Private PSK 1 SSID Two Networks

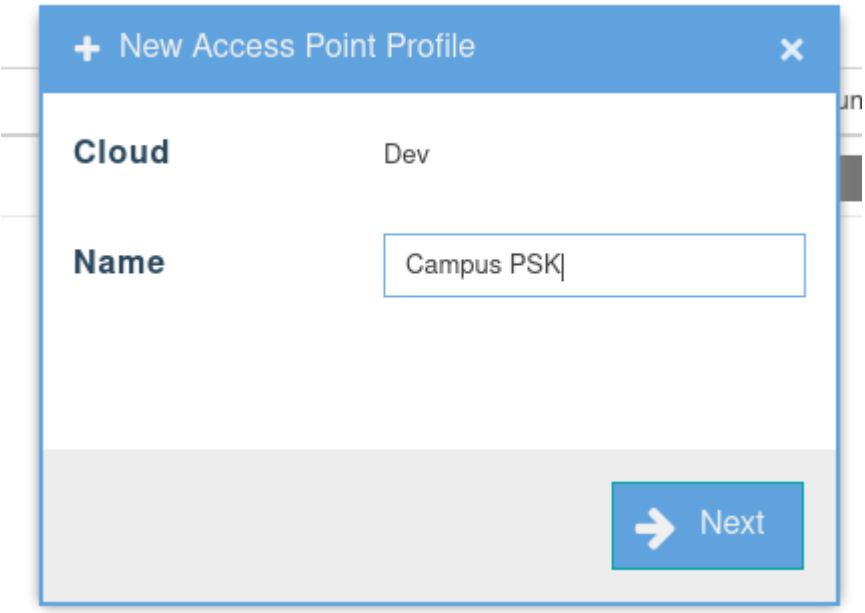
Introduction

- Please note that of Feb 2024 this component is under active development to make it even more feature rich and easy to use.
- Do check back here in order to find out when the development is completed and ready for production.

- This is our first use case and a very simple implementation.
- With this implementation we will:
  - Create a WiFi network with a SSID called **Campus PSK**.
  - Redirect unknown MAC Addresses to a captive portal.
  - Allow known MAC Addresses onto our network.
- We keep things simple by using the same PSK on both networks.
- **Although there are just one SSID and the PSK is the same, there are two networks and the network that the user will be landing on are determined by RADIUS.**
- There are two main components to Private PSK
  - The AP with the SSID that has Private PSK enabled.
  - The RADIUS which return a client's Private PSK key and optionally a VLAN the client needs to be on.

The AP side

- We will start with the configuration of the Access Point in AP Desk.
- Select a cloud to work in and go to **Networks → AP Profiles**. Click on the **Add** button.
- Here we create an AP Profile called **Campus PSK**.

