

# Entra ID Integration with OmniVista for Secure Wired and Wi-Fi Authentication



# Table of Contents

## Entra ID Integration with OV10 for Secure Wired and Wi-Fi Authentication

Introduction .....	3
<b>Prerequisites .....</b>	<b>4</b>
Entra ID account .....	4
OV10 cloud management access.....	4
Use Case.....	5
<b>Network Setup .....</b>	<b>6</b>
Entra ID.....	6
Creation of cloud identity on UPAM.....	12
Wired Connection Setup.....	13
Configure SSID on OV10 and Integrate OV10 with Entra ID.....	17
<b>Connection Testing .....</b>	<b>17</b>
Example of Client-Side Configuration. ....	17
<b>Conclusion .....</b>	<b>19</b>

# Introduction

This application note provides a guide for integrating Entra ID (formerly Azure AD) authentication with the OmniVista 10 network management platform. It covers the configuration process for Entra ID authentication across wired and wireless networks, using OV10 for managing network settings, including SSID configurations.

Entra ID, a cloud-based identity management solution, combined with the OmniVista 10 platform, optimizes and secures user authentication procedures. This integration removes the need for on-premises authentication systems, offering a fully cloud-based and efficient alternative. OV10 enables centralized network access management, simplifies SSID configuration, and securely integrates with Entra ID.

## Prerequisites

**Entra ID and Entra ID Account:** Entra ID is a cloud-based identity and access management solution that centralizes and secures user authentication. Each Entra ID account provides access to specific network resources.

For this project, Entra ID retrieves authorized users for Wi-Fi and wired network authentication, facilitating seamless integration via OV10

**OV10 cloud management access:** OV10, or OmniVista 10, is a network management platform that allows for the configuration and oversight of network settings, including both wired and wireless networks.

- In this project, OV10 configures the SSID and specifies "Cloud Identity" (Entra ID) as the authentication source, enhancing network security and user management.

**Required Tools and Devices:** An OV10-compatible Stellar access point and a valid Entra ID account are required. Supported models exclude AP1101 and AP1201L/H/HL. These elements ensure seamless SSID configuration and integration with OV10.

### Important Consideration:

This integration leverages Entra ID for centralized identity management and OV10 for cloud-based network access control, supporting both wired and wireless authentication securely.

## Application Note

Entra ID Integration with OV10 for Secure Wired and Wi-Fi Authentication

For this guide, Stellar access points (excluding AP1101 and AP1201L/H/HL) are used to demonstrate practical deployment and authentication in a controlled environment.

## Use Case

### Entra ID Integration with OV10 for Secure Wired and Wi-Fi Authentication:

- **OmniAccess Stellar Access Points:** OV10-compatible access points are used to connect users to the wireless network.
- **Entra ID:** A centralized identity management platform that authenticates users and manages secure network access through "Cloud Identity."
- **OmniVista (OmniVista Cirrus 10):** The network management platform that configures the SSID and integrates Entra ID as the authentication source, simplifying the process of managing authorized users and enhancing security.

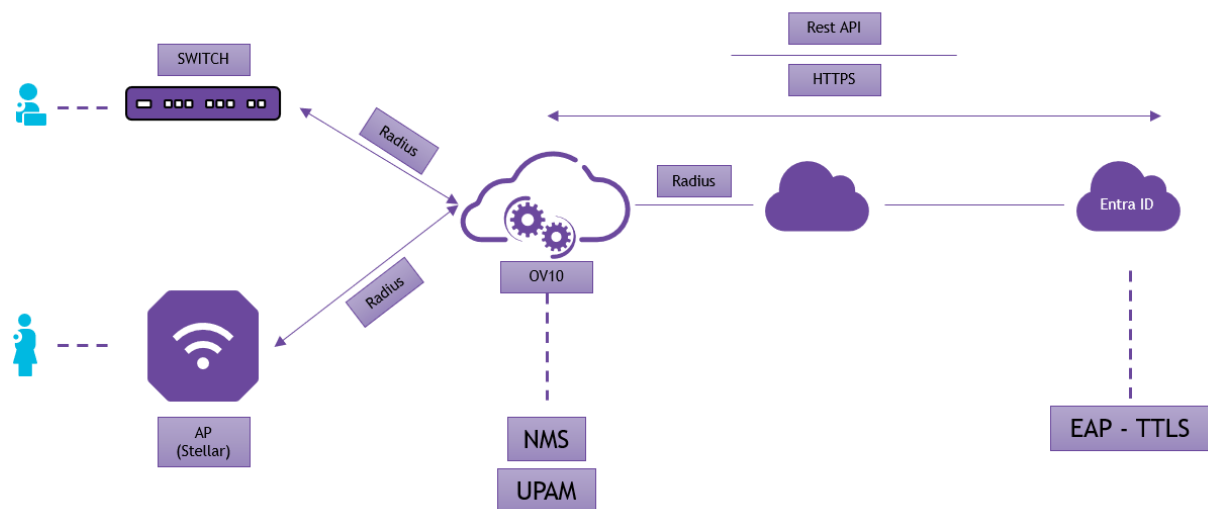


Fig. 1: Use Case

## Network Setup

### Entra ID:

The steps below are designed to gather the key information (Tenant ID, Client ID, and client secret) required to create a Cloud Identity in OV10.

#### Step 1: Generate and Save the Client Secret

#### Application Note

Entra ID Integration with OV10 for Secure Wired and Wi-Fi Authentication



The client secret is a crucial credential used for secure authentication between your registered application and Azure services. You will need this client secret to create the cloud identity in UPAM later in the process.

1. Access Your Account:

Log in to your Azure portal: <https://portal.azure.com/>

2. Navigate to App Registrations:

- ✓ Go to Microsoft Entra ID (formerly Azure AD).
- ✓ Select App registrations from the left-hand menu.

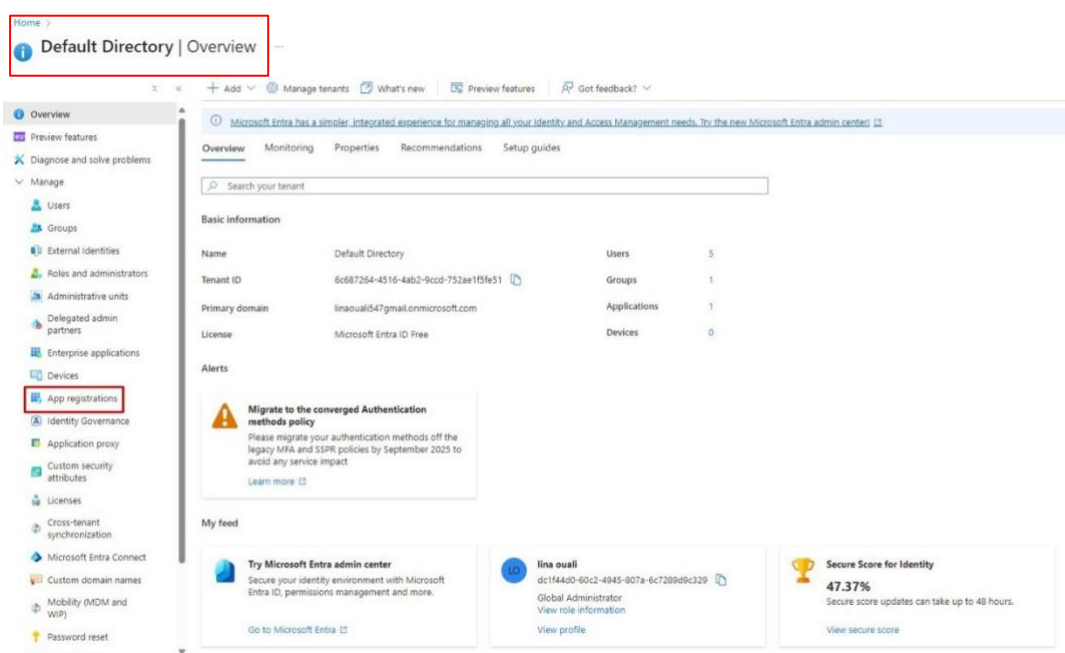


Fig. 2: Access to Entra ID > App Registrations

3. Select Your Application:

- ✓ Choose All Applications and locate your application.
- ✓ Click on your application to open its details.

