

# Amigopod and ArubaOS Integration

Version 1.0

## Copyright

© 2011 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.

## Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (“GPL”), GNU Lesser General Public License (“LGPL”), or other Open Source Licenses. The Open Source code used can be found at this site:

[http://www.arubanetworks.com/open\\_source](http://www.arubanetworks.com/open_source)

## Legal Notice

ARUBA DISCLAIMS ANY AND ALL OTHER REPRESENTATIONS AND WARRANTIES, WHETHER EXPRESSED, IMPLIED, OR STATUTORY, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NONINFRINGEMENT, ACCURACY AND QUIET ENJOYMENT. IN NO EVENT SHALL THE AGGREGATE LIABILITY OF ARUBA EXCEED THE AMOUNTS ACTUALLY PAID TO ARUBA UNDER ANY APPLICABLE WRITTEN AGREEMENT OR FOR ARUBA PRODUCTS OR SERVICES PURCHASED DIRECTLY FROM ARUBA, WHICHEVER IS LESS.

## Warning and Disclaimer

This guide is designed to provide information about wireless networking, which includes Aruba Network products. Though Aruba uses commercially reasonable efforts to ensure the accuracy of the specifications contained in this document, this guide and the information in it is provided on an “as is” basis. Aruba assumes no liability or responsibility for any errors or omissions.

ARUBA DISCLAIMS ANY AND ALL OTHER REPRESENTATIONS AND WARRANTIES, WHETHER EXPRESSED, IMPLIED, OR STATUTORY, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NONINFRINGEMENT, ACCURACY, AND QUIET ENJOYMENT. IN NO EVENT SHALL THE AGGREGATE LIABILITY OF ARUBA EXCEED THE AMOUNTS ACTUALLY PAID TO ARUBA UNDER ANY APPLICABLE WRITTEN AGREEMENT OR FOR ARUBA PRODUCTS OR SERVICES PURCHASED DIRECTLY FROM ARUBA, WHICHEVER IS LESS.

Aruba Networks reserves the right to change, modify, transfer, or otherwise revise this publication and the product specifications without notice.



[www.arubanetworks.com](http://www.arubanetworks.com)

1344 Crossman Avenue  
Sunnyvale, California 94089

Phone: 408.227.4500  
Fax 408.227.4550

## Table of Contents

<b>Chapter 1:</b>	<b>Introduction</b>	<b>5</b>
	<b>Reference Material</b>	<b>5</b>
<b>Chapter 2:</b>	<b>Captive Portal Authentication</b>	<b>6</b>
	<b>Captive Portal Overview</b>	<b>6</b>
	<b>ArubaOS or Amigopod for Visitor Management</b>	<b>7</b>
	<b>Captive Portal Authentication Workflow</b>	<b>10</b>
<b>Chapter 3:</b>	<b>ArubaOS Configuration</b>	<b>12</b>
	<b>Creating a RADIUS Server Instance</b>	<b>12</b>
	Modify NAS ID for Master Local Deployments	14
	Add RADIUS Server to a Server Group	15
	Creating an RFC3576 Server Instance	16
	<b>Creating a Captive Portal Profile</b>	<b>18</b>
	Configure Authentication for Captive Portal Profile	20
	Modify the AAA Profile	21
	Define a Policy to Permit Traffic to Amigopod	23
	Enable Captive Portal on Initial Role of Captive Portal Profile	25
	Verify Virtual AP Configuration	26
<b>Chapter 4:</b>	<b>Amigopod Configuration</b>	<b>27</b>
	<b>Check for Updated Amigopod Plugins</b>	<b>27</b>
	<b>Configure RADIUS NAS for an Aruba Controller</b>	<b>30</b>
	<b>Configure Web Login for Captive Portal Authentication</b>	<b>33</b>
	Optional Customization of the Web Login Page	34
	Amigopod Skins and Content Customization	35
	Web Login Access Lists	36
	<b>Configure the RADIUS User Role</b>	<b>37</b>
	<b>(Optional) Import Sample Welcome Page</b>	<b>38</b>
<b>Chapter 5:</b>	<b>Integration Verification</b>	<b>42</b>
	<b>Create a Test Account Within Amigopod Guest Manager</b>	<b>42</b>
	<b>Testing RADIUS</b>	<b>44</b>
	Test Basic RADIUS Transactions	44
	Test Login and Verify Successful RADIUS Transaction	46
	Check that RADIUS Accounting is Working as Expected	48

<b>Chapter 6: Troubleshooting Tips</b>	<b>49</b>
<b>Appendix A: Contacting Aruba Networks</b>	<b>50</b>
<b>Contacting Aruba Networks</b>	<b>50</b>

# Chapter 1: Introduction

Aruba supports advanced visitor management services through the combination of Aruba Mobility Controllers and APs running the ArubaOS software, and Aruba Amigopod guest management software. This guide describes the configuration process that must be performed on the Aruba Mobility Controllers and the Aruba Amigopod to create a fully integrated visitor management solution. The solution leverages the captive portal functionality and RADIUS authentication, authorization, and accounting (AAA) functions that are built into ArubaOS.

This guide is based on the Aruba controller running the base OS image and the additional Policy Enforcement Firewall (PEF) license enabled. The PEF license is needed to make the necessary changes to the default captive portal role to allow unauthenticated traffic to flow through to the Amigopod Web Login page.

The PEF license provides identity-based security to wired and wireless clients through user roles and firewall rules. You must purchase and install the PEF license on the mobility controller to use identity-based security features. Depending on whether the license is installed, the captive portal functions work differently and you configure captive portal differently.

The detailed configuration steps of the PEF features that relate to the operation of a working captive portal are outside the scope of this integration document. Detailed discussion on how to leverage the integrated firewall capabilities of the Aruba controller that are enabled by the PEF license are covered in the referenced VRD resources.

Table 1 lists the current software versions for this guide.

**Table 1 Aruba Software Versions**

Product	Version
ArubaOS™ (mobility controllers)	6.1
AmigopodOS	3.3

## Reference Material

- This guide assumes a working knowledge of Aruba products. This guide is based on the network detailed in the *Aruba Campus Wireless Networks VRD* and the *Base Designs Lab Setup for Validated Reference Design*. These guides are available for free at <http://www.arubanetworks.com/vrd>.
- The complete suite of Aruba technical documentation is available for download from the Aruba support site. These documents present complete, detailed feature and functionality explanations outside the scope of the VRD series. The Aruba support site is located at: <https://support.arubanetworks.com/>. This site requires a user login and is for current Aruba customers with support contracts.

## Chapter 2: Captive Portal Authentication

Captive portals are the simplest form of authentication for users. This section introduces the concepts behind the authentication and compares and contrasts Amigopod with the ArubaOS portal.

### Captive Portal Overview

Captive portal allows a wireless client to authenticate using a web-based portal page. Captive portals are typically used in wireless hotspots or for hotel in-room Internet access. After a user associates to the wireless network, their device is assigned an IP address. The user must start a web browser and pass an authentication check before access to the network is granted. An example page is shown in Figure 1.

The screenshot shows a web-based login interface for Amigopod. At the top left is the Aruba Networks logo, and to its right is the 'Amigopod' text. Below this is a large 'Login' heading. A message reads: 'Please login to the network using your amigopod username and password.' Below the message is a login form with the following fields: 'Username:' (required), 'Password:' (required), and 'Terms:' (checkbox for 'I accept the terms of use'). A 'Log In' button is located below the form. A legend below the form states '\* required field'. At the bottom of the page, there is a link: 'Contact a staff member if you are experiencing difficulty logging in.'

**Figure 1** Amigopod captive portal page

Captive portal authentication is the simplest form of authentication to use and it requires no software installation or configuration on the client. The guest SSID is typically open and does not use any form of encryption. The portal usually asks for some limited information such as a username and password and the exchange is encrypted using standard SSL encryption.








































However, portal authentication does not provide any form of encryption beyond the authentication process. To ensure privacy of client data, some form of link-layer encryption (such as WPA-PSK or WPA2-PSK) or higher-level VPN (such as IPsec or SSL) should be used when sensitive data will be sent over the wireless network.

## ArubaOS or Amigopod for Visitor Management

ArubaOS supports two methods of guest access: using just the mobility controller or using the mobility controller plus Amigopod. ArubaOS supports basic guest management and captive portal functionality, with guest access limited to a single master-local cluster. Aruba Amigopod extends the standard ArubaOS captive portal functionality by providing many advanced features, including:

- A fully branded user interface
- SMS integration for delivery of receipts
- Bulk upload of visitors for conference management
- Self-provisioning of users for public space environments

**Table 2 Comparison of ArubaOS Captive Portal and Amigopod**







Feature	ArubaOS	ArubaOS Plus Amigopod
Not supported =  Limited support =  Supported = 		
<b>Captive Portal Customization</b>		
Captive portal customization		
Captive portal per-SSID customization		
Anonymous logon		
One time tokens/access codes		
Welcome page with session statistics and logout		
Mobile browser aware captive portal pages		
Skins: UI branding customization		
<b>Guest Account Provisioning</b>		
Single point of management for guest account and captive portal in multiple master controller deployments		
Non-IT staff do not require IP access to master controller for provisioning guest accounts		
Guest-provisioning operator role		
Customizable guest-provisioning operator role		
External servers for operator logins		
Provisioning of nonguest user roles by operators		
Limit operators to view only the account they created		
Self-registration workflow with automated login		
Sponsor-approved self-registration		
Time zone support for guest access in distributed deployments		
Bulk provisioning of guest accounts (CSV import and automatic generation)		

**Table 2 Comparison of ArubaOS Captive Portal and Amigopod (Continued)**

Feature	ArubaOS	ArubaOS Plus Amigopod
Export/import of user database	✓	✓
Mandatory and nonmandatory fields	✗	✓
Guest password complexity requirements	✗	✓
Guest account information printing via templates	!	✓
Guest credential delivery through email and SMS	!	✓
Force password change on first login	✗	✓
Delete and/or disable guest accounts on expiration	!	✓
<b>Guest Session Management</b>		
Time and day policy	✓	✓
Guest access expiry timer starts on first login	✗	✓
Limit access based on total session time across multiple logins	✗	✓
Limit guest session data (total bytes)	✗	✓
Limit guest session bandwidth (Mb/s)	✓	✓
Limit guest session to single concurrent login	✓	✓
<b>Hotspot and Hospitality Features</b>		
Walled garden	✓	✓
Plug-and-play clients, any IP	✓	✓
VPN NAT (static NAT per client using public IP)	✓	✓
Credit card billing	✗	✓
Surveys and feedback forms	✗	✓
Target ads and promotions	✗	✓
Visitor data mining	✗	✓
MAC or cookie-based reauthentication (portal bypass)	✗	✓
<b>Reporting and Notification</b>		
Peak guest network usage	✗	✓
Total guest sessions (per day, per week, etc.)	✗	✓
Bandwidth usage on guest network	✗	✓
Top x users (session time and bandwidth)	✗	✓
Expiring passwords	✗	✓



**Table 2 Comparison of ArubaOS Captive Portal and Amigopod (Continued)**

Feature	ArubaOS	ArubaOS Plus Amigopod
<b>Enterprise Features and Scalability</b>		
Managing 1000s of accounts		
High availability/redundancy		
Expandability (plug-in architecture)		

Although ArubaOS supports internal and external captive portal functionality, this guide focuses on external captive portal functionality. The internal captive portal dictates the use of the internal login page on the controller itself. The login page is very basic and does not allow for the extensive customization that is possible with the Amigopod Web Logins feature.

