Alcatel-Lucent Enterprise - Stellar

Introduction

This document describes the configuration of the equipment below with Hotspot Manager platform :

Alcatel·Lucent Enterprise

OAW-AP1221
Validated versions :
4.0.3.3067
3.0.6.1041

We consider here that you already installed or have access to your Hotspot Manager server with necessary FQDNs registered and that all necessary ports are opened (80, 443, 1812, 1813...)
We'll use the URL examples below in this guide, **you must adapt what's in red to match your FQDN**.
The backend will be accessible on **wifi**-admin.**example.com**.
The hotspot will be accessible on **wifi.example.com**/hotspot.php.

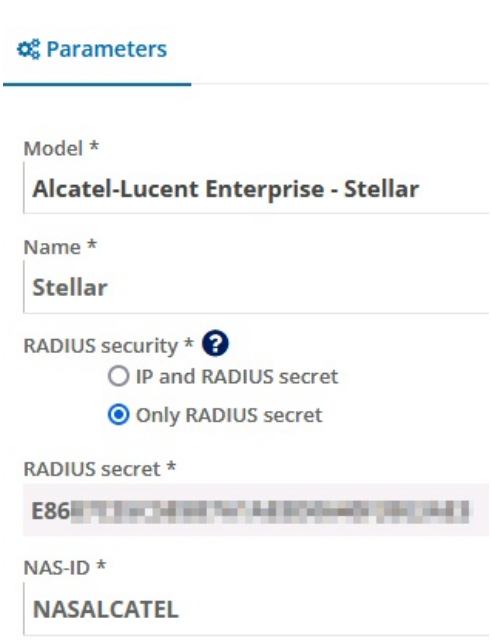
Important : Your equipments (access controllers and/or access points) and Hotspot Manager must be configured on the same timezone. This is to avoid shifts in the timestamp of sessions displayed in Hotspot Manager.

Configuration of Hotspot Manager

Connect to your Hotspot Manager backend (example : https://wifi-admin.example.com).

A. Add the controller in Hotspot Manager

Under **Configurations -> Access Controllers**, click on **Add an access controller.**



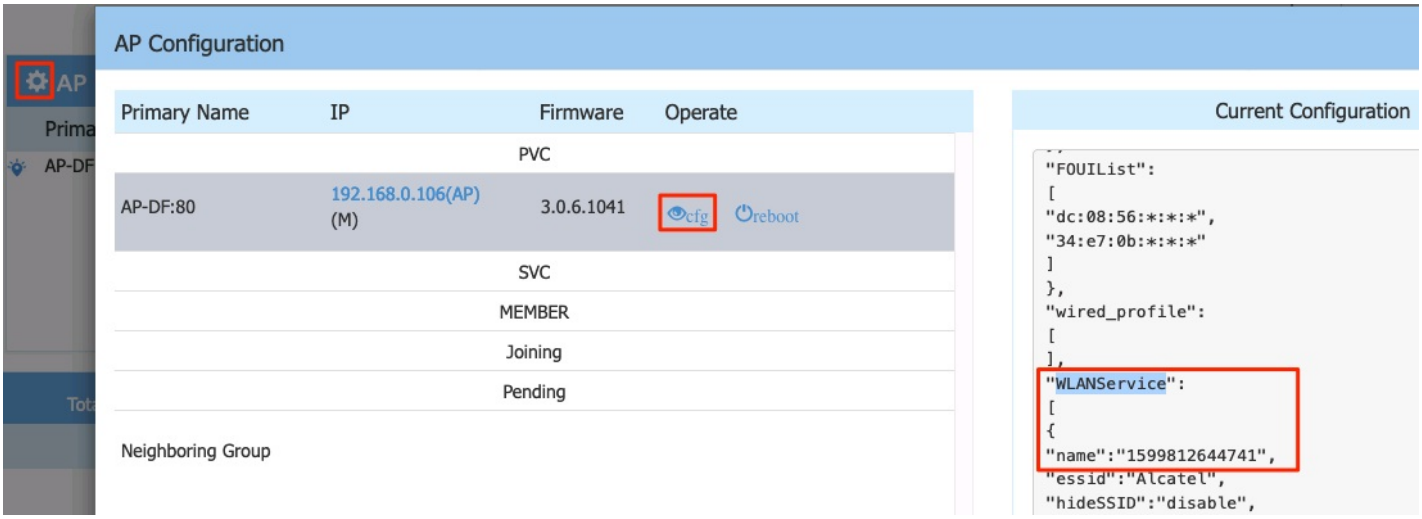
Select **Alcatel-Lucent Enterprise - Stellar** and set :

- **Name** of the controller in Hotspot Manager.
- **Radius security and secret** are used to secure the Radius traffic between your controller and Hotspot Manager.
  - **IP and RADIUS secret** : only from the public IP address of your controller with a complex secret to define **which must be the same in your controller.**
  - **Only RADIUS secret** : from any IP address using the self-generated RADIUS secret. Useful if the public IP address of your controller is dynamic.
- **NAS-ID** : is a unique string identifying the NAS (controller) originating the Radius Access-Request. **This value must must be the same in your controller**.