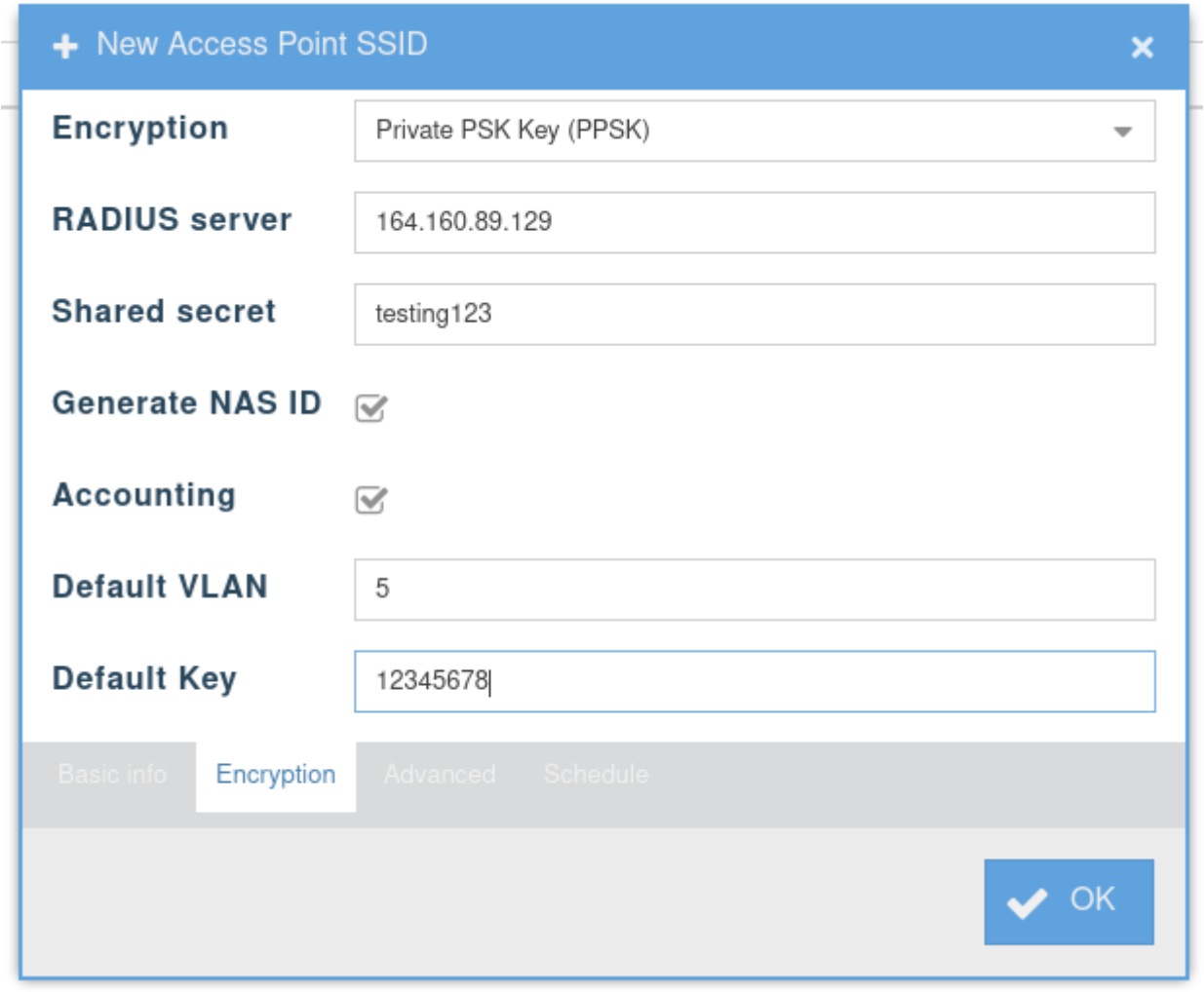


- After we created it we will edit it.
- Each AP Profile has the following sections.

    - General
    - SSIDs
    - Exit Points
    - Common Settings
    - Devices
- These section names should be self explanatory.
- We will be working on:
    - **SSIDs** - We will Add an SSID called **Campus PSK** with Private PSK configured.
    - **Exit Points** - We will define a bridge and Captive Portal. The Captive Portal will use An Internal Dynamic VLAN (We will use number5)
    - **Common Settings** - We will define an Internal VLAN for the Captive Portal (We will use number5)

SSIDs

- Add the SSID with **Private PSK** encryption.



- Specify the RADIUS server of your choice. We will point to our RADIUSdesk server (The same server)
- After you created it there will be a red alert stating it is not connected to an Exit Point.
- Next we will do the Exit point

Although we specify a default VLAN number and defauly key they are there only for

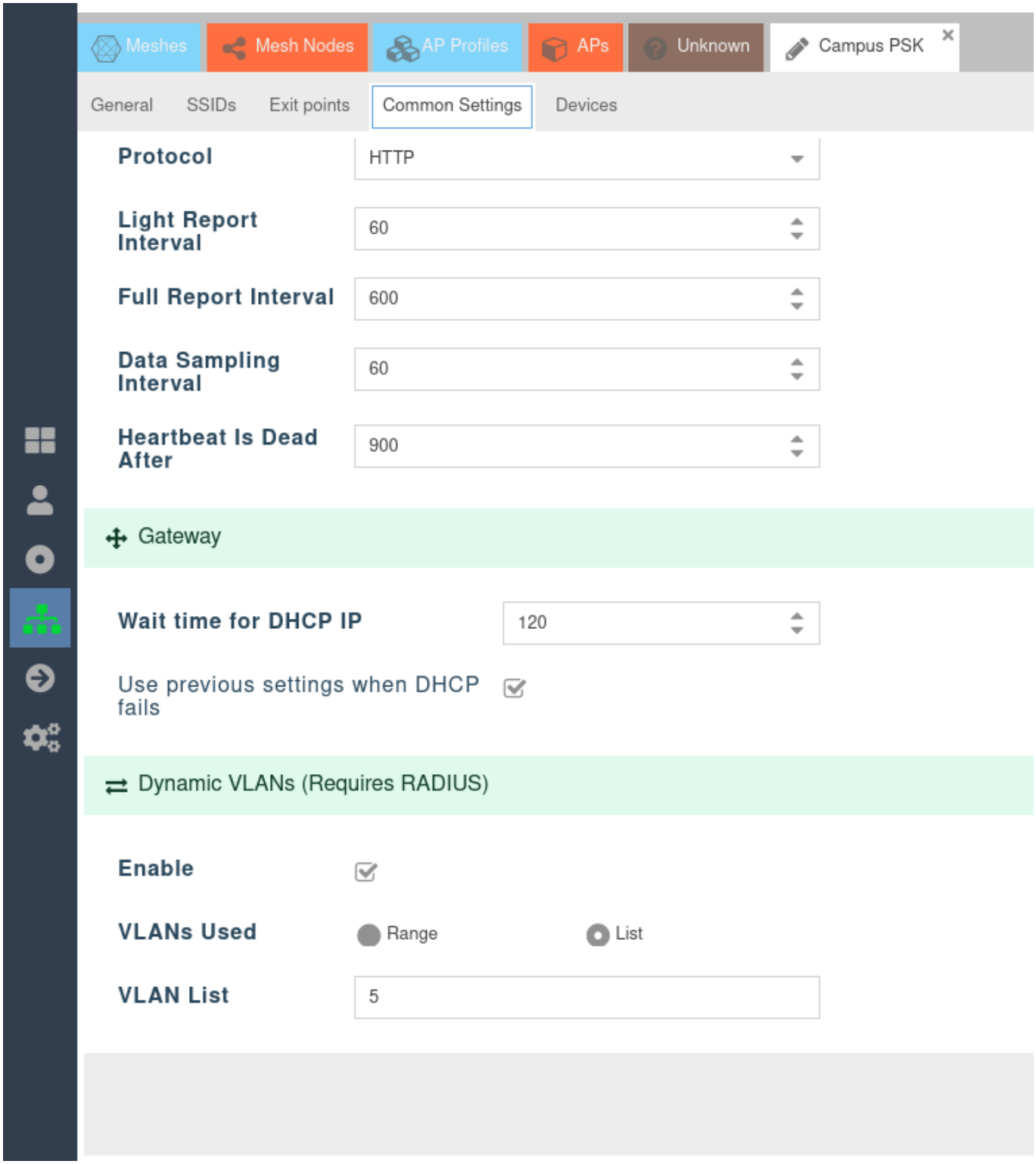
information purposes. Later when we configure the RADIUS Client we can consult these settings to specify matching values.

