Tech Tips – Using Alcatel-Lucent OmniVista 2500 UPAM RADIUS Server with third-party switches

Alcatel·Lucent Enterprise

Table of Contents

Introduction

Unified Policy Authentication Manager (UPAM) is a unified access management platform for the Alcatel-Lucent OmniSwitch® and Alcatel-Lucent OmniAccess® Stellar Access Points (APs). UPAM supports both a built-in captive portal server and a Remote Authentication Dial-In User Service (RADIUS) Server and can be used to implement multiple authentication methods, such as MAC authentication, 802.1X authentication and captive portal authentication. User profiles can be supported in the Alcatel-Lucent OmniVista® Network Management System (NMS) database or on external servers. UPAM can use its local database, an external Active Directory (AD)/Lightweight Directory Access Protocol (LDAP) server, or an external RADIUS Server as the authentication source.

Using the Unified Access application in OmniVista 2500 or OmniVista Cirrus NMS allows the implementation of unified security rules on OmniSwitches and OmniAccess Stellar APs. This provides coherence and unification of security rules on LAN and WLAN equipment. However, you might be required to configure the same policies on third-party network devices which do not support ALE's User Network Profiles (UNPs).

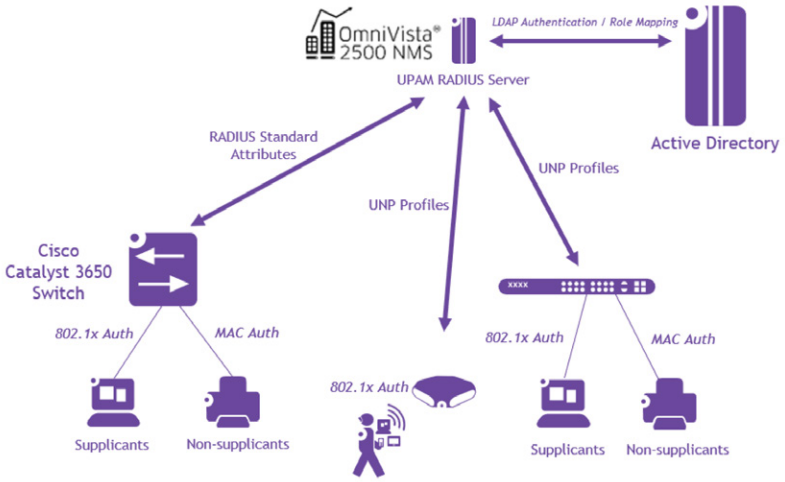
In this document we will cover one of the use cases where an OmniVista 2500 UPAM application is used as the RADIUS Server, an AD is used as the external authentication source and there is a hybrid solution of OmniAccess Stellar APs, OmniSwitch and third-party switches. An LDAP Role Mapping feature will also be used to assign Access Role Profile (ARP) and Policy List based on AD attributes. In this case, the AD "memberOf" attribute, which is the user's security group, will be used to assign the user to the correct UNP.

We can utilise standard or Vendor Specific Attributes (VSAs) to communicate between UPAM and third-party devices which allows for user Authentication, Authorization and Accounting (AAA) features. In this case, for dynamic VLAN assignment, the attributes which can be of specific benefit are below:

Attribute number	Attribute name	Description
64	Tunnel-Type	Protocol type of the tunnel. The value is fixed as 13, indicating VLAN. (Type: Integer)
65	Tunnel-Medium-Type	Medium type used on the tunnel. The value is fixed as 6, indicating Ethernet. (Type: Integer)
81	Tunnel-Private-Group-ID	Tunnel private group ID, which is used to deliver user VLAN IDs. (Type: String)

Topology setup

The topology used for this test case includes a hybrid solution made up of an OmniSwitch, OmniAccess Stellar APs and a Cisco Catalyst Switch as the access devices. OmniVista 2500 NMS will be used for most of the configuration and Active Directory will be used as the authentication source for 802.1x supplicants.



Hardware setup

The table below lists the devices used in this setup and the relevant release version.

Device/Appliance	Attribute name
OmniAccess Stellar AP1201	3.0.4.1030
OmniSwitch 6560-P24Z24	8.9.107.R02
OmniVista 2500	4.7R1 GA (Build 30)
Cisco Catalyst C3560-48PS	12.2(44)SE
Windows Server – Active Directory	Windows Server 2022

Pre-requisites

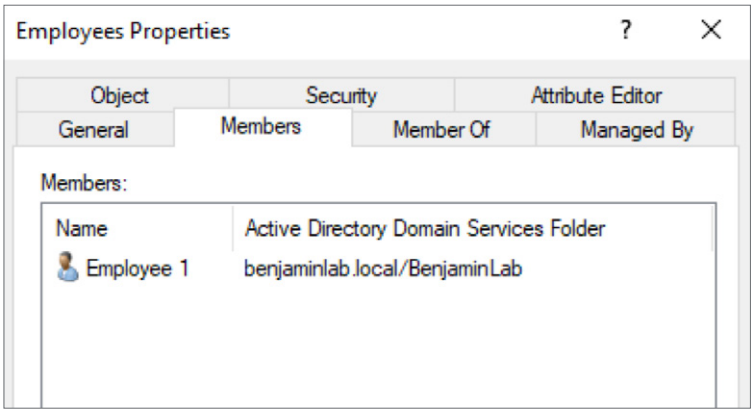
The below pre-requisites should be configured before implementation. We will not cover the configuration as part of this document:

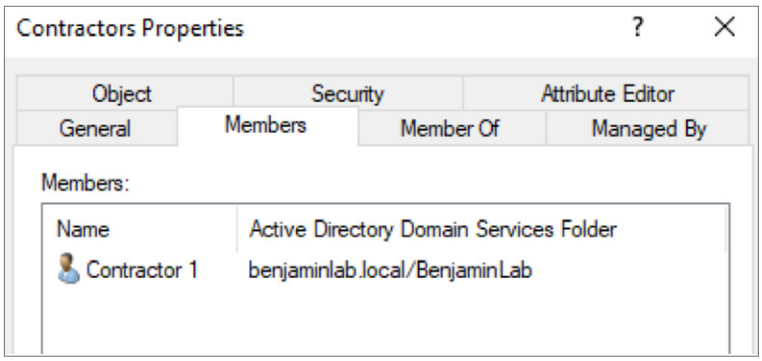
- The DHCP Server should be available and configured for the VLANs which will be used and mentioned in the Implementation Plan section
- IP interfaces, routing, DNS and other settings should be pre-configured as per the required addressing scheme. Below is the IP addressing for the devices used in this implementation:

Device	IP Address
OmniVista 2500 NMS	172.26.10.131
Cisco Switch	192.168.117.1

- The OmniSwitch and OmniAccess Stellar AP should be managed and provisioned in the OmniVista 2500 NMS
- The OmniAccess Stellar AP should be added to an AP Group

- Active Directory should be configured with the required security groups and users. For this implementation, we are using two security groups: Employees and Contractors. Two users were also created, employee1 and contractor1, and were added to the Employees and Contractors security groups, respectively, as shown below:





Implementation plan

We will implement a unified policy that will authenticate network devices depending on support of 802.1x authentication. Where a non-supplicant device is connected, it will use MAC authentication. The MAC addresses used for authentication are stored in the UPAM "Company Property". Once the user is connected using an 802.1x supported device, they will be prompted for credentials. UPAM will verify the credentials with AD server and will perform Role Mapping if the credentials are valid. AD will return the user's memberOf attribute which will be used by UPAM to map the user to the assigned UNP and at the same time send the RADIUS standard attribute for dynamic VLAN assignment. These attributes will be ignored by the OmniSwitch and OmniAccess Stellar devices, as these devices will use the UNP profile. The Cisco switch will use the RADIUS standard attributes to map the user to the correct VLAN.