Fields not mentioned are optional.

Important note regarding the NASID **only for an Alcatel in Express mode** (standalone, not managed through the cloud) :

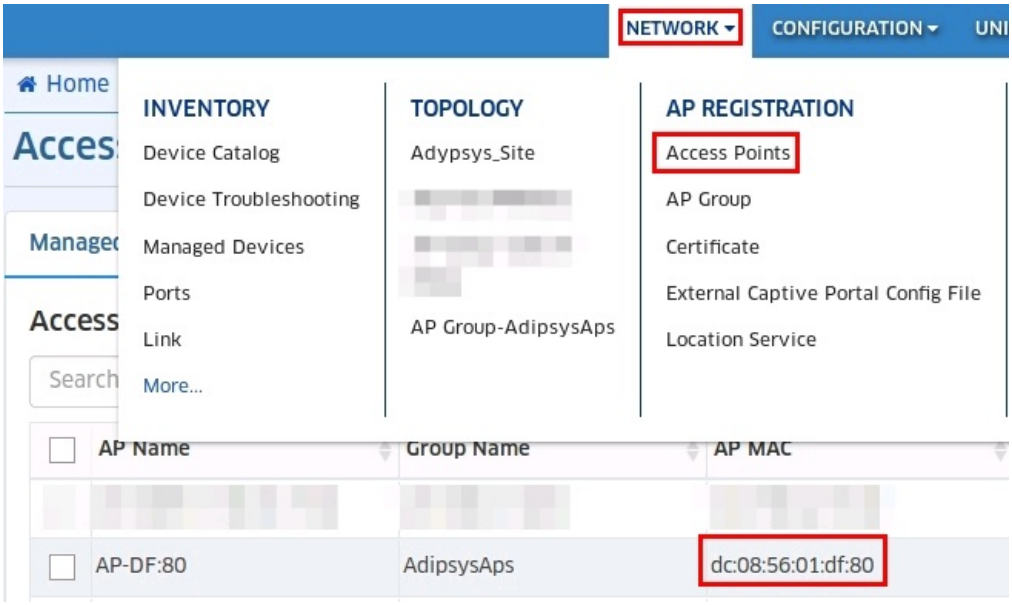
As the NASID isn't configurable on a standalone AP, you'll have to configure in HM the **WLANService** name visible from the interface by editing the AP :



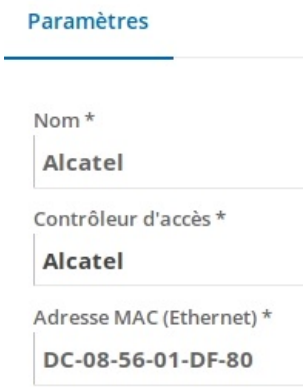
B. Hotspot configuration

Once the controller has been created, it has to be associated to a wifi zone and the AP will have to be associated to a hotspot. (Please refer to Hotspot Manager configuration guide for more details).

To get MAC addresses you'll have to declare, go to Alcatel Cloud under **Network -> Access Points** or in your AP details if it's standalone.



Once you have all necessaries MACs, you can create APs in Hotspot Manager under the APs tab of the hotspot parameters.



Set :

