

ArubaOS + Amigopod Integration Cheat Sheet

FOR ARUBA NETWORKS EMPLOYEES. CUSTOMERS AND PARTNERS

Table of Contents

1. Create RADIUS Server instance	3
2. Add RADIUS Server to a Server Group.....	3
3. Create Captive Portal Profile	4
4. Configure Authentication for Captive Portal Profile.....	5
5. Create AAA Profile	6
6. Enable Captive Portal on Initial Role of Captive Portal Profile	7
7. Ensure the Amigopod IP Address allowed in captiveportal policy	8
8. Configure Guest VAP with new AAA Profile	9
9. Configure RADIUS NAS for Aruba Controller	10
10. Configure Web Login for Captive Portal Authentication	11
11. Configure RADIUS User Role.....	15
13. Check RADIUS Accounting is working as expected.....	17
14. Troubleshooting Tips	18

1. Create RADIUS Server instance

The core of Amigopod is a RADIUS server so the basis of the integration in ArubaOS is the full AAA config. Amigopod uses the default ports of 1812 for Authentication and 1813 for Accounting.

The screenshot shows the ArubaOS Mobility Controller interface for configuring a RADIUS Server. The breadcrumb is **Security > Authentication > Servers**. The left sidebar shows the navigation menu with **Security > Authentication** selected. The main content area is titled **RADIUS Server > Guest-Auth** and contains the following configuration table:

Host	110.0.20.58	Key	***** Retype: *****
Auth Port	1812	Acct Port	1813
Retransmits	3	Timeout	5 sec
NAS ID	Aruba620	NAS IP	10.0.20.45
Use MD5	<input type="checkbox"/>	Mode	<input checked="" type="checkbox"/>

2. Add RADIUS Server to a Server Group

Add the newly created RADIUS Server to a Server Group so it is ready to be referenced in future AAA Profiles.

The screenshot shows the ArubaOS Mobility Controller interface for configuring a Server Group. The breadcrumb is **Security > Authentication > Servers**. The left sidebar shows the navigation menu with **Security > Authentication** selected. The main content area is titled **Server Group > Guest-Auth-Srv** and shows the following configuration:

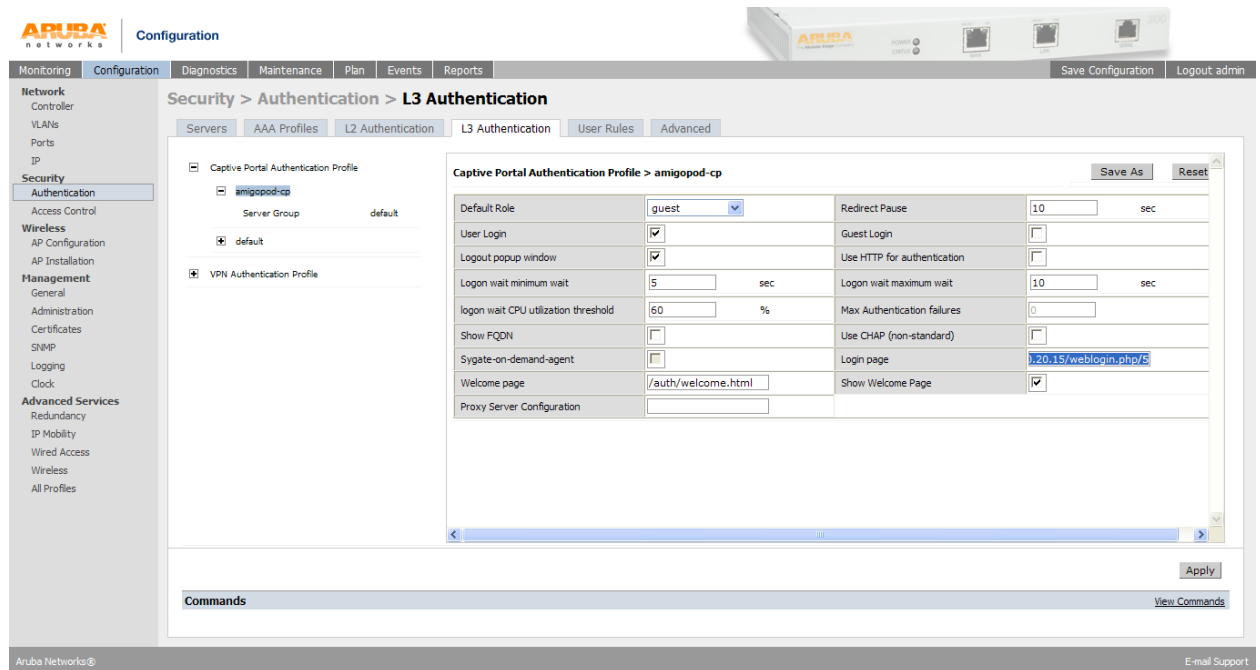
Fail Through:

