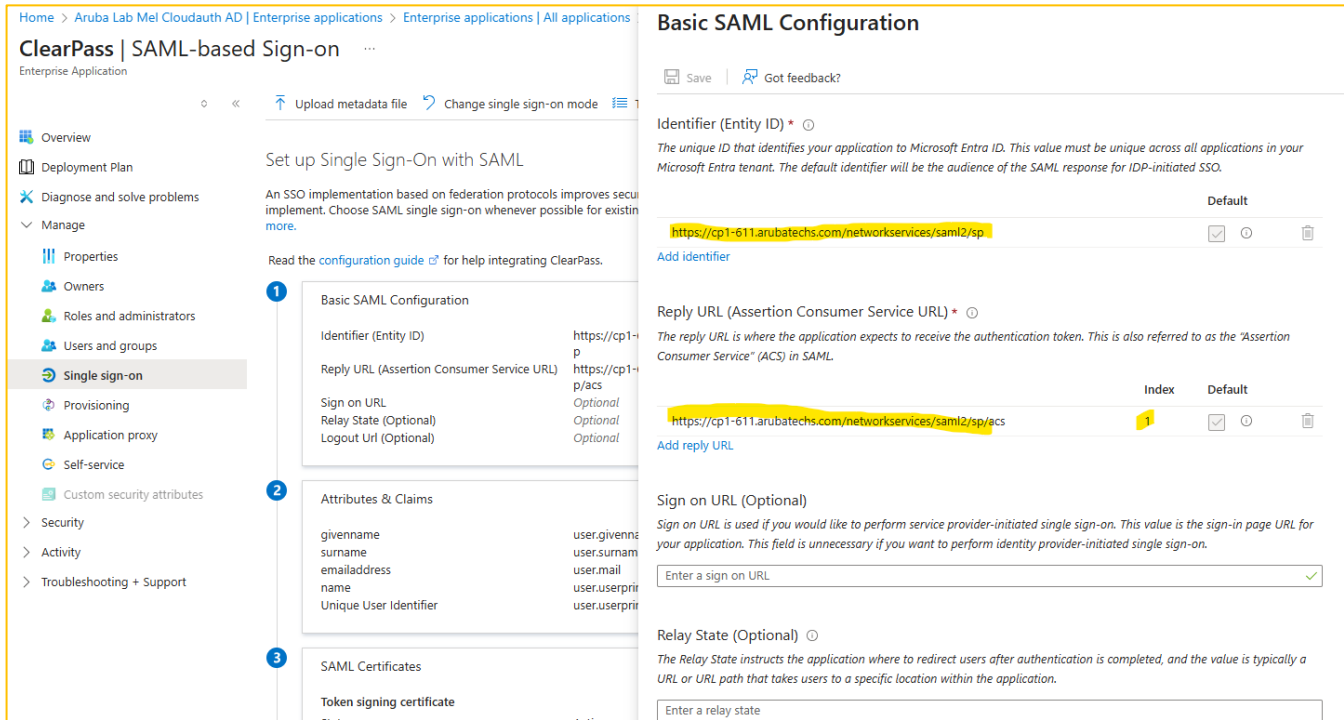
Password storage and replay using a web browser extension or mobile app.

You need two pieces of information which you should get from ClearPass SSO metadata.

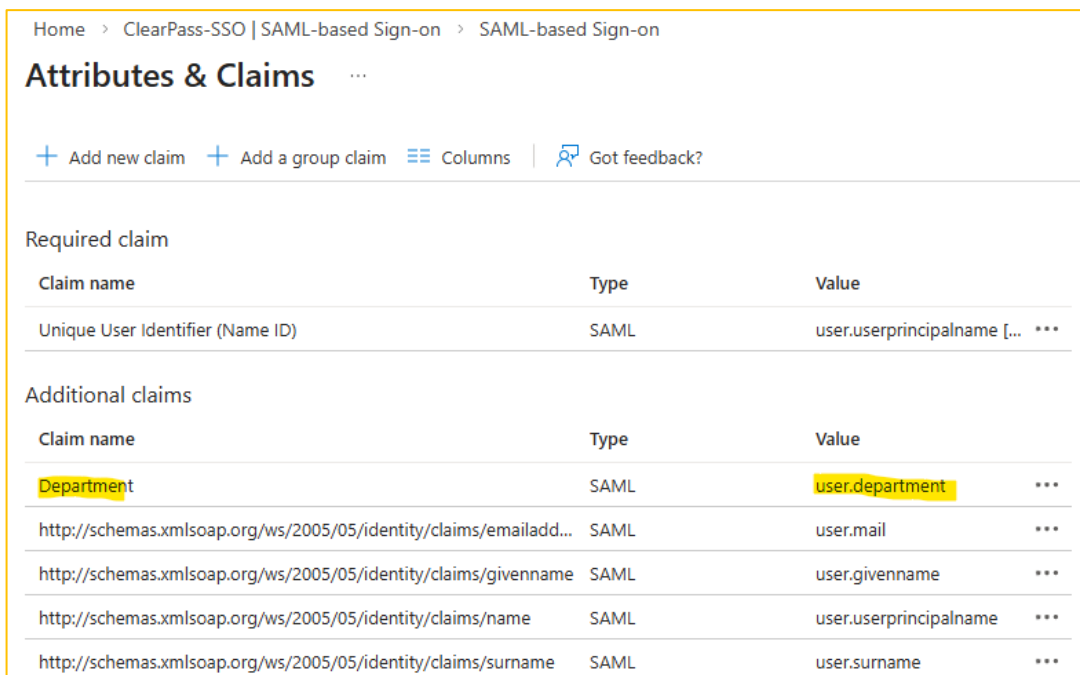
- Identifier (Entity ID)
- Reply URL (Assertion Consumer Service URL)



You can use the upload metadata file or just open it and copy the needed information.



You can also add any other SAML attribute to be sent to ClearPass, look for number 2 “Attributes & Claims”. Here I’ll add the “Department” attribute that I can use as authorisation in my policy.



and then save it.

For completeness here is the full configuration page for it.

ClearPass | SAML-based Sign-on

Enterprise Application

Upload metadata file | Change single sign-on mode | Test this application | Got feedback?

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
 - Properties
 - Owners
 - Roles and administrators
 - Users and groups
 - Single sign-on**
 - Provisioning
 - Application proxy
 - Self-service
 - Custom security attributes
- Security
- Activity
- Troubleshooting + Support

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating ClearPass.

- Basic SAML Configuration**

Identifier (Entity ID)	https://cp1-611.arubatechs.com/networkservices/saml2/sp
Reply URL (Assertion Consumer Service URL)	https://cp1-611.arubatechs.com/networkservices/saml2/sp/acs
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional
- Attributes & Claims**

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
- SAML Certificates**

Token signing certificate	Active
Status	Active
Thumbprint	[Redacted]
Expiration	[Redacted]
Notification Email	ariyap@hpe.com
App Federation Metadata Url	https://login.microsoftonline.com/0391024d-5b37... [Download]
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download
Verification certificates (optional)	
Required	No
Active	0
Expired	0
- Set up ClearPass**

You'll need to configure the application to link with Microsoft Entra ID.

Login URL	https://login.microsoftonline.com, [Download]
Microsoft Entra Identifier	https://sts.windows.net/0391024d [Download]
Logout URL	https://login.microsoftonline.com, [Download]
- Test single sign-on with ClearPass**

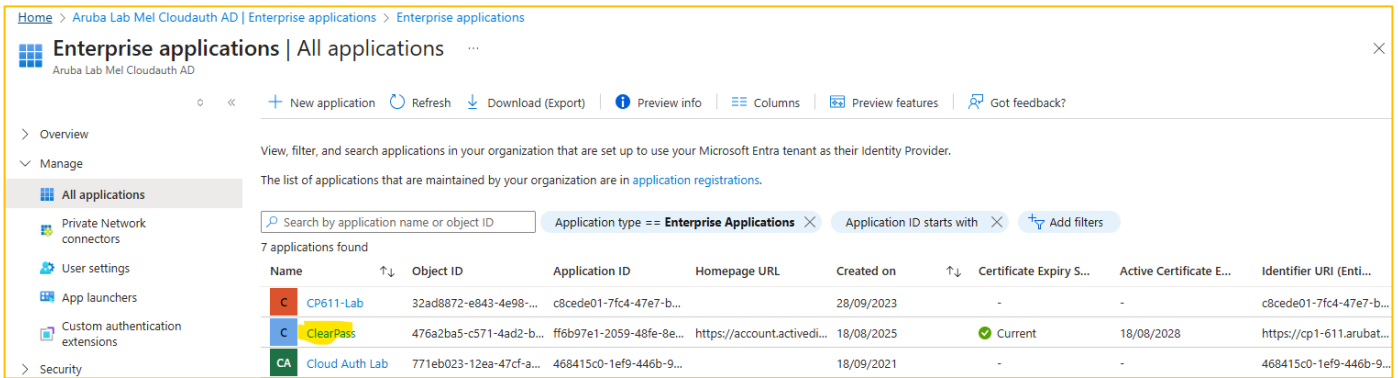
Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

