



## Bluesocket Integration Guide

Revision 1.0  
13 August 2009

United States of America  
+1 (888) 590-0882

Europe, Middle East & Asia  
+34 91 766 57 22

Australia & Pacific  
+61 2 8669 1140

<http://www.amigopod.com>

---

# Table of Contents

## Contents

Introduction .....	3
Test Environment .....	4
Integration .....	5
Bluesocket Configuration .....	6
Step 1 – Create New Wired and/or Wireless VLAN (Optional).....	6
Step 2 – Create RADIUS Accounting Server .....	7
Step 3 – Create RADIUS Authentication Server .....	8
Step 4 – Create Custom Web Login page .....	10
Step 5 – Selecting the Custom User Login for Managed Interface .....	13
Step 6 – Configure the Un-Registered Role .....	14
Amigopod Configuration.....	15
Step1 – Create RADIUS NAS for Bluesocket .....	15
Step 2 – Restart RADIUS Services .....	16
Step 3 – Configure Bluesocket Web Logins Page on Amigopod .....	17
Step 4 – Confirm External Captive Portal URL .....	19
Step 5 – Create a User account .....	27
Testing the Configuration .....	28
Step 1 – Test the RADIUS Authentication Server on the BlueSecure.....	28
Step 2 - Connect to the Amigopod wired or wireless network .....	29
Step 3 – Confirm DHCP IP Address received.....	30
Step 4 – Launch Web Browser and login .....	32
Step 5 – Confirm RADIUS debug messages on amigopod.....	34

---

## Introduction

This document outlines the configuration process on both the Bluesocket's BlueSecure wireless controller and the Amigopod appliance to create a fully integrated Visitor Management solution. The solution leverages the captive portal functionality built into the Bluesocket software image.

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

Captive portal authentication is the simplest form of authentication to use and requires no software installation or configuration on the client. The username/password 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 WEP or WPA-PSK) should be used when sensitive data will be sent over the wireless network.

Amigopod extends the standard Bluesocket captive portal functionality by providing many advanced features such as 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 to name a few.

---

## Test Environment

The test environment referenced throughout this integration guide is based on BSC-1200 controller. Although BSC-1200 is only one of its many hardware platform, the testing and therefore this procedure is valid for all hardware variants from Bluesocket in its BlueSecure Controller platform.

The following table shows the software versions used during the integration testing. This document will be updated in the future if changes in either Amigopod or Bluesocket subsequent releases affect the stability of this integration. It is advised that the customer always check for the latest integration guide available from either Amigopod or Bluesocket.

## Amigopod Configuration

The following table reviews the IP Addressing used in the test environment but this would be replaced with the site specific details of each customer deployment:

<b>Dated Tested:</b>	July 2009
<b>Amigopod Version:</b>	Kernel→2.0, Radius Services→ 2.0
<b>Plugins Required:</b>	Standard build only
<b>Bluesocket Version:</b>	6.4
<b>Integration:</b>	HTTP Captive Portal

## Bluesocket Configuration

The following table reviews the IP Addressing used in the test environment but this would be replaced with the site specific details of each customer deployment:

<b>Bluesocket IP Address</b>	192.168.160.118 (Protected Interface)
<b>Internet Gateway Address</b>	192.168.160.1
<b>Amigopod IP Address</b>	192.168.160.5
<b>Amigopod RADIUS port</b>	Auth 1812 Acc 1813 (default settings)

**Note:** Amigopod VMA LAN interface and the Bluesocket controller's Protected Interface were placed into the same subnet.

---

## Integration

Although the Bluesocket supports both internal and external captive portal functionality, this integration guide will focus on the later as the internal captive portal dictates the use of the internal login page resident on the controller itself. The login page is very basic and doesn't allow for significant customization as is possible with the Amigopod Web Logins feature.

**Note:** Bluesocket does allow for fully customized captive portal pages but this process requires a significant amount of web design experience to produce a professional result. One of amigopod's strongest selling points is the Skin Plugin technology where the presentation of the user interface is separated from the mechanics of the underlying application. This allows Amigopod to supply end users with a ready branded Skin for all Amigopod interaction (both Visitor and Administrators) for a small nominal fee at time of purchase.

The integration will also leverage the Bluesocket's ability to define and reference external RADIUS servers for the authentication and accounting of visitor accounts. In the standalone Bluesocket Guest provisioning solution the local database in each controller is used to store user credentials, limiting 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.

## Bluesocket Configuration

### Step 1 - Create New Wired and/or Wireless VLAN (Optional)

A new VLAN can be created to bind to the new Wireless LAN that will be used for the guest users. From the *Controller* → *Interfaces* screen, click on the *create* button and enter the new VLAN ID and name you wish to use and then click the *save* button.

**Note:** This is creation of a Managed-side VLAN interface.

This step is considered optional as depending on the complexity of the site deployment, the administrator may simply decide associated the new Wireless LAN with the default *Management* interface and all wireless traffic will be forwarded onto this LAN. The network design of each site will dictate whether a new VLAN is required for separation of traffic.

Please refer to the BSC administration guide for detailed steps in creating managed-side VLAN interface.

**Create a Managed VLAN**

Complete this form to create one or more virtual LANs on the managed side of your network.

**Managed VLAN Settings**

Enable

Name

VLAN ID

Must be in the range of 2 to 4094.

VLAN type

802.1q

**Interface Settings**

Enable DHCP relay?  
For DHCP addresses on user connections

IP address

Use an address in the range 10.0.0.0 to 10.255.255.255 or 192.168.0.0 to 192.168.255.255 as these are not assigned addresses and are not routed by the Internet.

Netmask

255.255.255.0 [See networks...](#)

Run DHCP Server

NAT the addresses to the protected interface address

Enable multicast for this interface

Force proxy ARP for this interface

Strict MAC enforcement of fixed IP addresses

**Fixed IP address assignments**

MAC address	IP address	Host name	Role	Row Management...
			- Authenticate -	
			- Authenticate -	
			- Authenticate -	
			- Authenticate -	
			- Authenticate -	

**IP Range assignments**

Start IP address	End IP address	Role	Row Management...
		- Authenticate -	
		- Authenticate -	

**Default Role**

Role

- Authenticate -

**Display**

Custom User Login

Default

Click the *Save* button to save the changes.

---

## Step 2 - Create RADIUS Accounting Server

In order for the Bluesocket to successfully send accounting data associated with traffic being generated by the guest users, accounting server must be created on the controller. From the *User Authentication* → *Accounting Servers* → *Create* → *External RADIUS Accounting Server* menu option in the top right corner, please create a new accounting server.

Enter the IP Address of your Amigopod deployment in the *Server Address* field. This can be found on the console of the booted Amigopod software. There is no need to change the default *RADIUS Port Number* as this is the default port used by amigopod.

**bluesocket**

Status **User Authentication** User Roles Voice General Web Logins Wireless Network Mobility Matrix Maintenance

### Edit the RADIUS Accounting server

Back Reset Delete Save

Enable server

**Name**  
Amigopodblue118 Accounting  
Name to identify this server.

**Accounting server settings**

Server address: 192.168.160.5 See hosts... Port: 1813  
The IP address or DNS name of the RADIUS Accounting server.

Shared secret: ..... Confirm shared secret: .....

Timeout: 5  
Timeout in seconds for RADIUS Server Response. Value must be greater than 0.

**Interim Accounting Records**

Enable Interim Accounting Records

Update Interval: 300  
Update Interval in Minutes.

**Notes**

Back Reset Delete Save

**Edit the RADIUS Accounting server**

Complete this form to edit the RADIUS accounting server configuration.

Create a Remote authentication dial-in user service (RADIUS) accounting server to record network activity and statistics including tracking user logins.

**Configurations Using This Server**  
None

Enter and make note of the *Shared Secret* used for authenticating the controller to the Amigopod RADIUS server as this will be required during the configuration of the Amigopod software.

Click the *Save* button to save the changes.

---

### Step 3 - Create RADIUS Authentication Server

In order for the Bluesocket to successfully authenticate the guest users that will be provisioned on the Amigopod system, a RADIUS definition needs to be defined on the BlueSecure controller. From the User Authentication → *Authentication Servers* → *Create* → *External Radius Authentication* menu option in the top right corner, please create a new RADIUS authentication server.

Enter the IP Address of your Amigopod deployment in the *Server IP Address* field. This can be found on the console of the booted Amigopod software. There is no need to change the default *RADIUS Port Number* as this is the default port used by amigopod.

