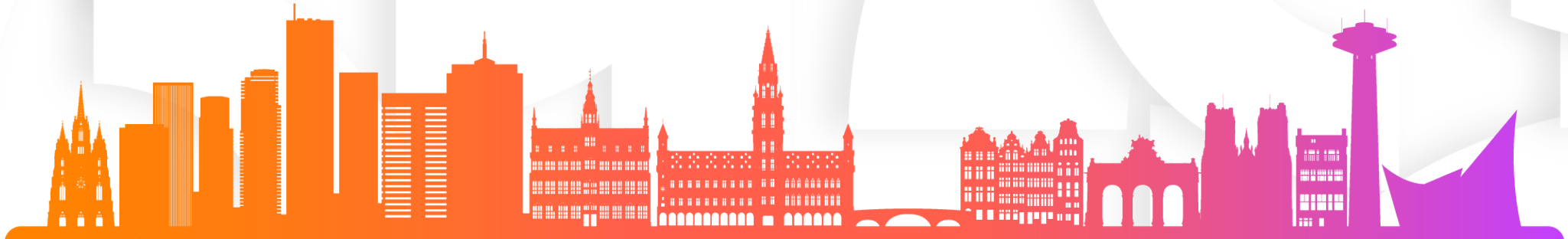
atmosphere'23
BELGIUM

ClearPass, Entra ID (Azure AD) and Intune

Herman Robers, Aruba CSE EMEA

October 2023



HPE aruba networking

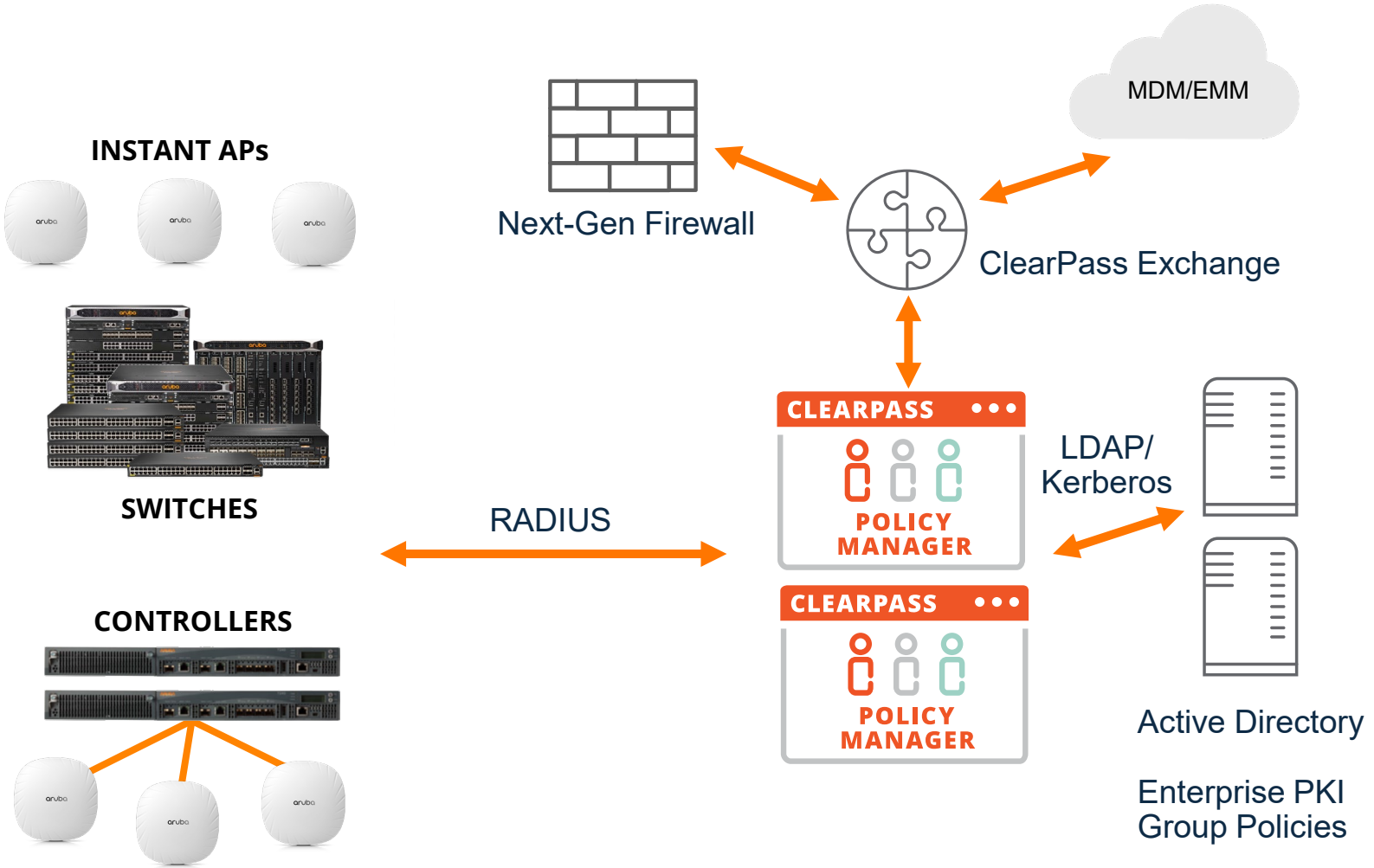
Agenda

- ClearPass and the Cloud
- ClearPass in the Cloud
- ClearPass with the Cloud
- ClearPass and Entra ID (Azure AD)
- ClearPass and Intune Endpoint Manager
- Q&A

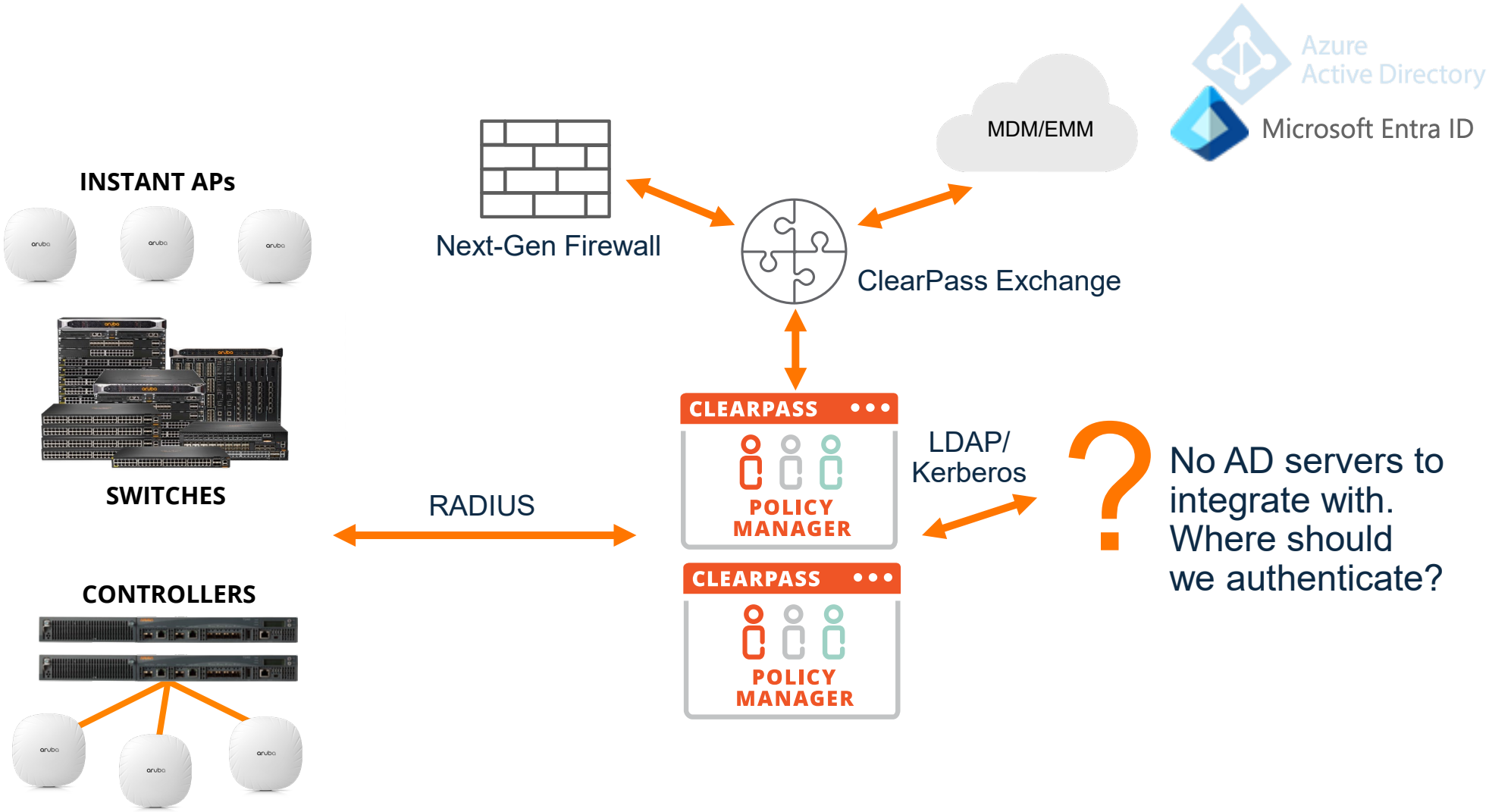
Authentication and the Cloud

When organizations go to the cloud

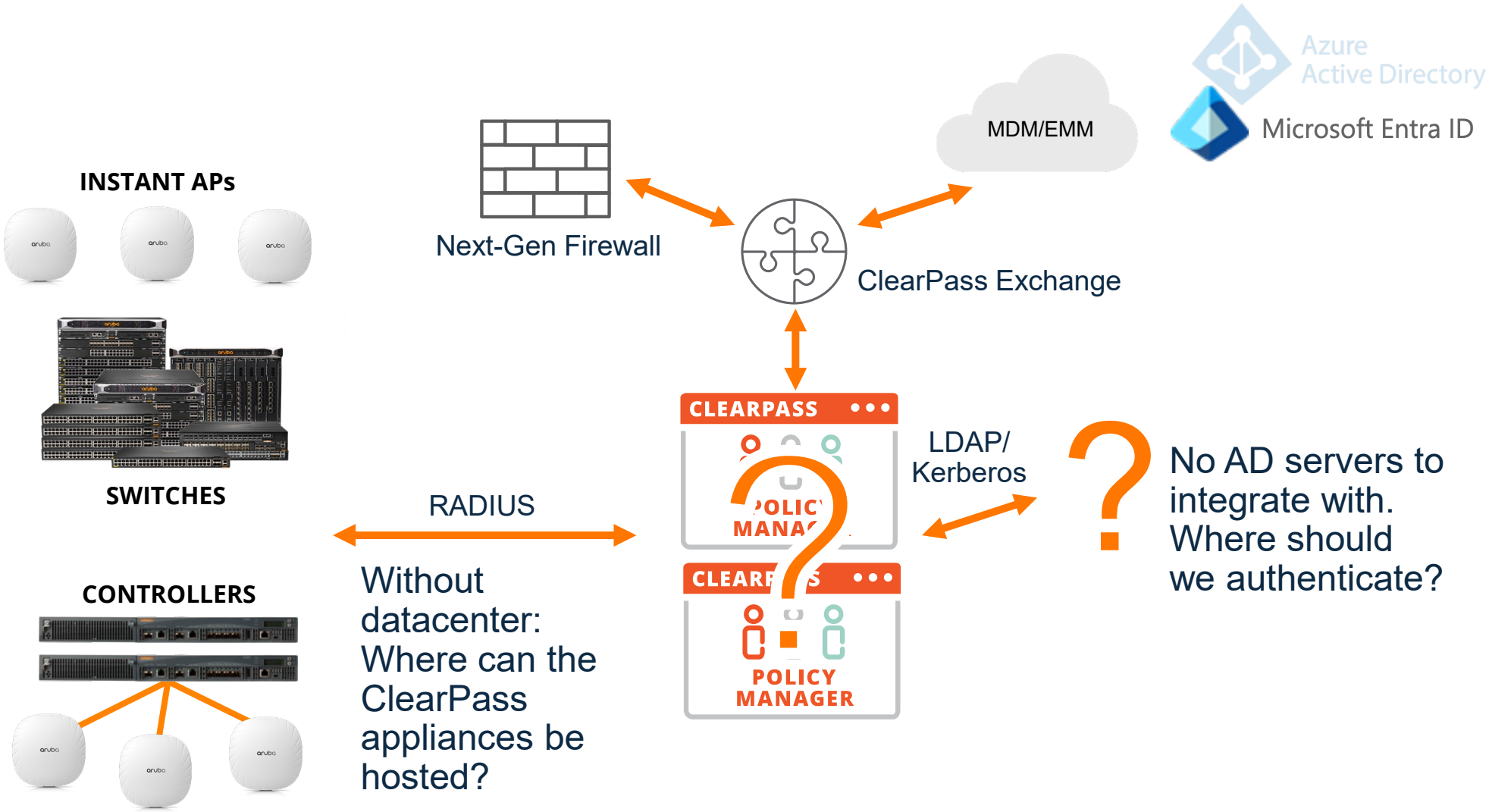
Traditional deployment (On-Premise)



What when customer fully moves to Entra ID (Azure AD)?



What when customer removes all datacenters and goes cloud only?



Authentication options in the cloud and on-premises

Identity Stores

Microsoft Entra ID

Google Workspace

In-the Cloud

Authentication Services

Cloud Guest

Cloud Auth

Runs on:

Aruba Central

SaaS

CLEARPASS

POLICY MANAGER

Runs on:

Microsoft Azure

aws

IaaS

Microsoft Active Directory

On-premises

Virtualized

KVM

vmware ESXi

Microsoft Hyper-V

CLEARPASS

POLICY MANAGER

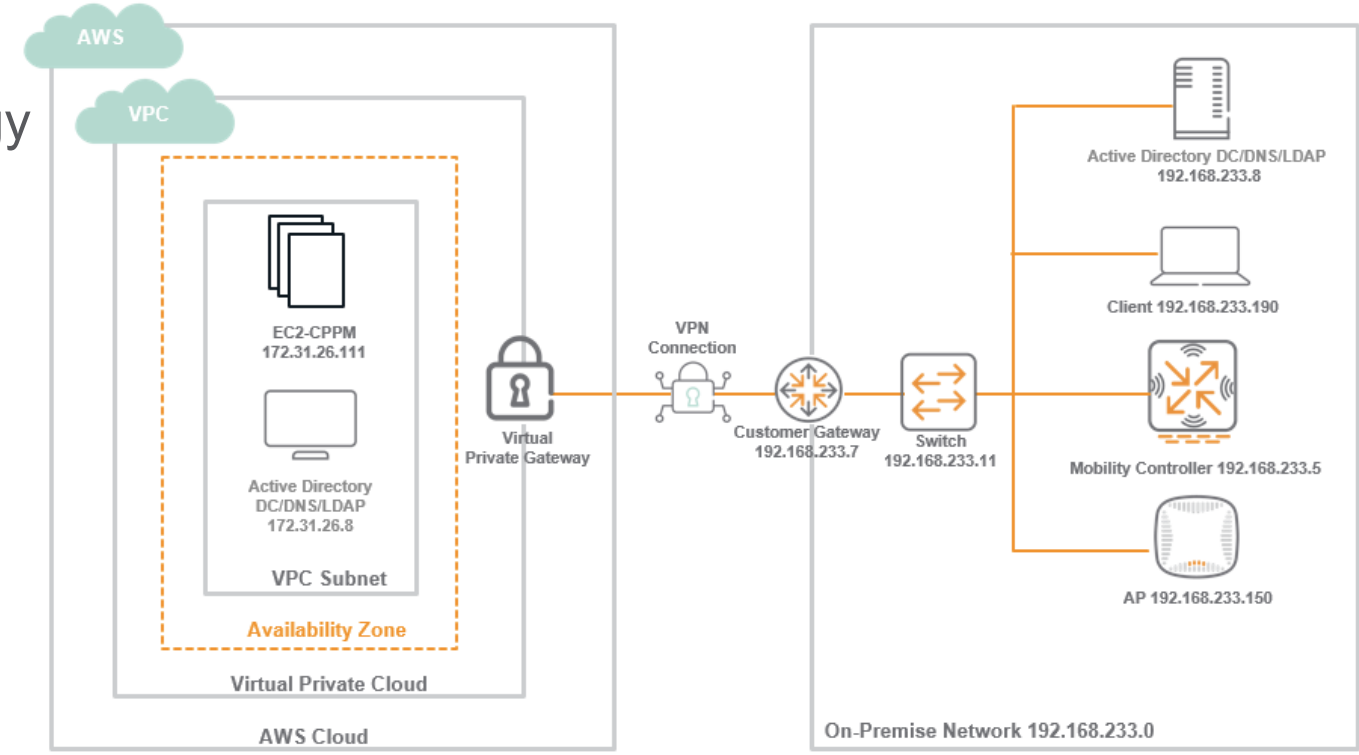
Hardware

ClearPass *in* the Cloud

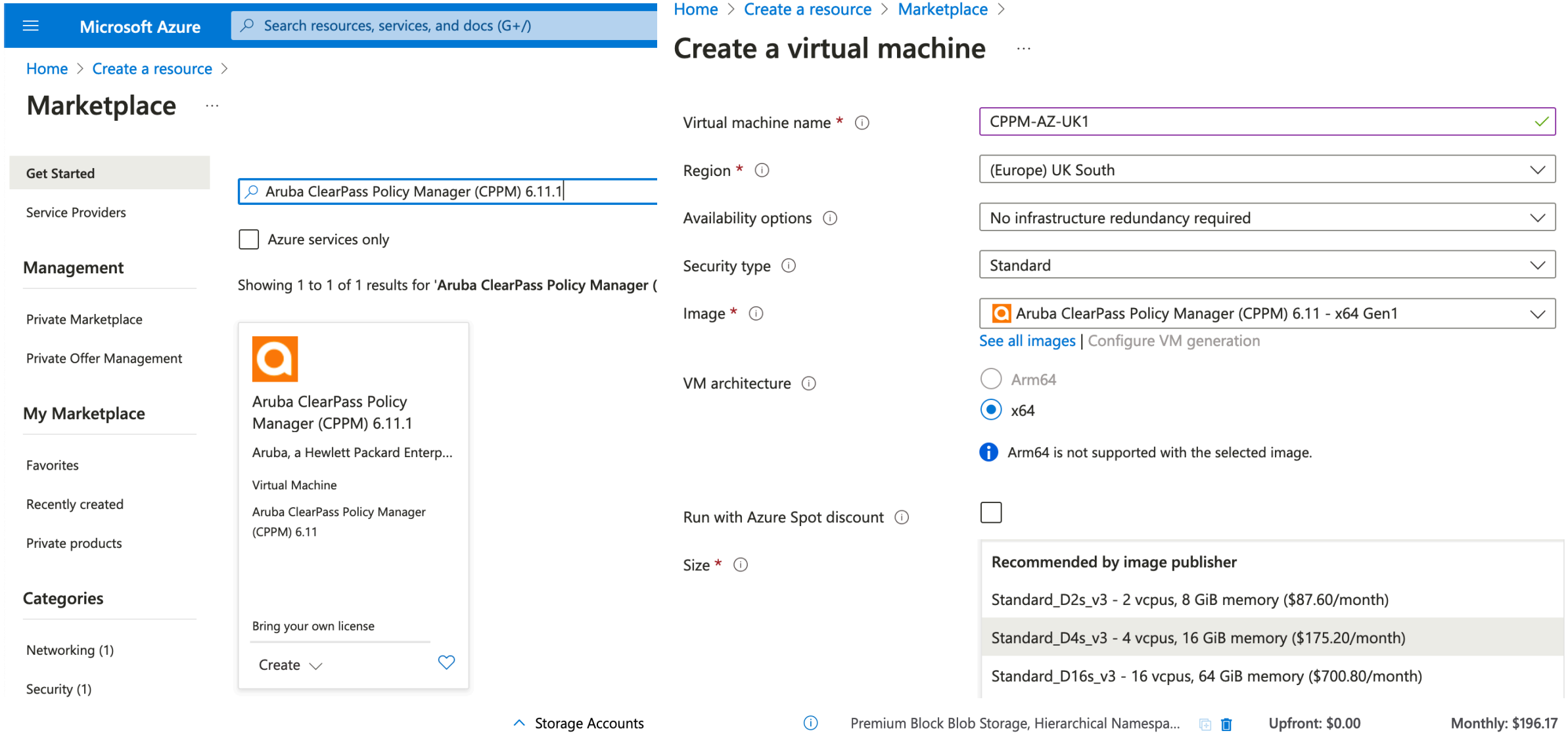
Options for ClearPass to run in and with the cloud

Running ClearPass in the cloud: AWS / Azure

- Runs in a Virtual Private Cloud (VPC)
- Same ClearPass as on-premise, it just runs in the cloud instead of in your datacenter
- Connectivity required between Branch and VPC. Normally part of cloud strategy already.
- Perfect match with Aruba EdgeConnect SD-Branch / Cloud Orchestrator.
- Flexibility to cluster ClearPass between cloud
  and on-prem (publisher/subscriber)



Running ClearPass in Azure: Marketplace



Running ClearPass in the cloud: Azure

Behavior Differences in an Azure Deployment

When ClearPass is hosted in Azure, users should be aware of the following differences:

- In the server configuration settings, **editing is disabled for the management port IP address, management port subnet mask, default gateway, data port IP address, data port subnet mask, and default gateway. SPAN port settings are also hidden.**
- The footer of the Policy Manager WebUI includes the indicator [Cloud] after the version number.
- The Policy Manager Cluster-Wide Parameters settings include the Virtual IP tab and its Failover Wait Time field, even though the **Virtual IP feature is not supported by ClearPass running on Azure.** Although these fields are available and a configuration can be entered, the configuration will not take effect.
- The CLI commands system factory-reset, system install-image, and system refresh-network are not available in ClearPass running on Azure.
- Common Criteria (CC) mode is not supported in ClearPass running on Azure.
- Starting with ClearPass 6.10, the system morph-vm command can be used to morph an instance of ClearPass on Azure to a larger or production virtual machine.
- **Network IP addresses in an Azure instance are managed by Azure, not by ClearPass, and the primary interface is the single default gateway.** If a user adds a new data port manually using the network IP routing CLI commands, it will not persist after a reboot. If your organization requires a different default gateway configuration, please contact the Aruba Technical Assistance Center (TAC).

