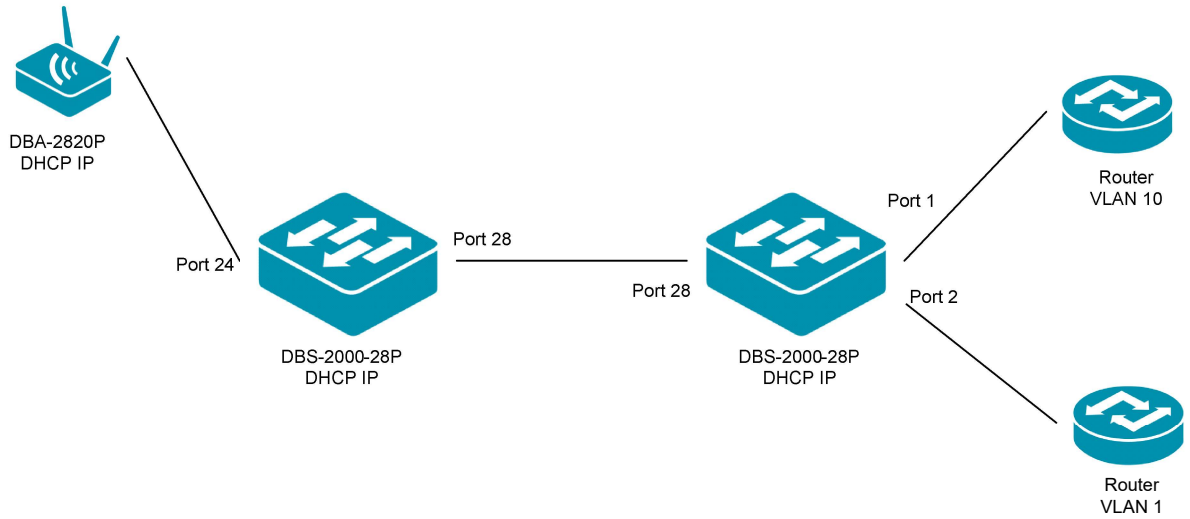
HowTo: setup MultiSSID with Nuclias Cloud

[requirements]

1. DBA-xxxx Nuclias managed AP
2. DBS-xxxx Nuclias managed Switch or any vlan capable switch

[scenario]

Within Nuclias Cloud you want to configure MultiSSID (2 SSIDs) which are separated by VLANs. The internal SSID is located within VLAN 1 and the guest SSID is located within VLAN 10. For each VLAN/SSID there is a dedicated router available.

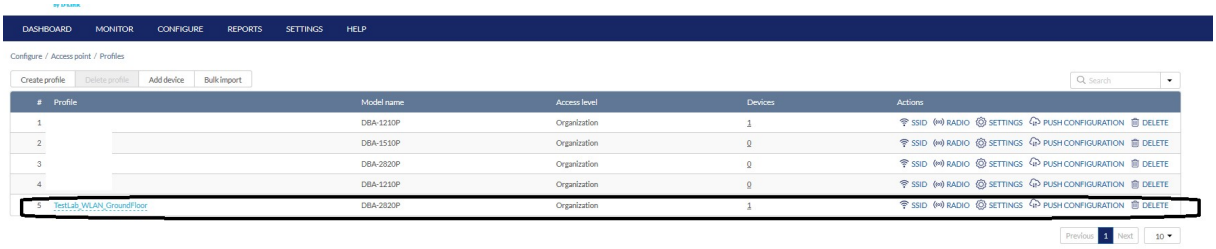


[preperation]

- ⇨ all nuclias managed devices are managed and synchronized within yor nuclias account
- ⇨ all APs are allocated to their AP Profile

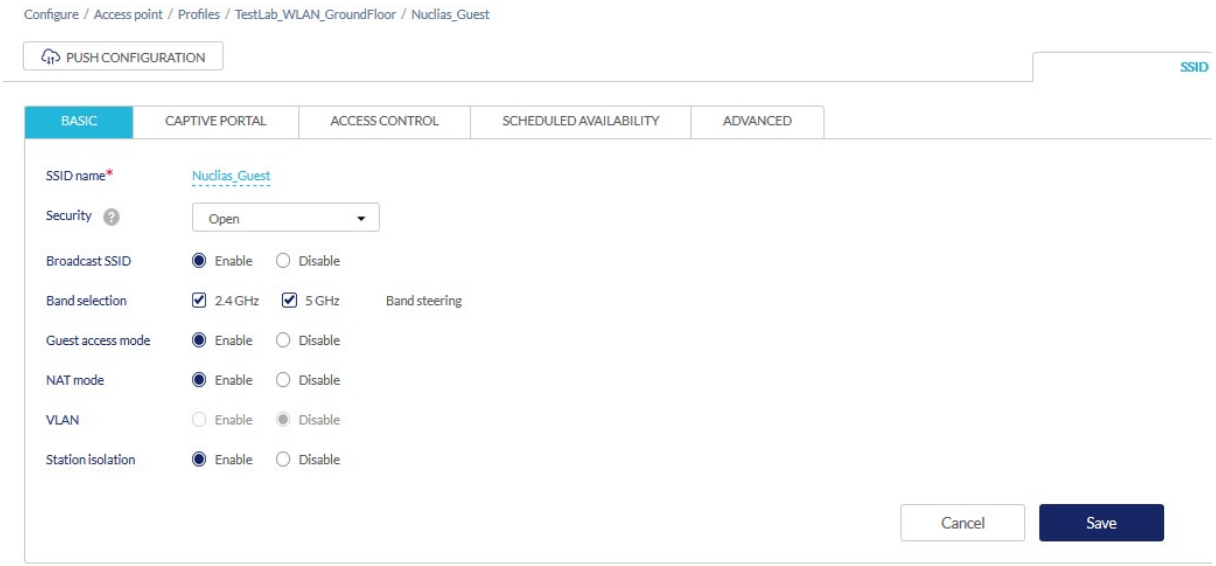
[MultiSSID within AP Profile]

Go to the AP Profile page



1.) klick SSID for your AP Profile

a. here you see now the default SSIDs “Nuclias_Guest” and “Nuclias_Office”
b. select then the “Nuclias_Guest” SSID, so that we can modify it



i. to change the SSID Name, click on the blueish name “Nuclias_Guest”, type your new SSID Name and confirm with Return
ii. choose the security to your liking from the drop down menu
    1. depending on your choice there will be now some additional menus about the authentication
iii. select if the SSID should be broadcasted, or not
iv. select, if you want to use Band steering, or not
v. select, if you want Guest Access Mode, or not
vi. select, if you want to NAT the Wifi, or not
vii. select, if you want to use VLAN assignmet for the SSID, or not