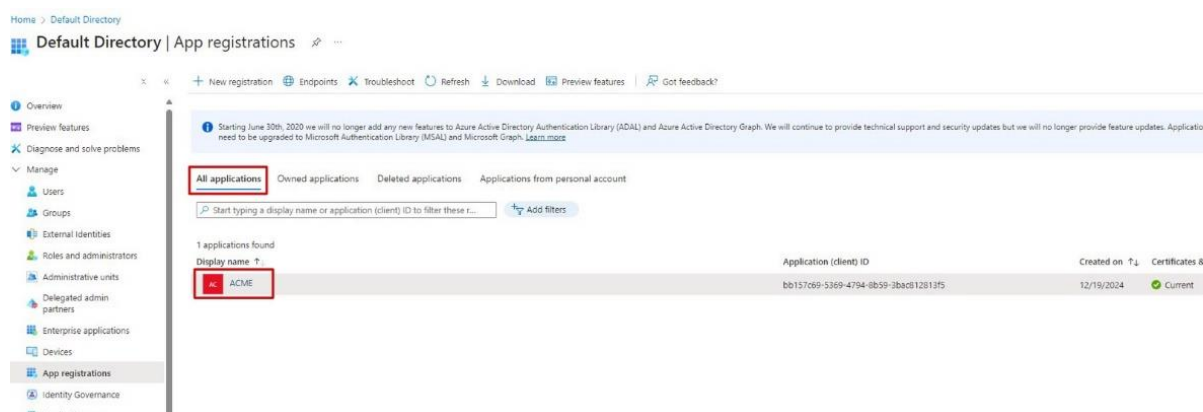


Fig. 3: View of Application Registrations in Entra ID

## Application Note

Entra ID Integration with OV10 for Secure Wired and Wi-Fi Authentication



#### 4. Generate the Client Secret:

- ✓ Go to Certificates & Secrets under your application settings.
- ✓ Click on New client secret to create a new secret.
- ✓ Copy the Value Immediately: The secret value is displayed only once. Save it securely, as you cannot retrieve it later.

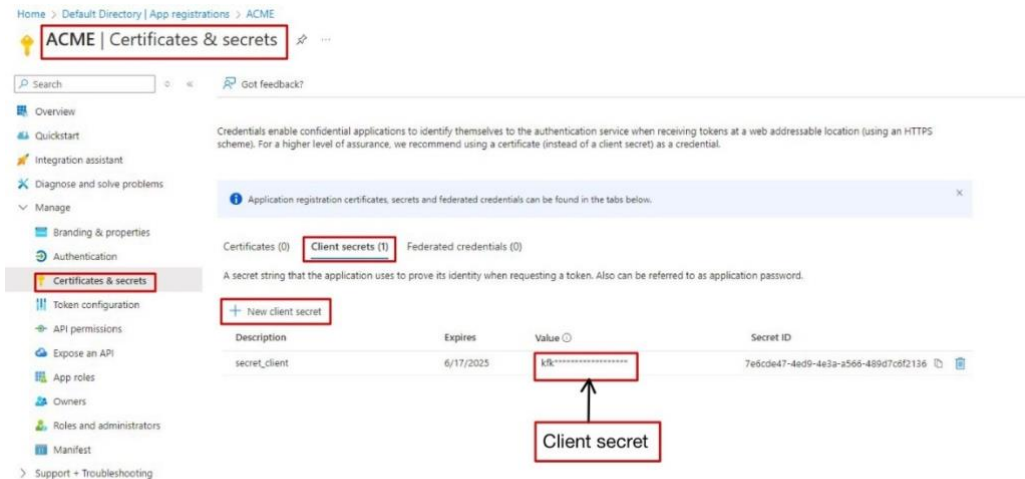


Fig. 4: Create a client secret in Entra ID

### Step 2: Retrieve Tenant ID and Client ID

The Tenant ID and Client ID are essential identifiers for your application in Azure AD. These values will also be required later to configure your application for secure access to Azure resources.

#### 1. Access Your Application Overview:

- ✓ In the Overview tab of your application, you will find the Tenant ID and Client ID.

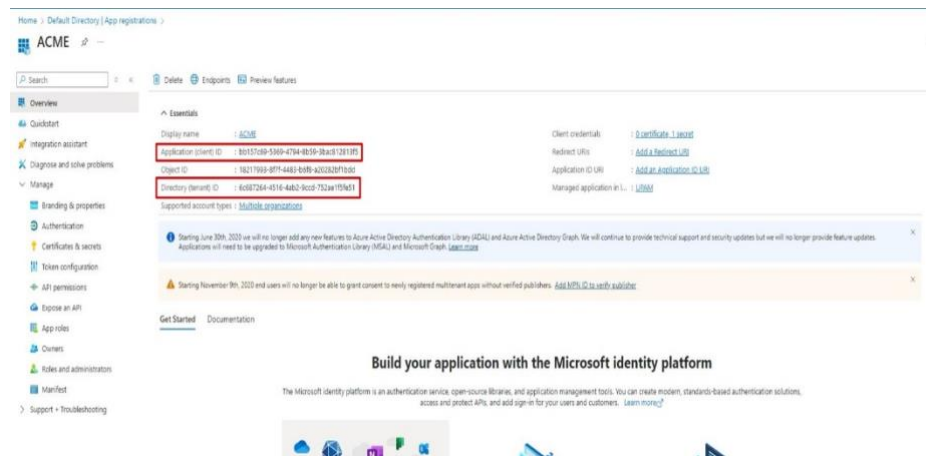


Fig. 5: Retrieve Client ID and Tenant ID for the REST API

### Application Note

Entra ID Integration with OV10 for Secure Wired and Wi-Fi Authentication

- ✓ you can retrieve the domain name (Email suffix) under “Custom domain names”

### Step 3: Example of Registering an application to Connect OV10 to Entra ID for User Authentication (I will change the title)

These steps guide you through connecting OV10 to Microsoft Entra ID for efficient user authentication. By registering an application (or using an existing one, with a detailed example provided), and configuring the necessary API permissions, OV10 ensures secure authentication for Azure users.

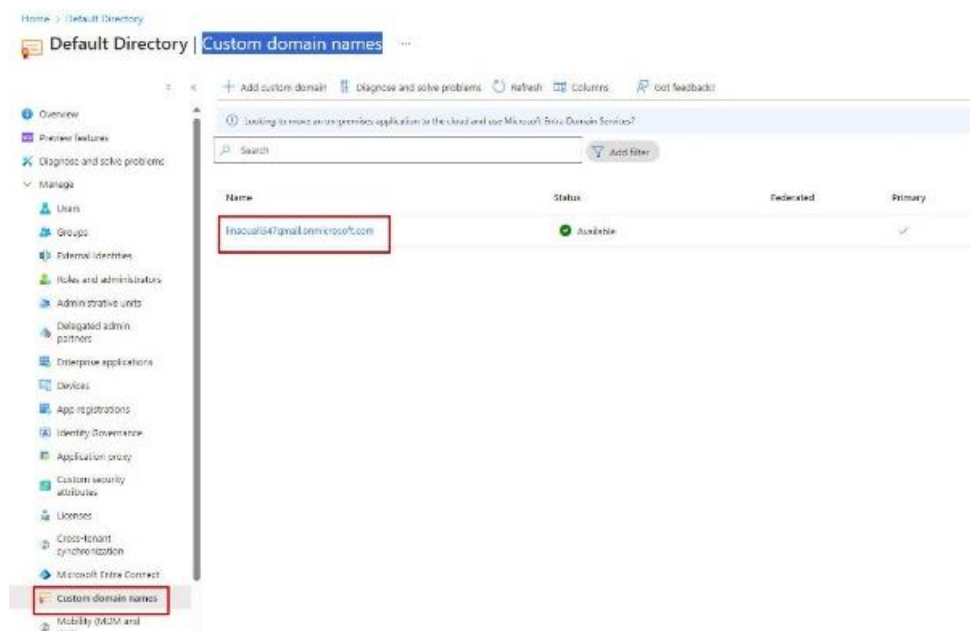


Fig. 6: Retrieve the domain name

Follow these steps to complete the registration:

1. Add an application:
  - ✓ Navigate to App registrations.

#### Application Note

Entra ID Integration with OV10 for Secure Wired and Wi-Fi Authentication



- ✓ Add a new application as shown in the figures below:

