

RAP Setup mit OVC

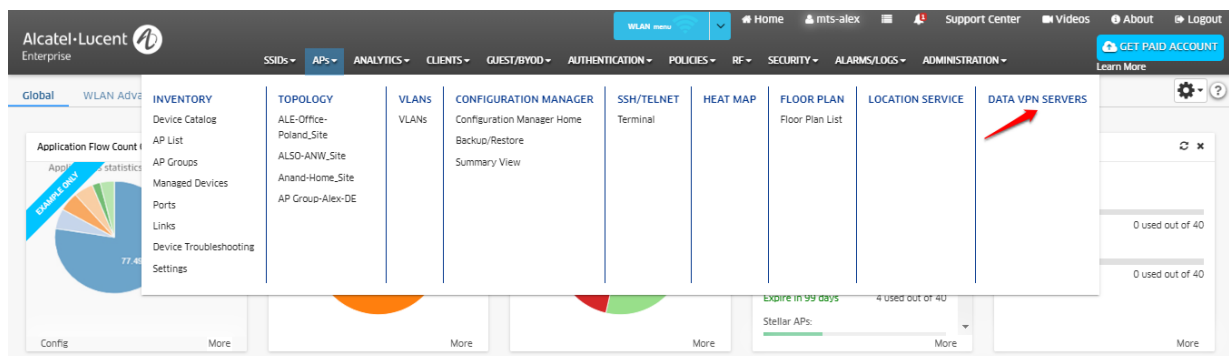
Erstellen von 2 SSIDs in unterschiedlichen VLANs und Konfiguration der Downlink-Ports an AP1201H.

Ziel: Verwenden von unterschiedlichen VLANs an AP1201H im RAP Mode.

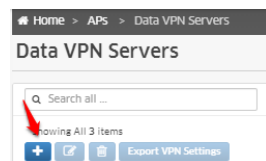
1. Erstellen der SSIDs mit unterschiedlichen Tunnel-Profilen

1.1 Anlegen der Data VPN Servers Profile

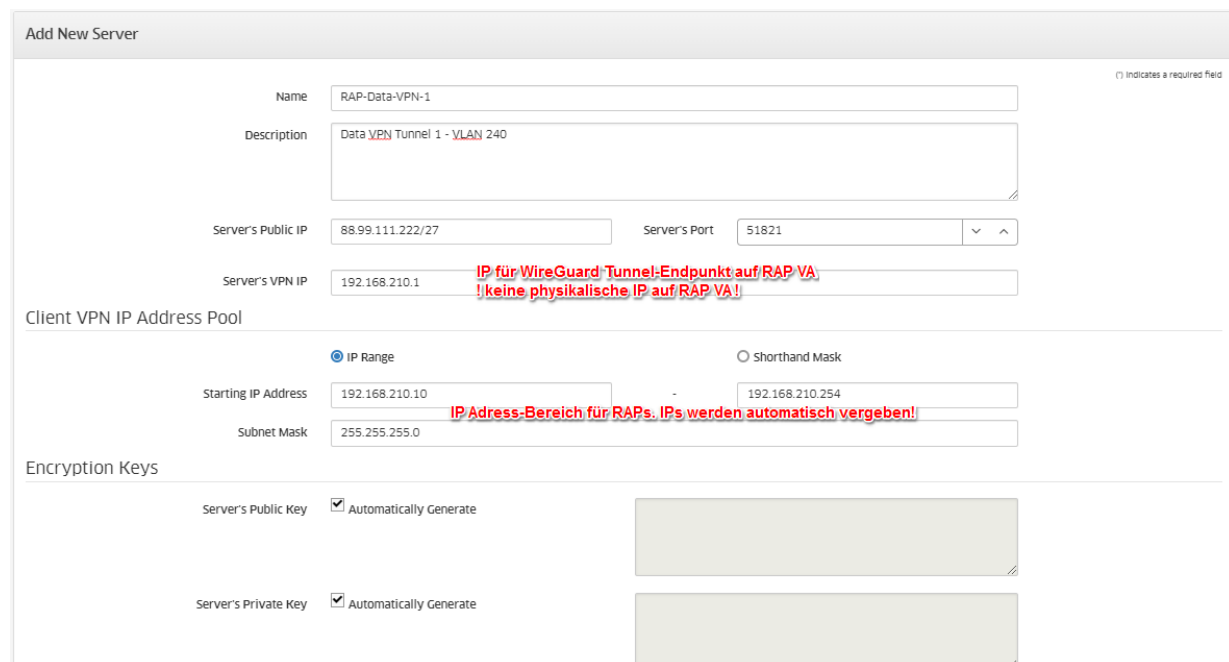
- Wechseln in das Menü: DATA VPN SERVERS (Ab OVC 4.5.1):