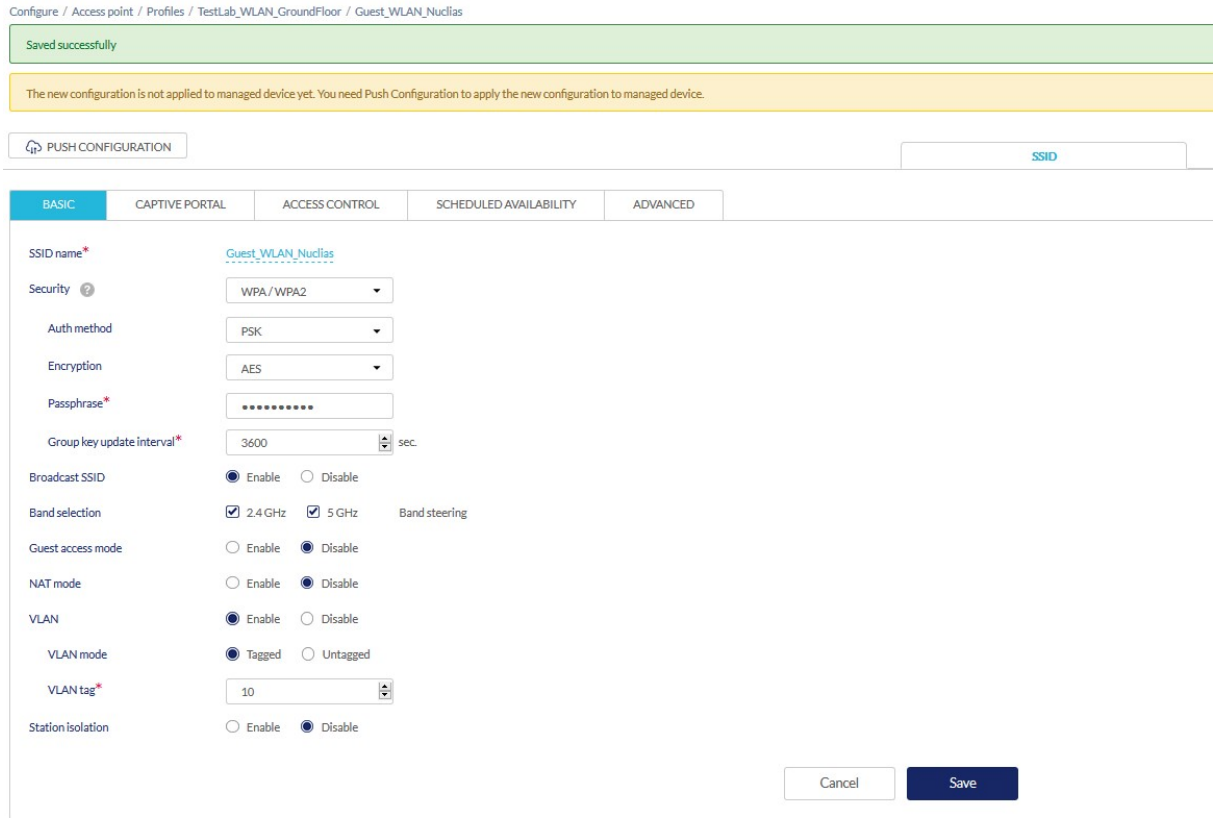
1. if you enable VLAN, then the default setting is VLAN "TAGGED", this setting is how the VLAN is transported at the LAN Port of the AP, so depending on your design and Switchport configuration the VLAN should be "Tagged" or "Untagged"
2. if you do not enable the VLAN, then the SSID will be transmitted within the Management VLAN of the AP, which is by default VLAN 1 untagged

viii. select, if you want WLAN Station isolation, or not

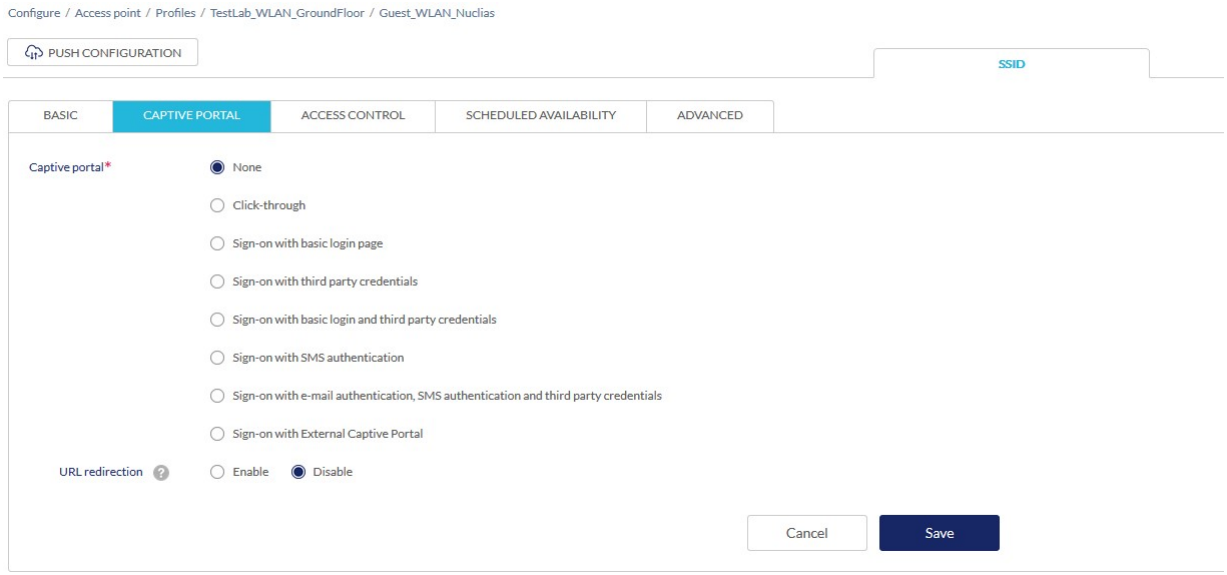
For our scenario we then define the SSIDs name as "Guest_WLAN_Nuclias" with WPA/WPA2 (AES) authentication. The SSID is being transmitted (displayed, not hidden).

The AP also can NOT band-steer clients from 2.4 GHz to 5 GHz vice versa.

Also the SSID is being assigned to VLAN 10 for our guest network.



Disable Captive Portal for the SSID, if you do not want to use it.