Exit Points Part1

- Add a bride exit point and connect it with the **Campus PSK** SSID.
- For the Captive Portal Exit Point we first have to create an Internal VLAN. We choose to use VLAN 5.
- This is specified under Common Settings.

Common Settings

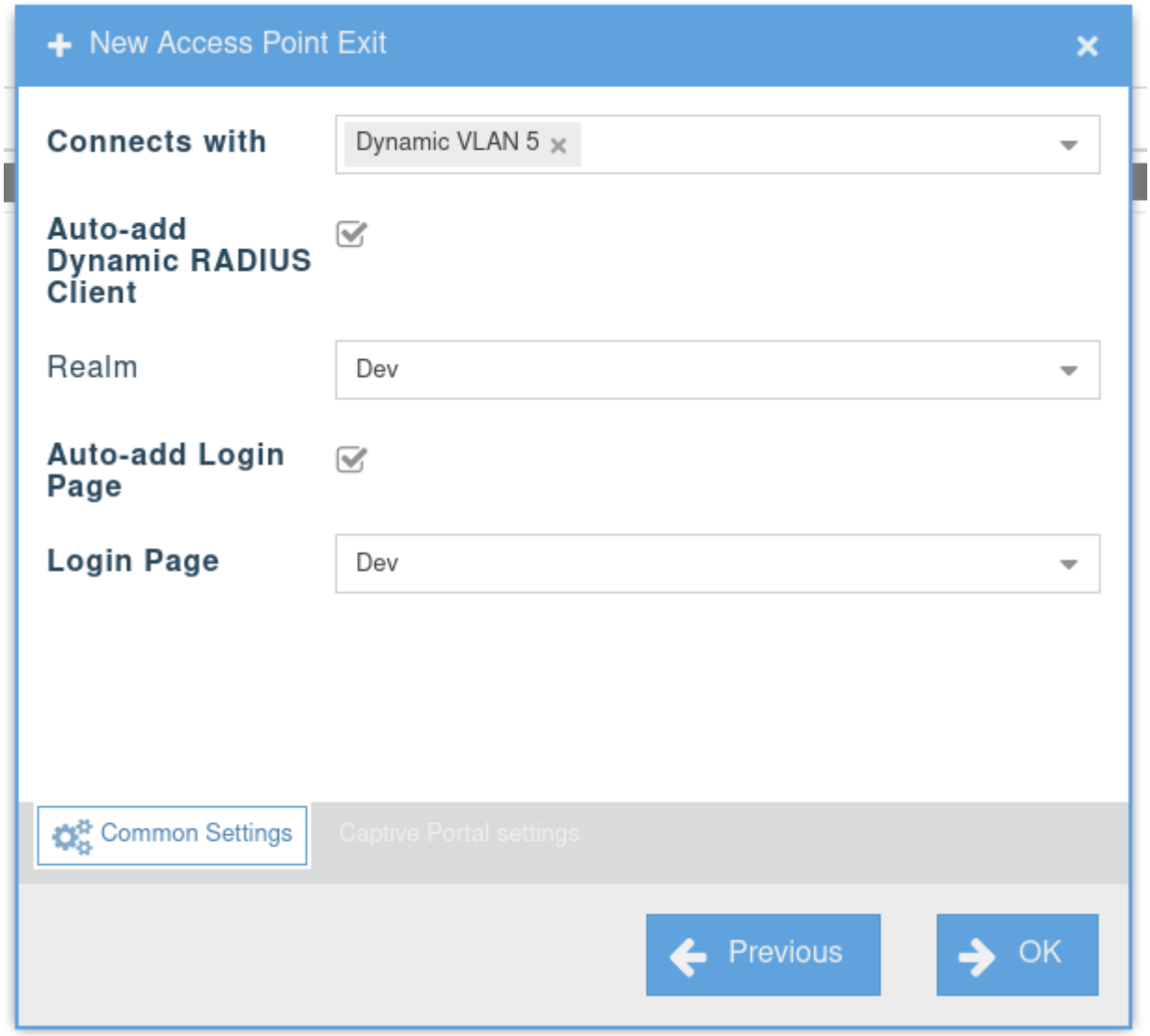
- We will only use one internal VLAN in the AP.