Servers				
Name	Server-Type	trim-FQDN	Match-Rule	Actions
Guest-Auth	Radius	No		Edit Delete ▲ ▼
New				

Server Rules								
Priority	Attribute	Operation	Operand	Type	Action	Value	Validated	Actions
New								

3. Create Captive Portal Profile

One of the key features of Amigopod is the ability to host the branded Web Login or Captive Portal pages on the Amigopod appliance. The Captive Portal profile allows us to configure both the Login and optionally Welcome Pages to be hosted by Amigopod.



For example, we could set these pages to the following:

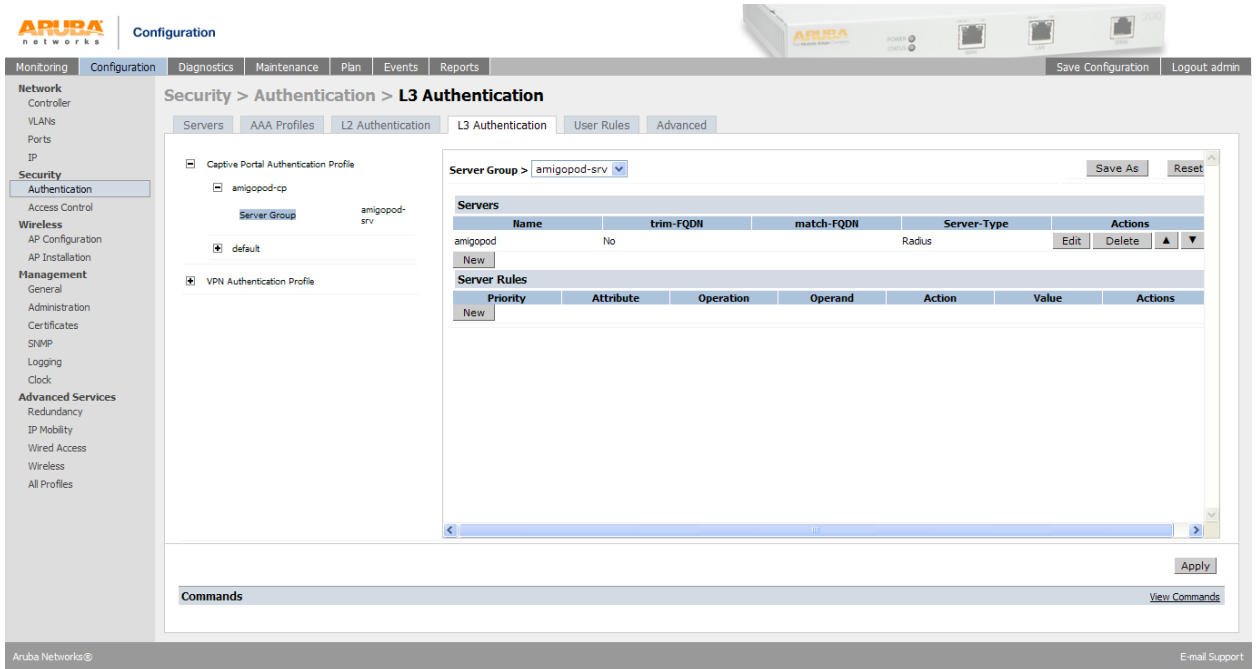
- **Login Page:** `https://<Amigopod IP Address or FQDN>/Aruba_login.php`
- **Welcome Page:** `https://<Amigopod IP Address or FQDN>/Aruba_welcome.php`

These URLs will be defined on the Amigopod in a later step as part of the Web Login configuration.

Note: Based on your customer's security policy make sure to change the Default Role of the Captive Portal profile to a Role that includes appropriate firewall policies.

4. Configure Authentication for Captive Portal Profile

Now the new Captive Portal Profile has been created, make sure the Server Group for the Amigopod RADIUS definition is selected as the authentication source.