Step 1: Create VLANs on all switches and AP Ports

- We will use the below VLANs on all switches and they should be tagged on all ports to OmniAccess Stellar APs:

VLAN ID	Name
100	Management
200	Employees
300	Contractors
400	Non-supplicants
999	Restricted

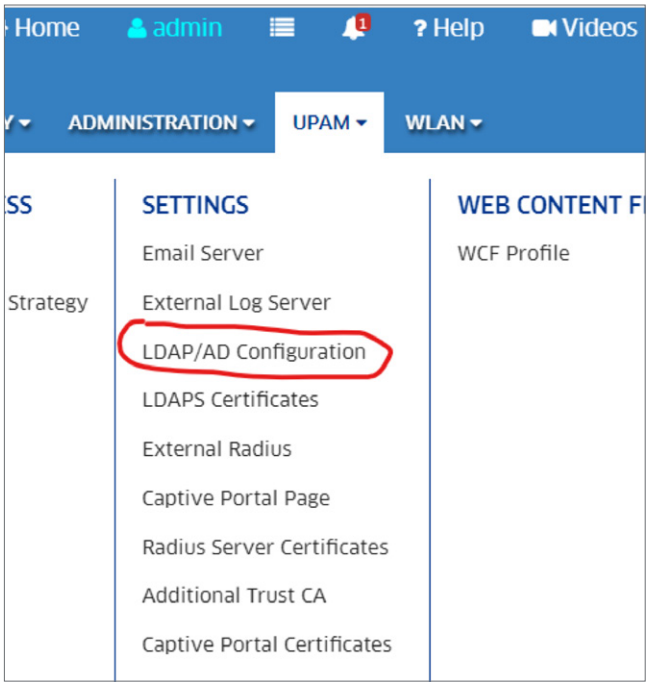
- Cisco switch configuration:

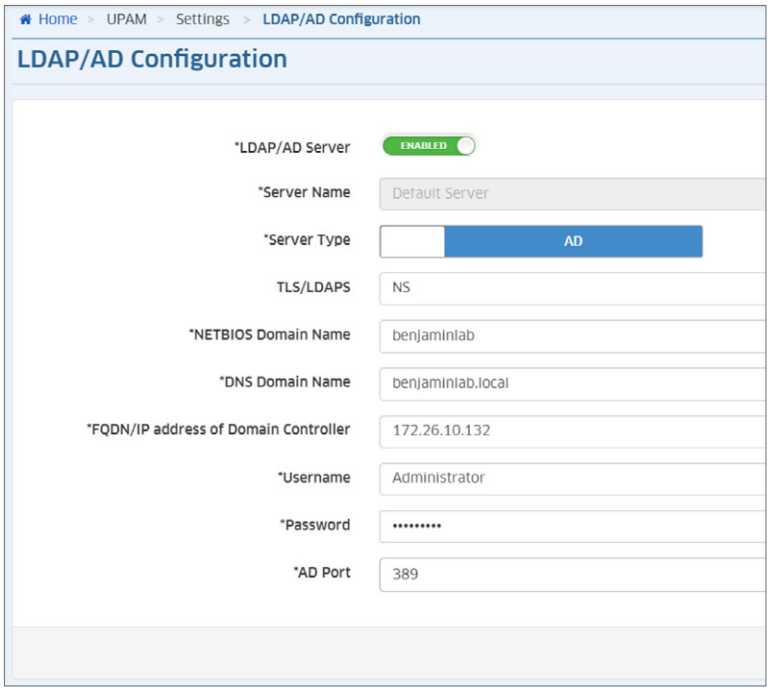
```
vlan 100
 name Management
!

vlan 200
 name Employees
!

vlan 300
 name Contractors
!

vlan 400
 name Non-supplicants
!

vlan 999
  name Restricted
```

- Ensure that the DHCP scope is created for the above VLANs based on any addressing scheme, and that IP interfaces and routing are configured.

Step 2: Active Directory Configuration

- Next step is to integrate Active Directory with OmniVista 2500 NMS. Navigate to the below settings and input the required fields:
  - UPAM -> Settings -> LDAP/AD Configuration

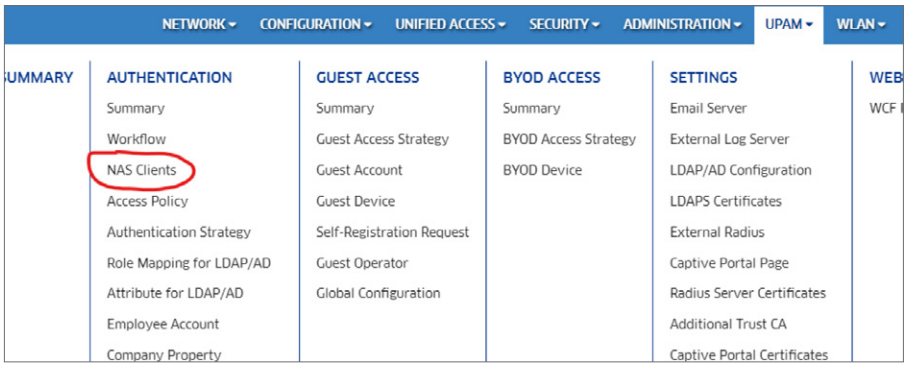


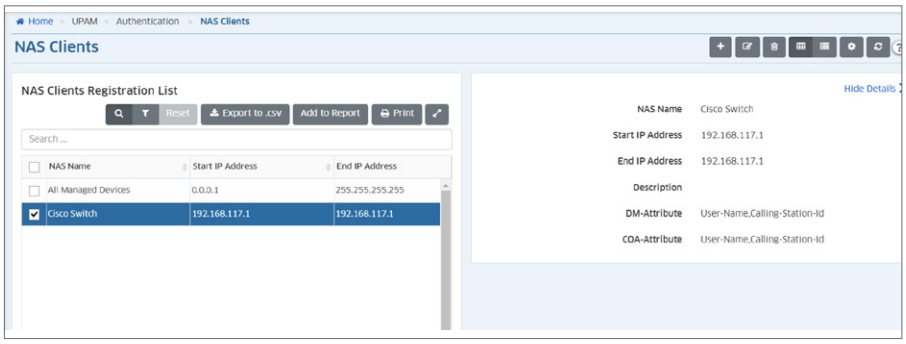


- Test the connection to make sure it is working.