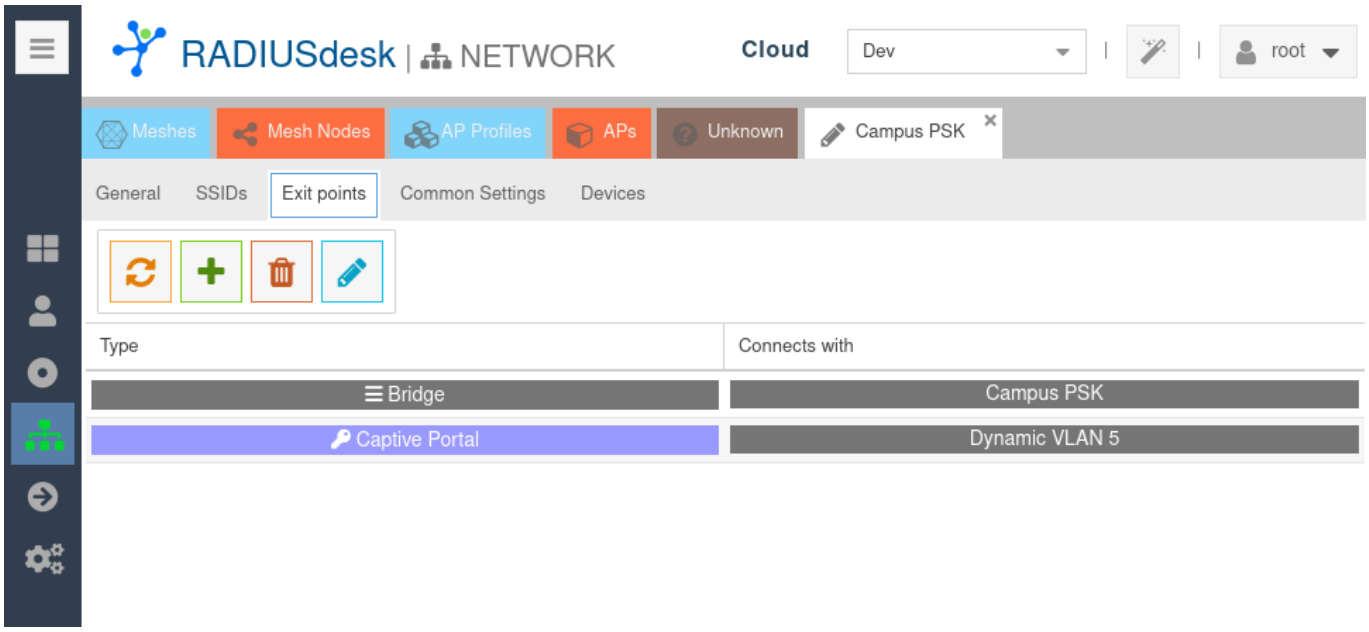
- We choose list and only specify one item (5).
- We can now co beck to SSIDs to define our Captive Portal Exit Point.

Exit Points Part2

- Add a Captive Portal Exit Point and specify that it connects with **Dynamic VLAN5**.



- Save everything.
- You should now have two exit points.



- As stated in the beginning we now have one SSID with Private PSK encryption and two networks.
- One network is a standard bridge.
- The other network is a Captive Portal.

The RADIUS side

RADIUS Components

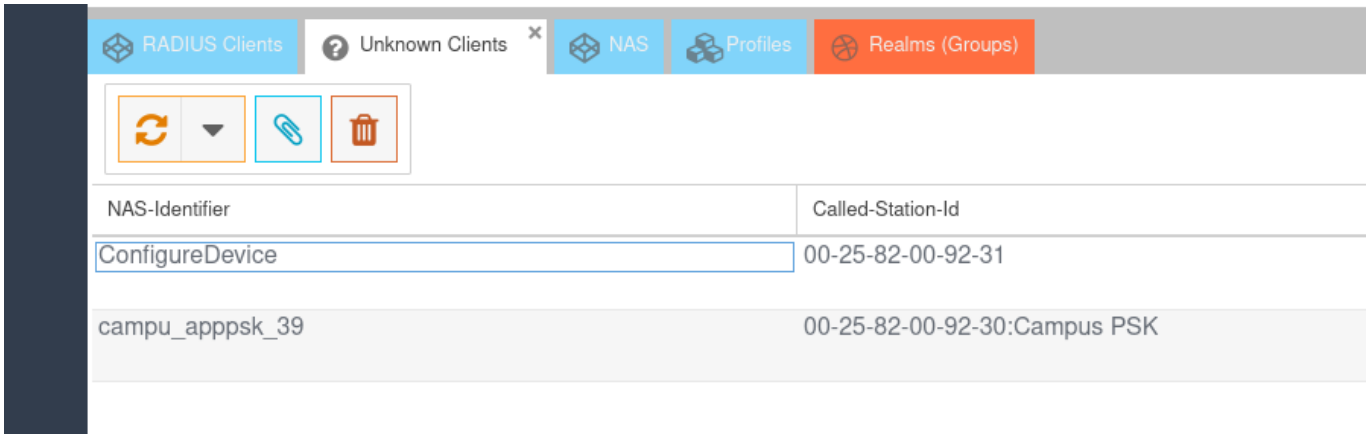
- The following RADIUSdesk components will be used
  - RADIUS Client - The Type of **Private PSK** selected.
  - A Profile used for user registration. This Profile will reply with Tunnel-Password 12345678.
  - A Login Page with User Registration Enabled and *Auto-add device after authentication* checked.