The screenshot shows the ArubaOS configuration interface. The main navigation menu on the left includes sections for Network, Security, Wireless, Management, and Advanced Services. The current view is 'Security > Authentication > L3 Authentication'. The 'Servers' tab is selected, showing a configuration for the 'amigopod-srv' server group. The 'Server Group' dropdown is set to 'amigopod-srv'. Below this, there are two tables: 'Servers' and 'Server Rules'. The 'Servers' table has one entry for 'amigopod' with a 'Server-Type' of 'Radius'. The 'Server Rules' table is currently empty.

Servers						
Name	trim-FQDN	match-FQDN	Server-Type	Actions		
amigopod	No		Radius	Edit	Delete	
New						

Server Rules						
Priority	Attribute	Operation	Operand	Action	Value	Actions
New						

5. Create AAA Profile

The AAA Profile should be configured to have the *Initial Role* reference the newly created Captive Portal Profile.

The screenshot displays the ArubaOS configuration interface. The top navigation bar includes 'Monitoring', 'Configuration', 'Diagnostics', 'Maintenance', 'Plan', 'Events', and 'Reports'. The left sidebar shows a tree view of configuration categories: Network, Security, Wireless, Management, and Advanced Services. The main content area is titled 'Advanced Services > All Profile Management'. It is divided into two panes: 'Profiles' and 'Profile Details'. The 'Profiles' pane shows a tree view with 'amigopod-aaa' selected. The 'Profile Details' pane shows the configuration for the 'amigopod-aaa' profile, including fields for 'Initial role' (amigopod-cp), '802.1X Authentication Default Role' (guest), 'MAC Authentication Default Role' (guest), 'User derivation rules' (--NONE--), 'Wired to Wireless Roaming' (checked), and 'SIP authentication role' (--NONE--). There are 'Save As' and 'Reset' buttons at the top right of the details pane, and an 'Apply' button at the bottom right. A 'Commands' section is visible at the bottom of the main area.

Also ensure the *RADIUS Accounting Server Group* of the AAA profile is pointing to the Server Group created in Step 2 above.

6. Enable Captive Portal on Initial Role of Captive Portal Profile

This step is easy to miss and the Captive Portal will not be triggered.

The screenshot shows the Aruba Mobility Controller configuration interface. The breadcrumb path is **Security > User Roles > Edit Role(GoogleGuest-guest-logout)**. The left sidebar contains a navigation menu with categories like **Wizards**, **Network**, **Security**, **Wireless**, **Management**, **Advanced Services**, and **Wired Access**. The **Access Control** option is selected. The main content area shows various configuration sections: **Firewall Policies** (table with logon-control and captiveportal rules), **Re-authentication Interval** (Disabled), **Role VLAN ID** (Not Assigned), **Bandwidth Contract** (Upstream/Downstream: Not Enforced), **VPN Dialer** (Not Assigned), **L2TP Pool** (default-l2tp-pool), **PPTP Pool** (default-pptp-pool), and **Captive Portal Profile** (GoogleGuest-cp_prof). The **Captive Portal Profile** section is circled in red, indicating the step to select a profile and click the **Change** button.

Select the configured Captive Portal profile from the dropdown box and click the Change button to activate the redirect to Amigopod.

7. Ensure the Amigopod IP Address allowed in captiveportal policy

An entry needs to be placed in the firewall policy used to control pre-authentication traffic for the guest users. Typically this is defined in the *captiveportal* policy can be modified easily through the CLI or GUI.

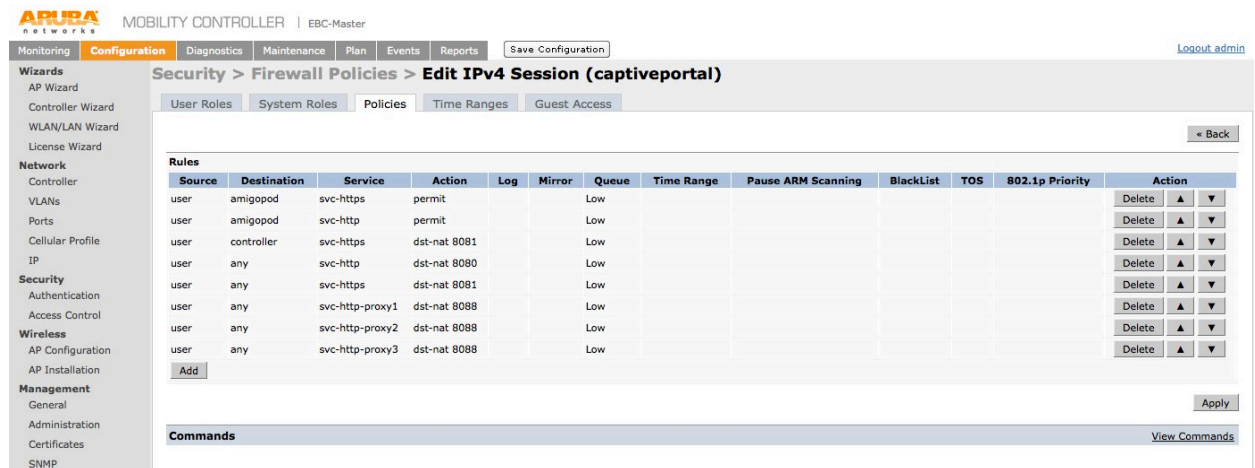
It is handy to define the Amigopod appliance in an alias definition as shown below:

```
netdestination Amigopod
    host 10.0.20.15
```