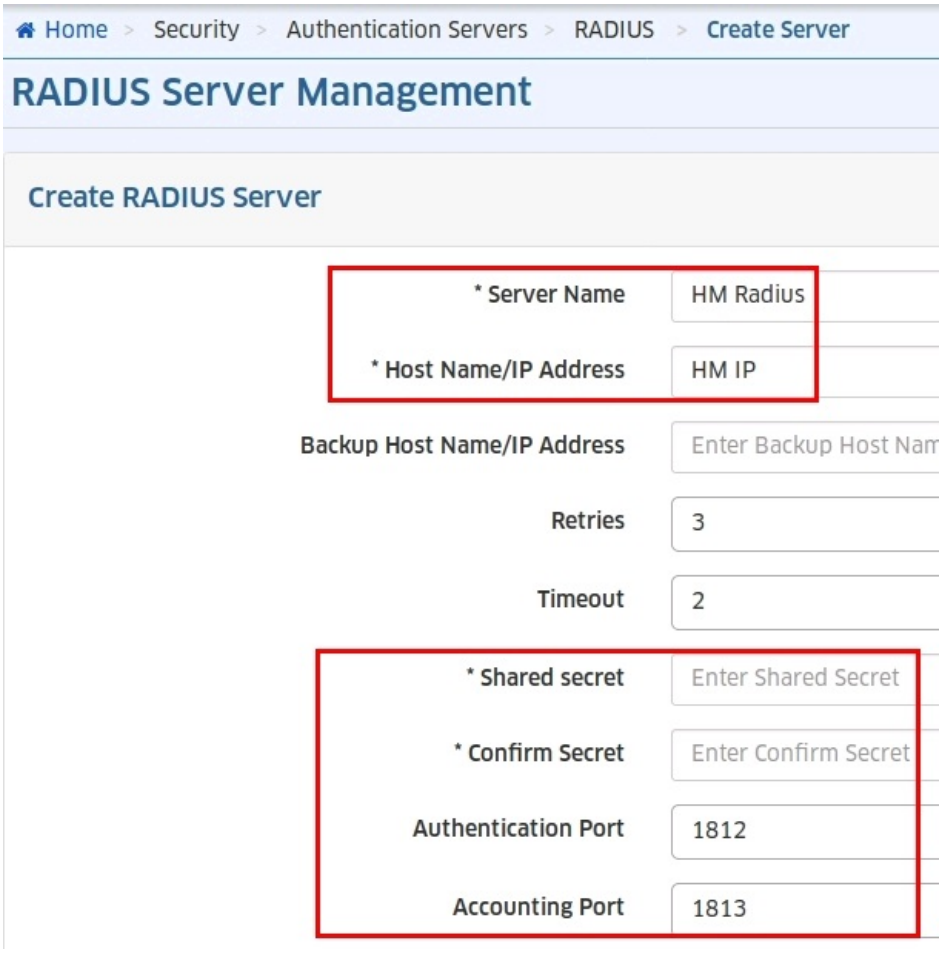
- the **Name** of the AP displayed in Hotspot Manager.
- the **Access Controller** to be linked with the AP.
- the **MAC address** of the AP.

Configuration of your Alcatel-Lucent Enterprise

We consider here that your AP is visible on Alcatel-Lucent OmniVista Cirrus/2500NMS cloud and you already have an AP Group in which to place it. If the AP Group does not exist, you can create it by leaving the default settings from **Network -> AP Registration -> AP Group**.
If your AP is in Express mode, it already has a default AP group. Configurations described below are essentially located under Access/Authentication and WLAN menus.

A. Configuration of Radius server on OmniVista Cirrus/2500NMS interface

Go to **Security -> Authentication Servers -> RADIUS** to add a radius server.



Set the following parameters :

- *Server Name* : of the radius server (Hotspot Manager).
- *Host Name / IP Address* : **IP of your Hotspot Manager server**.
- *Shared secret* : **configured previously in Hotspot Manager.**
- *Authentication Port* : **1812.**
- *Accounting Port* : **1813.**

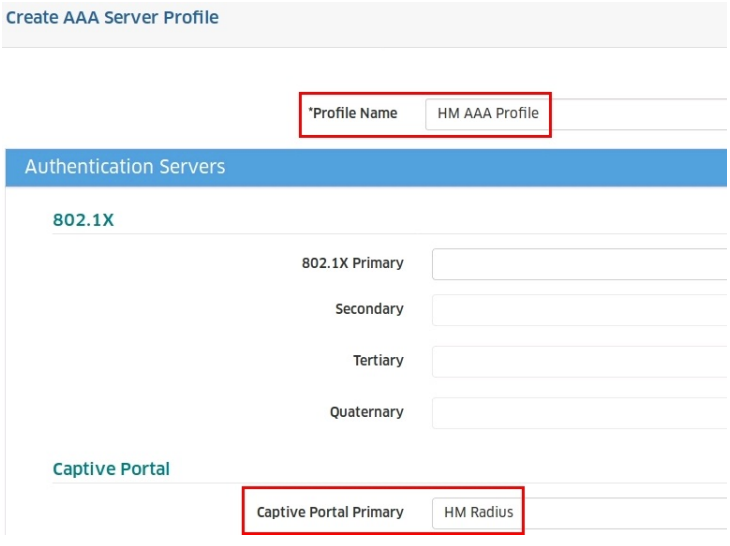
Click on **Apply.**

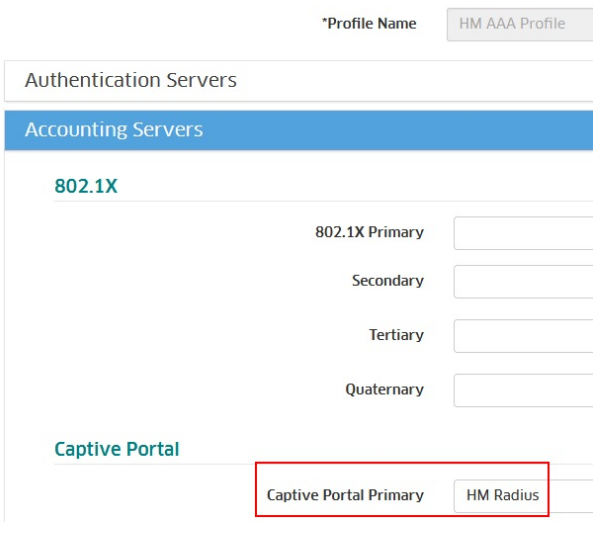
B. Configuration of AAA Server Profile on OmniVista Cirrus/2500NMS interface

Go to **WLAN -> WLAN Service (Expert)** then under **AAA Server Profile** (left menu) to create a new profile.

