

atmosphere'23

BELGIUM

ClearPass, Entra ID (Azure AD) and Intune

Herman Robers, Aruba CSE EMEA

October 2023



Agenda

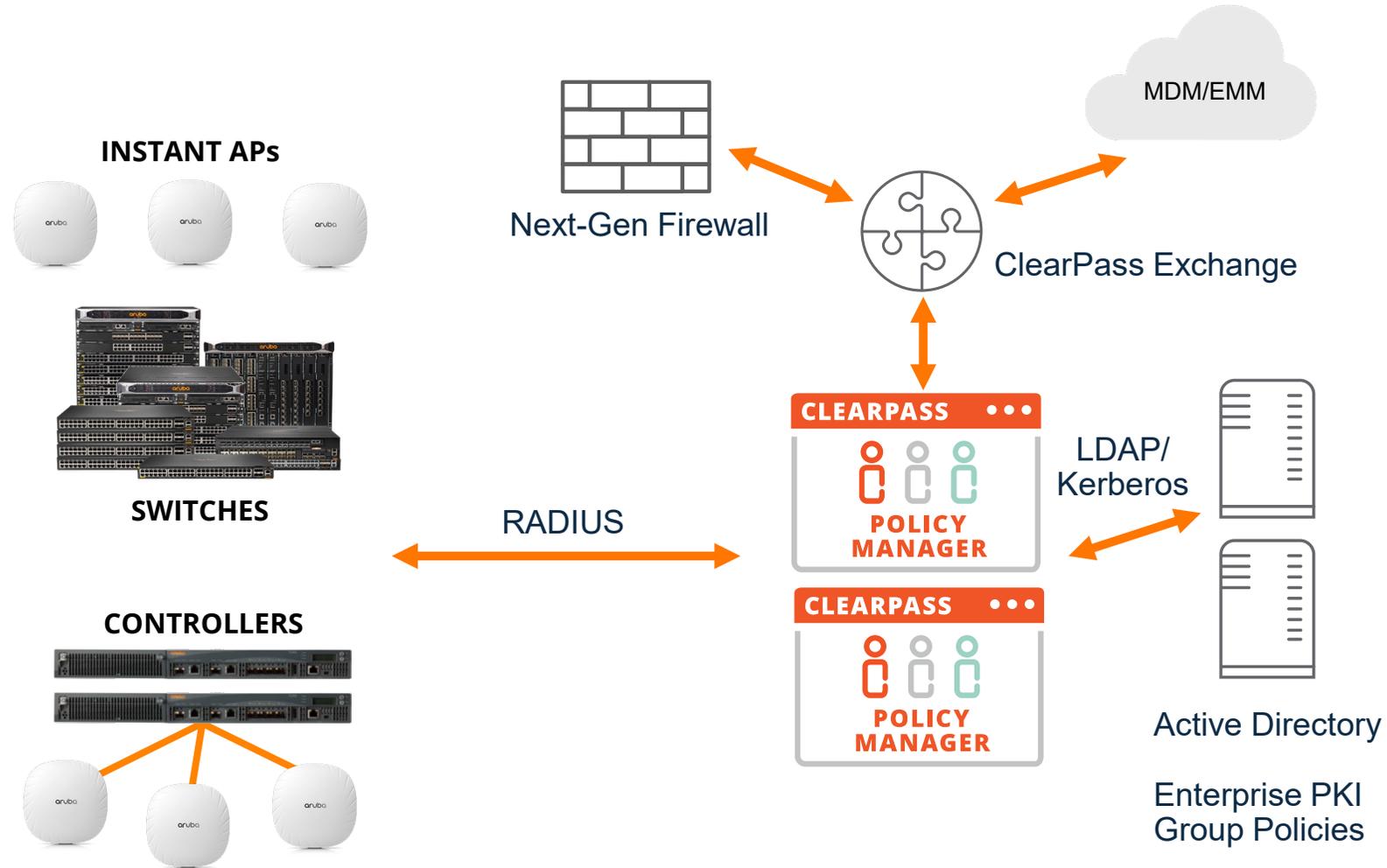
- ClearPass and the Cloud
- ClearPass in the Cloud
- ClearPass with the Cloud
- ClearPass and Entra ID (Azure AD)
- ClearPass and Intune Endpoint Manager
- Q&A



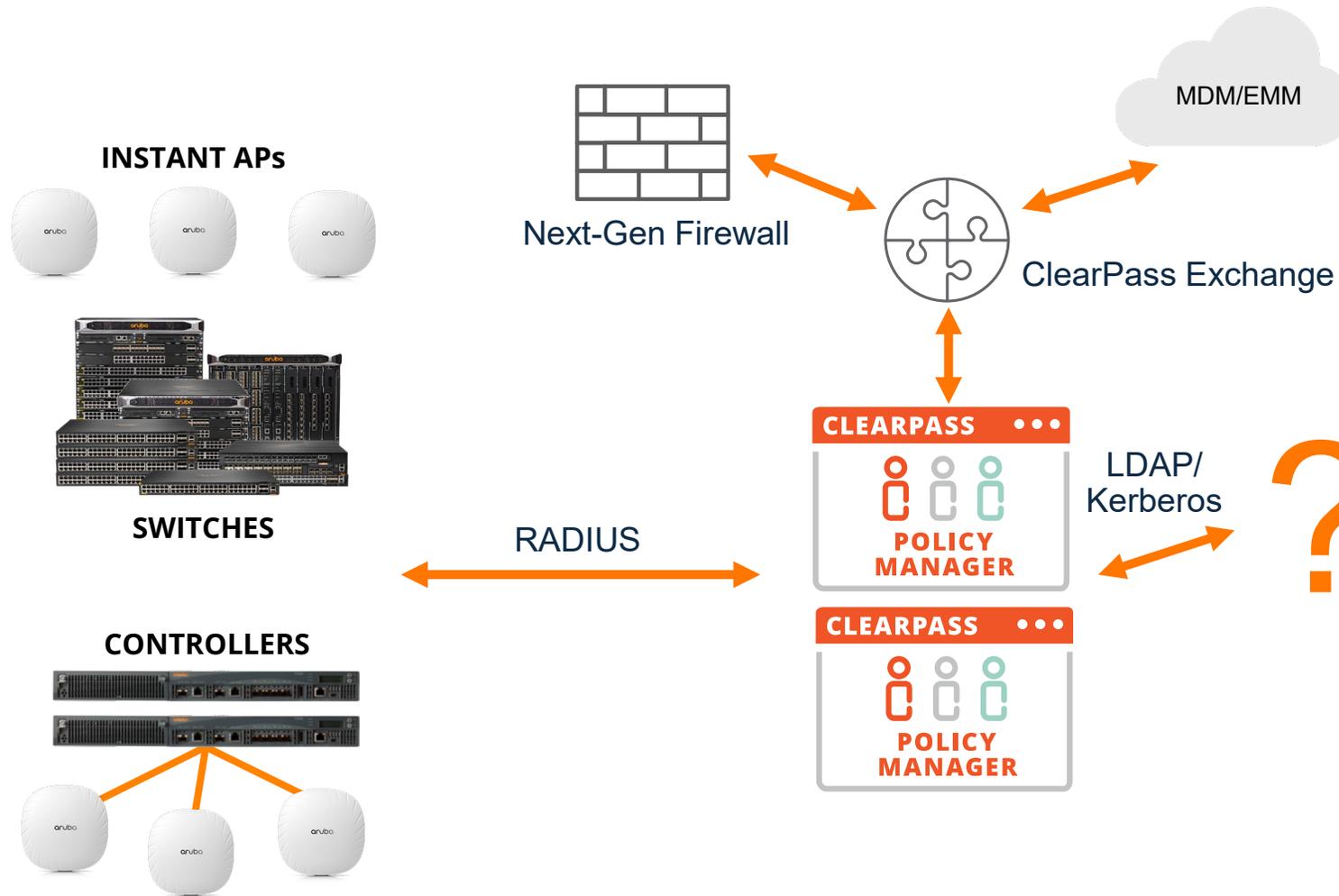
Authentication and the Cloud

When organizations go to the cloud

Traditional deployment (On-Premise)



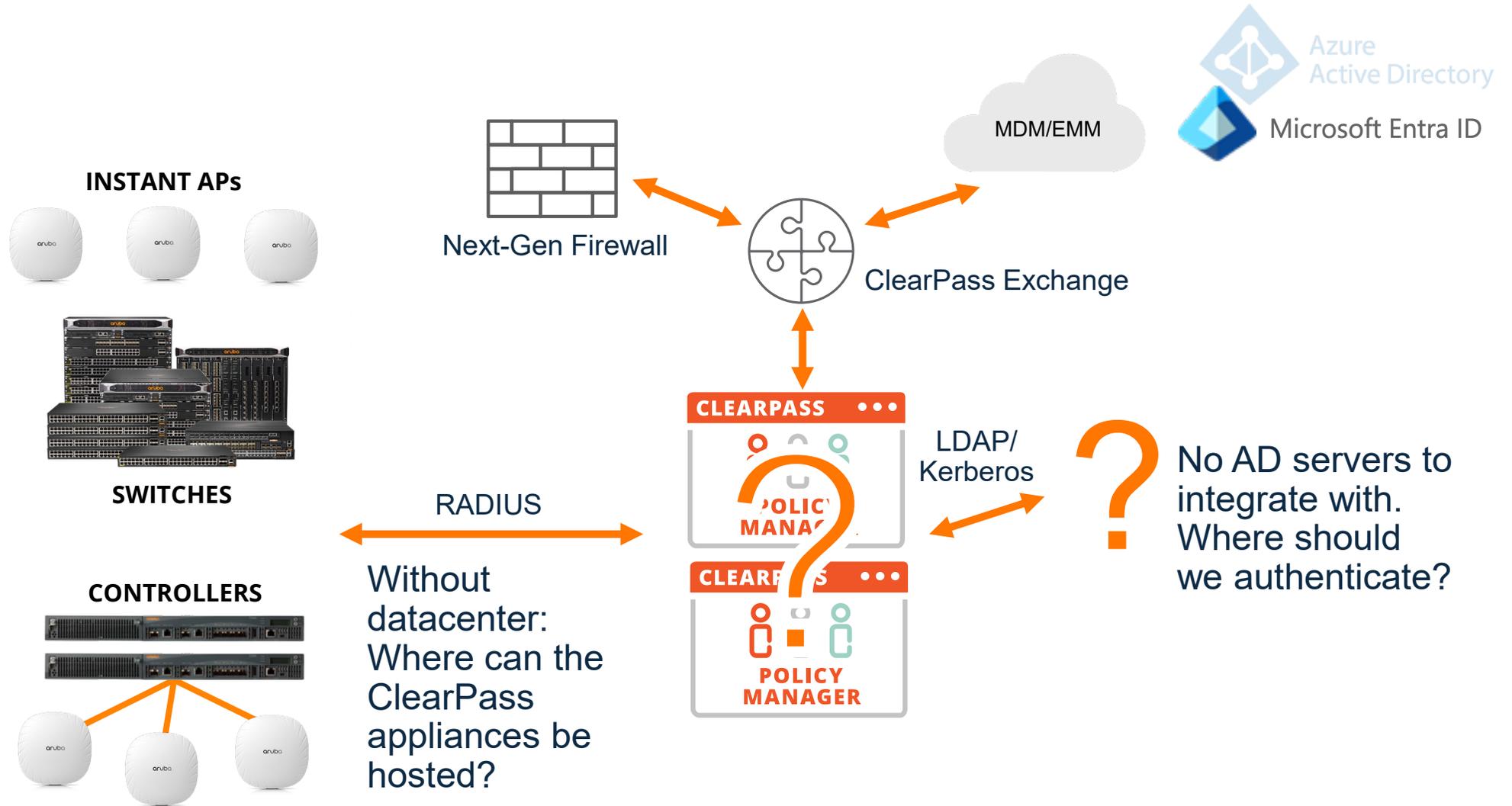
What when customer fully moves to Entra ID (Azure AD)?