Running ClearPass in the cloud: Azure and Clustering

ClearPass clustering (Publisher-Subscriber) is supported:

- Between cloud instances
- Within or between VPC, Regions, etc.
- Between Azure and On-Premise
- Between virtual and hardware appliances

… as long as the requirements for making a node a subscriber are met (below for ClearPass 6.11)
https://www.arubanetworks.com/techdocs/ClearPass/6.11/PolicyManager/Content/Deploy/Cluster%20Deployment/Design_guidelines.htm

- In a large-scale deployment, reduced bandwidth or high latency on the link (greater than **200 ms**) delivers a lower-quality user experience for all users of that Subscriber, even though static content is delivered locally almost instantaneously.
- In a large geographically dispersed cluster, the worst-case round-trip time (RTT) between a NAS/NAD and all potential servers in the cluster that might handle authentication is a design consideration.
- Aruba recommends that the round-trip time between the NAD/NAS and a Policy Manager server should not exceed 600 ms.
- The acceptable delay between cluster servers is less than 100 ms (RTT less than 200 ms).
- The link bandwidth should be greater than 10 Mbps.

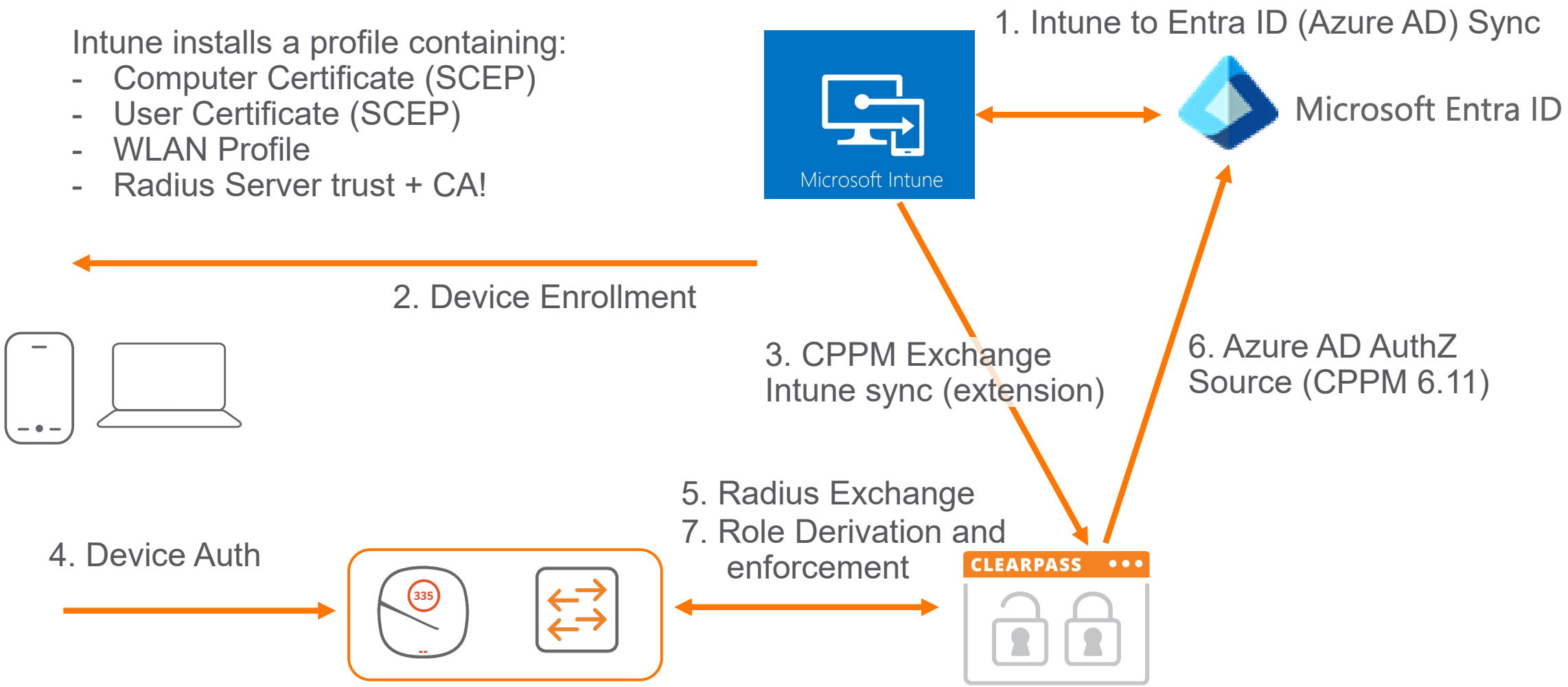
Running ClearPass in the Cloud Azure (Summary)

- Running ClearPass in Azure is very similar to running ClearPass On-Premises
- Think of it like running ClearPass on Microsoft's computer instead of on your own
- Performance numbers for Azure are reported slightly lower than for VM/Hardware for some customers → plan for some additional 'headroom'

ClearPass with the Cloud

Options for ClearPass to run *with* the cloud

Example: Entra ID (Azure AD) / Intune / CPPM integration



Authentication and Authorization: Authentication

Authentication = verify credentials

Does the password match?
Is the certificate valid?
Is it a valid MAC Address?

Auth Methods
MAC Auth
802.1X
Captive Portal

Against

Authentication sources:
Endpoint Repository
Local User Database
Guest User Database
MSCHAPv2 (AD)
TLS (Client Certificate)

Result in

Attributes like:
Authentication status (pass/fail)
Username
Client MAC
Certificate Attributes
(Intune Device ID)
Computer or User

Entra ID (Azure AD) and PEAP-MSCHAPv2 / Password Authentication

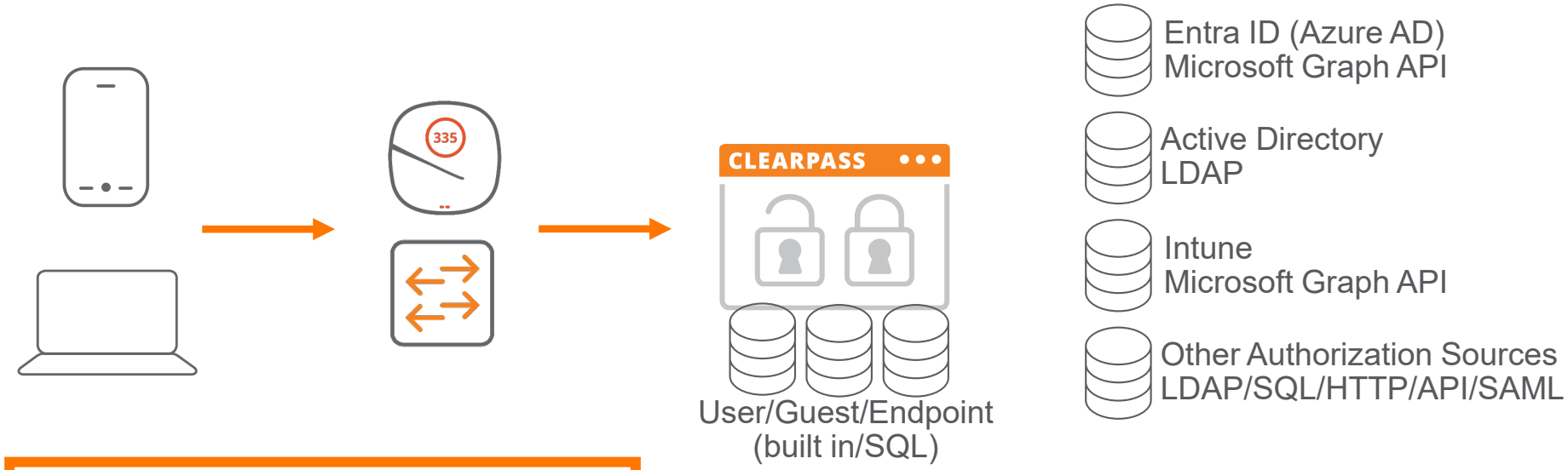
– Cloud providers are moving away from password authentication

– For MS-CHAPv2 authentication, access to the password is needed

– By design, in most Cloud Identity Stores access to the password is prohibited

– The only feasible WiFi/Wired 802.1X methods are ones with Client Certificates: EAP-TLS or TEAP (with EAP-TLS as inner methods)

Authentication and Authorization: Authorization



Authentication attributes like:
Authentication status (pass/fail)
Username
Client MAC
Certificate Attributes
(Intune Device ID)

Authorization depends on the available authentication attributes

Checked in…

Authorization sources:
Endpoint Repository
Local User Database
Guest User Database
Active Directory (LDAP)
Intune
Entra ID (Azure AD)

Retrieve…

Authorization Attributes like:
Compliance status
User Full Name
Group Membership
Device Type (profiling)

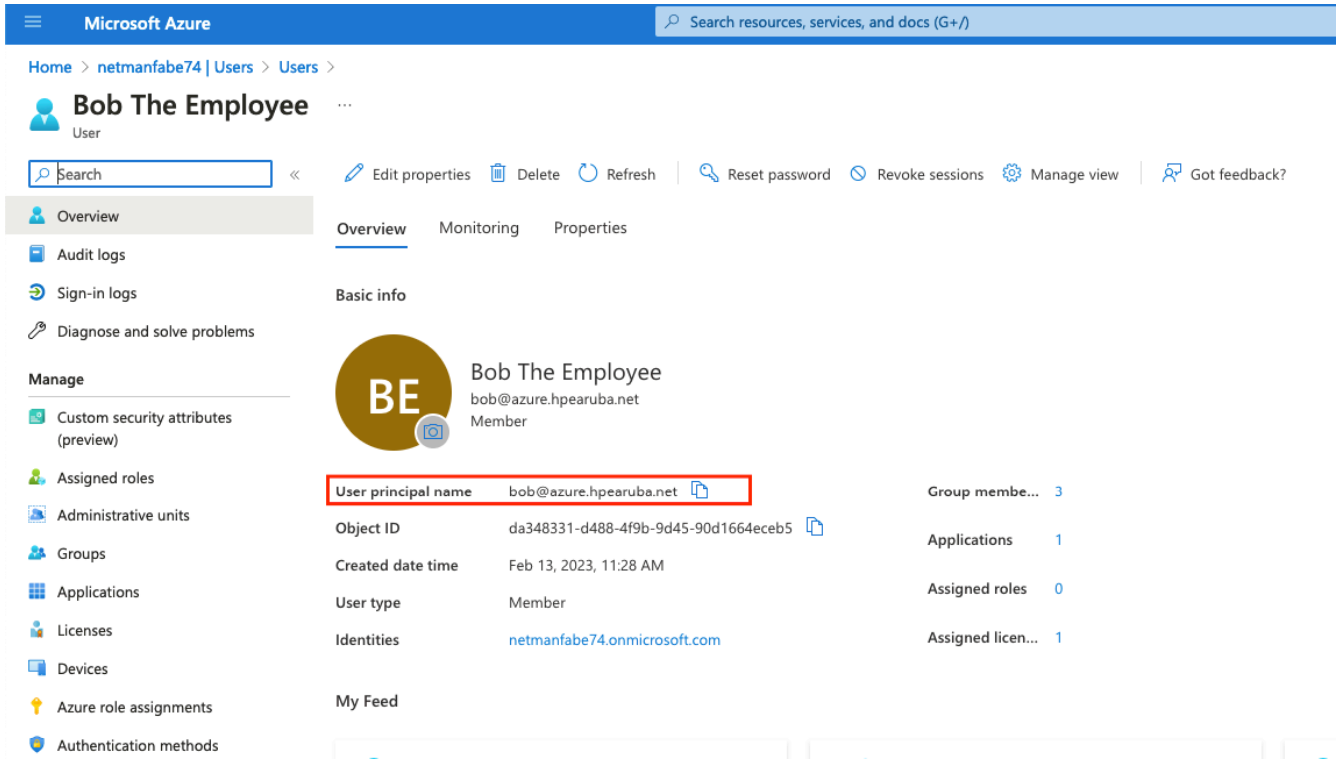
Used for…

Enforcement Policy:
ACCEPT/REJECT
Aruba-User-Role
VLAN
Post Authentication

Authentication of Entra ID Users

Azure AD Authorization Source

- Query Entra ID Group/Department/Email Information
- Authorization only
- Authentication preferred TLS Client Certificate, but can be anything that provides the userPrincipalName



Microsoft Entra ID

Azure AD AuthZ Source (CPPM 6.11)

CLEARPASS

Azure AD Authorization Source

- Query Entra ID Group/Department/Email Information
- Authorization only
- Authentication preferred TLS Client Certificate, but can be anything that provides the userPrincipalName

Microsoft Entra ID

Configuration » Authentication » Sources » Add - CIC-AzureAD

Authentication Sources - CIC-AzureAD

Summary | General | Primary | Attributes

General:

Name:	CIC-AzureAD
Description:	Display name: Genevia CIC CPPM AzureAD AuthZ Application (client) ID: bbd6d3e0-2368-42a5-a8a9-7b607638f331 Object ID: 262768b0-2fb8-4439-8347-8addd85982f0 Directory (tenant) ID: 6d648377-d3db-49f0-a0c8-f61acfc19fd3
Type:	Azure

Primary:

Base URL:	https://login.microsoftonline.com/%s/oauth2/v2.0/token/
Tenant Id:	6d648377-d3db-49f0-a0c8-f61acfc19fd3
Client Id:	bbd6d3e0-2368-42a5-a8a9-7b607638f331
Client Secret:	********

Attributes:

Filters :	1. users/?select=mail,userPrincipalName,id,department,accountEnabled&$filter=userPrincipalName%{Authentication:Username} /users/{id}/memberOf?select=displayName

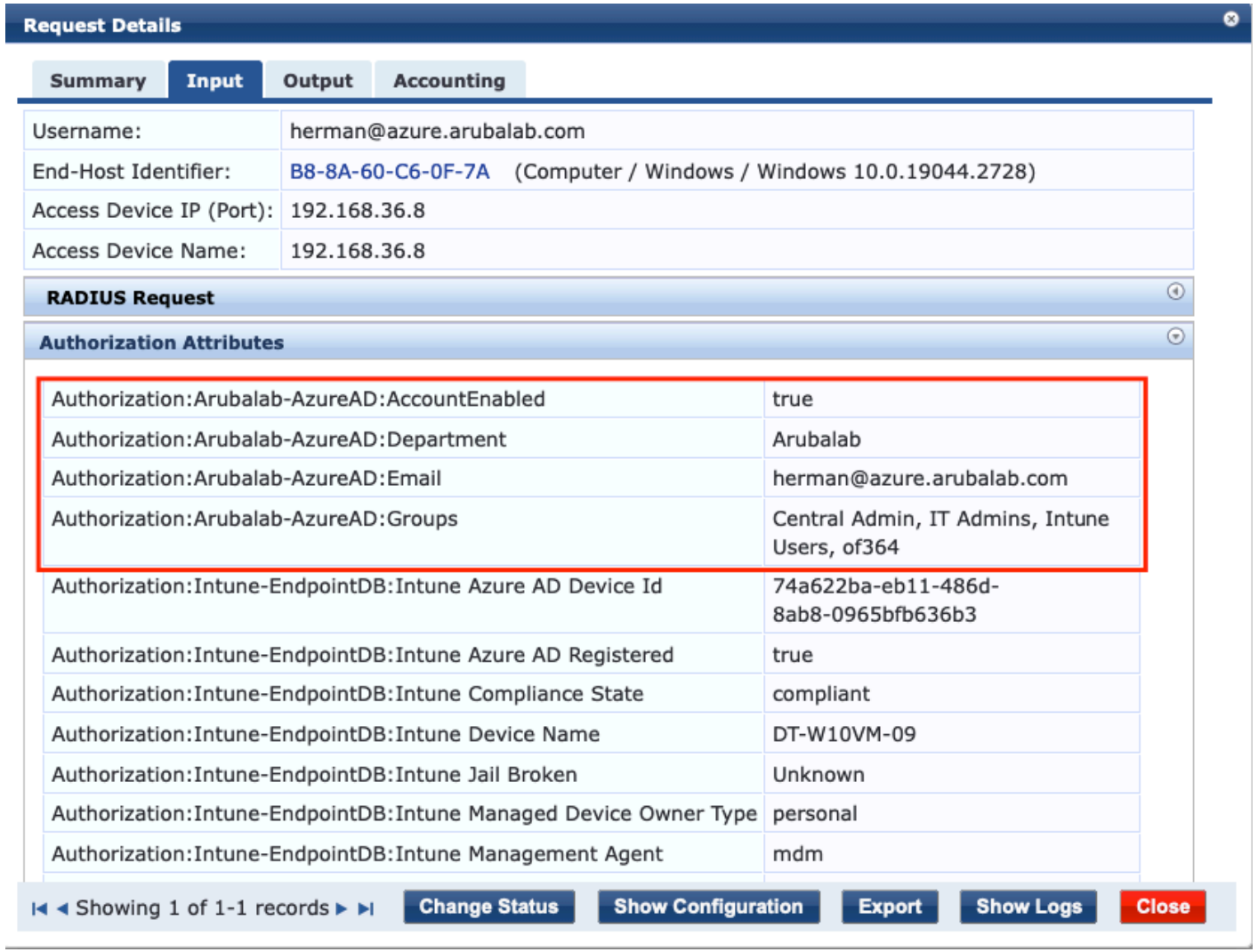
Summary | General | Primary | Attributes

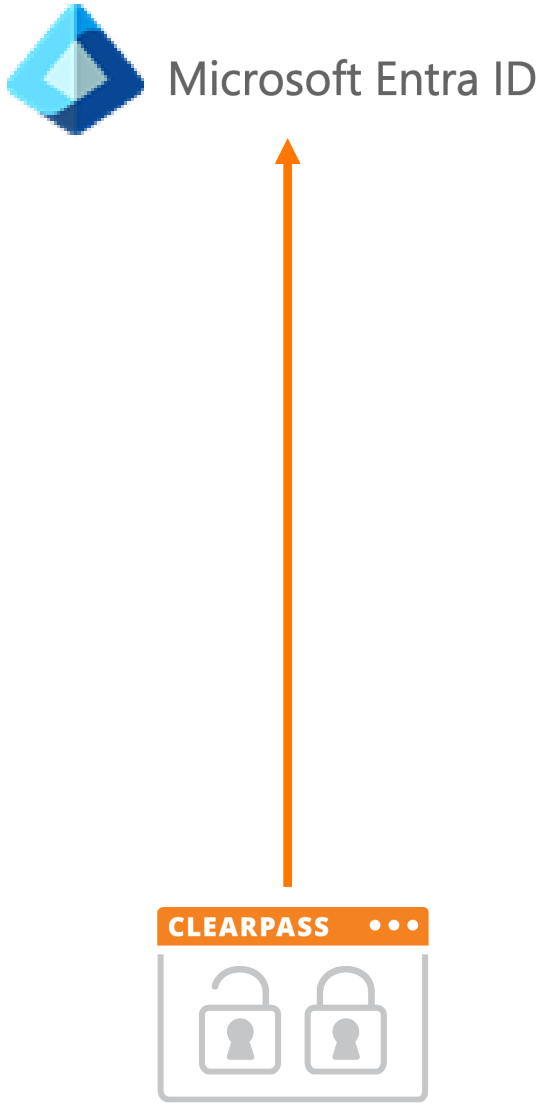
Specify filter queries used to fetch authentication and authorization attributes

	Filter Name	Attribute Name	Alias Name	Enabled As
1.	Groups	displayName	Groups	-
		department	Department	Attribute
		mail	Email	Attribute
		accountEnabled	AccountEnabled	Attribute

Azure AD Authorization Source

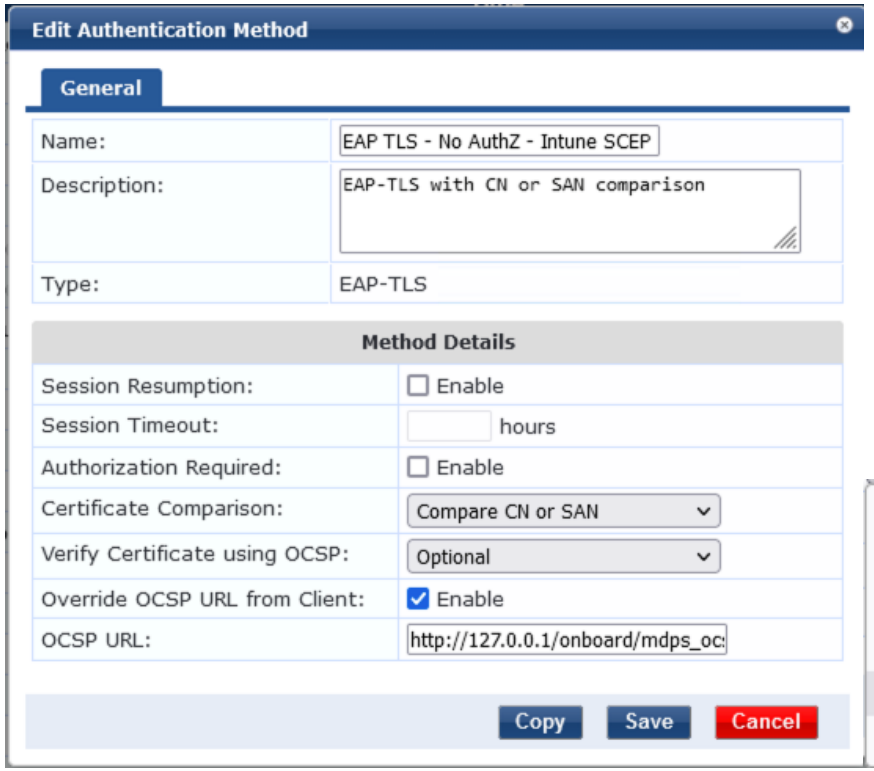
As documented: Only Groups is supported for Enforcement in current CPPM