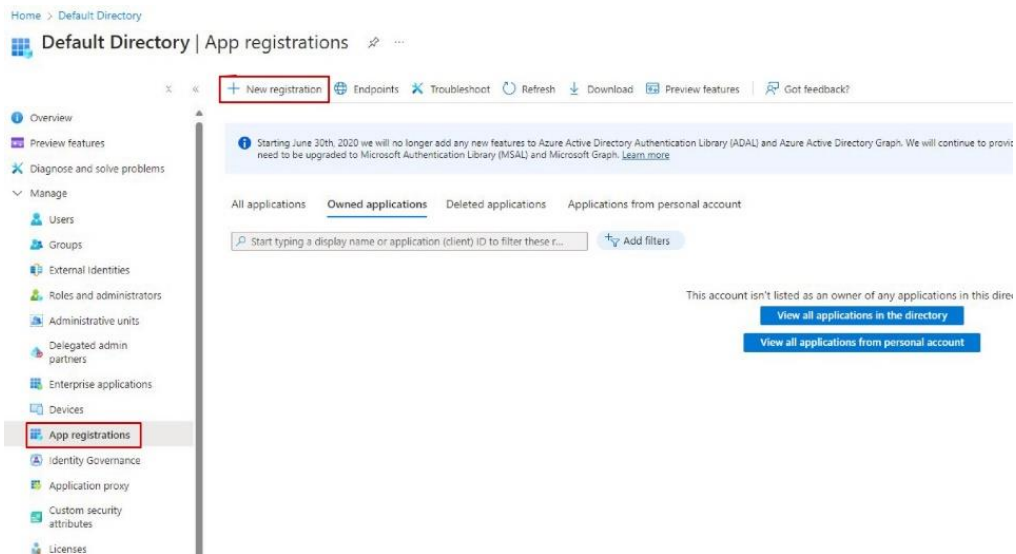


Fig. 7: Add a new application

## 2. Provide API Permissions:

This step is crucial to grant OV10 the necessary permissions to securely interact with Microsoft Entra ID

- ✓ Assign the necessary API permissions for ACME

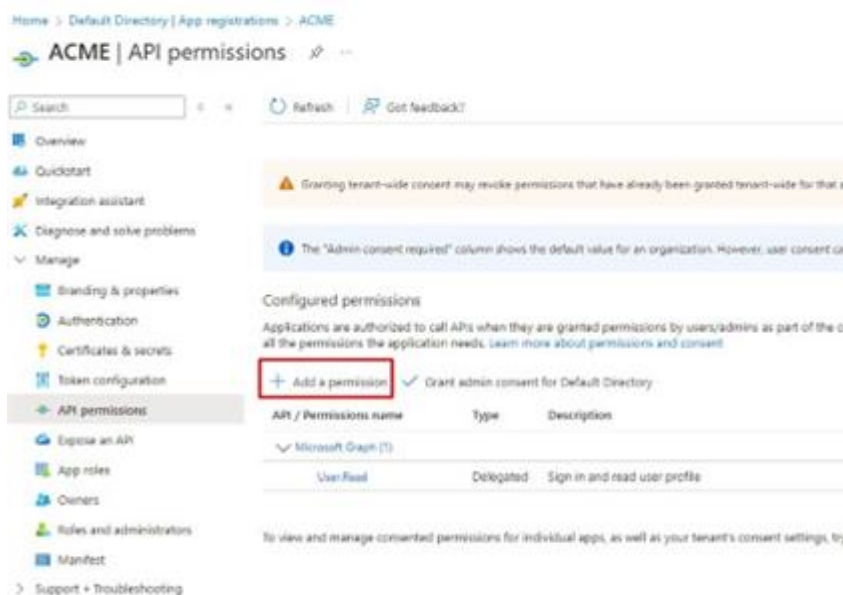


Fig. 8: Assign the necessary API permissions

- ✓ And then choose Microsoft graph to select the required permissions

## Application Note

Entra ID Integration with OV10 for Secure Wired and Wi-Fi Authentication



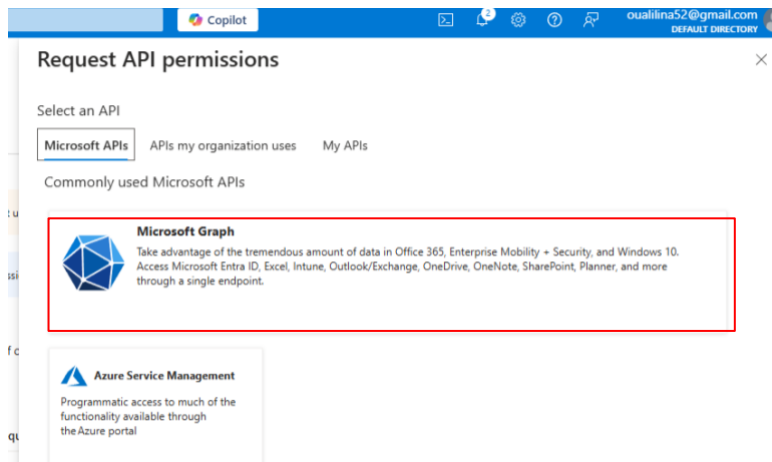


Fig. 9: Assign the necessary API permissions (Microsoft graph)

- ✓ Ensure the following delegated API permissions are granted

+ Add a permission		✓ Grant admin consent for Default Directory	
API / Permissions name	Type	Description	Admin consent requ... Status
Microsoft Graph (9)			
Directory.Read.All	Application	Read directory data	Yes <span>Granted for Default Dire...</span>
Group.Read.All	Application	Read all groups	Yes <span>Granted for Default Dire...</span>
Group.ReadWrite.All	Application	Read and write all groups	Yes <span>Granted for Default Dire...</span>
IdentityProvider.Read.All	Application	Read identity providers	Yes <span>Granted for Default Dire...</span>
offline_access	Delegated	Maintain access to data you have given it access to	No <span>Granted for Default Dire...</span>
openid	Delegated	Sign users in	No <span>Granted for Default Dire...</span>
profile	Delegated	View users' basic profile	No <span>Granted for Default Dire...</span>
User.Read	Delegated	Sign in and read user profile	No <span>Granted for Default Dire...</span>
User.ReadBasic.All	Application	Read all users' basic profiles	Yes <span>Granted for Default Dire...</span>

Fig. 10: delegated API

- ✓ Verify Authentication with a REST API To verify that authentication is functioning correctly, we can use a REST API application for confirmation.
- ✓ Copy the URL <your application> → <endpoints> → OAuth 2.0 token endpoint (v2)