- Erstellen von 2 DATA VPN SERVERS Profilen:



- Erstellen des VPN Server Profils für Data-VPN 1:

The screenshot shows the 'Add New Server' configuration form. The form has several sections:

- Name:** RAP-Data-VPN-1
- Description:** Data VPN Tunnel 1 - VLAN 240
- Server's Public IP:** 88.99.111.222/27
- Server's Port:** 51821
- Server's VPN IP:** 192.168.210.1. A red note below this field says: 'IP für WireGuard Tunnel-Endpunkt auf RAP VA! keine physikalische IP auf RAP VA!'
- Client VPN IP Address Pool:** The 'IP Range' radio button is selected. The 'Starting IP Address' is 192.168.210.10 and the 'Subnet Mask' is 255.255.255.0. A red note below the IP range says: 'IP Adress-Bereich für RAPs. IPs werden automatisch vergeben!'. The 'Shorthand Mask' radio button is unselected.
- Encryption Keys:** Both 'Server's Public Key' and 'Server's Private Key' have the 'Automatically Generate' checkbox checked.

- Erstellen des VPN Server Profils für Data VPN 2:

Add New Server

Name: RAP-Data-VPN-2

Description: Data VPN Tunnel 2 - VLAN 241

Server's Public IP: 88.99.111.222/28 **gleiche öffentl. IP, andere Subnetzmaske**

Server's Port: 51822 **zusätzlicher WG Port**

Server's VPN IP: 192.168.211.1

Client VPN IP Address Pool

IP Range Shorthand Mask

Starting IP Address: 192.168.211.10

Subnet Mask: 255.255.255.0

Encryption Keys

Server's Public Key: Automatically Generate

Server's Private Key: Automatically Generate

Zwei Data VPN Servers Profile mit unterschiedlichen WG Ports mit Verweis auf die gleiche öffentliche IP-Adresse:

Home > APs > Data VPN Servers

Data VPN Servers

Showing All 5 items

Name	Description	Server's Public IP	Server's VPN IP	Server's Port
RAP-Data-VPN-1	Data VPN Tunnel 1 - VLAN 240	88.99.111.222/27	192.168.210.1	51821
RAP-Data-VPN-2	Data VPN Tunnel 2 - VLAN 241	88.99.111.222/28	192.168.211.1	51822

Showing Page 1 of 1

- Erstellen der AP-Gruppe für RAP:

INVENTORY

Home > APs > Inventory > AP Groups

AP Group

Create New Group

General

*Group Name: AP-Group-RAP

Group Description:

Auto-Group VLANs:

*RF Profile: default profile

Time

Timezone: (UTC-01:00)Amsterdam,Berlin,Bern,Rome,Stockholm,Vienna

Daylight Saving Time: ON

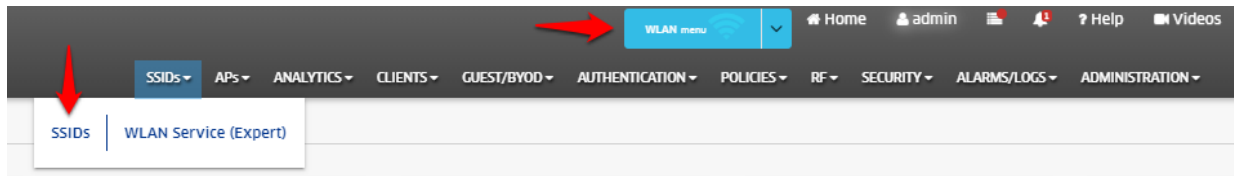
Data VPN Setting

Data VPN Server(s): RAP-Data-VPN-1, RAP-Data-VPN-2 **auswählen der 2 VPN DATA SERVERS Profile**

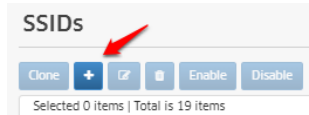
< Back Next Commit Cancel

1.2 Erstellen der SSIDs

- Wechseln in das SSID Menü:



- Erstellen einer SSID über:



- Name der ESSID und Verwendungszweck (z.B. PSK):

The screenshot shows the 'Create SSID' form. The fields are: '*SSID Service Name' (Stellar RAP Home VLAN 240), '*SSID' (Stellar RAP SSID 1), and 'Usage' (Protected Network (Pre-Shared Key & an optional Captive Portal)). There is a 'Do you want users to go through a Captive Portal?' toggle set to 'NO'. At the bottom, there are 'Create & Customize' and 'Cancel' buttons. Red arrows point to the 'Stellar RAP Home VLAN 240' field, the 'Stellar RAP SSID 1' field, and the 'Create & Customize' button.