RADIUS related workflow

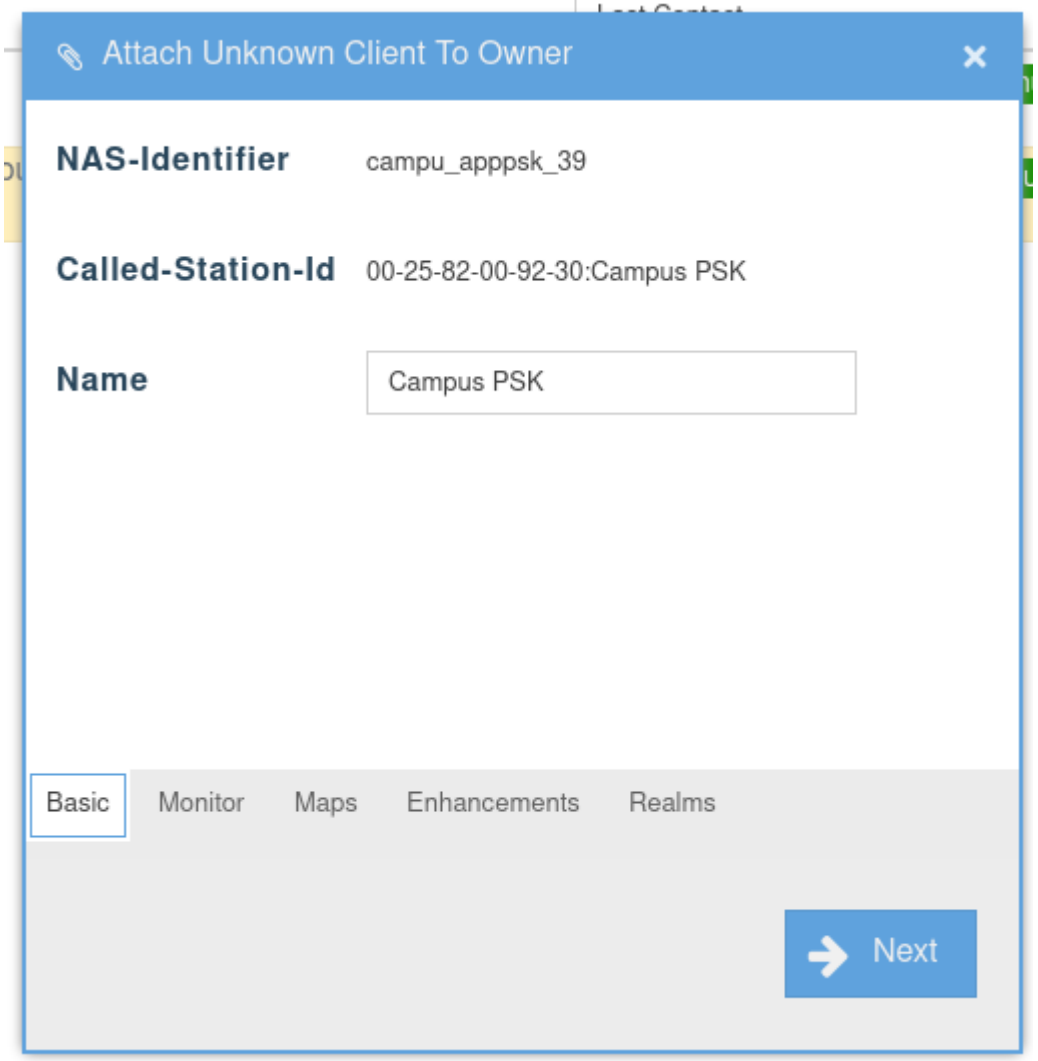
- When a user not known to RADIUS connects they will be redirected to a Captive Portal login page.
- With User Registration enabled; they can register.
- The User Registration will be configured as such that after the user register and log in, the device they logged in with will be automatically associated with them.
- Should the user wish to associate any other devices they will be redirected to the captive portal where they can use the existing username and password they already registered with to log in.
- Those devices will be also automatically associated with them.
- Once they disconnect and connect again to the WiFi network they will now be directly on the LAN.
- Next we can continue to prepare the environment for this setup.