[Test](#)

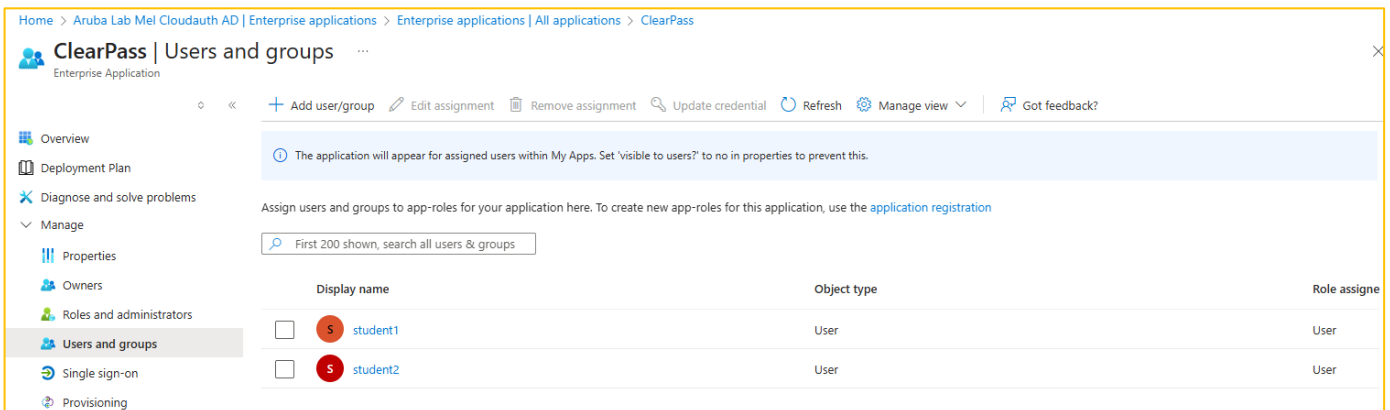
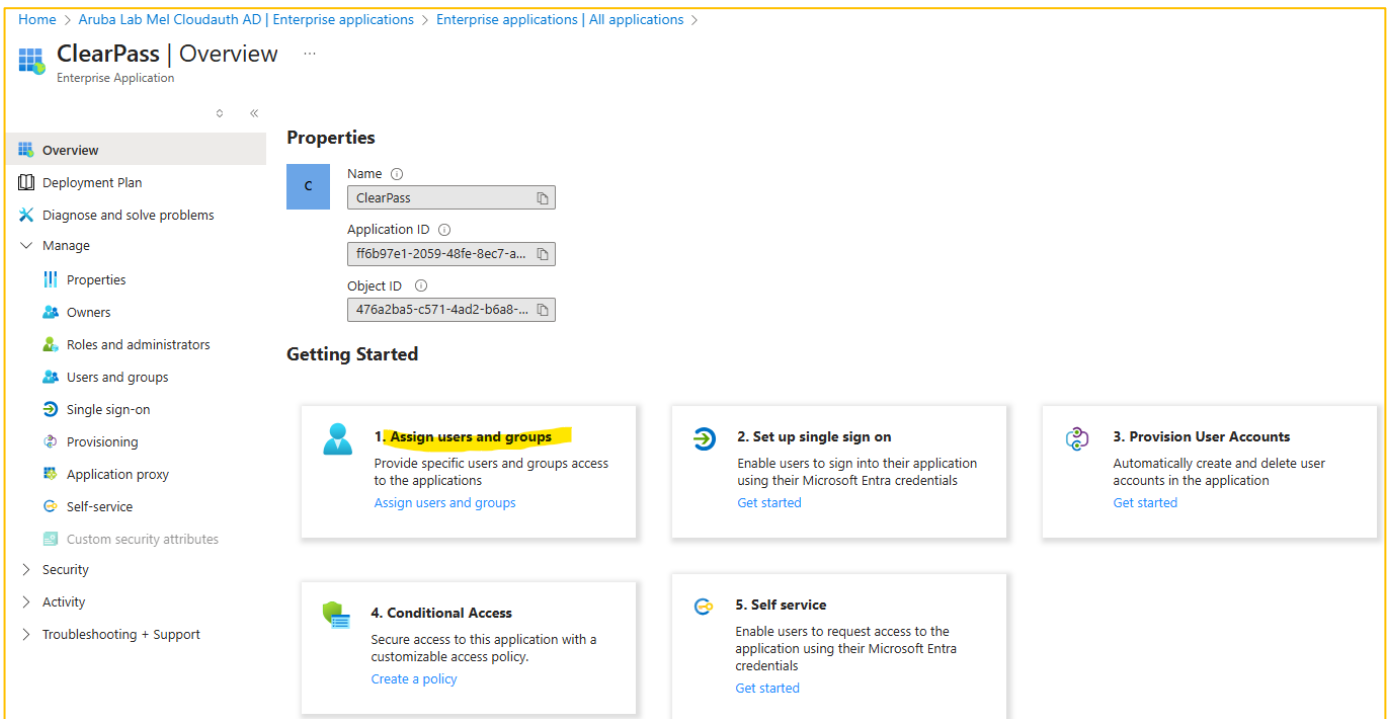
You need to download the "Certificate (Base64)" along with copy the "Login URL" as shown above, because we need it for ClearPass configuration.

https://login.microsoftonline.com/0391024d-[Redacted]/saml2

After you finish the SSO config you should have the new application as shown below.



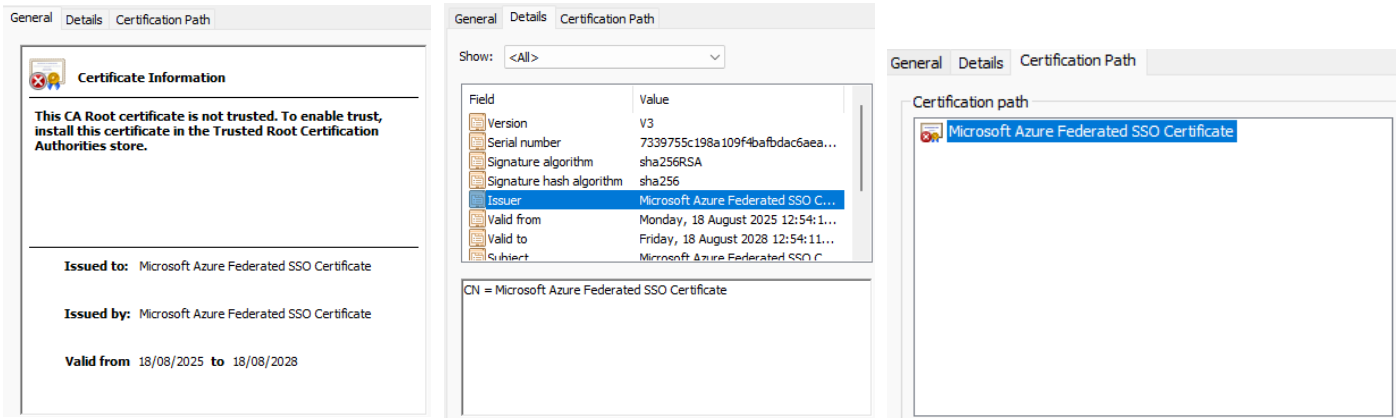
I'll now assign users. Remember I had two students with each in different departments.