Enter and make note of the *NAS Identifier* and *Shared Secret* used for authenticating the controller to the Amigopod RADIUS server as this will be required during the configuration of the Amigopod software. Also, make sure that the *Enable Server* check box is selected so that this RADIUS definition can be used to authenticate the Visitor transiting through the BlueSecure Controller.

Please select the accounting server created in step 2 of this document.

Completing the Mapping RADIUS Attribute to roles or selection of Default role is required to complete this Bluesocket form.

Click the *Save* button to save the changes.



**Edit the RADIUS server**

Back Reset Delete Save

Enable server

**Name**

AmigopodRadius118

Name to identify this server

**Precedence**

1

The precedence this server has for verifying username/passwords.

**RADIUS server settings**

**Server address**

192.168.160.5 [See hosts...](#)

**Port**

1812

The IP address or DNS name of the RADIUS server. NOTE: IP Address only if used for VPN Authentication.

**Shared secret**

.....

**Confirm shared secret**

.....

**Timeout**

5

Timeout in seconds for RADIUS Server Response. Value must be greater than 0.

**NAS Identifier**

amigopodblue118

Name of the NAS Identifier attribute for RADIUS. Leave blank to use configured hostname.

**NAC integration**

Enable MAC Address Authentication

Enable BlueSocketRole Vendor Attribute

Allows a NAS server to override the user's role. Used for BVMS Guest Manager and 3rd party NAC integration.

**Accounting**

**Accounting server**

Amigopodblue118 Accounting

For accounting logging with authentication.

**Mapping RADIUS attributes to roles**

When a user successfully authenticates against the server the following rules are checked in numerical order. If a rule matches then the user is assigned the role, and no further rule is checked. If no rules match, the user is assigned the default role.

	if Attribute	logic	Value	then Role is	Row Management...
1					
2					
3					
4					
5					

**Default role**

AMIGOPOD

Status [User Authentication](#) [User Roles](#) [Voice](#) [General](#) [Web Logins](#) [Wireless](#) [Network](#) [Mobility Matrix](#) [Maintenance](#)

[Authentication Servers](#) [Internal 802.1x Authentication](#) [Local Users](#) [MAC Device Authentication](#) [Accounting Servers](#) [Administrative Users](#)

Servers | [Authentication Test](#)

Actions	Enabled	Name	Default role	Type	Address	Precedence	Accounting server
<input type="checkbox"/>	All		All	All			All
<input type="checkbox"/>	Yes	AmigopodRadius118	AMIGOPOD	RADIUS	192.168.160.5	1	

Check All | Clear All

1 row download

## Step 4 - Create Custom Web Login page

Although the default web login page on the BlueSecure controller can be used, this integration document will show steps required in creation of a new web login page.

From the *Web Logins* → *Login Screens* → *Create* → *Login Screen* menu option, create a new login form. Please fill in the name field and the default setting is perfectly acceptable for rest of the form. Please refer to the Bluesocket administration guide for details of completing this form. Please note that I have unchecked the Allow guest logins, as it is not needed and it presents a possible security hole.

**bluesocket**

Status User Authentication User Roles Voice General **Web Logins** Wireless Network Mobility Matrix Maintenance

Login Form | HTML Text | Redirection | Hotspot Account Generation

**Edit custom login - Amigopod Self Registration**

Back Reset Delete Save Next

**Name**  
Amigopod Self Registration

**Login options**

Allow user logins  
 Allow guest logins  
Guest Role  
Guest

Logout popup enabled  
 External server choice enabled  
 Password change choice enabled  
Password changes are only available for local users.  
 Language change choice enabled  
 Login help button enabled  
 Install CA button enabled  
Remove if you do not require a chain certificate.

Terms of Service URL

If entered, users will be required to click 'I accept' to the terms.

Terms of Service text

**Login access**

Login attempts

Number of minutes to wait after the maximum number of login attempts is made

Number of active sessions per username/authentication type. "0" is unlimited.

Applies to External Server Authentication methods only

**HTML Body**

Title

Background color  
 <P

Foreground color  
 <P

Link Visited link Active link  
 <P  <P  <P

**Logos**

Top left logo

Size recommended is 133x64 pixels

Powered-By logo

Enable complete customization of the login screen

**User Login Page - Form Customization**

Complete this form to customize the appearance of the login form on the left side of the User Login Page.

Click to open a window containing the User Login Page as it is currently defined.

**Configurations Using This Page**

Interface Managed

Click the **Save** button to save the changes.

From the *Web Logins* → *Login Screens* menu option, edit (click on the pencil) the newly created login form.

Status User Authentication User Roles Voice General **Web Logins** Wireless Network Mobility Matrix Maintenance

Login Screens File Uploads Languages SSL Certificate

Actions	Name	Title	Font Size	Language
<input type="checkbox"/>	<input type="text" value="Default"/>	<input type="text" value="Wireless Network Log In"/>	<input type="text" value="Small"/>	<input type="text" value="English"/>
<input type="checkbox"/>	<a href="#">Amigopod Self Registration</a>	Amigopod Self Registration	Small	English
<input type="checkbox"/>	<a href="#">Amigopod Registration</a>	Amigopod Registration	Small	English

Check All | Clear All |

Click on the *Redirection* menu option and please fill in the Base URL field and please refer to the Bluesocket administration guide for details of completing rest of this form.  
 Base URL: "https://192.168.160.5/weblogin.php/2". Please refer to Step 4 of this integration guide under Amigopod configuration for details of the Base URL.

**Note:** Use of "http://192.168.160.5/weblogin.php/2" is an option as Amigopod will accept both URLs. However, "https" is preferable for security reasons.

Status User Authentication User Roles Voice General **Web Logins** Wireless Network Mobility Matrix Maintenance

Login Form | HTML Text | **Redirection** | Hotspot Account Generation

**Edit redirection for custom login "Amigopod Registration"**

Redirect clients to an external URL?  
 Base URL:

**Redirection Parameter Keys**

Client's Original URL

Client's IP Address

Client's MAC Address

Client's Access Point MAC Address

Client's Access Point Name

Client's Access Point SSID

Controller IP Address

Client's Managed VLAN ID

**User Login Page - Redirection**

This feature allows you to redirect clients to an external server for authentication.

Complete this form to customize the redirection for this web login.

Please ensure that the external server is reachable from the managed network. The external server must notify this controller when login succeeds using an URL of the form: `https://BSC_IP/login.pl?which_form=reg&source=CLIENT_IP&bs_name=NAME&bs_password=PASSWORD`

Click the Save button to save the changes.

Following is a screenshot of an optional Self Registration setup.

This step is identical to the above steps in creating a web login page on the BlueSecure controller. The only difference is the Base URL.

Base UR: "Https://192.168.160.5/guest\_register\_1.php". Please refer to Step 4 of this integration guide under Amigopod configuration for details of the Base URL.

**Note:** Use of "Http://192.168.160.5/ guest\_register\_1.php" is an option as Amigopod will accept both URLs. However, "Https" is preferable for security reasons.

The screenshot shows the BlueSocket configuration interface. At the top, there is a navigation menu with the following items: Status, User Authentication, User Roles, Voice, General, Web Logins (highlighted), Wireless, Network, Mobility Matrix, and Maintenance. Below the menu, there are several tabs: Login Form, HTML Text, Redirection (selected), and Hotspot Account Generation. The main content area is titled "Edit redirection for custom login 'Amigopod Self Registration'". It contains a form with the following fields and options:

- Redirect clients to an external URL?
- Base URL:
- Redirection Parameter Keys**
- Client's Original URL:
- Client's IP Address:
- Client's MAC Address:
- Client's Access Point MAC Address:
- Client's Access Point Name:
- Client's Access Point SSID:
- Controller IP Address:
- Client's Managed VLAN ID:

At the bottom of the form are buttons for Back, Reset, Save, and Next. To the right of the form, there is a section titled "User Login Page - Redirection" with the following text:

This feature allows you to redirect clients to an external server for authentication.

Complete this form to customize the redirection for this web login.

Please ensure that the external server is reachable from the managed network. The external server must notify this controller when login succeeds using an URL of the form: `https://BSC_IP/login.pl?which_form=reg&source=CLIENT_IP&bs_name=NAME&bs_password=PASSWORD`

Click the Save button to save the changes.



## Step 5 - Selecting the Custom User Login for Managed Interface

Newly created Web Login screen must be selected under the Managed Interface.