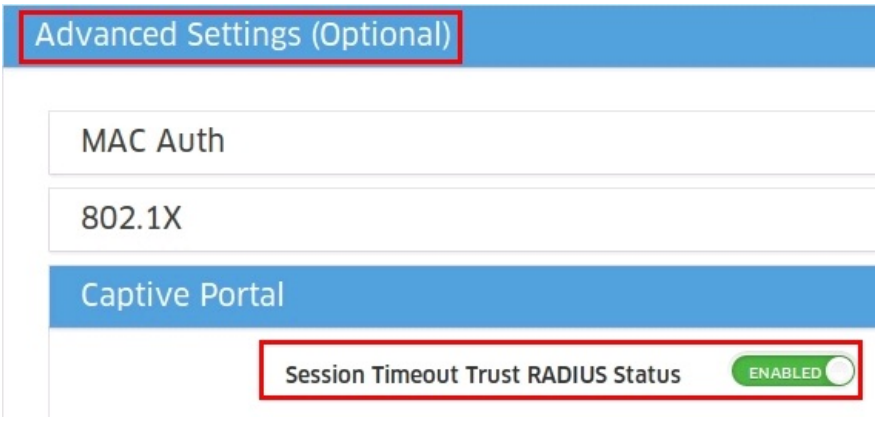
Set the following parameters :

- *Profile Name* displayed on the cloud.
- Under *Authentication Servers* and *Accounting Servers* sections, set *Captive Portal Primary* on the Radius server created previously.

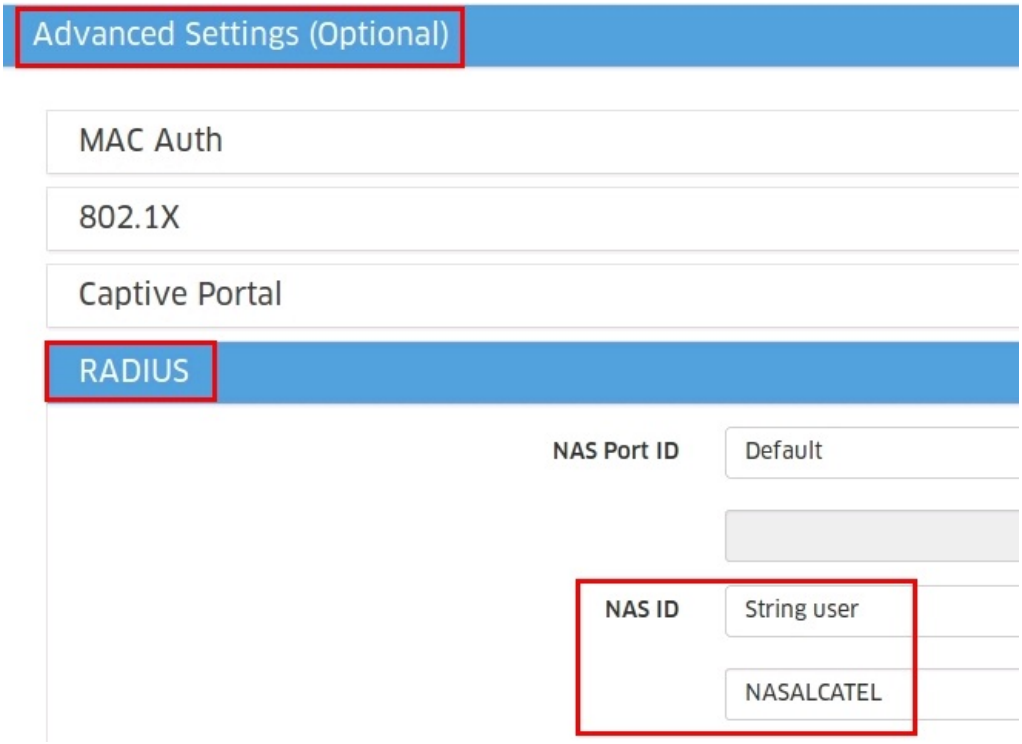




- Under *Advanced Settings/Captive portal* section, enable *Session Timeout Trust RADIUS Status* in order for this parameter to be applied when Hotspot Manager will send it according to the offer configured.