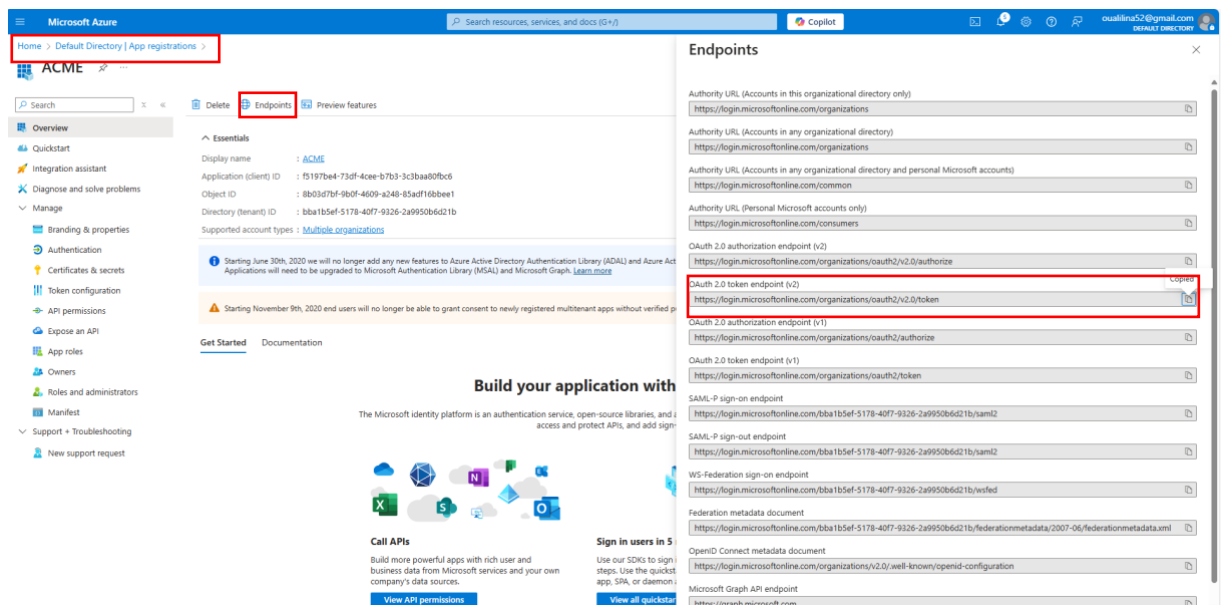


Fig. 11: URL To verify the authentication

## Application Note

Entra ID Integration with OV10 for Secure Wired and Wi-Fi Authentication

## ✓ Execute an API to Validate Credentials

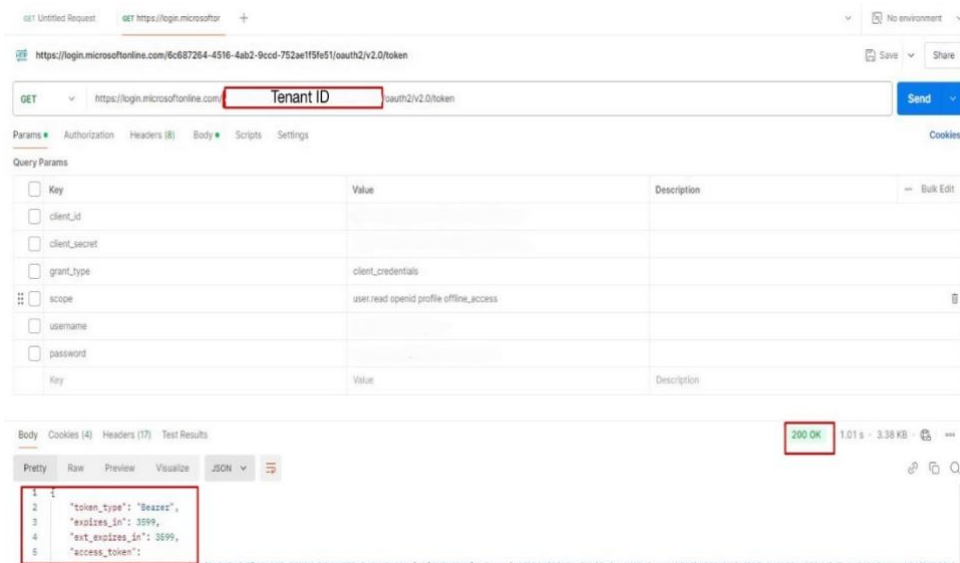


Fig. 12: Execute an API to Validate Credentials

If everything is working up to this point, you can now proceed to create Cloud Identity in UPAM.

## Creation of cloud identity on UPAM:

1. Navigate to **Network Access** in OV10 interface.
2. Go to UPAM - NAC and select External Source.
3. Choose Cloud Identity from the options.
4. Click on Create a Cloud Identity to proceed.

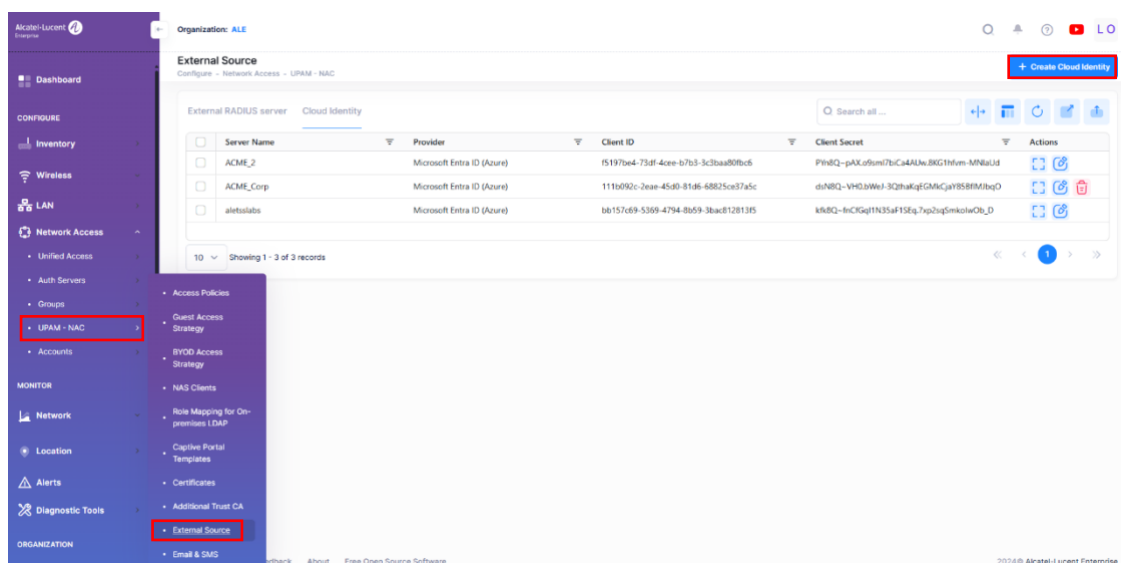


Fig. 13: Creation of cloud identity on UPAM 1

## Application Note

Entra ID Integration with OV10 for Secure Wired and Wi-Fi Authentication

5. Enter the retrieved values as explained in section I in step 1 and 2, and this will successfully create your authentication source.

Organization: ALE

**Create Cloud Identity**

Configure - Network Access - UPAM - NAC Cloud Identity

**Create Cloud Identity**

**Basic Information**

Server Name \*  
ACME\_Corp

Client ID \*  
1234567890

Tenant ID \*  
123455

Description  
Entra ID access

Provider \*  
Microsoft Entra ID (Azure)

Client Secret \*  
1234567

Email Suffix \*  
@linaouali547@gmail.onmicrosoft.com

Retrieve from the Entra ID account as specified in the following documentation

Cancel Create

Fig. 14: Creation of cloud identity on UPAM 2

## Wired Connection Setup:

The following steps outline the process for configuring Entra ID authentication in a wired network environment with OV10:

### 1. Configuring an AAA Server Profile:

Alcatel-Lucent Enterprise

Organization: ALE

**AAA Server Profile**

Configure - Network Access - Unified Access

**AAA Server Profile List**

AAA Server Profile	AuthServer. 802.1X Primary	AuthServer. Captive Portal Primary
<input type="checkbox"/> _SOLLAB_2.0	AD	AD
<input type="checkbox"/> _Network_Employee_TEST	UPAMRadiusServer	UPAMRadiusServer
<input type="checkbox"/> _ACMECorp	UPAMRadiusServer	UPAMRadiusServer
<input type="checkbox"/> _ACMECorp	UPAMRadiusServer	UPAMRadiusServer
<input type="checkbox"/> _ACMECorp	UPAMRadiusServer	-

Dashboard

CONFIGURE

- Inventory
- Wireless
- LAN
- Network Access
  - Unified Access
  - Auth Servers
  - Groups
  - UPAM - NAC
  - Accounts

MONITOR

- Access Auth Profile
- AAA Server Profile**
- Access Role Profiles
- Unified Policies
- Unified Policies List
- IoT Categorization

Fig. 15: Configuring an AAA Server Profile 1

- Choose the primary authentication server: **UPAMRadiusServer** AND use it for: **802.1X, MAC and Captive Portal**

## Application Note

Entra ID Integration with OV10 for Secure Wired and Wi-Fi Authentication

- Select Primary Accounting Server: **UPAMRadiusServer** AND use it for: **802.1X, MAC and Captive Portal**

Fig. 16: Configuring an AAA Server Profile 2

- **MAC as the Calling Station ID type** option for 802.1X, MAC, and Captive Portal authentication is selected by default.

Fig. 17: Configuring an AAA Server Profile 3

## 2. Access Auth Profile Configuration:

### a. Step 1:

- Choose your AAA server profile that you created in the previous setup **AND** enable the 802.1X Authentication.