Step 3: Configure the third-party switches as NAS Clients

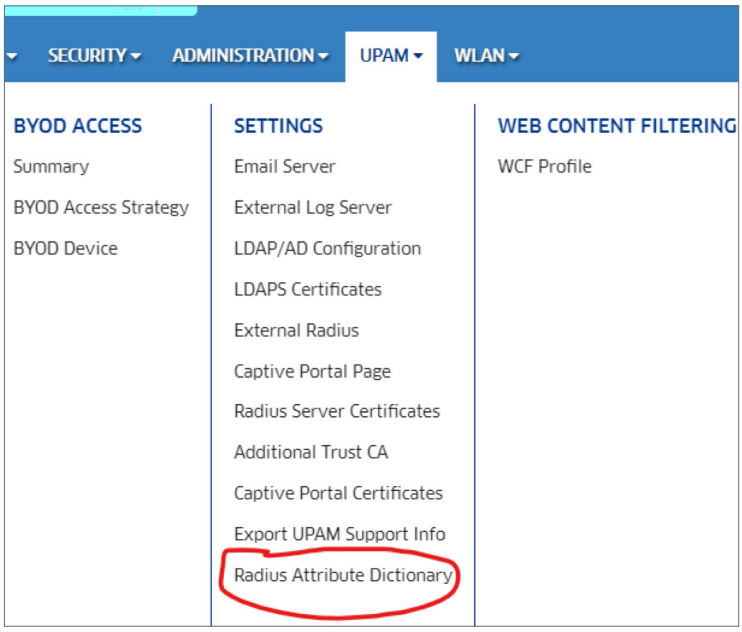
- Navigate to the menu below to configure the third-party switch as a NAS Client and input the required fields:
  - UPAM -> Authentication -> NAS Clients
- Add the management IP address of the switch (or range of IP addresses if using multiple switches) with the appropriate attributes





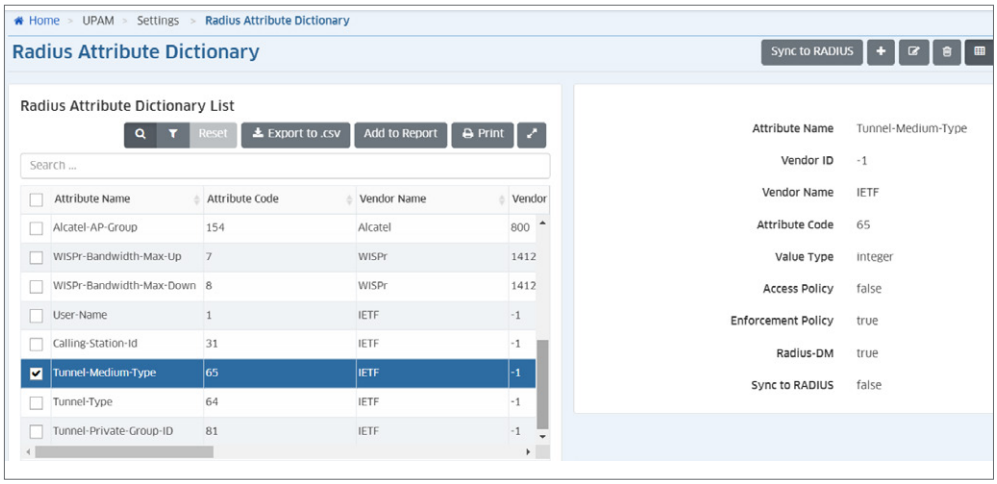
Step 4: Configure RADIUS attributes for dynamic VLAN assignment

- Navigate to the below menu to configure the RADIUS standard attributes which will be used for dynamic VLAN assignment:
  - UPAM -> Settings -> RADIUS Attribute Dictionary



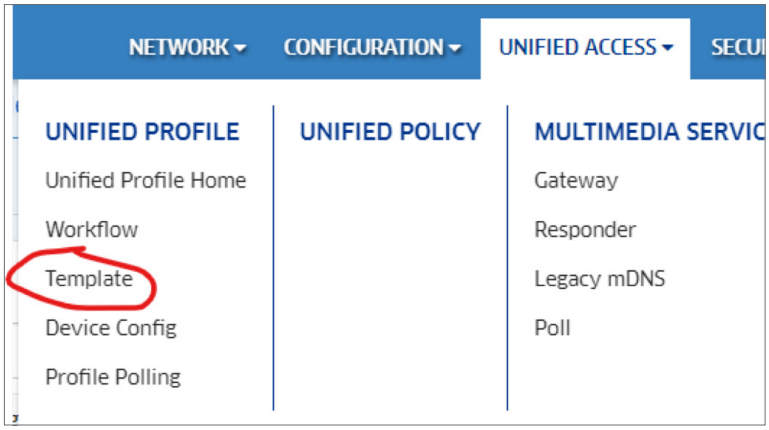
- Add the below three RADIUS attributes as IETF attributes and add them to following locations: Enforcement Policy and Radius-DM

Attribute number	Attribute name	Description
64	Tunnel-Type	Protocol type of the tunnel. The value is fixed as 13, indicating VLAN. (Type: Integer)
65	Tunnel-Medium-Type	Medium type used on the tunnel. The value is fixed as 6, indicating Ethernet. (Type: Integer)
81	Tunnel-Private-Group-ID	Tunnel private group ID, which is used to deliver user VLAN IDs. (Type: String)



Step 5: Create Access Role Profile for each UNP and apply to all switches and AP Group with the specific VLAN

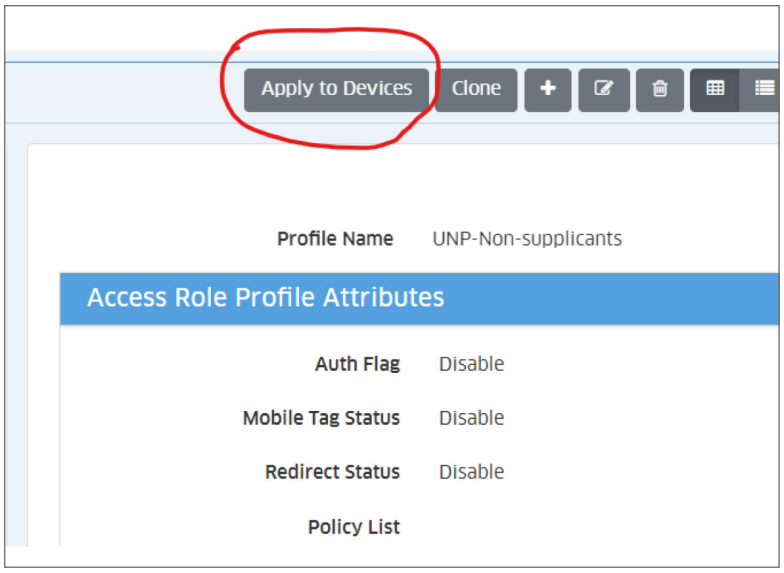
- Navigate to the below settings page to configure the Access Role Profiles (ARP) which will be used for each category of user:
  - Unified Access -> Unified Profile -> Template -> Access Role Profile