This integration guide uses the physical Managed Interface as its interface for the guest subnet. If VLAN interface is used, then the proper VLAN interface must be selected for this step.

**Note:** If the Default login screen is used, then this step can be skipped.

**Note:** If VLAN Managed interface is in use (an optional step unique to each customer's environment), then this step must be for such VLAN Managed interface.

From the *Network* → *Managed* menu option, scroll down the bottom to the Display section of the form. Under Custom User Login pull down menu, select the newly created login form.

The screenshot displays the 'Edit Managed interface (eth1)' configuration page in the Bluesocket web interface. The page is divided into several sections:

- Enable DHCP relay?** (unchecked)
- IP address:** 192.168.170.1
- Netmask:** 255.255.255.0
- Run DHCP Server:** (checked)
- NAT the addresses to the protected interface address:** (checked)
- Enable multicast for this interface:** (unchecked)
- Force proxy ARP for this interface:** (unchecked)
- Strict MAC enforcement of IP addresses:** (checked)
- Deny admin functionality from this interface:** (unchecked)

**Fixed IP address assignments:**

MAC address	IP address	Host name	Role	Row Management...
			- Authenticate -	
			- Authenticate -	
			- Authenticate -	
			- Authenticate -	
			- Authenticate -	

**IP Range assignments:**

Start IP address	End IP address	Role	Row Management...
		- Authenticate -	
		- Authenticate -	

**Default Role:** Un-registered

**Ignore link down error on this interface:** (unchecked)

**Port settings:**

	1	2	3	4
Speed	Auto	Auto	Auto	Auto
Duplex	Auto	Auto	Auto	Auto
Power Over Ethernet	Disabled	Disabled	Disabled	Disabled

**Display:** Custom User Login

**Notes:**

**Current Status:**

Current Status	
MAC Address	00:19:92:02:B0:2A
Link	Up
IP Address	192.168.170.1
Netmask	255.255.255.0
Broadcast	192.168.170.255
Duplex	Full
Speed	1000 Mbps
PoE Status	Unpowered

Click the Save button to save the changes.

## Step 6 - Configure the Un-Registered Role

**NOTE:** Only follow this step if the initial step of redirection to the Amigopod's login screen is unreachable. Step 5 "Creation of Customer Login Screen" is supposed to dynamically open the un-registered role to the specified base URL. However, during creation and testing of this document, it was found that manual edit of the un-registered role was required.

From the *User Roles* → *Roles* tab the BlueSecure controller, edit the Un-registered role's policies to include Service type of HTTPS. Though many options are available, Action of "Allow", Service of "HTTPS", Direction of "Outgoing", Destination to "Amigopod" Schedule of "Any" & User Location of "Any" is recommended.

**Note:** Creation of "Amigopod" destination (Amigopod LAN interface's IP address) is a required step. Please refer to the Bluesocket Administration Guide for details in creating destination.

The screenshot shows the 'Edit role - Un-registered' configuration page. The top navigation bar includes 'Status', 'User Authentication', 'User Roles', 'Voice', 'General', 'Web Logging', 'Wireless', 'Network', 'Mobility Matrix', and 'Maintenance'. The main configuration area is titled 'Edit role - Un-registered' and contains the following sections:

- Un-registered** - this role is assigned to all connections when they first access the system.
- Bandwidth - Incoming Traffic (Protected->Managed)**
  - Bandwidth allocation: 0 Kbits/second, Total for role selected.
  - Priority: Medium selected, Override with per service setting? checked.
  - DSCP Value: Unchanged, Override with per service setting? checked.
- Bandwidth - Outgoing Traffic (Managed->Protected)**
  - Bandwidth allocation: 0 Kbits/second, Total for role selected.
  - Priority: Medium selected, Override with per service setting? checked.
  - DSCP Value: Unchanged, Override with per service setting? checked.
- Policies**

Network traffic is checked against the following policies. If the service, direction, and destination match, the action is taken and checking ends. If no policy matches the traffic is denied.

Policy	Action	Service	Direction	Destination	during Schedule	with User Location	Row Management...
1	Allow	DNS	Outgoing	Any	Any	Any	
2	Allow	HTTPS	Outgoing	Amigopod	Any	Any	
3							
4							
5							
6							
7							
8							
- VLAN Tag**: None
- BlueProtect Endpoint Scanning**: BlueProtect Scanning Interval: Disabled
- Notes**: Empty text area.

Buttons for 'Back', 'Reset', 'Delete', and 'Save' are located at the top right and bottom right of the configuration area.

Click the Save button to save the changes.

# Amigopod Configuration

## Step1 - Create RADIUS NAS for Bluesocket

In order for the Bluesocket to authenticate users it needs to be able to communicate with the Amigopod RADIUS instance. Back in Step 2 of the Bluesocket configuration, a RADIUS server definition was defined. This step configures the Amigopod NAS definition for the Bluesocket. The RADIUS key used in Step 2 needs to be configured exactly the same here for the RADIUS transactions to be successful.

From the *RADIUS Services* → *Network Access Servers* screen click on the *Create* button to add a new NAS device. Enter the IP Address of the Bluesocket, select the *NAS Type* as *Bluesocket* and enter the key from Step 2 in the *Shared Secret* field.

The screenshot shows the Amigopod web interface for configuring RADIUS Network Access Servers. On the left is a navigation menu with categories like Home, Guest Manager, Hotspot Manager, Reporting Manager, Administrator, and RADIUS Services. The main content area is titled 'radius network access servers' and includes a 'Create' button. Below this is a 'Create Network Access Server' form with the following fields:

- Name:** amigopodblue118
- IP Address:** 192.168.160.118
- NAS Type:** Bluesocket
- Shared Secret:** [Redacted]
- Confirm Shared Secret:** [Redacted]
- Description:** [Empty text area]

Buttons at the bottom of the form are 'Create NAS Device', 'Reset Form', and 'Cancel'. Below the form is a table of existing NAS devices:

Name	Hostname	Type	Comments
amigopodblue118	192.168.160.118	bluesocket	

Below the table, it shows '1 network access server' and a 'Reload' button. The page footer includes 'RADIUS Services'.

Click the *Create NAS* button to commit the change to the RADIUS database.

## Step 2 - Restart RADIUS Services

A restart of the RADIUS Service is required for the new NAS configuration to take affect.

Click the *Restart RADIUS Server* button shown below and wait a few moments for the process to complete.

**radius server control**

- Home
  - Start Here
  - Language
  - Time Zone
- Guest Manager
  - Start Here
  - Create Account
  - Create Multiple
  - List Accounts
  - Edit Accounts
  - Active Sessions
  - Import Accounts
  - Export Accounts
  - Print Templates
  - Customization
- Hotspot Manager
  - Start Here
  - Self Provisioning
  - Self Service
  - Manage Hotspot
  - Manage Plans
  - Manage Customer Info
  - Manage Invoice
  - Manage User Interface
- Reporting Manager
  - Start Here
  - List Reports
- Administrator
  - Start Here
  - Backup & Restore
  - Content Manager
  - Network Setup
  - Operator Logins
  - OS Updates
  - Plugin Manager
  - Server Time
  - System Control
  - System Information
- RADIUS Services**
  - Start Here
  - Server Control**
  - Server Configuration
  - Database List
  - Dictionary
  - NAS List
  - User Roles
  - Web Logins
- SMS Services

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.