Fig. 18: Access Auth Profile Configuration 1

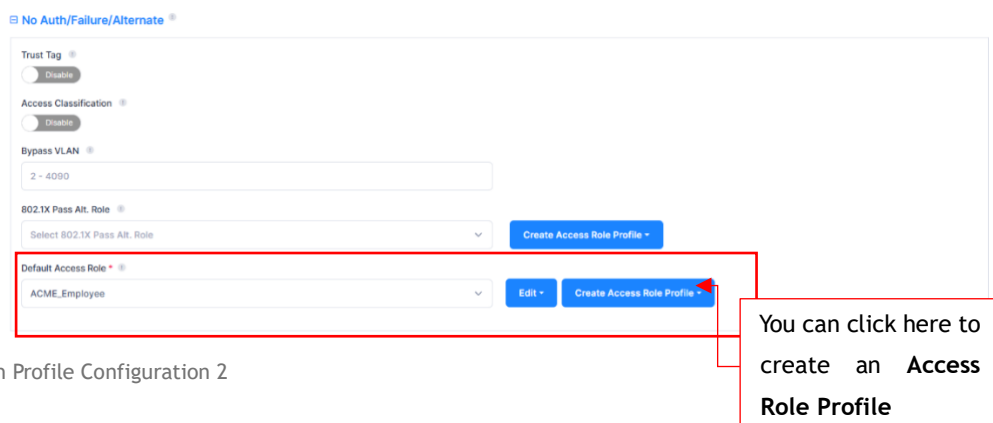
- And define your Default Access Role: (ex: ACME-Employee) In which you have the ability to create in

**Network Access → Unified Access → Access Role Profile**

## Application Note

Entra ID Integration with OV10 for Secure Wired and Wi-Fi Authentication





☐ No Auth/Failure/Alternate

Trust Tag  
☐ Disable

Access Classification  
☐ Disable

Bypass VLAN  
 2 - 4090

802.1X Pass Alt. Role  
 Select 802.1X Pass Alt. Role

Create Access Role Profile

Default Access Role  
 ACME\_Employee

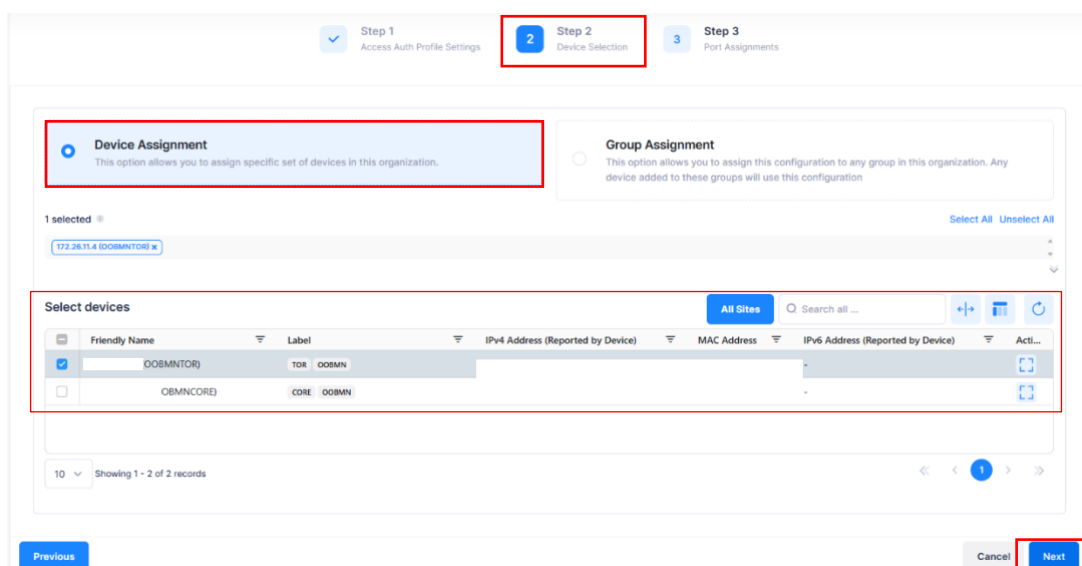
Edit Create Access Role Profile

You can click here to create an Access Role Profile

Fig. 19: Access Auth Profile Configuration 2

## b. Step 2:

- In the second setup, select your device assignment.



Step 1 Access Auth Profile Settings
 Step 2 Device Selection
 Step 3 Port Assignments

Device Assignment  
 This option allows you to assign specific set of devices in this organization.

Group Assignment  
 This option allows you to assign this configuration to any group in this organization. Any device added to these groups will use this configuration

1 selected

172.26.11.4 (OBSMNTOR)

Select devices

	Friendly Name	Label	IPv4 Address (Reported by Device)	MAC Address	IPv6 Address (Reported by Device)	Act...
<input checked="" type="checkbox"/>	OBSMNTOR	TOR OBSM				
<input type="checkbox"/>	OBSMNCORE	CORE OBSM				

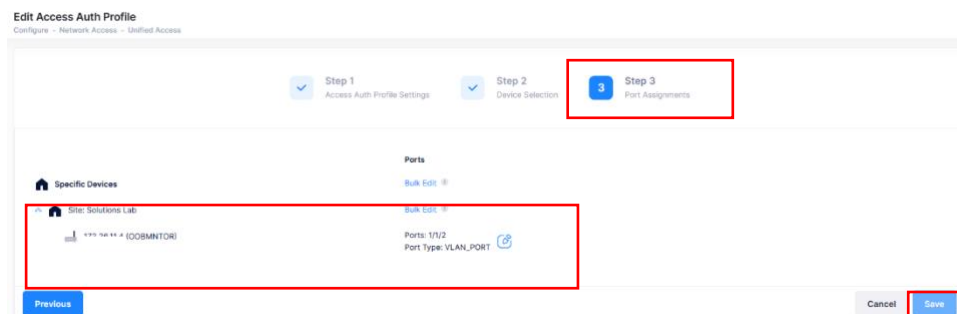
Showing 1 - 2 of 2 records

Previous
 Cancel
 Next

Fig. 20: Access Auth Profile Configuration 3

## c. Step 3:

- Please select the appropriate port for the wired connection to ensure proper access authentication configuration.



Edit Access Auth Profile  
 Configure - Network Access - Unified Access

Step 1 Access Auth Profile Settings
 Step 2 Device Selection
 Step 3 Port Assignments

Specific Devices

Site: Solutions Lab

Ports

Bulk Edit

Bulk Edit

Ports: 1/12  
 Port Type: VLAN\_PORT

Previous
 Cancel
 Save

Fig. 21: Access Auth Profile Configuration 4

## Application Note

Entra ID Integration with OV10 for Secure Wired and Wi-Fi Authentication

### 3. Access Policy Configuration:

- Choose a name for the access policy you want to create, and the precedence defaults to 1.



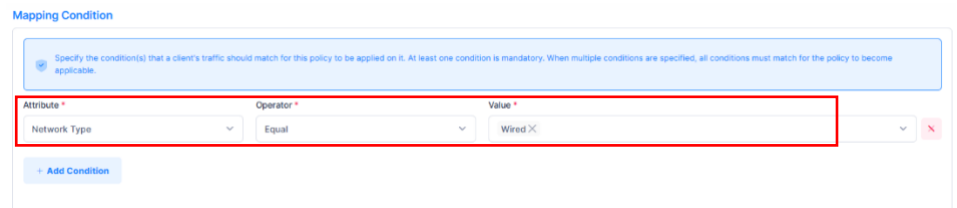
Basic Information

Policy Name: ACMI\_wired

Precedence: 1

Fig. 22: Access Policy Configuration 1

- **Mapping Condition:**
  - ✓ Attribute: Network Type
  - ✓ Operator: Equal
  - ✓ Value: wired



Mapping Condition

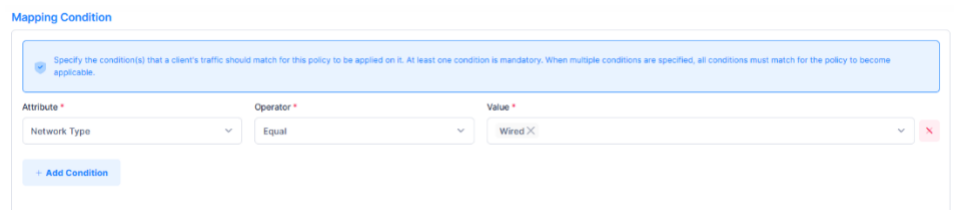
Specify the condition(s) that a client's traffic should match for this policy to be applied on it. At least one condition is mandatory. When multiple conditions are specified, all conditions must match for the policy to become applicable.

Attribute: Network Type Operator: Equal Value: Wired X

+ Add Condition

Fig. 24: Mapping Condition of Access Policy

- **Authentication Method:**



Mapping Condition

Specify the condition(s) that a client's traffic should match for this policy to be applied on it. At least one condition is mandatory. When multiple conditions are specified, all conditions must match for the policy to become applicable.