? No AD servers to integrate with. Where should we authenticate?

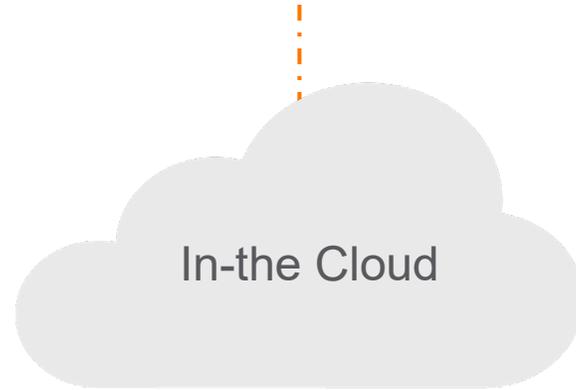


What when customer removes all datacenters and goes cloud only?

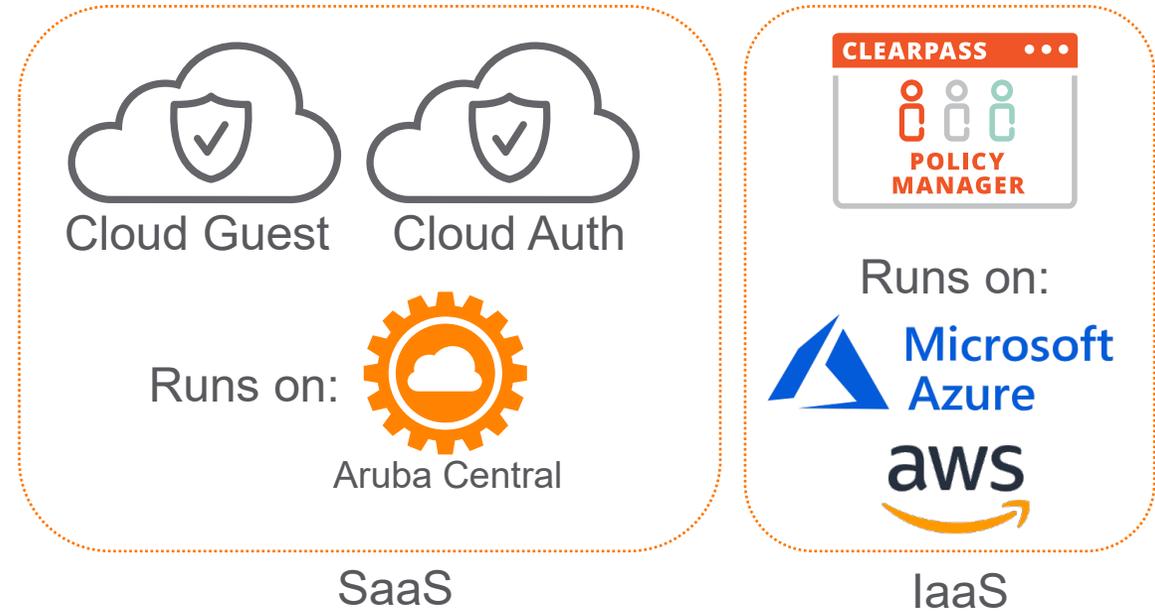


Authentication options in the cloud and on-premises

Identity Stores



Authentication Services



On-premises



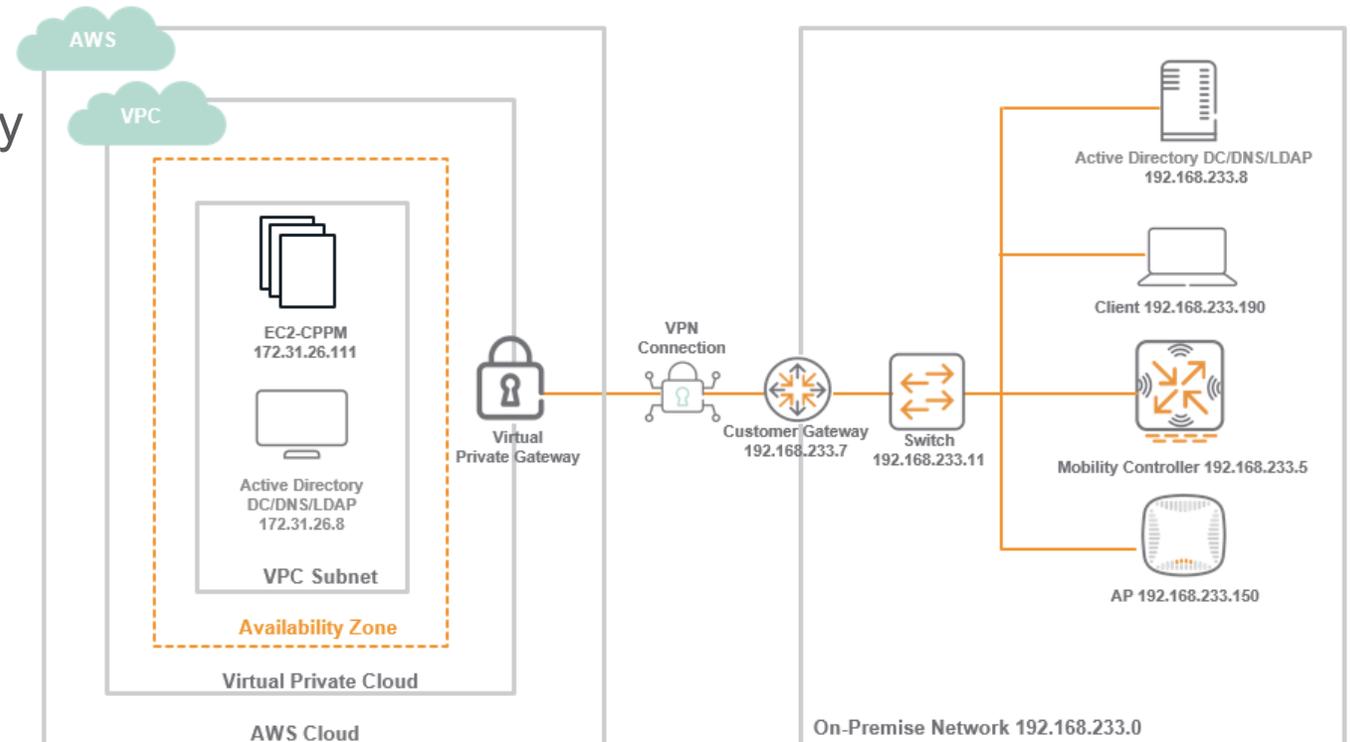
ClearPass *in* the Cloud

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

Create a virtual machine

Marketplace

Get Started

Service Providers

Management

Private Marketplace

Private Offer Management

My Marketplace

Favorites

Recently created

Private products

Categories

Networking (1)

Security (1)

Aruba ClearPass Policy Manager (CPPM) 6.11.1

Azure services only

Showing 1 to 1 of 1 results for 'Aruba ClearPass Policy Manager (



Aruba ClearPass Policy Manager (CPPM) 6.11.1
Aruba, a Hewlett Packard Enterp...
Virtual Machine
Aruba ClearPass Policy Manager (CPPM) 6.11
Bring your own license
Create 

Virtual machine name * ⓘ

CPPM-AZ-UK1 

Region * ⓘ

(Europe) UK South 

Availability options ⓘ

No infrastructure redundancy required 

Security type ⓘ

Standard 

Image * ⓘ

 Aruba ClearPass Policy Manager (CPPM) 6.11 - x64 Gen1 

[See all images](#) | [Configure VM generation](#)

VM architecture ⓘ

Arm64

x64

 Arm64 is not supported with the selected image.

Run with Azure Spot discount ⓘ

Size * ⓘ

Recommended by image publisher

Standard_D2s_v3 - 2 vcpus, 8 GiB memory (\$87.60/month)

Standard_D4s_v3 - 4 vcpus, 16 GiB memory (\$175.20/month)

Standard_D16s_v3 - 16 vcpus, 64 GiB memory (\$700.80/month)

 Storage Accounts



Premium Block Blob Storage, Hierarchical Namespa...  

Upfront: \$0.00

Monthly: \$196.17



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'



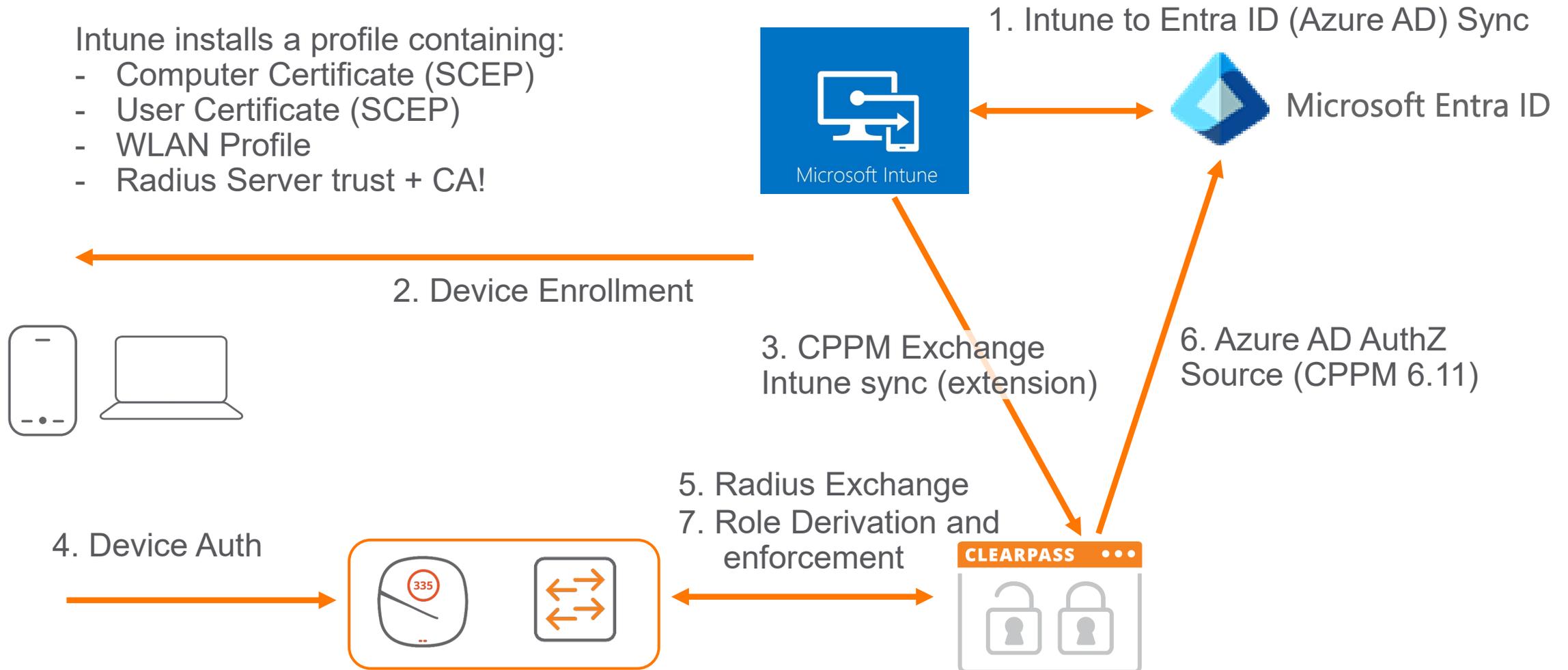
ClearPass with the Cloud

Options for ClearPass to run *with* the cloud

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

Intune installs a profile containing:

- Computer Certificate (SCEP)
- User Certificate (SCEP)
- WLAN Profile
- Radius Server trust + CA!