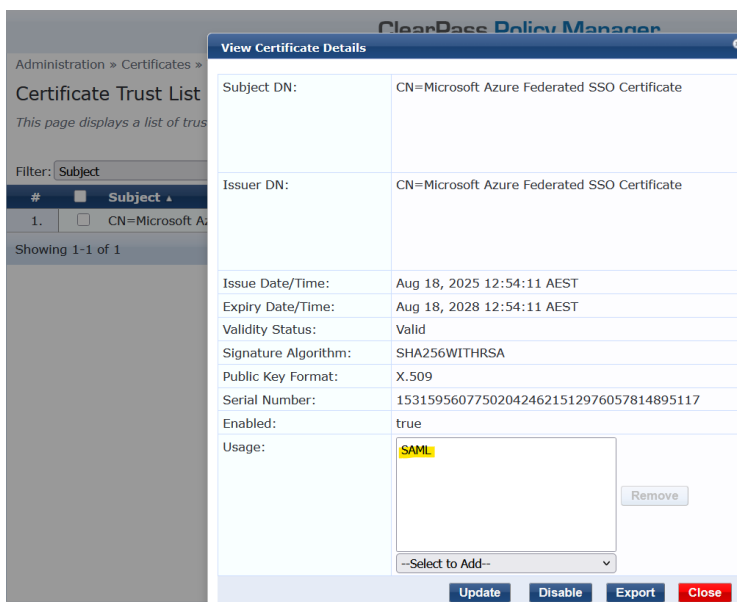
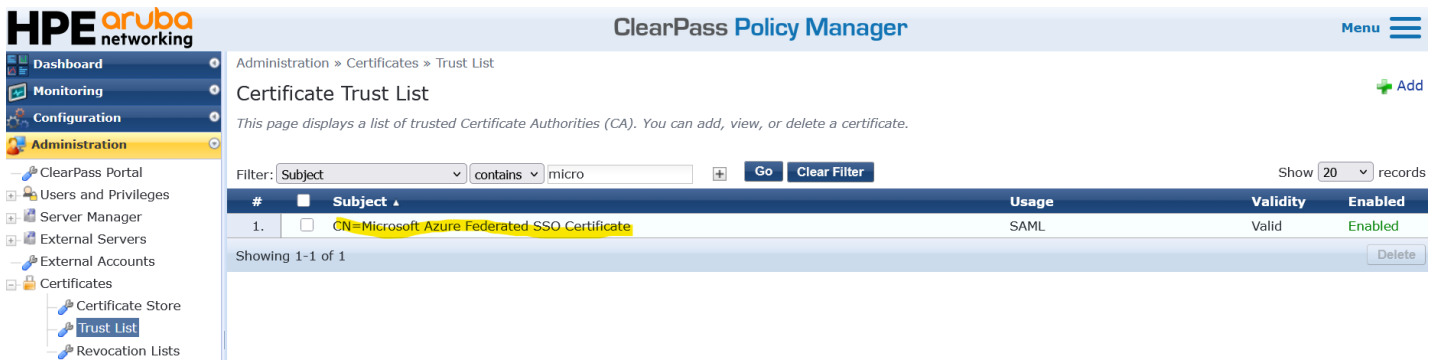
Now we are done with the Azure configuration.

3.2 Adding Microsoft Azure federated SSO certificate in ClearPass

When you download the base64 SAML certificate from your application in Entra and then open it looks like this.



Now I'll add Microsoft Azure federated SSO certificate to ClearPass Certificate Trust List and I'll make sure that the usage type is set to SAML.



3.3 Policy Manager SSO Identity Configuration

Next, we need to create SSO as an identity.

Here is the copy of the Login URL for the SSO application we created in Entra.

<https://login.microsoftonline.com/0391024d-.../saml2>

Note that here we'll be using only Onboard application to use this SSO identity as shown below.

Single Sign-On (SSO)

This page allows users to access the Policy Manager, Guest, Onboard, Insight applications, and administration settings without reauthenticating.

SAML SP Configuration

SAML IdP Configuration

Identity Provider (IdP) URL:

Enable SSO for

Insight	<input type="checkbox"/>	Enable access to Insight application
Guest	<input type="checkbox"/>	Enable Guest Web Login access for Guest and Onboard applications
PolicyManager	<input type="checkbox"/>	Enabled access to Policy Manager administration
GuestOperators	<input type="checkbox"/>	Enable Operator Login access for Guest and Onboard applications
Onboard	<input checked="" type="checkbox"/>	Enable access to Onboard device provisioning portals

ClearPass Service Provider (SP) Signing Certificate

Select Certificate:

Note: This Certificate is used to sign the SAML request from SP. Add the certificate under Service & Client Certificates, if not listed above.

ClearPass Service Provider (SP) Metadata

SP Metadata: [Download](#)

SP Metadata URI:

Identity Provider (IdP) Signing Certificate

Select Certificate:

Subject DN:

Issuer DN:

Issue Date/Time:

Expiry Date/Time:

Validity Status:

Serial Number:

Note: This Certificate is used to verify the signed SAML response from the IdP. Add and enable the certificate under Certificate Trust List, if not listed above.

Identity Provider (IdP) Encryption Certificate

Select Certificate:

Note: This Certificate is used to decrypt the encrypted SAML assertion from the IdP. Add the certificate under Service & Client Certificates, if not listed above.

Force Authentication: Enable to always re-authenticate the user, even if the user already has an active session

Delete
Reset
Update
Cancel

3.4 Policy Manager SSO Service

We also need to configure a policy manager service for SAML-based SSO access to ClearPass Policy Manager Onboard via Entra.

Summary

Service

Roles

Enforcement

Name:

Description:

Type:

Status:

Monitor Mode: Enable to monitor network access without enforcement

More Options: Authorization

Service Rule

Matches ANY or ALL of the following conditions:

	Type	Name	Operator	Value
1.	Authentication	Type	EQUALS	SSO
2.	Application	Name	BELONGS_TO	Onboard

Summary	Service	Roles	Enforcement
Use Cached Results:	<input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions		
Enforcement Policy:	Entra ClearPass Admin SSO Login (SAML SP Service) Enforcement Policy		Modify Add New Enforcement Policy
Enforcement Policy Details			
Description:			
Default Profile:	[Deny Application Access Profile]		
Rules Evaluation Algorithm:	first-applicable		
Conditions	Enforcement Profiles		
1. (Application:SSO:Department EQUALS secondary)	[Allow Application Access Profile]		
2. (Tips:Role EQUALS [User Authenticated])	Entra ClearPass Admin SSO Login (SAML SP Service) Enforcement Profile		

Look at the first rule above, I just wanted to highlight, that you can use this as a SSO authorisation policy. So, assuming you have assigned all the Entra users to use this SSO application, because I have added “Department” SAML attribute, here in this rule I can check for its value and if it is equals “secondary” then only they are allowed to continue to onboard their devices.

Note that “Department” corresponds to the SSO application dictionary attribute name that you can find navigating to [Administration » Dictionaries » Applications](#). If you add any SAML attribute in Entra application, you need a corresponding name in this dictionary. You can export this dictionary; make you changes to it and then import it back. Also note that it is in XML format.

3.5 Policy Manager Onboard Authorisation Service

We also need an authorisation service for Onboard application. This is shown below and gets used when the user starts the QuickConnect application to configure /onboard their devices. You’ll see it in action in the testing section. But basically, this service will only allow windows devices to be onboarded any day of the week.

Summary	Service	Roles	Enforcement
Name:	Basic Onboard Authorization		
Description:	Onboard Authorization Service for Applications		
Type:	Aruba Application Authorization		
Status:	Enabled		
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement		
More Options:	<input type="checkbox"/> Authorization		
Service Rule			
Matches	<input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions:		
Type	Name	Operator	Value
1. Application	Name	EQUALS	Onboard
2. Application:ClearPass	Device-Name	EXISTS	

Summary	Service	Roles	Enforcement
Role Mapping Policy:	oo Onboard AppAuth Role Mapping Modify		
Role Mapping Policy Details			
Description:			
Default Role:	[Guest]		
Rules Evaluation Algorithm:	first-applicable		
Conditions	Role		
1. (Application:ClearPass:Device-Name BEGINS_WITH Android)	[Onboard Android]		
2. (Application:ClearPass:Device-Name BEGINS_WITH Windows)	[Onboard Windows]		
3. (Application:ClearPass:Device-Product BEGINS_WITH iPad)	[Onboard iOS]		
OR (Application:ClearPass:Device-Product BEGINS_WITH iPod)			
OR (Application:ClearPass:Device-Product BEGINS_WITH iPhone)			
4. (Application:ClearPass:Device-Product BEGINS_WITH MacBook)	[Onboard macOS]		
5. (Application:ClearPass:Device-Name BEGINS_WITH Chrome)	[Onboard Chromebook]		
6. (Application:ClearPass:Device-Name BEGINS_WITH Ubuntu)	[Onboard Linux]		

Summary Service Roles **Enforcement**

Use Cached Results: Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: Basic Onboard AppAuth Enforcement Policy Modify

Enforcement Policy Details

Description:

Default Profile: [Deny Application Access Profile]

Rules Evaluation Algorithm: evaluate-all

Conditions	Enforcement Profiles
1. (Tips:Role <i>EQUALS</i> [Onboard Windows])	[Allow Application Access Profile]
2. (Date:Day-of-Week <i>BELONGS_TO</i> Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday)	[Allow Application Access Profile]

3.6 Policy Manager EAP-TLS Service

Here I am modifying the exiting EAP-TLS service to cater for the BYODs with Onboard certificates.

Summary **Service** Authentication Authorization Roles Enforcement

Name: Basic Aruba Wireless dot1x-TLS

Description: dot1x service for A0510

Type: Aruba 802.1X Wireless

Status: Enabled

Monitor Mode: Enable to monitor network access without enforcement

More Options: Authorization Posture Compliance Audit End-hosts Profile Endpoints Accounting Proxy

Service Rule

Matches ANY or ALL of the following conditions:

Type	Name	Operator	Value
1. Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)
2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3. Radius:Aruba	Aruba-Essid-Name	EXISTS	

Summary Service **Authentication** Authorization Roles Enforcement

Authentication Methods: EAP-TLS No Auth OCSP

Move Up ↑
Move Down ↓
Remove
View Details
Modify

--Select to Add--

Authentication Sources: [Local User Repository] [Local SQL DB] [Onboard Devices Repository] [Local SQL DB]

Move Up ↑


I am adding the Entra ID authorisation source (shown below) so that I can get user group information that I'll make use of, in my role-mapping policy.