### RADIUS Server Time

The RADIUS server time is currently: **Wednesday, July 08, 2009 7:23:32 PM -0400**

### RADIUS Log Snapshot

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

```
Wed Jul 8 19:23:19 2009 : Info: Ready to process requests.
Wed Jul 8 19:23:19 2009 : Info: rlm_sql (sql): Attempting to connect to amigopod@localhost:5432/amigopod
Wed Jul 8 19:23:19 2009 : Info: rlm_sql (sql): Driver rlm_sql_postgresql (module rlm_sql_postgresql) loaded and linked
Wed Jul 8 19:23:19 2009 : Info: rlm_exec: Wait=yes but no output defined. Did you mean output=none?
Wed Jul 8 19:23:19 2009 : Info: Using deprecated naslist file. Support for this will go away soon.
Wed Jul 8 19:21:07 2009 : Info: Ready to process requests.
Wed Jul 8 19:21:07 2009 : Info: rlm_sql (sql): Attempting to connect to amigopod@localhost:5432/amigopod
Wed Jul 8 19:21:07 2009 : Info: rlm_sql (sql): Driver rlm_sql_postgresql (module rlm_sql_postgresql) loaded and linked
Wed Jul 8 19:21:07 2009 : Info: rlm_exec: Wait=yes but no output defined. Did you mean output=none?
Wed Jul 8 19:21:07 2009 : Info: Using deprecated naslist file. Support for this will go away soon.
Wed Jul 8 18:59:46 2009 : Auth: Login OK: [skim] (from client amigopodblue118 port 0 cli 00:12:3f:fa:e2:5f)
Wed Jul 8 18:55:19 2009 : Auth: Login OK: [skim] (from client amigopodblue118 port 0 cli 00:12:3f:fa:e2:5f)
Wed Jul 8 18:52:57 2009 : Auth: Login incorrect: [mike] (from client amigopodblue118 port 0 cli 00:12:3f:fa:e2:5f)
Wed Jul 8 18:50:25 2009 : Auth: Login OK: [skim] (from client amigopodblue118 port 0 cli 00:12:3f:fa:e2:5f)
Wed Jul 8 18:49:32 2009 : Auth: Login OK: [skim] (from client amigopodblue118 port 0 cli 00:12:3f:fa:e2:5f)
Wed Jul 8 18:46:10 2009 : Auth: Login OK: [skim] (from client amigopodblue118 port 0 cli 00:12:3f:fa:e2:5f)
Wed Jul 8 18:43:38 2009 : Auth: Login OK: [skim] (from client amigopodblue118 port 0 cli 00:12:3f:fa:e2:5f)
Wed Jul 8 18:16:34 2009 : Info: Ready to process requests.
Wed Jul 8 18:16:34 2009 : Info: rlm_sql (sql): Attempting to connect to amigopod@localhost:5432/amigopod
Wed Jul 8 18:16:34 2009 : Info: rlm_sql (sql): Driver rlm_sql_postgresql (module rlm_sql_postgresql) loaded and linked
```



## Step 3 - Configure Bluesocket Web Logins Page on Amigopod

By default the Amigopod comes pre-configured with Web Login templates (*RADIUS Services*→*Web Logins*) for all the major wireless manufactures. The Bluesocket template can be modified to suit the local deployment by adding custom HTML code or defined a unique Amigopod skin for each captive portal page hosted by the Amigopod install as shown below:

From the *RADIUS Services*→*Web Logins* page select the *Bluesocket Login* entry and Click the *Edit* button.

**radius web logins**

Many NAS devices support Web-based authentication for visitors.

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.

Name	Page Title	Page Skin
<b>Aruba Networks Login</b> Login page for Aruba 200/800/2400/6000 Mobility Controllers.	amigopod Login	(Default)
<b>Bluesocket Login</b> Login page for Bluesocket 600/1200 /2100/5200/7200 BlueSecure Controllers.	Guest Login	(Default)
<a href="#">Edit</a> <a href="#">Duplicate</a> <a href="#">Delete</a> <a href="#">Test</a>		
<b>ChilliSpot Login</b> Login page suitable for use with the ChilliSpot captive portal.	amigopod Login	(Default)
<b>Cisco 4400 Login</b> Login page for Cisco 4400 Series Wireless LAN Controllers.	amigopod Login	(Default)
<b>Trendnet Login</b> Login page for Trendnet TEW-453APB Hotspot Access Points.	amigopod Login	(Default)

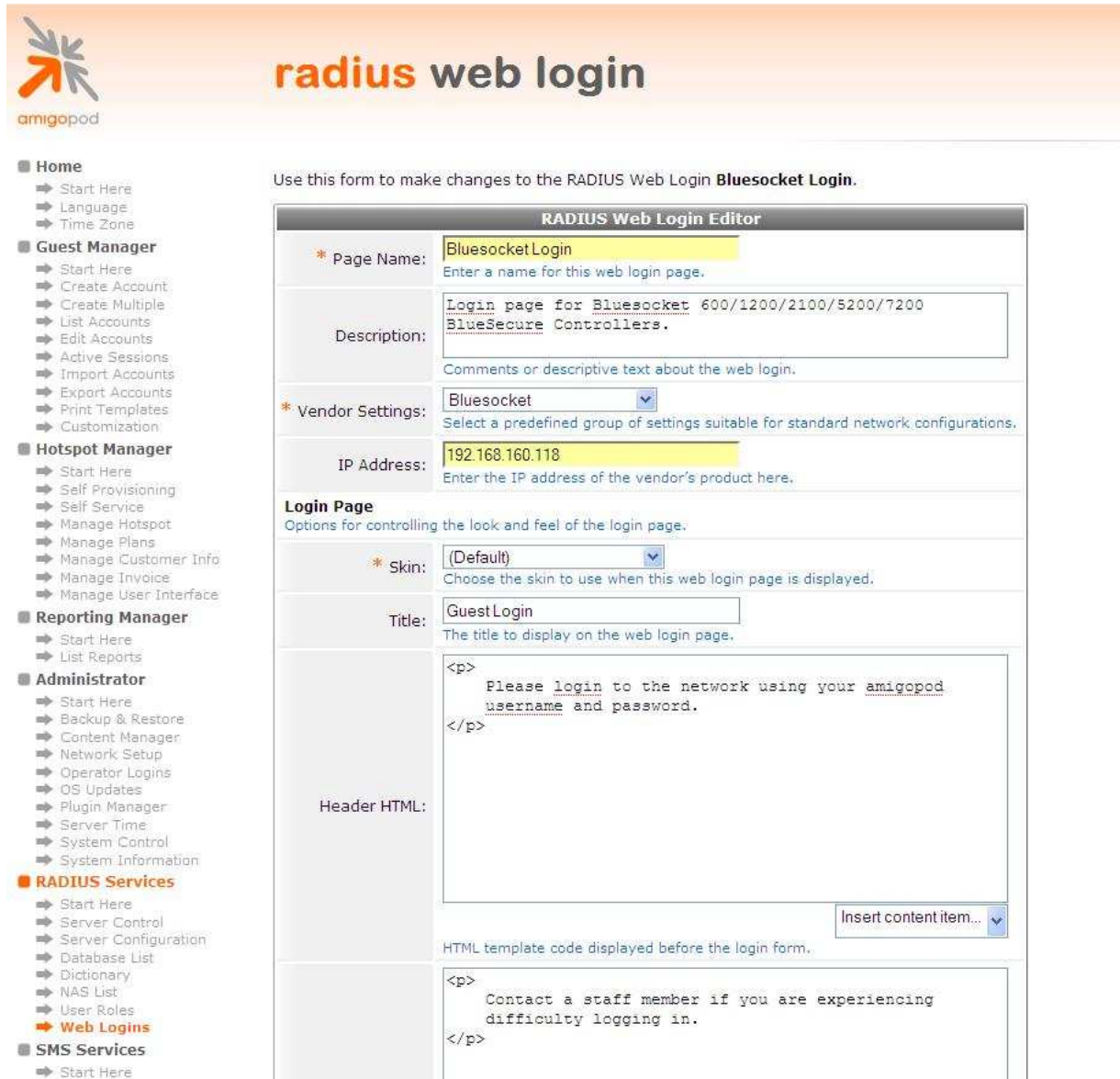
5 web logins [Reload](#)

[Create a new web login page](#)

[RADIUS Services](#)

[Back to main](#)

From the *RADIUS Web Login* page select the *Skin* that you would like presented as the branding for the Captive Portal page.



Use this form to make changes to the RADIUS Web Login **Bluesocket Login**.

**RADIUS Web Login Editor**

\* Page Name:   
Enter a name for this web login page.

Description:   
Comments or descriptive text about the web login.

\* Vendor Settings:   
Select a predefined group of settings suitable for standard network configurations.

IP Address:   
Enter the IP address of the vendor's product here.

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

\* 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:   
HTML template code displayed before the login form.

Footer HTML:   
HTML template code displayed after the login form.

Modify the sample HTML in the *Header HTML*, *Footer HTML* and *Login Message* section to customize for your local environment. Click the *Save Changes* button to commit the changes.

## Step 4 - Confirm External Captive Portal URL

The URL that needs to be configured in the Bluesocket External Captive Portal section covered in Step 4 of Bluesocket configuration can be confirmed by clicking on the test button shown on the screen below under the *RADIUS Services* → *Web Logins* screen:

The screenshot shows the 'radius web logins' configuration page in the amigopod interface. The page title is 'radius web logins'. Below the title, there is a navigation menu on the left and a main content area. The main content area contains a table of web login pages and a 'Test' button for the 'Bluesocket Login' entry.