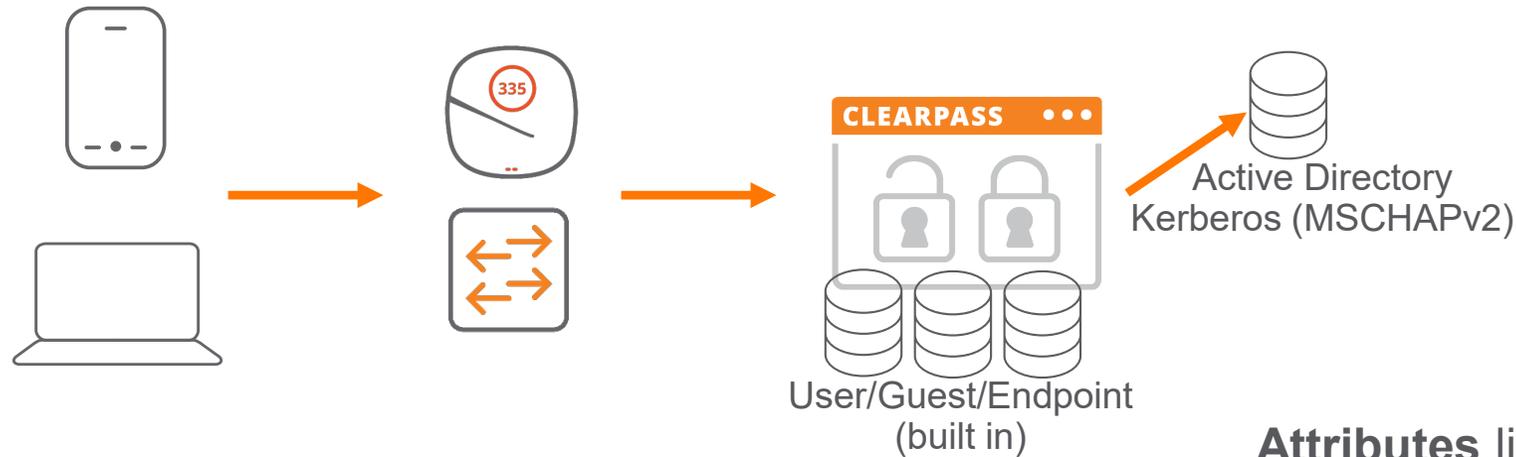
Authentication and Authorization: Authentication

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



Authentication sources:

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



Attributes like:

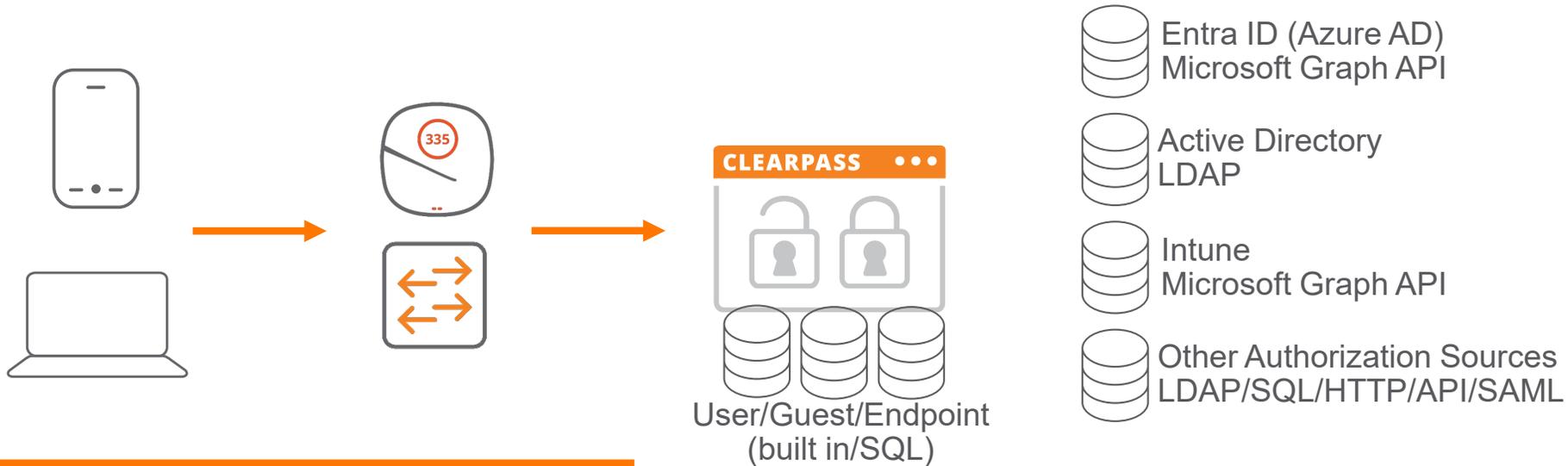
Authentication status (pass/fail)
Username
Client MAC
Certificate Attributes (Intune Device ID)
Computer or User

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



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



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



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

The screenshot shows the Microsoft Azure portal interface. At the top, there is a search bar and navigation links. Below that, the user profile for 'Bob The Employee' is displayed. The profile includes a search bar, navigation tabs (Overview, Monitoring, Properties), and a 'Basic info' section. The 'User principal name' is highlighted with a red box and is 'bob@azure.hpearuba.net'. Other details include Object ID, Created date time, User type, and Identities.

Basic info	
User principal name	bob@azure.hpearuba.net
Object ID	da348331-d488-4f9b-9d45-90d1664eceb5
Created date time	Feb 13, 2023, 11:28 AM
User type	Member
Identities	netmanfab74.onmicrosoft.com

Azure AD AuthZ Source (CPPM 6.11)



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: 262768b0-2fb8-4439-8347-8add85982f0 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



Microsoft Entra ID

Request Details

Summary | **Input** | Output | Accounting

Username:	herman@azure.arubalab.com
End-Host Identifier:	B8-8A-60-C6-0F-7A (Computer / Windows / Windows 10.0.19044.2728)
Access Device IP (Port):	192.168.36.8
Access Device Name:	192.168.36.8

RADIUS Request

Authorization Attributes

Authorization:Arubalab-AzureAD:AccountEnabled	true
Authorization:Arubalab-AzureAD:Department	Arubalab
Authorization:Arubalab-AzureAD:Email	herman@azure.arubalab.com
Authorization:Arubalab-AzureAD:Groups	Central Admin, IT Admins, Intune Users, of364
Authorization:Intune-EndpointDB:Intune Azure AD Device Id	74a622ba-eb11-486d-8ab8-0965bfb636b3
Authorization:Intune-EndpointDB:Intune Azure AD Registered	true
Authorization:Intune-EndpointDB:Intune Compliance State	compliant
Authorization:Intune-EndpointDB:Intune Device Name	DT-W10VM-09
Authorization:Intune-EndpointDB:Intune Jail Broken	Unknown
Authorization:Intune-EndpointDB:Intune Managed Device Owner Type	personal
Authorization:Intune-EndpointDB:Intune Management Agent	mdm

Showing 1 of 1-1 records | Change Status | Show Configuration | Export | Show Logs | Close



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



Microsoft Entra ID

- 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

Edit Authentication Method

General

Name: EAP TLS - No AuthZ - Intune SCEP

Description: EAP-TLS with CN or SAN comparison

Type: EAP-TLS

Method Details

Session Resumption: Enable

Session Timeout: hours

Authorization Required: Enable

Certificate Comparison: Compare CN or SAN

Verify Certificate using OCSP: Optional

Override OCSP URL from Client: Enable

OCSP URL: http://127.0.0.1/onboard/mdps_oc

Do not compare

Compare Distinguished Name (DN)

Compare Common Name (CN)

Compare Subject Alternate Subject Name (SAN)

Compare CN or SAN

Compare Binary

Copy Save Cancel



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



Microsoft Entra ID

- 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

Configuration » Services » Edit - WLAN-WPA3 (Intune TEAP)

Services - WLAN-WPA3 (Intune TEAP)

Summary Service **Authentication** Authorization Roles Enforcement

Authentication Methods: TEAP-Intune

Authentication Sources: ~~Arubalab-AzureAD [Azure]~~

Strip Username Rules: Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

Service Certificate: --Select to Add--

Services - WLAN-WPA3 (Intune TEAP)

Summary Service Authentication **Authorization** Roles Enforcement

Authorization Details:

Authorization sources from which role mapping attributes are fetched (for each...)

Authentication Source

- [Local User Repository] [Local SQL DB]

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

- [Endpoints Repository] [Local SQL DB] [Remove] [View Details]
- [Time Source] [Local SQL DB] [Remove] [View Details]
- Arubalab-AzureAD [Azure]** [Remove] [View Details] [Modify]

--Select to Add--

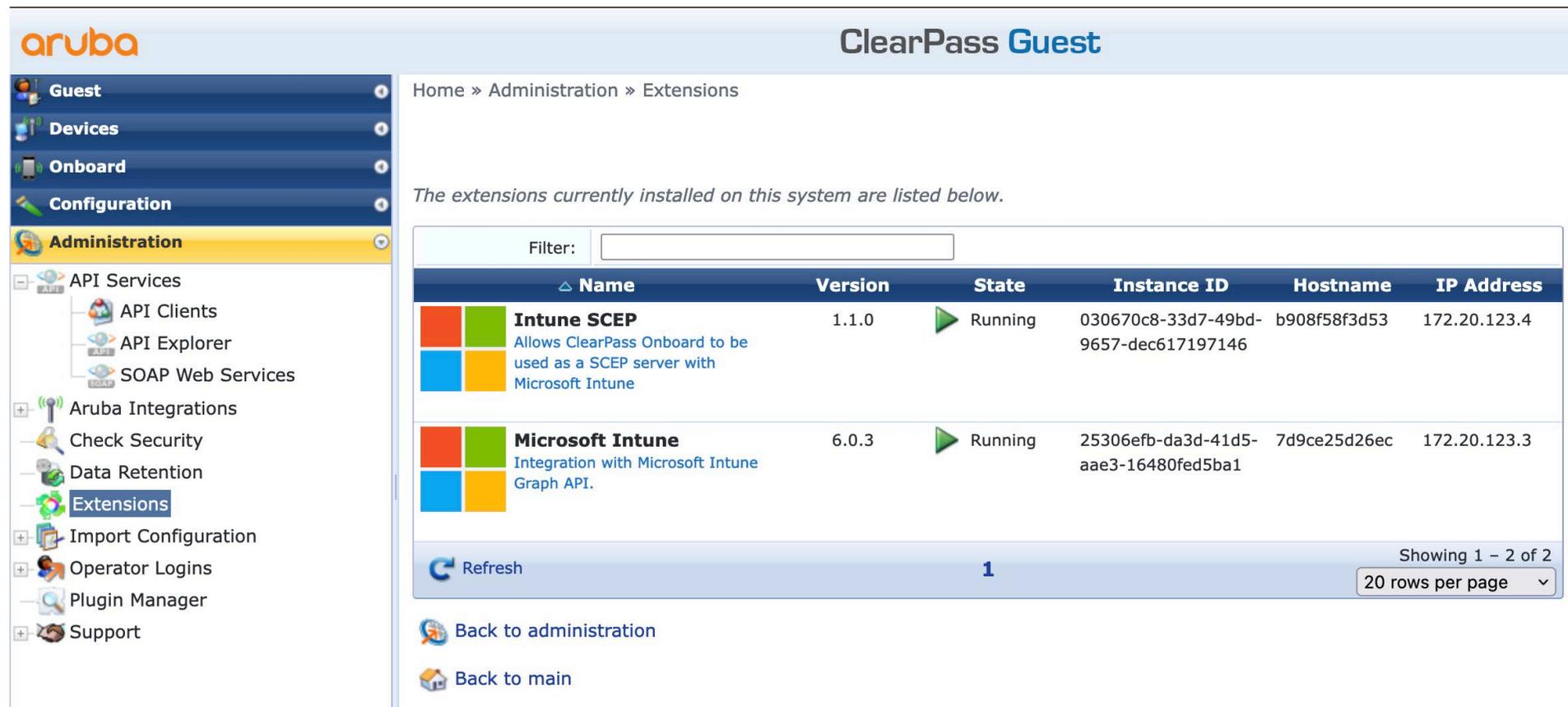


Microsoft Intune

(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.