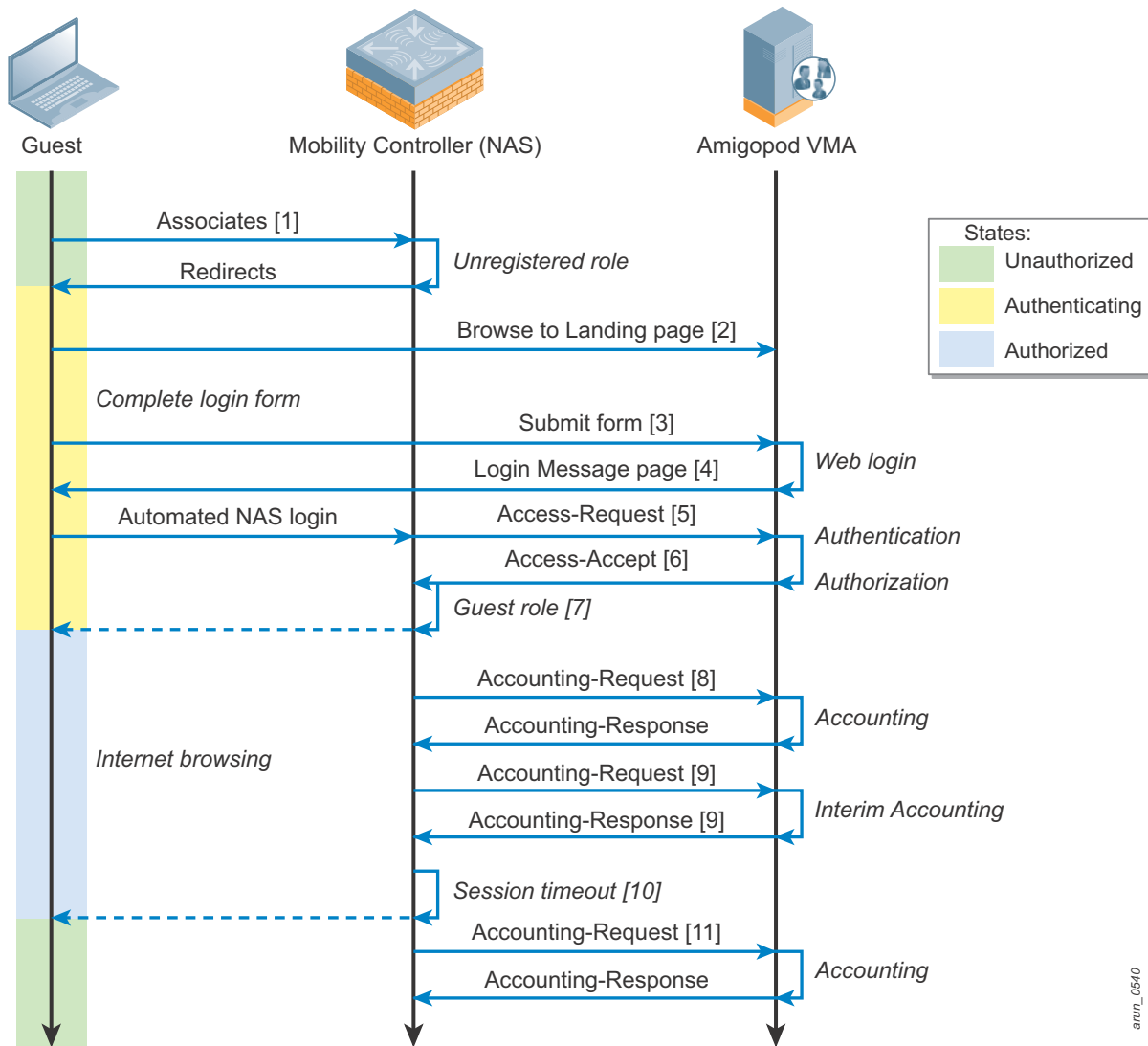


Amigopod provides the Skin plugin technology where the presentation of the UI is separated from the mechanics of the underlying application. This separation allows Aruba to supply end users with a branded skin for all Amigopod interaction (both visitor and administrators) for a nominal fee at the time of purchase. Users can also customize the skin themselves with the requisite skills. ArubaOS now allows for fully customized captive portal pages to be uploaded to the controller. However, this process requires a significant amount of web design and JavaScript experience to produce a professional result.

The integration of Amigopod with the mobility controller also leverages the ability of ArubaOS to define and reference external RADIUS servers for the authentication and accounting of visitor accounts. In the standalone Aruba guest-provisioning solution, the local database in each controller stores user credentials, which limits the solution to the scope of the local deployment. With the introduction of Amigopod, all visitor accounts are created, authenticated, and accounted for on the Amigopod internal RADIUS server.

## Captive Portal Authentication Workflow

Figure 2 shows the phases that a guest user passes through during a captive portal authentication process. In the Aruba system, the mobility controller acts as the network access server (NAS) and Amigopod acts as the RADIUS server. Figure 2 details the captive portal authentication workflow.



**Figure 2 Workflow for captive portal authentication**

1. The guest user associates their Wi-Fi device to the guest SSID. In the baseline VRD configuration, this SSID is “Guest-Network.”
2. The guest user opens a browser. Based on the configured home page or requested web page, the initial HTTP traffic is intercepted by the Aruba controller and redirected to the Amigopod web login page defined in the captive portal profile.
3. The guest user enters their user credentials on the Amigopod web login page. Amigopod performs any preauthorization checks that are required and displays the login message to the guest user.

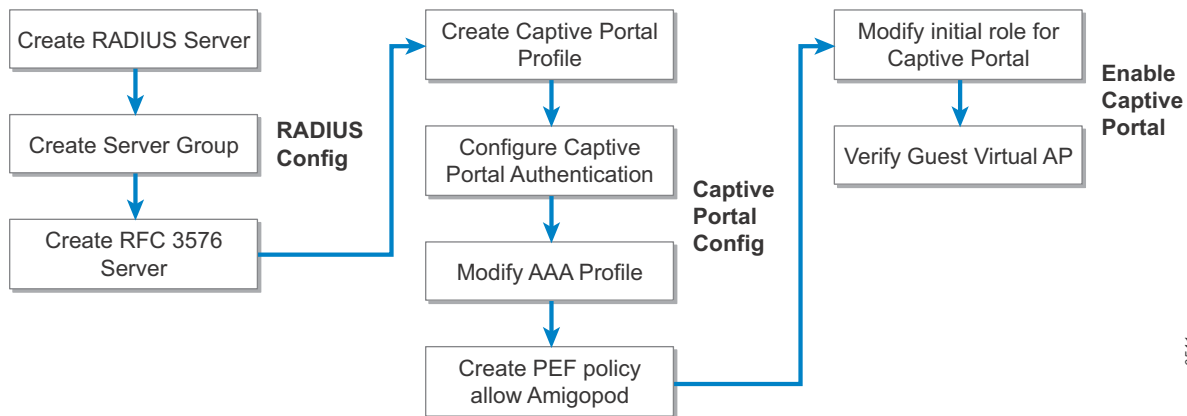
4. The login message instructs the guest user's browser to submit the user credentials directly to the Aruba controller as a HTTPS POST for authentication processing.
5. When the Aruba controller receives the user credentials, it creates a corresponding RADIUS session and sends an Access-Request message to the defined Amigopod RADIUS server.
6. The Amigopod processes the Access-Request message by referring to its local database and optionally any configured proxy authentication servers defined. Any defined authorization rules are processed at this point.
7. Based on the results of the authentication and authorization processing, the Amigopod responds with either an Access-Accept or Access-Reject message. If the authentication is successful, the Access-Accept message contains one or more RADIUS attributes to define the context of the guest user session. These attributes can include but are not limited to the session duration of the guest login and the Aruba controller user role that defines the PEF policies and bandwidth contracts that could be applied to the session. When the Aruba controller receives the Access-Accept message, it changes the role of the guest user session and their device is permitted access to the network.
8. If RADIUS accounting has been configured correctly on the Aruba controller, an Accounting-Start packet is sent to the Amigopod, which defines the beginning of the session statistics for the guest user.
9. Based on the default interval of [600 seconds] the Aruba controller will provide updates to these session statistics by sending Interim Accounting update messages to the Amigopod.
10. Based on the Session-Timeout received in the original Access-Accept packet from Amigopod, the Aruba controller counts down the remaining time that is valid for the current guest user session. When the time has expired, the controller terminates the session.
11. When the session ends (Session-Timeout, Idle-Timeout, User Logout, Admin Disconnect), the controller sends a RADIUS Accounting-Stop message to close the session within the Amigopod accounting database. This stop message includes the final update of the session statistics.

## Chapter 3: ArubaOS Configuration

Three phases make up the configuration of the ArubaOS controller to support external captive portal based authentication leveraging the RADIUS protocol:

1. Base RADIUS configuration
2. Captive portal configuration
3. Enabling captive portal on existing guest WLAN

Figure 3 summarizes the steps covered in this chapter to successfully complete the ArubaOS configuration that is needed to integrate with the Amigopod external captive portal and RADIUS server.



**Figure 3** Workflow for ArubaOS configuration

### Creating a RADIUS Server Instance

For the Aruba controller to successfully authenticate the guest users that will be provisioned on the Amigopod system, a RADIUS definition must be defined on the controller.

The RADIUS server definition requires that the following fields be configured:

- Host should be configured to the Amigopod IP address.
- Key is the shared secret that is needed to secure RADIUS communications.
- Amigopod uses the default ports of 1812 for authentication and 1813 for accounting.
- The default Retransmit and Timeout value are adequate for most installs

The following configuration must be performed on the master controller. This RADIUS definition is then replicated to all local controllers. In a standalone controller deployment, this RADIUS server instance must be created on each controller individually.



Do not set the NAS ID or NAS IP now. You will configure the NAS ID and NAS IP on each controller in the next step.

## Adding a RADIUS Server

```
aaa authentication-server radius "Amigopod"
host 10.169.130.50
key *****
```

### Security > Authentication > Servers

Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

Server Group

- [-] RADIUS Server
  - Amigopod
  - NPS1
- [-] LDAP Server
- [-] Internal DB
- [-] Tacacs Accounting Server
- [-] TACACS Server
- [-] XML API Server
- [-] RFC 3576 Server
- [-] Windows Server

**RADIUS Server > Amigopod** Show Reference Save As Reset

Host	<input type="text" value="10.169.130.50"/>	Key	<input type="password" value="*****"/> Retype: <input type="password" value="*****"/>
Auth Port	<input type="text" value="1812"/>	Acct Port	<input type="text" value="1813"/>
Retransmits	<input type="text" value="3"/>	Timeout	<input type="text" value="5"/> sec
NAS ID	<input type="text"/>	NAS IP	<input type="text"/>
Source Interface	<input type="text"/>	Use MD5	<input type="checkbox"/>
Mode	<input checked="" type="checkbox"/>		