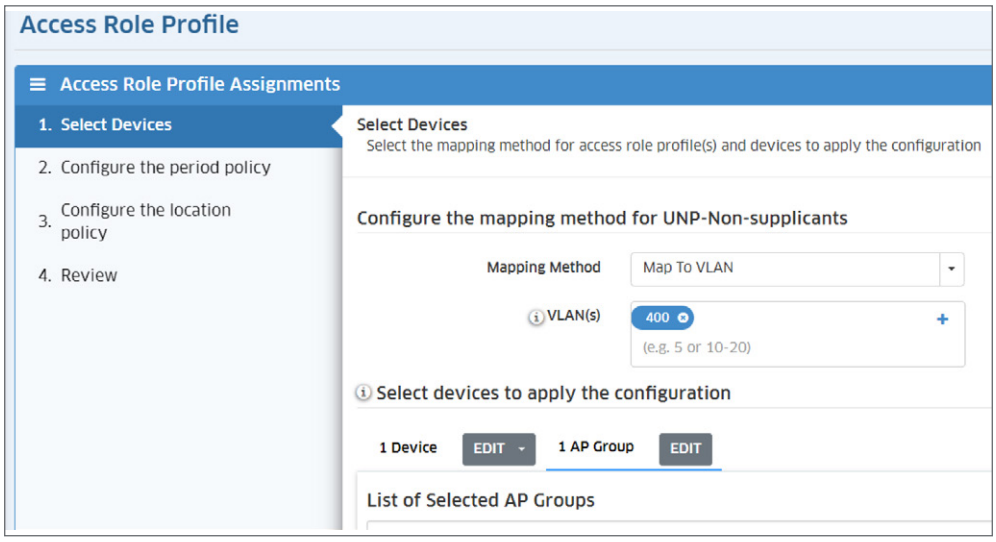


- Create an ARP for each UNP Profile that will be used. In our implementation, we will use the below UNPs:

VLAN ID	Name	UNP
200	Employees	UNP_Employees
300	Contractors	UNP_Contractors
400	Non-supplicants	UNP_Non-supplicants
999	Restricted	UNP_Restricted

- We will keep default settings of the UNP, but specific attributes such as bandwidth control settings can be configured here
- Then, we will apply these UNPs to the OmniSwitch and OmniAccess Stellar APs in our topology. Select each UNP and click on "Apply to Devices" and Map to the UNP VLAN and apply to all OmniSwitch access switches and AP Groups. Do not apply this to third-party switches.

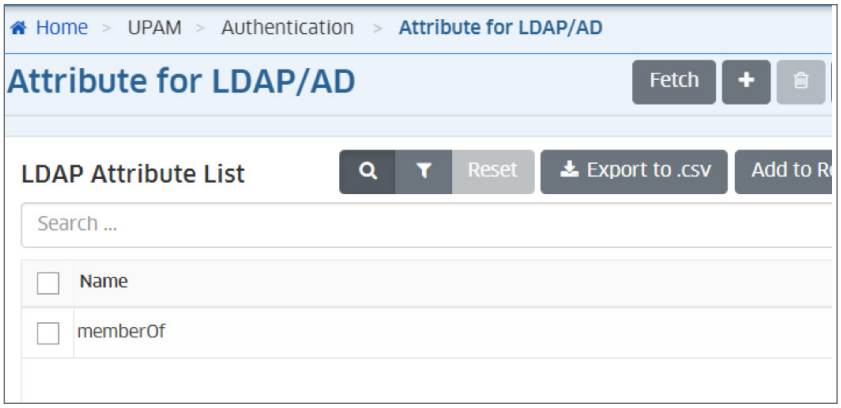




- Here we have mapped the UNP "UNP_Non-supplicants" to the VLAN 400 and applied it to the OmniSwitch and the AP Group of the OmniAccess Stellar AP

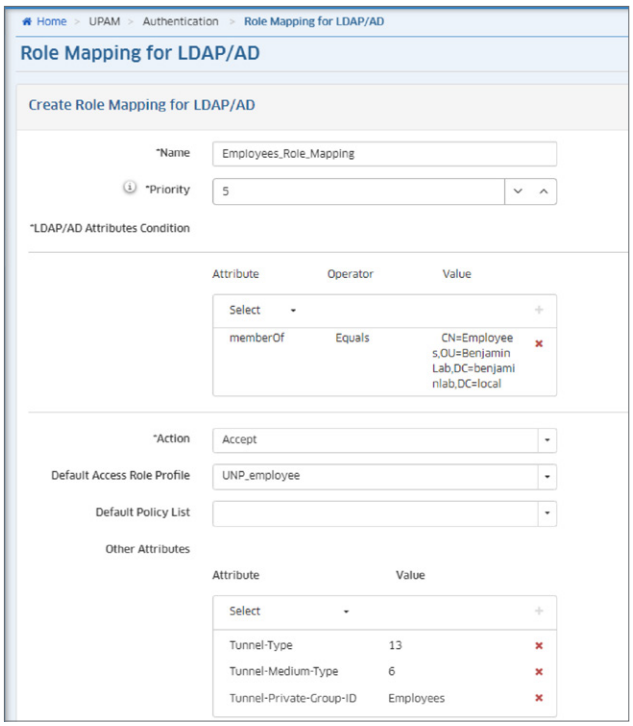
Step 6: Create LDAP/AD Attribute "memberOf"

- Navigate to the below menu to configure the LDAP attribute "memberOf" which will be used for Role Mapping the user to the correct UNP. You can fetch directly from AD, or add it manually.
  - UPAM -> Authentication -> Attribute for LDAP/AD