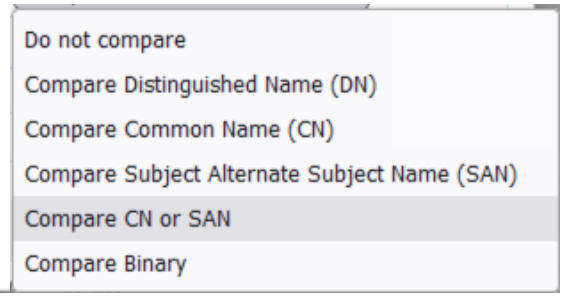


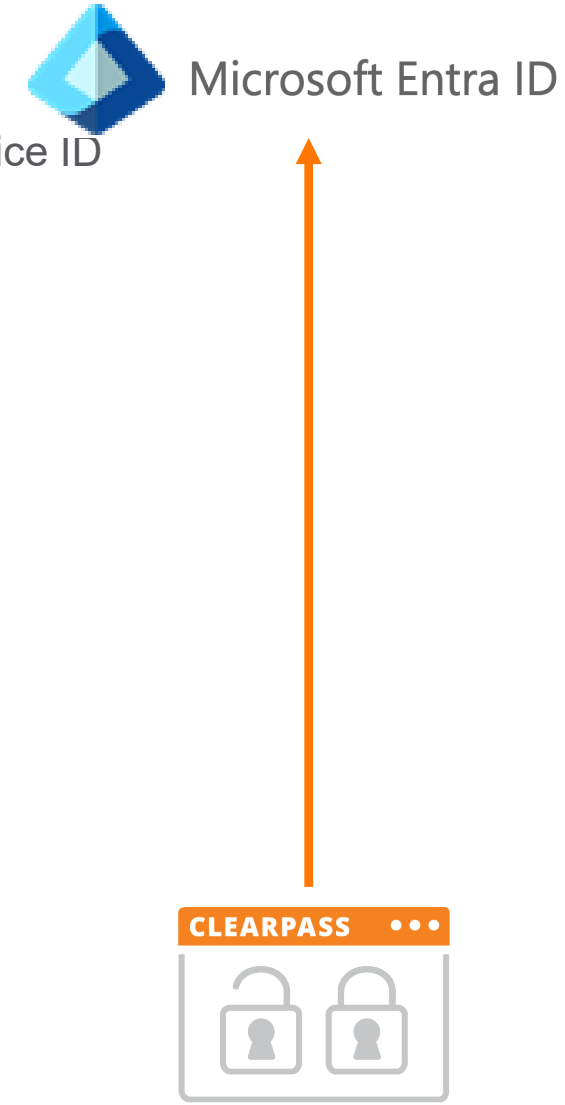


EAP-TLS Authentication Method with Entra ID (Azure AD)

- Disable Authorization
  - This is needed because there is no authentication source that can validate the Intune Device ID
- DO Set Certificate Comparison to: Compare CN or SAN
  - to prevent username spoofing



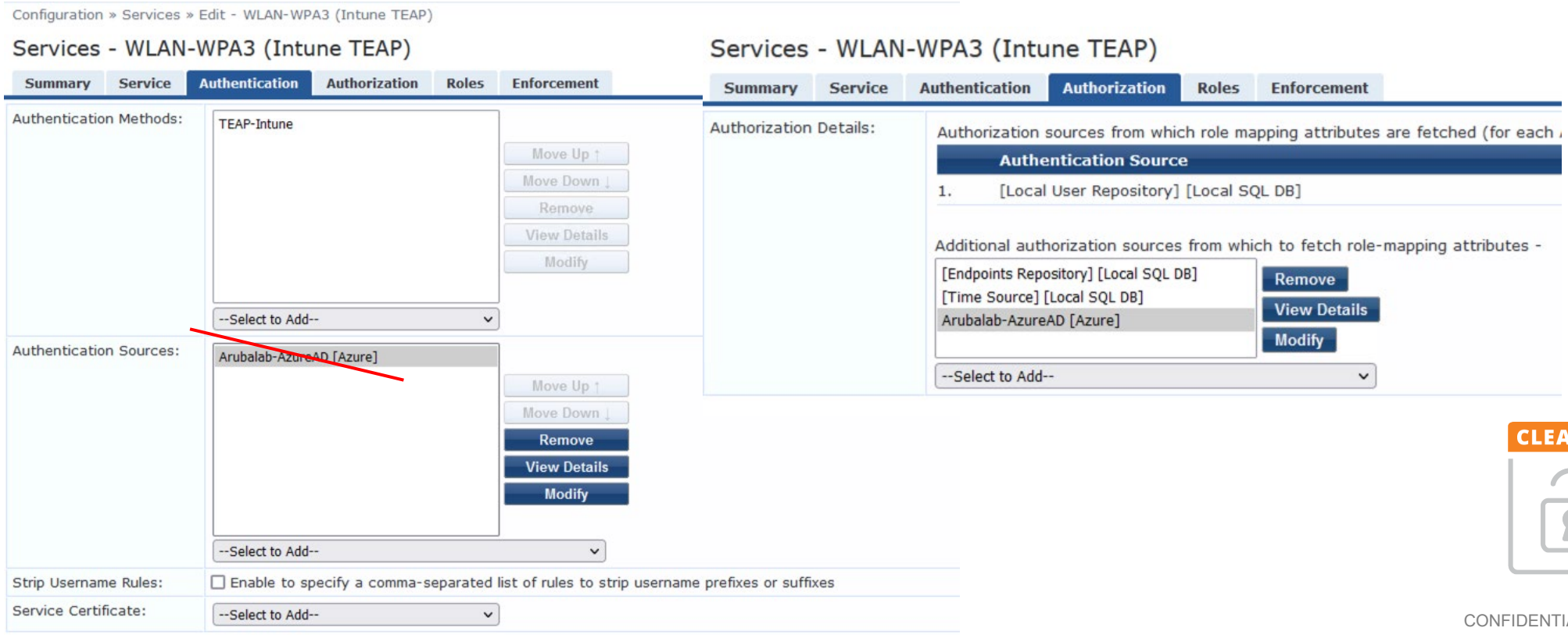




EAP-TLS Authentication Method with Entra ID (Azure AD)

- Do NOT add Azure AD as Authentication source.
  - Or…. RADIUS Service will STOP [expected to be fixed in future release]
- Add as Authorization source only

Microsoft Entra ID

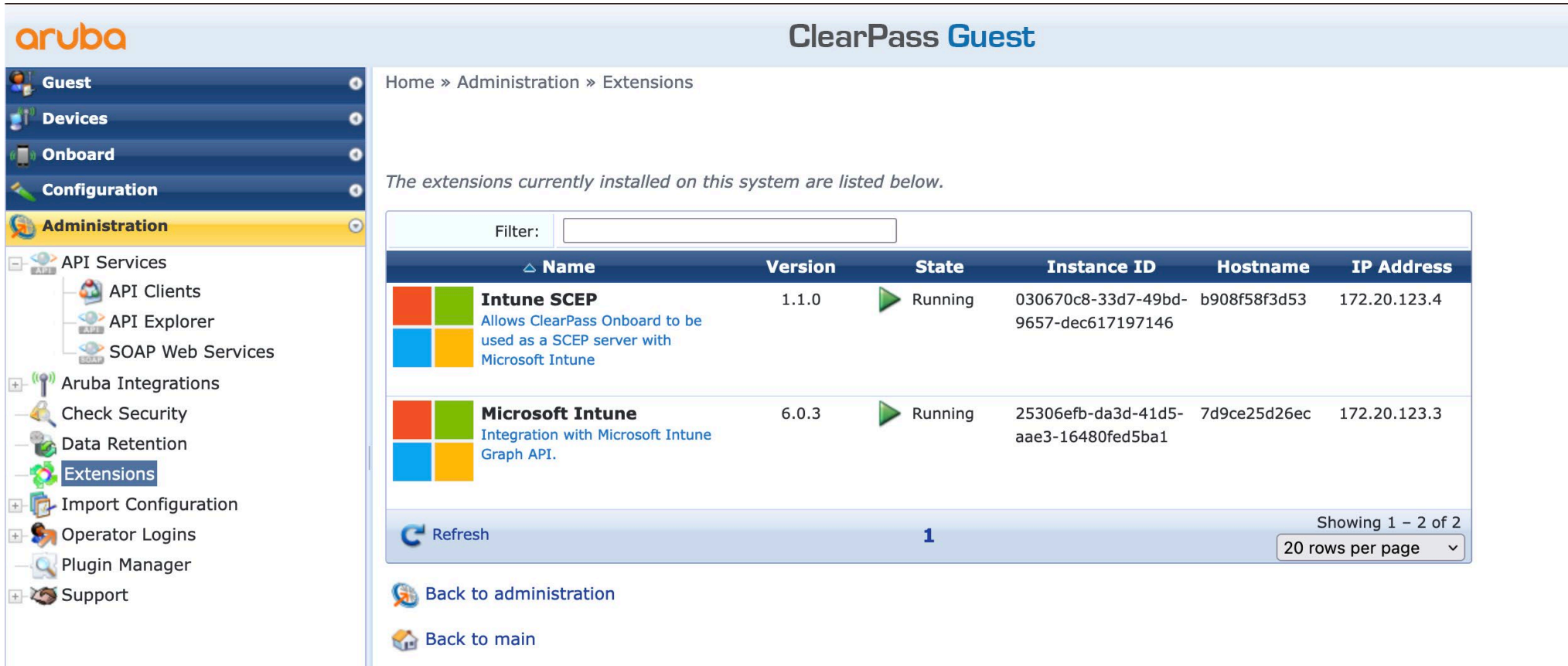


Microsoft Intune

(Authorization)

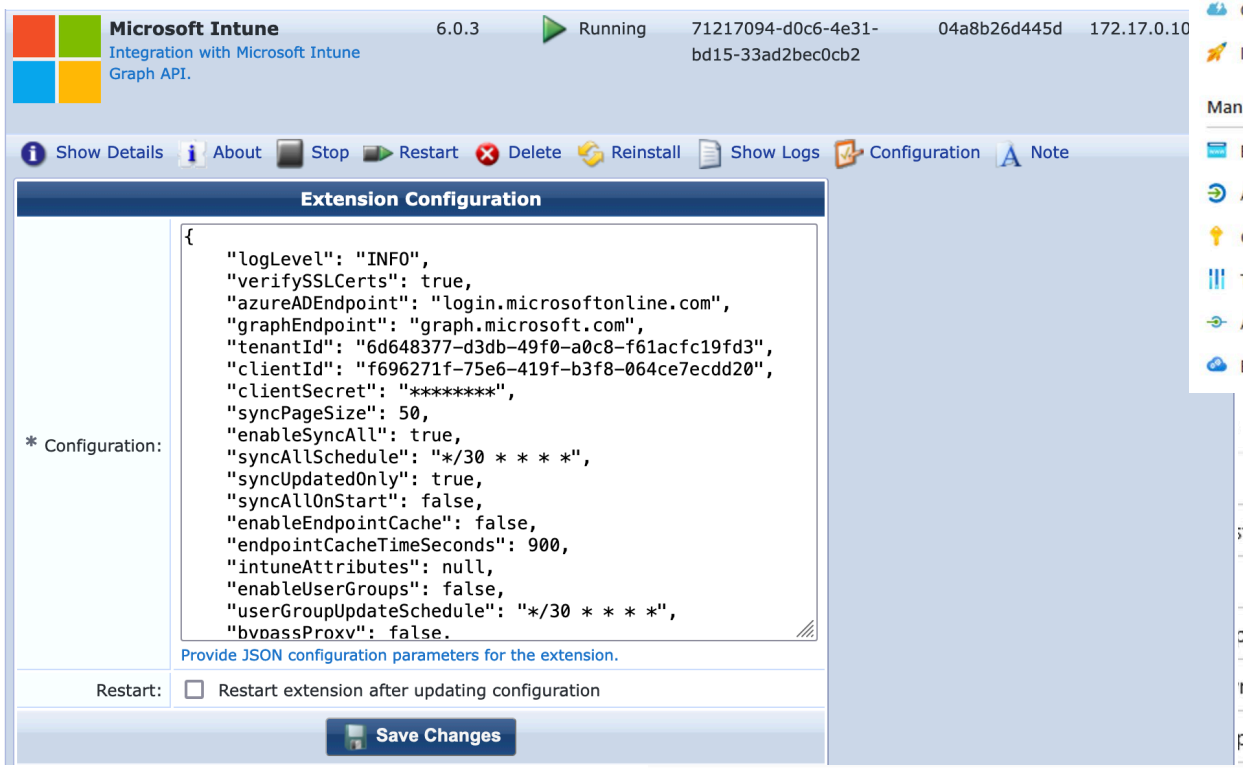
ClearPass Extensions – What are Extensions?

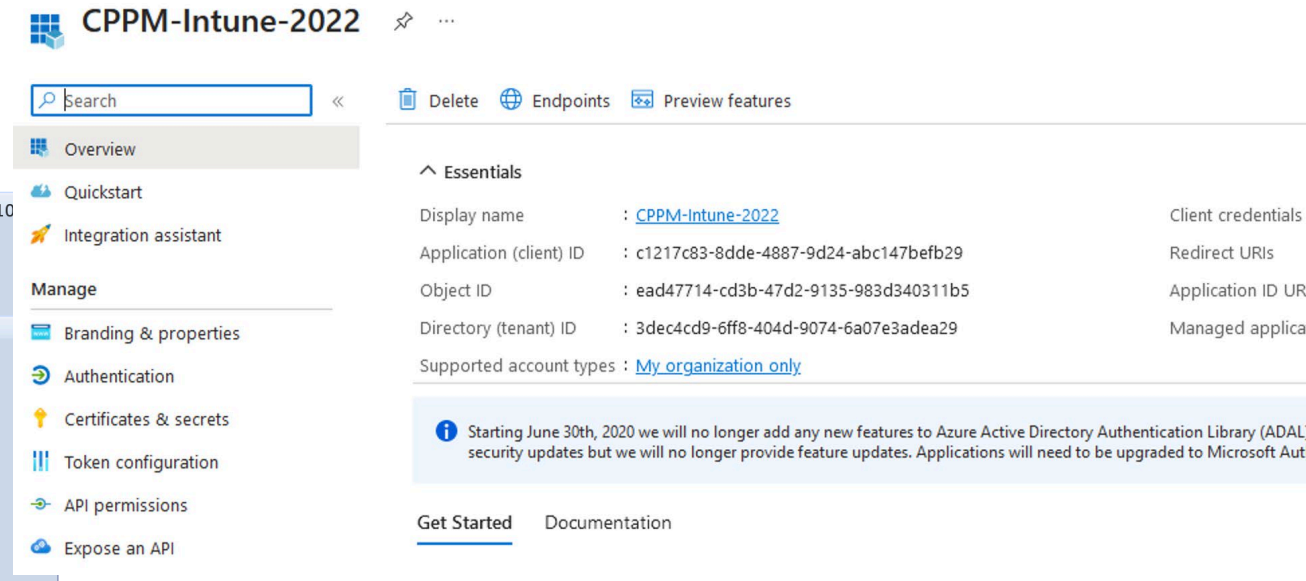
- Software package running inside ClearPass
- Adds functionality independent of the ClearPass version
- Install from the ClearPass Extension Store
- No additional cost, included in ClearPass Access License. Some partners may charge on their side.



ClearPass Intune Extension

- API/App registration in Entra ID

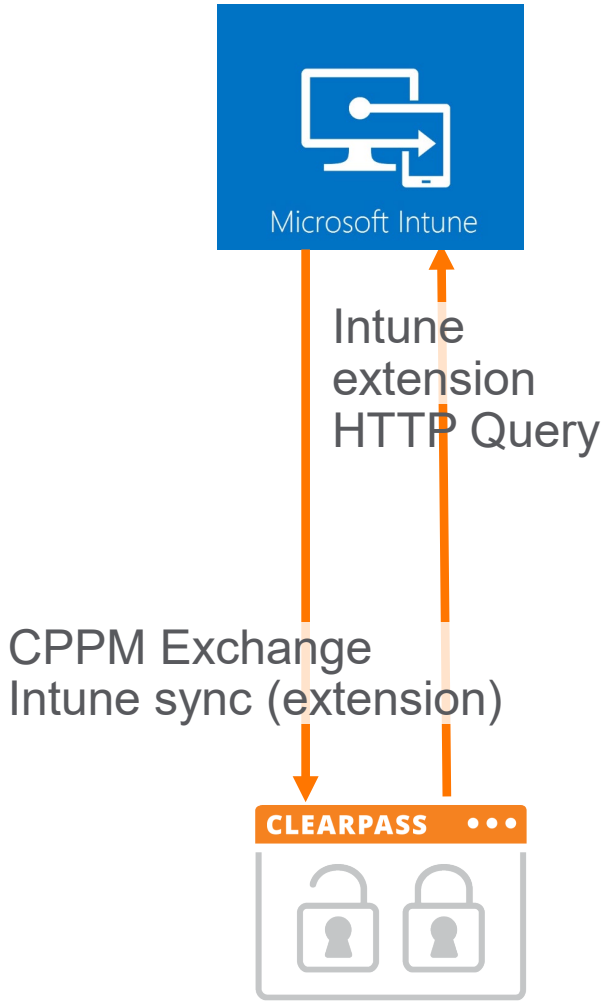




			Admin consent req...	Status
		tate and compliance information from Micro...	Yes	Granted for of364
		plications	Yes	Granted for of364
		rite all applications	Yes	Granted for of364
		ps that this app creates or owns	Yes	Granted for of364
DeviceManagementApps.Read.A	Application	Read Microsoft Intune apps	Yes	Granted for of364
DeviceManagementManagedDe	Application	Read Microsoft Intune devices	Yes	Granted for of364
DeviceManagementManagedDe	Application	Read and write Microsoft Intune devices	Yes	Granted for of364
Directory.Read.All	Application	Read directory data	Yes	Granted for of364
User.Read	Delegated	Sign in and read user profile	No	Granted for of364

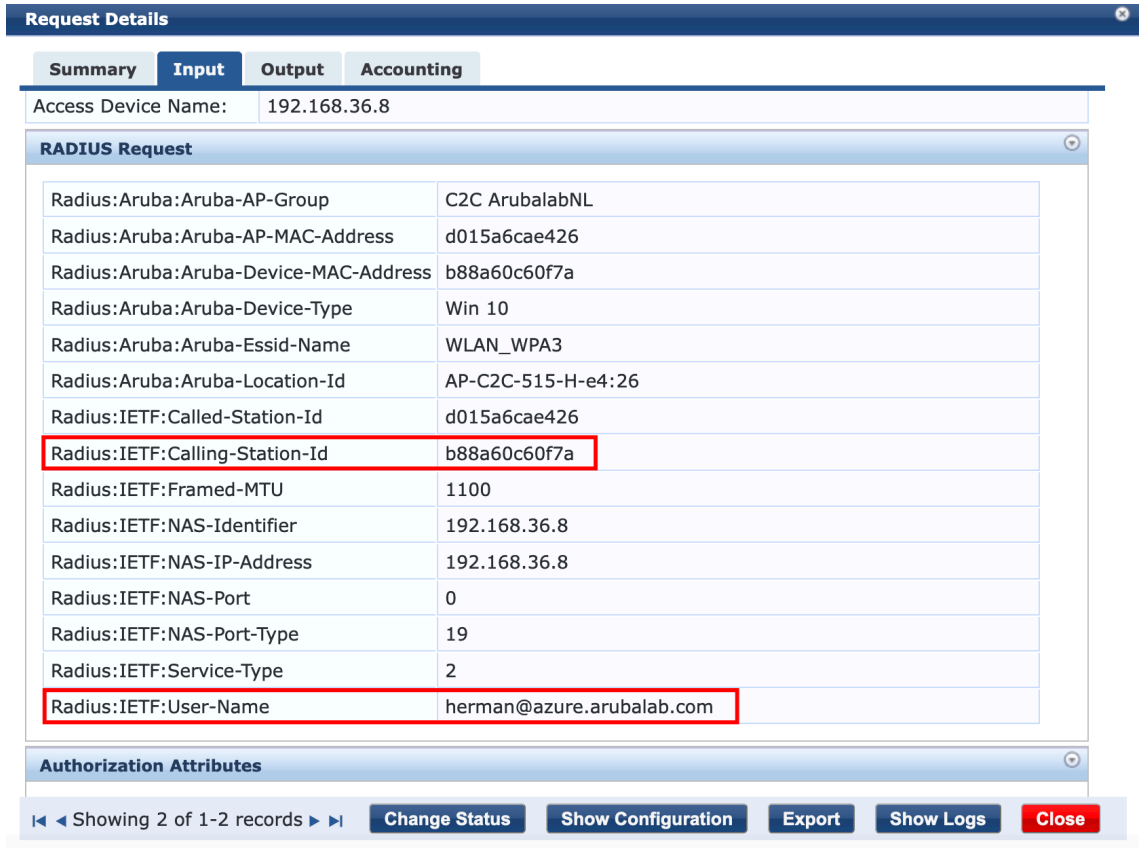
ClearPass Intune Extension Methods (Authorization)