Add an entry that allows the client based HTTPS traffic to reach the hosted Captive Portal pages on the Amigopod appliance:

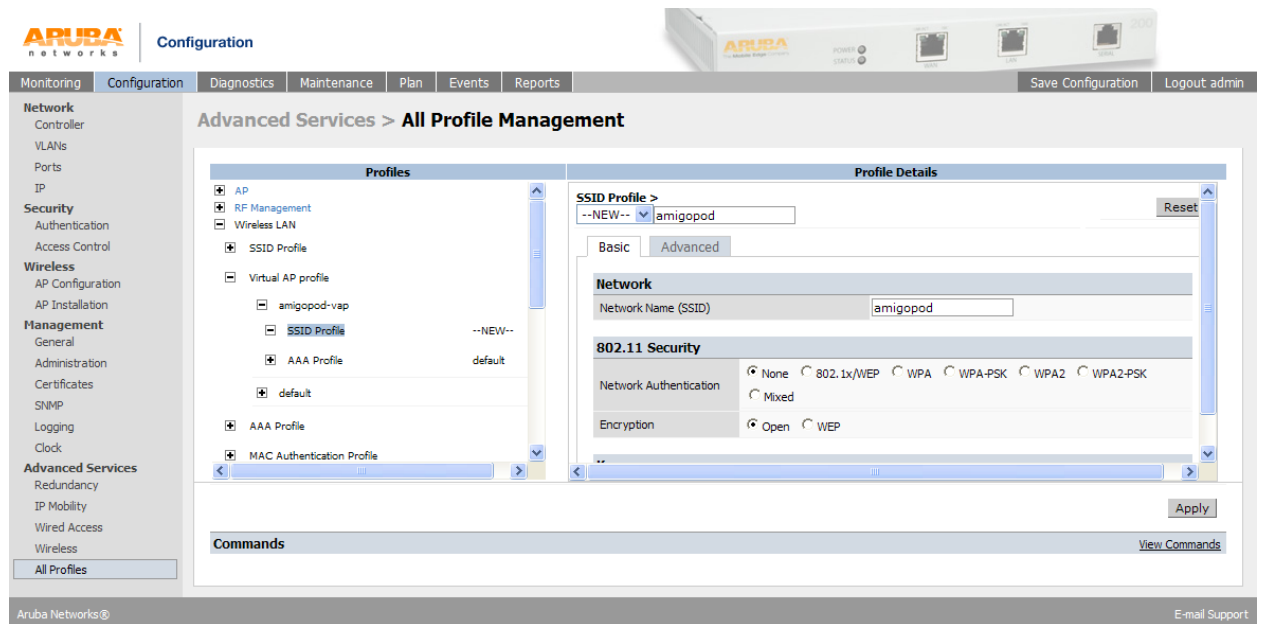
```
ip access-list session captiveportal
    user alias Amigopod svc-http permit
    user alias mswitch svc-https dst-nat
    user any svc-http dst-nat 8080
    user any svc-https dst-nat 8081
```

The equivalent the GUI configuration will look something like the screenshot below:



8. Configure Guest VAP with new AAA Profile

This cheat sheet assumes you have already got a Guest SSID up and running and the associated VAP deployed to an appropriate AP Group. To activate the new Amigopod specific Guest configuration, edit your VAP and ensure the *AAA Profile* for the VAP is set to the new AAA Profile configured in the previous step.



Assuming all this setup correctly the Aruba Controller should now be attempting to redirect to the Amigopod hosted Web Login page.

The next steps are to setup the corresponding components on the Amigopod configuration.