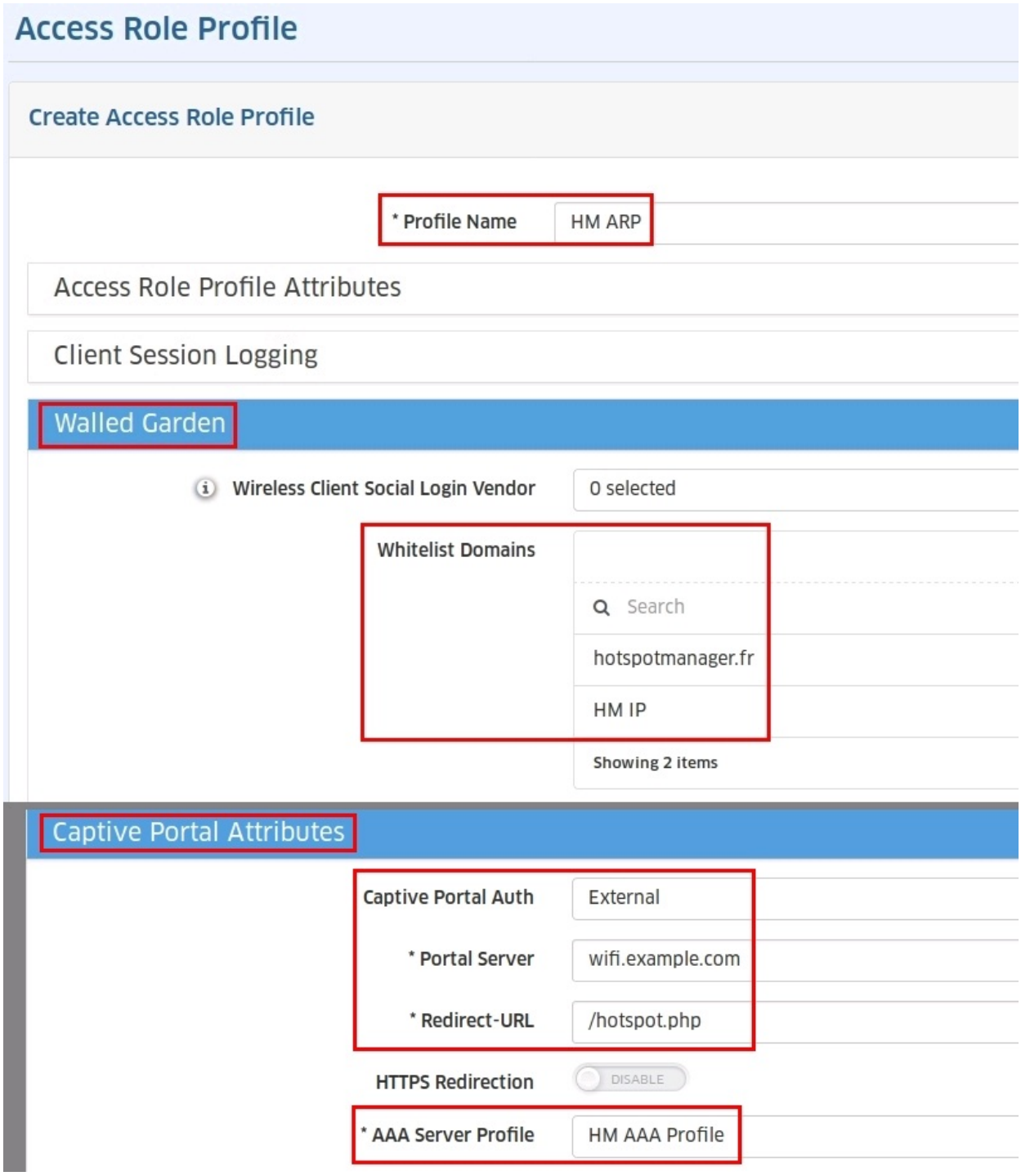
- Under *Advanced Settings/RADIUS* section, set the **NAS ID** (*String user*) in order to math the one configured in Hotspot Manager.



Click on **Create.**

C. Configuration of Access Role Profile on OmniVista Cirrus/2500NMS interface

Go to **Access Role Profile** (left menu) to create a profile.