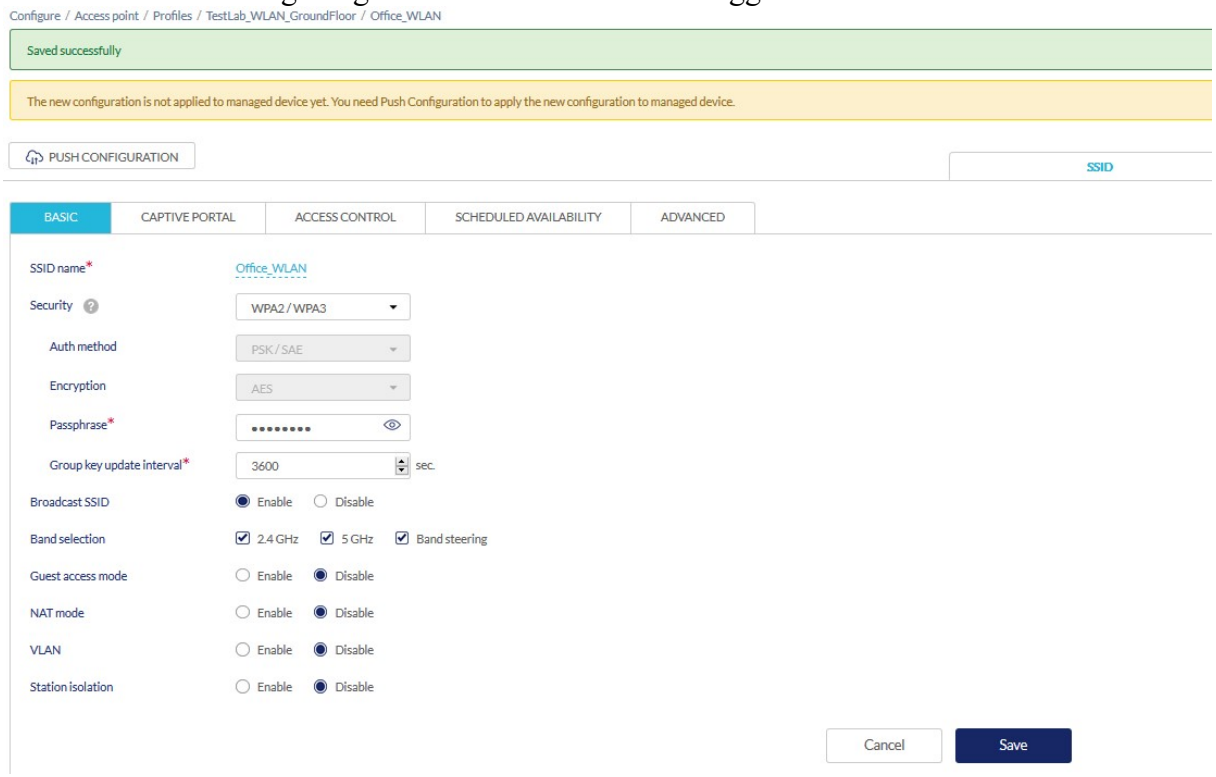


Repeat the step now for the 2nd SSID

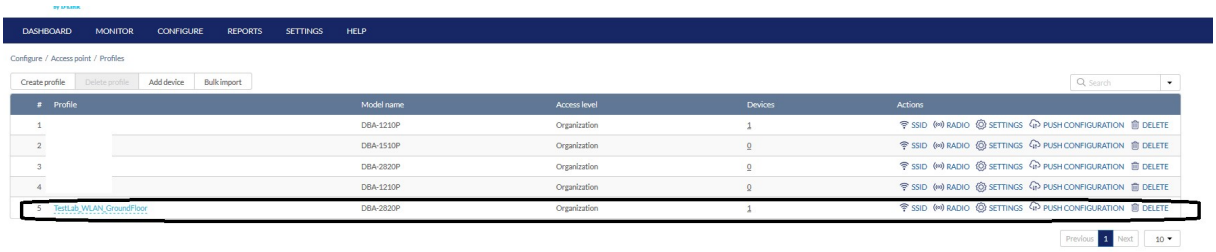
For our scenario we then define the SSIDs name as “Office_Nuclias” with WPA2/WPA3 (AES/SAE) authentication. The SSID is being transmitted (displayed, not hidden).

The AP also can band-steer clients from 2.4 GHz to 5 GHz vice versa.

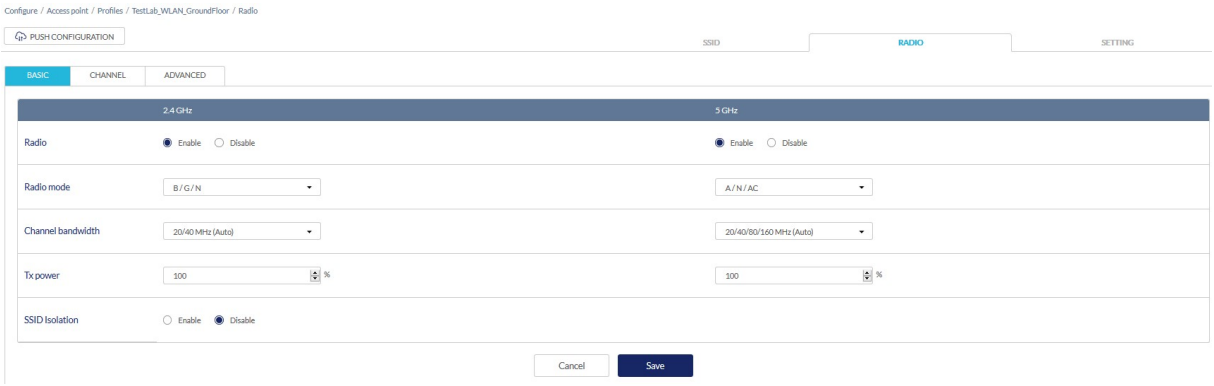
Also the SSID is being assigned to default VLAN 1 untagged.