9. Configure RADIUS NAS for Aruba Controller

An entry for the Aruba Controller needs to be created under the Amigopod RADIUS Services→NAS List. The NAS Type should always be set for *Aruba (RFC 3576)* to allow the Amigopod to enable the support for RADIUS Dynamic Authorization.

As usual the shared secret must match on the Amigopod and the ArubaOS RADIUS Server definition.

The screenshot shows the 'RADIUS Network Access Servers' configuration page in the Aruba Networks web interface. The main heading is 'RADIUS Network Access Servers' with a sub-heading 'Each network access server that will use this RADIUS server for authentication or accounting purposes should be defined here.' Below this is a 'Create Network Access Server' form. The form has the following fields and options:

- Name:** Text input field containing 'Aruba-6000'. Description: 'A descriptive name for the network access server (NAS). This name is used to identify each NAS.'
- IP Address:** Text input field containing '10.0.20.58'. Description: 'The IP address or hostname of the network access server.'
- NAS Type:** Dropdown menu with 'Aruba (RFC 3576 support)' selected. Description: 'Select the type of NAS.'
- Shared Secret:** Password input field with masked characters. Description: 'The shared secret used by this network access server.'
- Confirm Shared Secret:** Password input field with masked characters. Description: 'Confirm the shared secret for this network access server.'
- Description:** Text area for notes. Description: 'Enter notes or descriptive text here.'
- Web Login:** A checked checkbox with the label 'Create a RADIUS Web Login page for this network access server'.

At the bottom of the form are three buttons: 'Create NAS Device', 'Reset Form', and 'Cancel'. A legend at the bottom left indicates '* required field'.

You can optionally check the *Web Login* option at the bottom of the form to automatically create the Web Login form based on the Aruba Networks presets.

Note: Once you have clicked the *Create NAS Device* you will be prompted to Restart the RADIUS Server. This is essential, as the RADIUS Server within Amigopod will reject any request from the Aruba Controller as unknown until the restart has been performed.

10. Configure Web Login for Captive Portal Authentication

Assuming you selected the *Web Login* checkbox on the previous step, there will already be a newly created Web Login page under the RADIUS Services → Web Logins. The screenshot below shows you the automatically created Web Login but you can equally create a new one manually at a later stage.

The screenshot shows the Aruba Networks RADIUS Web Login Editor interface. The page title is "RADIUS Web Login" and the subtitle is "Use this form to make changes to the RADIUS Web Login Aruba-6000 Login." The form is titled "RADIUS Web Login Editor" and contains several sections:

- Name:** Aruba-6000 Login
- Page Name:** Aruba_login
- Description:** Auto-generated web login for NAS Aruba-6000
- Vendor Settings:** Aruba Networks, Address: 10.0.20.58, Secure Login: Use vendor default
- Login Form:**
 - Custom Form: Provide a custom login form
 - Custom Labels: Override the default labels and error messages
 - Pre-Auth Check: Perform a local authentication check
 - Terms: Require a Terms and Conditions confirmation
- Default Destination:**
 - Default URL:
 - Override Destination: Force default destination for all clients

The *Page Name* field is what defines the URL that will be hosted on the Amigopod appliance. For example in step 3 of this document we configured the Login Page of the Captive Portal Profile to be the following URL:

```
https://<Amigopod IP Address or FQDN>/Aruba_login.php
```

As you can see the screenshot has got the Aruba_login name defined – there is no need to include the .php extension as this will be automatically appended.

The IP Address should be set to Aruba Controller IP Address. That is, this address needs to be available from the wireless/wired client via the *captiveportal* policy on the controller.

As you can see there are several Login Form options that allow you to override the default Login Form and Labels used to reference User and Password fields. These typically do not need to be changed.

The *Pre-Auth Check* is only required for Advanced configurations where you might need to ensure the username and password pair is valid before initiating the RADIUS transaction from the Aruba Controller. Given the Web Login and RADIUS database is hosted on the same appliance we can perform a query locally prior to firing a RADIUS transaction.

You can enable the display of an Accept Terms & Conditions option of the login page if required. This refers to the default T&Cs URL defined under Guest Manager → Customization → Customize Guest Manager.

Terms Of Use URL:	<input type="text" value="external/terms.html"/> <small>The URL of a terms and conditions page. If non-blank, this will enable a "terms of use" checkbox on the create account page, which must be checked in order to create a new account. The URL here is specified as the terms of use and is opened in a new window.</small>
-------------------	--

Unfortunately, as of ArubaOS 6.x there is an issue default the Default Destination capability shown in the Web Login configuration. This option is designed to allow you to define an override URL that the wireless/wired user is sent to post authentication. The obvious work around this issue is to set the post authentication URL in the Welcome Page of the ArubaOS Captive Portal Profile.