Summary Service Authentication **Authorization** Roles Enforcement

Authorization Details: Authorization sources from which role mapping attributes are fetched (for each Authentication Source)

Authentication Source	Attributes Fetched From
1. [Local User Repository] [Local SQL DB]	[Local User Repository] [Local SQL DB]
2. [Onboard Devices Repository] [Local SQL DB]	[Onboard Devices Repository] [Local SQL DB]

Additional authorization sources from which to fetch role-mapping attributes -

Ariya-AAD [Azure]  Remove Add New

Summary	Service	Authentication	Authorization	Roles	Enforcement
Role Mapping Policy: <input type="text" value="basic dot1x"/> <input type="button" value="Modify"/>					
Role Mapping Policy Details					
Description:					
Default Role:	[Other]				
Rules Evaluation Algorithm:	first-applicable				
Conditions	Role				
1. (Radius:IETF:User-Name EQUALS staff1) AND (Authentication:OuterMethod EQUALS EAP-PEAP)	staff				
2. (Radius:IETF:User-Name EQUALS staff1) AND (Authorization:[Local User Repository]:Role_Name EQUALS staff)	person of interest				
3. (Certificate:Subject-CN EQUALS test-user@test.com)	person of interest				
4. (Authentication:TLS-Version EQUALS 1.0)	quarantine				
5. (Authorization:[Local User Repository]:Role_Name EQUALS Employee)	staff				
6. (Authentication:OuterMethod EQUALS EAP-TLS) AND (Certificate:Issuer-C CONTAINS Onboard) AND (Authorization:Ariya-AAD:Groups CONTAINS Stude)	student-entra-byod				

Based on the above criteria, these devices will have student-entra-byod role that I am using in the enforcement policy.

Summary	Service	Authentication	Authorization	Roles	Enforcement
Use Cached Results: <input checked="" type="checkbox"/> Use cached Roles and Posture attributes from previous sessions					
Enforcement Policy: <input type="text" value="Aruba basic policy"/> <input type="button" value="Modify"/> Add New Enforcement					
Enforcement Policy Details					
Description:					
Default Profile:	[Deny Access Profile]				
Rules Evaluation Algorithm:	first-applicable				
Conditions	Enforcement Profiles				
1. (Tips:Role EQUALS person of interest)	Aruba staff access, Person of Interest notification				
2. (Tips:Role EQUALS quarantine)	Aruba quarantine-redirect, Quarantine notification				
3. (Tips:Role EQUALS [Contractor])	Aruba contractor access				
4. (Tips:Role EQUALS student-entra-byod)	Aruba student-entra-byod access, Update Endpoint Location				

3.7 ClearPass Onboard Configuration

Here we'll configure ClearPass Onboard.

3.7.1 Network Setting

Home » Onboard » Configuration » Network Settings

The screenshot shows the 'Network Settings » Network Access' configuration page in ClearPass Onboard. The left sidebar is expanded to 'Onboard' and then 'Configuration', with 'Network Settings' selected. The main configuration area includes the following fields and options:

- Name:** Entra-BYOD
- Description:** (Empty text area)
- Network Type:** Wireless only
- Security Type:** Enterprise (802.1X)
- Wireless Network Settings:**
 - Security Version:** WPA2 with AES (recommended)
 - SSID:** byod
 - Wireless:** Hidden network
 - Auto Join:** Automatically join network

Network Settings » Enterprise Protocols

Access Protocols Authentication Trust Windows Proxy

Enterprise Protocols
Options for 802.1X protocols supported on the network.

iOS & macOS EAP

Accepted EAP Types
 TLS PEAP EAP-SIM
 TTLS EAP-FAST
 Select the authentication protocols to use when configuring an iOS or macOS 10.7+ (Lion or later) device.

Legacy OS X EAP

Legacy OS X EAP: PEAP with MSCHAPv2
 Select the authentication protocol to use when configuring OS X 10.5/6 (Leopard/Snow Leopard) devices.

Android EAP

Android EAP: TLS
 Select the authentication protocol to use when configuring an Android device.

Windows EAP

Windows EAP: TLS
 Select the authentication protocol to use when configuring a Windows device.

Ubuntu EAP

Ubuntu EAP: TLS
 Select the authentication protocol to use when configuring an Ubuntu device.

Previous Next Save Changes Cancel

Network Settings » Enterprise Trust

Access Protocols Authentication Trust Windows Proxy

Enterprise Trust
Certificate trust options for 802.1X protocols supported on the network.

Configure Trusted Servers: Automatically configure trusted servers (recommended)
 Automatic settings will trust all ClearPass servers currently in the cluster. You should manually enter server names if:
 - You are not using ClearPass for RADIUS authentication
 - You plan to expand your ClearPass cluster at a later date (use a wildcard or suffix match rule in this case)

Configure Trust: Automatically configure trust settings (recommended)
 Use automatic configuration if you are using Policy Manager for authentication. Otherwise, select manual configuration.

Previous Next Save Changes Cancel

3.7.2 Configuration Profile

Home » Onboard » Deployment and Provisioning » Configuration Profiles

Profile

* Name: Entra-BYOD
 Enter a name for the profile.

Description: [Empty text area]
 Enter a description for the profile.

AirPlay: None
 Choose the AirPlay settings to include in the profile.

AirPrint: None
 Choose the AirPrint settings to include in the profile.

Access Point Name (APN): None
 Choose the APN settings to include in the profile.

App Set: None
 Choose the app set to include in the profile.

Calendar: None
 Choose the calendar settings to include in the profile.

Contacts: None
 Choose the contacts settings to include in the profile.

Device Restrictions: None
 Choose the device restrictions settings to include in the profile.

Email: None
 Choose the email settings to include in the profile.

Exchange ActiveSync: None
 Choose the ActiveSync settings to include in the profile.

Networks:

- CentralNAC
- Entra-BYOD
- ES-net
- Example Network
- school

 Choose the networks to include in the profile.

Passcode Policy: None
 Choose the passcode policy to include in the profile.

Subscribed Calendar: None
 Choose the calendar subscription settings to include in the profile.

VPN Settings: None
 Choose the VPN configuration to include in the profile.

Web Clips: (no items)
 Choose the web clips to include in the profile.

3.7.3 Provisioning Setting

Home » Onboard » Deployment and Provisioning » Provisioning Settings

Device Provisioning Settings	
<p>General Supported Devices Web Login Instructions & Messages Onboard Client Sponsorship Confirmation</p>	
* Name:	<input type="text" value="Entra-BYOD-prov"/> Enter a name for this configuration set.
Description:	<input type="text"/> Enter a description for the configuration set.
* Organization:	<input type="text" value="Tech-Lab"/> Enter an organization name for this configuration set. The organization name is displayed by the device during provisioning.

Identity	
These options control the generation of device credentials.	
* Certificate Authority:	<input type="text" value="Local Certificate Authority"/> Select the certificate authority that will be used to sign profiles and messages.
* Signer:	<input type="text" value="Onboard Certificate Authority"/> Select the source that will be used to sign TLS client certificates.
* TLS Certificate Authority:	<input type="text" value="Local Certificate Authority"/> Select the certificate authority that will be used to sign TLS client certificates.
* Key Type:	<input type="text" value="2048-bit RSA - created by device"/> Select the type of private key to use for TLS certificates.
* Unique Device Credentials:	<input checked="" type="checkbox"/> Include the username in unique device credentials When checked, the username is prefixed to the device's PEAP credentials. This unique set of credentials is used to identify the user and device on the network.

Actions	
These options control actions that may be taken after device provisioning.	
Certificate Expiry:	<input type="checkbox"/> Notify users before their device credentials expire If checked users will receive an email notification when their device's network credentials are due to expire.
Revoke Inactive:	<input type="checkbox"/> Revoke certificates for inactive devices If checked the certificates for devices will be revoked after a period where the device is not seen on the network.
Delete Duplicates:	<input type="checkbox"/> Delete duplicate certificates for devices If checked then old certificates from previous enrollments of a device will be automatically deleted.

Device Provisioning Settings	
<p>General Supported Devices Web Login Instructions & Messages Onboard Client Sponsorship Confirmation</p>	
Web Login Page Options for the weblogin landing page for Onboard.	
* Page Name:	<input type="text" value="device_provisioning_3"/> Enter a page name for this web login. The web login will be accessible from "/onboard/page_name.php".
Page Redirect Options for specifying parameters passed in the initial redirect.	
Security Hash:	<input type="text" value="Do not check - login will always be permitted"/> Select the level of checking to apply to URL parameters passed to the web login page. Use this option to detect when URL parameters have been modified by the user, for example their MAC address.
Login Form Options for specifying the behaviour and content of the login form.	
Custom Fields:	<input type="text"/> Choose additional fields to be displayed on the login form. These values entered in these fields will be added to the subject alt-name of the client's certificate.