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

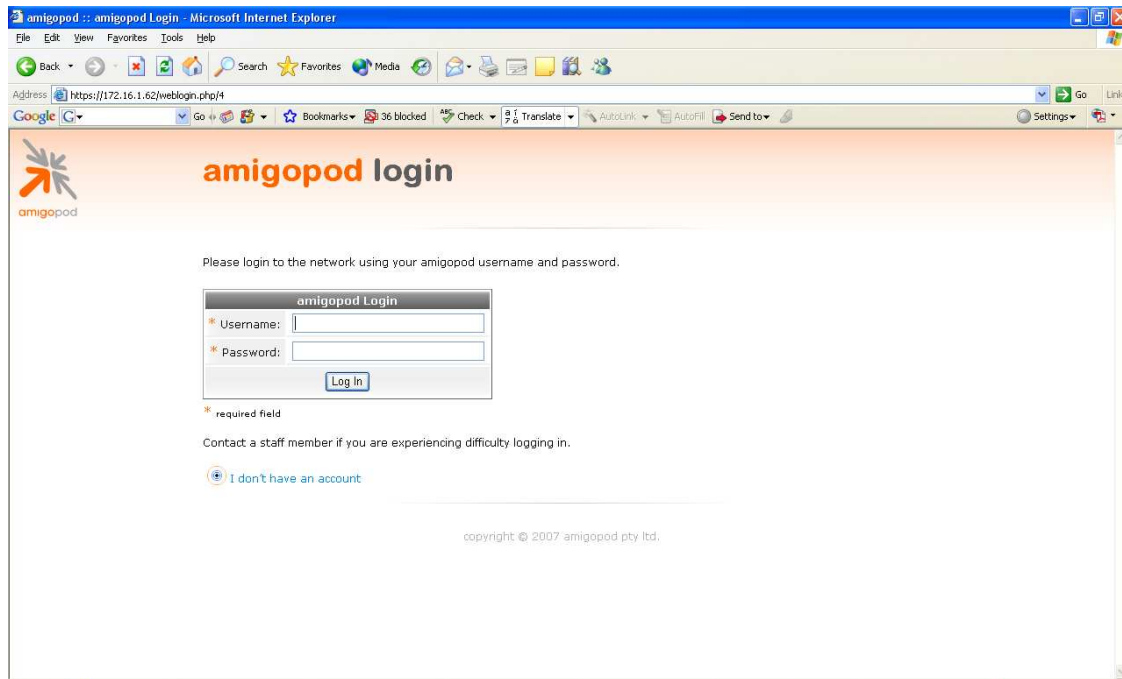
Name	Page Title	Page Skin
<b>Aruba Networks Login</b> Login page for Aruba 200/800/2400/6000 Mobility Controllers.	amigopod Login	(Default)
<b>Bluesocket Login</b> Login page for Bluesocket 600/1200 /2100/5200/7200 BlueSecure Controllers.	Guest Login	(Default)
<b>ChilliSpot Login</b> Login page suitable for use with the ChilliSpot captive portal.	amigopod Login	(Default)
<b>Cisco 4400 Login</b> Login page for Cisco 4400 Series Wireless LAN Controllers.	amigopod Login	(Default)
<b>Trendnet Login</b> Login page for Trendnet TEW-453APB Hotspot Access Points.	amigopod Login	(Default)

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

[Create a new web login page](#)  
[RADIUS Services](#)  
[Back to main](#)

**Click on the Test button**

A Test page will be presented and the URL can be copied from the address bar:



**Note:** Make note of the URL presented in the web browser after the *Test* button has been clicked. This URL will be required in the configuration of the captive portal settings on the Bluesocket, Step 4 of Bluesocket configuration. An example of the URL is shown below:

<http://192.168.160.5/weblogin.php/2>

<https://192.168.160.5/weblogin.php/2>

Please note that "Https" is recommended for security reasons.

Guest Self-Registration is also an option. Following are steps in setting up the Amigopod for Guest Self-Registration.

Under the *Guest Manager* → *Customization* → *Guest Self Registration* screen, open the built-in Guest Self-Registration option and select the Duplicate.

Use this list view to manage the pages used for guest self-registration.


Name	Register Page	Skin
<b>Bluesocket Self-Registration</b> Default settings for visitor self-registration.	guest_register_1	amigopod Skin
<b>Guest Self-Registration</b> Default settings for visitor self-registration.	guest_register	Aerohive Networks Skin

2 items [Reload](#) 10 rows per page

[Create new self-registration page](#)  
[Back to customization](#)  
[GuestManager services](#)  
[Back to main](#)

**Click to Edit**

Click the Edit under the newly created Guest Self-Registration to edit.



## customize guest registration

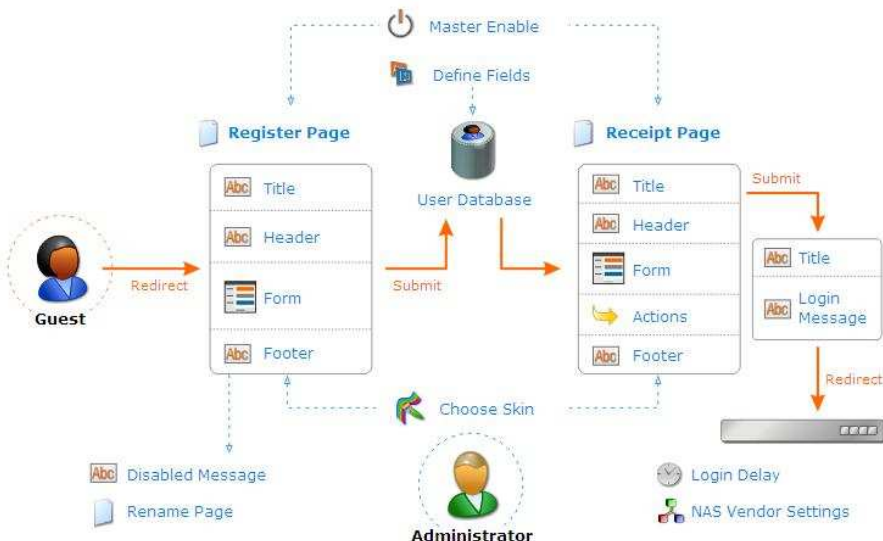
---

- **Home**
  - ➔ Start Here
  - ➔ Language
  - ➔ Time Zone
- **Guest Manager**
  - ➔ Start Here
  - ➔ Create Account
  - ➔ Create Multiple
  - ➔ List Accounts
  - ➔ Edit Accounts
  - ➔ Active Sessions
  - ➔ Import Accounts
  - ➔ Export Accounts
  - ➔ Print Templates
  - ➔ **Customization**
    - ➔ Customize Fields
    - ➔ Customize Forms & Views
    - ➔ **Guest Self-Registration**
- **Hotspot Manager**
  - ➔ Start Here
  - ➔ Self Provisioning
  - ➔ Self Service
  - ➔ Manage Hotspot
  - ➔ Manage Plans
  - ➔ Manage Customer Info
  - ➔ Manage Invoice
  - ➔ Manage User Interface
- **Reporting Manager**
  - ➔ Start Here
  - ➔ List Reports
- **Administrator**
  - ➔ Start Here
  - ➔ Backup & Restore
  - ➔ Content Manager
  - ➔ Network Setup
  - ➔ Operator Logins
  - ➔ OS Updates
  - ➔ Plugin Manager
  - ➔ Server Time
  - ➔ System Control
  - ➔ System Information
- **RADIUS Services**
  - ➔ Start Here
  - ➔ Server Control
  - ➔ Server Configuration
  - ➔ Database List
  - ➔ Dictionary

The process for guest self-registration is shown below. Click an item to edit.

### Guest Self-Registration 'Self-Registration'

Launch this guest registration page



[Advanced editor](#)  
[Back to guest self-registration](#)  
[Back to customization](#)  
[GuestManager services](#)  
[Back to main](#)



Click on the Master Enable and check the Enable guest self-registration option.