Attribute: Network Type Operator: Equal Value: Wired X

+ Add Condition

Fig. 25: Authentication Method 1

- ✓ Allowed methods: EAP-TTLS



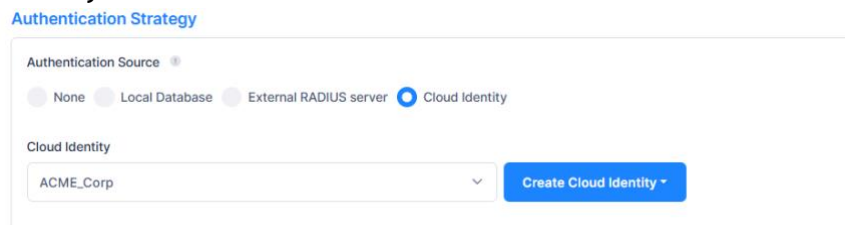
Authentication Method

Allow All EAPs: No

Allowed methods: EAP-TLS EAP-PEAP EAP-TTLS

Fig. 26: Authentication Method 2

- Authentication Strategy:
  - ✓ Authentication Source : Cloud Identity and choose your cloud identity created.



Authentication Strategy

Authentication Source: None Local Database External RADIUS server Cloud Identity

Cloud Identity: ACME\_Corp

Create Cloud Identity

Fig. 26: Authentication Strategy

### 4. Let's test the connection:

- 1- Connect your computer to the switch port you previously defined.
- 2- In the **Network** → **Ethernet** tab on your computer, click **Connect**.

### Application Note

Entra ID Integration with OV10 for Secure Wired and Wi-Fi Authentication



- 3- Enter your credentials (an initial login is required, along with a password reset).

**Reminder:** During your first login to your Microsoft account, a password reset is mandatory.

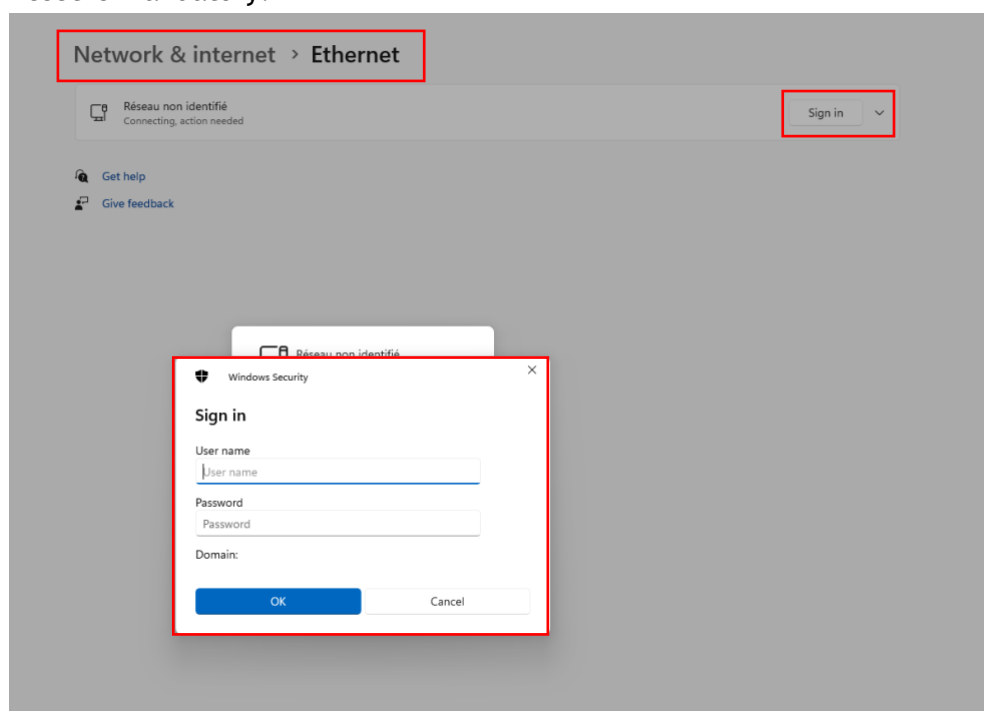


Fig. 27: test connection

We are now connected, as confirmed in the logs for OV10 and Entra ID.

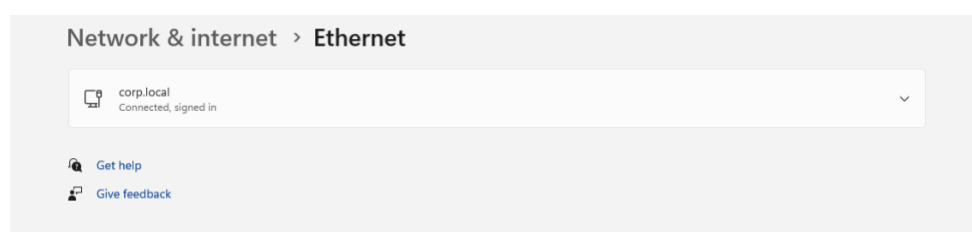


Fig. 28: Successful Connection

## A- In OV

Authentication Record Information					
Basic		Basic		Enforcement Policy	
Device MAC:	8C:8C:AA:E5:C3:0D	Authentication Method:	EAP-TTLS	Service Type:	Framed-User
Device Type:	Employee	Auth Resource:	Cloud-Identity	Access Device SSID:	-
Username:	anonymous	Network Type:	Wired	Port Desc:	Cluster.MGT_HostL_ymlnc0
Authentication Result:	SUCCESSFUL	NAS IP Address:	100.64.65.41	NAS ID:	OOBMNTOR
Reject Reason:	-	NAS Source IP Address:	100.64.65.41	NAS Port ID:	1/1/2
Session Start:	Feb 26, 2025 10:50:41 am	NAS Device MAC:	78-24-59-0F-63-AF	NAS Port Type:	Wired
Session Stop:	Feb 26, 2025 10:53:12 am	SSID:	-	NAS Port:	1002
Session Time:	2Min 31s	Access Policy:	ACME_WIRED	Framed MTU:	1400
Account Terminate Cause:	Port-Error	Web Access Policy:	-	Alcatel Device MAC:	78-24-59-0F-63-AF
Account Session ID:	100.64.65.41_26/02/2025_09:50:40_8c8cae5c30d	Final Access Role Profile:	ACME_Employee	Alcatel Device Name:	OOBMNTOR
Account Multi Session ID:	100.64.65.41_26/02/2025_09:50:40_8c8cae5c30d			Called Station ID:	7824590F63AF
Authentication Type:	802.1X			Authentication Method:	EAP-TTLS
				Alcatel Device Location:	Colombes-Solution-LAB
				Alcatel Access Point Group:	-
				Slot Port:	-
				Roaming Information:	-