The screenshot displays the Aruba ClearPass Guest Administration interface. The left sidebar shows the navigation menu with 'Administration' selected. The main content area shows the 'Extensions' page, which lists installed extensions in a table. The table has columns for Name, Version, State, Instance ID, Hostname, and IP Address. Two extensions are listed: 'Intune SCEP' and 'Microsoft Intune'. Below the table, there is a 'Refresh' button and a page indicator showing '1' row. At the bottom, there are links for 'Back to administration' and 'Back to main'.

aruba ClearPass Guest

Home » Administration » Extensions

The extensions currently installed on this system are listed below.

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

Filter:

Refresh 1 Showing 1 - 2 of 2
20 rows per page

[Back to administration](#)
[Back to main](#)



ClearPass Intune Extension

● API/App registration in Entra ID

Microsoft Intune 6.0.3 Running 71217094-d0c6-4e31-04a8b26d445d 172.17.0.10

Integration with Microsoft Intune Graph API.

Extension Configuration

```

{
  "logLevel": "INFO",
  "verifySSLCerts": true,
  "azureADEndpoint": "login.microsoftonline.com",
  "graphEndpoint": "graph.microsoft.com",
  "tenantId": "6d648377-d3db-49f0-a0c8-f61acfc19fd3",
  "clientId": "f696271f-75e6-419f-b3f8-064ce7ecdd20",
  "clientSecret": "*****",
  "syncPageSize": 50,
  "enableSyncAll": true,
  "syncAllSchedule": "* / 30 * * * *",
  "syncUpdatedOnly": true,
  "syncAllOnStart": false,
  "enableEndpointCache": false,
  "endpointCacheTimeSeconds": 900,
  "intuneAttributes": null,
  "enableUserGroups": false,
  "userGroupUpdateSchedule": "* / 30 * * * *",
  "bvpasProxv": false.
}
    
```

Restart: Restart extension after updating configuration

Save Changes

CPPM-Intune-2022

Search

Delete Endpoints Preview features

Overview

Quickstart

Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API

Essentials

Display name : [CPPM-Intune-2022](#)

Application (client) ID : c1217c83-8dde-4887-9d24-abc147befb29

Object ID : ead47714-cd3b-47d2-9135-983d340311b5

Directory (tenant) ID : 3dec4cd9-6ff8-404d-9074-6a07e3adea29

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

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Aut...

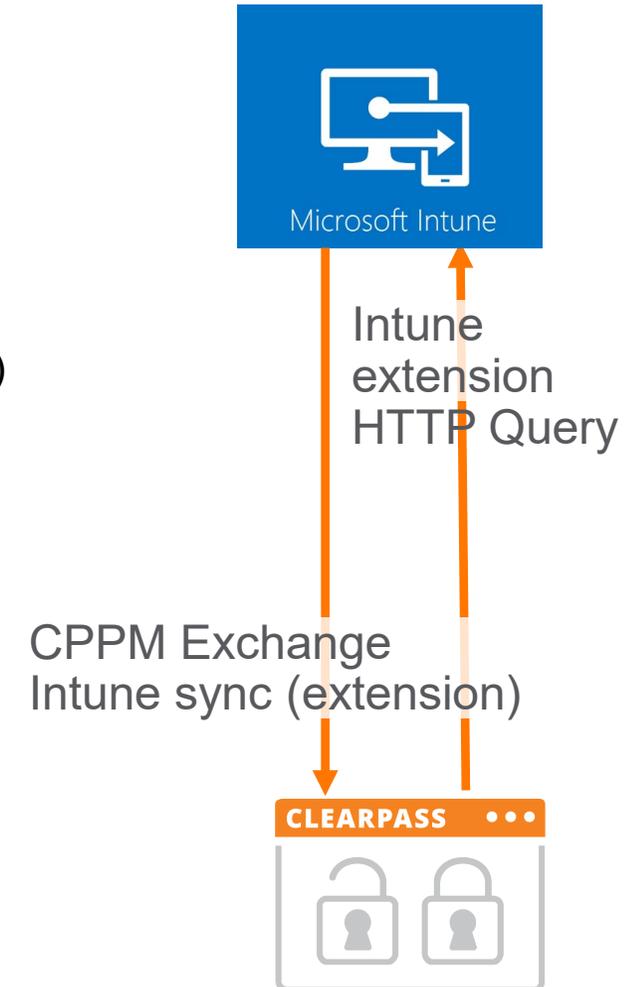
Get Started Documentation

	Admin consent req...	Status
		...
state and compliance information from Micro...	Yes	✔ Granted for of 364
		...
lications	Yes	✔ Granted for of 364
rite all applications	Yes	✔ Granted for of 364
ps that this app creates or owns	Yes	✔ Granted for of 364
DeviceManagementApps.Read	Application	Read Microsoft Intune apps
DeviceManagementManagedDe	Application	Read Microsoft Intune devices
DeviceManagementManagedDe	Application	Read and write Microsoft Intune devices
Directory.Read.All	Application	Read directory data
User.Read	Delegated	Sign in and read user profile



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 synchronize 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

Request Details

Summary Input Output Accounting

Access Device Name: 192.168.36.8

RADIUS Request

Radius:Aruba:Aruba-AP-Group	C2C ArubalabNL
Radius:Aruba:Aruba-AP-MAC-Address	d015a6cae426
Radius:Aruba:Aruba-Device-MAC-Address	b88a60c60f7a
Radius:Aruba:Aruba-Device-Type	Win 10
Radius:Aruba:Aruba-Essid-Name	WLAN_WPA3
Radius:Aruba:Aruba-Location-Id	AP-C2C-515-H-e4:26
Radius:IETF:Called-Station-Id	d015a6cae426
Radius:IETF:Calling-Station-Id	b88a60c60f7a
Radius:IETF:Framed-MTU	1100
Radius:IETF:NAS-Identifier	192.168.36.8
Radius:IETF:NAS-IP-Address	192.168.36.8
Radius:IETF:NAS-Port	0
Radius:IETF:NAS-Port-Type	19
Radius:IETF:Service-Type	2
Radius:IETF:User-Name	herman@azure.arubalab.com

Authorization Attributes

Showing 2 of 1-2 records

Change Status Show Configuration Export Show Logs Close

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-07eb7142dccb, AzureADDeviceId:74a622ba-eb11-486d-8ab8-0965bfb636b3
Certificate:Subject-CN	fdd2d322-27fd-4f82-a5da-07eb7142dccb
Certificate:Subject-DN	CN=fdd2d322-27fd-4f82-a5da-07eb7142dccb
Certificate:Version	3
Connection:AP-Name	AP-C2C-515-H-e4:26
Connection:Client-Mac-Address	b88a60c60f7a
Connection:Client-Mac-Address-Colon	b8:8a:60:c6:0f:7a
Connection:Client-Mac-Address-Dot	b88a.60c6.0f7a
Connection:Client-Mac-Address-Hyphen	b8-8a-60-c6-0f-7a
Connection:Client-Mac-Address-NoDelim	b88a60c60f7a
Connection:Client-Mac-Address-Upper-Hyphen	B8-8A-60-C6-0F-7A
Connection:Client-Mac-Vendor	Intel Corporate
Connection:Dest-IP-Address	192.168.36.51

Showing 2 of 1-2 records

Change Status Show Configuration Export Show Logs Close



Using the Intune Device Id to lookup Attributes in Endpoint

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

Request Details	
Summary	Input
Certificate:Issuer	Geneva
Certificate:Not-Valid-After	2024-05-04 14:27:57
Certificate:Public-Key-Algorithm	rsaEncryption
Certificate:Public-Key-Length	2048
Certificate:Serial-Number	01:48
Certificate:Signature-Algorithm	sha512WithRSAEncryption
Certificate:Subject-AltName-Email	bob@hpearuba.net
Certificate:Subject-AltName-msUPN	bob@azure.hpearuba.net
Certificate:Subject-AltName-URI	IntuneDeviceId:310c5ce8-e2d5-4869-a27c-3aafc5ea5957, AAD_Device_ID:2c280c74-60aa-4d99-a94e-fc02bbafca3
Certificate:Subject-CN	310c5ce8-e2d5-4869-a27c-3aafc5ea5957
Certificate:Subject-DN	CN=310c5ce8-e2d5-4869-a27c-3aafc5ea5957
Certificate:Version	3
Connection:AP-Name	CP1-AP345-01
Connection:Client-Mac-Address	c83a35a80b65
Connection:Client-Mac-Address-Colon	c8:3a:35:a8:0b:65
Connection:Client-Mac-Address-Dot	c83a.35a8.0b65
Connection:Client-Mac-Address-Hyphen	c8-3a-35-a8-0b-65
Connection:Client-Mac-Address-NoDelim	c83a35a80b65
Connection:Client-Mac-Address-Upper-Hyphen	C8-3A-35-A8-0B-65

Edit Endpoint		
Endpoint	Attributes	Device Fingerprints
16.	Intune Exchange Last Successful Sync Date Time	= 0001-01-01T00:00:00Z
17.	Intune Free Storage Space in Bytes	= 58540949504
18.	Intune ID	= 310c5ce8-e2d5-4869-a27c-3aafc5ea5957
19.	Intune Is Encrypted	= false
20.	Intune Is Supervised	= false
21.	Intune Jail Broken	= Unknown
22.	Intune Last Sync Date Time	= 2023-05-23T12:53:18Z

Authentication Sources - Intune-EndpointDB

Summary	General	Primary	Attributes
General:			
Name:	Intune-EndpointDB		
Description:	Query the Endpoint Database by Intune DeviceID		
Type:	Sql		
Use for Authorization:	Enabled		
Authorization Source:	Intune-EndpointDB		
Primary:			
Server Name:	Intune-EndpointDB		
Database Name:	tipsdb		
Login Username:	*****		
Log Password:	*****		
Timeout:	30		
ODBC Driver:	PostgreSQL		
Password Type:	Password		
Attributes:			
Filters:	1. 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' FROM tips_endpoints WHERE attributes->>'Intune ID' = LOWER('%{Certificate:Subject-CN}')		

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" 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-07eb7142dccb, AzureADDeviceId:74a622ba-eb11-486d-8ab8-0965bfb636b3
Certificate:Subject-CN	fdd2d322-27fd-4f82-a5da-07eb7142dccb
Certificate:Subject-DN	CN=fdd2d322-27fd-4f82-a5da-07eb7142dccb

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 6.0.3 Running 25306efb-da3d-41d5-7d9ce25d26ec 172.20.123.3 aae3-16480fed5ba1

Integration with Microsoft Intune Graph API.