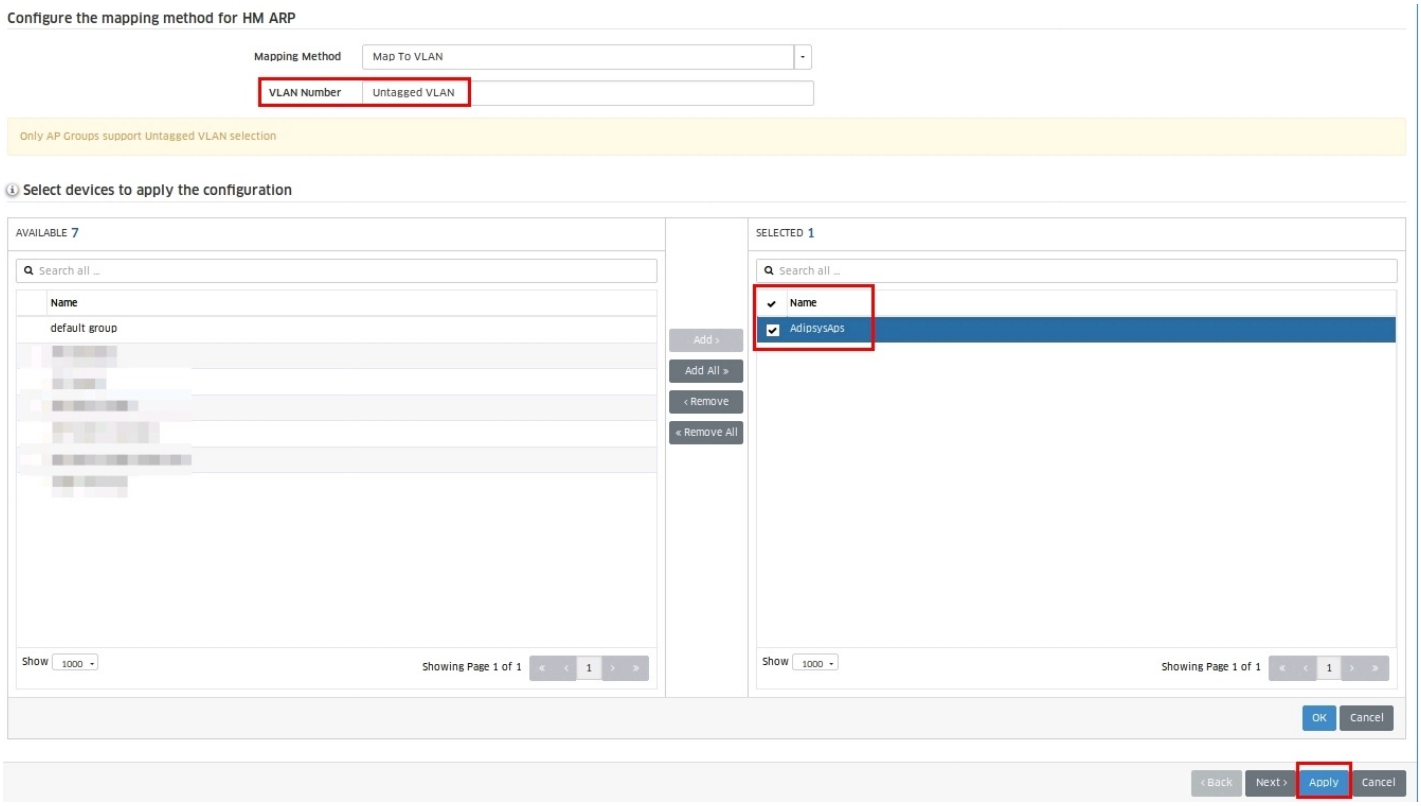


Configure the following parameters :

- *Profile Name* displayed on the cloud.
- Section *Walled Garden* : enter here at least the IP and the URL of your Hotspot Manager server. Example : **wifi.example.com** (adapt what's in red to your FQDN). Later you will also be able to configure domains/IP that need to be reachable by unauthentified devices (e.g. Facebook Connect or Paypal payment).
- Section *Captive Portal Attributes* :
  - *Captive Portal Auth* : **External**.
  - *Portal Server* : URL of your Hotspot Manager server. Example : **wifi.example.com** (adapt what's in red to your FQDN).
  - *Redirect-URL* : **/hotspot.php**
  - *AAA Server Profile* : select the one created previously.