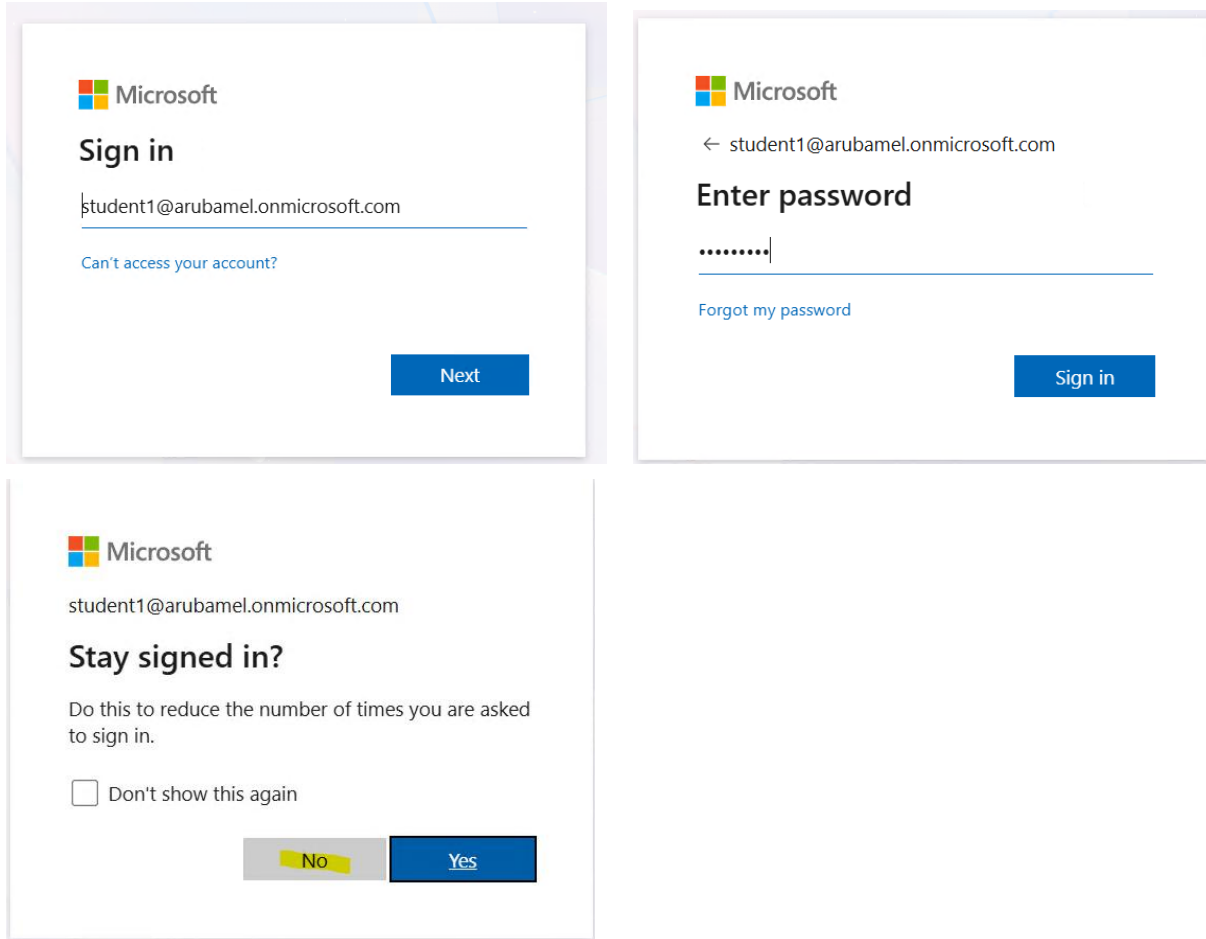
Device Provisioning Settings	
<p>General Supported Devices Web Login Instructions & Messages Onboard Client Sponsorship Confirmation</p>	
Device Provisioning Options for Windows, Android and Legacy OS X (10.5/6) device provisioning. These settings are not used for iOS, iPadOS or macOS 10.7+ (Lion or later) devices.	
* Code-Signing Certificate:	<input type="text" value="None - Use Aruba factory signature"/> Select a code signing certificate for signing the Windows provisioning application.
* Provisioning Address:	<input type="text" value="CP1-611 (requires DNS resolution)"/> Select the hostname or IP address to use for device provisioning.
Provisioning Access:	<input type="text" value="To be provisioned, devices must be able to access CP1-611 via HTTPS."/>
* Validate Certificate:	<input type="text" value="Yes, validate this web server's certificate (recommended)"/> Specify whether the web server's certificate is to be validated during device provisioning. When testing with the default self-signed web server certificate, you may need to disable validation. This option applies to Windows, Android, and OS X 10.5/6 devices only.

Note that the complete URL for client onboarding is `http://<FQDN for clearpass>/guest/<weblogin page name>`
 In my case it is `https://cp1-611.arubatechs.com/guest/device_provisioning_3.php`
 The above URL will use SSO and get the login prompt from Entra ID application.

4 User Onboarding Test

You can provide the full onboarding URL on your web portal for users or include it as part of a guest captive portal. In this scenario, we assume it has been added to the organisation's web portal and is accessible to all users. When users visit the onboarding URL, they are redirected to Microsoft Entra via SSO integration and prompted to log in.

Here is the workflow for student1 that clicks on the ClearPass onboarding URL and gets redirected to Microsoft Entra SSO login page.



At this point you'll see the first authentication session in ClearPass access tracker.

Access Tracker Mar 25, 2026 17:29:05 AEDT Auto Refresh

The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.

[All Requests] CP1-611 (192.168.1.101) Last 2 days before Today Edit

Filter: Request ID contains [] Go Clear Filter Show 50 records

#	NAS IP Address	Server Name	Source	Username	Service	Login Status	Enforcement Profiles	Request Timestamp
1.		CP1-611	Application	student1@arubamel.onmicrosoft.com	Entra ClearPass Admin SSO Login (SAML S P Service)	ACCEPT	Entra ClearPass Admin SSO Login (SAML SP Service) Enforcement Profile	2026/03/25 17:27:36

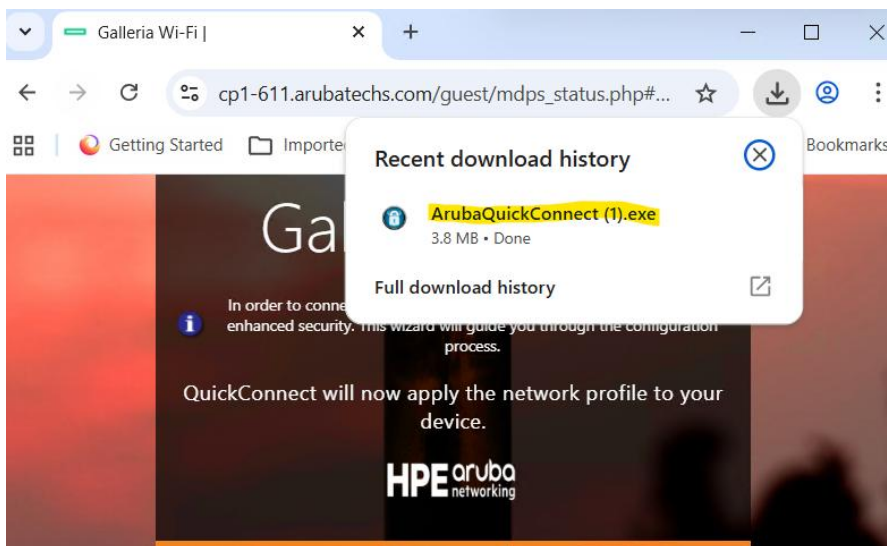
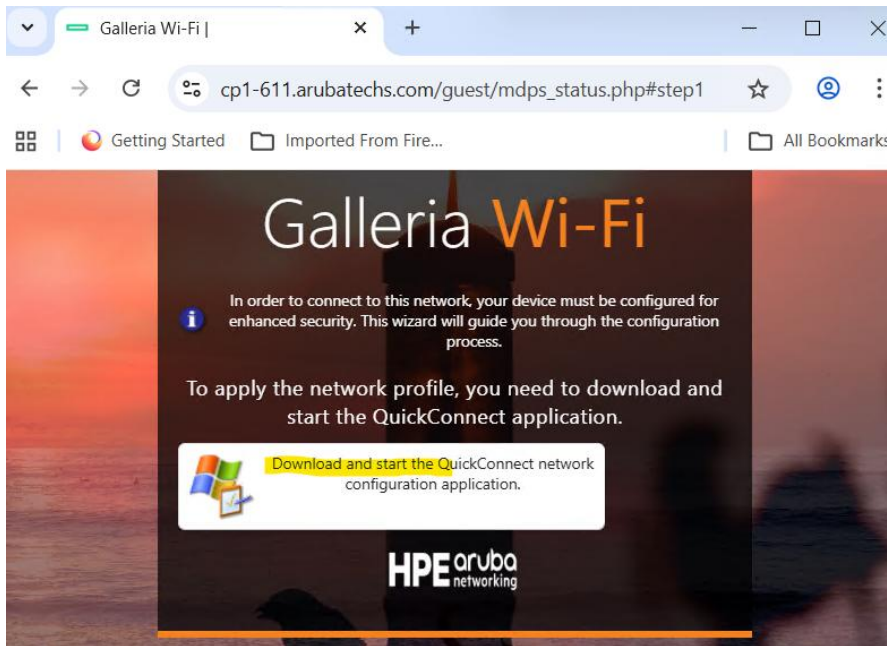
As shown above it is matching the SSO application service that we created earlier. Let's look at the details.