**Figure 4 Adding a RADIUS server**

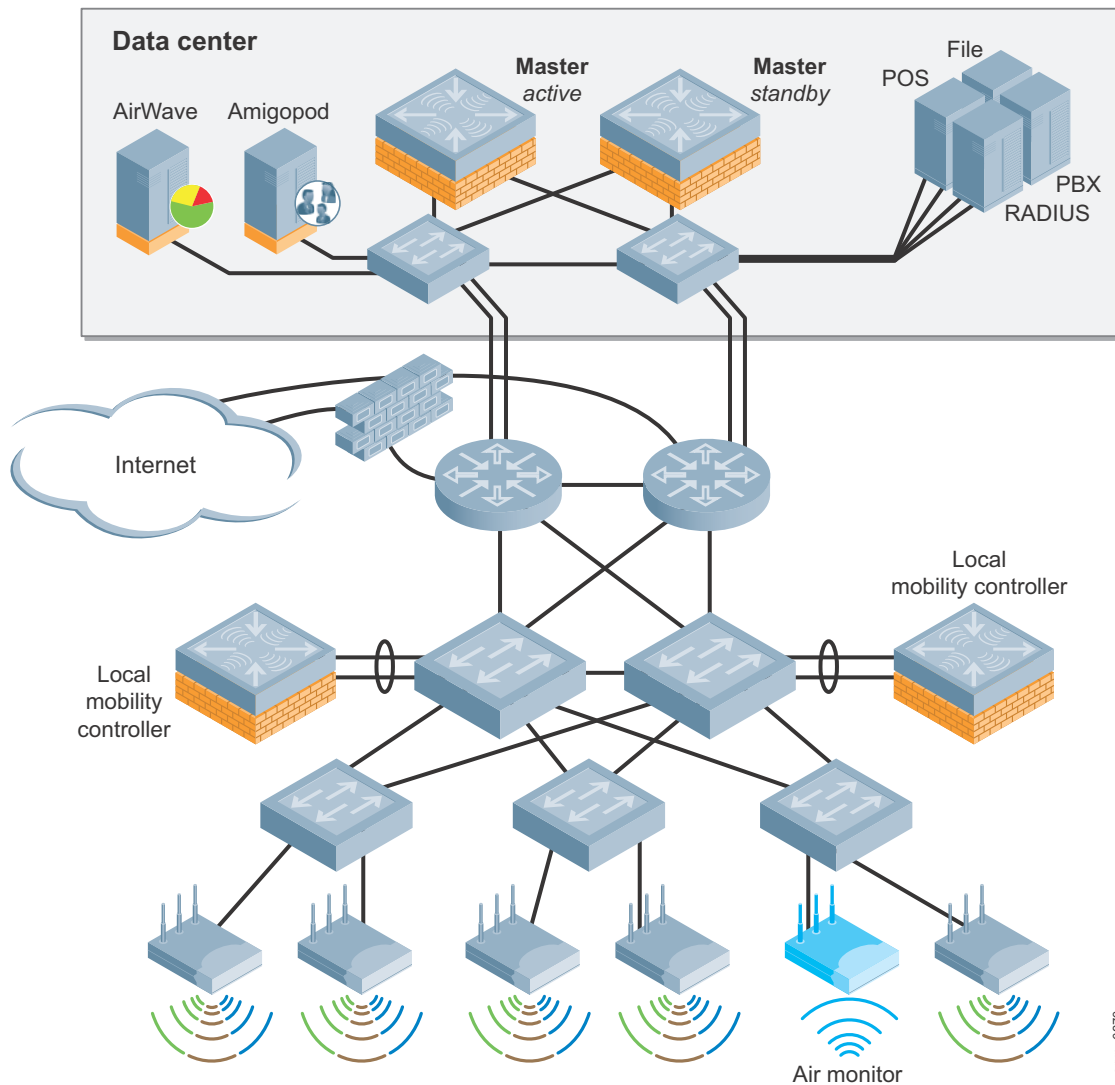


Ensure that the key is recorded, because you will need this shared secret for a later step in the Amigopod configuration. For security purposes, each NAS should have its own key.

## Modify NAS ID for Master Local Deployments

In an Aruba master local deployment, you must modify the NAS ID of the local controllers to ensure that the correct identifier is recorded in the RADIUS accounting traffic sourced from each local controller that is responsible terminating the APs.

In the VRD campus topology, the local controllers are deployed on the 10.169.145.0/24 network (VLAN 145). This network is used to send the RADIUS transactions toward the Amigopod deployed on 10.169.130.50.



Based on the VLAN numbering in the VRD Local Controller deployment, the following modifications are recommended:

- Set the local controller NAS IP to the IP address on VLAN 145.
- Define the source interface for RADIUS traffic to use VLAN 145 also.

These configuration changes must be performed on each local controller using the local interface of the controller.

## Modify RADIUS Client Settings

```
ip radius nas-ip 10.169.145.4
ip radius source-interface vlan 145
```

The screenshot displays the configuration page for RADIUS Client settings. The breadcrumb path is Security > Authentication > Advanced. The page has several tabs: Servers, AAA Profiles, L2 Authentication, L3 Authentication, User Rules, and Advanced. The configuration is organized into three main sections:

- Authentication Timers:** Includes fields for User Idle Timeout (300 sec), Authentication Server Dead Time (10 min), Logon User Lifetime (5 min), and User Interim stats frequency (300 sec).
- RADIUS Client:** Includes fields for NAS IP Address (10.169.145.4) and Source Interface (145). There is a dropdown menu for the source interface currently set to None.
- DNS Query Interval:** Includes a field for DNS Query Interval (15 min).

At the bottom right of the configuration area is an **Apply** button. Below the configuration area is a **Commands** section with a **View Commands** link.

**Figure 5** Modify RADIUS client setting

## Add RADIUS Server to a Server Group

A server group must be created to define which authentication server will be referenced during the authentication of visitor accounts. This server group is then referenced in the subsequent captive profile configuration.

Make these configurations in the newly created server group definition:

- Select the previously created Amigopod RADIUS server entry.
- The remaining settings for server rules can be left as their defaults.

## Adding a AAA Server Group

```
aaa server-group "Guest-Amigopod"
auth-server "Amigopod" position 1
```

The screenshot displays the configuration page for a AAA server group named 'Guest-Amigopod'. On the left, a tree view shows various server types, with 'Guest-Amigopod' under the 'RADIUS Server' category selected. The main area shows the configuration for this group, including a 'Fail Through' checkbox and a table of servers. The 'Servers' table has columns for Name, Server-Type, trim-FQDN, Match-Rule, and Actions. The 'Amigopod (Radius)' server is highlighted. Below the table, there are fields for Match Type (set to 'Authstring'), Operator (set to 'contains'), and Match String. There are also 'Add Rule' and 'Delete Rule' buttons. At the bottom, there is a 'Server Rules' table with columns for Priority, Attribute, Operation, Operand, Type, Action, Value, Validated, and Actions, and a 'New' button.

**Figure 6 Adding a AAA server group**

## Creating an RFC3576 Server Instance

RFC3576 is an extension to the RADIUS standard that allows for a RADIUS server initiated control of an established RADIUS AAA session. The two primary functions of the RFC are represented by the following two messages:

- Disconnect messages: The RADIUS server sends a Disconnect-Request packet to terminate a user session on a NAS and removes all associated session context. The Disconnect-Request packet is sent to UDP port 3799 and it identifies the user session to be terminated by inclusion of the session identification attributes.
- Change of Authorization (CoA) messages: CoA-request packets contain information for dynamically changing session authorizations. Typically these messages are used to change the context of the user session. For ArubaOS, this means changing the user role that the current session is assigned. This feature enables many different business rules, such as bandwidth throttling after a quota is exceeded.

## Configuring an RFC3576 Server

As part of the guest access solution addressed by this guide, Amigopod serves as the RFC3576 server and can perform the disconnect and CoA functions.

Make these configurations in the RFC3576 server definition:

- The name of the RFC3576 server definition must be the IP address of the Amigopod.
- The Key must match the shared secret configuration that was defined for the RADIUS server.



## RFC3576 Server Configuration

```
aaa rfc-3576-server "10.169.130.50"  
key wireless
```

### Security > Authentication > Servers

The screenshot shows the configuration page for an RFC 3576 server. On the left is a tree view of server types, including Server Group, RADIUS Server, LDAP Server, Internal DB, Tacacs Accounting Server, TACACS Server, XML API Server, RFC 3576 Server (selected), and Windows Server. The RFC 3576 Server is expanded to show the IP address 10.169.130.50. The main panel is titled 'RFC 3576 Server > 10.169.130.50' and contains a 'Key' field with two masked input boxes for the key and its retype, along with 'Show Reference', 'Save As', and 'Reset' buttons.

**Figure 7** RFC3576 server configuration

## Creating a 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. With the captive portal profile, you can configure the login and optional welcome pages to be hosted by Amigopod.

The captive portal authentication profile also defines several critical components of the working solution such as the security role that will be used to control visitors that successfully authenticate with Amigopod. Another component that is defined is that the Amigopod RADIUS server should be referenced for this authentication traffic via the definition of the previous server group. The captive portal profile definition is described in [Table 3](#).

**Table 3 Captive Portal Profile Fields**

Page	Required?	Description
Login Page	Yes	Location of the login page on the server
Default Role	Yes	Post authentication role
Welcome Page	Optional	Post authentication page
Logout Popup	No	Small window to allow the user to log out
Redirect Pause	No	How long the user waits at the welcome page before continuing on to their original destination
SwitchIP	Optional	The local IP of the controller in a multiswitch environment

In this example, the login and welcome page URLs are configured. In a later step, these URLs will be defined on the Amigopod as part of the web login configuration. The redirect pause will be shortened to 3 seconds, and no logout window is needed. The default role will be set to `auth-guest`.




---

Based on the local deployment security policy, you must change the default role of the captive portal profile to a role that includes appropriate firewall policies.

---

## Captive Portal Profile Configuration

```

aaa authentication captive-portal "guestnet"
  default-role auth-guest
  redirect-pause 3
  no logout-popup-window
  login-page https://10.169.130.50/Aruba_Login.php
  welcome-page https://10.169.130.50/Aruba_welcome.php
  switchip-in-redirection-url

```

### Security > Authentication > L3 Authentication

Servers | AAA Profiles | L2 Authentication | **L3 Authentication** | User Rules | Advanced

Captive Portal Authentication Profile

- default
- guestnet**

Server Group: Guest-Amigopod

WISPr Authentication Profile

VPN Authentication Profile

Stateful NTLM Authentication Profile

VIA Authentication Profile

VIA Connection Profile

VIA Web Authentication

**Captive Portal Authentication Profile > guestnet** Show Reference Save As Reset

Default Role	auth-guest	Default Guest Role	guest
Redirect Pause	3 sec	User Login	<input checked="" type="checkbox"/>
Guest Login	<input type="checkbox"/>	Logout popup window	<input type="checkbox"/>
Use HTTP for authentication	<input type="checkbox"/>	Logon wait minimum wait	5 sec
Logon wait maximum wait	10 sec	logon wait CPU utilization threshold	60 %
Max Authentication failures	0	Show FQDN	<input type="checkbox"/>
Use CHAP (non-standard)	<input type="checkbox"/>	Login page	.130.50/Aruba_Login.php
Welcome page	.130.50/Aruba_welcome.g	Show Welcome Page	<input checked="" type="checkbox"/>
Add switch IP address in the redirection URL	<input checked="" type="checkbox"/>	Allow only one active user session	<input type="checkbox"/>
White List	<input type="text"/> <span>Delete</span> <span>Add</span>	Black List	<input type="text"/> <span>Delete</span> <span>Add</span>
Show the acceptable use policy page	<input type="checkbox"/>		

Apply

**Figure 8** Captive portal profile configuration



**NOTE**

The example captive portal profile shows the use of HTTPS as the protocol for the redirect URLs for the login and welcome pages. Based on this configuration, the best practice is to install a trusted server certificate on the Amigopod and the controller's web server components of the controller. These trusted server certificates can be obtained from an internal Certificate Authority, if present at the customer site, or various public commercial Certificate Authorities available online. If no trusted server certificate is installed on the Amigopod and the Aruba controller, the user experience will include some browser warning messages regarding the untrusted state of the default certificates. Examples of commercial Certificate Authorities are Verisign, Thawte, Entrust, GeoTrust, GoDaddy.

## Configure Authentication for Captive Portal Profile

Now that the new captive portal profile has been created, you must select the server group for the Amigopod RADIUS definition as the authentication source.

### Configure the Authentication Source

```
aaa authentication captive-portal "guestnet"
server-group "Guest-Amigopod"
```

#### Security > Authentication > L3 Authentication

Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

[-] Captive Portal Authentication Profile

- [+] default
- [-] guestnet

Server Group    Guest-Amigopod

- [+] WISPr Authentication Profile
- [+] VPN Authentication Profile
- [+] Stateful NTLM Authentication Profile
- [+] VIA Authentication Profile
- [+] VIA Connection Profile
- [+] VIA Web Authentication

Server Group > Guest-Amigopod Show Reference Save As Reset

Fail Through

Servers									
Name	Server-Type	trim-FQDN	Match-Rule	Actions					
Amigopod	Radius	No		Edit Delete ▲ ▼					
<span>New</span>									
Server Rules									
Priority	Attribute	Operation	Operand	Type	Action	Value	Validated	Actions	
<span>New</span>									

Apply

**Figure 9**    *Configure the authentication source*

## Modify the AAA Profile

The AAA profiles define how users are authenticated. The AAA profile determines the user role for unauthenticated clients (initial role) and the user role to be applied after successful authentication (default role) based on the authentication type. The AAA profile also defines the server group that is used for RADIUS accounting and an RFC3576 server if present.