■ Home

- ➔ Start Here
- ➔ Language
- ➔ Time Zone

■ Guest Manager

- ➔ Start Here
- ➔ Create Account
- ➔ Create Multiple
- ➔ List Accounts
- ➔ Edit Accounts
- ➔ Active Sessions
- ➔ Import Accounts
- ➔ Export Accounts
- ➔ Print Templates
- ➔ Customization
  - ➔ Customize Fields
  - ➔ Customize Forms & Views
- ➔ Guest Self-Registration

■ Hotspot Manager

- ➔ Start Here
- ➔ Self Provisioning
- ➔ Self Service
- ➔ Manage Hotspot
- ➔ Manage Plans
- ➔ Manage Customer Info
- ➔ Manage Invoice
- ➔ Manage User Interface

■ Reporting Manager

- ➔ Start Here
- ➔ List Reports

■ Administrator

- ➔ Start Here
- ➔ Backup & Restore
- ➔ Content Manager
- ➔ Network Setup
- ➔ Operator Logins

Use this form to make changes to the guest self-registration instance **Bluesocket Self-Registration**.

[← Back to guest self-registration editor](#)

### Customize Guest Registration

#### Basic Properties

Options controlling basic operation of guest self-registration.

\* Name:   
Enter a name to identify the guest self-registration instance. This is visible only to administrators.

Description:   
Enter comments about this instance of guest self-registration. This is visible only to administrators.

Enabled:  Enable guest self-registration

\* Register Page:   
Enter the base page name for the guest registration page.

\* User Database: Local RADIUS Server  
Self provisioned visitor accounts are created using this service handler.

\* Skin:   
Choose the skin for the self-registration pages.

\* required field

[Back to guest self-registration](#)

[Back to customization](#)

[GuestManager services](#)

**Note:** When using the duplicate feature, the name of the newly create login will be “Copy of XXX”. It is preferable (not required) to rename the field to meet your naming convention.

Click *Save Changes* to save configuration.

Click on the NAS Vendor Settings and check the Enable automatic guest login to a Network Access Server. Then, Select Bluesocket under Vendor Settings pull down menu and type in the IP address of the BlueSecure controller.

**customize guest registration**

amigopod

- Home
  - Start Here
  - Language
  - Time Zone
- Guest Manager
  - Start Here
  - Create Account
  - Create Multiple
  - List Accounts
  - Edit Accounts
  - Active Sessions
  - Import Accounts
  - Export Accounts
  - Print Templates
- Customization
  - Customize Fields
  - Customize Forms & Views
- Guest Self-Registration
- Hotspot Manager
  - Start Here
  - Self Provisioning
  - Self Service
  - Manage Hotspot
  - Manage Plans
  - Manage Customer Info
  - Manage Invoice
  - Manage User Interface

Use this form to make changes to the guest self-registration instance **Bluesocket Self-Registration**.

[Back to guest self-registration editor](#)

### Customize Guest Registration

#### NAS Login

Options controlling automatic login to NAS for self-registered guests.

Enabled:  Enable automatic guest login to a Network Access Server

\* Vendor Settings: Bluesocket  
Select a predefined group of settings suitable for standard network configurations.

IP Address: 192.168.160.118  
Enter the IP address of the vendor's product here.

[Save Changes](#)

\* required field

[Back to guest self-registration](#)

[Back to customization](#)

[GuestManager services](#)

[Back to main](#)

Click *Save Changes* to save configuration.



The URL that needs to be configured in the Bluesocket External Captive Portal section covered in Step 4 of Bluesocket configuration can be confirmed by clicking on the Launch this guest registration page from the main Customize Guest Self-Registration page.

**customize guest registration**

amigopod

- Home
  - Start Here
  - Language
  - Time Zone
- Guest Manager
  - Start Here
  - Create Account
  - Create Multiple
  - List Accounts
  - Edit Accounts
  - Active Sessions
  - Import Accounts
  - Export Accounts
  - Print Templates
  - Customization
    - Customize Fields
    - Customize Forms & Views
  - Guest Self-Registration
- Hotspot Manager
  - Start Here
  - Self Provisioning
  - Self Service
  - Manage Hotspot
  - Manage Plans
  - Manage Customer Info
  - Manage Invoice
  - Manage User Interface
- Reporting Manager
  - Start Here
  - List Reports
- Administrator
  - Start Here
  - Backup & Restore
  - Content Manager
  - Network Setup
  - Operator Logins
  - OS Updates
  - Plugin Manager
  - Server Time
  - System Control
  - System Information
- RADIUS Services
  - Start Here
  - Server Control
  - Server Configuration
  - Database List
  - Dictionary

The process for guest self-registration is shown below. Click an item to edit.

**Guest Self-Registration 'Self-Registration'**

Launch this guest registration page

Master Enable

Define Fields

Register Page

Receipt Page

User Database

Guest

Administrator

Choose Skin

Disabled Message

Rename Page

Advanced editor

Back to guest self-registration

Back to customization

GuestManager services

Back to main

Submit

Submit

Redirect

Redirect

Login Delay

NAS Vendor Settings

Click on this link to open the self-registration page

A Test page will be presented and the URL can be copied from the address bar:



**Note:** Make note of the URL presented in the web browser after the *Test* button has been clicked. This URL will be required in the configuration of the captive portal settings on the Bluesocket, Step 4 of Bluesocket configuration. An example of the URL is shown below:

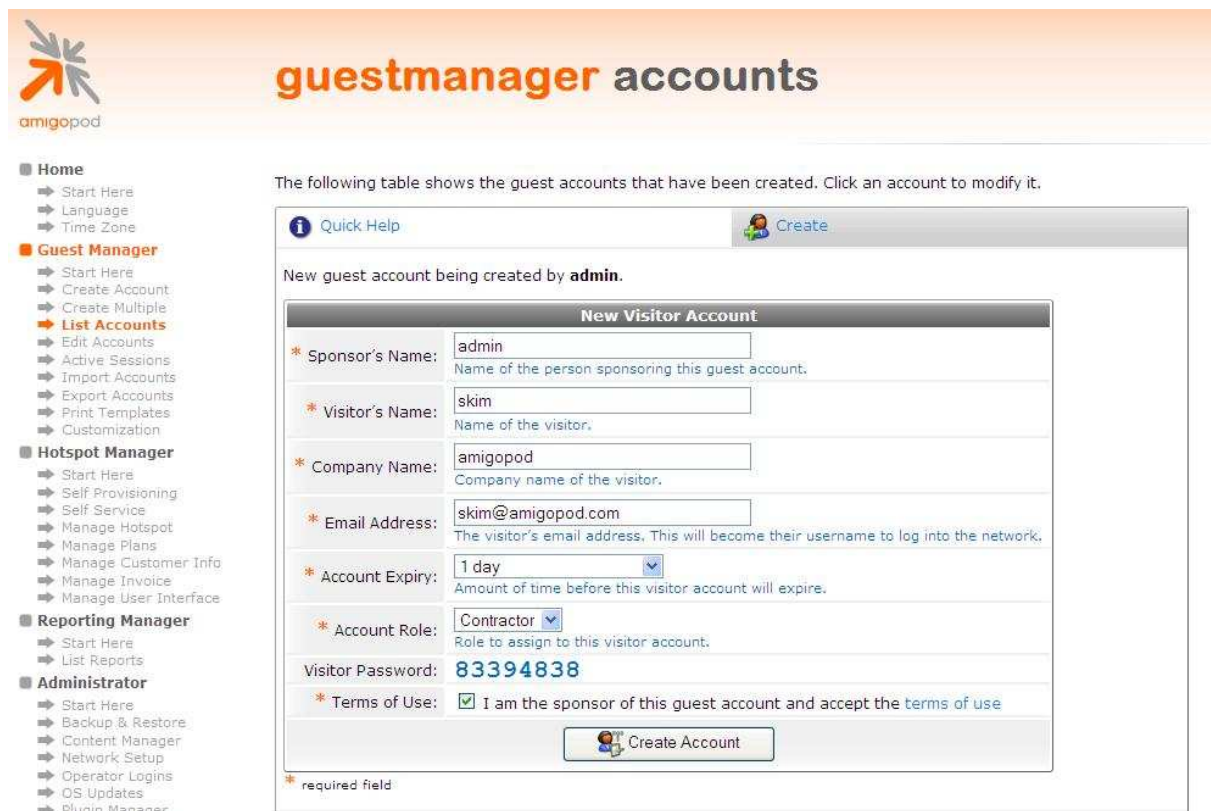
[http://192.168.160.5/guest\\_register\\_1.php](http://192.168.160.5/guest_register_1.php)

[https://192.168.160.5/guest\\_register\\_1.php](https://192.168.160.5/guest_register_1.php)

Please note that “Https” is recommended for security reasons.

