

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**

Users(2)	Type
GUtest	Employee
EMtest	Employee

Add new user:

Username:

Password:

Retype:

Type:

- 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 Employee 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 interface with the 'WLAN Settings' tab selected. The interface is divided into several sections:

- Name & Usage:** Name (SSID) is 'Company'. Primary usage is 'Employee'.
- Broadcast/Multicast:** Broadcast filtering is 'All', DTIM interval is '1 beacon', Multicast transmission optimization is 'Enabled', and Dynamic multicast optimization is 'Enabled'.
- Transmit Rates:** 2.4 GHz: Min: 12, Max: 54; 5 GHz: Min: 24, Max: 54.
- Bandwidth Limits:** Includes checkboxes for 'Airtime' and 'Each radio', and input fields for 'Downstream' and 'Upstream' (both in kbps) with 'Per user' checkboxes.
- Miscellaneous:** Content filtering is 'Disabled', Band is 'All', Inactivity timeout is '1000 secs', and 'Can be used without uplink' is checked.

Buttons for 'Next' and 'Cancel' are visible at the bottom right.

- 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 interface with the 'VLAN' tab selected. The section is titled 'Client IP & VLAN Assignment'.

- Client IP assignment:** 'Network assigned' is selected.
- Client VLAN assignment:** 'Dynamic' is selected.
- VLAN Assignment Rules:** A table with one row: 'Default VLAN: 100'.

Buttons for 'New', 'Edit', 'Delete', and arrows are located below the table. 'Back', 'Next', and 'Cancel' buttons are at the bottom right.

- 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
 - Enterprise
 Personal
 Open
 Less Secure

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
 - Role-based
 - Network-based
 - Unrestricted
 Less Control

Roles: default_wired_port_profile, wired-instant, EAruba
 Access Rules: (empty)

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.