Begin with the existing AAA profile defined as part of the baseline for guest access in the campus VRD resource. Then modify the guestnet AAA profile as follows:

- The initial role remains as the guest-logon role, but it is modified in the next step to enable the new captive portal profile.
- (Optionally) Enable RADIUS interim accounting to receive incremental updates on guest access usage.
- Enable the RADIUS accounting server group to point to the Amigopod.
- Enable the RFC3576 server to point to the Amigopod.

## Modify AAA Profile RADIUS Settings

```
aaa profile "guestnet"
  initial-role guest-logon
  radius-interim-accounting
  radius-accounting "Guest-Amigopod"
```

Security > Authentication > Profiles

Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

AAA Profile > guestnet Show Reference Save As Reset

Initial role	guest-logon	MAC Authentication Default Role	guest
802.1X Authentication Default Role	guest	L2 Authentication Fail Through	<input type="checkbox"/>
RADIUS Interim Accounting	<input checked="" type="checkbox"/>	User derivation rules	--NONE--
Wired to Wireless Roaming	<input checked="" type="checkbox"/>	SIP authentication role	--NONE--
Device Type Classification	<input checked="" type="checkbox"/>	Enforce DHCP	<input type="checkbox"/>

Apply

**Figure 10** Modify AAA profile RADIUS settings

Next enable RFC3576 support for the server group.

### Enable 3576 Support

```
aaa profile "guestnet"  
    rfc-3576-server "10.169.130.50"
```

Navigation tabs: **AAA Profiles** | L2 Authentication | L3 Authentication | User Rules | Advanced

- default
- default-dot1x
- default-dot1x-psk
- default-mac-auth
- default-open
- default-xml-api
- [-] guestnet
  - MAC Authentication Profile
  - MAC Authentication Server Group
  - 802.1X Authentication Profile
  - 802.1X Authentication Server Group
  - RADIUS Accounting Server Group
- [+] XML API server
- [-] RFC 3576 server

#### RFC 3576 servers

Name	Actions
10.169.130.50	Delete

Add a profile

**Figure 11** Enabling RFC3576 support

## Define a Policy to Permit Traffic to Amigopod

A new firewall policy must be created and assigned to the initial role allocated to unauthenticated guest users to allow the successful redirect to the captive portal page defined on Amigopod.

These policies can be simplified by using the existing network destination alias as defined in the campus VRD baseline configuration.

### Amigopod Netdestination Alias

```
netdestination Amigopod
  host 10.169.130.50
```

#### Advanced Services > Stateful Firewall > Destinations > Edit Destination (Amigopod)

The screenshot shows the configuration page for the destination 'Amigopod'. The breadcrumb trail is 'Advanced Services > Stateful Firewall > Destinations > Edit Destination (Amigopod)'. The page has several tabs: 'Global Setting', 'White List BW Contracts', 'Network Services', 'Destination', 'BW Contracts', and 'BW Contracts E'. The 'Destination' tab is active. The configuration fields are as follows:

- IP Version: IPv4 (dropdown)
- Destination Name: Amigopod
- Invert:

Type	IP Address	NetMask/Range	Actions
host	10.169.130.50	32	Delete ▲ ▼

There is an 'Add' button at the bottom left of the table.

**Figure 12** Amigopod netdestination alias

Based on the nature of the captive portal traffic, HTTP and HTTPS traffic are permitted through this policy to the Amigopod IP address.

Depending on the routing topology in place at each customer environment, Network Address Translation (NAT) may be used to hide the source address space allocated to guest users. NAT can be implemented in the following two methods within the ArubaOS controller:

- Source NAT all traffic from the guest VLAN on the controller.
- Source NAT traffic per application through the use of policies in the PEF configuration on the controller.

Based on these topology and routing decisions, the configuration of the policies to permit the initial redirect traffic to Amigopod will change slightly.

### Source NAT on VLAN

If you are performing a source NAT on the VLAN, use this configuration.

## Example of Source NAT on VLAN

```
ip access-list session "amigopod"
  alias "user" alias "Amigopod" "svc-http" permit queue low
  alias "user" alias "Amigopod" "svc-https" permit queue low
```

### Security > Firewall Policies > Add New Policy

User Roles	System Roles	Policies	Time Ranges	Guest Access						
Policy Name: <input type="text" value="amigopod"/>										
Policy Type: <input type="text" value="Session"/>										
<b>Rules</b>										
IP Version	Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	Pause ARM Scanning	BlackList
IPv4	user	Amigopod	svc-http	permit			low		No	No
IPv4	user	Amigopod	svc-https	permit			low		No	No
<input type="button" value="Add"/>										
<b>Commands</b>										

**Figure 13** Amigopod access – source NAT on VLAN example

## Source NAT per Application

If you are using application-based source NAT, use this configuration.

## Example of Source NAT per Application Policy

```
ip access-list session "amigopod"
  alias "user" alias "Amigopod" "svc-http" src-nat queue low
  alias "user" alias "Amigopod" "svc-https" src-nat queue low
```

### Security > Firewall Policies > Add New Policy

User Roles	System Roles	Policies	Time Ranges	Guest Access						
Policy Name: <input type="text" value="amigopod"/>										
Policy Type: <input type="text" value="Session"/>										
<b>Rules</b>										
IP Version	Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	Pause ARM Scanning	BlackList
IPv4	user	Amigopod	svc-http	src-nat			low		No	No
IPv4	user	Amigopod	svc-https	src-nat			low		No	No
<input type="button" value="Add"/>										
<b>Commands</b>										

**Figure 14** Example of source NAT per application policy



## Enable Captive Portal on Initial Role of Captive Portal Profile

In the previous step, the initial role for this captive portal authentication configuration is configured as guest-logon. This role must be modified to enable the newly created Amigopod captive portal profile. If you forget this step, the captive portal is not triggered when a new guest connects to the guest Wi-Fi SSID. Also, the amigopod policy must be added to the initial role to ensure that traffic from the unauthenticated guest users can be redirected successfully to the Amigopod web login page.

If these policies are not in place, the controller attempts to redirect the browser session to the Amigopod web login URL defined in your captive portal profile. This attempt fails because the default captiveportal policy is matched for http traffic. The session will consequently be redirected a second, third, and fourth time, in an endless loop. The result is a “too many redirects” error message or a browser that keeps flicking between the controller and Amigopod web login URL.



The amigopod policy must be placed in position 1 of the access list to ensure that it is processed first.

## Captive Portal Logon Role Configuration

```
user-role "guest-logon"
  access-list session "amigopod" position 1
  access-list session "captiveportal" position 2
  access-list session "guest-logon-access" position 3
  access-list session "block-internal-access" position 4
  access-list session "v6-logon-control" position 5
  access-list session "captiveportal6" position 6
  captive-portal "guestnet"
```

Security > User Roles > Edit Role(guest-logon)

User Roles System Roles Policies Time Ranges Guest Access

Back

**Firewall Policies**

Name	Rule Count	Location	Action
amigopod	2		Edit Delete ▲ ▼
captiveportal	3		Edit Delete ▲ ▼
guest-logon-access	3		Edit Delete ▲ ▼

Add

**Re-authentication Interval**

Disabled  Change (0 disables re-authentication. A positive value enables authentication 0 - 4096 )

**Role VLAN ID**

Not Assigned  Not Assigned Change

**Bandwidth Contract**

Upstream: Not Enforced  Change Per Role

Downstream: Not Enforced  Change Per Role

**VPN Dialer**

Not Assigned  Not Assigned Change

**PPTP Pool**

default-pptp-pool  Not Assigned Change

**Captive Portal Profile**

guestnet  guestnet Change

**Figure 15** Captive portal logon role configuration

## Verify Virtual AP Configuration

Based on the baseline configuration detailed in the campus VRD resource, the guest virtual AP should have the appropriate SSID and AAA profile applied.

### Virtual AP Configuration

```
wlan virtual-ap "guestnet"
  ssid-profile "guestnet"
  aaa-profile "guestnet"
```

Advanced Services > All Profile Management

The screenshot displays the configuration page for a Virtual AP profile named 'guestnet'. The interface is divided into two main sections: 'Profiles' on the left and 'Profile Details' on the right.

**Profiles:** A tree view on the left shows the hierarchy of configurations. Under 'Virtual AP profile', the 'guestnet' profile is selected and highlighted in blue. Other profiles listed include 'Corp-App-LC1-Sunnyvale-6000', 'Corp-App-LC2-Sunnyvale-6000', 'Corp-Employee-LC1-Sunnyvale-6000', 'Corp-Employee-LC2-Sunnyvale-6000', 'default', 'AAA Profile', '802.11K Profile', 'SSSID Profile', 'WMM Traffic Management Profile', 'test-rde-tunnel', 'VIA Client WLAN Profile', and 'AAA Profile'.

**Profile Details:** The right-hand section shows the configuration for the 'Virtual AP profile > guestnet'. It includes a table of settings:

Virtual AP profile > guestnet		Show Reference Save As Reset	
Virtual AP enable	<input checked="" type="checkbox"/>	Allowed band	all
VLAN	900	Forward mode	tunnel
Deny time range	--NONE--	Mobile IP	<input checked="" type="checkbox"/>
HA Discovery on-association	<input type="checkbox"/>	DoS Prevention	<input type="checkbox"/>
Station Blacklisting	<input checked="" type="checkbox"/>	Blacklist Time	3600 sec
Dynamic Multicast Optimization (DMO)	<input type="checkbox"/>	Dynamic Multicast Optimization (DMO) Threshold	6
Authentication Failure Blacklist Time	3600 sec	Multi Association	<input type="checkbox"/>
Strict Compliance	<input type="checkbox"/>	VLAN Mobility	<input type="checkbox"/>
Preserve Client VLAN	<input type="checkbox"/>	Remote-AP Operation	standard
Drop Broadcast and Multicast	<input type="checkbox"/>	Convert Broadcast ARP requests to unicast	<input type="checkbox"/>
Deny inter user traffic	<input type="checkbox"/>	Band Steering	<input checked="" type="checkbox"/>
Steering Mode	prefer-5ghz		

An 'Apply' button is located at the bottom right of the configuration area.

**Figure 16 Virtual AP configuration**

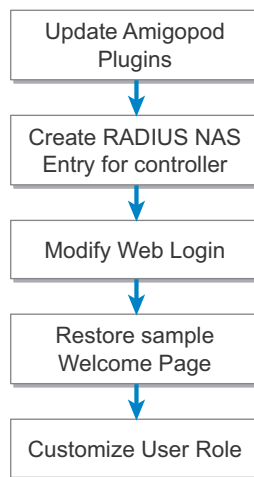
All the configurations from the previous steps have been applied to the campus VRD baseline, so the Aruba controller should now be attempting to redirect guest users to the web login page that is hosted by Amigopod.

The next chapter describes how to set up the corresponding components on the Amigopod configuration.

## Chapter 4: Amigopod Configuration

Leveraging the baseline configurations in the campus VRD design, this guide assumes that the Amigopod appliance is installed and available on the network. The reference design has Amigopod installed on an IP address of 10.169.130.50 and the assumption is that there is Internet access available to this IP address.

Figure 17 summarizes the steps to successfully mirror the RADIUS and captive portal configurations of the ArubaOS controller.



arun\_0642

**Figure 17** Amigopod configuration process

### Check for Updated Amigopod Plugins

Aruba publishes regular updates for the Amigopod solution via the online software distribution server, which is accessible from a standard Internet connection via the HTTPS protocol. Each Amigopod install is identified on the distribution server by a unique key known as a subscription ID, which is provided at the time of purchase or during an evaluation electronically. The subscription ID is entered into the Amigopod wizard during the initial installation, which triggers a download of all licensed software and updates for the individual deployment at hand. A subscription ID is in this format, which has been modified for illustration purposes:

- zdwpmn-xxxxxx-c8cy7b-yyyyyy-x228jr

A correctly configured subscription ID can be verified by browsing to **Amigopod Administrator > Plugin Manager > Manage Subscriptions** as shown in [Figure 18](#).

