

How to provide Guest and Employ access with the same SSID using Instant solution with WAP2-Enterprise

The idea of the tutorial was to be able to introduce new clients to the Aruba solution with the minimal investment in the hardware. Once the client would understand the benefits of getting Aruba hardware in his environment and would require an increase in scale we would depending on the size campus solution or we would stick with the instant solution.

High level the solution is to use a WPA2-Enterprise and internal Radius server in order to provide 2 or more user roles.

The first thing that we want first to think about is how to do the separation of the usernames between the Guest and Employee. The way I will do it is to use a set of character specific to each type, for Guest the username will start with "GU" and the employee will start with "EM"

Now we will configure the Users:

- Under **Security -> Users for Internal Server** we will add our usernames and passwords using the type **Employee**

The screenshot shows the 'Security' configuration window with the 'Users for Internal Server' tab selected. The window has a blue header with 'Security' and a 'Help' link. Below the header are several tabs: 'Authentication Servers', 'Users for Internal Server' (active), 'Roles', 'Blacklisting', 'Firewall Settings', 'Walled Garden', and 'External Captive Portal'. The main area contains a table with two columns: 'Users(2)' and 'Type'. The table lists two users: 'GUtest' and 'EMtest', both with the type 'Employee'. To the right of the table is a form titled 'Add new user:' with fields for 'Username:', 'Password:', 'Retype:', and 'Type' (a dropdown menu currently showing 'Guest'). Below the 'Type' dropdown is an 'Add' button. At the bottom left of the table area are buttons for 'Edit', 'Delete', and 'Delete All'. At the bottom right of the window are 'OK' and 'Cancel' buttons.

- Next step will be to create the 2 user roles that we will want to give to the Guest users will be put under "Guest_wpa" and Employ users will be put under "Employee_wpa"

At this stage we will start to configure the SSID that will bring all this together:

- Step 1 :

The screenshot shows the 'New WLAN' configuration page with the 'WLAN Settings' tab selected. The page is divided into several sections:

- Name & Usage:** Name (SSID) is 'Company'. Primary usage is 'Employee' (selected), with 'Voice' and 'Guest' as options.
- Broadcast/Multicast:** Broadcast filtering is 'All'. DTIM interval is '1 beacon'. Multicast transmission optimization is 'Enabled'. Dynamic multicast optimization is 'Enabled'. DMO channel utilization threshold is 0%.
- Transmit Rates:** 2.4 GHz: Min: 12, Max: 54. 5 GHz: Min: 24, Max: 54.
- Bandwidth Limits:** Airtime and Each radio are unchecked. Downstream and Upstream rates are 0 kbps, both with 'Per user' checkboxes.
- Background WMM share:** 0%.
- Best effort WMM share:** 0%.
- Video WMM share:** 0%.
- Voice WMM share:** 0%.
- Miscellaneous:** Content filtering is 'Disabled'. Band is 'All'. Inactivity timeout is 1000 secs. Hide SSID and Disable SSID are unchecked. Can be used without uplink is checked. Max clients threshold and Local probe request threshold are 0.

At the bottom, there is a 'Hide advanced options' link and 'Next' and 'Cancel' buttons.

- Step 2 (We could do Virtual Controller assigned or Network with VLAN's and Client VLAN Assignment Dynamic if we want to split the users on VLAN's too)

The screenshot shows the 'New WLAN' configuration page with the 'VLAN' tab selected. The page is titled 'Client IP & VLAN Assignment'.

- Client IP assignment:** 'Virtual Controller assigned' and 'Network assigned' are options, with 'Network assigned' selected.
- Client VLAN assignment:** 'Default', 'Static', and 'Dynamic' are options, with 'Dynamic' selected.
- VLAN Assignment Rules:** A table with one rule: 'Default VLAN: 100'.
- Buttons:** 'New', 'Edit', 'Delete', and two arrow buttons (up and down) are located below the table.

At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

- Step 3 – we will choose Enterprise with Key management WPA-2 Enterprise and of course we will choose for the Authentication server the internal server:

New WLAN Help

1 WLAN Settings 2 VLAN 3 **Security** 4 Access

Security Level

More Secure
Less Secure

Enterprise
Personal
Open

Key management: WPA-2 Enterprise ☒ Opportunistic Key Caching(OKC)

802.11r roaming: Enabled

Termination: Disabled

Authentication server 1: InternalServer

Reauth interval: 8 hrs.

MAC authentication: ☐ Perform MAC authentication before 802.1X
☐ MAC authentication fail-thru

Internal server: [2 Users](#)

Internal server: Default certificate [Upload certificate](#)

Blacklisting: Enabled

Max authentication failures: 2

Back Next Cancel

- Step 4 – Access rules will be Rule-based and then we create the Role Assignment Rules as in the picture below:

New WLAN Help

1 WLAN Settings 2 VLAN 3 Security 4 **Access**

Access Rules

More Control
Less Control

Role-based
Network-based
Unrestricted

Roles: default_wired_port_profile, wired-instant, EAruba

Access Rules

Role Assignment Rules

If User-Name starts-with GU assign role Guest_wpa

Default role: Company

New Role Assignment Rule

Attribute: User-Name Operator: starts-with String: EM Role: Employee_wpa

OK Cancel

☐ Enforce Machine Authentication

Back Finish Cancel

The only improvement that I would like to see for this setup is to have the Reauth interval defined on the user role.