

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

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 simple external captive portal, because this option provides access to the role base authentication on the iAP, with the internal Radius server. The external captive portal can be hosted on any computer that has apache with php installed.

We will start first with preparing the core code for the HTML pages that we will use to give access:

- Index.html will provide the choice of Guest or Employ access :

```
<form method=POST action="http://securelogin.arubanetworks.com/cgi-bin/login">
  <input name=user value="GUsername" type="hidden">
  <input name=password value="GUpassword" type="hidden">
  <input name=cmd value="authenticate" type="hidden">
  <input name=mac value="" type="hidden">
  <input name=ip value="" type="hidden">
  <input name=ssid value="" type="hidden">
  <input name=url value="http://www.google.com" type="hidden">
  <BR><input type="submit" name="Guest" value="login" class="button" />
</form>
<a href="employ.html"><button type="button">Employ Access </button></a>
```

- Employ.html will provide the possibility to enter a username and password

```
<form method=POST action="http://securelogin.arubanetworks.com/cgi-bin/login">
  Username: <input name=user value="">
  Password: <input name=password value="" type="password" size=25>
  <input name=cmd value="authenticate" type="hidden">
  <input name=mac value="" type="hidden">
  <input name=ip value="" type="hidden">
  <input name=ssid value="" type="hidden">
  <input name=url value="http://www.google.com" type="hidden">
  <BR><input type="submit" name="Guest" value="login" class="button" />
</form>
```

Now that the pages are done we will start to configure the iAP to provide different roles based on what username is typed:

- We will configure first the captive portal profile on the iAP:
 - o Under **Security** -> **External Captive Portal** we will click the New button

The screenshot shows the 'Security' configuration window with the 'External Captive Portal' tab selected. A modal dialog titled 'ext_portal' is open, allowing configuration of a new captive portal profile. The fields are as follows:

Field	Value
Type	Radius Authentication
IP or hostname	10.255.47.119
URL	/cp/
Port	80
Use https	Disabled
Captive Portal failure	Deny internet
Automatic URL Whitelisting	Disabled
Redirect URL	http://google.com (optional)

Buttons: OK, Cancel

- Now we will configure the Users:
 - o Under **Security** -> **Users for Internal Server** we will add our usernames and passwords using the type **Guest**

The screenshot shows the 'Security' configuration window with the 'Users for Internal Server' tab selected. It displays a list of existing users and a form to add a new user.

Username	Type
GUsername	Guest
EMdan	Guest

Buttons: Edit, Delete, Delete All

Add new user:

Username:	
Password:	
Retype:	
Type	Guest

Button: Add

Buttons: OK, Cancel

- 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_cp” and Employ users will be put under “Employ_cp”

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 'Guest' (selected).
- Broadcast/Multicast:** Broadcast filtering is 'Disabled'. DTIM interval is '1 beacon'. Multicast transmission optimization is 'Disabled'. Dynamic multicast optimization is 'Disabled'. DMO channel utilization threshold is '0 %'.
- Transmit Rates:** 2.4 GHz: Min: 11, Max: 54. 5 GHz: Min: 12, Max: 54.
- Bandwidth Limits:** Airtime and Each radio are unchecked. Downstream and Upstream rates are set to '0 kbps' with 'Per user' selected. Background WMM share, Best effort WMM share, Video WMM share, and Voice WMM share are all set to '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 set to '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' and contains the following sections:

- Client IP assignment:** 'Virtual Controller assigned' and 'Network assigned' (selected).
- Client VLAN assignment:** 'Default' (selected), 'Static', and 'Dynamic'.
- VLAN Assignment Rules:** A table with one rule: 'Default VLAN: 100'.

At the bottom, there are 'New', 'Edit', 'Delete', and arrow buttons, and 'Back', 'Next', and 'Cancel' buttons.

- Step 3 – we will choose the Slash page type to external and choose the Captive portal profile to the one that we have created previously (Marked in red are the options that need to be changed the other options are optional):

New WLAN [Help](#)

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

Security Level

Splash page type: External

Captive portal profile: ext_portal [Edit](#)

WISPr: Disabled

MAC authentication: Disabled

Auth server 1: InternalServer

Reauth interval: 0 min.

Internal server: 3 Users

Blacklisting: Disabled

Walled garden: Blacklist: 0 Whitelist: 0

Disable if uplink type is: ☐ 3G/4G ☐ Wifi ☐ Ethernet

Encryption: Disabled

[Back](#) [Next](#) [Cancel](#)

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

Edit Company [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

EAruha

[New](#) [Delete](#)

Access Rules

[New](#) [Edit](#) [Delete](#) [Up](#) [Down](#)

Role Assignment Rules

If User-Name starts-with GU assign role Guest_CP

Default role: Company

New Role Assignment Rule

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

[OK](#) [Cancel](#)

☐ Assign pre-authentication role

[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