ARUBA networks Amigopod

Logged in as admin | amigopod.localdomain

## Amigopod Subscription

A subscription ID is a unique number used to identify your software license and any custom software modules that are part of your amigopod solution. [Help](#)

Subscription ID:

You can provide more than one subscription identifier by placing each subscription ID on a different line.

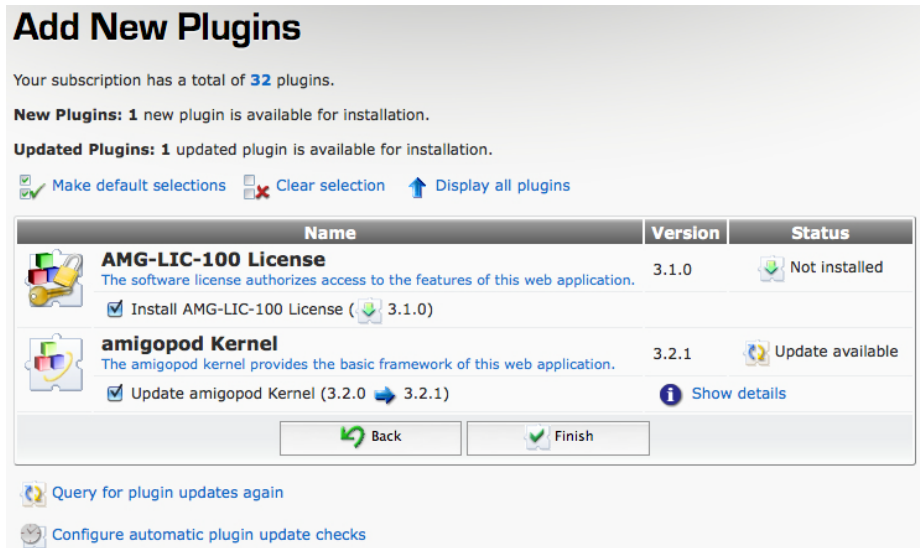
[Save and Continue](#)

- [Check for plugin updates](#)
- [Configure automatic plugin update checks](#)
- [Back to plugin manager](#)
- [Back to administrator](#)
- [Back to main](#)

Copyright © 2011 Aruba Networks, Inc. All rights reserved.

**Figure 18 Amigopod Subscription Manager**

If you click **Check for plugin updates**, the software update process begins on the Amigopod appliance. As shown in [Figure 19](#), the system contacts the software distribution server and downloads any new updates to the Amigopod system, any new licensed plugins, and other licensing updates.









**Add New Plugins**

Your subscription has a total of **32** plugins.

**New Plugins:** 1 new plugin is available for installation.

**Updated Plugins:** 1 updated plugin is available for installation.

Make default selections  Clear selection  Display all plugins

Name	Version	Status
 <b>AMG-LIC-100 License</b> The software license authorizes access to the features of this web application.	3.1.0	 Not installed
<input checked="" type="checkbox"/> Install AMG-LIC-100 License (  3.1.0 )		
 <b>amigopod Kernel</b> The amigopod kernel provides the basic framework of this web application.	3.2.1	 Update available
<input checked="" type="checkbox"/> Update amigopod Kernel (3.2.0  3.2.1) <a href="#">Show details</a>		

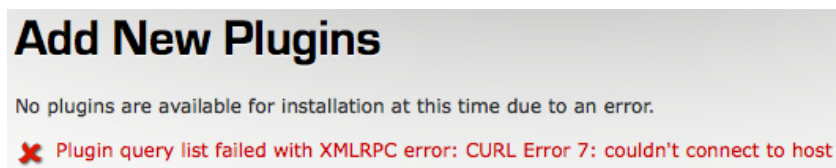
[Query for plugin updates again](#)

[Configure automatic plugin update checks](#)

**Figure 19 Add new Amigopod plugins**


If updates are available, they are listed and can be selected individually for installation. To complete the installation of any new plugins or updates, click **Finish**. For the updates to take effect, you must follow any prompted instruction to restart services after the installation of new or updated plugins. Plugins must be updated to ensure that Amigopod has downloaded its correct commercial license and all purchased features have been unlocked and are ready to use.

If an attempt to download the latest plugin fails with the error message shown in [Figure 20](#), the Amigopod does not have direct access to the Internet.



**Add New Plugins**

No plugins are available for installation at this time due to an error.

 Plugin query list failed with XMLRPC error: CURL Error 7: couldn't connect to host

**Figure 20 Plugin server unreachable**

To troubleshoot the issue, begin your investigations in these areas:

- Firewall rules
- Upstream proxies (Amigopod support proxy integration under the **Administrator > Network Setup** section)
- Correct default gateway for the Amigopod
- DNS resolution for the Amigopod

A useful diagnostic tool to verify that Amigopod has Internet connectivity via HTTP is available under **Administrator > Network Setup > Network Diagnostics** shown in [Figure 21](#).

**Network Diagnostic Tools**

✓ No network problems found. [Re-run network test](#)

Use this form to test or diagnose any network setup.

✓ Address was accessed successfully.

**Network Diagnostic Tools**

\* Diagnostic:

\* URL:   
The URL you wish to access.

\* required field

**Figure 21** Amigopod diagnostics

## Configure RADIUS NAS for an Aruba Controller

For the Aruba controller to authenticate users, it must be able to communicate with the Amigopod RADIUS instance. In first step of the Aruba controller configuration, a RADIUS server definition was defined. This step configures the opposing Amigopod NAS definition for the Aruba controller as seen in [Figure 22](#). For the RADIUS transactions to be successful, the RADIUS key used in the first Aruba controller configuration step must be entered exactly the same here.

To add a new RADIUS NAS entry, browse to **RADIUS > Network Access Servers** and click **Create**.

## RADIUS Network Access Servers

Each network access server that will use this RADIUS server for authentication or accounting purposes should be defined here.

Quick Help		Create	
Name	Hostname	Type	Comments
Guest-AAA	10.169.145.4	aruba_3576	
LC2-Sunnyvale-6000	10.169.145.5	aruba_3576	
MC1-Sunnyvale-3600 Login	10.169.130.6	aruba_3576	
remote-branch-guest	10.169.131.6	aruba_3576	

4 network access servers [Reload](#) 20 rows per page

[Import a list of network access servers](#)

[Back to RADIUS](#)

[Back to main](#)

**Figure 22** RADIUS NAS servers

The following fields must be configured in the RADIUS NAS definition as seen in [Figure 23](#):

- Name the NAS entry to match the local controller naming convention (need not be present in DNS).
- Enter IP address of the Aruba controller.
- The NAS Type should be set to **Aruba Networks (RFC3576 support)**.
- The Shared Secret (called the Key in the first Aruba controller step) must be configured and confirmed.
- Check **Create a RADIUS Web Login page for this network access server**, which will be used in the next step. The Aruba Networks presets are used to set up the web login page.



Additional RADIUS NAS entries must be created in master local environments because each local controller sources its own RADIUS client traffic.

The screenshot shows the Aruba Amigopod web interface for configuring RADIUS Network Access Servers. The main heading is "RADIUS Network Access Servers". Below the heading is a "Create Network Access Server" form. The form fields are:

- Name:** MC1-Sunnyvale-3600 Login
- IP Address:** 10.169.130.6
- NAS Type:** Aruba Networks (RFC 3576 support)
- Shared Secret:** (masked)
- Confirm Shared Secret:** (masked)
- Description:** (empty)
- Web Login:**  Create a RADIUS Web Login page for this network access server

Below the form is a table with the following columns: Name, Hostname, Type, Comments. The table is currently empty, with a message: "There are no network access servers to display." The page also includes a "Create NAS Device" button, a "Reset Form" button, and a "Cancel" button.

**Figure 23** NAS server configuration

Click **Create NAS Device**, and you are prompted to restart the RADIUS server as seen in [Figure 24](#). You must restart the server, because the RADIUS server within Amigopod rejects any request from the Aruba controller as unknown until the restart has been performed.

**RADIUS Network Access Servers**

The local RADIUS server needs to be restarted to complete the changes made.

Restart RADIUS Server

Each network access server that will use this RADIUS server for authentication or accounting purposes should be defined here.

Name	Hostname	Type	Comments
MC1-Sunnyvale-3600	10.169.130.6	aruba_3576	

Quick Help Create

Edit Delete Ping Edit Web Login Launch Web Login

The Network Access Server is responding to pings:

```
PING 10.169.130.6 (10.169.130.6) 56(84) bytes of data.
64 bytes from 10.169.130.6: icmp_seq=1 ttl=64 time=20.8 ms

--- 10.169.130.6 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 20.820/20.820/20.820/0.000 ms
```

1 network access server Reload 20 rows per page

**Figure 24** Restart the RADIUS server



## Configure Web Login for Captive Portal Authentication

If you clicked **Create Web Login** in the previous step, a newly created web login page can be seen in **Customization > Web Logins**. [Figure 25](#) shows the automatically created web login, but a new one can be created manually at a later stage.

The screenshot displays the 'RADIUS Web Login Editor' interface. The configuration is for a web login named 'MC1-Sunnyvale-3600 Login'. The 'Page Name' is 'Aruba\_login'. The 'Description' is 'Auto-generated web login for NAS MC1-Sunnyvale-3600 Login'. The 'Vendor Settings' are set to 'Aruba Networks'. The 'Address' is '10.169.130.6'. The 'Secure Login' is set to 'Use vendor default'. The 'Dynamic Address' checkbox is checked, indicating that the controller will send the IP to submit credentials. The 'Allowed Dynamic' field contains the IP addresses: 10.169.130.6, 10.169.130.7, 10.169.145.4, and 10.169.145.5. The 'Denied Dynamic' field is empty.

**Figure 25** Automatically generated web login page

The Page Name field defines the URL that is hosted on the Amigopod appliance. For example, in the Aruba controller configuration chapter of this document, the Login Page entry of the captive portal profile was defined as the following URL:

```
https://10.169.130.50/Aruba_login.php
```

The Page Name field allows the administrator to customize what web page name is published at the root of the Amigopod web server. [Figure 25](#) shows that the Aruba\_login name is defined to match the configuration of the captive portal profile on the Aruba controller.



You need not include the .php extension because it is appended automatically.

The Address field should be set to the IP address of the Aruba controller. That is, this address needs to be available from the guest client device via the captiveportal policy on the controller.

Alternatively, the switchip variable that is sent as part of the redirect URL can be parsed automatically and used as the IP address for the web login credential submission. This option should be selected in multicontroller environments so that the web login page dynamically is aware of which controller the guest user is currently connected to and therefore which controller must be part of the authentication transaction.

Here is a sample redirect URL that includes the switchip variable:

```
https://10.169.130.50/Aruba_login.php?cmd=login&switchip=10.169.130.6&mac=00:21:00:95:61:29&ip=10.0.20.58&ssid=guestnet&url=http%3A%2F%2Fwww%2Egoogle%2Ecom%2F
```

To make use of the switchip variable, enable **Dynamic Address** as shown in [Figure 25](#). Additional security mechanisms have been implemented in the form of white and black lists that allow the administrator to define valid IP addresses of the controller deployment in their environment. This additional security measure prevents modification of the redirect URL by individuals that might attempt to extract user credentials by spoofing the form submission to a device in their control. If the Amigopod receives a switchip value that does not match the white list, the Amigopod responds to the default address.

The example in [Figure 25](#) shows that the master and local controllers defined in the campus VRD are permitted in the white list of valid controller IP addresses.

The web login page now is configured and is ready to be tested against the previous Aruba controller configurations.

## Optional Customization of the Web Login Page

Several Login Form options allow you to override the default login form and labels used to reference user and password fields. These fields are shown in [Figure 26](#), but typically they do not need to be changed.

<b>Login Form</b>	
Options for specifying the behaviour and content of the login form.	
Custom Form:	<input type="checkbox"/> Provide a custom login form If selected, you must supply your own HTML login form in the Header or Footer HTML areas.
Custom Labels:	<input type="checkbox"/> Override the default labels and error messages If selected, you will be able to alter labels and error messages for the current login form.
Pre-Auth Check:	<input type="checkbox"/> Perform a local authentication check If checked, the username and password will be checked locally before proceeding to the NAS authentication. This option should not be selected if an external authentication server is in use.
Terms:	<input checked="" type="checkbox"/> Require a Terms and Conditions confirmation If checked, the user will be forced to accept a Terms and Conditions checkbox.