Fig. 29: Logs on OV10

## Application Note

Entra ID Integration with OV10 for Secure Wired and Wi-Fi Authentication

## B- In Entra ID,

Sign-in logs

Date	Request ID	Correlation ID	Authentication requirement	Status	Continuous access evaluation	Troubleshoot Event	User	Username	User ID	Sign-in identifier	Session ID	App owner tenant ID	Resource owner tenant ID	User type	Cross tenant access type	Application	Application ID	Resource	Resource ID	Resource tenant ID	Home tenant ID
2/26/2025, 12:11:31 PM	6b9c9c9b-89a0-444a-9f...		Single-factor authentication	Success			employee	employee@ouallina52gmail.onmicrosoft.com	211c0310-92b1-4f5b-97ac-0e6e2710121e	employee@ouallina52gmail.onmicrosoft.com	00228409-5693-a5e8-fc16-e21b923cd3b1	bba1b5ef-5178-40f7-9326-2a9950b6d21b	f8cdef31-a31e-4b4a-93e4-5f571e91255a	Member	None	ACME	f5197be4-73df-4cee-b7b3-3c3baa80fbc6	Microsoft Graph	00000003-0000-0000-c000-000000000000	bba1b5ef-5178-40f7-9326-2a9950b6d21b	bba1b5ef-5178-40f7-9326-2a9950b6d21b
2/26/2025, 12:15:53 PM	6a8cf8ed-71db-4db2-a...		Single-factor authentication	Success			employee														
2/26/2025, 12:15:26 PM	3d0883e6-f64c-46e5-a3...		Single-factor authentication	Success			employee														
2/26/2025, 12:13:18 PM	1457f5cd-445b-482a-a3...		Single-factor authentication	Success			employee														
2/26/2025, 12:09:38 PM	78a67800-aa12-4ac6-b...		Single-factor authentication	Success			employee														
2/26/2025, 12:07:09 PM	a0b7645e-fc11-4a6b-ad...		Single-factor authentication	Success			employee														
2/26/2025, 12:01:27 PM	a7953379-d485-4fc3-b1...		Single-factor authentication	Success			employee														
2/26/2025, 11:51:45 AM	29ebdbb3-266b-466d-8...		Single-factor authentication	Success			employee														
2/26/2025, 11:38:13 AM	1189f123-a215-4598-b0...		Single-factor authentication	Success			employee														
2/26/2025, 11:34:39 AM	d35368fc-5497-4bf3-83...		Single-factor authentication	Success			employee														
2/26/2025, 10:54:09 AM	f6b5a2ee-266f-4b8b-af...		Single-factor authentication	Success			employee														
2/26/2025, 10:50:41 AM	cf5858be-4c97-492b-8d...		Single-factor authentication	Success			employee														
2/26/2025, 10:48:39 AM	8310076f-cf62-49c9-a7...		Single-factor authentication	Success			employee														
2/26/2025, 10:48:39 AM	f9a4c7cb-b3a7-419b-b3...		Single-factor authentication	Success			employee														
2/26/2025, 10:48:39 AM	29a812c4-c117-4710-b4...		Single-factor authentication	Success			employee														
2/26/2025, 10:48:35 AM	a87096ec-7293-47e6-8...		Single-factor authentication	Success			employee														
2/26/2025, 10:48:32 AM	ea640cad-a5c5-4b79-b...		Single-factor authentication	Success			employee														
2/26/2025, 10:45:57 AM	4bd813bd-1f3f-4ae6-84...		Single-factor authentication	Interrupted			employee														
2/26/2025, 10:43:54 AM	4db2eadd-d73c-4f99-8...		Single-factor authentication	Interrupted			employee														
2/26/2025, 10:37:53 AM	d40e5dc9-2304-4fcf-b7...		Single-factor authentication	Failure			employee														
2/26/2025, 10:22:42 AM	a7953379-d485-4fc3-b1...		Single-factor authentication	Failure			employee														
2/26/2025, 10:12:45 AM	3b4b580e-04cd-4e67-8...		Single-factor authentication	Failure			employee														
2/26/2025, 10:12:09 AM	3d18e1d1-a398-4a9a-9...		Single-factor authentication	Failure			employee														
2/26/2025, 9:58:12 AM	0261caee-f595-49a0-92...		Single-factor authentication	Success			lina ouali														

Fig. 30: Logs on Entra ID

## Configure SSID on OV10:

### How to create a new SSID?

From the main menu, select **Wireless > SSIDs**. This will direct you to the SSID management page, where you can view and configure your SSIDs.

On the SSIDs management page, click the **Create SSID** button to begin creating a new SSID. This action will open the "Add new SSID" window.

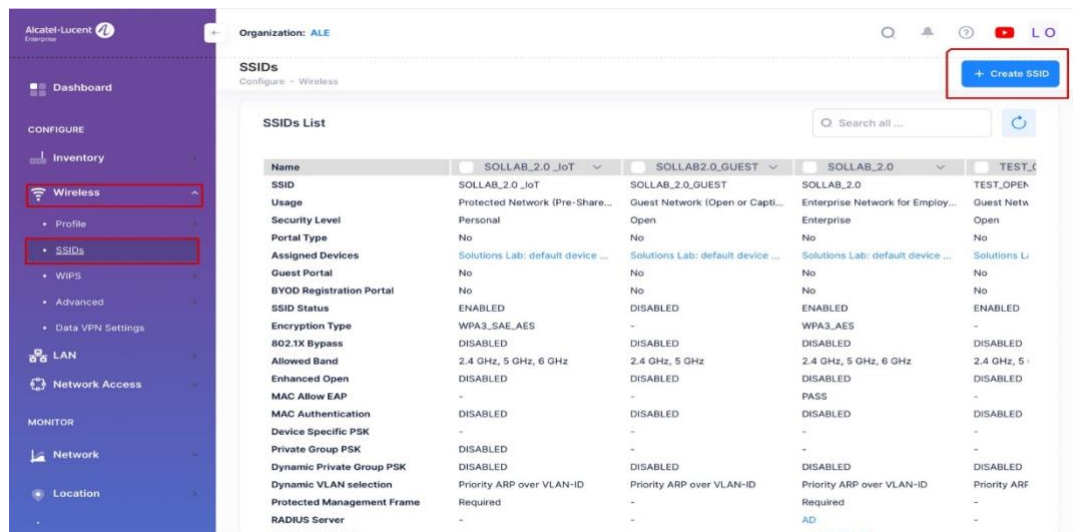


Fig. 31: Create SSID

### Step 1:

1. **Profile Name:** A unique name to identify a wireless service, with multiple SSID services able to share the same profile name.

### Application Note

Entra ID Integration with OV10 for Secure Wired and Wi-Fi Authentication

2. **SSID:** Unique SSID name broadcasted in the air.
3. **Usage:** In SSID usage, select "Enterprise network for employees (802.1X)".

Fig. 32: Create SSID - Usage

4. **Authentication Strategy:** RADIUS Server: UPAMRadiusServer
5. **Authentication Strategy->Access Policy:** Choose configure access policy.

Fig. 33: Authentication Strategy

6. **Authentication Source:**
  - ✓ Cloud Identity.

## Application Note

Entra ID Integration with OV10 for Secure Wired and Wi-Fi Authentication



- ✓ Select the Cloud Identity you created.

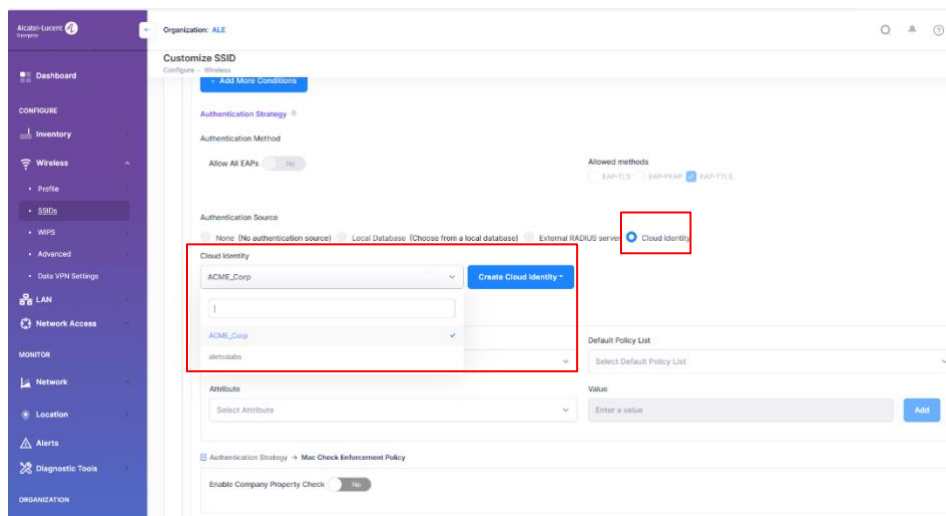


Fig. 34: Authentication Source → Cloud Identity

7. In the Default VLAN/Network section, select "Configure Access Role Attributes".
8. click "Next"

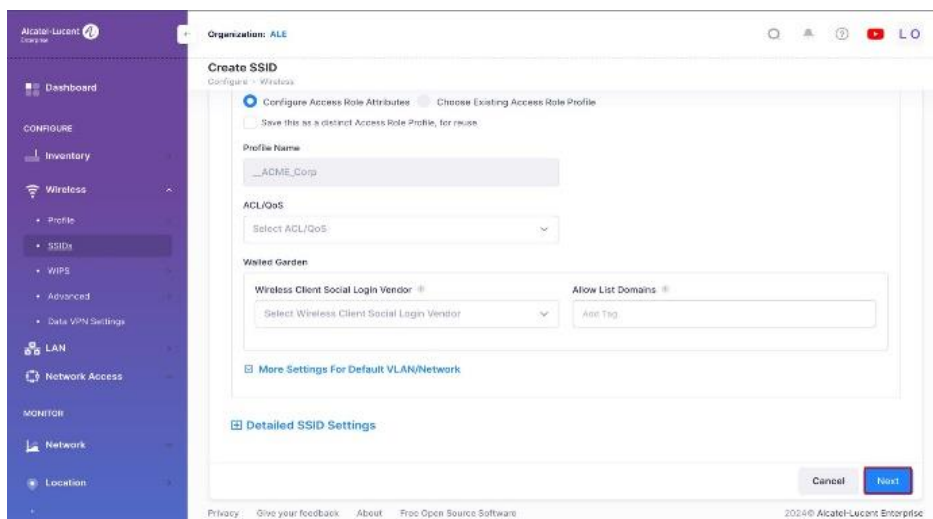


Fig. 35: Configure Access Role Attributes

## Step 2:

Apply the SSID to one site:

- Select your 'site' and all the 'AP groups' you want, then click "Next".