- Auswählen des Untagged VLANs und VPN Servers Profils:


The screenshot shows the configuration page for the SSID. The fields are: 'SSID Service Name' (Stellar RAP Home VLAN 240), 'SSID' (Stellar RAP SSID 1), 'Usage' (Protected Network (Pre-Shared Key & an optional Captive Portal)), 'Security Level' (Personal), 'Guest Portal' (No), 'Allowed Band' (All), 'Encryption Type' (WPA3_PSK_SAE_AES), '*Password' (*****), '*Confirm Password' (*****), and 'Device Specific PSK' (Disabled).

The screenshot shows the 'Authentication Strategy' and 'Default VLAN/Network' sections. The 'Authentication Strategy' section has 'MAC Authentication' set to 'DISABLED'. The 'Default VLAN/Network' section has 'Configure Access Role Attributes' selected. The 'VLAN(s)' field is set to 'Untagged VLAN'. The 'Use Tunnel' checkbox is checked. The 'Config Tunnel' section has '*Tunnel ID' set to '0' and '*GRE Tunnel Server IP Address/Data VPN Server' set to 'RAP-Data-VPN-1 (192.168.210.1)'. At the bottom, there are 'Support of Entropy' (DISABLED) and 'Allow Local Breakout' (DISABLED) toggles. A red arrow points to the 'Untagged VLAN' field, another red arrow points to the 'RAP-Data-VPN-1 (192.168.210.1)' field, and a third red arrow points to the 'Save and Apply to AP Group' button at the bottom right.

- Ausrollen auf die AP-Gruppe für RAP:

SSID Service Name


SSID

AP Group(s)  1 selected AP Group(s) [Change Selection](#)

Set same schedule for all selected AP Groups | [Edit Schedule](#) ⓘ

AP-Group-RAP ⓘ

Show Showing Page 1 of 1 [<](#) [<](#) [1](#) [>](#) [>](#)

 [Apply](#) [Cancel](#)

- Wiederholen der Schritte 1.3.3 bis 1.3.5 für SSID 2!

2. [Zuweisen der VLANs auf die Downlink-Ports des AP1201H](#)

2.1 Ausrollen von Access Auth Profiles auf die Downlink-Ports

- Wechseln in das Menü WLAN Service (Expert):

WLAN menu

SSIDs ▾ APs ▾ ANALYTICS ▾ CLIENTS ▾ GUEST/BYOD ▾ AUTHENTICATION ▾ POLICIES ▾ RF ▾

SSIDs | **WLAN Service (Expert)**

- Wechseln in das Untermenü Access Auth Profile und anlegen eines Profils (ohne Authentifizierung)
- Erstellen des Access Auth Profils für z.B. VLAN 240:

TEMPLATE

Home > Policies > Unified Profile > Template > Access Auth Profile

Access Auth Profile

Create Access Auth Profile

* Profile Name ⓘ indicates a required field

Default Settings

AAA Server Profile

Port-Bounce

MAC Auth

802.1X Auth

Customer Domain ID

No Auth/Failure/Alternate

Trust Tag

Access Classification

Default Access Role Profile

802.1X Authentication

- Übertragen des Profils auf die AP-Gruppe:

The screenshot shows the 'Access Auth Profile' configuration page in the Alcatel-Lucent Enterprise management console. The left sidebar contains a navigation menu with categories like 'Access Auth Profile', 'Access Policies', and 'Global Configuration'. The main area displays a table of profiles. The profile 'Access Auth Profile: VLAN 240' is selected, and a red arrow points to the 'Apply to Devices' button at the top right. The right-hand pane shows the 'Default Settings' for this profile, including AAA Server Profile, Port-Bounce, MAC Auth, and 802.1X Auth settings.

- Auswählen des/der Ports für z.B. VLAN 240:

The screenshot shows the 'Access Auth Profile Assignments' page. It displays the assignment of the 'Access Auth Profile: VLAN 240' to a device group. The 'Devices' section shows '0 Devices' and '1 AP Group'. The 'List of Selected AP Groups' section shows 'AP-Group-RAP' with three ports: 'Eth1', 'Eth2', and 'Eth3'. The 'Eth3' checkbox is checked, and a red arrow points to it. At the bottom right, the 'Apply' button is highlighted with a red arrow.

Wiederholen der o.a. Schritte für weitere VLANs und ausrollen auf die Downlinkports des AP1201H

Zusammenfassung:

Mit dieser Konfigurationsanleitung wird das Ausrollen von SSIDs und VLANs auf die Downlinkports im RAP_Modus beschrieben. Im Beispiel wird der Stellar AP1201H verwendet.

Systemvoraussetzung:

OmniVista Cirrus: Release 4.5.1 oder neuer

Stellar WLAN: AWOS 4.0.0.42 oder neuer

Access Point: Stellar AP1201H