**Figure 26 Login Form options**

The Pre-Auth Check is required only for advanced configurations where you might need to ensure that the username and password pair is valid before the RADIUS transaction is initiated from the Aruba controller. The web login and RADIUS database are hosted on the same appliance, so a query can be performed locally before a RADIUS transaction is initiated.

You can enable the display of an Accept Terms & Conditions option on the login page. This option refers to the default terms and conditions URL defined under **Customization > Guest Manager Settings** as seen in [Figure 27](#).

	external/terms.html
Terms Of Use URL:	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.

**Figure 27** Configuration of terms and conditions

## Amigopod Skins and Content Customization

You can leverage the Amigopod skin technology to brand the captive portal that is displayed to the wireless and wired users. These skins are available as a professional service as a purchasable SKU or custom and blank skins are available for customers who want to perform their own HTML and CSS style customization. [Figure 28](#) shows the login page customization screen.

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:	Login The title to display on the web login page.
Header HTML:	<pre>{if \$errmsg} {nwaicontext type=error}{\$errmsg}{/nwaicontext} {/if}  &lt;p&gt; Please login to the network using your amigopod username and password. &lt;/p&gt;</pre> <p>Insert content item...    Insert self-registration link...</p> <p>HTML template code displayed before the login form.</p>
Footer HTML:	<pre>&lt;p&gt; Contact a staff member if you are experiencing difficulty logging in. &lt;/p&gt;</pre> <p>Insert content item...    Insert self-registration link...</p> <p>HTML template code displayed after the login form.</p>
Login Message:	<pre>&lt;p&gt; Logging in, please wait... &lt;/p&gt;</pre>

**Figure 28** Login page customization

The Title field allows you to customize the page title that is displayed in the browser. The Header, Footer, and Login fields allow the administrator to add and modify the displayed text and content displayed on the web login page. You can choose **Insert Content** to display content items that have been uploaded via **Customization > Content Manager**. You can also choose **Insert self-registration link**, which directly inserts the required HTML to display self registration links found under **Customization > Guest Self Registration**.



The code at the top of the Header HTML field parses the redirect URL from the Aruba controller. If an authentication error occurs, the controller returns an error message in the `errmsg` variable.

You can set a login delay, which pauses the login process at the point where the contents of the Login Message HTML is displayed. This delay is useful for many reasons. If you need to troubleshoot any captive portal issues, this delay is a good time to obtain the contents of a view source in the client's browser. Alternatively this delay can be used to display additional branding and messaging to the guest users during the login process.

## Web Login Access Lists

The web login page can be configured with access lists to allow or deny specific IP source address ranges. You can select how you want the web server to behave when responding to an invalid request, as seen in [Figure 29](#).

**Network Login Access**  
Controls access to the login page.

Allowed Access:	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <p style="font-size: small; color: #0070C0; margin-top: 5px;">Enter the IP addresses and networks from which logins are permitted.</p>
Denied Access:	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <p style="font-size: small; color: #0070C0; margin-top: 5px;">Enter the IP addresses and networks that are denied login access.</p>
* Deny Behavior:	<div style="border: 1px solid #ccc; padding: 2px;"> <span style="font-size: small;">Send HTTP 404 Not Found status</span> <span style="float: right; font-size: 10px;">⌵</span> </div> <p style="font-size: small; color: #0070C0; margin-top: 5px;">Select the response of the system to a request that is not permitted.</p>

Save Changes

Save and Reload

**Figure 29** Network Login Access window

## Configure the RADIUS User Role

The RADIUS user role is a collection of one or many RADIUS standard or vendor-specific attributes (VSAs). These attributes can be used to signal role-based access control context back to the Aruba controller as shown in [Figure 30](#).

The screenshot displays the 'RADIUS User Role Definition' page in the Amigopod web interface. The page is titled 'RADIUS User Role Definition' and shows the configuration for a role named 'Guest'. The role ID is 2. The role name is 'Guest' and the description is 'Default role for guest accounts.' Below this, there is a section for 'RADIUS Attributes' with a 'RADIUS Attribute Editor' form. The attribute is set to Vendor: Aruba, Attribute: Aruba-User-Role, Value: auth-guest, and Condition: Always. There is an 'Add Attribute' button and a 'Save Changes' button at the bottom.

**Figure 30 RADIUS user role definition**

The **Aruba-User-Role** is an example of an Aruba VSA that allows a RADIUS authentication session to automatically have a user role applied. The example of auth-guest is a user role that is defined as part of the campus VRD baseline configuration.

Amigopod automatically calculates the available time of a guest session and return this value in the session-timeout attribute so the controller can manage the termination of the session. For example, if a guest account was created with a 2-hour expiry, Amigopod returns a session-timeout value of 7200 seconds.

This RADIUS role is presented as a selection when creating new guest accounts via the **Create User** screens of the Amigopod Guest Manager or can be hard coded as a hidden field in the self-registration pages to ensure that each user session gets managed appropriately on the Aruba controller.

## (Optional) Import Sample Welcome Page

As part of the Aruba controller configuration, the captive-portal profile defines a proposed welcome page of:

```
https://10.169.130.50/Aruba_welcome.php
```

This page is not installed by default on the Amigopod system and therefore it must be created if the installation requires a locally hosted welcome page. Some deployments choose to configure the welcome page to point towards the corporate public website or other website of interest. But many customers prefer to leverage the ability of Amigopod to host a welcome page locally and enable additional user experience options such as:

- Integrated graphical Wi-Fi Logout button.
- Present an option for the guest user to continue to their originally request URL.
- Display information regarding the terms of service.
- Display a summary of session statistics that could optionally include a time or quota countdown.
- Leverage the welcome page as a branding platform for advertising or other information delivery.

To demonstrate some of these deployment options, a backup of a preconfigured sample welcome page has been made and published for download. This backup file includes all the required graphics and configuration details to implement several of these additional features.

The backup of a previously created Amigopod web login page is available in zip file with this document. To install this backup file, browse to **Administrator > Backup & Restore > Configuration Restore**.

**Configuration Restore: Step 1**

**Step 1:** Specify the backup file you want to restore.

[Restore a backup from a URL](#)

If the backup file is larger than the maximum file upload size, you must specify a URL for the backup file instead.

**Upload File**

Size Limit: Maximum file upload size: 5.0 MB

\* Backup File:  [Browse...](#)

[Select the backup file to start the restore process.](#)

[Continue](#)

\* required field

[Back to backup & restore](#)

[Back to administrator](#)

[Back to main](#)

**Figure 31** Restore backup configuration

Enter the download link and click **Continue** to start the restore process.

## Configuration Restore: Step 2

**Step 2:** Select the configuration items you want to restore.

**Configuration Backup**

Backup: **Amigopod VRD Welcome Logout pages** (custom)

Configuration Item	Restore
<b>RADIUS Services</b>	✕ ↓ ✓
<b>RADIUS Web Logins</b>	✕ ↓ ✓
Amigopod VRD Logout	✕ ✓
Amigopod VRD Welcome	✕ ✓
<b>Server Configuration</b>	✕ ↓ ✓
<b>Uploaded Files in Content Manager</b>	✕ ↓ ✓
MOVE_banner.jpg	✕ ✓
wifi-logout.png	✕ ✓
<span style="color: red;">✕ Unselect All</span> <span style="float: right;">10 rows per page</span>	

Select the items from this configuration backup to restore.

**\* Confirm:**  Restore settings from backup  
 Select this option to confirm the restore operation. Caution! This may overwrite your current settings.

[Restore Configuration](#)

\* required field

[Back to step 1](#)

[Back to administrator](#)

[Back to main](#)

**Figure 32** Restore welcome page

To restore the customized welcome page, check **Restore settings from backup** and click **Restore Configuration**. When the restore is complete, browse to **Customize > Web Logins** and verify that the web login page has been successfully restored to the local deployment, as seen in [Figure 33](#).

## RADIUS Web Logins

Many NAS devices support Web-based authentication for visitors. ? Help

By defining a web login page on the amigopod you are able to provide a customised graphical login page for visitors accessing the network through these NAS devices.

Use this list view to define new web login pages, and to make changes to existing web login pages.

[Create a new web login page](#)

Name	Page Title	Page Name	Page Skin
<b>Amigopod VRD Logout</b> <a href="#">Custom Amigopod VRD Logout page</a>	You have been successfully Logged Out	Aruba_logout	(Default)
<b>Amigopod VRD Welcome</b> <a href="#">Custom Amigopod VRD Welcome page</a>	Welcome to Aruba Guest WIFI	Aruba_welcome	(Default)
<b>MC1-Sunnyvale-3600 Login</b> <a href="#">Auto-generated web login for NAS MC1-Sunnyvale-3600 Login</a>	Login	Aruba_login	(Default)
<b>MDPS Enrollment</b> <a href="#">Mobile Device Provisioning enrollment page.</a>	Employee Smartphone and Tablet Registration	device_provisioning	(Default)

4 web logins [Reload](#) 20 rows per page

[Back to customization](#)

[Back to main](#)

**Figure 33** RADIUS Web Logins page

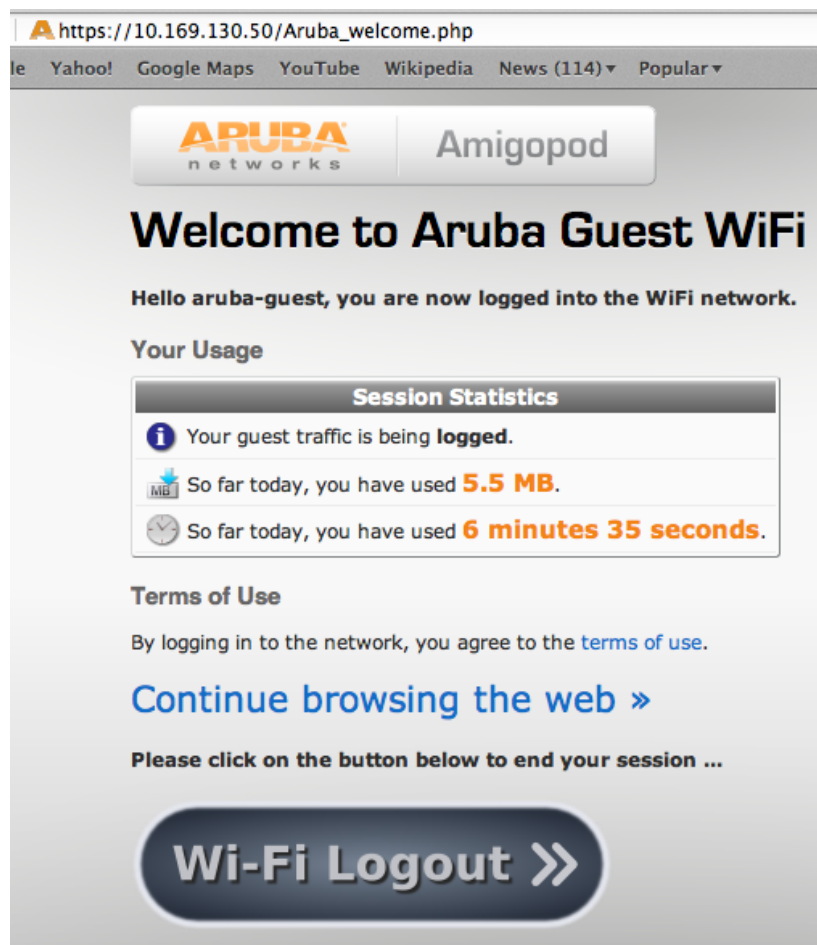
As seen in the Page Name column in [Figure 33](#), this web login page is hosted at the following address:

`https://10.169.130.50/Aruba_welcome.php`

This URL can be changed to suit each local deployment and the corresponding captive portal profile on the ArubaOS controller must be modified to match any changes made.