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

Request Details

Summary Input Output Accounting

Authorization Attributes

Authorization:Arubalab-AzureAD:AccountEnabled	true
Authorization:Arubalab-AzureAD:Department	Arubalab
Authorization:Arubalab-AzureAD:Email	herman@azure.arubalab.com
Authorization:Arubalab-AzureAD:Groups	Central Admin, IT Admins, Intune Users, of364
Authorization:Intune-EndpointDB:Intune Azure AD Device Id	74a622ba-eb11-486d-8ab8-0965bfb636b3
Authorization:Intune-EndpointDB:Intune Azure AD Registered	true
Authorization:Intune-EndpointDB:Intune Compliance State	compliant
Authorization:Intune-EndpointDB:Intune Device Name	DT-W10VM-09
Authorization:Intune-EndpointDB:Intune Jail Broken	Unknown
Authorization:Intune-EndpointDB:Intune Managed Device Owner Type	personal
Authorization:Intune-EndpointDB:Intune Management Agent	mdm
Authorization:Intune-EndpointDB:Intune Model	VMware Virtual Platform
Authorization:Intune-EndpointDB:Intune Operating System	Windows
Authorization:Intune-EndpointDB:Intune User Principal Name	herman@azure.arubalab.com
Authorization:Intune ExtRT:Intune Azure AD Device Id	74a622ba-eb11-486d-8ab8-0965bfb636b3
Authorization:Intune ExtRT:Intune Compliance State	compliant

Showing 2 of 1-2 records

Change Status Show Configuration Export Show Logs Close

Request Details

Summary Input Output Accounting

Authorization:Intune-EndpointDB:Intune User Principal Name	herman@azure.arubalab.com
Authorization:Intune ExtRT:Intune Azure AD Device Id	74a622ba-eb11-486d-8ab8-0965bfb636b3
Authorization:Intune ExtRT:Intune Compliance State	compliant
Authorization:Intune ExtRT:Intune Device Name	DT-W10VM-09
Authorization:Intune ExtRT:Intune Managed Device Owner Type	personal
Authorization:Intune ExtRT:Intune User Principal Name	herman@azure.arubalab.com
Authorization:LabAD:UserDN	

Computed Attributes

Authentication:ErrorCode	0
Authentication:Full-Username	herman@azure.arubalab.com
Authentication:InnerMethod	EAP-TLS
Authentication:MacAuth	NotApplicable
Authentication:OuterMethod	TEAP
Authentication:Posture	Unknown
Authentication:Status	User, Machine
Authentication:TEAP-Method-1	EAP-TLS
Authentication:TEAP-Method-1-Status	Success
Authentication:TEAP-Method-1-Username	fdd2d322-27fd-4\$

Showing 2 of 1-2 records

Change Status Show Configuration Export Show Logs Close

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

The screenshot displays the Microsoft Intune admin center interface. On the left is a navigation pane with categories: Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area shows the breadcrumb path: Home > Devices | All devices > DT-W10-WLAN-03. Below this is the title 'DT-W10-WLAN-03 | Hardware' and a search bar. A list of management and monitoring options is shown, with 'Hardware' selected. The hardware details are presented in a table format:

MEID	
Manufacturer	VMware, Inc.
Model	VMware7,1
Processor Architecture	x64
Phone number	
TPM Version	
TPM manufacturer ID	
TPM manufacturer version	
System management BIOS version	VMW71.00V.16707776.B64.2008070230
Network details	
Subscriber carrier	
Cellular technology	
Wi-Fi MAC	C83A35A80B65
Ethernet MAC	005056B70D42
ICCID	
Wi-Fi IPv4 address	172.16.101.100
Wi-Fi subnet ID	172.16.101.0
Wired IPv4 address	10.7.12.115
Network service	
Enrolled date	5/4/2023, 10:14:37 AM
Last contact	5/17/2023, 12:33:29 PM
Conditional access	
Activation lock bypass code	
Apple ID registered	Yes



Endpoint Sync only with Wi-Fi MAC

Request Details

Summary Input Output Accounting

Authorization Attributes

Authorization:Arubalab-AzureAD:AccountEnabled	true
Authorization:Arubalab-AzureAD:Department	Arubalab
Authorization:Arubalab-AzureAD:Email	herman@azure.arubalab.com
Authorization:Arubalab-AzureAD:Groups	Central Admin, IT Admins, Intune Users, of364
Authorization:Intune-EndpointDB:Intune Azure AD Device Id	74a622ba-eb11-486d-8ab8-0965bfb636b3
Authorization:Intune-EndpointDB:Intune Azure AD Registered	true
Authorization:Intune-EndpointDB:Intune Compliance State	compliant
Authorization:Intune-EndpointDB:Intune Device Name	DT-W10VM-09
Authorization:Intune-EndpointDB:Intune Jail Broken	Unknown
Authorization:Intune-EndpointDB:Intune Managed Device Owner Type	personal
Authorization:Intune-EndpointDB:Intune Management Agent	mdm
Authorization:Intune-EndpointDB:Intune Model	VMware Virtual Platform
Authorization:Intune-EndpointDB:Intune Operating System	Windows
Authorization:Intune-EndpointDB:Intune User Principal Name	herman@azure.arubalab.com
Authorization:Intune ExtRT:Intune Azure AD Device Id	74a622ba-eb11-486d-8ab8-0965bfb636b3
Authorization:Intune ExtRT:Intune Compliance State	compliant

Showing 2 of 1-2 records

Change Status Show Configuration Export Show Logs Close

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

The screenshot shows the Microsoft Intune admin center interface. The left sidebar contains navigation options: Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area displays the hardware details for device DT-W10-A1P5. The 'Hardware' section is selected, and the 'Wi-Fi MAC' field is highlighted with a red box, indicating it is empty. Other fields include MEID, Manufacturer (VMware, Inc.), Model (VMware7,1), Processor Architecture (x64), Phone number, TPM Version, TPM manufacturer ID, TPM manufacturer version, System management BIOS version (VMW71.00V.16707776.B64.2008070230), Network details (Subscriber carrier, Cellular technology), Ethernet MAC (005056B72BCC), ICCID, Wi-Fi IPv4 address, Wi-Fi subnet ID, Wired IPv4 address (10.7.12.159), Network service (Enrolled date: 5/4/2023, 10:26:45 AM; Last contact: 5/17/2023, 5:27:40 PM), and Conditional access (Activation lock bypass code, Azure AD registered: Yes, Compliance: Compliant, FAS activated: No).

Property	Value
MEID	
Manufacturer	VMware, Inc.
Model	VMware7,1
Processor Architecture	x64
Phone number	
TPM Version	
TPM manufacturer ID	
TPM manufacturer version	
System management BIOS version	VMW71.00V.16707776.B64.2008070230
Subscriber carrier	
Cellular technology	
Wi-Fi MAC	
Ethernet MAC	005056B72BCC
ICCID	
Wi-Fi IPv4 address	
Wi-Fi subnet ID	
Wired IPv4 address	10.7.12.159
Enrolled date	5/4/2023, 10:26:45 AM
Last contact	5/17/2023, 5:27:40 PM
Activation lock bypass code	
Azure AD registered	Yes
Compliance	Compliant
FAS activated	No



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

Request Details

Summary Input Output Alerts Accounting

Access Device IP (Port): 10.7.12.34 (3)
Access Device Name: CP1-6300-1

RADIUS Request

Authorization Attributes

Authorization:Aruba Geneva AD:Email	bob@hpearuba.net
Authorization:Aruba Geneva AD:Groups	employees
Authorization:Aruba Geneva AD:memberOf	CN=employees,OU=ACN-Demo,OU=hpedemo,DC=aruba,DC=local
Authorization:Aruba Geneva AD:Name	Bob the Employee
Authorization:Aruba Geneva AD TEAP Computer:UserDN	
Authorization:Aruba Geneva AD:UserDN	CN=Bob the Employee,OU=ACN-Demo,OU=hpedemo,DC=aruba,DC=local
Authorization:CIC-Intune:Intune Azure AD Device Id	5dda571e-b220-4c4c-938c-acd68199c44a
Authorization:CIC-Intune:Intune Compliance State	compliant
Authorization:CIC-Intune:Intune Device Name	DT-W10-A1P5
Authorization:CIC-Intune:Intune Managed Device Owner Type	company
Authorization:CIC-Intune:Intune User Principal Name	bob@azure.hpearuba.net

Computed Attributes

Endpoint Attributes

Showing 2 of 1-1000 records | Change Status | Show Configuration | Export | Show Logs | Close

Request Details

Summary Input Output Alerts Accounting

Error Code: -
Error Category: Success
Error Message: Success

Alerts for this Request

Policy server	Failed to get value for attributes=[Intune Azure AD Device Id, Intune Azure AD Registered, Intune Compliance State, Intune Device Name, Intune Jail Broken, Intune Managed Device Owner Type, Intune Management Agent, Intune Model, Intune Operating System, Intune User Principal Name]
---------------	---

Endpoint query will fail!

Showing 2 of 1-1000 records | Change Status | Show Configuration | Export | Show Logs | Close



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)

The screenshot shows the Azure AD application registration interface for 'Intune-SCEP'. The application is in a 'Ready' state and is registered for the tenant 'of364'. The interface includes a navigation pane on the left with options like 'Show Details', 'Stop', 'Overview', 'Quickstart', and 'Integration assistant'. The main content area displays the application's 'Essentials' and a table of permissions.

Application Details:

- Name:** Intune-SCEP
- Version:** (Not specified)
- State:** Ready
- Instance ID:** (Not specified)
- Hostname:** (Not specified)
- IP Address:** (Not specified)
- Display name:** Intune-SCEP
- Application (client) ID:** cd641545-a6c4-42f6-96a3-6a4b078f2e8b
- Object ID:** 4b356004-79ef-41b2-8015-602b4227d636
- Directory (tenant) ID:** 3dec4cd9-6ff8-404d-9074-6a07e3adea29

Permissions Table:

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

Code Snippet:

```
{
  "azuread-tenantid": "a6c4-42f6-96a3-6a4b078f2e8b",
  "azuread-clientid": "cd641545-a6c4-42f6-96a3-6a4b078f2e8b",
  "tenantid": "3dec4cd9-6ff8-404d-9074-6a07e3adea29",
  "name": "Intune-SCEP"
}
```

Additional Information:

- Client credentials: 0 certificates
- Redirect URIs: 1 web redirect URI
- Application ID URI: Add an application ID URI
- Managed application in I...: Intune-SCEP



ClearPass Enable ClearPass Onboard CA for SCEP

The screenshot shows the Aruba ClearPass Onboard web interface. The top navigation bar includes the Aruba logo, the title "ClearPass Onboard", and a "Menu" button. The breadcrumb trail is "Home » Onboard » Certificate Authorities". A sidebar on the left contains navigation links for "Guest", "Devices", and "Onboard". The main content area is titled "SCEP Server" and includes a sub-header "These options control access to the SCEP server for this CA." Below this, there are four configuration rows:

SCEP Server:	<input checked="" type="checkbox"/> Enable access to the SCEP server Allows this CA to issue tls-client certificates via SCEP	Enable SCEP
SCEP URL:	http://cppm.nl.arubalab.com/guest/mdps_scep.php/10	
* SCEP Validation:	External Validator ▾ Select the method by which the SCEP request is validated.	Select External Validator
* External SCEP Validator:	Intune SCEP 030670c8-33d7-49bd-9657-dec617197146 ▾ Select the extension with which to validate SCEP.	Select the Extension as External validator

On the right side of the interface, there is a "Create new certificate authority" button and a list of certificate authorities with entries like "p.php/10", "p.php/7", and "p.php/11".