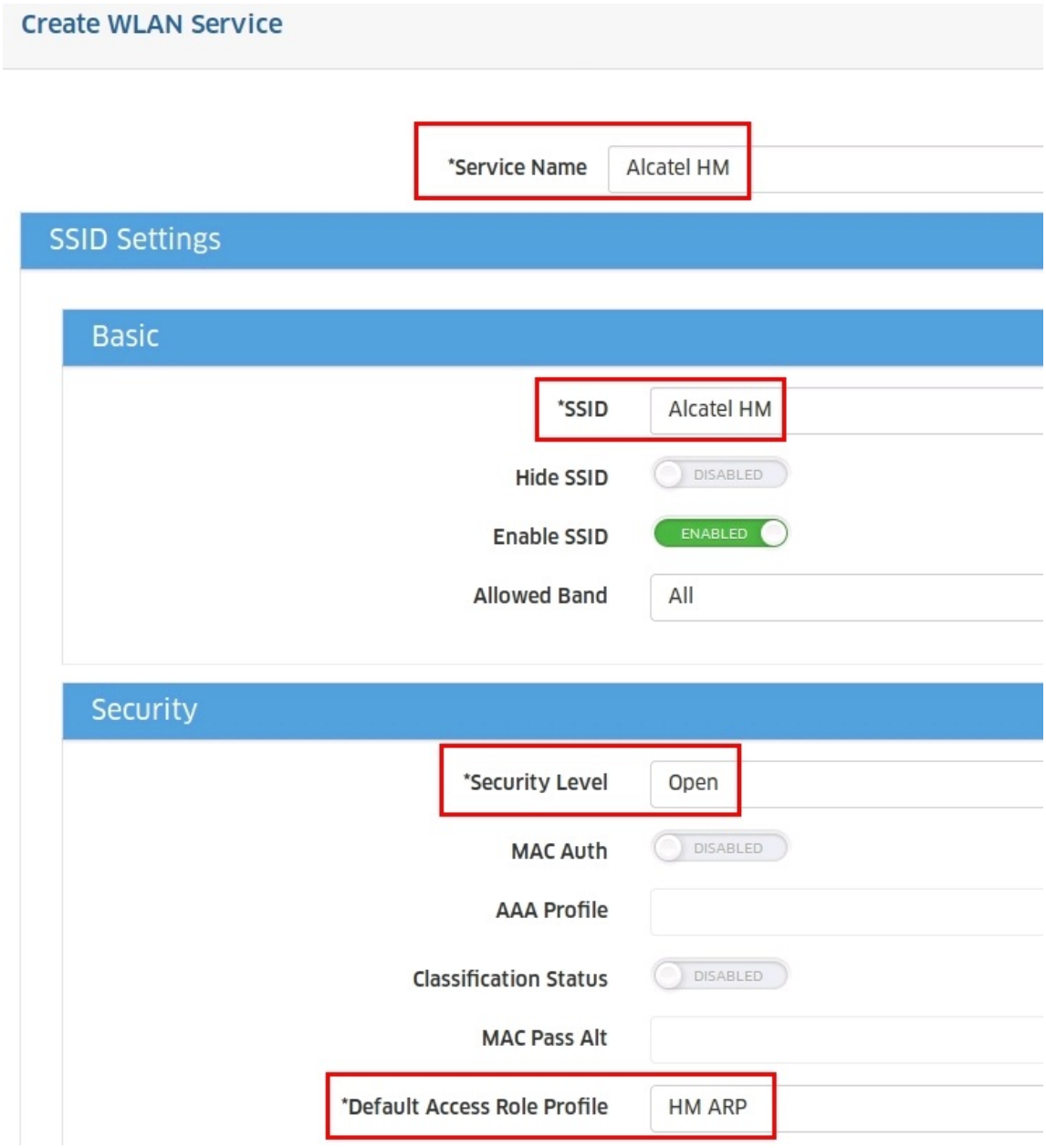
Click on **Create** then on **Apply to Devices** (top right) :

In *VLAN Number* select **Untagged VLAN** then add your AP Group and click on **Apply.**



D. Configuration of the SSID on OmniVista Cirrus/2500NMS interface

Go to **WLAN Service (Expert)** (left menu) to add a SSID.



Configure the following parameters :

- *Service Name* displayed on the cloud.
- *SSID* broadcasted by APs.
- *Security Level* : **Open**.
- *Default Access Role Profile :* select the profile created previously.

Click on **Create** then on **Apply to Devices** (top right) then add your AP Group and click on **Apply.**

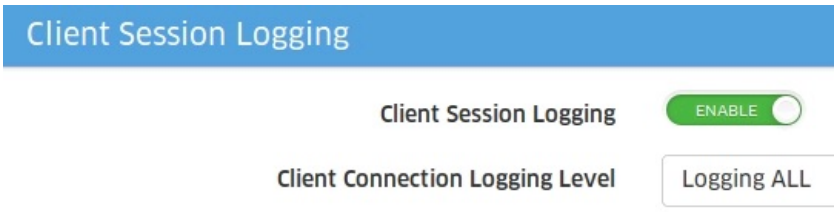
Setup finished. Now when a device will connect to the SSID broadcasted by this equipment, it will be redirected to the associated captive portal.
If you're getting an error message on the portal (end-user display), check APs MAC addresses configured in the hotspot.
If you're not getting the configuration to work, open a ticket on support.adipsys.com (https://docs.adipsys.com/support.adipsys.com) and attach a snapshot if it's possible.

E. Syslog (optional)

User trafic can be logged and sent to an external server (Hotspot Manager for example).