[Figure 34](#) shows the sample welcome page developed for this guide. This welcome page highlights the following integration points between the Amigopod and ArubaOS controllers:

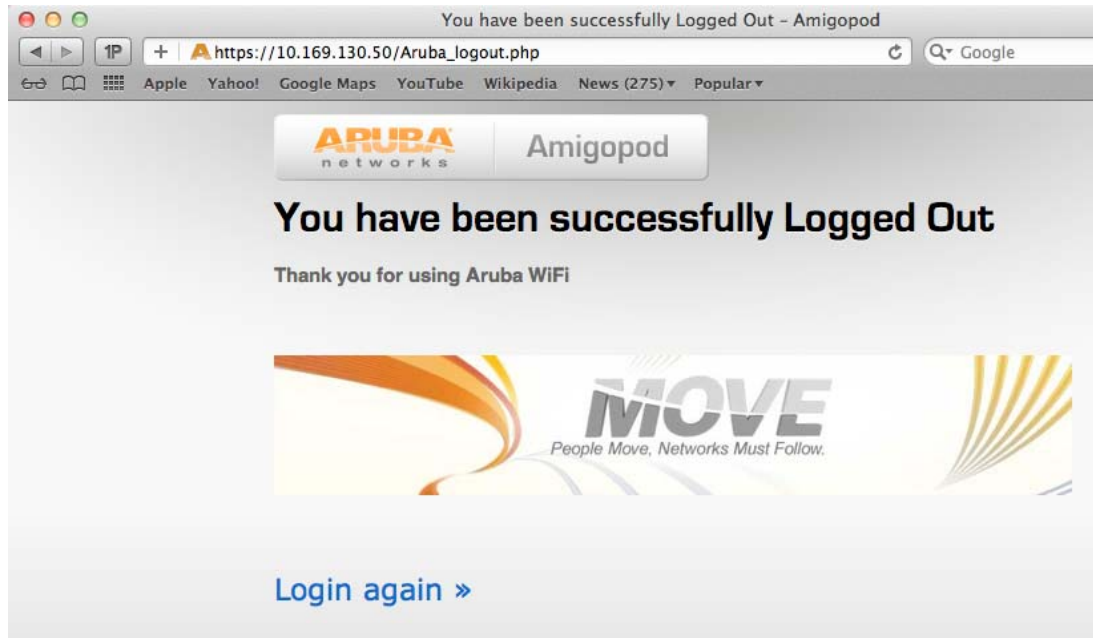
- Detection of guest user name logged into the Aruba Wi-Fi network
- Ability to display and track usage of each guest session
- Linking to a Terms of Use page or other relevant information to the deployment
- Caching of the guest user's originally requested URL and providing an option to continue to that page
- Hosting a Wi-Fi Logout button to allow the guest user to initiate a logout of their session



**Figure 34** Captive portal welcome page



A logout page is also included in the sample backup file. This page is linked to the Wi-Fi Logout button on the previous welcome page and allows for further messaging to be displayed on the logout page. As shown in [Figure 35](#), the inclusion of this sample logout page allows for a consistent user experience and also another opportunity of branding or messaging to the guest Wi-Fi user.



**Figure 35** Logout page

## Chapter 5: Integration Verification

If you complete the steps in [Chapter 3: ArubaOS Configuration](#) and [Chapter 4: Amigopod Configuration](#), you should have the base configuration for a functioning guest access solution that can be further customized to suit each local deployment.

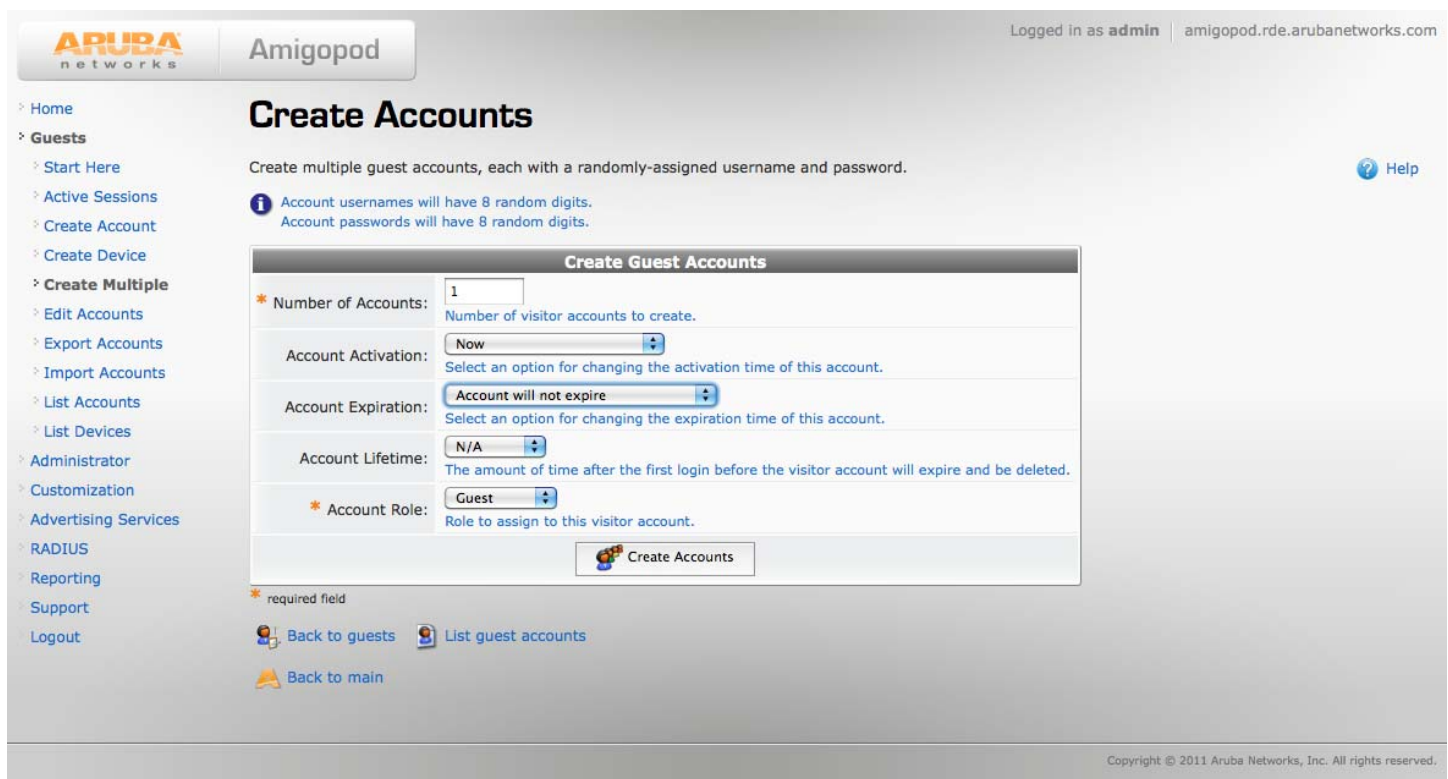
The chapter provides some simple verification tests that can be performed to ensure that all the functional components are in place and are working as expected.

### Create a Test Account Within Amigopod Guest Manager

To start testing the guest access functionality, an account must be created in the Amigopod local database. Accounts can be created through the Amigopod WebUI in many different ways:

- Create a single guest account (**Guests > Create Account**).
- Create multiple guest accounts (**Guests > Create Multiple**).
- Import from CSV (**Guests > Import Device**).
- Create a MAC device (**Guest > Create Device**).

Any of these methods can be used to create the testing accounts. In the example in [Figure 36](#), **Create Multiple** has been selected as a quick method to create one or more guest accounts.



The screenshot displays the Amigopod WebUI interface for creating guest accounts. The page title is "Create Accounts" and the subtitle is "Create multiple guest accounts, each with a randomly-assigned username and password." The form includes the following fields:

- Number of Accounts:** 1 (required field)
- Account Activation:** Now (dropdown menu)
- Account Expiration:** Account will not expire (dropdown menu)
- Account Lifetime:** N/A (dropdown menu)
- Account Role:** Guest (dropdown menu)

A "Create Accounts" button is located at the bottom of the form. Below the form, there are navigation links: "Back to guests", "List guest accounts", and "Back to main". The footer of the page contains the copyright notice: "Copyright © 2011 Aruba Networks, Inc. All rights reserved."

**Figure 36** Create an Amigopod guest account

The resulting account is created with random digits for both the username and password as shown in [Figure 37](#).

**Finished Creating Guest Accounts**

Finished creating one guest account.

The details about each of the accounts created are shown below.

Account Details	
Username	22163841
Password	65652839
Role	Guest

Open print window using template...

Save list for scratch cards (CSV file)

Back to guests   List guest accounts

Back to main

**Figure 37** Completed guest account

If numeric user credentials will be challenging during your testing phase, these credentials can be edited easily by clicking the **List guest accounts** option. Click the newly created guest account to display the actions that are available for the new account. Click **Edit** to make changes to the user credentials.

**Guest Manager Accounts**

The following table shows the guest accounts that have been created. Click an account to modify it.

Quick Help   Create   More Options

Filter:

Username	Role	Status	Expiration
22163841	Guest	Enabled	N/A

Reset password   Change expiration   Remove   Edit   Sessions

Print

To update the properties of this guest account, use the form below:

**Edit Account**

\* Visitor's Name:  Test Account  
Name of the visitor.

\* Username:  aruba-guest  
Name of the visitor account.

Account Activation:  (No changes: Account is active)  
Select an option for changing the activation time of this account.

Account Expiration:  (No changes: Account will not expire)  
Select an option for changing the expiration time of this account.

Account Lifetime:  (No changes: N/A)  
The amount of time after the first login before the visitor account will expire and be deleted.

Allowed Usage:  (No changes: N/A)  
Select an option for changing the allowed usage time of this account.

Account Role:  (No changes: Guest)  
Role to assign to this visitor account.

\* Password:  Type in a new password  
Select an option for editing the visitor account's password.

New password:  \*\*\*\*\*  
Type in a new password to assign to the visitor account.

Confirm Password:  \*\*\*\*\*  
Repeat the new password for the visitor account.

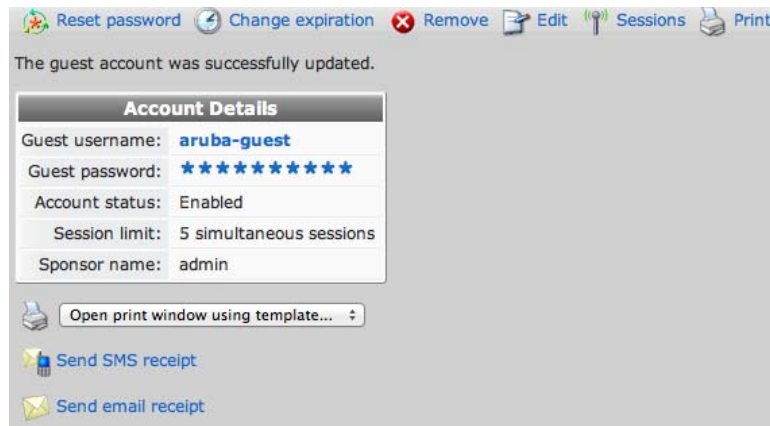
Session Limit:  5  
The number of simultaneous sessions allowed for this visitor account. Type 0 for unlimited use.

Update Account

\* required field

**Figure 38** Editing a guest account

On the Edit screen, a new username and password can be defined manually to make any level of repetitive testing easier on the administrator. Click **Update Account** to display the confirmation page as shown in [Figure 39](#).



**Figure 39 Updated guest account**

## Testing RADIUS

This section shows how RADIUS transactions with the Amigopod server can be tested to confirm that the configuration is correct.

### Test Basic RADIUS Transactions

Diagnostic RADIUS transactions can be initiated from the controller from either the WebUI or the CLI as shown.