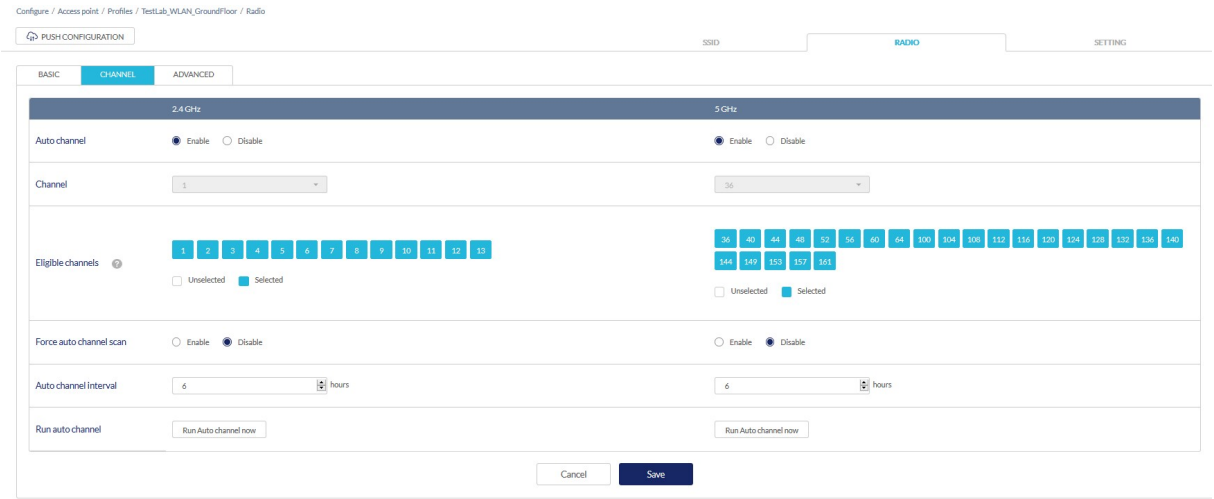
Within the AP Profile you also modify some radio settings, by clicking “Radio”.



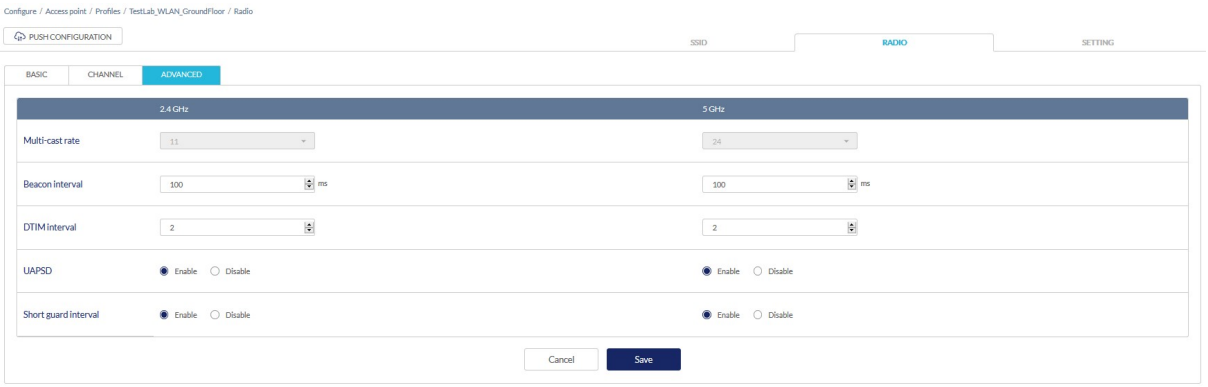
Here you can select the Radio Settings for each radio band and radio mode.



As well as selecting the available channels for each radio.

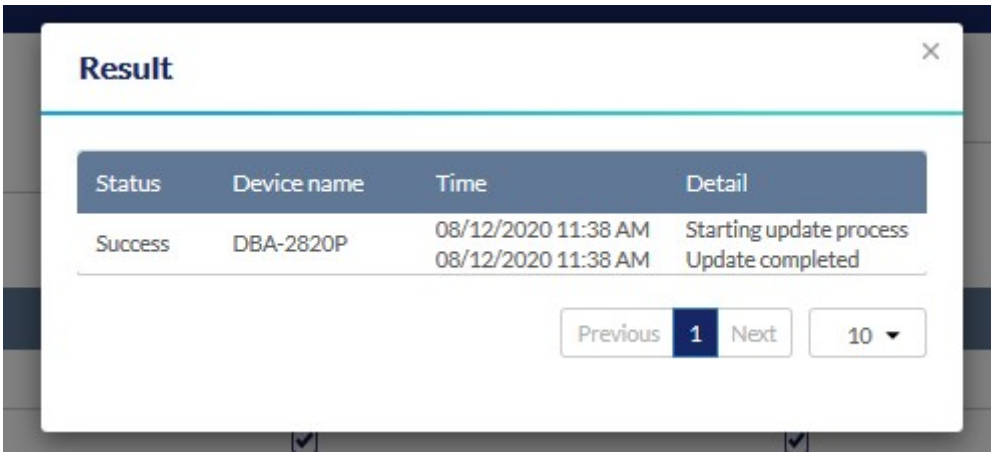


Also some advanced features like DTIM and Beacon Interval as well as UAPSD (power saving for clients) can be modified according to your requirements.



After you've finished configuring the AP Profile you can push it to all the

APs



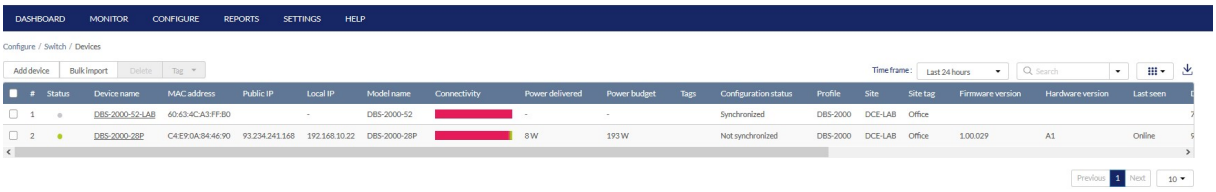
The APs now start to transmit the SSIDs according to your settings.

! At this point, only clients within the Office_Nuclias" SSID can connect and have internet access, since this SSID is located within VLAN 1. The Guest Clients can connect to the SSID "Guest_WLAN_Nuclias" but will not obtain an IP Address or have internet access, since the VLAN 10 is currently not defined at your switch !

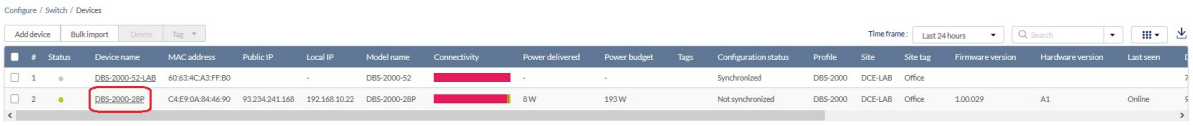
(If you use 3rd party switches, or non-Nuclias Switches, you must now set the VLAN assignment there manually.)