Summary	Input	Output
Login Status:		ACCEPT
Session Identifier:		W00000004-05-69c38056
Date and Time:		Mar 25, 2026 17:27:36 AEDT
End-Host Identifier:		-
End-Host Profile:		-
End-Host Status:		
Username:		student1@arubamel.onmicrosoft.com
Access Device IP (Port):		-
Access Device Name:		-
System Posture Status:		UNKNOWN (100)
Policies Used -		
Service:		Entra ClearPass Admin SSO Login (SAML SP Service)
Authentication Method:		Not applicable
Authentication Source:		-
Authorization Source:		[Local User Repository]
Roles:		[User Authenticated]
Enforcement Profiles:		Entra ClearPass Admin SSO Login (SAML SP Service) Enforcement Profile
Service Monitor Mode:		Disabled
Online Status:		Not Available

Summary	Input	Output
Username:		student1@arubamel.onmicrosoft.com
End-Host Identifier:		-
Access Device IP (Port):		-
Access Device Name:		-
Computed Attributes		
Application:Name		Onboard
Application:SSO:http://schemas.microsoft.com/claims/authnmethodsreferences		http://schemas.microsoft.com/identity/authenticationmethk
Application:SSO:http://schemas.microsoft.com/identity/claims/displayname		student1
Application:SSO:http://schemas.microsoft.com/identity/claims/identityprovider		https://sts.windows.net/0391024d-5b37-4bb6-8e40-ba8477cbfa8d/
Application:SSO:http://schemas.microsoft.com/identity/claims/objectidentifier		87df4a5b-9e1b-4306-9564-1
Application:SSO:http://schemas.microsoft.com/identity/claims/tenantid		0391024d-5b37-4bb6-8e40-
Application:SSO:http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname		Student1
Application:SSO:http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name		student1@arubamel.onmicr
Authentication:Full-Username		student1@arubamel.onmicr
Authentication:Full-Username-Normalized		student1@arubamel.onmicr
Authentication:Status		User
Authentication:Type		SSO
Authentication:Username		student1@arubamel.onmicr
Authorization:Sources		[Local User Repository]
Connection:Protocol		Application
Connection:Src-IP-Address		192.168.1.149
Date:Date-of-Year		2026-03-27
Date:Date-Time		2026-03-27 09:31:48
Date:Day-of-Week		Friday
Date:Time-of-Day		09:31:48

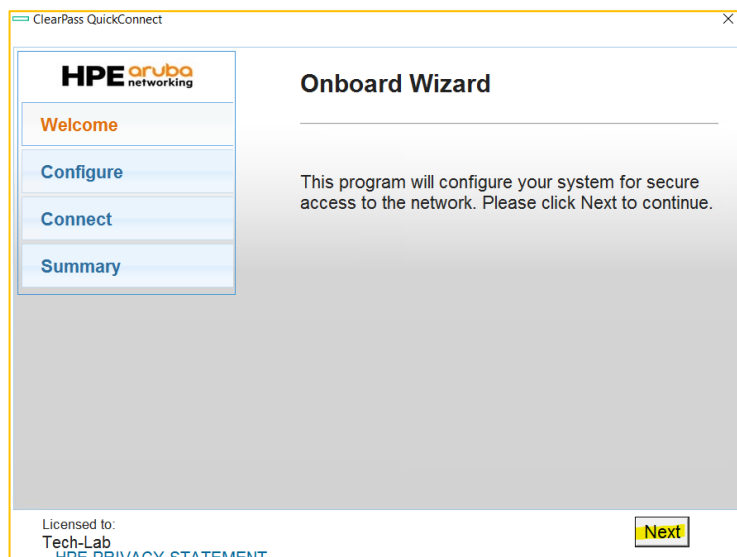
Summary	Input	Output
Enforcement Profiles:		Entra ClearPass Admin SSO Login (SAML SP Service) Enforcement Profile
System Posture Status:		UNKNOWN (100)
Application Response		
Application:SSORole		Super Administrator

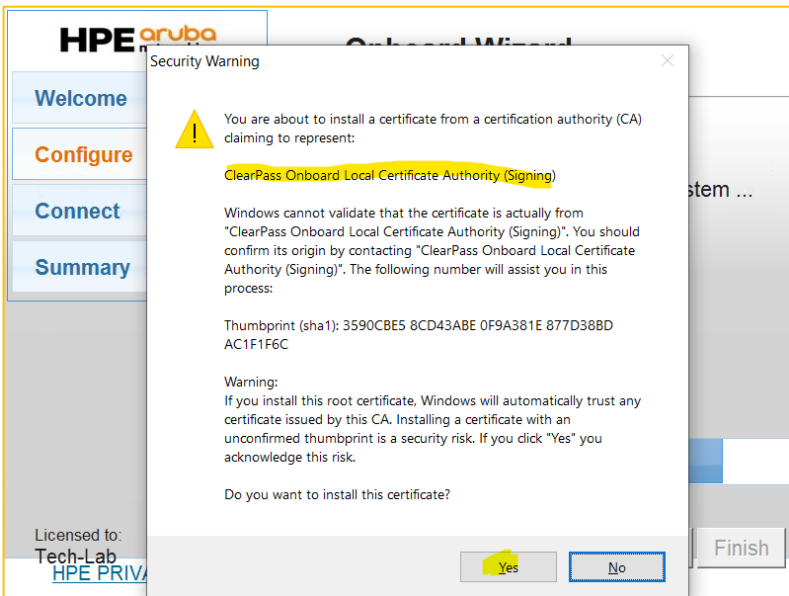
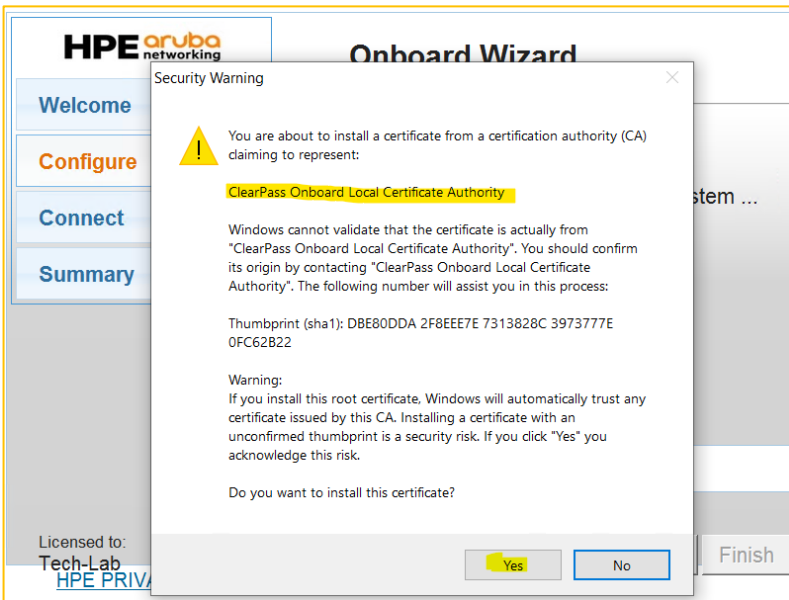
Back to the studnet1's workflow, studnet1 is now shown this captive portal to download QuickConnect network configuration application for a windows laptop.



Then when I run the application it adds the user certificate and the server/signing certificate (both from ClearPass Onboard) on the laptop. It also configures the WLAN profile for the SSID with EAP-TLS authentication.