#### Testing the AAA Server

```
(LC1-Sunnyvale-6000) #aaa test-server mschapv2 Amigopod aruba-guest *****
Authentication Successful
```



**Figure 40 Testing the AAA server**

On the Amigopod side, you can also look at the end of the RADIUS log to verify that the transactions are executing on that side.

ARUBA networks | Amigopod | Logged in as admin | amigopod.rde.arubanetworks.com

## RADIUS Server Control

Control the local RADIUS server using these command links.

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: **Tue Aug 30 16:31:42 2011 -0700**

### RADIUS Log Snapshot

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

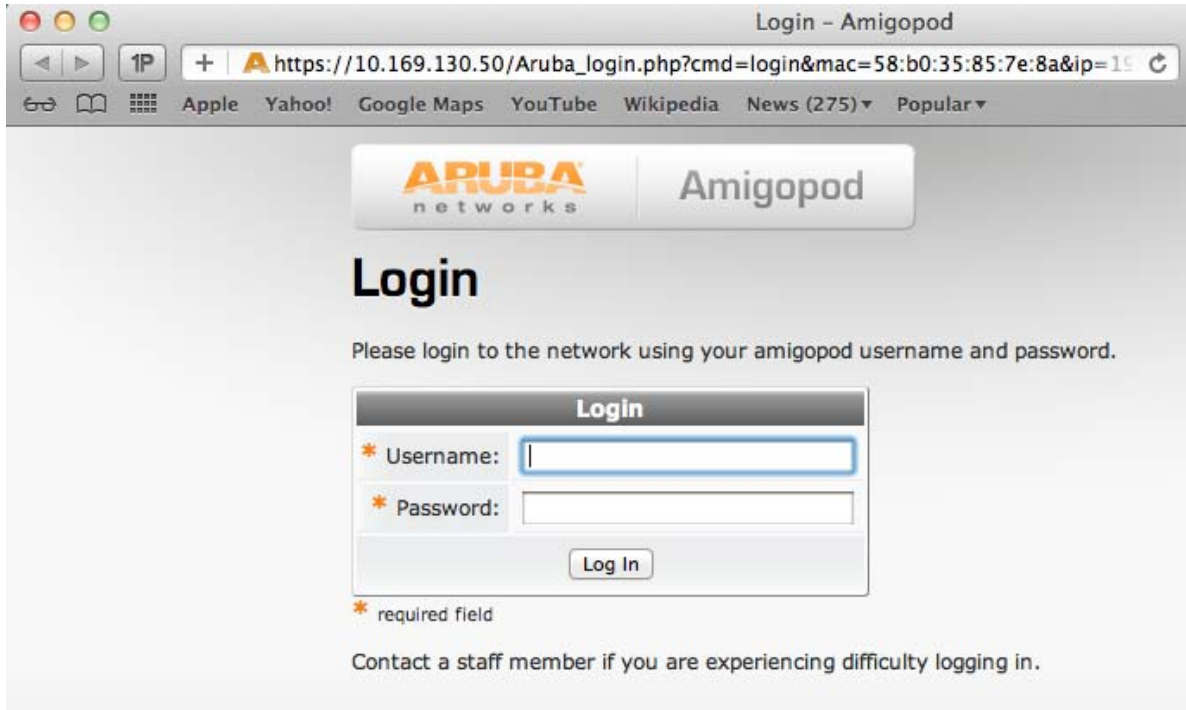
```
Tue Aug 30 16:30:38 2011 : Auth: Login OK: [aruba-guest] (from client LC1-Sunnyvale-6000 port 0 cli 000000000000)
Tue Aug 30 16:26:38 2011 : Auth: Login OK: [aruba-guest] (from client LC2-Sunnyvale-6000 port 0 cli 000000000000)
Tue Aug 30 16:23:59 2011 : Info: Ready to process requests.
Tue Aug 30 16:23:59 2011 : Info: Loaded virtual server <default>
```

**Figure 41 RADIUS log tail**

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

## Test Login and Verify Successful RADIUS Transaction

Now that everything is set up on the Amigopod and the Aruba controller, attempt to connect a test wireless or wired client to the network. The session should be redirected successfully to the Amigopod web login page.



**Figure 42** Amigopod portal Page

After you enter the test user account credentials and click **Log In**, a successful end-to-end RADIUS transaction should be the result. You can verify by referring to the end of the RADIUS log as shown in [Figure 43](#). Note that the client MAC address is now visible in the RADIUS log entry because it was driven by the captive portal authentication process on the controller.

The screenshot displays the Amigopod web interface for RADIUS Server Control. The page title is "RADIUS Server Control" and it includes a navigation menu on the left with options like Home, Guests, Administrator, Customization, Advertising Services, RADIUS, Authentication, Database List, Dictionary, NAS List, Server Control, User Roles, Reporting, Support, and Logout. The main content area shows the status "The RADIUS server is currently running." and several action buttons: "Restart RADIUS Server", "Stop RADIUS Server", "Debug RADIUS Server", "View Failed Authentications", and "Test RADIUS Authentication". Below these buttons, the "RADIUS Server Time" is shown as "Tue Aug 30 16:35:02 2011 -0700". The "RADIUS Log Snapshot" section displays the most recent log entries, including a successful login for the [aruba-guest] user from client LC1-Sunnyvale-6000.

```

Tue Aug 30 16:33:35 2011 : Auth: Login OK: [aruba-guest] (from client LC1-Sunnyvale-6000 port 0 cli 002608F1B1EB)
Tue Aug 30 16:30:38 2011 : Auth: Login OK: [aruba-guest] (from client LC1-Sunnyvale-6000 port 0 cli 000000000000)
Tue Aug 30 16:26:38 2011 : Auth: Login OK: [aruba-guest] (from client LC2-Sunnyvale-6000 port 0 cli 000000000000)
Tue Aug 30 16:23:59 2011 : Info: Ready to process requests.
Tue Aug 30 16:23:59 2011 : Info: Loaded virtual server <default>

```

**Figure 43** Successful RADIUS log entry on Amigopod

## Check that RADIUS Accounting is Working as Expected

If RADIUS accounting traffic is not being received by Amigopod, you will not find a corresponding entry in the **Guests > Active Sessions** page shown in [Figure 44](#).

Given the Interim Accounting support in ArubaOS 6.1, this page displays live traffic statistics based on these updates.

If you also have configured RFC 3576 on your Aruba controller, you can click any active session and click **Disconnect** to terminate that session on the Aruba controller. The user is returned to the initial role that corresponds to the configured AAA profile.

The screenshot shows the Amigopod web interface. The top navigation bar includes the Aruba Networks logo, the Amigopod title, and the user 'admin' logged in. The left sidebar contains a navigation menu with 'Active Sessions' selected. The main content area is titled 'Active Sessions' and displays a table of active sessions. The table has columns for Username, IP Address, MAC Address, Role, NAS, Session Start, Session Time, and Session Traffic. A single session is listed for 'aruba-guest' with an IP of 192.168.200.252 and a role of 'Guest'. The session started on 2011-08-30 at 16:33 and has a duration of 19 minutes and 45 seconds, with 0.8 MB of traffic. Below the table, there are links for 'Back to guests' and 'Back to main'.

Username	IP Address	MAC Address	Role	NAS	Session Start	Session Time	Session Traffic
aruba-guest	192.168.200.252	00:26:08:f1:b1:eb	Guest	LC1-Sunnyvale-6000	2011-08-30 16:33	19min 45sec	0.8 MB

**Figure 44** Amigopod Active Sessions displays RADIUS accounting data



## Chapter 6: Troubleshooting Tips

This chapter provides basic troubleshooting steps to use for specific issues.

If the test device is not being redirected to the Amigopod captive portal:

- Check the DNS resolution because the client will not be redirected if it cannot resolve the initially requested webpage. Command line tools such as nslookup and ping can be used.
- Check the initial role that is assigned to the guest AAA profile and ensure that traffic is permitted to the Amigopod IP address for the redirect via HTTP or HTTPS via an appropriate policy.
- Verify that the Amigopod has a route back to the address space of the test client. Look at how NAT and the default gateway of Amigopod are referenced as part of your troubleshooting steps.

If the login process stalls and the logs show that no RADIUS request was received from the Aruba controller:

- Check the web login page and ensure that the correct IP address for controller is configured.
- Check the captive portal policy and ensure that traffic is permitted to the configured IP address of the controller.

If you receive an error message in the RADIUS logs about an unknown client:

- Check the RADIUS NAS list and ensure that it has an entry that matches the IP address listed in the error message. The Aruba controller may be using loopback instead of the 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.

If you receive an error message in the RADIUS logs about an incorrect login:

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

## Appendix A: Contacting Aruba Networks

### Contacting Aruba Networks

Web Site Support	
Main Site	<a href="http://www.arubanetworks.com">http://www.arubanetworks.com</a>
Support Site	<a href="https://support.arubanetworks.com">https://support.arubanetworks.com</a>
Software Licensing Site	<a href="https://licensing.arubanetworks.com/login.php">https://licensing.arubanetworks.com/login.php</a>
Wireless Security Incident Response Team (WSIRT)	<a href="http://www.arubanetworks.com/support/wsirt.php">http://www.arubanetworks.com/support/wsirt.php</a>
Support Emails	
Americas and APAC	<a href="mailto:support@arubanetworks.com">support@arubanetworks.com</a>
EMEA	<a href="mailto:emea_support@arubanetworks.com">emea_support@arubanetworks.com</a>
WSIRT Email Please email details of any security problem found in an Aruba product.	<a href="mailto:wsirt@arubanetworks.com">wsirt@arubanetworks.com</a>

Validated Reference Design Contact and User Forum	
Validated Reference Designs	<a href="http://www.arubanetworks.com/vrd">http://www.arubanetworks.com/vrd</a>
VRD Contact Email	<a href="mailto:referencedesign@arubanetworks.com">referencedesign@arubanetworks.com</a>
AirHeads Online User Forum	<a href="http://airheads.arubanetworks.com">http://airheads.arubanetworks.com</a>

Telephone Support	
Aruba Corporate	+1 (408) 227-4500
FAX	+1 (408) 227-4550
Support	
<ul style="list-style-type: none"> <li>● United States</li> </ul>	+1-800-WI-FI-LAN (800-943-4526)
<ul style="list-style-type: none"> <li>● Universal Free Phone Service Numbers (UIFN):</li> </ul>	
<ul style="list-style-type: none"> <li>■ Australia</li> </ul>	Reach: 1300 4 ARUBA (27822)
<ul style="list-style-type: none"> <li>■ United States</li> </ul>	1 800 9434526 1 650 3856589
<ul style="list-style-type: none"> <li>■ Canada</li> </ul>	1 800 9434526 1 650 3856589
<ul style="list-style-type: none"> <li>■ United Kingdom</li> </ul>	BT: 0 825 494 34526 MCL: 0 825 494 34526

## Telephone Support

### ● Universal Free Phone Service Numbers (UIFN):

■ Japan	IDC: 10 810 494 34526 * Select fixed phones IDC: 0061 010 812 494 34526 * Any fixed, mobile & payphone KDD: 10 813 494 34526 * Select fixed phones JT: 10 815 494 34526 * Select fixed phones JT: 0041 010 816 494 34526 * Any fixed, mobile & payphone
■ Korea	DACOM: 2 819 494 34526 KT: 1 820 494 34526 ONSE: 8 821 494 34526
■ Singapore	Singapore Telecom: 1 822 494 34526
■ Taiwan (U)	CHT-I: 0 824 494 34526
■ Belgium	Belgacom: 0 827 494 34526
■ Israel	Bezeq: 14 807 494 34526 Barack ITC: 13 808 494 34526
■ Ireland	EIRCOM: 0 806 494 34526
■ Hong Kong	HKTI: 1 805 494 34526
■ Germany	Deutsche Telekom: 0 804 494 34526
■ France	France Telecom: 0 803 494 34526
■ China (P)	China Telecom South: 0 801 494 34526 China Netcom Group: 0 802 494 34526
■ Saudi Arabia	800 8445708
■ UAE	800 04416077
■ Egypt	2510-0200 8885177267 * within Cairo 02-2510-0200 8885177267 * outside Cairo
■ India	91 044 66768150