You can leverage the Amigopod skin technology to quickly brand the Captive Portal displayed to the wireless/wired users. These skins are available as a professional service as a purchasable SKU or there are also Custom and Blank Skins available for those customer's that wish to perform their own HTML/CSS style customization.

The *Title* field allows you to customize the Page Title displayed in the Browser.

Default Destination
Options for controlling the destination clients will redirect to after login.

Default URL:
Enter the default URL to redirect clients.
Please ensure you prepend "http://" for any external domain.

Override Destination: Force default destination for all clients
If selected, the client's default destination will be overridden regardless of its value.

Login Page
Options for controlling the look and feel of the login page.

* Skin: Aruba Networks Skin
Choose the skin to use when this web login page is displayed.

Title:
The title to display on the web login page.

Header HTML:

```
{if $errmsg}
{nwa_icontext type=error}{$errmsg}/{nwa_icontext}
{/if}

<p>
  Please login to the network using your amigopod
  username and password.
</p>
```

Insert content item...
Insert self-registration link...

HTML template code displayed before the login form.

Footer HTML:

```
<p>
Contact a staff member if you are experiencing
difficulty logging in.
</p>
```

Insert content item...
Insert self-registration link...

HTML template code displayed after the login form.

```
<p>
Logging in, please wait...
</p>
```

The *Header, Footer, Login* HTML allow you add and modify the displayed text and/or content displayed on the Web Login page. As you can see there are options to Insert Content and Self-Registration page (respectively found in Administrator → Content Manager & Guest Manager → Customization → Guest Self Registration).

You will notice the code at the top of the Header HTML that parses the redirect URL from the Aruba Controller – if there has been an authentication error the controller returns an error message in the *errmsg* variable.

There is an option to set a *Login Delay* option which will pause the login process at the point where the contents of the above Login Message HTML will be displayed. This is a useful point to grab the contents of a View Source in the client's browser if you need to troubleshoot any Captive Portal issues.

Finally, each Web Login page can be configured with Access Lists to allow or deny specific IP Source Address ranges. There is an option to select the web server behavior when responding to an invalid request.

The screenshot shows a configuration page for Network Login Access. At the top, there is a required field for "Login Delay" set to 0, with a tooltip: "The time in seconds to delay while displaying the login message." Below this is the "Network Login Access" section, which controls access to the login page. It contains two text input fields: "Allowed Access" and "Denied Access", both with tooltips: "Enter the IP addresses and networks from which logins are permitted." and "Enter the IP addresses and networks that are denied login access." respectively. At the bottom of this section is a dropdown menu for "Deny Behavior" set to "Send HTTP 404 Not Found status", with a tooltip: "Select the response of the system to a request that is not permitted." At the very bottom of the form are two buttons: "Save Changes" and "Save and Reload". A legend at the bottom left indicates that an asterisk (*) denotes a required field.

* Login Delay: The time in seconds to delay while displaying the login message.

Network Login Access
Controls access to the login page.

Allowed Access:
Enter the IP addresses and networks from which logins are permitted.