Intune SCEP profiles

Home > Devices

Devices | Configuration profiles

Search

Chrome OS (preview)

Linux

Device enrollment

Enroll devices

Provisioning

Windows 365

Policy

Compliance policies

Conditional access

Configuration profiles

Scripts

Group Policy analytics (preview)

Update rings for Windows 10 and later

Profiles

+ Create profile Refresh Export Columns

7 profiles filtered

Search



Platform : Windows Phone 8.1, Windows 8.1 and later + 3



Add filter

Profile name ↑	Platform ∨	Profile type	Last modified
Arubalab - AD RootCA	Windows 8.1 and later	Trusted certificate	11-12-2019 16:43 ...
Arubalab - AD RootCA (User Store)	Windows 8.1 and later	Trusted certificate	23-08-2022 11:18 ...
Arubalab - SCEP RootCA	Windows 8.1 and later	Trusted certificate	02-08-2022 13:43 ...
Arubalab - SCEP Signing CA	Windows 8.1 and later	Trusted certificate	02-08-2022 17:13 ...
Arubalab - Windows Device Client Cert (ClearPass)	Windows 8.1 and later	SCEP certificate	09-08-2022 16:17 ...
Arubalab - Windows User Client Cert (ClearPass)	Windows 8.1 and later	SCEP certificate	19-08-2022 11:33 ...
WLAN_WPA3	Windows 10 and later	Wi-Fi	23-08-2022 12:58 ...



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

^ SCEP Certificate

Certificate type	Device												
Subject name format	CN={{DeviceID}}												
Subject alternative name	<table><thead><tr><th>Attribute</th><th>Value</th></tr></thead><tbody><tr><td>URI</td><td>IntuneDeviceId//{{DeviceID}} </td></tr><tr><td>URI</td><td>AADDeviceId//{{AAD_DeviceID}} </td></tr></tbody></table>	Attribute	Value	URI	IntuneDeviceId//{{DeviceID}}	URI	AADDeviceId//{{AAD_DeviceID}}						
Attribute	Value												
URI	IntuneDeviceId//{{DeviceID}}												
URI	AADDeviceId//{{AAD_DeviceID}}												
Certificate validity period	1 Years												
Key storage provider (KSP)	Enroll to Trusted Platform Module (TPM) KSP if present, otherwise Software KSP												
Key usage	Key encipherment, Digital signature												
Key size (bits)	2048												
Hash algorithm	SHA-2												
Root Certificate	Arubalab - SCEP Signing CA												
Extended key usage	<table><thead><tr><th>Name</th><th>Object Identifier</th><th>Predefined values</th></tr></thead><tbody><tr><td>Client Authentication</td><td>1.3.6.1.5.5.7.3.2</td><td>Client Authentication</td></tr><tr><td>Any Purpose</td><td>2.5.29.37.0</td><td>Any Purpose (2.5.2)</td></tr><tr><td>Secure Email</td><td>1.3.6.1.5.5.7.3.4</td><td>Secure Email (1.3.6)</td></tr></tbody></table>	Name	Object Identifier	Predefined values	Client Authentication	1.3.6.1.5.5.7.3.2	Client Authentication	Any Purpose	2.5.29.37.0	Any Purpose (2.5.2)	Secure Email	1.3.6.1.5.5.7.3.4	Secure Email (1.3.6)
Name	Object Identifier	Predefined values											
Client Authentication	1.3.6.1.5.5.7.3.2	Client Authentication											
Any Purpose	2.5.29.37.0	Any Purpose (2.5.2)											
Secure Email	1.3.6.1.5.5.7.3.4	Secure Email (1.3.6)											
Renewal threshold (%)	20												
SCEP Server URLs	https://cppm.arubalab.com/onboard/mdps_scep.php/10												



Client Enrolled

certlm - [Certificates - Local Computer\Personal\Certificates]

File Action View Help

Certificates - Local Computer

- Personal
 - Certificates
 - Trusted Root Certification
 - Enterprise Trust
 - Intermediate Certification
 - Trusted Publishers
 - Untrusted Certificates
 - Third-Party Root Certification
 - Trusted People
 - Client Authentication Issu
 - Preview Build Roots
 - Test Roots
 - AAD Token Issuer
 - eSIM Certification Authori
 - Homegroup Machine Cer
 - Local NonRemovable Cert
 - Remote Desktop

Issued To	Issued By	Expiration
DT-W10VM-09.nl.arubalab.com	ArubalabNL-CA	29
fdd2d322-27fd-4f82-a5da-07eb...	Intune SCEP Local Certificate Aut...	16

Personal store contains 2 certificates.

Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer

Issued to: fdd2d322-27fd-4f82-a5da-07eb7142dccf

Issued by: Intune SCEP Local Certificate Authority (Signing)

Valid from: 26/01/2023 to 26/01/2024

You have a private key that corresponds to this certificate.

Issuer Statement

OK

certmgr - [Certificates - Current User\Personal\Certificates]

File Action View Help

Certificates - Current User

- Personal
 - Certificates
 - Trusted Root Certification Au
 - Enterprise Trust
 - Intermediate Certification Au
 - Active Directory User Object
 - Trusted Publishers
 - Untrusted Certificates
 - Third-Party Root Certificatio
 - Trusted People
 - Client Authentication Issuers
 - Local NonRemovable Certific
 - Certificate Enrollment Reque
 - Smart Card Trusted Roots

Issued To	Issued By	Expiration
74a622ba-eb11-486d-8ab8-096...	MS-Organization-Access	23
fdd2d322-27fd-4f82-a5da-07eb...	Intune SCEP Local Certificate Aut...	26
herman	Geneva CIC - ClearPass Devices L...	26
Herman ADM. Robers	ArubalabNL-CA	29
herman@azure.arubalab.com	Cloud Authentication Private Roo...	22
S-1-5-21-1532318898-26253868...	S-1-5-21-1532318898-2625386876...	23

Personal store contains 6 certificates.

Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer

Issued to: fdd2d322-27fd-4f82-a5da-07eb7142dccf

Issued by: Intune SCEP Local Certificate Authority (Signing)

Valid from: 17/04/2023 to 16/04/2024

You have a private key that corresponds to this certificate.

Issuer Statement

OK



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

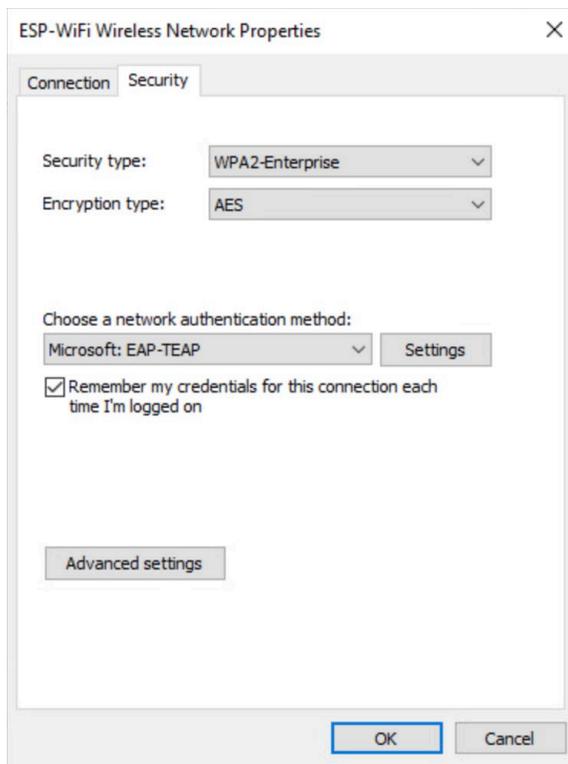
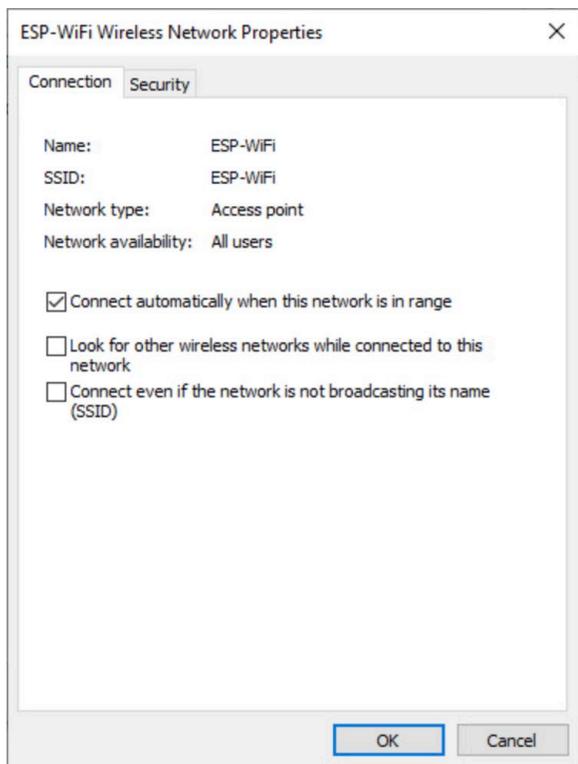
- For advanced configuration, like certificate selection or TEAP, use XML WiFi Export/Import
- <https://learn.microsoft.com/en-us/mem/intune/configuration/wi-fi-settings-import-windows-8-1>
 - Manually configure the SSID/Network on a Windows client
 - Export XML of the settings:

```
netsh wlan show profiles
netsh wlan export profile name="ContosoWiFi" folder=c:\Wifi
```
 - Create Intune Configuration Profile Windows 8.1 – Wi-Fi import