[MultiSSID within AP Profile]

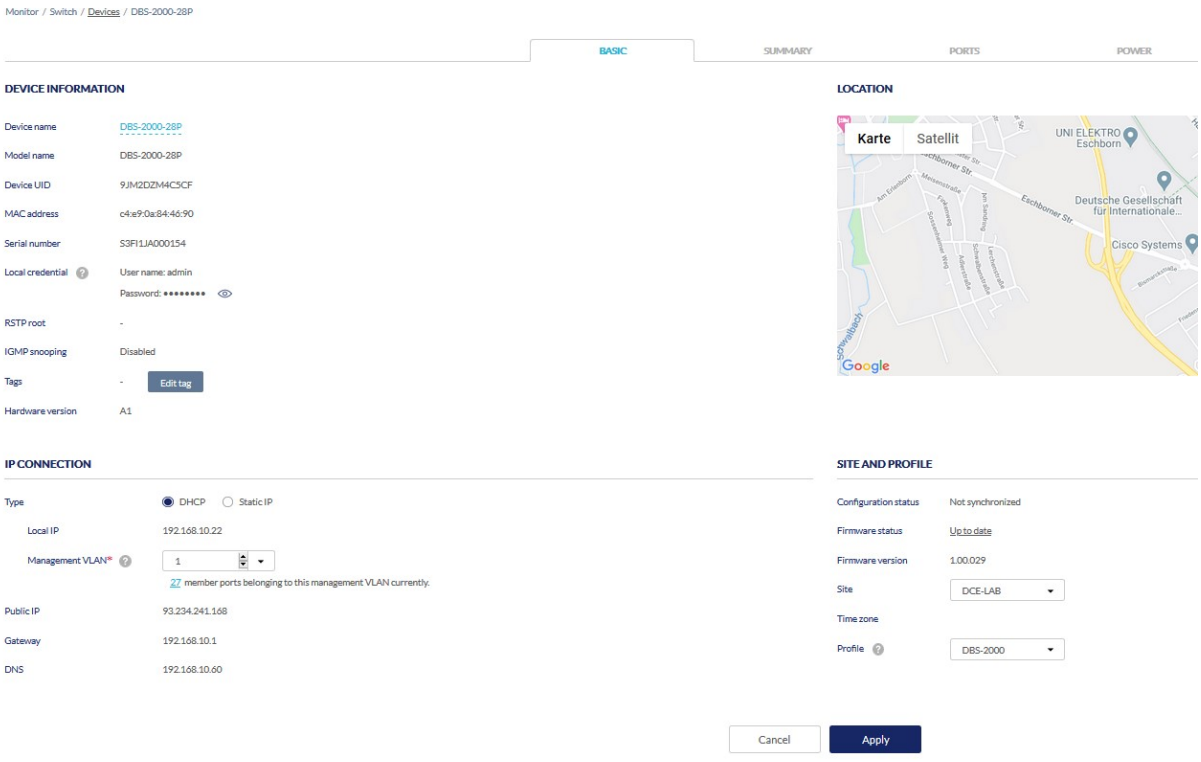
Go to the Switch device page



Select the switch you want to modify by clicking on the device name.



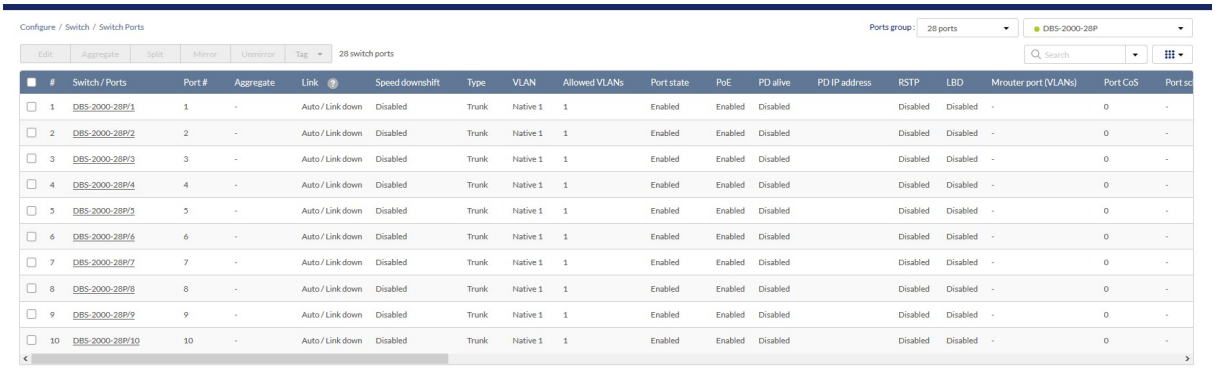
Here you can now modify some basic management settings, as well as change Site, Profile and Management-VLAN for the switch.



To modify the Port-VLANs go to “Ports”.

Here you also can see if a port is connected, the connection speed and when supported if PoE is delivered.

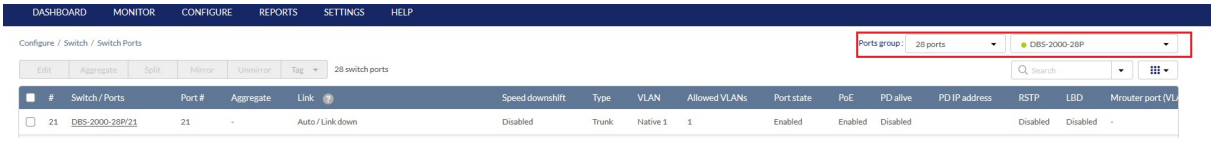
Click now on “configure ports on the switch” to manually modify the specific switch/port.



Now you can select the ports you want to configure.

! This settings will become active immediately!

! TIPP #1: Filter the Switch type and Profile you want, otherwise all switches within the Profile will be displayed.



! TIPP #2: provide each switch a unique name, otherwise it might be difficult to differentiate in between them.

! TIPP #3: when configuring the ports later, at some browsers it will not be displayed immediately correctly, so refreshing the page can solve this.

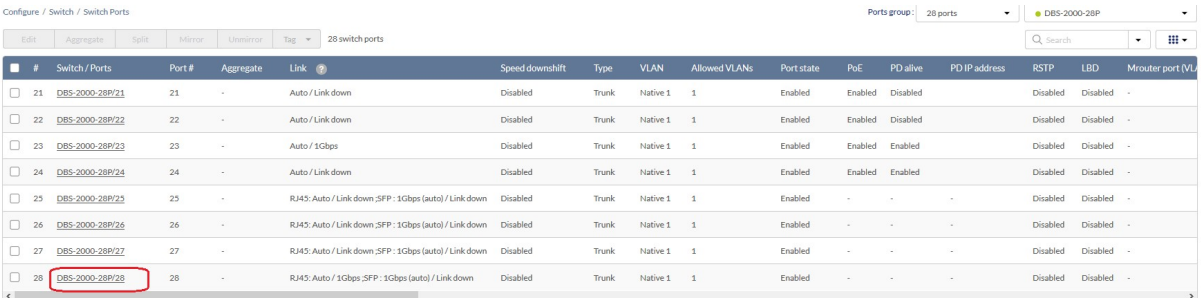
For our scenario we need to configure Port 28 as VLAN Trunk with VLAN 1 = untagged and VLAN 10 = tagged as Uplink to the other Switch.