Go to OmniVista Cirrus/2500NMS interface, under **Network -> AP REGISTRATION / AP Group** menu to edit your AP Group and configure the following section :

Then go to OmniVista Cirrus/2500NMS interface, **WLAN -> WLAN Service (Expert)** menu then in **Access Role Profile** (left menu) to edit your profile and configure the following section :



Click on **Apply** then on **Apply to Devices** (top right) then add your AP Group and click on **Apply.**

Log sample sent by this equipment :

Oct 28 16:41:02 sop06-1-82-00-00-00.fbx.proxad.net 6c: 40:08:b6:83:d0/ZONE_1-test@adp.fr/www.adipsys.com/TCP/192.168.0.107/50689/54.36.54.80/80

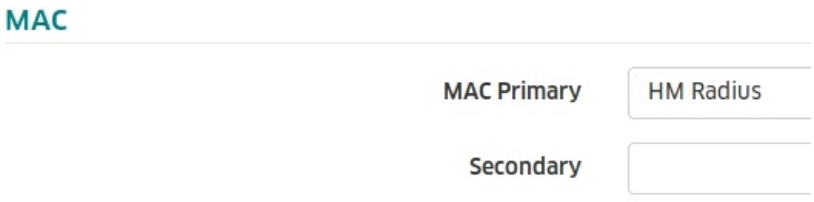
F. Multi-SSID (optional)

This equipment is natively compatible with multi SSID feature in Hotspot Manager.
For more details about multi-SSID please refer to the documentation (https://docs.adipsys.com/content/3/24/en/multi-ssid-configure-a-different-portal-for-each-ssid.html).

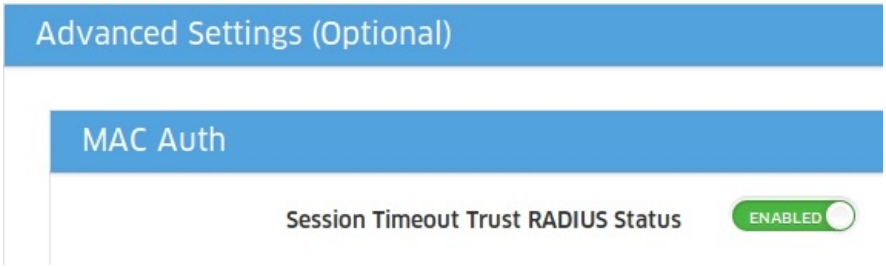
G. MAC authentication (optional)

If you want a device to bypass the captive portal and be authenticated directly to get Internet access you will have to configure the controller with the following parameters.

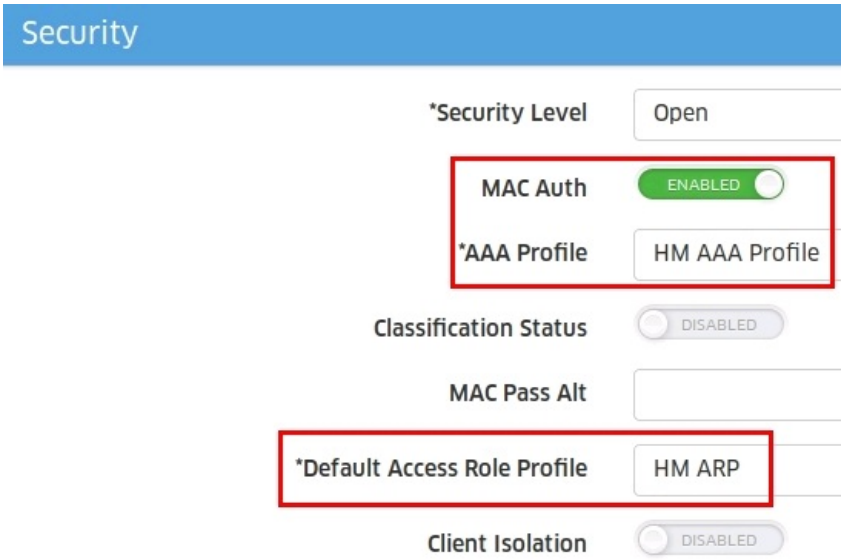
Go to OmniVista Cirrus/2500NMS interface, **WLAN -> WLAN Service (Expert)** menu then in **AAA Server Profile** (left menu) to edit your profile and configure the Radius server (Hotspot Manager) for **authentication and accounting** by MAC :



Under *Advanced Settings/Captive portal* section, enable *Session Timeout Trust RADIUS Status* in order for this parameter to be applied when Hotspot Manager will send it according to the offer configured.



Then on OmniVista Cirrus/2500NMS interface, **WLAN -> WLAN Service (Expert)** menu, edit your WLAN to configure the following parameters.



Click on **Apply** then on **Apply to Devices** (top right) then add your AP Group and click on **Apply.**

You must also configure Hotspot Manager properly to process MAC authentications.
For more details about MAC authentication please refer to the documentation (https://docs.adipsys.com/content/3/53/en/mac-address-authentication.html).

Hotspot Manager compliancy matrix

Features available, compatible or not with this equipment and Hotspot Manager.

Please refer to the Compliancy Matrix. (https://docs.adipsys.com/index.php?action=artikel&cat=5&id=23)

Last modified : 28-03-2022