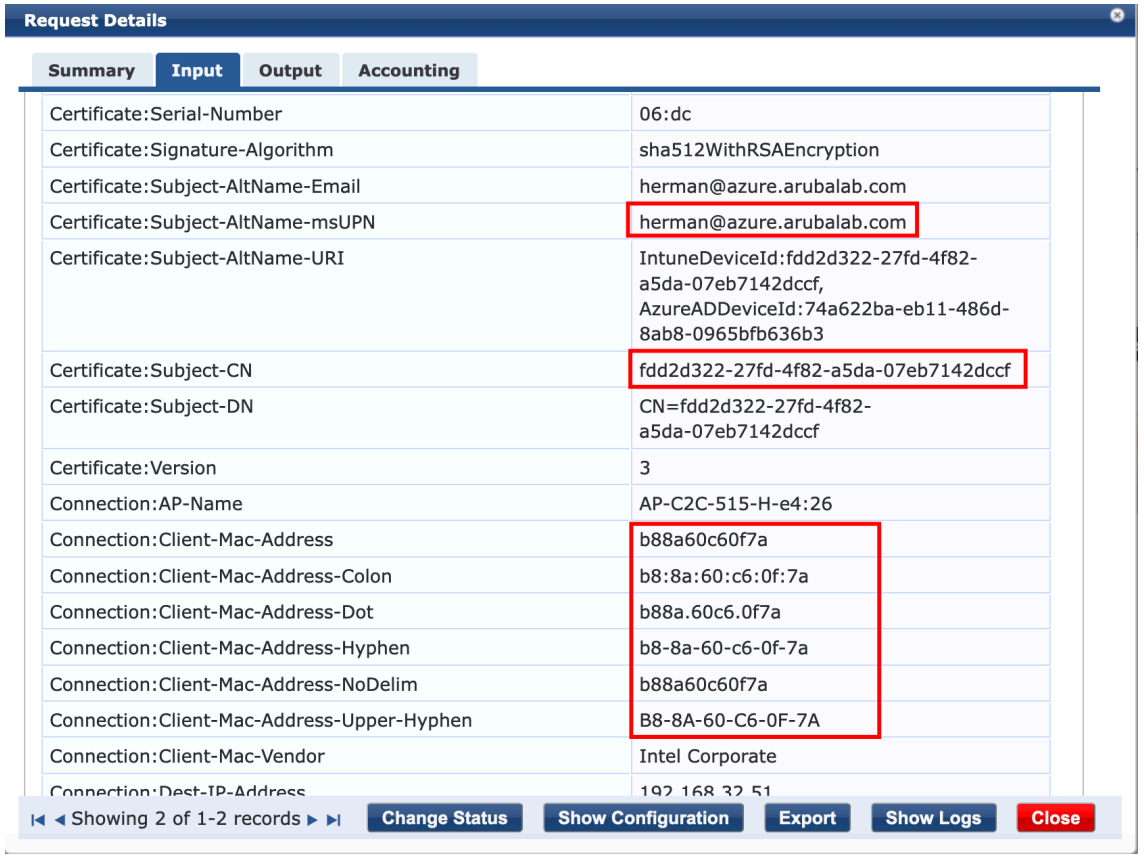
- Endpoint database
  - Pull attributes from Intune periodic (incremental) sync
  - **+** No external dependencies, fast as data is in ClearPass already
  - **-** Possible latency in status updates between last sync and authentication
  - **+** Only needs to run on a single ClearPass instance in the cluster (or two for redundancy)
- HTTP
  - Localhost HTTP Query to the Intune Extension
  - **+** Real-time (and cached)
  - **+** No need to sychronize full Intune database into ClearPass Endpoint DB
  - **-** Cloud dependency
  - **-** Small latency to query Intune (GraphAPI)



Sample Authentication Attributes

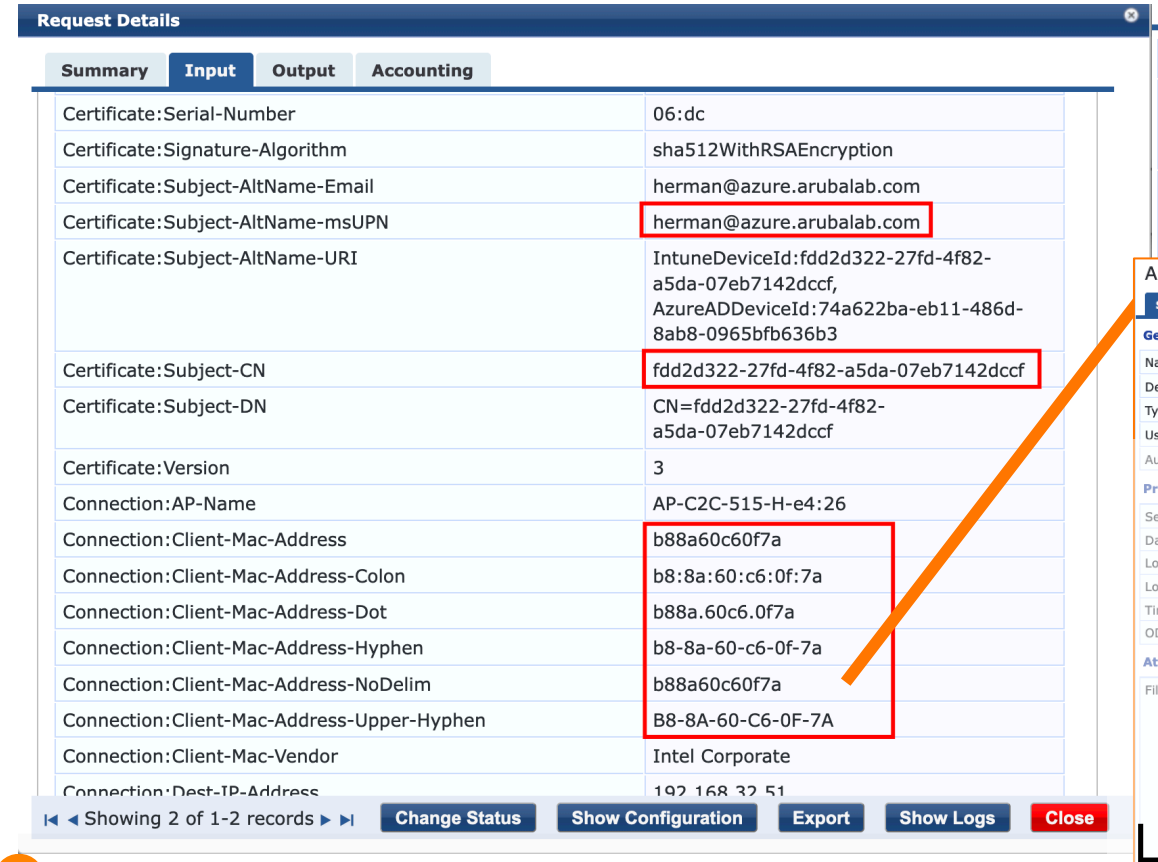
Certificate information only with EAP-TLS / EAP-TEAP

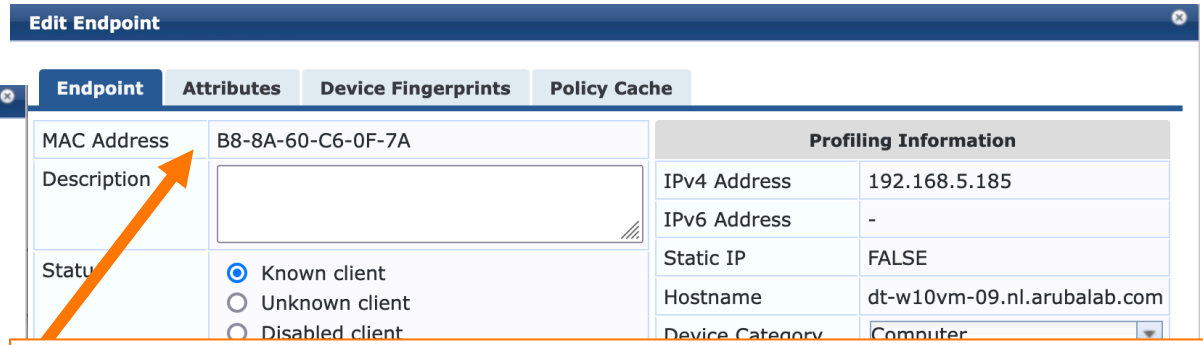


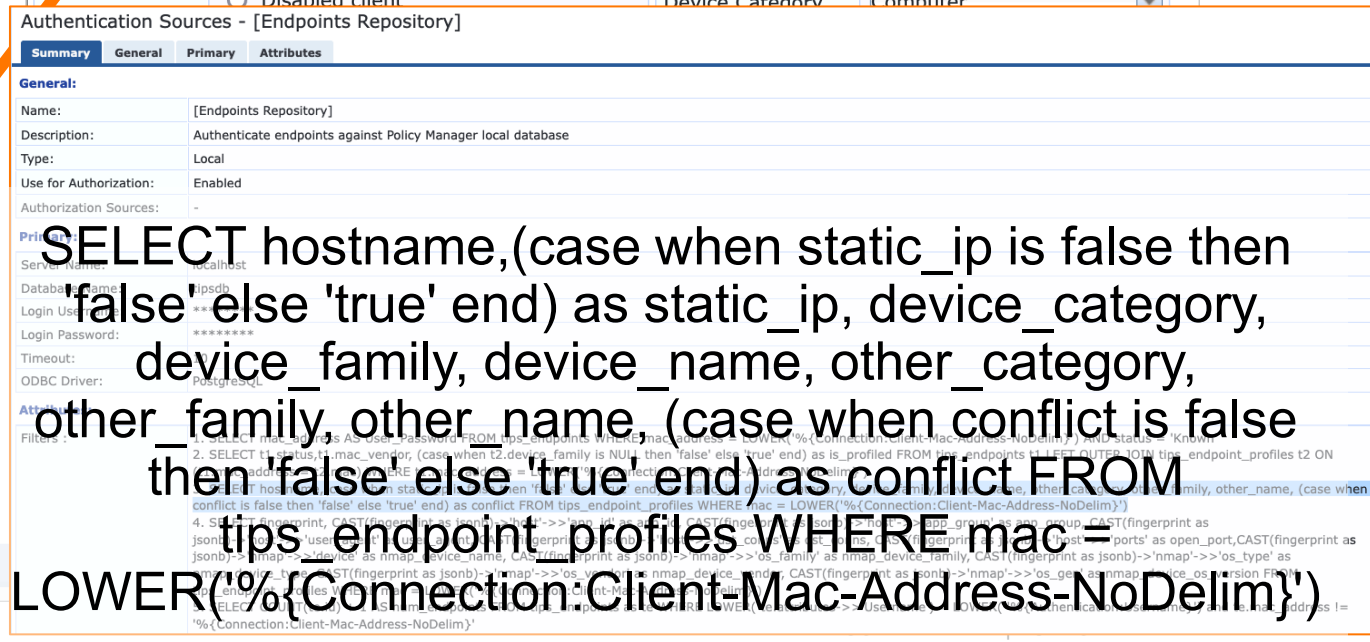


Using the MAC address to look up Intune Attributes in Endpoint

- Deprecated, risk of MAC spoofing
- Incompatible with wired as the wireless MAC address is used
- Incompatible with MAC Randomization



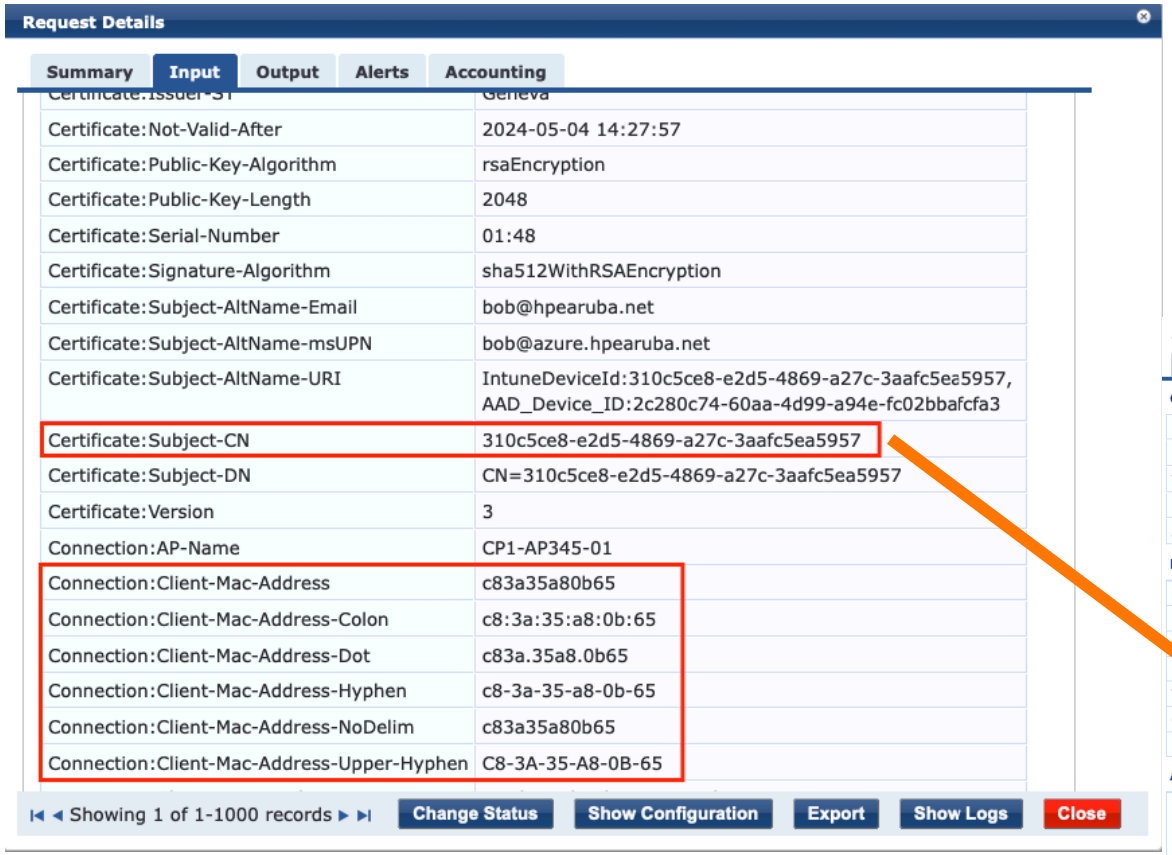


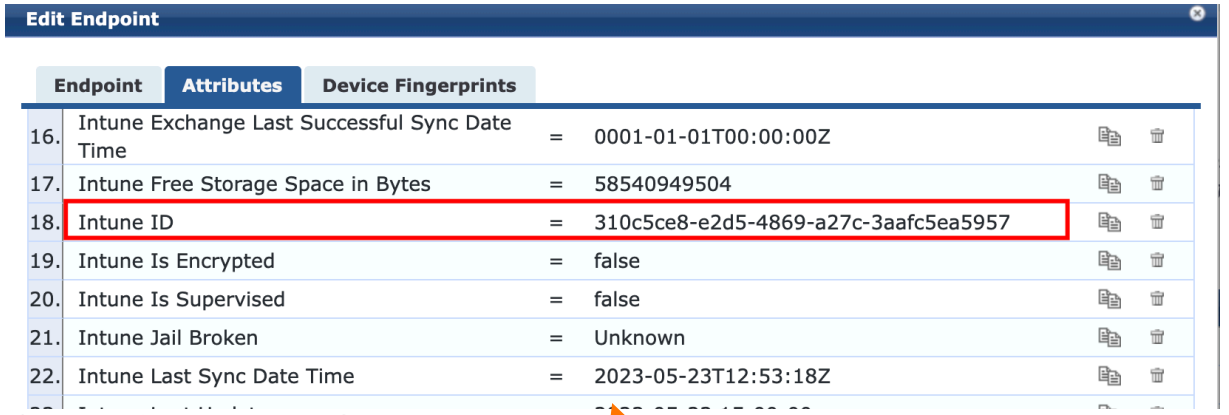


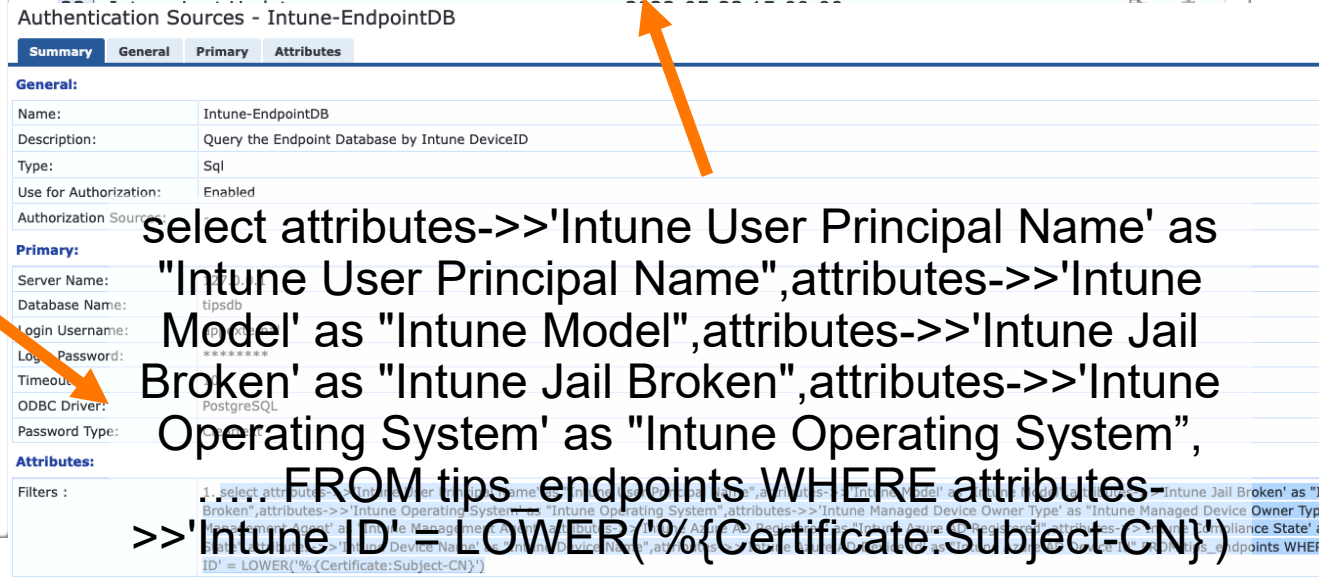
SELECT hostname,(case when static_ip is false then 'false' else 'true' end) as static_ip, device_category, device_family, device_name, other_category, other_family, other_name, (case when conflict is false then 'false' else 'true' end) as conflict FROM tips_endpoint_profiles WHERE mac = LOWER('%{Connection:Client-Mac-Address-NoDelim}')

Using the Intune Device Id to lookup Attributes in Endpoint

- Recommended method
- Independent of MAC Adress, supports MAC randomization and wired
- Prevents MAC spoofing








```
select attributes->>'Intune User Principal Name' as "Intune User Principal Name",attributes->>'Intune Model' as "Intune Model",attributes->>'Intune Jail Broken' as "Intune Jail Broken",attributes->>'Intune Operating System' as "Intune Operating System", FROM tips_endpoints WHERE attributes->>'Intune ID' = LOWER('%{Certificate:Subject-CN}')
```

Using the Intune Device Id to lookup Attributes from Extension (realtime)

Request Details

Summary | Input | Output | Accounting

Certificate:Serial-Number	06:dc
Certificate:Signature-Algorithm	sha512WithRSAEncryption
Certificate:Subject-AltName-Email	herman@azure.arubalab.com
Certificate:Subject-AltName-msUPN	herman@azure.arubalab.com
Certificate:Subject-AltName-URI	IntuneDeviceId:fdd2d322-27fd-4f82-a5da-07eb7142dccf, AzureADDeviceId:74a622ba-eb11-486d-8ab8-0965bfb636b3
Certificate:Subject-CN	fdd2d322-27fd-4f82-a5da-07eb7142dccf
Certificate:Subject-DN	CN=fdd2d322-27fd-4f82-a5da-07eb7142dccf

Configure Filter

Configuration

Filter Name: Intune-Attributes

Filter Query:

```
select attributes->>'Intune User Principal Name' as "Intune User Principal Name",attributes->>'Intune Model' as "Intune Model",attributes->>'Intune Jail Broken' as "Intune Jail Broken",attributes->>'Intune Operating System' as "Intune Operating System",attributes->>'Intune Managed Device Owner Type' as "Intune Managed Device Owner Type",attributes->>'Intune Management Agent' as "Intune Management Agent",attributes->>'Intune Azure AD Registered' as "Intune Azure AD Registered",attributes->>'Intune Compliance State' as "Intune Compliance State",attributes->>'Intune Device Name' as "Intune Device Name",attributes->>'Intune Azure AD Device Id' as "Intune Azure AD Device Id" FROM tips_endpoints WHERE attributes->>'Intune ID' = LOWER('%{Certificate:Subject-CN}')
```

	Name	Alias Name	Data type	Enabled As
1.	Intune User Principal Name	Intune User Principal Name	String	Attribute
2.	Intune Model	Intune Model	String	Attribute
3.	Intune Jail Broken	Intune Jail Broken	String	Attribute
4.	Intune Operating System	Intune Operating System	String	Attribute
5.	Intune Managed Device	Intune Managed Device	String	Attribute

Save | Close

Extension should run on each of your subscribers as well, and with the same IP address

Microsoft Intune Integration with Microsoft Intune Graph API.	6.0.3	Running	25306efb-da3d-41d5-aae3-16480fed5ba1	7d9ce25d26ec	172.20.123.3

Authentication Sources - Intune ExtRT

Summary | General | Primary | Attributes

General:

Name:	Intune ExtRT
Description:	Realtime lookup in Intune Extension
Type:	HTTP
Use for Authorization:	Enabled
Authorization Sources:	-