Step 7: Configure Role Mapping for LDAP/AD

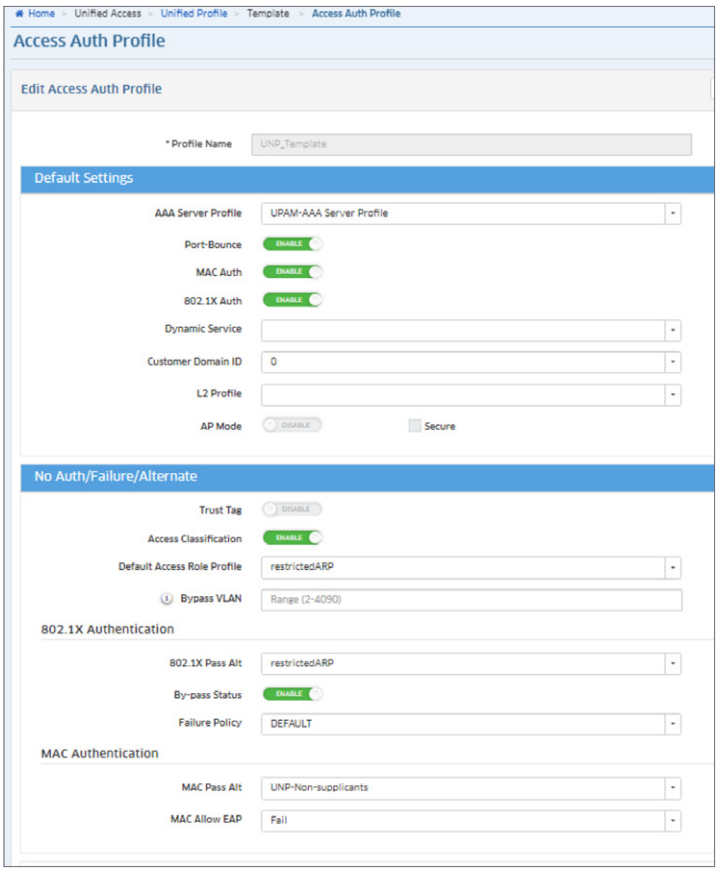
- Navigate to the below settings menu to configure Role Mapping for each category of user such as Employees and Contractors
  - UPAM -> Authentication -> Role Mapping
- Configure Role Mapping based on "memberOf" attribute for each type of security group required (Employees, Contractors). For example:
  - LDAP/AD attributes condition:
  - Attribute: memberOf
  - Operator: Equals
  - Value: CN=Employees,OU=lab,DC=lab,DC=local
  - Action: Accept
  - Default Access Role Profile: UNP_Employee
  - Other attributes:
    - Tunnel-Type = 13 (Which is the type for VLAN)
    - Tunnel-Medium-Type = 6 (which is the type for 802)
    - Tunnel-Private-Group-ID = VLAN Name or VLAN ID which will be mapped to this user type



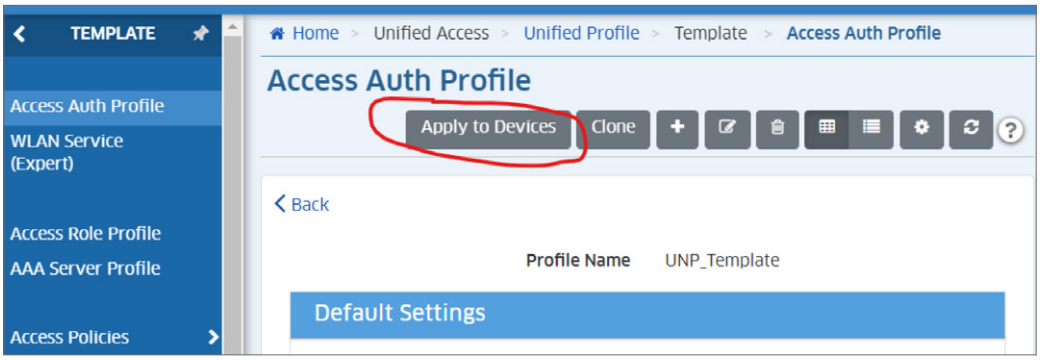
Step 8: Create and apply an Access Authentication Profile for the OmniSwitch

- Navigate to the below settings menu to create an Access Authentication Profile which contains the type of authentication (802.1x and MAC Auth) that will be applied to the OmniSwitch:
  - Unified Access -> Unified Profile -> Template -> Access Auth Profile
- Create a new Access Auth Profile by clicking the '+' button
- Set a name for the profile and configure the settings depending on your requirements. Select the default "UPAM-AAA Server Profile" which uses UPAM as the RADIUS Server for both 802.1x and MAC authentication. The default ARP and the 802.1x Pass Alt UNP will be the restricted UNP. The user shall be assigned a Pass-Alternate UNP in case the 802.1X authentication does not result in a valid UNP for the pass branch. We will assign the "UNP_Non-supplicants" to the MAC Pass Alt, which will be assigned after passing authentication. Bypass option will be enabled and the Failure Policy will be set to the default.

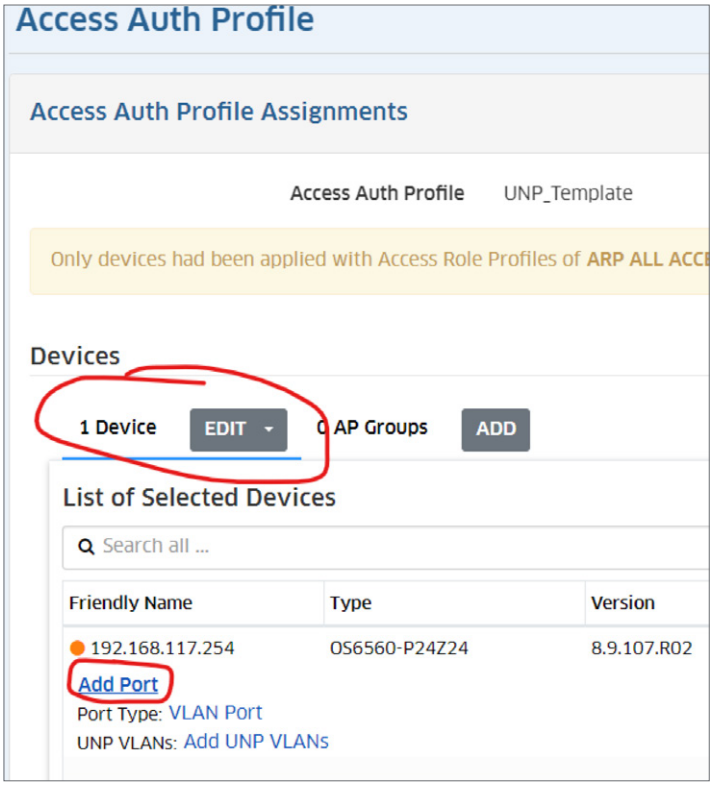
The failure policy sets the authentication method used if 802.1X authentication fails. Finally, the "MAC Allow EAP" option will be set to Fail. This allows 802.1x (EAP frame) authentication if the supplicant fails MAC authentication.