Add RADIUS Client

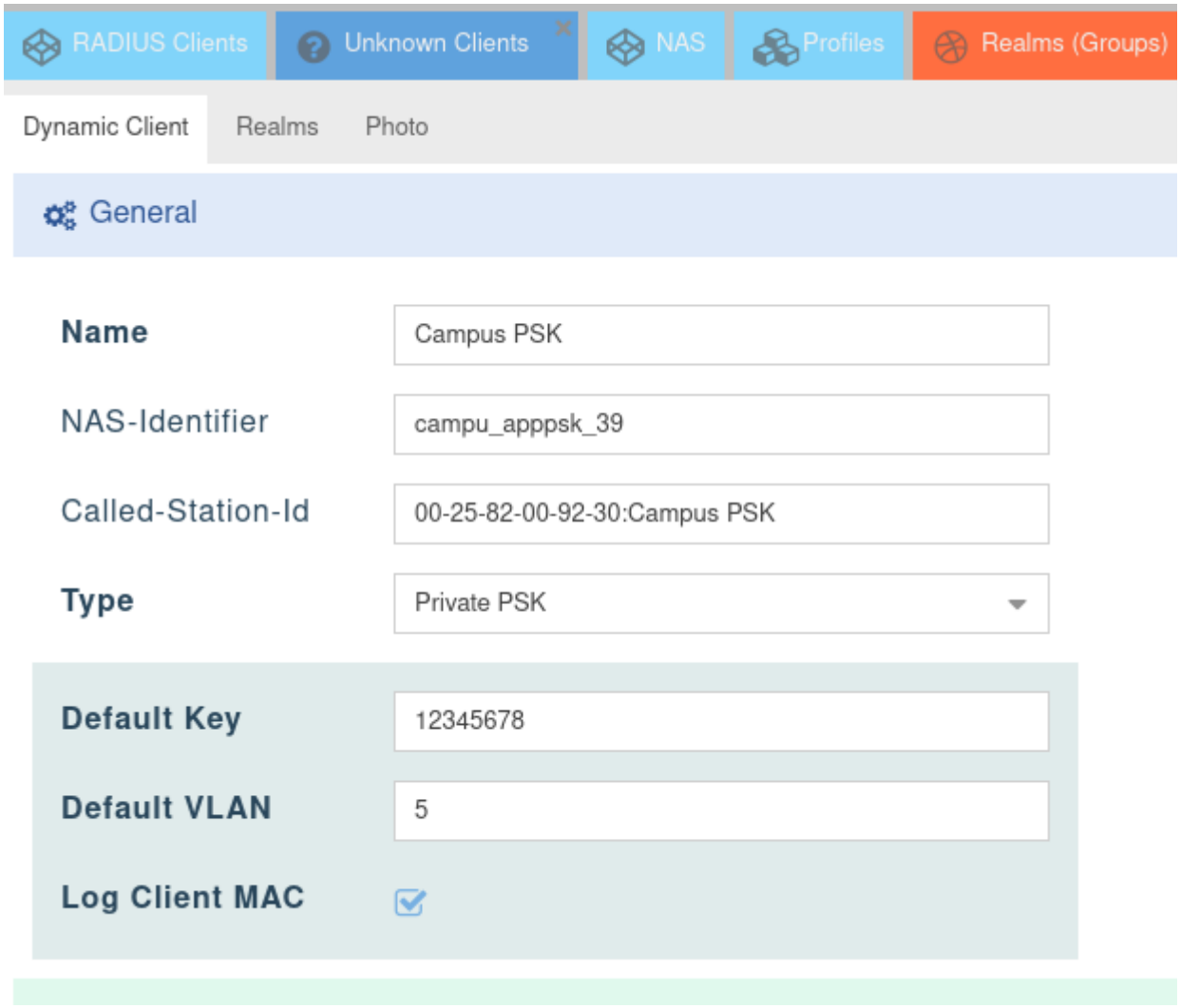
- We assume you attached an AP to the AP Profile we just created, fired it up and see that it is broadcasting the **Campus PSK** SSID.
- Next we can add the Private PSK (done by the hostapd program) as a RADIUS Client.
- Go to the RADIUS menu on the left and select the **Unknown Clients** button under **RADIUS Clients**.
- If all works correct you should see the AP made contact with the RADIUS server.



- Add it as a RADIUS Client.