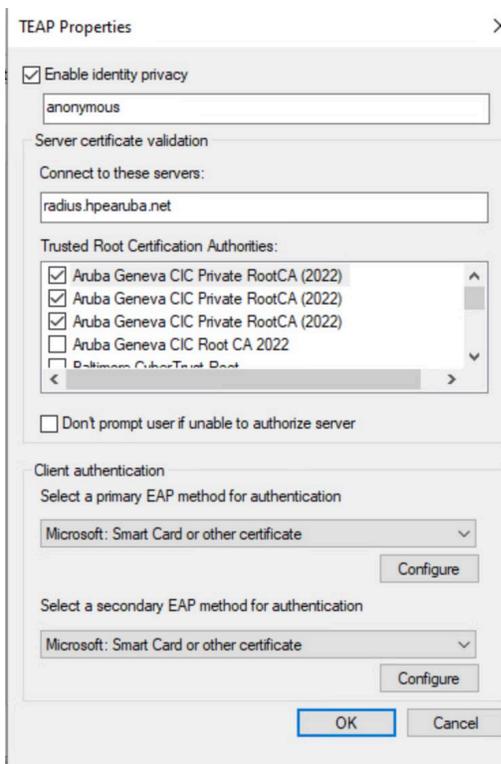


Intune XML WiFi configuration – Configure & test one client

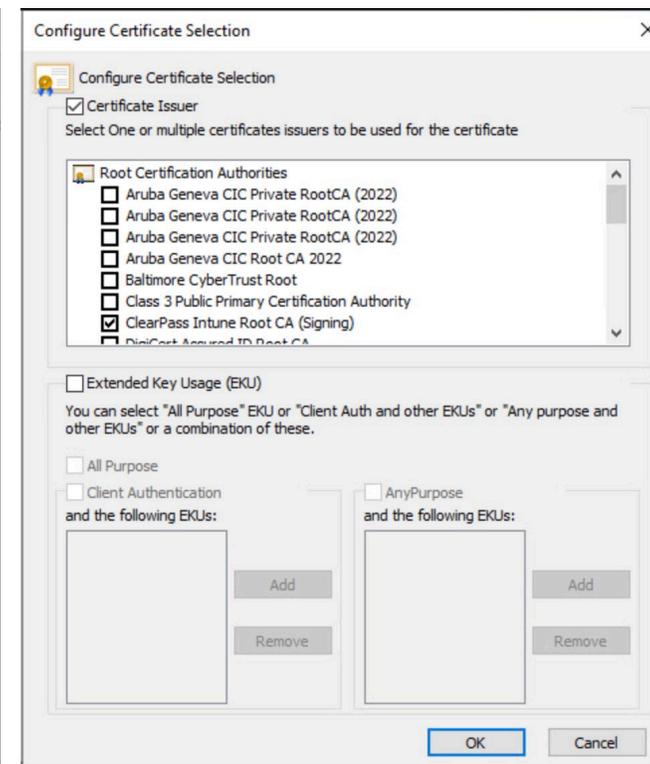
– Manually configure one client



Configure TEAP method



Configure Server trust and Method-1 & 2

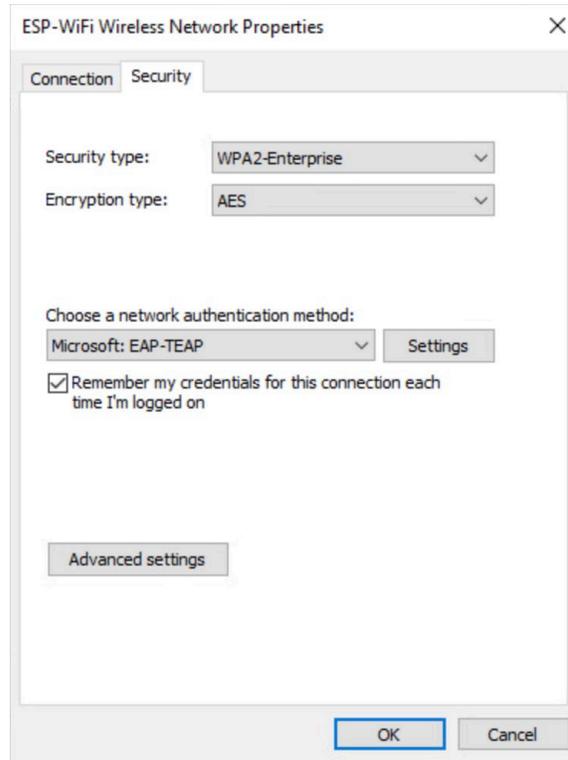
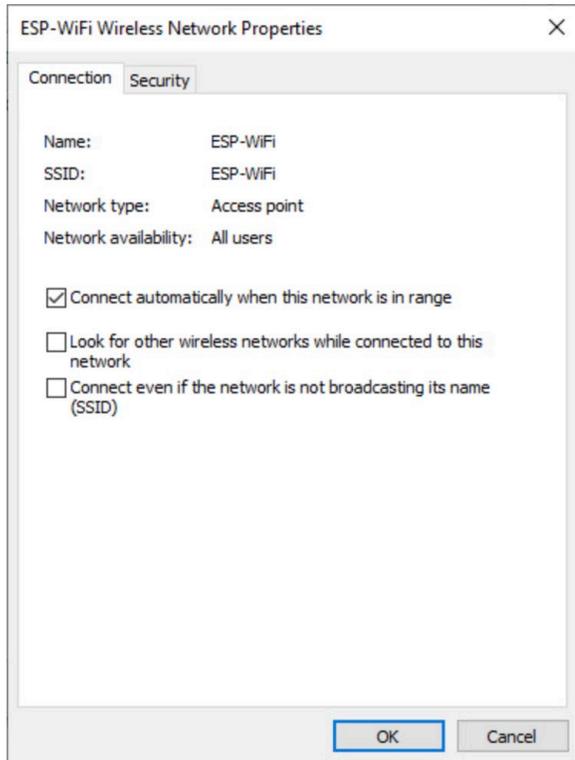


With multiple client certs select the Certificate issuer

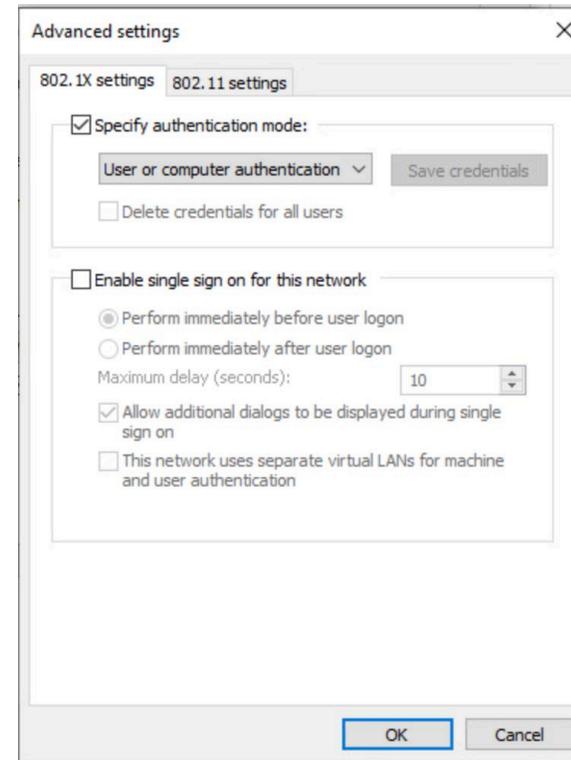


Intune XML WiFi configuration – Configure & test one client

– Manually configure one client



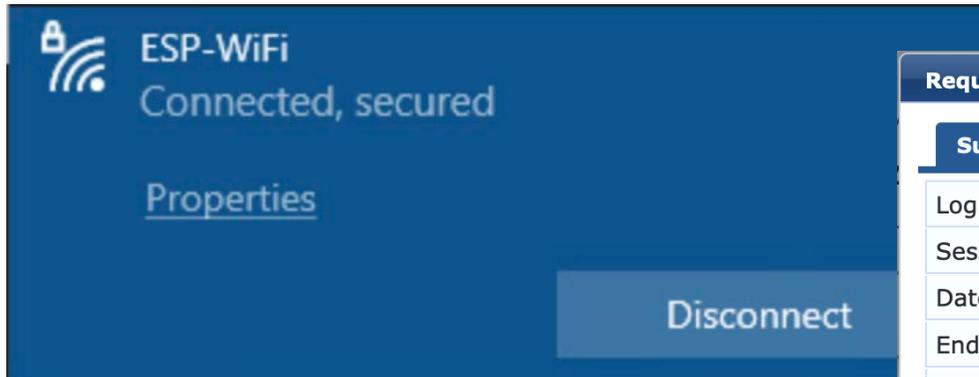
Under Advanced settings...



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.
```

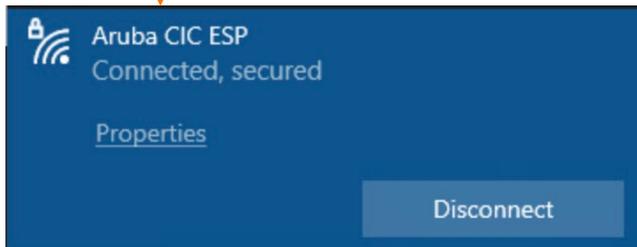
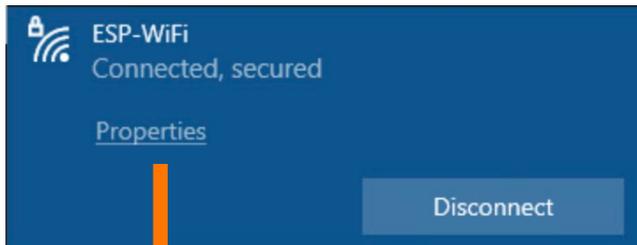
Intune XML WiFi configuration – Optionally: modify the network name

- 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 .....
```

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>
    <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 .....
```

Intune XML WiFi configuration - Create Wi-Fi import profile

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

[Home](#) > [Devices | Configuration](#) >

Wi-Fi import ...

Windows 8.1 and later

- 1 Basics
- 2 Configuration settings
- 3 Assignments
- 4 Review + create

Name *

Aruba CIC ESP-WiFi



Description

ESP-WiFi (TEAP/Intune)

Platform

Windows 8.1 and later

Profile type

Wi-Fi import



Intune XML WiFi configuration – Create Wi-Fi import profile

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

[Home](#) > [Devices | Configuration](#) >

Wi-Fi import

Windows 8.1 and later

✓ Basics **2 Configuration settings** 3 Assignments 4 Review + create

Connection name * ⓘ

Aruba CIC ESP-WiFi ✓

Profile XML *

"Wi-Fi-ESP-WiFi-modif.xml"

"Wi-Fi-ESP-WiFi-modif.xml" 📄

```
1 <?xml version="1.0"?>
2 <WLANProfile xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">
3   <name>Aruba CIC ESP</name>
4   <SSIDConfig>
5     <SSID>
6       <hex>4553502D57694669</hex>
7       <name>ESP-WiFi</name>
8     </SSID>
9     <nonBroadcast>>false</nonBroadcast>
10  </SSIDConfig>
11  <connectionType>ESS</connectionType>
12  <connectionMode>auto</connectionMode>
13  <autoSwitch>>false</autoSwitch>
14  <MSM>
```



Intune XML WiFi configuration – force update client

– Trigger update/sync from the client

Access work or school

Get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.



 Work or school account
bob@azure.hpearuba.net
[Manage your account](#)



← Settings

🏠 Managed by netmanfabe74

Connection info

Management Server Address:

https://r.manage.microsoft.com/devicegatewayproxy/cimhandler.ashx

Exchange ID:

977FF6406D759C3E79616D2EB6EC7497

Device sync status

Syncing keeps security policies, network profiles, and managed applications up to date.

Last Attempted Sync:

The sync was successful

19/07/2023 16:26:17



Advanced Diagnostic Report

Your IT or support person may want additional information to help with troubleshooting.

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 ‘friendly’ name.

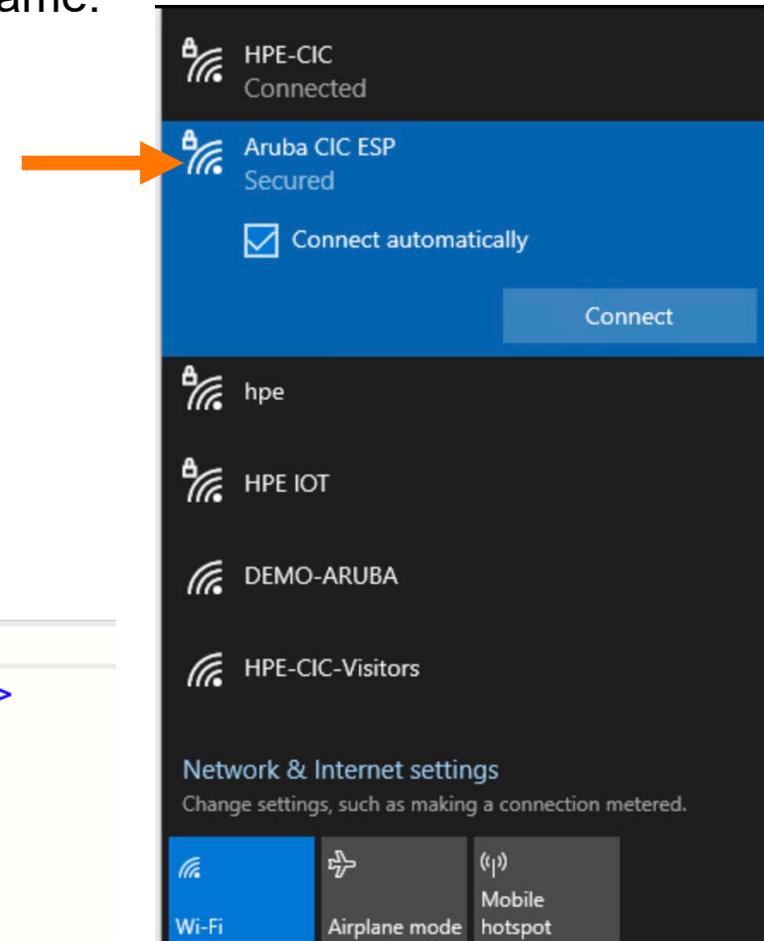
```
C:\Users\bob>netsh wlan show profiles