For our scenario we need to configure Port 24 as VLAN Trunk with VLAN 1 = untagged and VLAN 10 = tagged as Uplink to the AP.

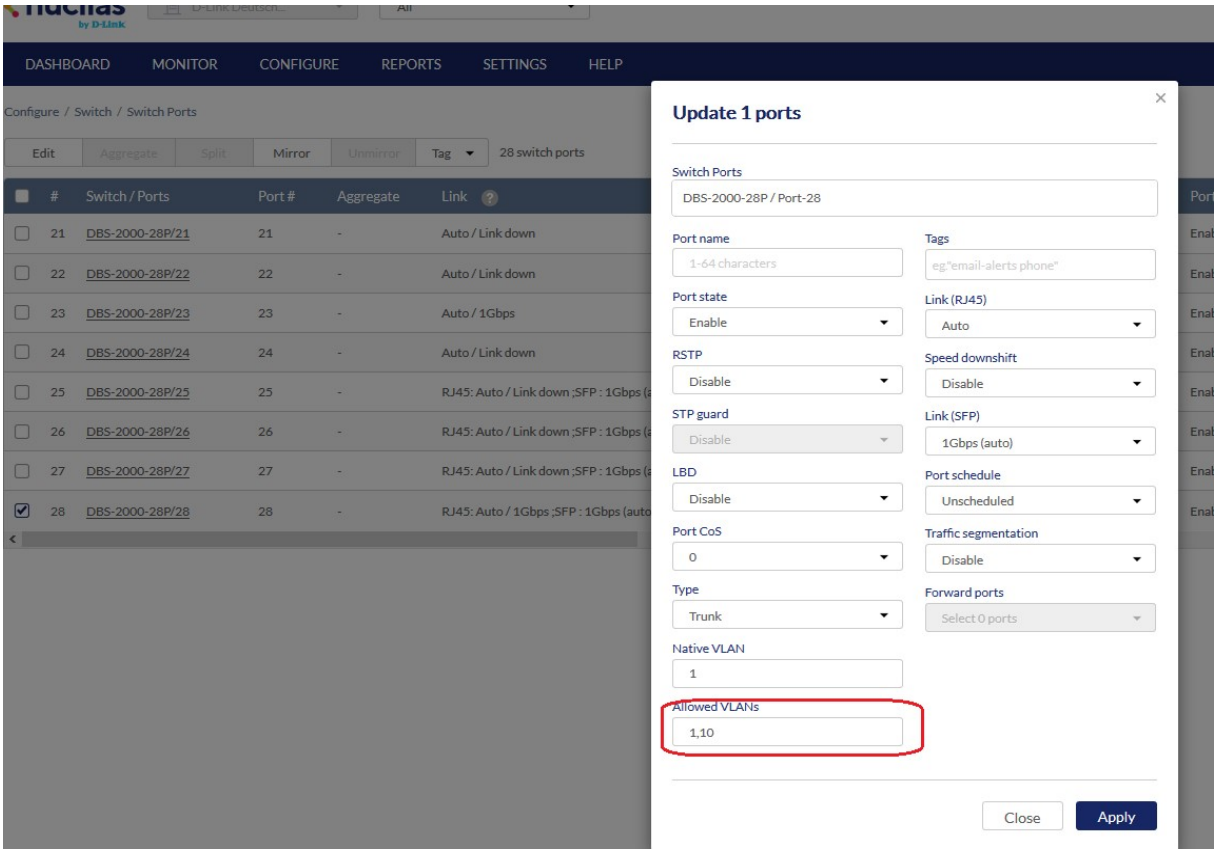
So now slide the sides, till you reach the port you want to configure.

At first we modify the Uplink, so that the VLANs are being transmitted to other switches too.

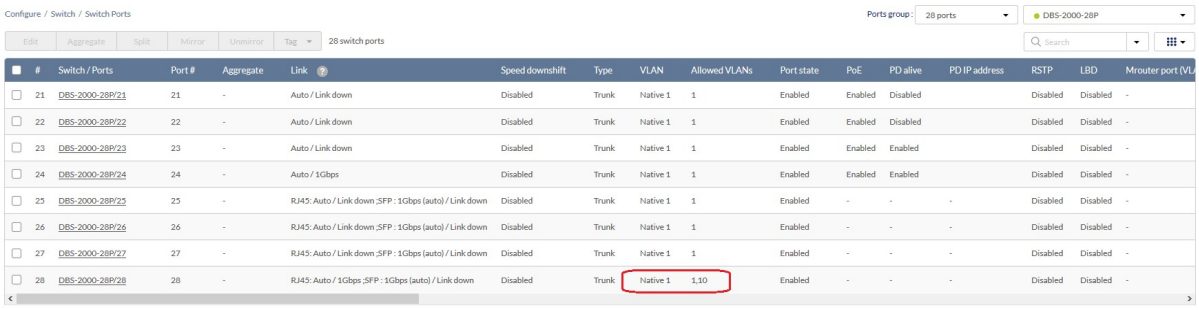
Click on the Switch/Port to modify the settings.