- Once created, we can then apply this Access Auth Profile to the switchports by clicking the "Apply to Devices" button:

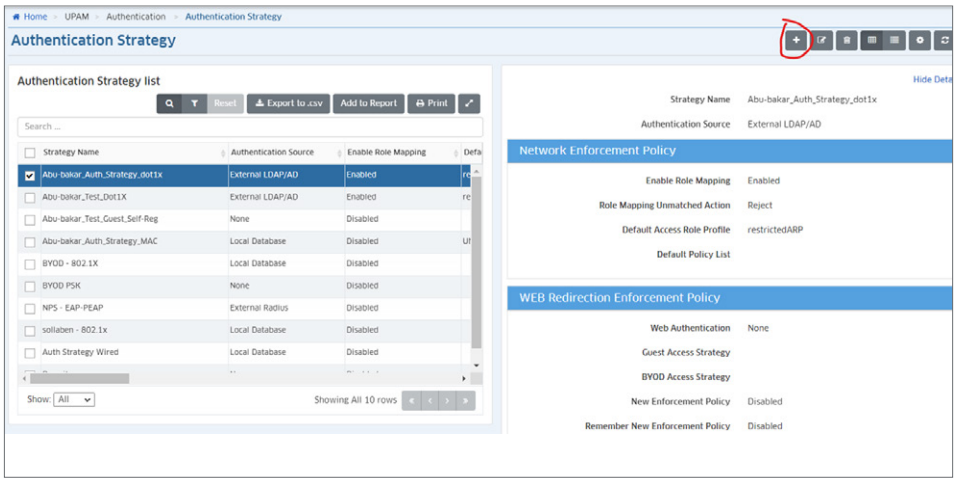


- Select the OmniSwitch and the switchports where the Access Auth Profile will be applied from the Switch Picker:



Step 9: Create an Authentication Strategy for the third-party switch with LDAP as Authentication Source for 802.1x Authentication

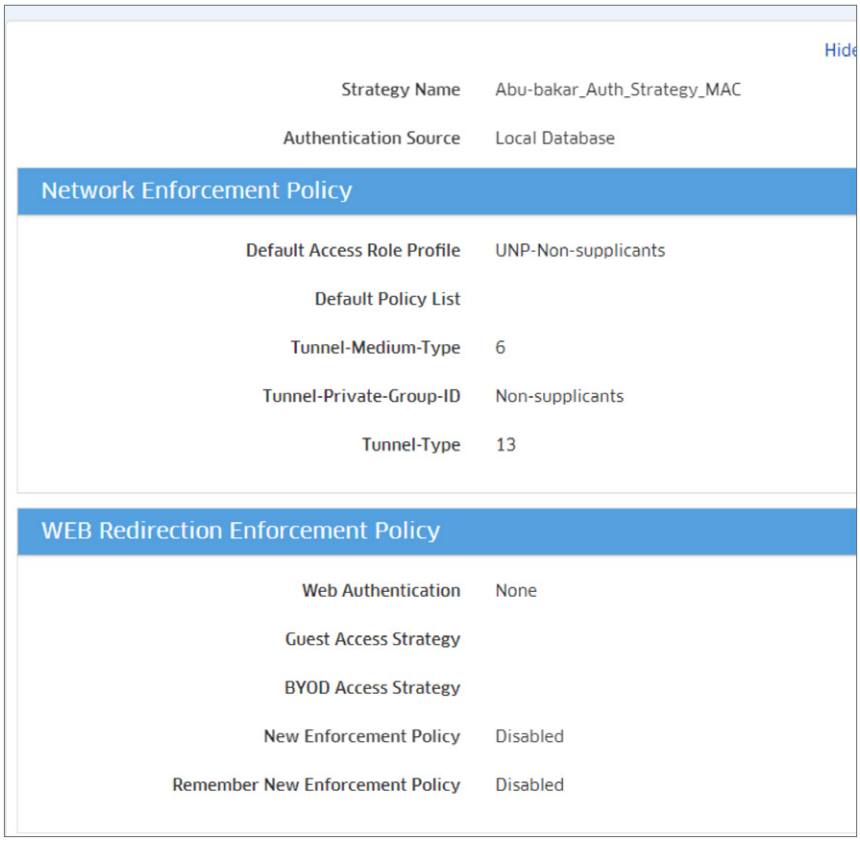
- Navigate to the below settings menu to configure an authentication strategy for 802.1x authentication that will be used by the third-party switch:
  - UPAM -> Authentication -> Authentication Strategy
- Click the '+' button to create a new strategy



- Select "External LDAP/AD" as Authentication Source
- Enable Role Mapping
- Select "Reject" for "Role Mapping Unmatched Action"
- Select the restricted UNP as "Default Access Role Profile"

Step 10: Create an Authentication Strategy for the third-party switch with Local Database as Authentication Source for MAC Authentication

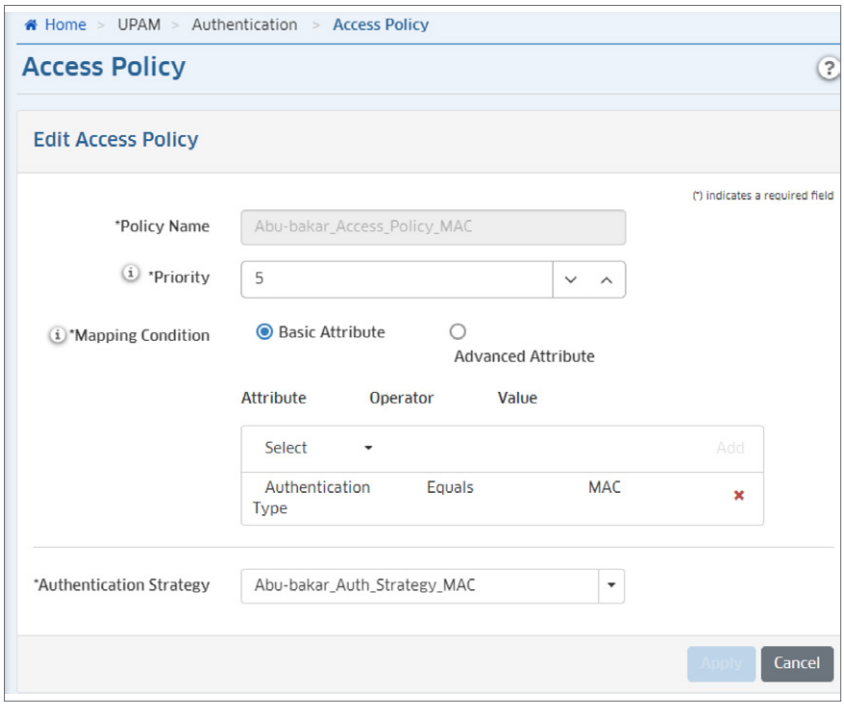
- Navigate to the below settings menu to configure an authentication strategy for MAC authentication which will be used by the third-party switch:
  - UPAM -> Authentication -> Authentication Strategy
- Click the '+' button to create a new strategy