Profiles on interface Wi-Fi:

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

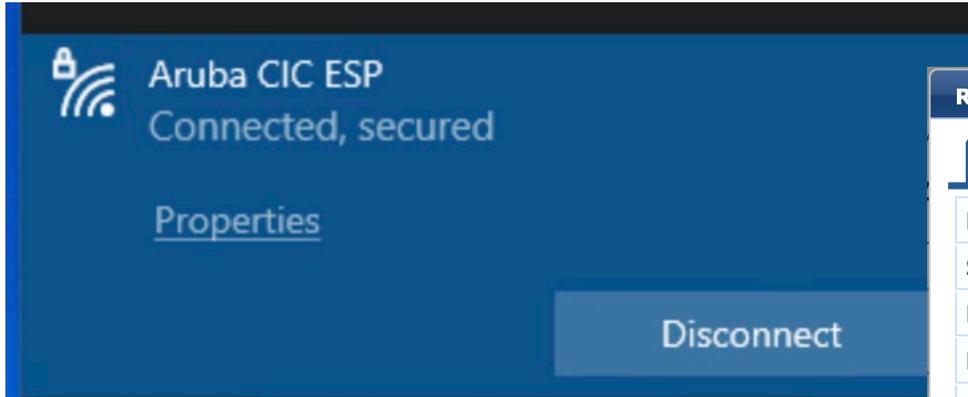
User profiles
-----
    All User Profile      : Aruba CIC ESP ←
    All User Profile      : HPE-CIC
```

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



Intune XML WiFi configuration – validate: connected

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

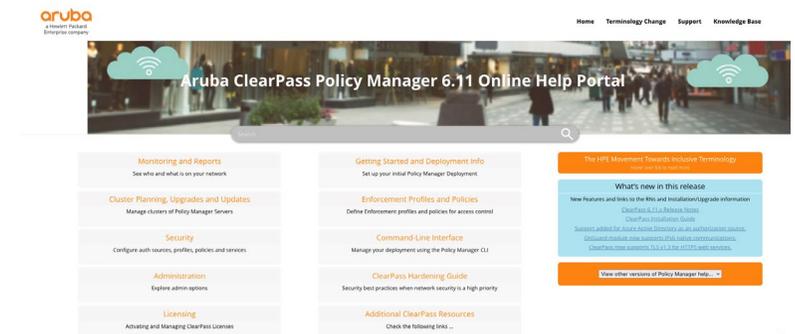


Request Details			
Summary	Input	Output	Accounting
Login Status:	ACCEPT		
Session Identifier:	R00005f68-10-64b802cb		
Date and Time:	Jul 19, 2023 17:35:46 CEST		
End-Host Identifier:	C8-3A-35-A4-0A-A1	Open in Central	Open in AirWave
End-Host Profile:	Computer / Windows / Windows 10		
End-Host Status:	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...

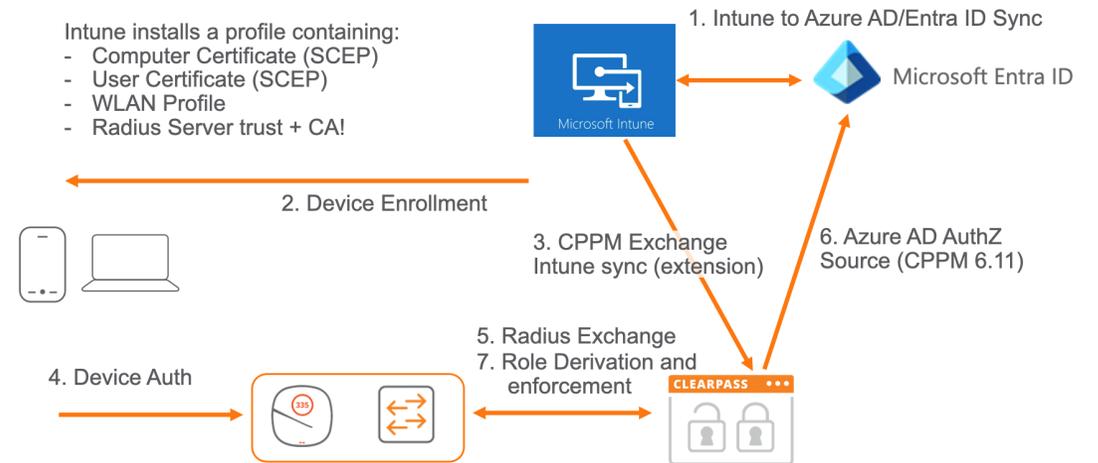
Documentation Portal

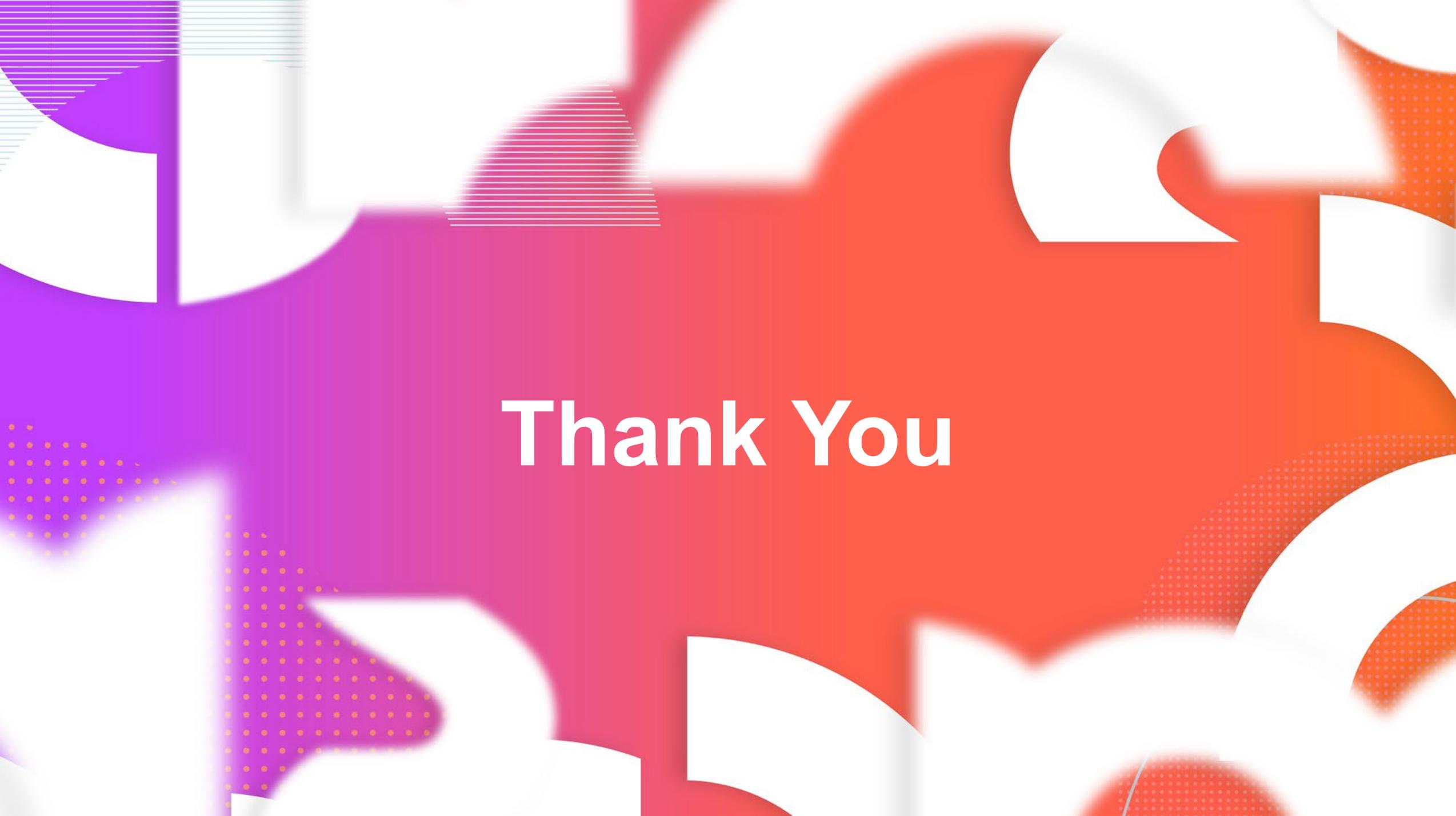
- <https://www.arubanetworks.com/techdocs/ClearPass/6.11/PolicyManager/Content/home.htm>
- Cloud Deployments: Microsoft Azure Cloud Service
<https://www.arubanetworks.com/techdocs/ClearPass/6.10/Installation-Guide/Default.htm#InstallationGuide/Cloud-Azure/CD-AZ-introduction.htm>
- Azure Authorization Source:
https://www.arubanetworks.com/techdocs/ClearPass/6.11/PolicyManager/Content/CPM_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

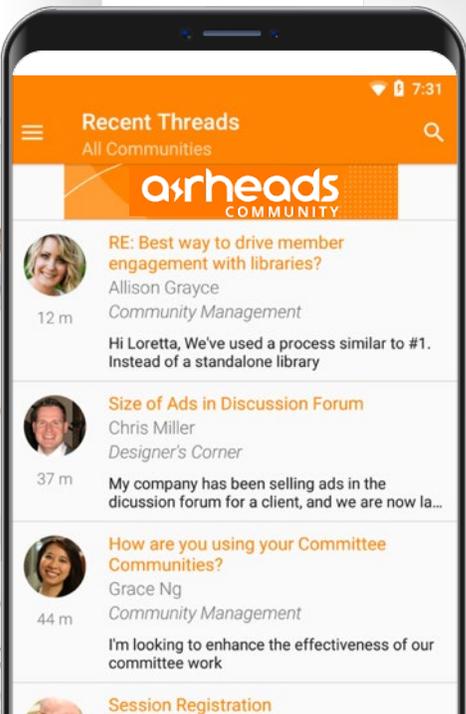
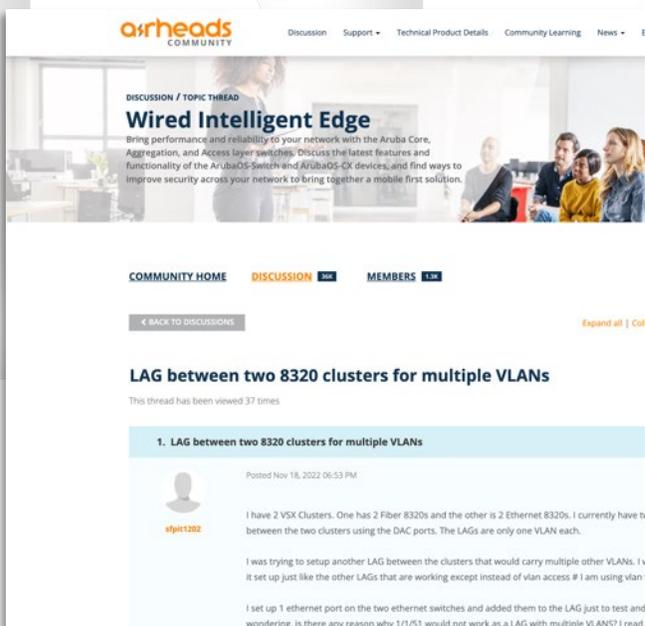
- Running ClearPass in the Cloud (Azure) is similar to on-premises
- Azure AD Authorization Source (ClearPass 6.11)
 - Entra ID
 - Authorization only
 - Get username during authentication
- Microsoft Intune Extension
 - Attributes synced to Endpoint Repository
 - HTTP Query to the Intune Extension
 - 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



arheads
COMMUNITY

Join Today!

www.community.arubanetworks.com