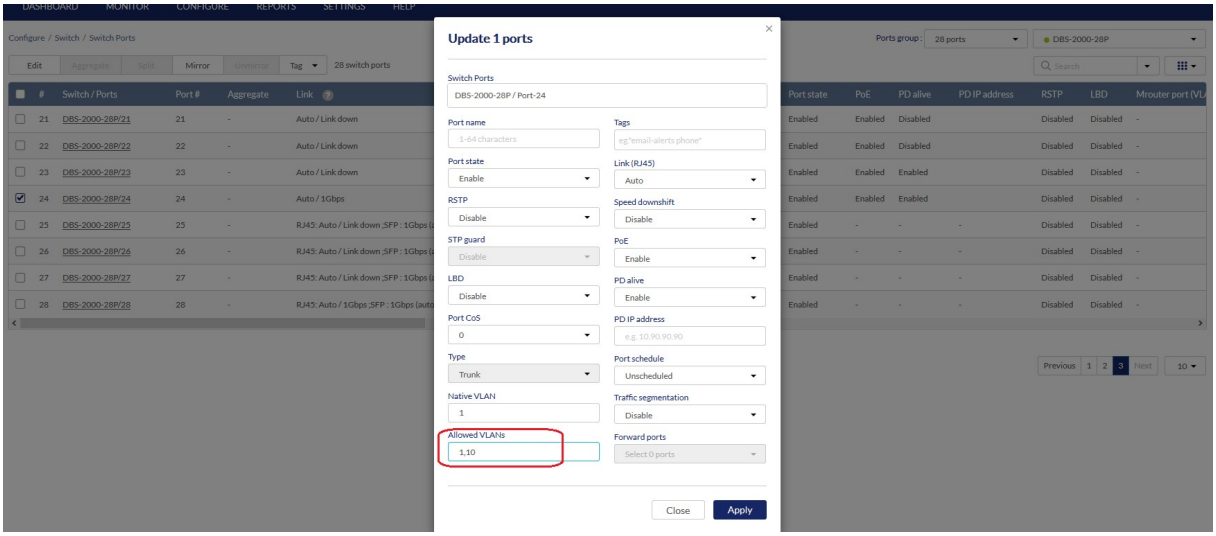
Add the VLAN 10 to allowed VLANs, so that it can be transmitted correctly.



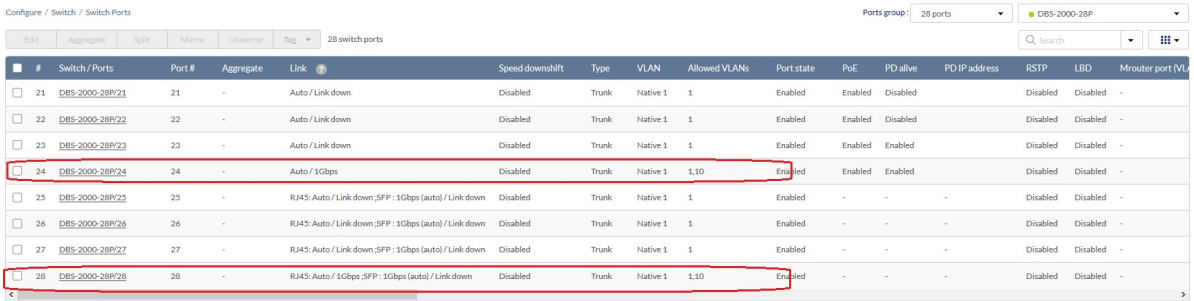
(After refreshing the browser) it will be displayed like this, showing that VLAN 10 is now transmitted correctly.



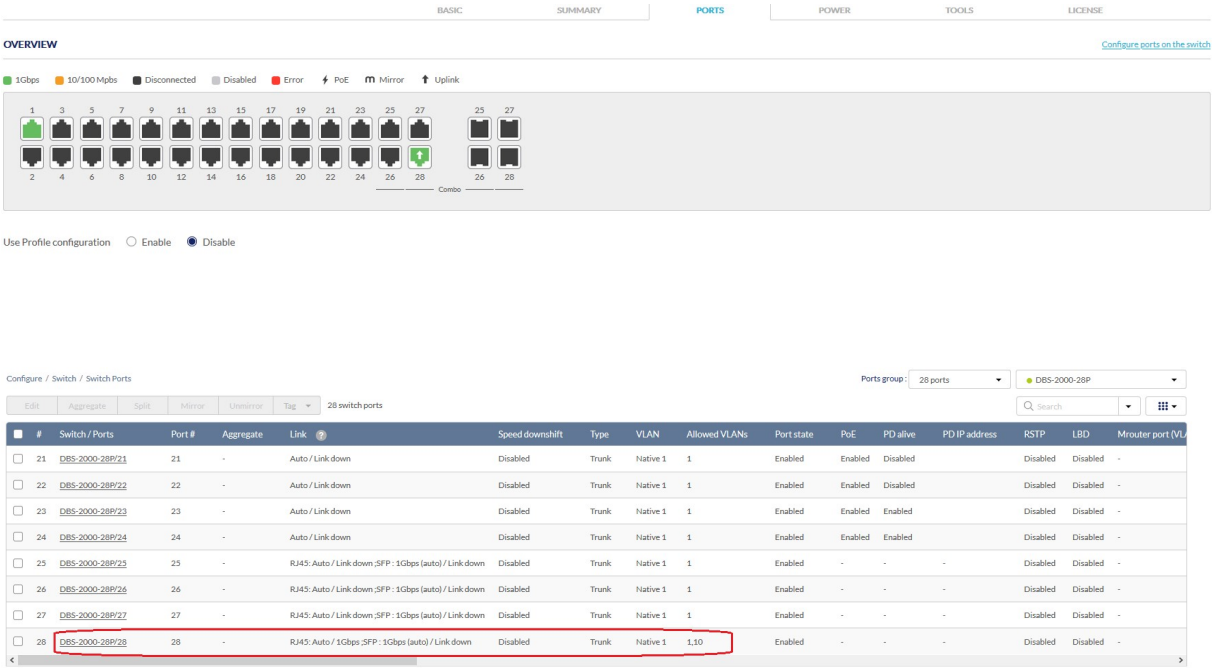
The settings of the AP Port now are exactly the same according to our scenario, so modifying Port 24 will look like this.