## Step 5 - Create a User account

Within the Amigopod RADIUS Server a test user account can be created using the Amigopod *Guest Manager*. From the *Guest Manager* menu, select the *Create New Guest Account* option. Enter the test user details as detailed on the form below and click the *Create Account* button to save the new test user account.



The screenshot displays the Amigopod Guest Manager interface. On the left is a navigation menu with categories: Home, Guest Manager, Hotspot Manager, Reporting Manager, and Administrator. The main content area shows a 'New Visitor Account' form with the following fields:

- Sponsor's Name:** admin
- Visitor's Name:** skim
- Company Name:** amigopod
- Email Address:** skim@amigopod.com
- Account Expiry:** 1 day
- Account Role:** Contractor
- Visitor Password:** 83394838
- Terms of Use:**  I am the sponsor of this guest account and accept the terms of use

A 'Create Account' button is located at the bottom of the form. A note above the form states: 'The following table shows the guest accounts that have been created. Click an account to modify it.'

**Note:** Make note of the randomly generated *Visitor Password* as this will be required during the integration testing. If this password is proving difficult to remember during testing you can use the *List guest accounts* option on the screen to then edit the account and change the password to a more user friendly string.

---

## Testing the Configuration

Now that the configuration of both the Bluesocket and the Amigopod solution is complete, the following steps can be followed to verify the setup.

### Step 1 - Test the RADIUS Authentication Server on the BlueSecure

Using the Authentication Test feature, BlueSecure controller can test the validity of the RADIUS Server configuration and connectivity.

From the User Authentication → *Authentication Servers* → *Authentication Test* menu option, please test the newly created RADIUS authentication server.

Enter the User name and Password of a user account on the Amigopod's RADIUS DB to tests. Please select the proper external server (RADIUS Server created in Step 2) to test.

The screenshot shows the Bluesocket web interface. At the top, there is a navigation menu with options: Status, User Authentication, User Roles, Voice, General, Web Logins, Wireless, Network, Mobility Matrix, and Maintenance. Below this, a sub-menu is open for 'User Authentication', showing options: Authentication Servers, Internal 802.1x Authentication, Local Users, MAC Device Authentication, Accounting Servers, and Administrative Users. The 'Authentication Servers' option is selected, and a sub-menu is open for 'Servers', showing 'Authentication Test' as the active page.

Below the navigation, there is a section titled 'Successful authentication' with the text: 'skim would be assigned the 'AMIGOPOD' role.'

The main content area is titled 'External Authentication Test'. It contains a form with the following fields:

- User name: skim
- Password: [masked]
- External server: AmigopodRadius118 (dropdown menu)
- User location: Your VLAN (dropdown menu)

There are two 'Submit' buttons: one at the top right of the form and one at the bottom right. To the right of the form, there is a text box that says: 'Use this form to test external servers. Enter the user name, password and select the external server and then press the "Submit" button.'

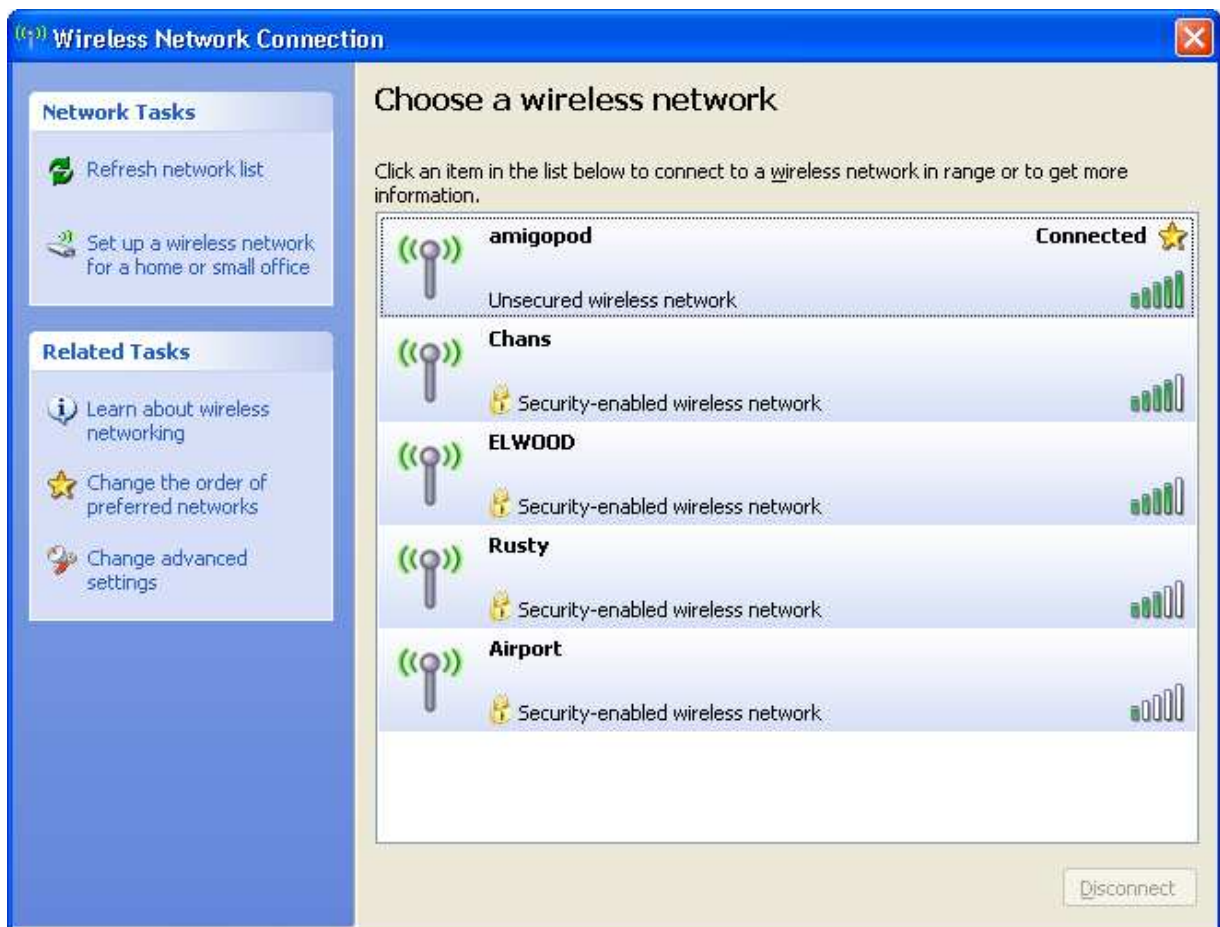
Below the text box, there is a section titled 'Attributes and values:' with the following text:

```
'Reply-Message' => 'Employee',  
'User-Name' => 'skim'
```

Click the *Submit* button to test the authentication server configuration.

## Step 2 - Connect to the Amigopod wired or wireless network

Using a test laptop, connect to the wired or wireless network. The screen capture below is an example that shows the interface used on a Windows XP SP2 based laptop. Although the process differs from laptop to laptop depending on the wired and wireless card drivers installed and different operating systems in use, the basic premise of connecting to the unsecured Guest network should be fundamentally the same. Refer to your laptop manufacturer's documentation on the procedure for connecting to wireless networks if you experience basic connectivity.