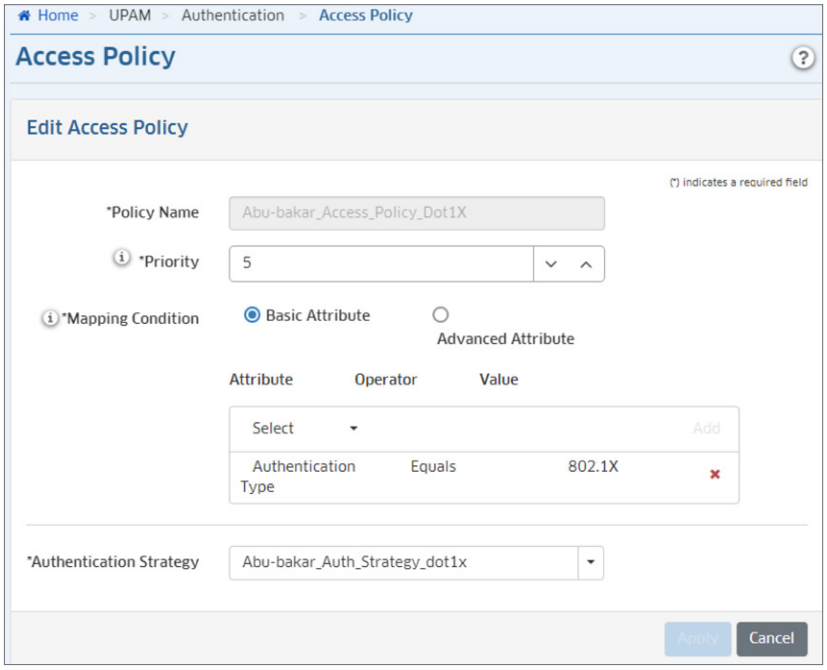
- Select Local Database as Authentication Source and "UNP_Non-supplicants" as Default Access Role Profile which will be assigned to the authenticated devices. Finally, enter the RADIUS Standard attributes which will be used for dynamically assigning the device to the "Non-supplicants" VLAN after successful authentication.

Step 11: Create Access Policies for the third-party switch for mapping to the authentication strategies created in steps 9 and 10

- Navigate to the below settings menu to configure the Access Policies which will be used to map the different authentication types to the authentication strategies created earlier:
  - UPAM -> Authentication -> Access Policy
- Click the '+' button to create a new Access Policy and create an Access Policy for 802.1X Authentication. For example:
  - Policy Name: AAA_802.1X_Auth
  - Priority: 5
  - Mapping Condition:
  - Attribute: Authentication Type
  - Operator: Equals
  - Value: 802.1X
  - Authentication Strategy: Select Authentication Strategy created in step 9
  - Click Apply

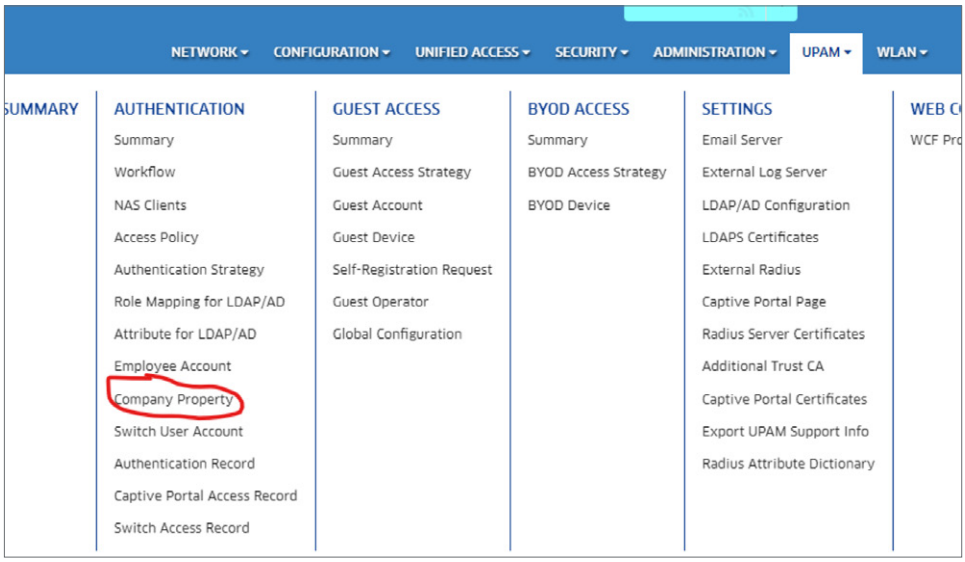


- Click the '+' button to create a new Access Policy and create an Access Policy for MAC Authentication. For example:
  - Policy Name: AAA_MAC_Auth
  - Priority: 5
  - Mapping Condition:
  - Attribute: Authentication Type
  - Operator: Equals
  - Value: MAC
  - Authentication Strategy: Select Authentication Strategy created in step 10

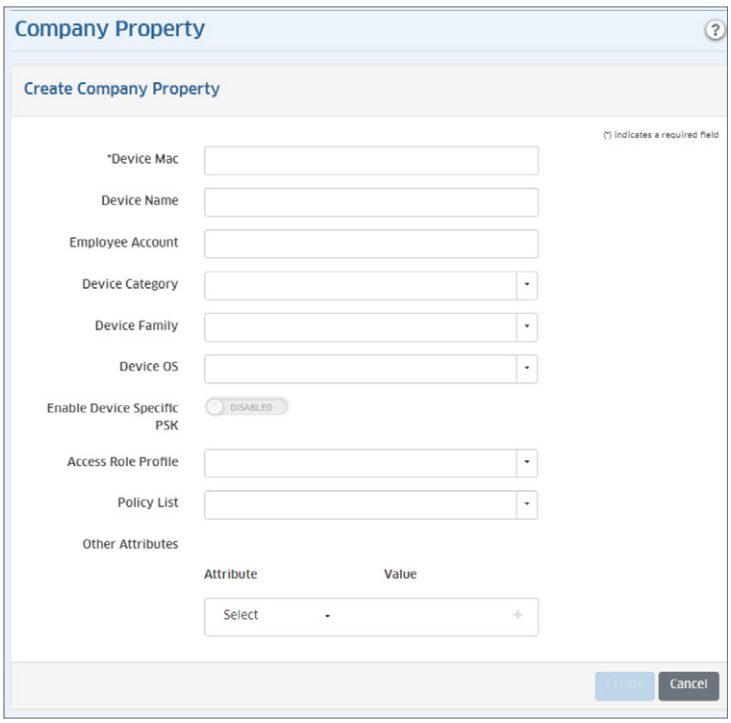


Step 12: Add the MAC Address of non-supplicants to Company Property

- Navigate to the below settings menu to add the non-supplicant devices' MAC Addresses to the UPAM Database
  - UPAM -> Authentication -> Company Property



- Click the '+' button to add the MAC Addresses individually. You may also bulk import the list of MAC addresses using a template by clicking the 'import' button.
- Enter the MAC address and keep the default settings. These settings can be modified depending on your requirements.