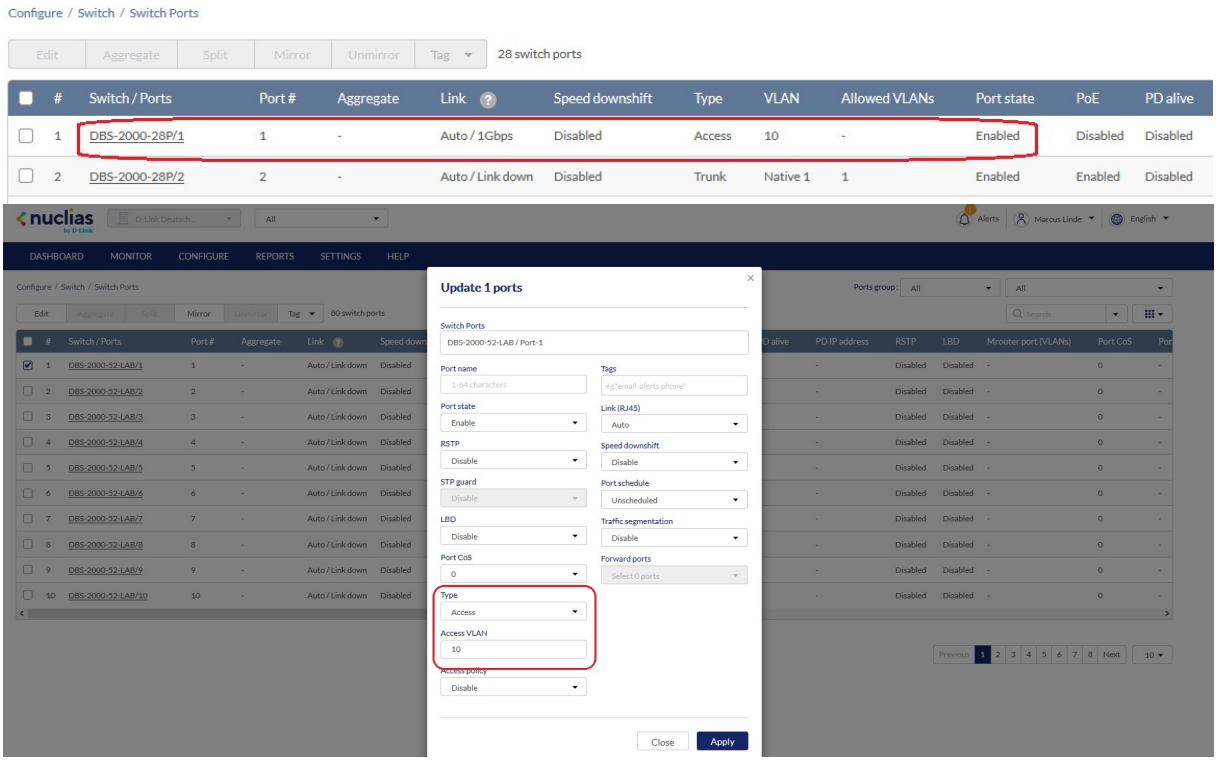
Now the APs GuestSSID VLAN also will be passed trough the switch.



Repeat the steps now for the Switch with the router Access-Ports.

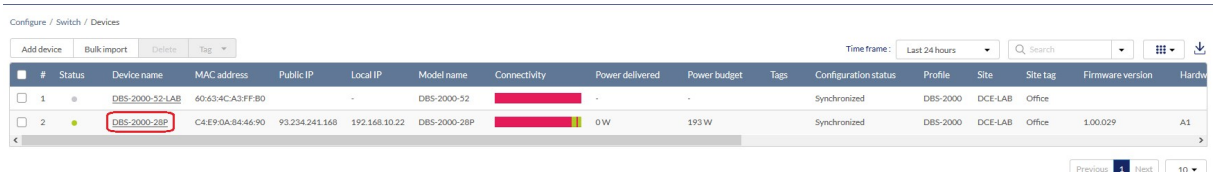


For the Access-Port now select the Port 1 and modify it to “ACCESS” VLAN 10.

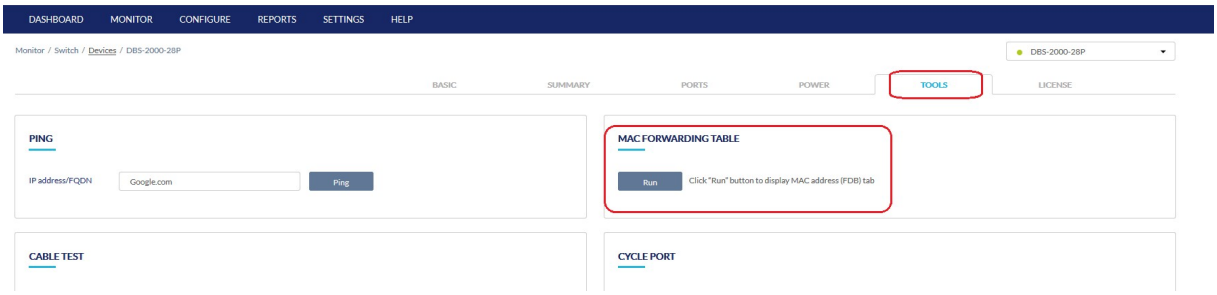


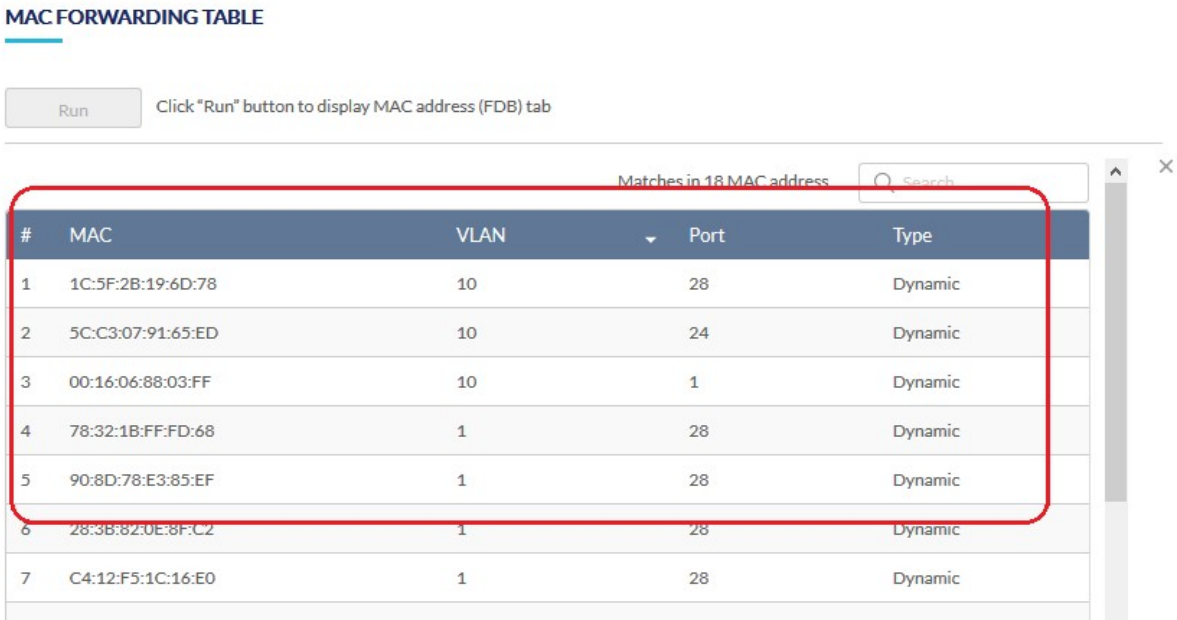
If you want to verify the VLAN working correctly, you can check the device's FDB (Forwarding Data Base).

Go to the Switch's Device overview.



Select the Switch you want to check and then go to "Tools" and select "Run" at the MAC Forwarding Table.





The MAC Address in the FDB is the same as the one from the connected WLAN Client.