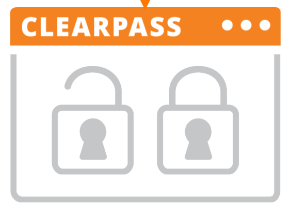
Primary:

Base URL:	http://172.20.123.3/device/info/id/
Login Username:	notuser
Login Password:	********
Timeout:	60

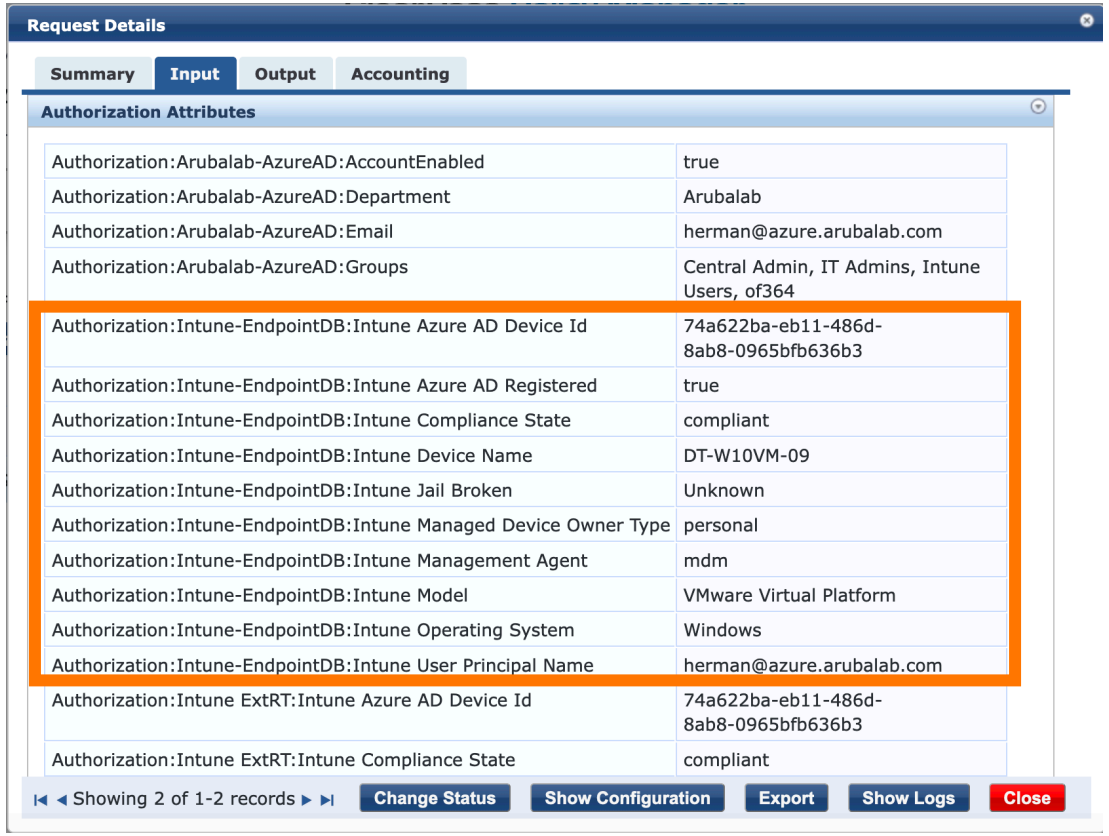
Attributes:

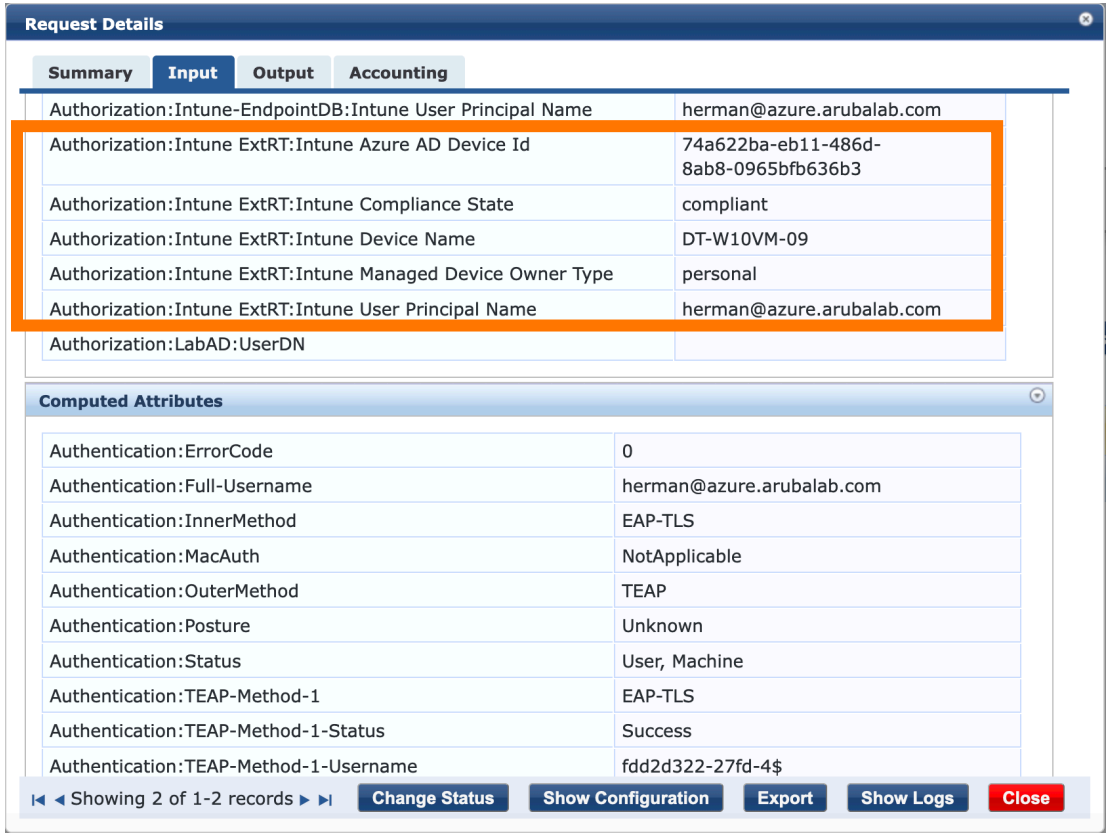
Filters :	1. %{Certificate:Subject-CN}

CPPM Exchange Intune sync (extension)



Intune Client in Access Tracker



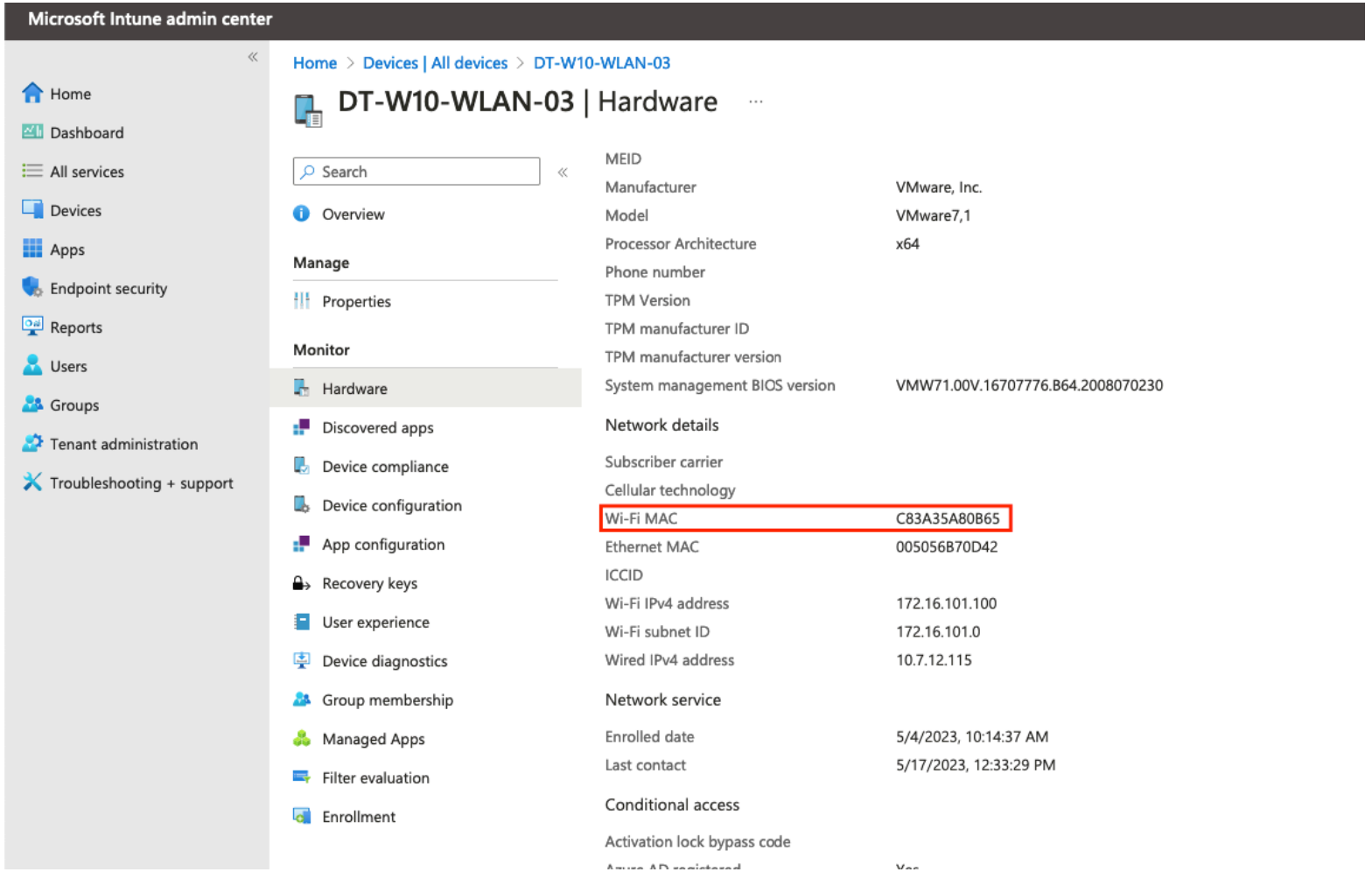


Authorization:Intune ExtRT => HTTP (Realtime Query)

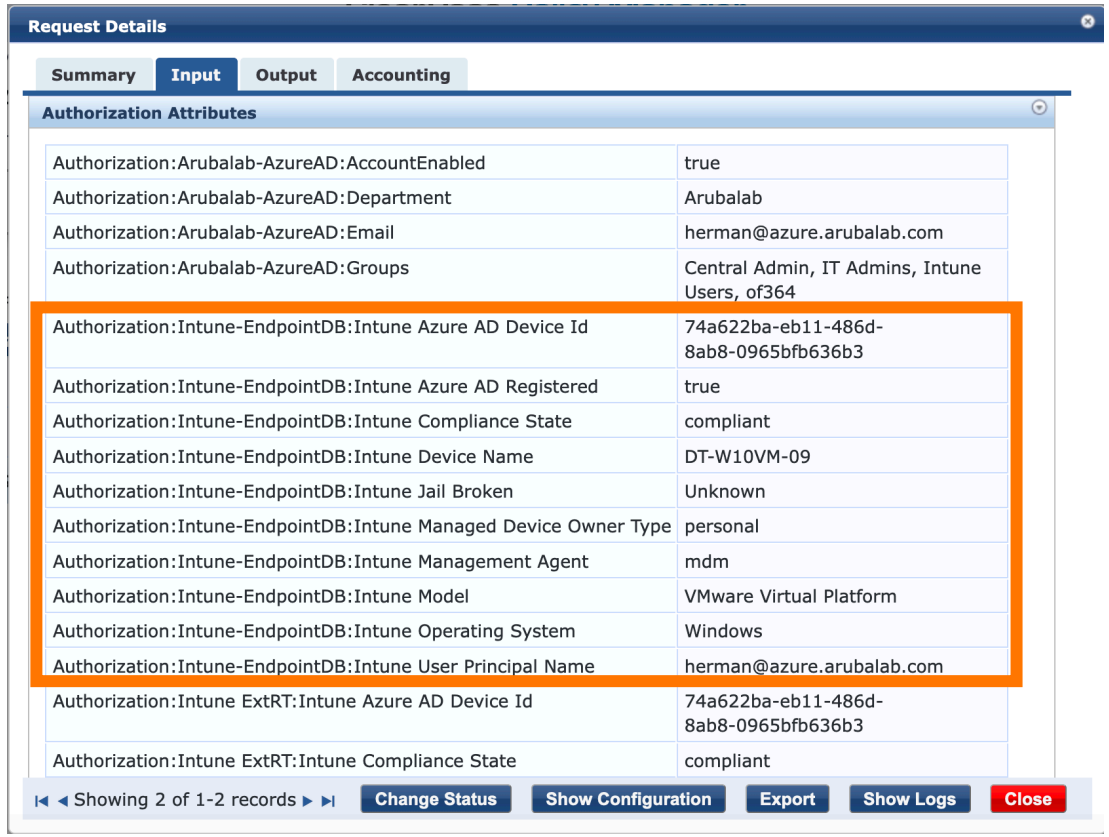
Authorization:Intune-EndpointDB => Endpoint DB query based on Intune Device Id

Endpoint Sync only with Wi-Fi MAC

Sample client in Intune: Wi-Fi MAC is present



Endpoint Sync only with Wi-Fi MAC

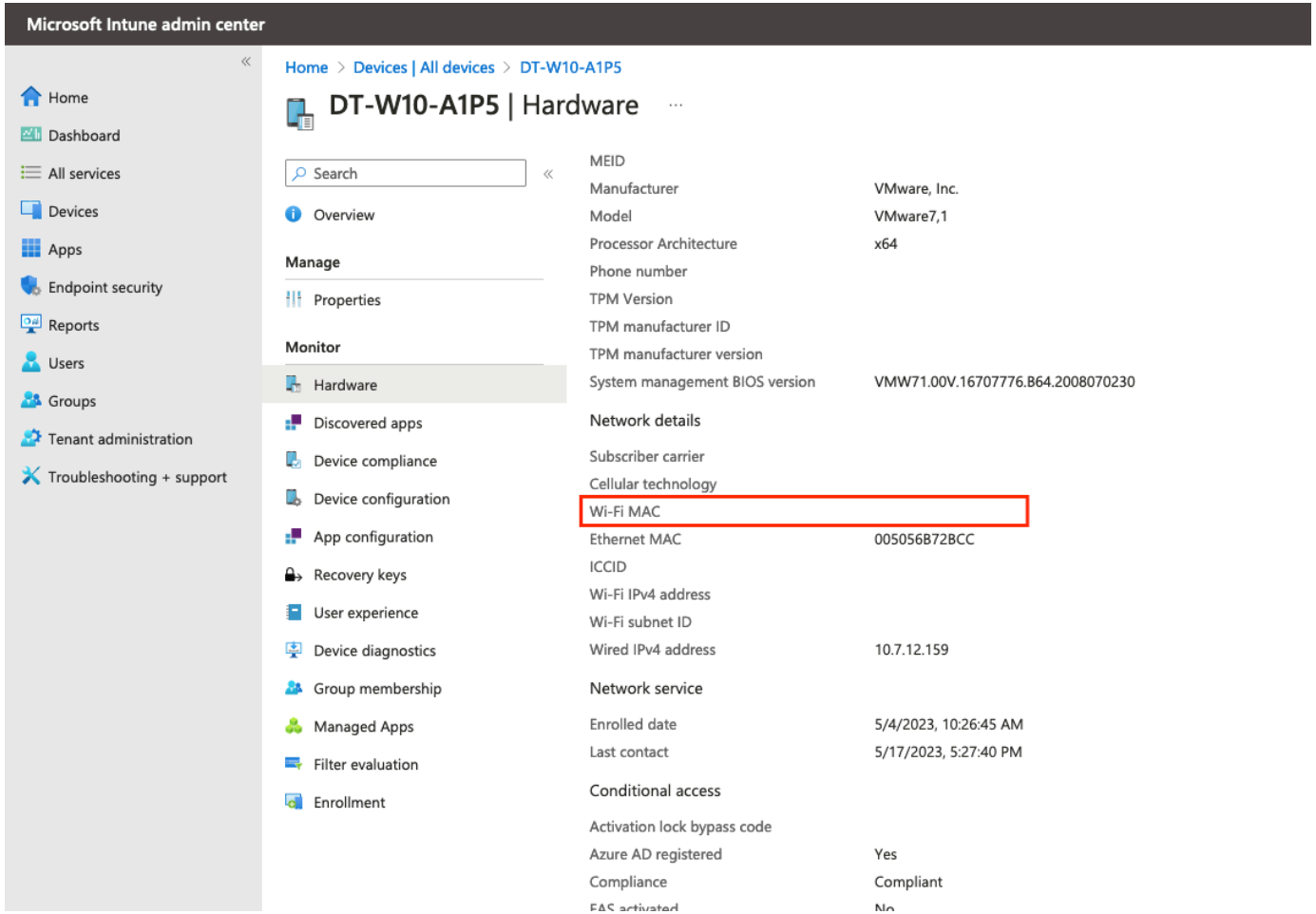


Authorization:Intune-EndpointDB => Endpoint DB query based on Intune Device Id

Intune Client Wired only

If an Intune client has no WiFi MAC (wired only):

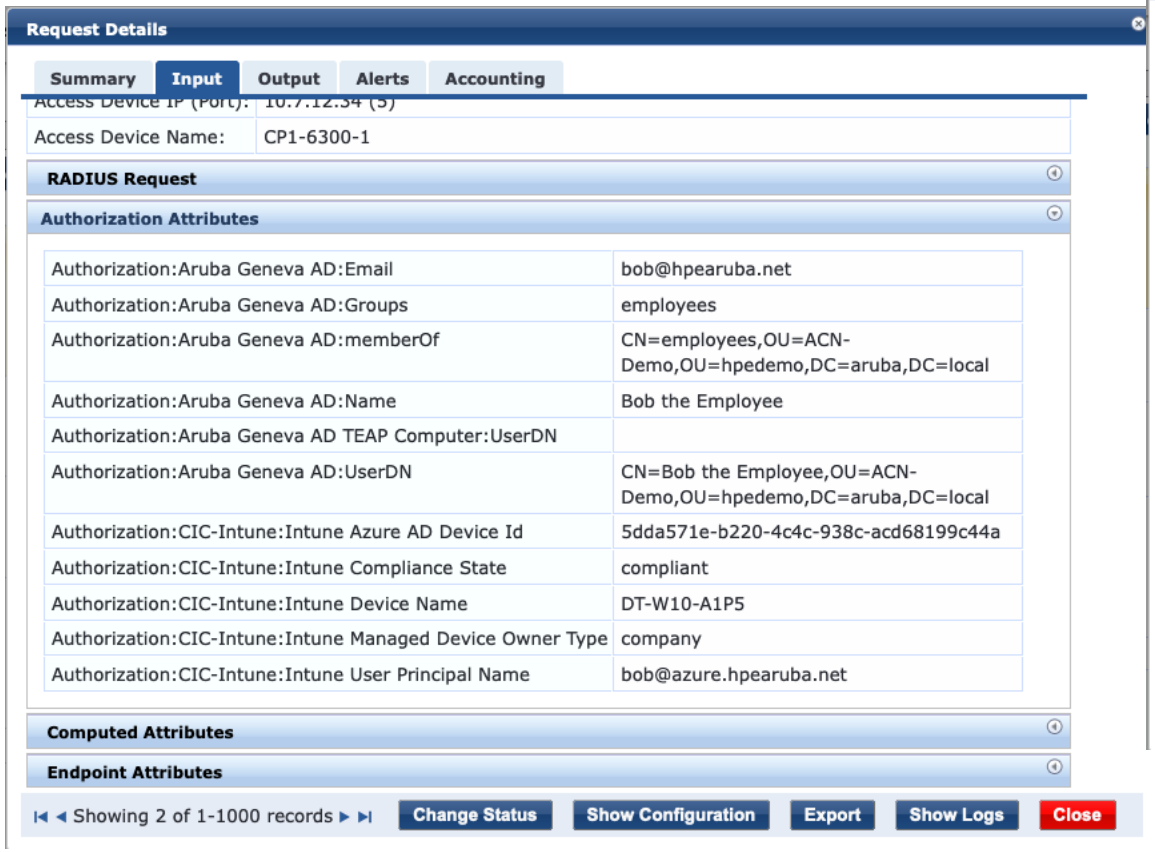
- you will need the Intune Device Id (TLS/Certificate)
- only real-time lookup is supported (HTTP)
- not synced to Endpoint Repository

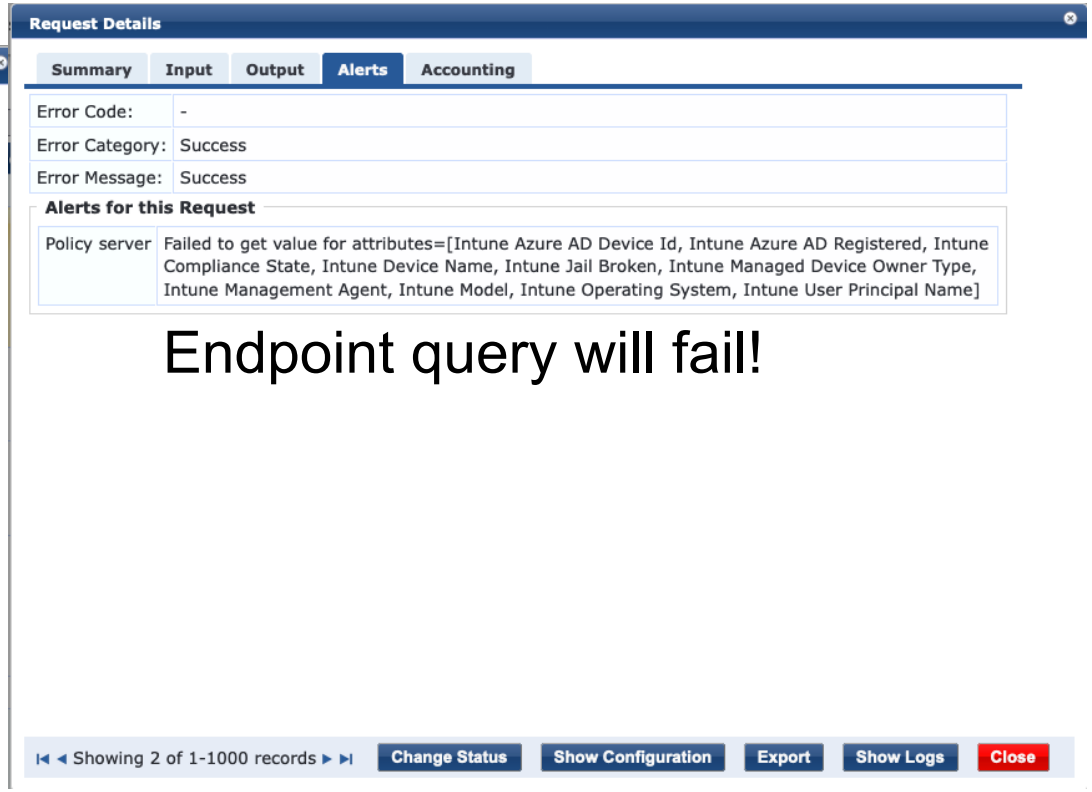


Intune Client Wired only

If an Intune client has no WiFi MAC (wired only):

- you will need the Intune Device Id (TLS/Certificate)
- only real-time lookup is supported (HTTP)
- not synced to Endpoint Repository





Endpoint query will fail!