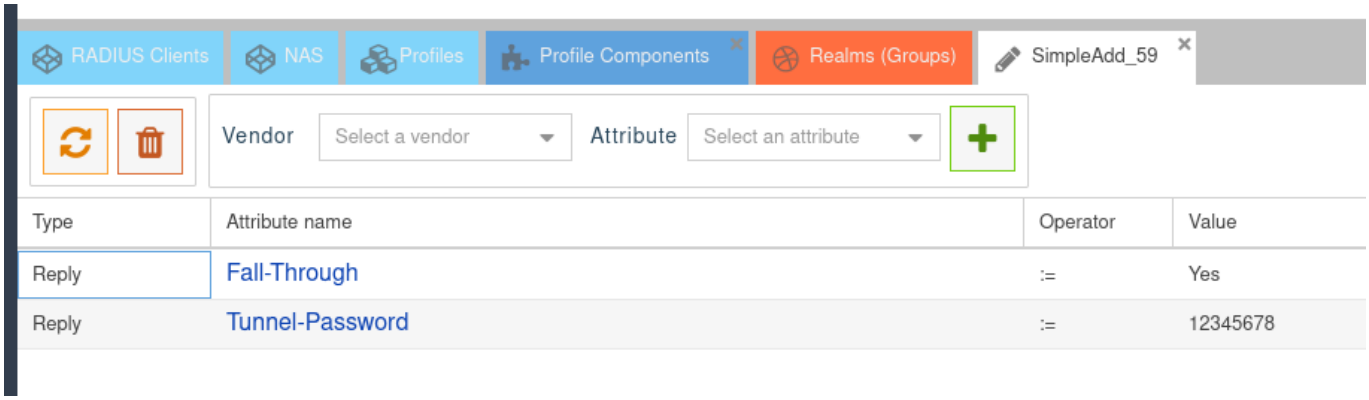
- Then edit it after you added it.
- The following section is very important to specify the Type
- We specify Type as **Private PSK**.
- We also specify a default VLAN and default key (This matches the values we specified earlier with the SSID)
- Then we also opt for the logging of MAC Addresses. (This is handy for IOT devices and Printers)
- These are MAC Addresses which are not known to RADIUS and which will be directed to VLAN5 (Our Captive Portal)



- Save everything and try to connect to the SSID.
- If everything works correct you should be redirected to the Captive Portal's Login Page.

Profile for Registered Users

- RADIUSdesk has an option that allow for users to register through the captive portal login page.
- The registered user has to belong the a realm and have a profile.
- We will now create the profile.
- Our profile will be very simple and just reply with the Tunnel-Password (PSK) which we will make *12345678*.
- Navigate to RADIUS → Profiles. Click on **Add**.
- We create one called **CampusPSK-Student**.
- Keep the defaults (no limits imposed) and click **Save**.
- You will see that the system created a Profile Component and associated it with the profile.
- In our case its called **SimpleAdd_59**.
- Edit the Profile Component called **SimpleAdd_59** and add a Reply attribute of Tunnel-Password := 12345678.



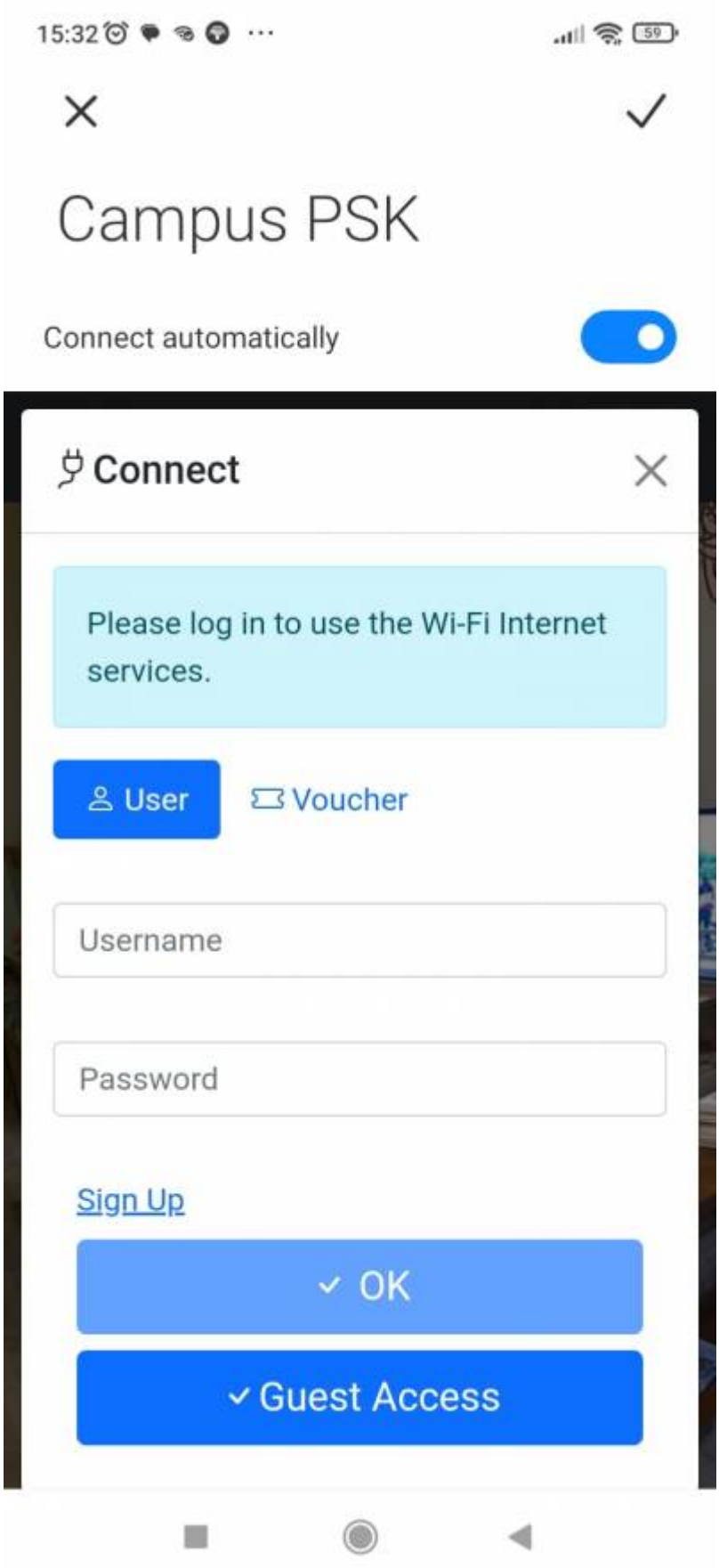
- Now everything is in place for us to configure user registration in the login page.