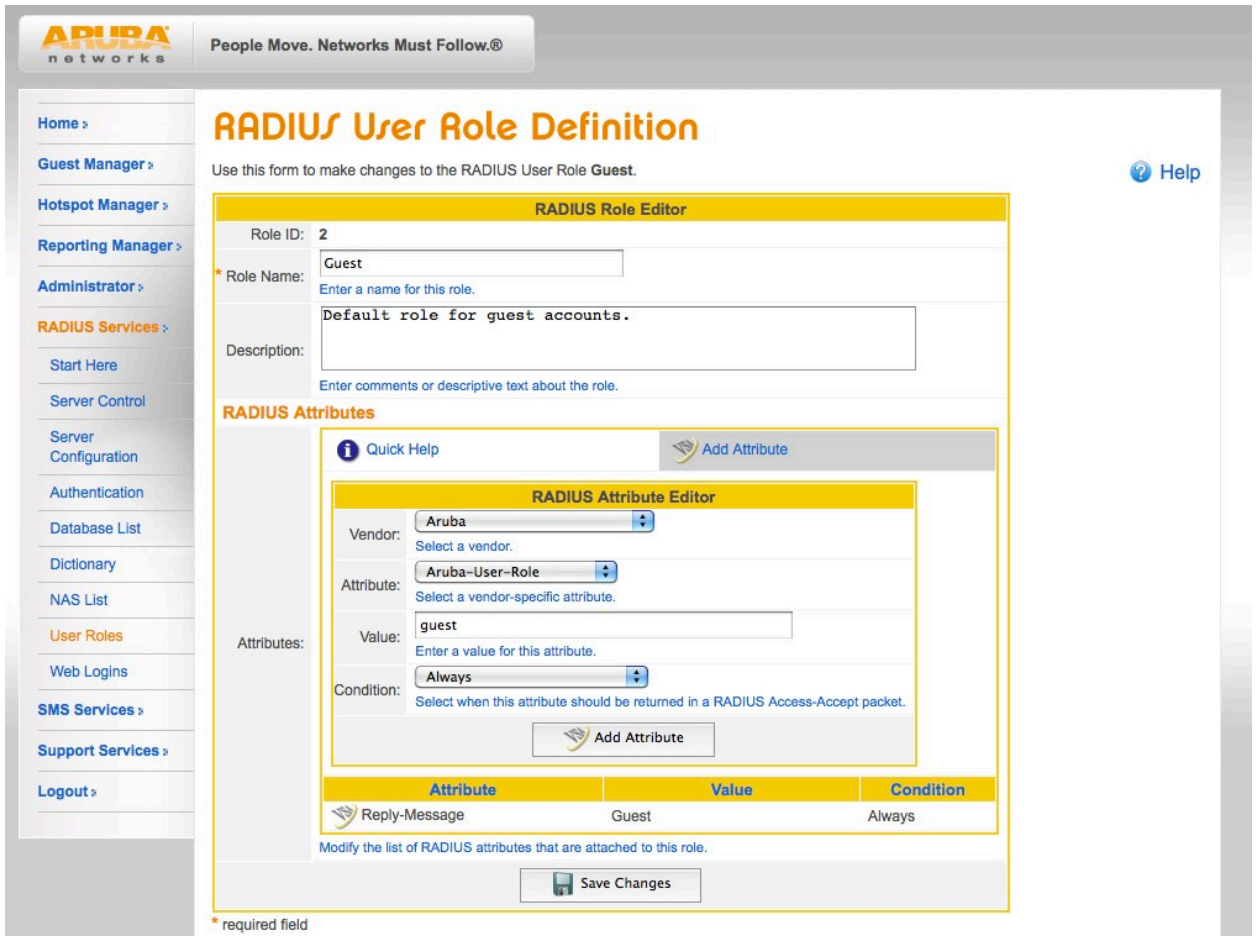
Denied Access:
Enter the IP addresses and networks that are denied login access.

* Deny Behavior: Select the response of the system to a request that is not permitted.

* required field

11. Configure RADIUS User Role

The RADIUS User Role is a collection of 1 or many RADIUS Standard or Vendor Specific Attributes. These attributes can be used to signal role based access control context back to the Aruba Controller as shown in the example screenshot.



This RADIUS Role is presented in the Create User screens of Amigopod’s Guest Manager or can be hard coded as a hidden field in Self Registration pages to ensure each user’s session gets managed appropriately on the Aruba Controller.

12. Test Login and verify successful RADIUS transaction

Now that everything is setup on both the Amigopod and the Aruba Controller, attempt to connect a test wireless/wired client to the network and their session should be successfully redirected to the Amigopod Web Login page.

Use the Amigopod Guest Manager to create a test account and then attempt to login via the redirected Web Login page. If you have been able to successfully authenticate you will see a *Login OK* message in the RADIUS Services → Server Control page where a tail of the RADIUS log is always displayed.

If you are experiencing any issues with the authentication process, the RADIUS debugger can also be enabled from this page for more detailed analysis.

ARUBA networks People Move. Networks Must Follow.®

RADIUS Server Control

Control the local RADIUS server using these command links. [Help](#)

▶ The RADIUS server is currently running.

- Restart RADIUS Server**
Restart the local RADIUS server.
- Stop RADIUS Server**
Stop the local RADIUS server.
- Debug RADIUS Server**
Run the local RADIUS server and see detailed log output.
- View Failed Authentications**
View a list of recent failed authentications.
- Test RADIUS Authentication**
Check a username and password, or verify the RADIUS attributes for a user role.