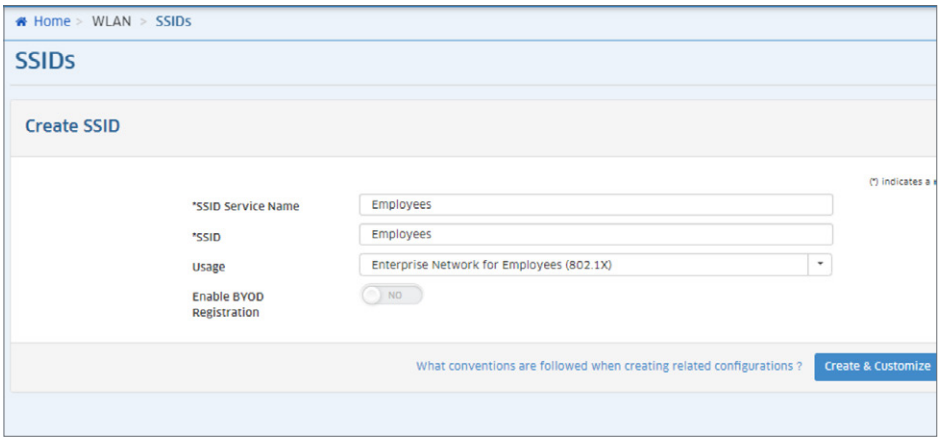
Step 13: Configure the third-party switch for 802.1x and MAC Authentication

- Cisco switch configuration:

```
aaa new-model
!
aaa group server radius OV2500
 server 172.26.10.131 auth-port 1812 acct-port 1813
!
aaa authentication dot1x default group OV2500
aaa authorization network default group OV2500
aaa accounting dot1x default start-stop group OV2500
!
dot1x system-auth-control
!
interface FastEthernet0/2
 switchport mode access
 dot1x pae authenticator
 dot1x port-control auto
 dot1x host-mode multi-host
 dot1x mac-auth-bypass
!
interface Vlan100
 ip address 192.168.117.1 255.255.255.192
!
ip default-gateway 192.168.117.62
!
radius-server host 172.26.10.131 auth-port 1812 acct-port 1813 key xxxxxx
radius-server vsa send authentication
```

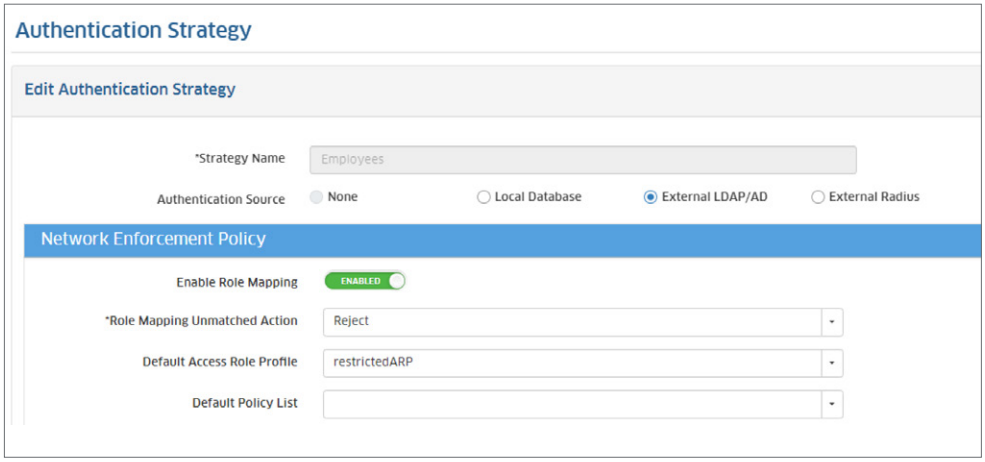
Step 14: Create an Employee SSID with 802.1X Authentication

- Navigate to the below settings menu to create a new Employee SSID with 802.1x authentication
  - ¬ WLAN -> SSID
- In the wizard page, enter the SSID Name and select the template for "Enterprise Network for Employees (802.1X)" as shown below:

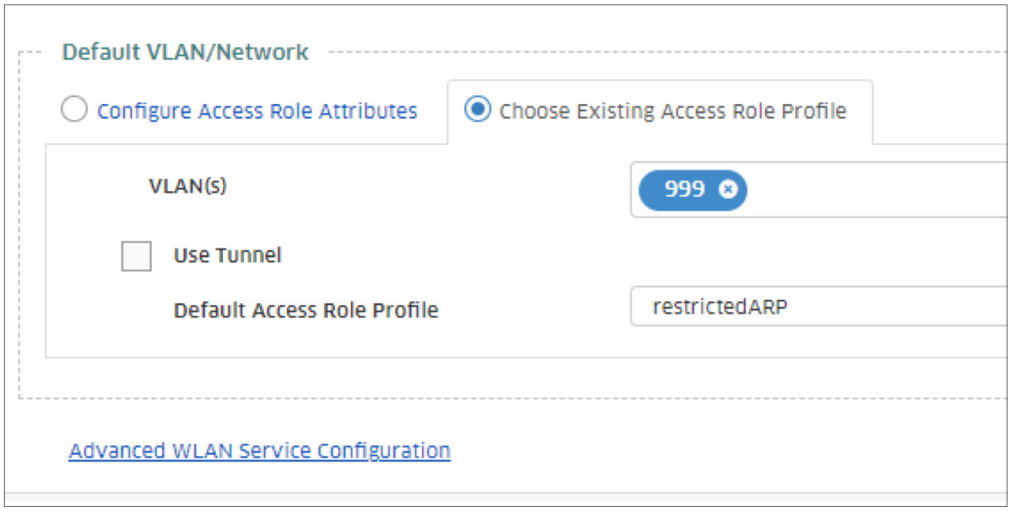


- Click on "Create & Customize"
- In Authentication Strategy, Click Advanced Configuration:

- Configure the below settings:
  - Authentication Source: External LDAP/AD
  - Enable Role Mapping
  - Select “Reject” for “Role Mapping Unmatched Action”
  - Select the Restricted UNP as Default Access Role Profile



- In Default VLAN/Network, input the default VLAN for the Restricted UNP. You may choose the existed ARP created earlier, or create a new one.



- Click “Save and Apply to AP Group”. Then choose the “AP Group” for the OmniAccess Stellar AP to which you wish to apply this configuration.

Additional resources

[1] OV 2500 NMS-E 4.7R1 User Guide (Rev. B)

[2] RFC2868 - RADIUS Attributes for Tunnel Protocol Support - https://www.ietf.org/rfc/rfc2868.txt

Summary

This document provides the implementation steps required to perform dot1x and MAC Authentication on a mixed-vendor infrastructure based on Alcatel-Lucent Enterprise and third-party switches using OmniVista 2500 NMS UPAM as the RADIUS Server. Keep in mind that this implementation would be much simpler when using an OmniSwitch, OmniAccess Stellar APs and OmniVista 2500 or OmniVista Cirrus unified infrastructure solution.

Alcatel·Lucent Enterprise