

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 dialog box titled 'ext_portal' is open, displaying the following configuration fields:

- 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 for 'OK' and 'Cancel' are visible at the bottom of the dialog box and the main window.

- 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. The interface displays a table of existing users and a form to add a new user.

Users(2)	Type
GUsername	Guest
EMdan	Guest

Buttons for 'Edit', 'Delete', and 'Delete All' are located below the table.

Add new user:

- Username:
- Password:
- Retype:
- Type: Guest

An 'Add' button is located below the 'Type' dropdown.

Buttons for 'OK' and 'Cancel' are visible at the bottom of the main window.

- 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 :

- 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)

- Step 3 – we will choose the Splash 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

Less Control

Role-based
 Network-based
 Unrestricted

Roles

default_wired_port_profile
wired-instant
EAruba

New Delete

Access Rules

New Edit Delete ↑ ↓

Role Assignment Rules

If User-Name starts-with GU assign role Guest_CP

Default role: Company

New Role Assignment Rule

Attribute: Operator: String: Role:

User-Name starts-with EM 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