RADIUS Server Time

The RADIUS server time is currently: **Thu Dec 16 18:13:10 2010 -0800**

RADIUS Log Snapshot

The most recent entries in the RADIUS server log file are shown below.

```
Thu Dec 16 17:13:29 2010 : Auth: Login OK: [steve@arubanetworks.com] (from client apollo port 0 cli 5855CAF59251)
Thu Dec 16 15:30:27 2010 : Auth: Login OK: [steve@arubanetworks.com] (from client apollo port 0 cli DBA25E6E8CF5)
Thu Dec 16 15:30:19 2010 : Auth: Login OK: [mhyson@arubanetworks.com] (from client apollo port 0 cli 00216A7F431E)
Thu Dec 16 15:18:45 2010 : Auth: Login OK: [cjoseph@arubanetworks.com] (from client apollo port 0 cli 5855CAF5302D)
Thu Dec 16 13:57:52 2010 : Info: Ready to process requests.
Thu Dec 16 13:57:52 2010 : Info: rlm_sql (sql): Attempting to connect to amigopod@localhost:5432/amigopod
Thu Dec 16 13:57:52 2010 : Info: rlm_sql (sql): Driver rlm_sql_postgresql (module rlm_sql_postgresql) loaded and linked
Thu Dec 16 13:57:52 2010 : Info: rlm_exec: Wait=yes but no output defined. Did you mean output=none?
```


13. Check RADIUS Accounting is working as expected

If the RADIUS Accounting traffic is not being received by Amigopod, you will not find a corresponding entry in the Guest Manager → Active Sessions screen shown below.

Given the Interim Accounting support in ArubaOS 6.1 this screen will display live traffic statistics based on these updates.

Assuming you have configured RFC 3576 on your Aruba Controller as well, you can click on any given Active Session and select the Disconnect button to terminate their session on the Aruba Controller. This will return the user to the login or initial role that corresponds to the configured AAA Profile.

ARUBA networks People Move. Networks Must Follow.®

Active Sessions

Use this list view to view and manage the active sessions on the server.

Quick Help Manage Multiple Filter More Options

Filter:

Showing: Active sessions only.

	Username	IP Address	Role	NAS	Session Start	Session Time	Session Traffic	Termination Cause
	aruba-guest	10.69.18.146		apollo	2010-12-15 19:22		0.0 MB	

Refresh 1 Showing 1 - 1 of 1 20 rows per page

GuestManager services Back to main

14. Troubleshooting Tips

Test device is not being redirected to the Amigopod Captive Portal:

- Check DNS resolution as client will not be redirected if it can't resolve initially requested webpage.
- Check the captiveportal policy and ensure traffic is permitted to the Amigopod IP Address for the redirect via HTTP or HTTPS.
- Does the amigopod have a route back to the test client's address space – look at use of NAT, default gateway of Amigopod etc.

Login process stalls and never receive RADIUS request from Aruba Controller in logs:

- Check the Web Login page and ensure correct IP address for controller is configured
- Check the captiveportal policy and ensure traffic is permitted to configured IP address of the controller in the step above

Receiving error message in RADIUS Logs about unknown client:

- Check the RADIUS NAS List and make sure there is an entry present that matches the IP address listed in the error message. Aruba Controller maybe using loopback instead of interface address as source for RADIUS traffic.
- Make sure you restarted the RADIUS Server after you added the new RADIUS NAS entry for the Aruba controller.
- Run test RADIUS authentication from the Aruba Controller to ensure basic connectivity using UDP 1812 / 1813.

Receiving error message in RADIUS Logs about login incorrect

- Check the username and password has been entered correctly – reset password if required.
- Check that the shared secrets are the same on both Amigopod and ArubaOS – reset on both ends to be sure.
- Run RADIUS debugger on Amigopod for deeper analysis of the transaction.

Aruba Networks

1344 Crossman Ave.

Sunnyvale, CA 94089-1113

Phone: +1-408-227-4500

Fax: +1-408-227-4550

[Get Directions »](#)

General Inquiries:

info@arubanetworks.com

© 2010 Aruba Networks, Inc. AirWave®, Aruba Networks®, Aruba Mobility Management System®, Bluescanner, For Wireless That Works®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFprotect®, The All Wireless Workplace Is Now Open For Business, Green Island, and The Mobile Edge Company® are trademarks of Aruba Networks, Inc. All rights reserved. Aruba Networks reserves the right to change, modify, transfer, or otherwise revise this publication and the product specifications without notice. While Aruba uses commercially reasonable efforts to ensure the accuracy of the specifications contained in this document, Aruba will assume no responsibility for any errors or omissions. Note: All scaling metrics outlined in this document are maximum supported values. The scale may vary depending upon the deployment scenario and features enabled.