Enable User Registration

- Go to Login and select the login page that you use for the captive portal.
- Edit its settings and enable user registration.
- Make sure you also selected **Auto-add device after authentication**.
- Save it.
- Everything is now ready to test.

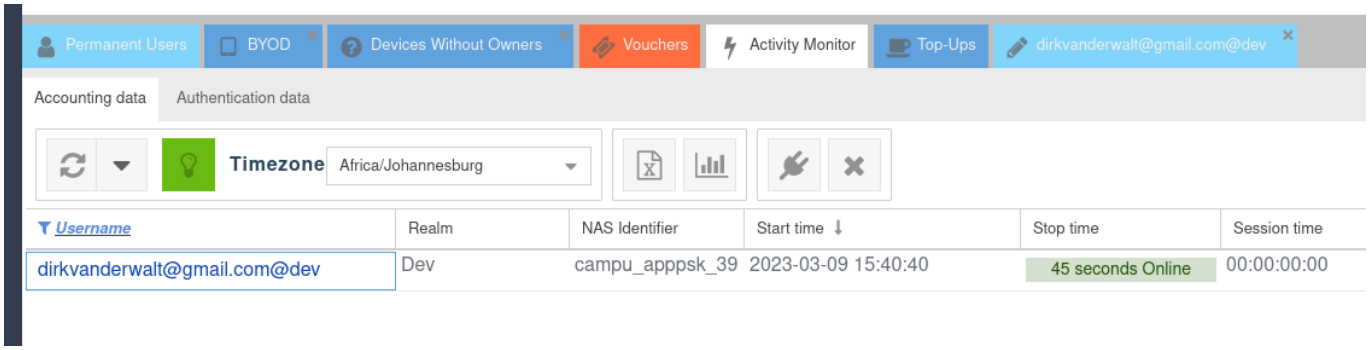
Final Testing

- Connect to the Captive Portal.
- You Login Page should look similar to the one below.



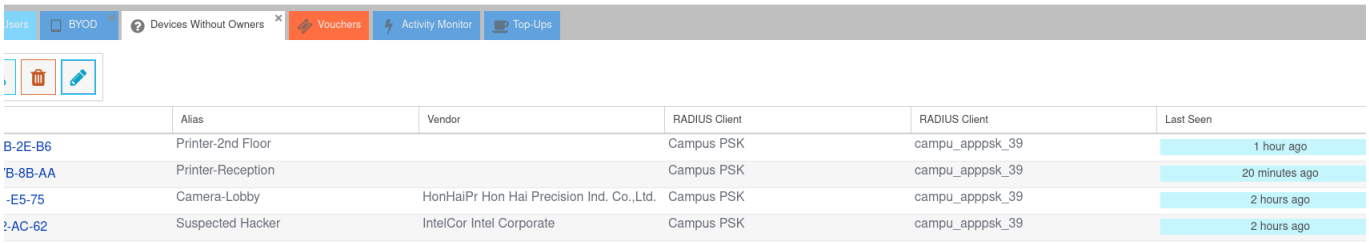
- After you register and logged in you can confirm that the user's MAC Address has been associated with them.
- Ask the user to leave the WiFi network and connect again.
- The user should now be connected directly onto the LAN through the WiFi.

- Here we see under Activity Monitor that the user is connected using PPSK (Our NAS Identifier uses a convention with **ppsk** in the value.



Devices Without Browsers

- The Captive Portal works well for adding devices what has a browser.
- Some devices however needs access to the WiFi network but they do not have any screen to pop up a browser.
- These include sensors, WiFi Cameras and Printers.
- For these we have a handy applet that can be launched from Users → Permanent Users.
- The **Devices Without Owners** applet will list all the MAC Addresses which connected to the SSID and were assigned to the default VLAN.



- We also give an indication when last it was seen on the network which makes it even more easy to locate.
- On top of that we offer the opportunity to give them an alias in case you need to tag those devices first.
- Then you can attach them to a permanent user.
- Our recommendation is to have a dedicated special Permanent User for a class of devices. e.g. su-printers for printers and su-cameras (su is short for special user).

Banning Devices

- You might ask, since all the users will have a common PSK, will it be possible to stop a specific device from gaining access to the network **without** forcing all the other devices to change the PSK they are configured with.
- Yes it is possible.
- Simply navigate to the BYOD applet and select the device(es) you want to stop the select the Enable / Disable button to complete the action.