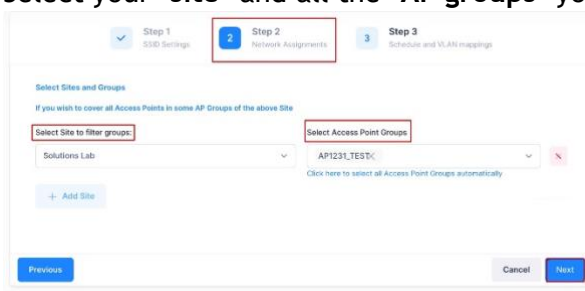


Fig. 36: Create SSID - Step 2

## Application Note

Entra ID Integration with OV10 for Secure Wired and Wi-Fi Authentication

### **Step 3:**

Schedule and VLAN mappings:

- Select your 'VLAN' (tagged/untagged). And click create.

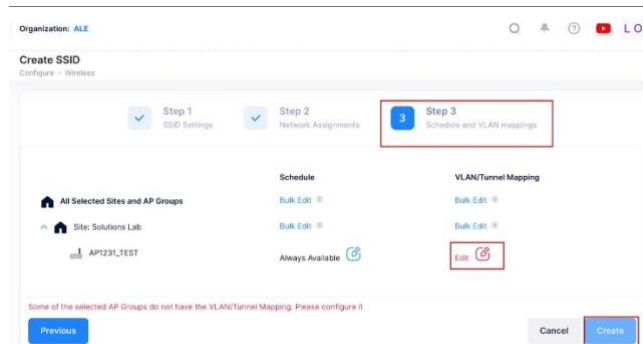


Fig. 37: Create SSID - Step 3- VLAN

- If you have completed the steps up to this point, your SSID has been successfully created. You can now proceed to test the connection.

## **III. Connection Testing**

### **Example of Client-Side Configuration:**

- ✓ If the user has recently been added to your organization, they must perform an initial login to their Microsoft account
  - Access this site to log in to your account:  
<https://login.microsoftonline.com/>
  - Change your password

**If this is your first login, you may see this window after entering your username and temporary password.**

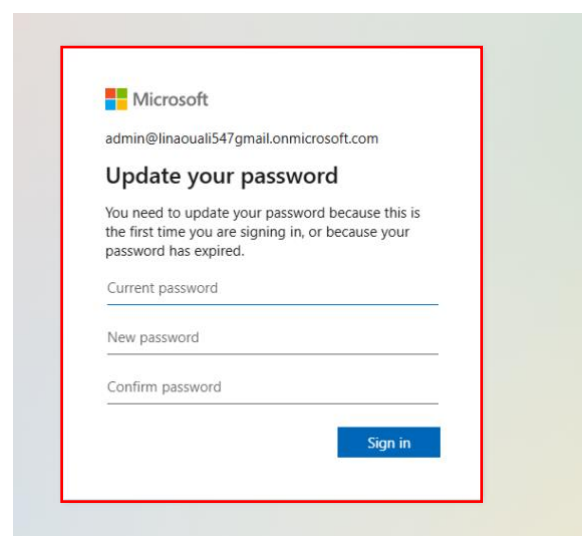


Fig. 38: Change your password in first login

### **Application Note**

Entra ID Integration with OV10 for Secure Wired and Wi-Fi Authentication



- ✓ If not, enter your account username and password, and you will be connected to Wi-Fi.

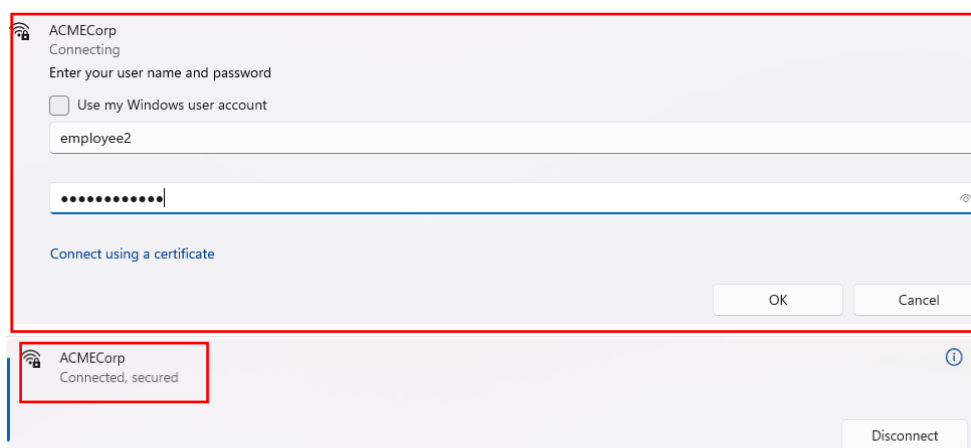


Fig. 39: Successful Connection

- ✓ To view the authentication logs, go to: **Network → Access Records → Authentication Record.**
- ✓ It can be seen in the logs that the user was authenticated using EAP-TTLS.

Authentication Record Information

Basic		Basic		Enforcement Policy	
Device MAC:	64:9C:58:E7:84:A7	Authentication Method:	EAP-TTLS	Service Type:	Framed-User
Device Type:	Employee	Auth Resource:	Cloud-Identity	Access Device SSID:	ACMECorp
Username:	employee2	Network Type:	Wireless	Port Desc:	ACMECorp
Authentication Result:	SUCCESSFUL	NAS IP Address:	192.168.201.56	NAS ID:	ACMECorp
Reject Reason:	-	NAS Source IP Address:	100.64.64.63	NAS Port ID:	wifi-5G
Session Start:	Dec 30, 2024 4:35:08 pm	NAS Device MAC:	DC:08:56:00:2D:B0	NAS Port Type:	Wireless
Session Stop:	Dec 30, 2024 4:37:13 pm	SSID:	ACMECorp	NAS Port:	3
Session Time:	2Min 5s	Access Policy:	__ACMECorp	Framed MTU:	1400
Account Terminate Cause:	User-Request	Web Access Policy:	-	Alcatel Device MAC:	DC:08:56:00:2D:B0
Account Session ID:	192.168.201.56_30/12/2024_16:34:36_64bc58e784a7	Final Access Role Profile:	__ACMECorp	Alcatel Device Name:	AP1231_L
Account Multi Session ID:	192.168.201.56_30/12/2024_16:34:36_64bc58e784a7			Called Station ID:	DC0856002DB0:ACMECorp
Authentication Type:	802.1X			Authentication Method:	EAP-TTLS
				Alcatel Device Location:	2c:fa:a2:9a:62:8f1/1/3
				Alcatel Access Point Group:	AP1231_TEST
				Slot Port:	-
				Roaming Information:	-

Close

Fig. 40: Logs on OV10

## Application Note

Entra ID Integration with OV10 for Secure Wired and Wi-Fi Authentication





# Conclusion

In this application note, we have provided a comprehensive approach to integrating Entra ID, a cloud-based identity management solution, with the OV10 platform, a robust enterprise network management solution, for secure authentication across wired and Wi-Fi networks. By leveraging Entra ID's centralized identity management capabilities and OV10's network configuration tools, organizations can streamline access management, enhance security, and eliminate the complexities associated with on-premises authentication systems.

Key takeaways from this integration include:

- ✓ **Centralization and Efficiency:** Simplified user management through a cloud-based integration.
- ✓ **Enhanced Security:** Improved network protection through modern protocols and optimized configurations.
- ✓ **Fully Cloud-Based Solution:** Improved operational efficiency and cost-effectiveness by reducing the need for physical infrastructure and enabling seamless remote management.

By implementing the steps detailed in this guide, enterprises can optimize network authentication processes, enhance security, and provide a user-friendly experience. This integration highlights the synergy between cloud identity management and enterprise network management tools to meet evolving connectivity and security needs.