Microsoft Intune SCEP Extension

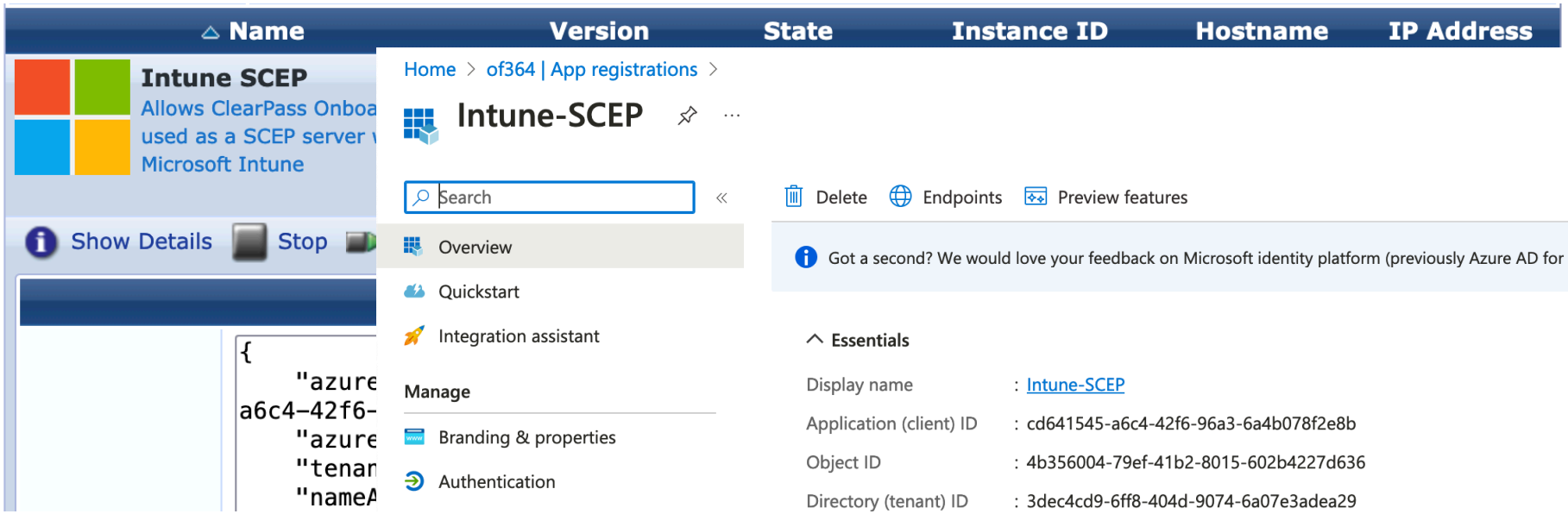
ClearPass Intune SCEP Extension

- Clients need to request/have Client Certificates
- Intune can let clients request a certificate through SCEP
- One option: Microsoft CA + NDES plugin
- Compatible third party products:
  - https://learn.microsoft.com/en-us/mem/intune/protect/certificate-authority-add-scep-overview#third-party-certification-authority-partners
    - Cogito Group
    - DigiCert
    - EJBCA
    - Entrust
    - EverTrust
    - GlobalSign
    - HID Global
    - IDnomic
    - KeyTalk
    - Keytos
    - Nexus Certificate Manager
    - SCEPman
    - Sectigo
    - SecureW2
    - Venafi
  - …and ClearPass Onboard

ClearPass Intune SCEP Extension

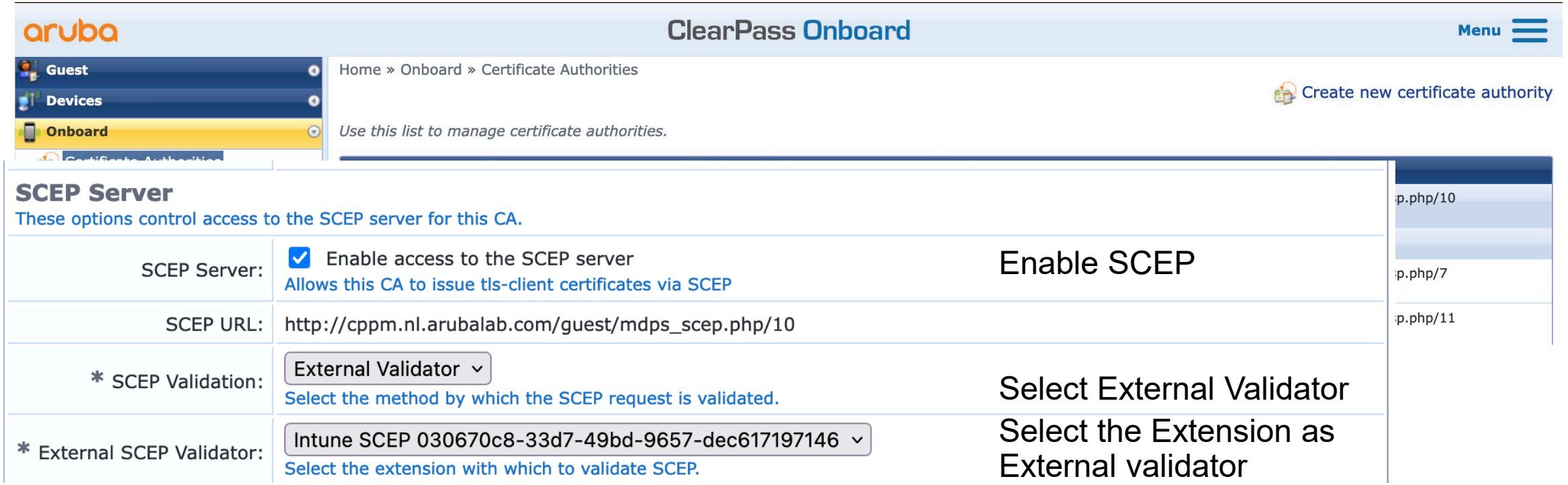
- Benefit: Built-in to ClearPass
- Benefit: No need to setup, configure, maintain another PKI
- Most applicable if no other PKI is present, no need for PKI, or if customer does not want to issue client certificates from the existing CA
- Yes, Onboard license needed (per user)

ClearPass Intune SCEP Extension (Entra ID Application Registration)

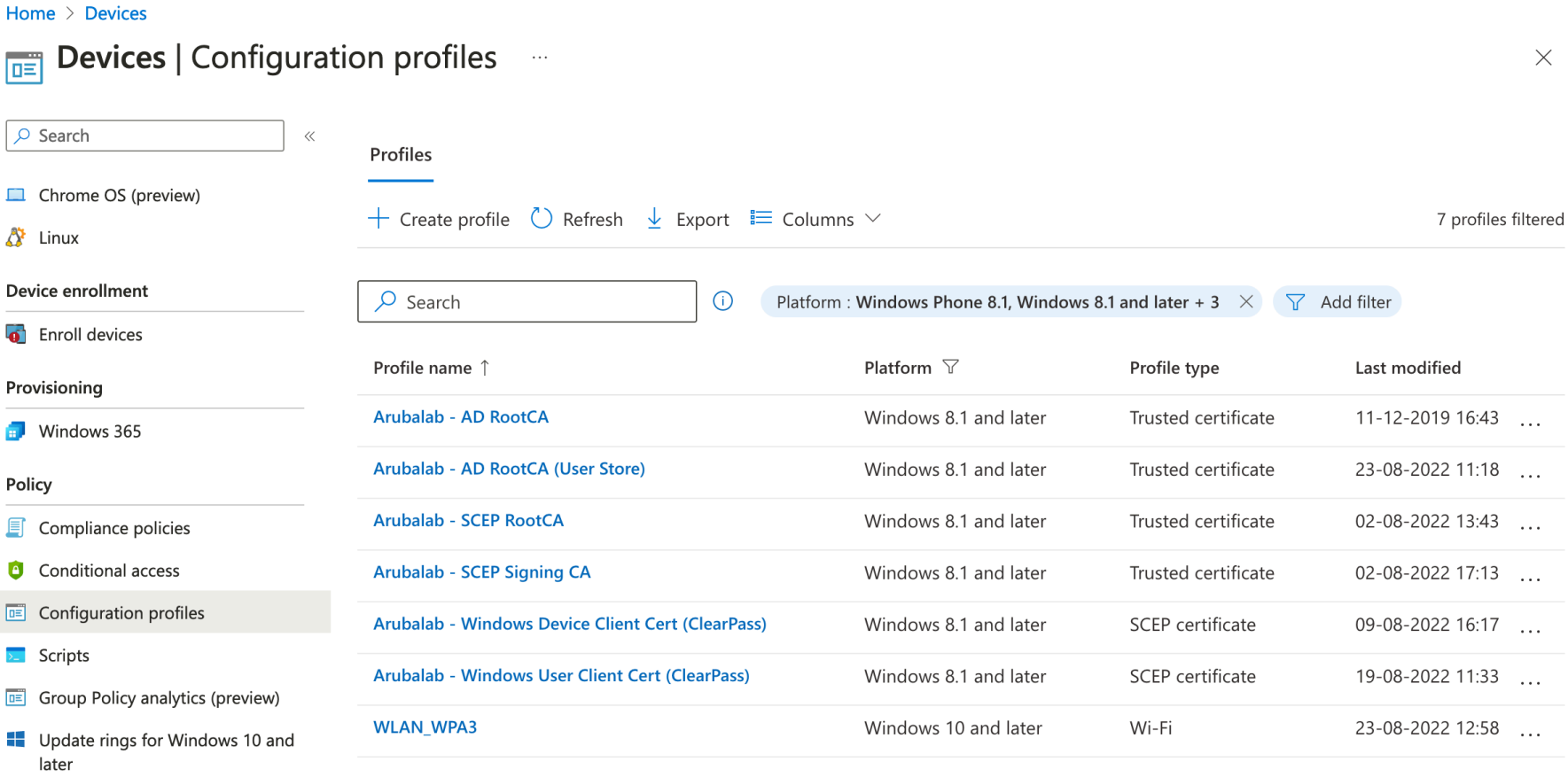


API / Permissions name	Type	Description	Admin consent requ...	Status
Intune (5)				
get_data_warehouse	Delegated	Get data warehouse information from Microsoft Intune	No	Granted for of364
get_device_compliance	Application	Get device state and compliance information from Micros...	Yes	Granted for of364
scep_challenge_provider	Application	SCEP challenge validation	Yes	Granted for of364
update_device_attributes	Application	Send device attributes to Microsoft Intune	Yes	Granted for of364
update_device_health	Application	Send device threat information to Microsoft Intune	Yes	Granted for of364
Microsoft Graph (5)				
Application.Read.All	Delegated	Read applications	Yes	Granted for of364
Application.Read.All	Application	Read all applications	Yes	Granted for of364
Directory.Read.All	Delegated	Read directory data	Yes	Granted for of364
Directory.ReadWrite.All	Delegated	Read and write directory data	Yes	Granted for of364
User.Read	Delegated	Sign in and read user profile	No	Granted for of364

ClearPass Enable ClearPass Onboard CA for SCEP

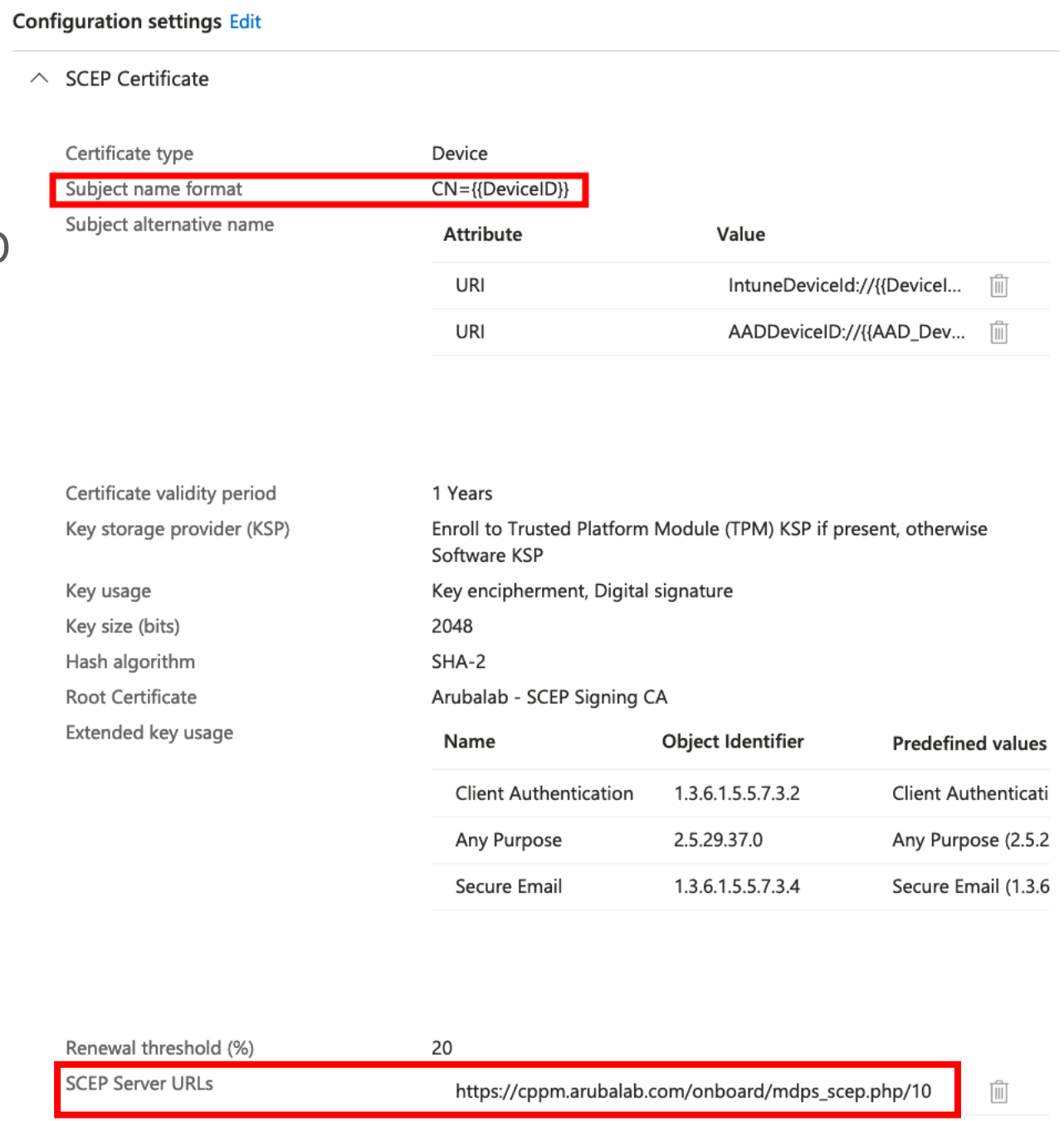


Intune SCEP profiles

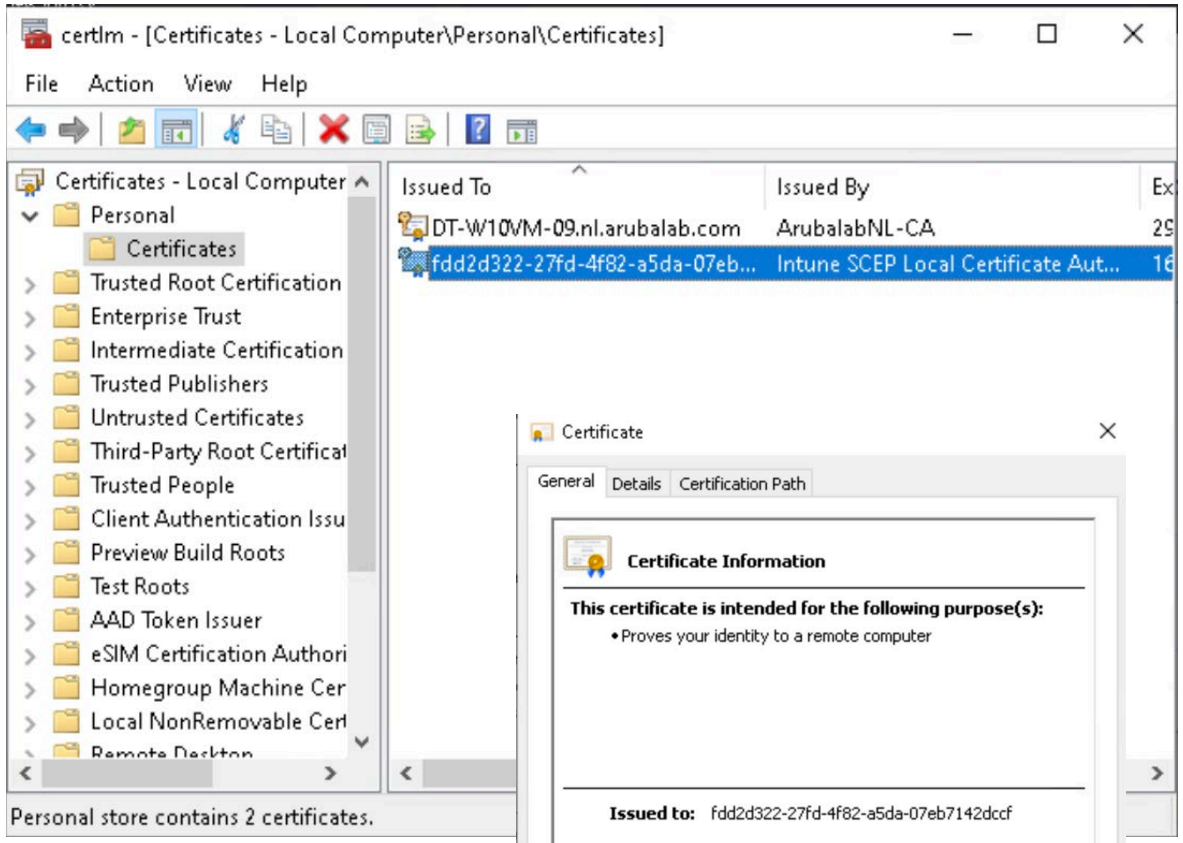


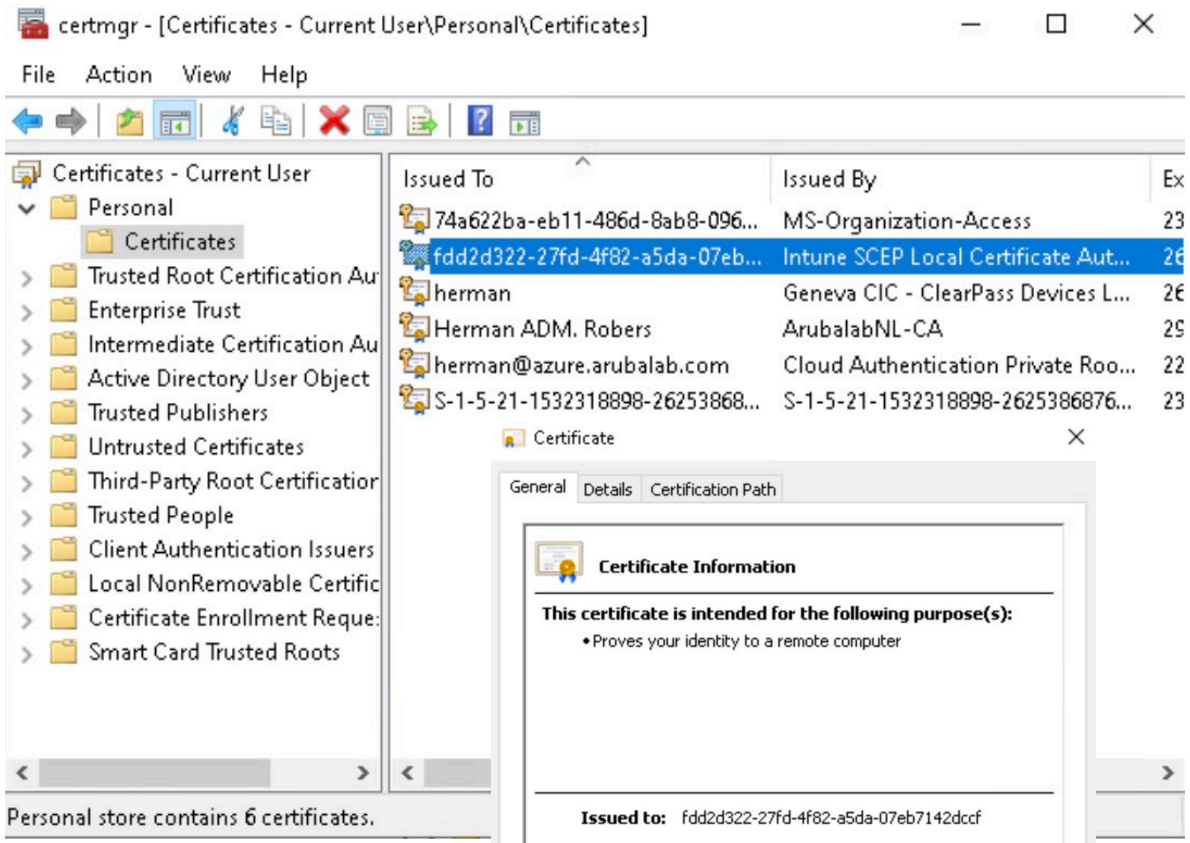
SCEP Configuration Profile

- Important! Change Subject name format to CN={{DeviceID}} to put the Intune Device ID as the Certificate Common Name and lookup the Intune attributes based on the Intune Device ID
- SCEP Server URL: ClearPass Onboard or other server URL



Client Enrolled





Meanwhile in the Extension logs….