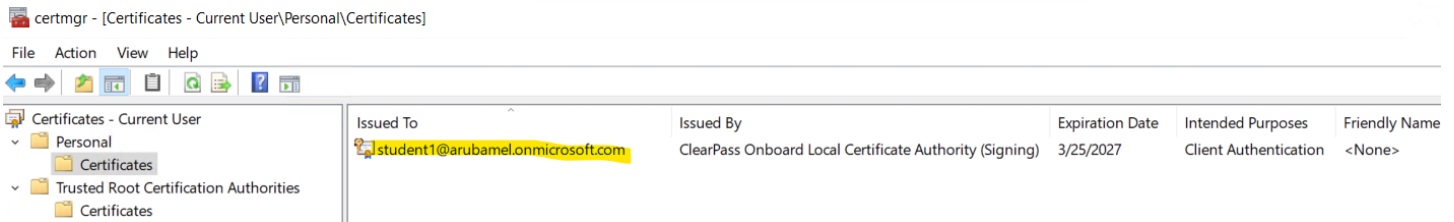
So now studnet1 has double clicked on the ArubaQuickConnect.exe



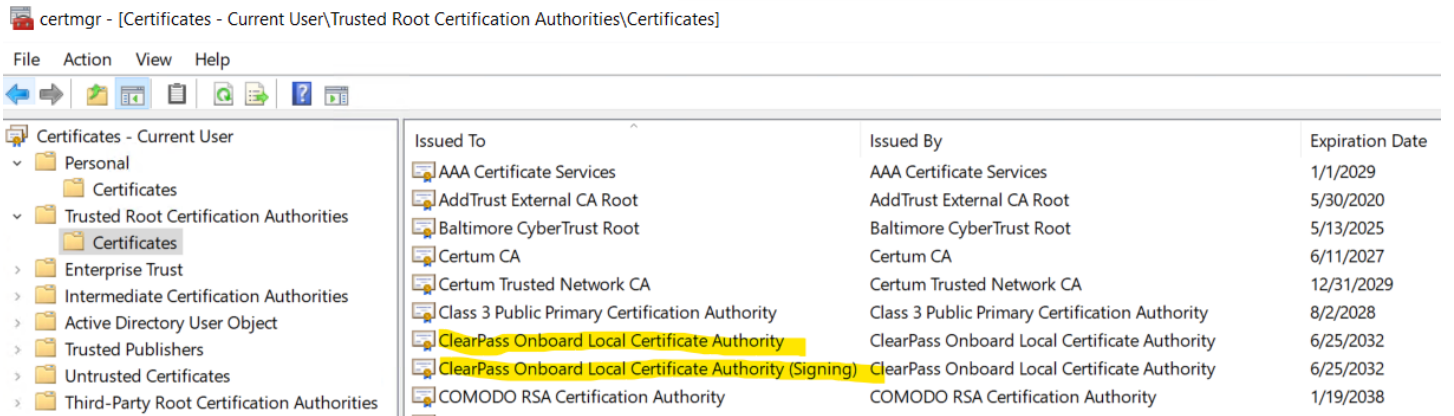


Once you click on the Connect button, it will automatically connect to the "byod" SSID.

Let's do a few checks now. Firstly, check the certmgr to see the user certificate that was installed. We have one for the user.

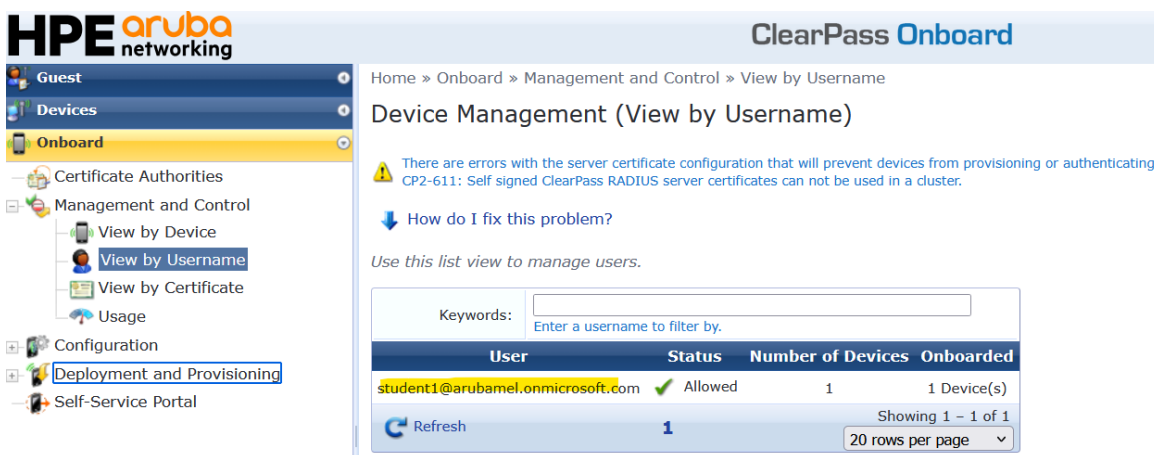


And two server certificates added in the Trusted Root section.



4.1 ClearPass Onboard Certificate Management

Here we'll check the user certificates that were issued by ClearPass Onboard Certificate Authority (CA).



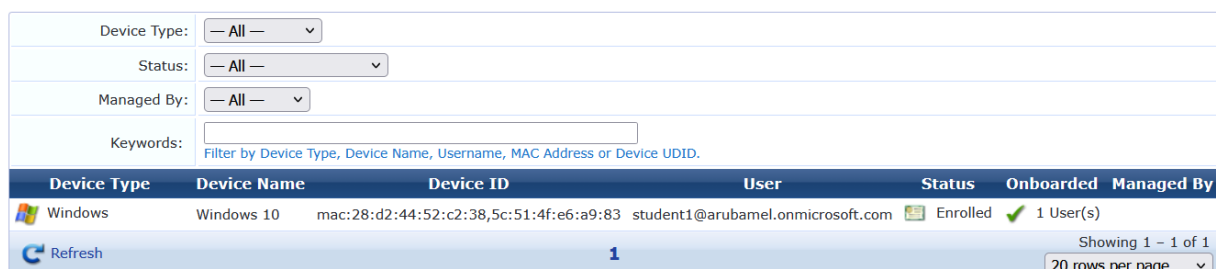
Home » Onboard » Management and Control » View by Device

Device Management (View by Device)

There are errors with the server certificate configuration that will prevent devices from provisioning or authenticating:
CP2-611: Self signed ClearPass RADIUS server certificates can not be used in a cluster.

How do I fix this problem?

Use this list view to manage devices.



4.2 WLAN Connectivity Test

After I clicked on the “Connect” button of QuickConnect app during studnet1 onboarding, I get the other two authentication sessions that show up in access tracker. So, all up there are three authentication sessions for each client onboarding as shown below.

Filter: Request ID contains + Go Clear Filter Show 50 records

#	NAS IP Address	Server Name	Source	Username	Service	Login Status	Enforcement Profiles	Request Timestamp
1.	10.10.10.40	CP1-611	RADIUS	student1@arubamel.onmicrosoft.com	Basic Aruba Wireless dot1x-TLS	ACCEPT	Update Endpoint Location, Aruba student-entra-byod access	2026/03/28 15:28:27
2.		CP1-611	Application	student1@arubamel.onmicrosoft.com	Basic Onboard Authorization	ACCEPT	[Allow Application Access Profile]	2026/03/28 15:28:10
3.		CP1-611	Application	student1@arubamel.onmicrosoft.com	Entra ClearPass Admin SSO Login (SAML SP Service)	ACCEPT	[Allow Application Access Profile]	2026/03/28 15:27:57

Starting with Session #3, this was generated when the user successfully authenticated against Entra SSO.

Summary	Input	Output
Login Status:		ACCEPT
Session Identifier:		W0000000e-05-69c758cc
Date and Time:		Mar 28, 2026 15:27:57 AEDT
End-Host Identifier:		-
End-Host Profile:		-
End-Host Status:		
Username:		student1@arubamel.onmicrosoft.com
Access Device IP (Port):		-
Access Device Name:		-
System Posture Status:		UNKNOWN (100)
Policies Used -		
Service:		Entra ClearPass Admin SSO Login (SAML SP Service)
Authentication Method:		Not applicable
Authentication Source:		-
Authorization Source:		[Local User Repository]
Roles:		[User Authenticated]
Enforcement Profiles:		[Allow Application Access Profile]
Service Monitor Mode:		Disabled
Online Status:		Not Available

Below you'll see the “Department” SSO attribute that we are matching comes through.