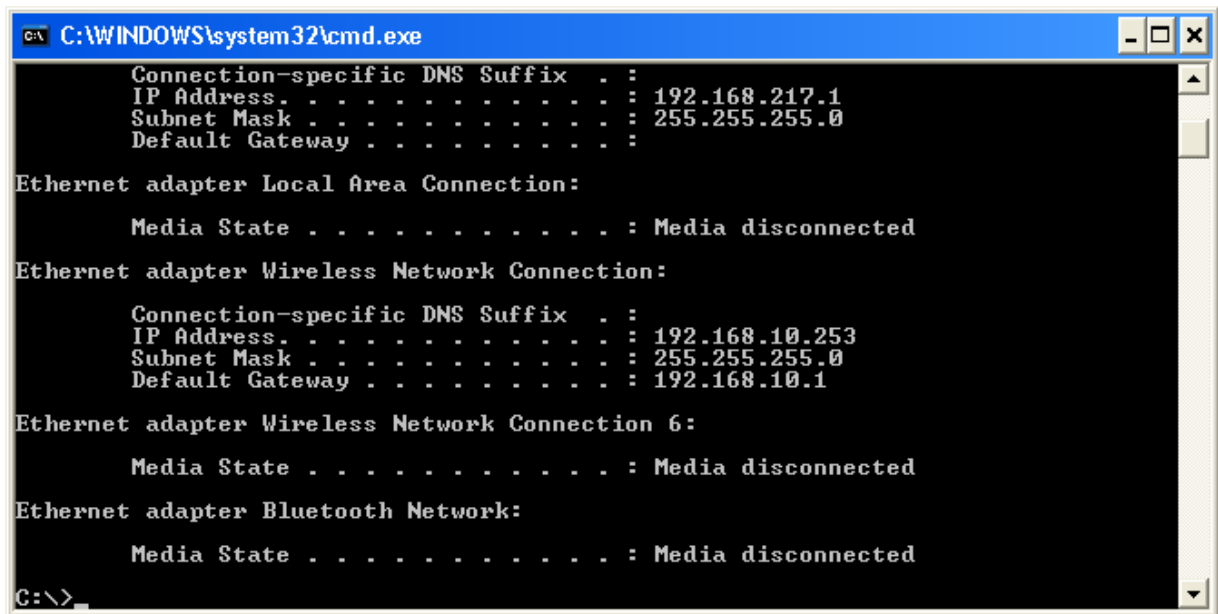


---

### Step 3 - Confirm DHCP IP Address received

Using the Windows Command Prompt or equivalent in the chosen operating system, confirm that a valid IP Address has been received from the DHCP server defined on the Bluesocket.

Issue the *ipconfig* command from the Windows Command Prompt to display the IP information received from the DHCP process. As seen from example below, the Wireless adaptor an IP Address of *192.168.10.253* has been received.

A screenshot of a Windows Command Prompt window titled "C:\WINDOWS\system32\cmd.exe". The window displays the output of the `ipconfig` command. The output shows network configuration for several adapters. The first section shows a connection with IP address 192.168.217.1. The second section, "Ethernet adapter Local Area Connection:", shows "Media State : Media disconnected". The third section, "Ethernet adapter Wireless Network Connection:", shows IP address 192.168.10.253. The fourth section, "Ethernet adapter Wireless Network Connection 6:", shows "Media State : Media disconnected". The fifth section, "Ethernet adapter Bluetooth Network:", shows "Media State : Media disconnected". The prompt "C:\>" is visible at the bottom left.

```
C:\WINDOWS\system32\cmd.exe
Connection-specific DNS Suffix . :
IP Address. . . . . : 192.168.217.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

Ethernet adapter Local Area Connection:

    Media State . . . . . : Media disconnected

Ethernet adapter Wireless Network Connection:

    Connection-specific DNS Suffix . :
    IP Address. . . . . : 192.168.10.253
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.1

Ethernet adapter Wireless Network Connection 6:

    Media State . . . . . : Media disconnected

Ethernet adapter Bluetooth Network:

    Media State . . . . . : Media disconnected

C:\>
```

**Note:** On Mac OS X and Linux operating system variants use a Terminal window and enter the *ifconfig* command to display the same information.

Following is a screenshot of the Bluesocket controller's Active Connections list after the client connects and receives an IP address.

bluesocket 

Status User Authentication User Roles Voice General Web Logins Wireless Network Mobility Matrix Maintenance

Active Connections Logs Summary Reports Diagnostics Monitor

All Connections | [IDS](#) | [APs](#) | [RFIDS](#) | [Contained Devices](#)

This page will refresh in 56 seconds.

Actions	Name	Address	MAC Address	Role	Authentication	Current/Average Kbps
<input type="checkbox"/>				All		
<input type="checkbox"/>		192.168.170.254	00:12:3f:fa:e2:5f	Un-registered		0/0

Check All | Clear All | Override Role... | Apply | Logout

1 row [download](#)

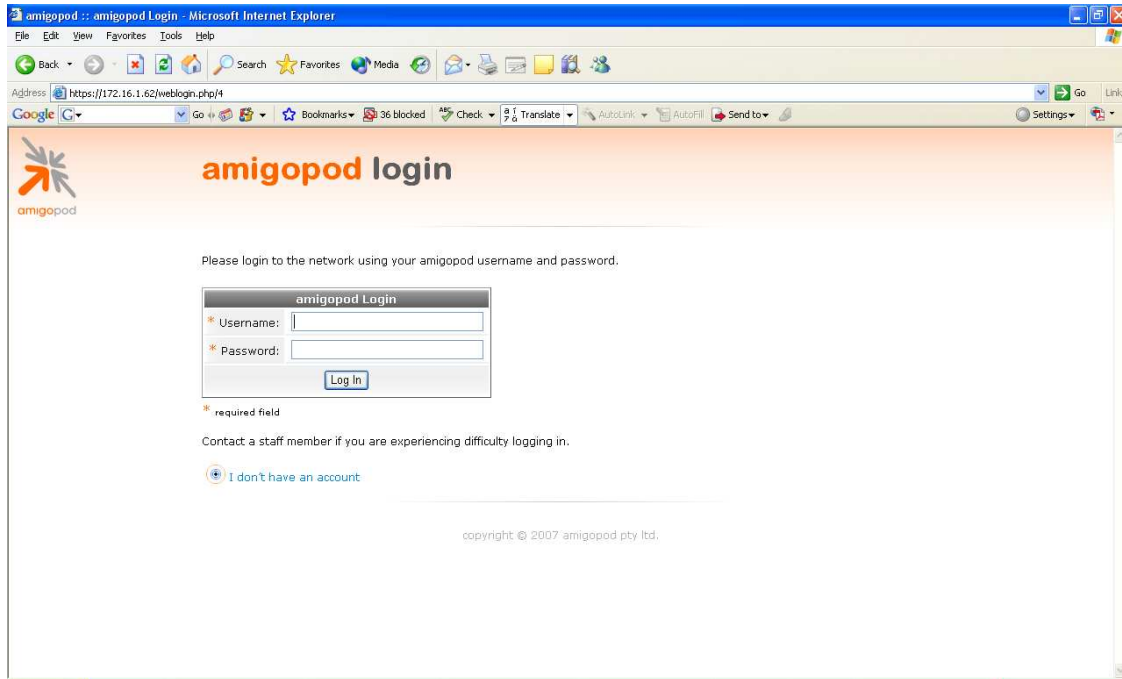
font size ●●



---

## Step 4 - Launch Web Browser and login

When the web browser on the test laptop is launched the Bluesocket will automatically capture the session and redirect the user to the Amigopod hosted login page as shown below:



Enter the test user details entered and recorded in Step 5 of the Amigopod configuration procedure and click the *Login* button.


At this point the test user should be successfully authenticated and allowed to transit through the controller and onto the Internet or Corporate network.

**Note:** If the web browser fails to redirect check that the DNS server configured in the DHCP Server defined in the Bluesocket is available and successfully resolving domain names. Without name resolution working the web browser will never attempt to connect to the website defined in web browser home page and therefore there is no session for the Bluesocket to redirect. Other situations that can cause issues with the captive portal include but are not limited to:

- Web browser home page set to intranet site not available in current DNS
- Proxy Server configuration in browser using non standard HTTP ports



Following is a screenshot of the Bluesocket controller's Active Connections list after the client has successfully completed the login process.

bluesocket 

Status | User Authentication | User Roles | Voice | General | Web Logins | Wireless | Network | Mobility Matrix | Maintenance

Active Connections | Logs | Summary | Reports | Diagnostics | Monitor

All Connections | [IDS](#) | [APs](#) | [RF IDS](#) | [Contained Devices](#)

This page will refresh in 56 seconds.

Actions	Name	Address	MAC Address	Role	Authentication	Current/ Average Kbps
<input type="checkbox"/>	<input type="text" value="skim"/>	192.168.170.254	00:12:3f:fa:e2:5f	All	AmigopodRadius118	1.45/0.86

[Check All](#) | [Clear All](#) | [Override Role...](#) | [Apply](#) | [Logout](#)

1 row [download](#)

font size 

---

## Step 5 - Confirm RADIUS debug messages on amigopod

Once the test laptop has successfully authenticated and now able to browse the Internet, an entry should appear in the RADIUS logs confirming the positive authentication of the test user – in this example, [test@acme.com](mailto:test@acme.com).

Select the *RADIUS Services* → *Server Control* menu option and the following screen should be displayed showing the status of the RADIUS server and a tail of the log file, including an entry for the positive authentication transaction.