Name	Version	State	Instance ID	Hostname	IP Address
Intune SCEP Allows ClearPass Onboard to be used as a SCEP server with Microsoft Intune	1.1.0	Running	030670c8-33d7-49bd-9657-dec617197146	b908f58f3d53	172.20.123.4

Show Details | Stop | Restart | Delete | Reinstall | Show Logs | Configuration | Note

```
    "tenantId": "3dec4cd9-6ff8-404d-9074-6a07e3adea29",
    "threadCount": 10,
    "nameAndVersion": "azurearubalabv001",
    "azureApplicationId": "cd641545-a6c4-42f6-96a3-6a4b078f2e8b",
    "restartPolicy": "always"
}
[2023-03-06T14:53:47.10 CET] [INFO] Intune SCEP - Starting web server
[2023-04-17T13:43:17.38 CEST] [INFO] Intune SCEP - Validated transaction 415f4f91256167f11e53f99b72020e4a0cbfff56
```

Intune XML WiFi & Wired Configuration

Intune XML WiFi configuration - Steps

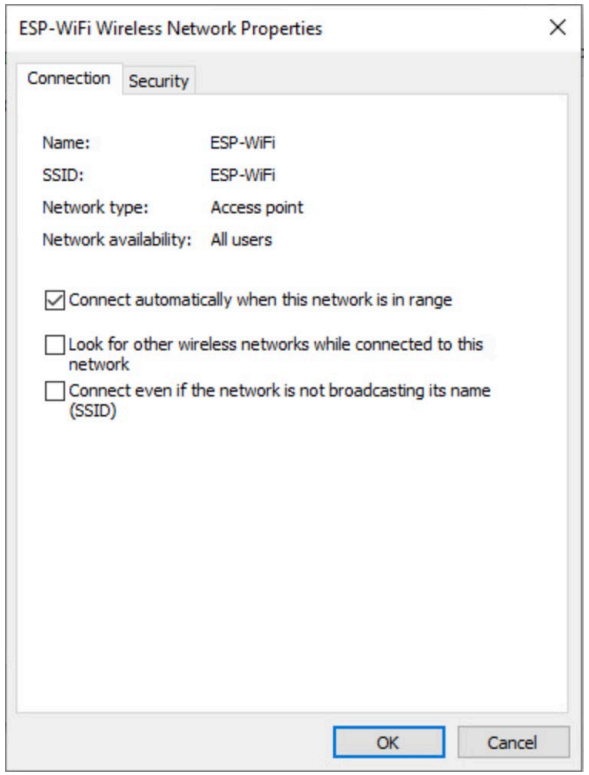
- For advanced configuration, like certificate selection or TEAP, use XML WiFi Export/Import
- https://learn.microsoft.com/en-us/mem/intune/configuration/wi-fi-settings-import-windows-8-1
  - Manually configure the SSID/Network on a Windows client
  - Export XML of the settings:

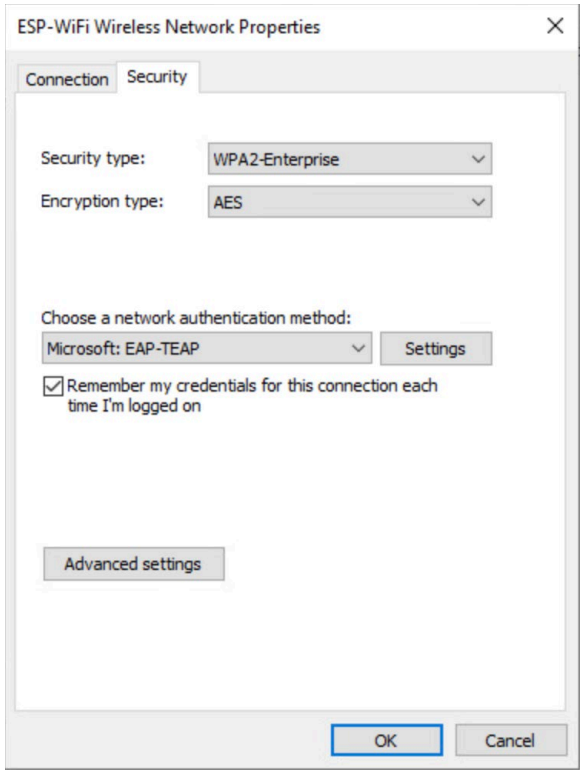
```
netsh wlan show profiles
netsh wlan export profile name="ContosoWiFi" folder=c:\Wifi
```

  - Create Intune Configuration Profile Windows 8.1 – Wi-Fi import

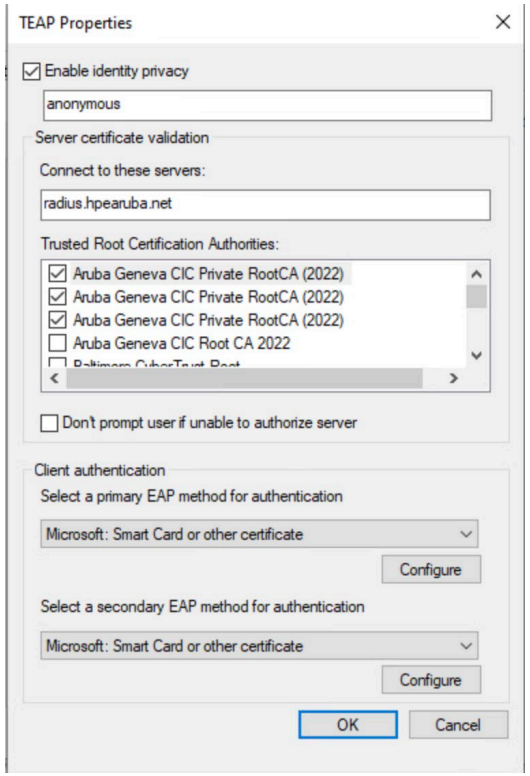
Intune XML WiFi configuration – Configure & test one client

– Manually configure one client

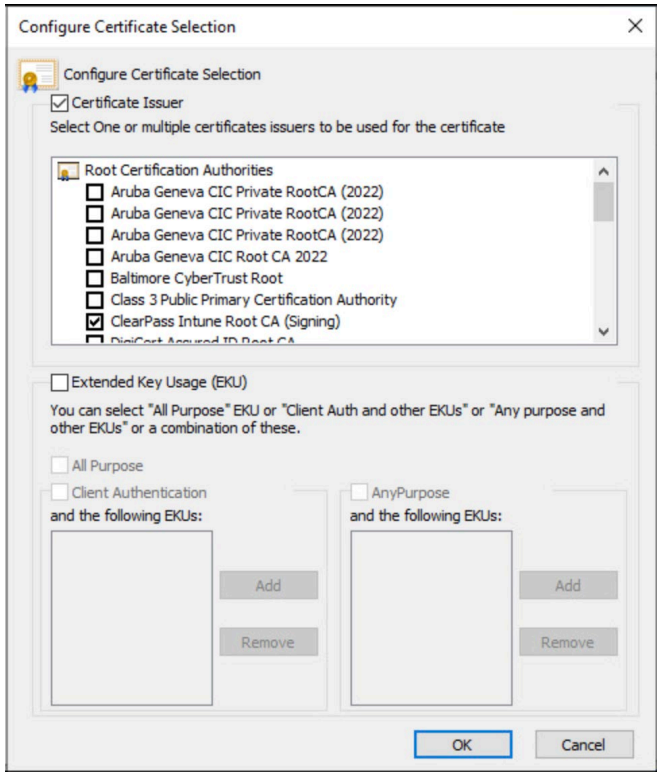




Configure TEAP method



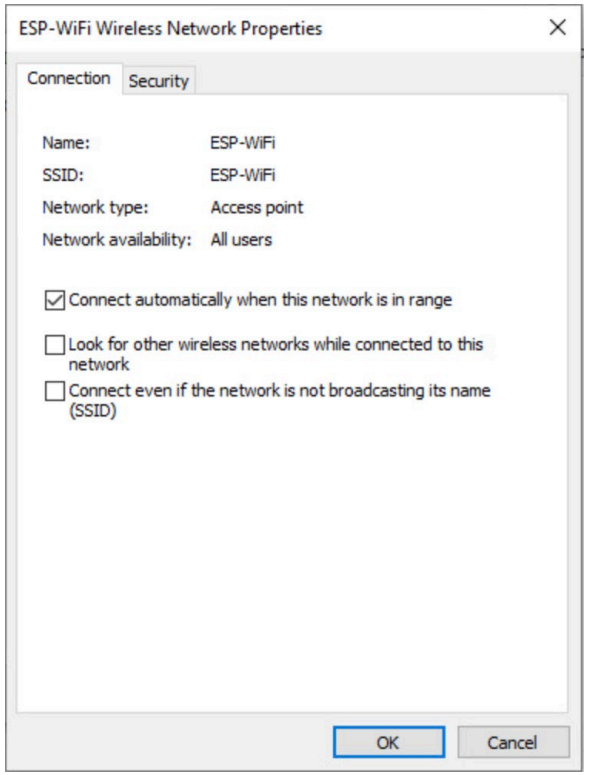
Configure Server trust and Method-1 & 2

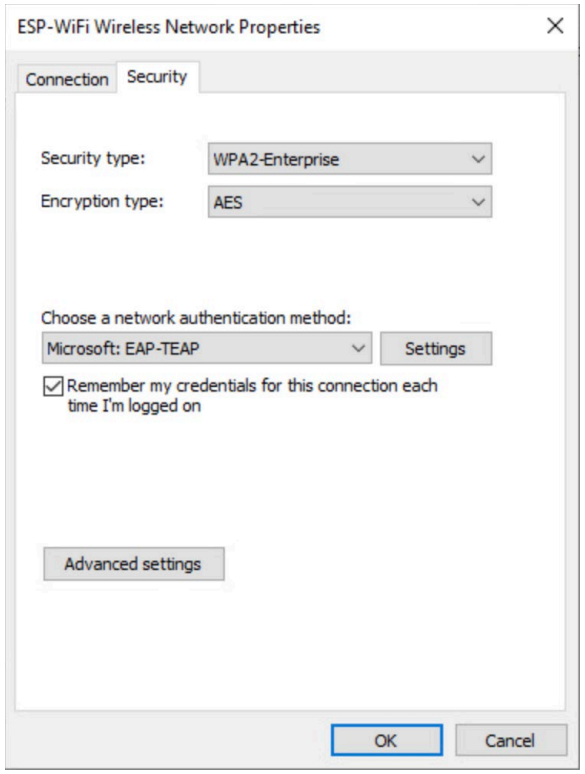


With multiple client certs select the Certificate issuer

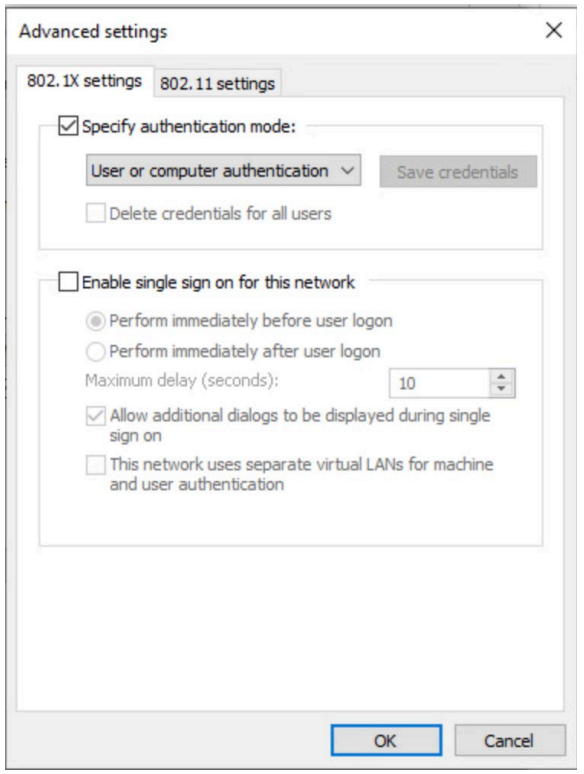
Intune XML WiFi configuration – Configure & test one client

– Manually configure one client





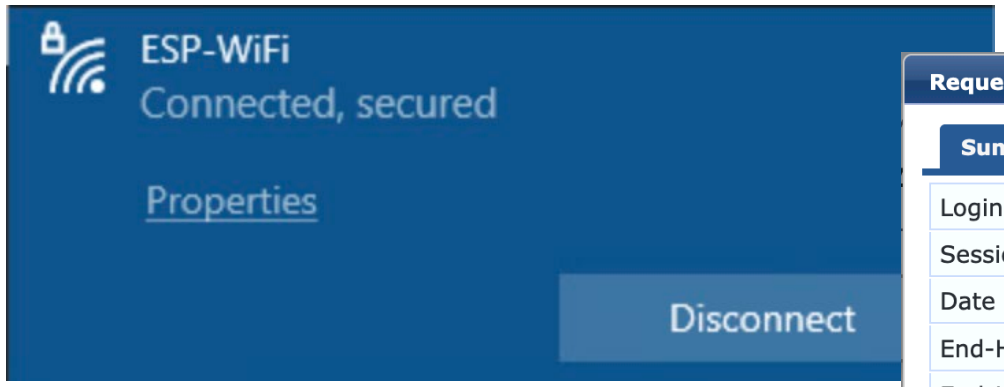
Under Advanced settings…



Specify User or Computer authentication

Intune XML WiFi configuration – validate test client connected

– Create Configuration Profile in Intune (Wi-Fi Windows 8.1 and later)



Request Details

Summary | **Input** | **Output** | **Accounting**

Login Status:	ACCEPT
Session Identifier:	R00005f68-10-64b802cb
Date and Time:	Jul 19, 2023 17:35:46 CEST
End-Host Identifier:	C8-3A-35-A4-0A-A1 Open in Central Open in AirWave
End-Host Profile:	Computer / Windows / Windows 10
End-Host Status:	Known
Username:	bob@azure.hpearuba.net
Access Device IP (Port):	172.16.200.252
Access Device Name:	172.16.200.108
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	ESP-dot1x-wireless
Authentication Method:	TEAP (EAP-TLS ,EAP-TLS)
Authentication Source:	AD:10.12.1.11
Authorization Source:	Aruba Geneva AD, Aruba Geneva AD TEAP Computer, CIC-AzureAD, CIC-Intune, Intune-EndpointDB
Roles:	Intune Compliant, Intune User, [Machine Authenticated], [User Authenticated]

Intune XML WiFi configuration – Extract configuration XML from client

– Export XML of the settings:

```
netsh wlan show profiles
netsh wlan export profile name="ContosoWiFi" folder=c:\Wifi
```

```
C:\Users\bob>netsh wlan show profiles

Profiles on interface Wi-Fi:

Group policy profiles (read only)
---------------------------------
    <None>

User profiles
-------------
    All User Profile     : ESP-WiFi
    All User Profile     : DEMO-ARUBA
    All User Profile     : HPE-CIC
```

```
C:\Users\bob>netsh wlan export profile name="ESP-WiFi" folder=.

Interface profile "ESP-WiFi" is saved in file ".\Wi-Fi-ESP-WiFi.xml" successfully.
```

Intune XML WiFi configuration – Optionally: modify the network name

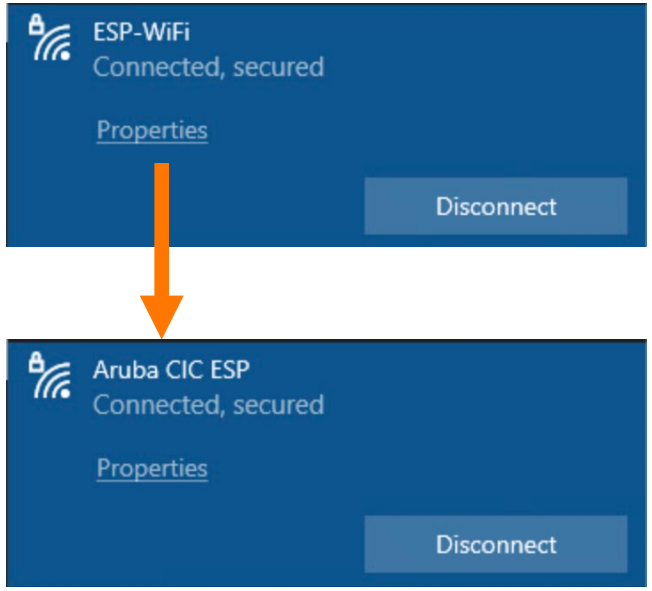
– Review, optionally change name of the profile

```
<?xml version="1.0"?>
<WLANProfile xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">
        <name>ESP-WiFi</name>
        <SSIDConfig>
                <SSID>
                        <hex>4553502D57694669</hex>
                        <name>ESP-WiFi</name>
                </SSID>a
                <nonBroadcast>false</nonBroadcast>
        </SSIDConfig>
        <connectionType>ESS</connectionType>
        <connectionMode>auto</connectionMode>
        <autoSwitch>false</autoSwitch>
        <MSM>
                <security>
                        <authEncryption>
                                <authentication>WPA2</authentication>
                                <encryption>AES</encryption>
                                <useOneX>true</useOneX>a
                        </authEncryption>
                        <OneX xmlns="http://www.microsoft.com/networking/OneX/v1">
                                <cacheUserData>true</cacheUserData>
                                <authMode>machineOrUser</authMode>
                                <EAPConfig><…… CONFIG XML IS HERE ….>
……
</WLANProfile>
```

Intune XML WiFi configuration – Optionally: modify the network name

– Review, optionally change name of the profile

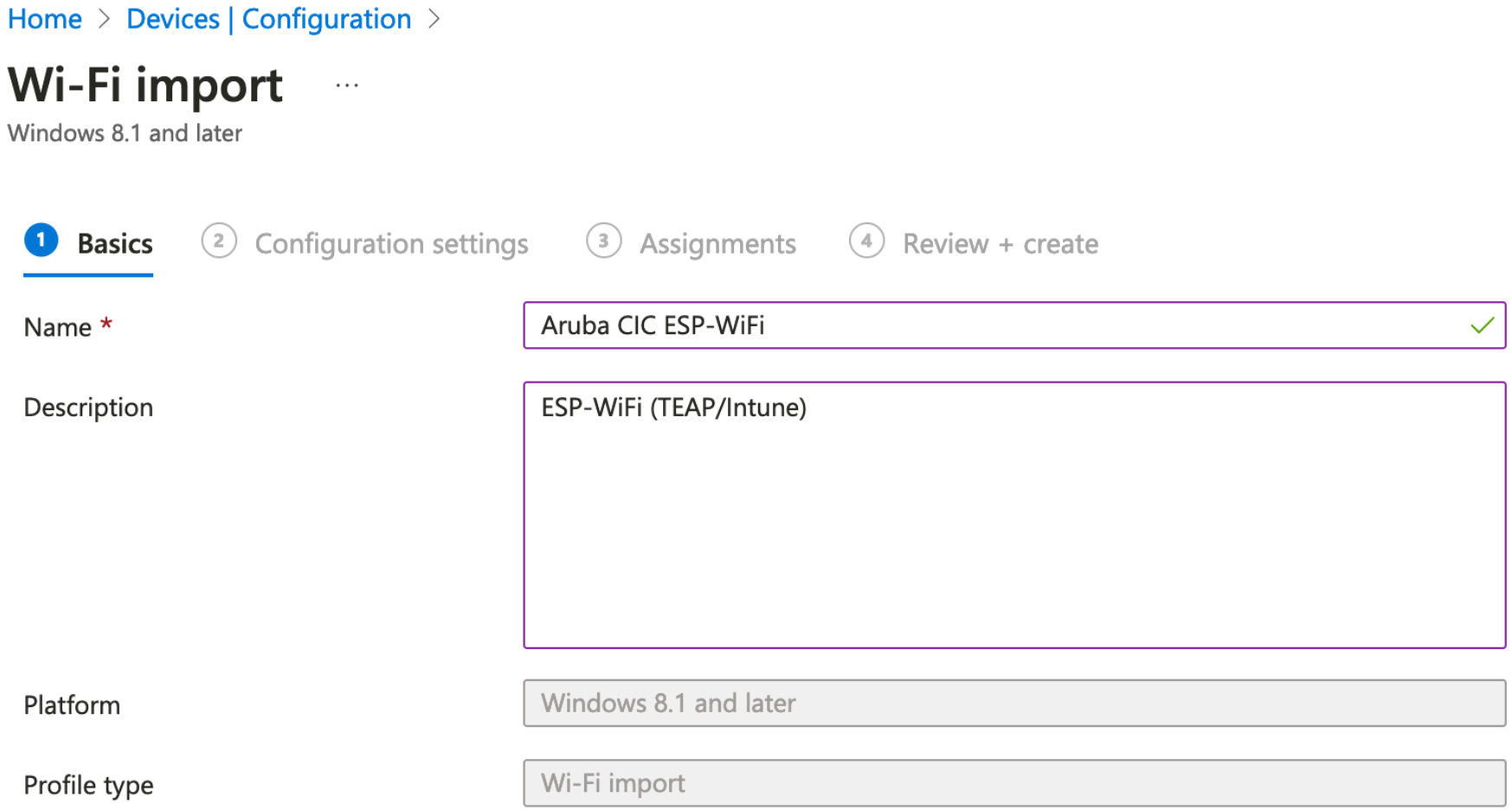
– Profile name is shown in the WiFi network lists instead of the actual SSID




```
<?xml version="1.0"?>
<WLANProfile xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">
        <name>Aruba CIC ESP</name>
        <SSIDConfig>
                <SSID>
                        <hex>4553502D57694669</hex>
                        <name>ESP-WiFi</name>
                </SSID>a
                <nonBroadcast>false</nonBroadcast>
        </SSIDConfig>
        <connectionType>ESS</connectionType>
        <connectionMode>auto</connectionMode>
        <autoSwitch>false</autoSwitch>
        <MSM>
                <security>
                        <authEncryption>
                                <authentication>WPA2</authentication>
                                <encryption>AES</encryption>
                                <useOneX>true</useOneX>a
                        </authEncryption>
                        <OneX xmlns="http://www.microsoft.com/networking/OneX/v1">
                                <cacheUserData>true</cacheUserData>
                                <authMode>machineOrUser</authMode>
                                <EAPConfig><…… CONFIG XML IS HERE ….>
……
</WLANProfile>
```