Summary	Input	Output
Username:		student1@arubamel.onmicrosoft.com
End-Host Identifier:		-
Access Device IP (Port):		-
Access Device Name:		-
Computed Attributes		
Application:Name		Onboard
Application:SSO:Department:		secondary
Application:SSO:http://schemas.microsoft.com/claims/authnmethodsreferences		http://schemas.microsoft.com/identity/authenticationmethc
Application:SSO:http://schemas.microsoft.com/identity/claims/displayname		student1
Application:SSO:http://schemas.microsoft.com/identity/claims/identityprovider		https://sts.windows.net/0391024d-5b37-4bb6-8e40-ba8477cbfa8d/
Application:SSO:http://schemas.microsoft.com/identity/claims/objectidentifier		87df4a5b-9e1b-4306-9564-1
Application:SSO:http://schemas.microsoft.com/identity/claims/tenantid		0391024d-5b37-4bb6-8e40-
Application:SSO:http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname		Student1
Application:SSO:http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name		student1@arubamel.onmicrc
Authentication:Full-Username		student1@arubamel.onmicrc

Summary	Input	Output
Enforcement Profiles:	[Allow Application Access Profile]	
System Posture Status:	UNKNOWN (100)	

Session #2, is when the user clicked on the “Configure” or “Next” button of QuickConnect App. This is authorisation check to only allow windows devices to be onboarded.

Summary	Input	Output
Login Status:		ACCEPT
Session Identifier:		W0000000f-05-69c758da
Date and Time:		Mar 28, 2026 15:28:10 AEDT
End-Host Identifier:		-
End-Host Profile:		-
End-Host Status:		
Username:		student1@arubamel.onmicrosoft.com
Access Device IP (Port):		-
Access Device Name:		-
System Posture Status:		UNKNOWN (100)
Policies Used -		
Service:		Basic Onboard Authorization
Authentication Method:		Not applicable
Authentication Source:		-
Authorization Source:		-
Roles:		[Onboard Windows], [User Authenticated]
Enforcement Profiles:		[Allow Application Access Profile]
Service Monitor Mode:		Disabled
Online Status:		Not Available

Summary	Input	Output
Username:		student1@arubamel.onmicrosoft.com
End-Host Identifier:		-
Access Device IP (Port):		-
Access Device Name:		-
Computed Attributes		
Application:ClearPass:Device-ICCID		
Application:ClearPass:Device-IMEI		
Application:ClearPass:Device-MAC		28:d2:44:52:c2:38,5c:51:4f:e6:a9:83
Application:ClearPass:Device-Name		Windows 10
Application:ClearPass:Device-Product		
Application:ClearPass:Device-Serial		
Application:ClearPass:Device-UDID		
Application:ClearPass:Device-Version		
Application:ClearPass:Onboard-Request-Type		New
Application:ClearPass:Page-Name		device_provisioning_3
Application:ClearPass:Provisioning-Settings-ID		4
Application:Name		Onboard
Application:WebLoginURL:SSO-Role		
Application:WebLoginURL:sso_token		Dcs5goIwAADAB1Eol0JhQQgsypENKAQ6IIKoEcMV9PW70885UyMofJ2pdw6koNnO4qfSnXM6gWLZu0LRxl2IKY04zpEBJBFUhyUzG5D7D1lbEalxX18w2eSgkfdn8=
Authentication:Full-Username		student1@arubamel.onmicrosoft.com
Authentication:Full-Username-Normalized		student1@arubamel.onmicrosoft.com
Authentication:Status		User
Authentication:Username		student1@arubamel.onmicrosoft.com
Connection:Protocol		Application
Connection:Src-IP-Address		127.0.0.1

Summary	Input	Output
Enforcement Profiles:	[Allow Application Access Profile]	
System Posture Status:	UNKNOWN (100)	

Session #1, is when the user connects to the EAP-TLS WLAN.

Summary	Input	Output	Alerts	Accounting
Login Status:		ACCEPT		
Session Identifier:		R00000002-05-69c758ea		
Date and Time:		Mar 28, 2026 15:28:27 AEDT		
End-Host Identifier:		5C-51-4F-E6-A9-83		Open in Central
End-Host Profile:		Computer / Windows / Windows 10		
End-Host Status:		Unknown		Mark as Known
Username:		student1@arubamel.onmicrosoft.com		
Access Device IP (Port):		10.10.10.40		
Access Device Name:		10.10.10.40		
System Posture Status:		UNKNOWN (100)		
Policies Used -				
Service:		Basic Aruba Wireless dot1x-TLS		
Authentication Method:		EAP-TLS		
Authentication Source:		None		
Authorization Source:		[Local User Repository], [Onboard Devices Repository], Ariya-AAD		
Roles:		[User Authenticated], student-entra-byod		
Enforcement Profiles:		Update Endpoint Location, Aruba student-entra-byod access		
Service Monitor Mode:		Disabled		
Online Status:		✔ Online		

Summary	Input	Output	Alerts	Accounting
Username:		student1@arubamel.onmicrosoft.com		
End-Host Identifier:		5C-51-4F-E6-A9-83 (Computer / Windows / Windows 10)		
Access Device IP (Port):		10.10.10.40		
Access Device Name:		10.10.10.40		
RADIUS Request				
Authorization Attributes				
Authorization:Ariya-AAD:AccountEnabled		true		
Authorization:Ariya-AAD:Department		secondary		
Authorization:Ariya-AAD:Groups		Students		
Authorization:Ariya-AAD:Mail				

Computed Attributes	
Authentication:ErrorCode	0
Authentication:Full-Username	student1@arubamel.onmicrosoft.com
Authentication:Full-Username-Normalized	student1@arubamel.onmicrosoft.com
Authentication:MacAuth	NotApplicable
Authentication:OuterMethod	EAP-TLS
Authentication:Posture	Unknown
Authentication:Status	User
Authentication:TLS-Version	1.2
Authentication:Username	student1@arubamel.onmicrosoft.com
Authorization:Sources	[Local User Repository], [Onboard Devices Repository]
Certificate:Extended-Key-Usage	TLS Web Client Authentication
Certificate:Issuer-C	US
Certificate:Issuer-CN	ClearPass Onboard Local Certificate Authority (Signing
Certificate:Issuer-DN	emailAddress=6f520c29-58b7-4ecd-a73c-d288ad2dcf
Certificate:Issuer-emailAddress	6f520c29-58b7-4ecd-a73c-d288ad2dcf50@example.c

Certificate:Issuer-L	Sunnyvale
Certificate:Issuer-O	Aruba Networks
Certificate:Issuer-ST	California
Certificate:Not-Valid-After	2027-03-27 20:54:35
Certificate:Public-Key-Algorithm	rsaEncryption
Certificate:Public-Key-Length	2048
Certificate:Serial-Number	1e
Certificate:Signature-Algorithm	sha512WithRSAEncryption
Certificate:Subject-AltName-DirName-DN	OnboardEmailAddress=student1@arubamel.onmicroso 10,OnboardDeviceType=Windows
Certificate:Subject-AltName-DirName-OnboardDeviceName	Windows 10
Certificate:Subject-AltName-DirName-OnboardDeviceType	Windows
Certificate:Subject-AltName-DirName-OnboardEmailAddress	student1@arubamel.onmicrosoft.com
Certificate:Subject-AltName-DirName-OnboardMACAddress	28:d2:44:52:c2:38, 5c:51:4f:e6:a9:83
Certificate:Subject-AltName-DirName-OnboardUserName	student1@arubamel.onmicrosoft.com
Certificate:Subject-AltName-Email	student1@arubamel.onmicrosoft.com
Certificate:Subject-AltName-msUPN	student1@arubamel.onmicrosoft.com
Certificate:Subject-C	US
Certificate:Subject-CN	student1@arubamel.onmicrosoft.com
Certificate:Subject-DN	CN=student1@arubamel.onmicrosoft.com,O=Tech-Lal
Certificate:Subject-L	Sunnyvale
Certificate:Subject-O	Tech-Lab
Certificate:Subject-ST	California
Certificate:Version	3
Connection:AP-Name	Board-Room-AP
Connection:Protocol	RADIUS
Connection:Src-IP-Address	10.10.10.40
Connection:Src-Port	57724
Connection:SSID	byod
Date:Date-Time	2026-03-27 20:39:51
Endpoint:Device Insight Tags	[Computers & Servers]
Endpoint:Device Name	Windows 10
Endpoint:Device Type	Windows
Endpoint:Expanded Device Type	Windows
Endpoint:Last Known Location	10.10.10.40:Board-Room-AP
Endpoint:Owner	student1@arubamel.onmicrosoft.com

Summary	Input	Output	Alerts	Accounting
Enforcement Profiles:	Update Endpoint Location, Aruba student-entra-byod access			
System Posture Status:	UNKNOWN (100)			
Audit Posture Status:	UNKNOWN (100)			
RADIUS Response				
Endpoint:Last Known Location	10.10.10.40:Board-Room-AP			
Radius:Aruba:Aruba-User-Role	Student-entra-byod			

And this is the view from Aruba Central.

The screenshot shows the Aruba Central interface for 'Demo-Branch1'. The network status is 'Poor' with 3 devices. The 'Clients' section shows 1 client connected. The client details table is as follows:

Name	Type	MAC Address	IP Address	WLAN	VLAN	Role
student1@arubamel.onmicrosoft.com	Wireless	5c51:4fe6:a9:83	10.10.12.30	byod	12	Student-entra-byod