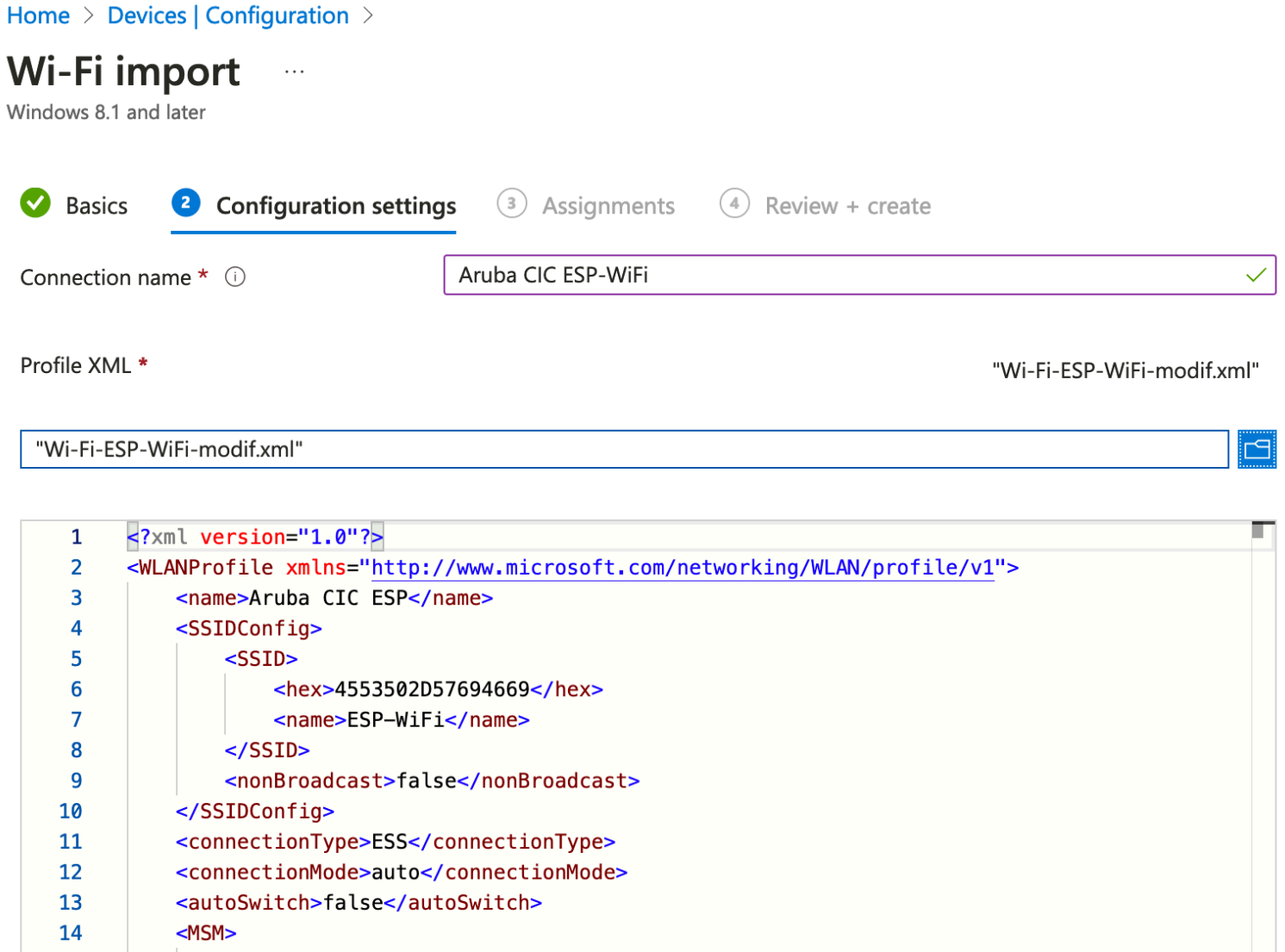
Intune XML WiFi configuration - Create Wi-Fi import profile

– Create Configuration Profile in Intune (Wi-Fi Windows 8.1 and later)



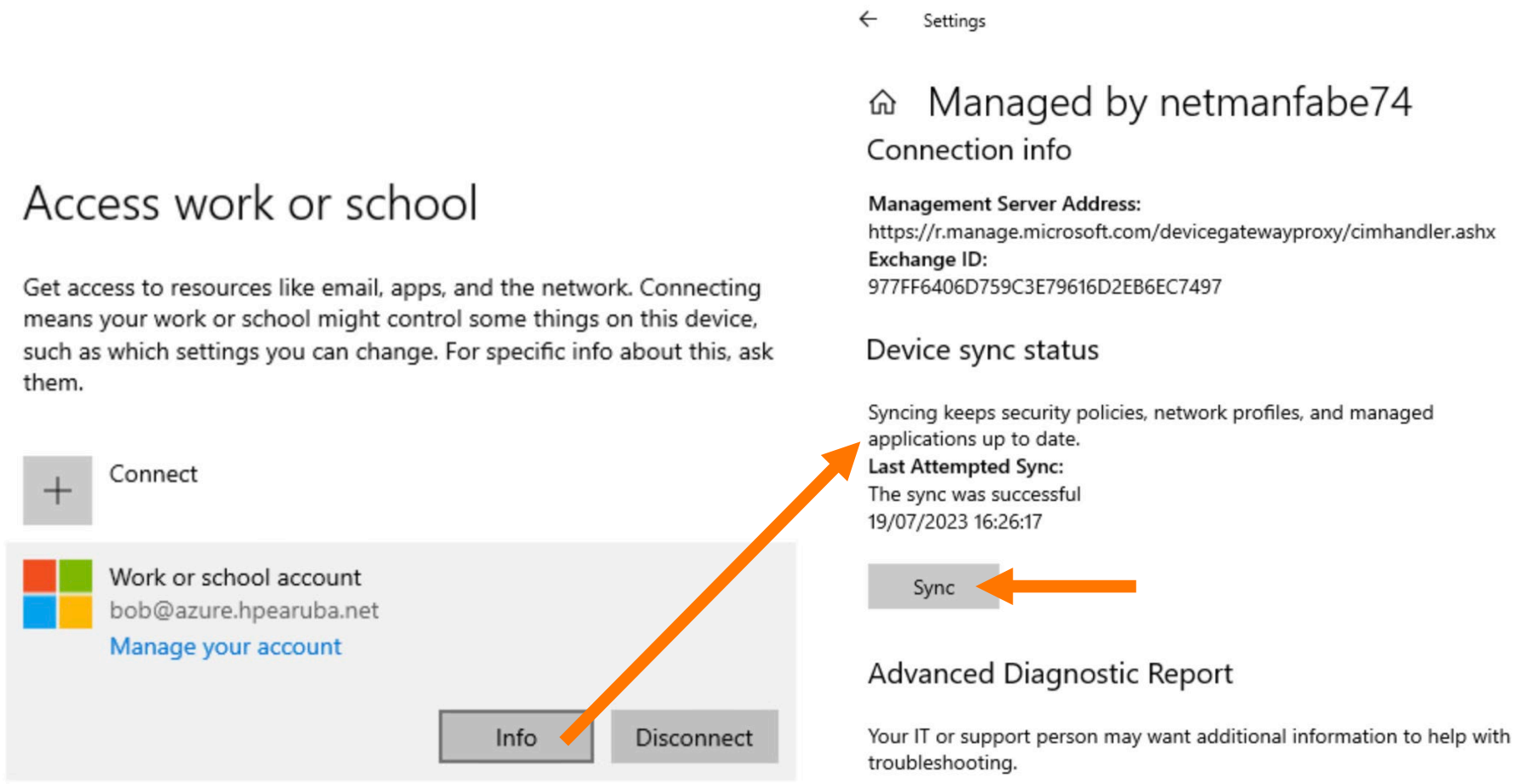
Intune XML WiFi configuration – Create Wi-Fi import profile

– Create Configuration Profile in Intune (Wi-Fi Windows 8.1 and later)



Intune XML WiFi configuration – force update client

– Trigger update/sync from the client



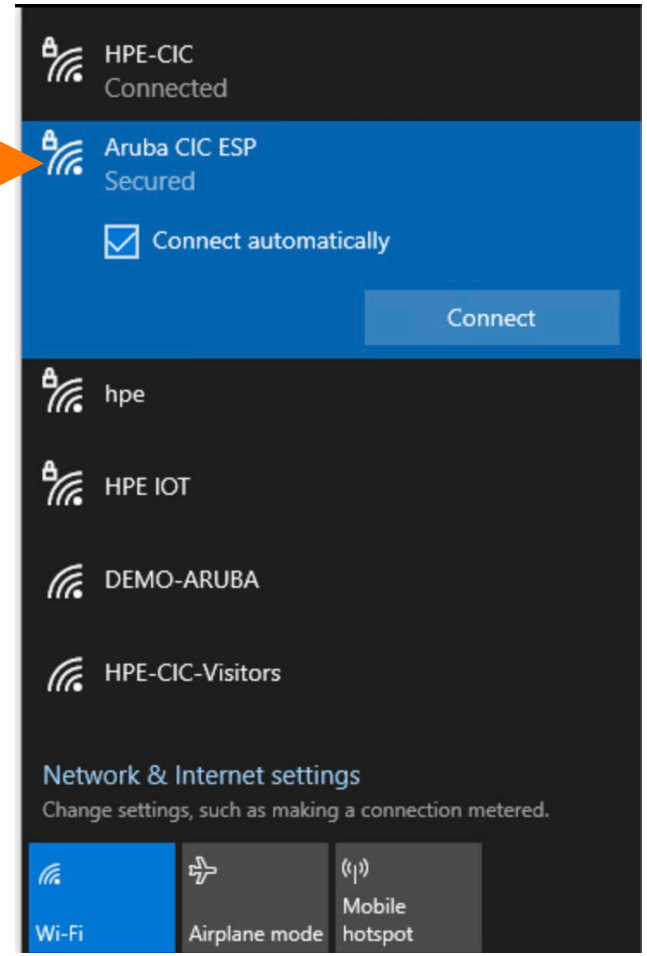
Intune XML WiFi configuration – validate: profile deployed

– After push by Intune see that the profile has been pushed with the name entered in the XML

– Note: the actual SSID is still ESP-WiFi, but Windows displays the ‘frienly’ name.

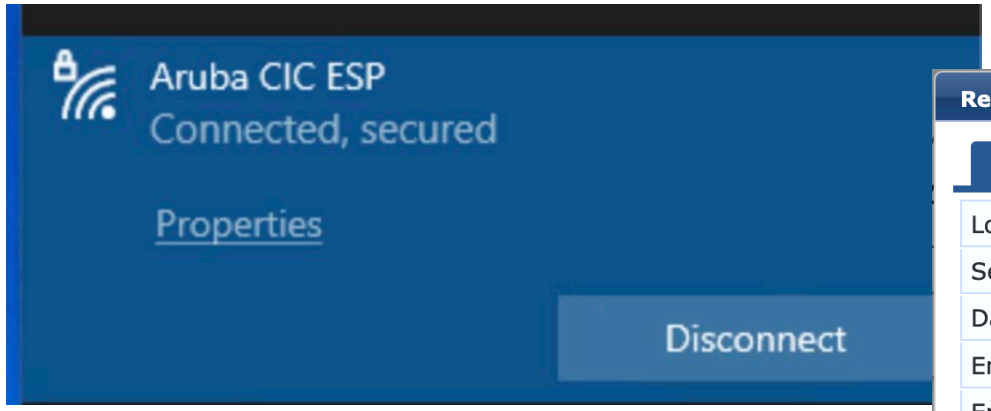
```
C:\Users\bob>netsh wlan show profiles

Profiles on interface Wi-Fi:

Group policy profiles (read only)
---------------------------------
    <None>

User profiles
-------------
    All User Profile     : Aruba CIC ESP
    All User Profile     : HPE-CIC
```

```xml
<?xml version="1.0"?>
<WLANProfile xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">
    <name>Aruba CIC ESP</name>
    <SSIDConfig>
        <SSID>
            <hex>4553502D57694669</hex>
            <name>ESP-WiFi</name>
        </SSID>
```



Intune XML WiFi configuration – validate: connected

– Create Configuration Profile in Intune (Wi-Fi Windows 8.1 and later)



Request Details

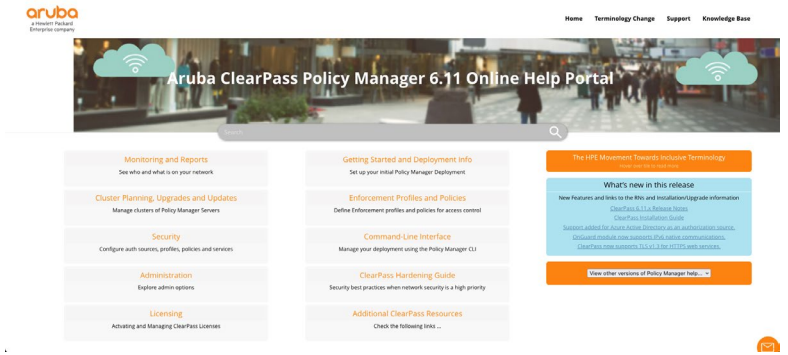
Summary | **Input** | **Output** | **Accounting**

Login Status:	ACCEPT		
Session Identifier:	R00005f68-10-64b802cb		
Date and Time:	Jul 19, 2023 17:35:46 CEST		
End-Host Identifier:	C8-3A-35-A4-0A-A1	Open in Central	Open in AirWave
End-Host Profile:	Computer / Windows / Windows 10		
End-Host Status:	Known		
Username:	bob@azure.hpearuba.net		
Access Device IP (Port):	172.16.200.252		
Access Device Name:	172.16.200.108		
System Posture Status:	UNKNOWN (100)		
Policies Used -			
Service:	ESP-dot1x-wireless		
Authentication Method:	TEAP (EAP-TLS ,EAP-TLS)		
Authentication Source:	AD:10.12.1.11		
Authorization Source:	Aruba Geneva AD, Aruba Geneva AD TEAP Computer, CIC-AzureAD, CIC-Intune, Intune-EndpointDB		
Roles:	Intune Compliant, Intune User, [Machine Authenticated], [User Authenticated]		

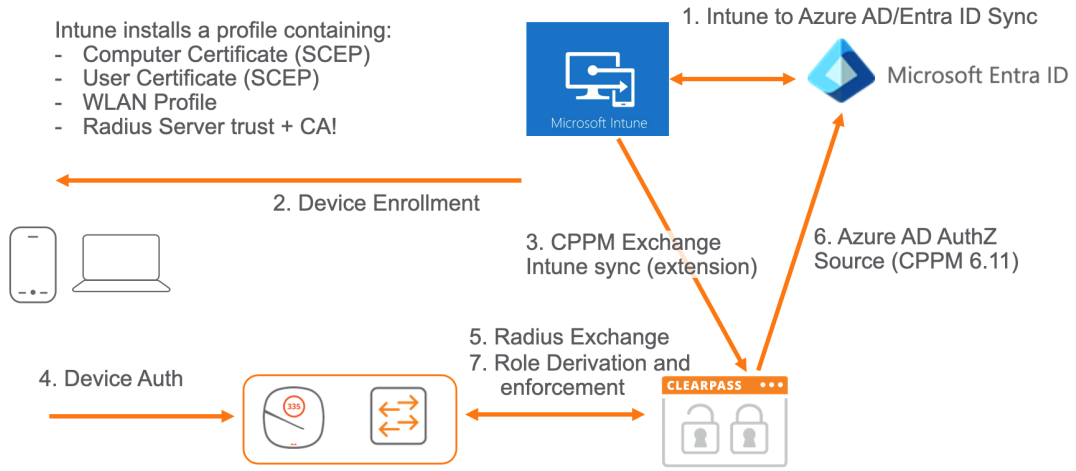
Further Reading…

Documentation Portal

- https://www.arubanetworks.com/techdocs/ClearPass/6.11/PolicyManager/Content/home.htm
- Cloud Deployments: Microsoft Azure Cloud Service
  https://www.arubanetworks.com/techdocs/ClearPass/6.10/Installation-Guide/Default.htm#InstallationGuide/Cloud-Azure/CD-AZ-introduction.htm
- Azure Authorization Source:
  https://www.arubanetworks.com/techdocs/ClearPass/6.11/PolicyManager/Content/CPPM_UserGuide/Auth/AuthSource_Azure.htm
- Intune SCEP Extension:
  https://www.arubanetworks.com/techdocs/ClearPass/TechNotes/Extensions-Intune-Onboard/Default.htm
- Intune Extension:
  https://support.hpe.com/hpesc/public/docDisplay?docId=a00112290en_us



Summary – What we discussed



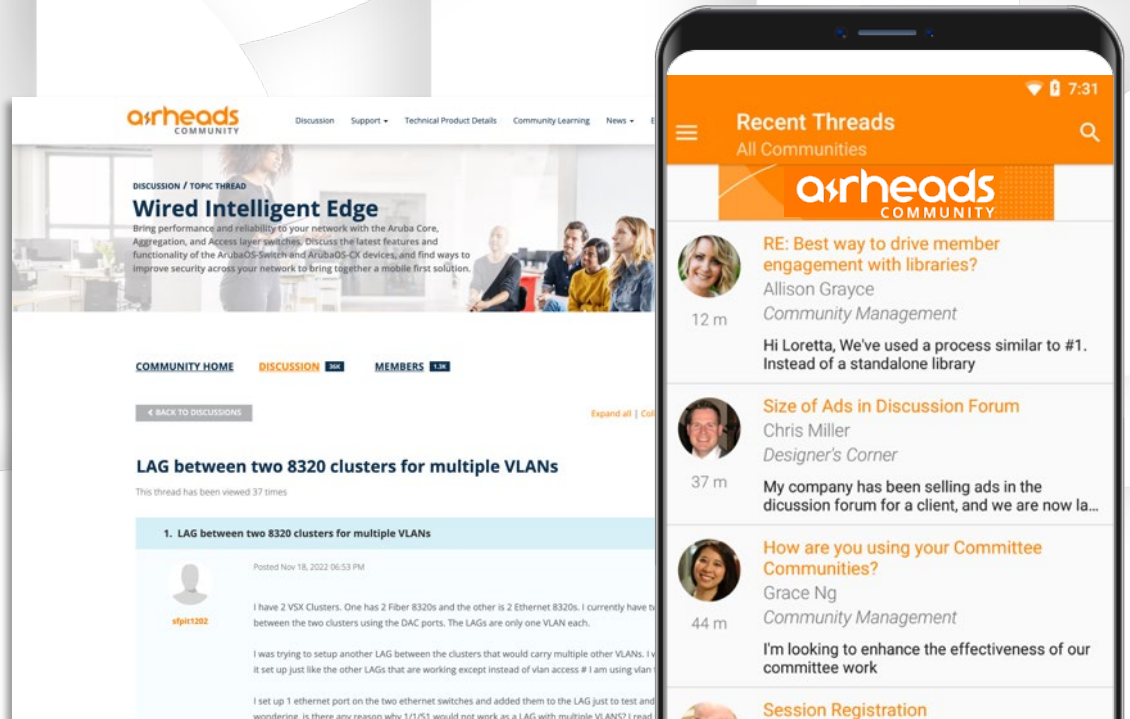
- Running ClearPass in the Cloud (Azure) is similar to on-premises

- Azure AD Authorization Source (ClearPass 6.11)
  - Entra ID
  - Authorization only
  - Get username during authentication
- Microsoft Intune Extension
  - Attributes synced to Endpoint Repository
  - HTTP Query to the Intune Extension
  - Query on Intune Device ID (not on Client MAC Address)
  - Implicitly means: TLS User Certificate authentication to get the Intune Device ID
- Intune SCEP Extension
  - Great when no PKI is available
  - Uses Onboard Certificate Authority and licenses

- Together with Entra ID and Intune ‘closed loop’ solution for managed devices

Thank You

Q&A



COMMUNITY

Join Today!

www.community.arubanetworks.com