amigopod

Xirrus Array Integration Guide

Revision	0.90
Date	23 April 2010
	Copyright © 2009 amigopod Pty Ltd
amigopod Headquarters	amigopod Pty Ltd Suite 101 349 Pacific Hwy North Sydney, NSW 2060 Australia
	ABN 74 124 753 421
Web	www.amigopod.com
Phone	+61 2 8669 1140
Fax	+61 7 3009 0329

Table of Contents

Introduction 3
Test Environment 3
Integration 5
Xirrus Array Configuration 6
Step 1 – Create RADIUS Authentication Server Instance 7
Step 2 – Create an SSID and Configure/Enable Web Page Redirect 8
Step 3 – RADIUS Configuration 9
Amigopod Configuration 10
Step1 – Create RADIUS NAS for Xirrus Array 11
Step 2 – Restart RADIUS Services 12
Step 3 – Configure Xirrus Array Web Logins Page 13
Step 3 – Confirm External Captive Portal URL 15
Step 3 – Create a test user account 16
Testing the Configuration 17
Step 1 - Connect to the amigopod wireless network 17
Step 2 – Confirm DHCP IP Address received 18
Step 3 – Launch Web Browser and login 19
Step 4 – Confirm RADIUS debug messages on amigopod 20

Introduction

This document outlines the configuration process on both the Xirrus Array and the amigopod appliance to create a fully integrated Visitor Management solution. The solution leverages the captive portal functionality built into the Xirrus Array 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 Xirrus Array 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 the Xirrus Array. Testing procedure is valid for all hardware variants from Xirrus in its Array family of products.

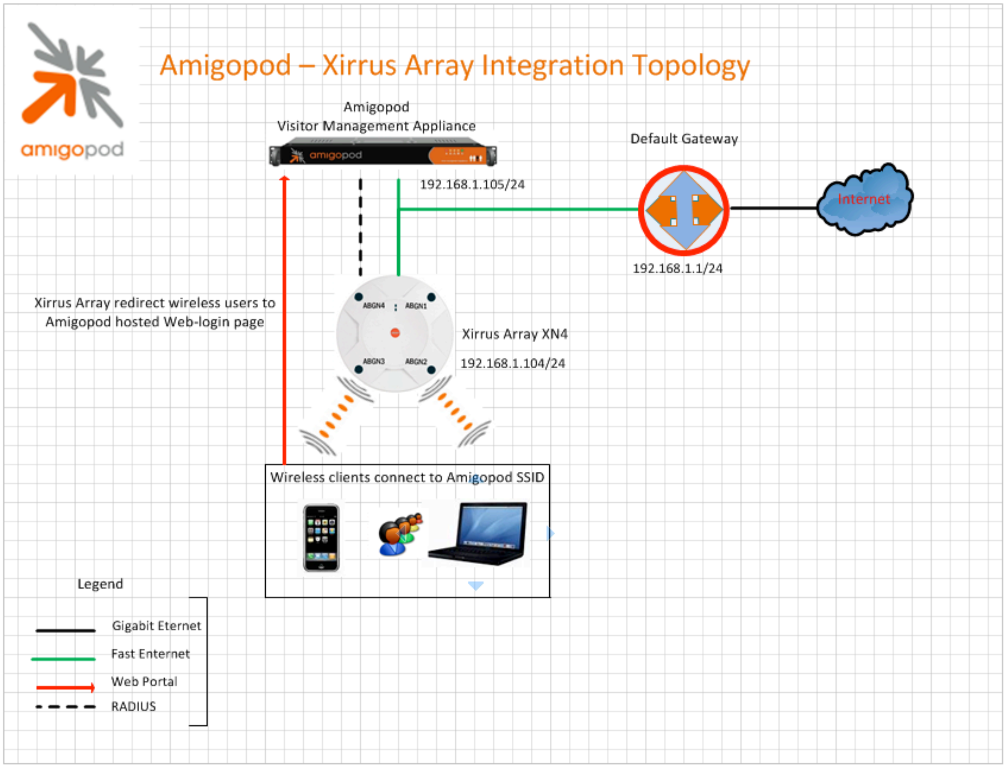
The following table shows the software versions used during the integration testing. This document will be updated in the future if changes in either amigopod or Cisco subsequent releases affect the stability of this integration. It is advised that the customer always check for the latest integration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

Dated Tested:	April 2010
AmigoPod Version:	Kernel→2.1, Radius Services→ 2.1
Plugins Required:	Standard build only
Xirrus Array:	System Software - 4.0.6 Build 1169
	SCD Firmware - 2.21 Build 3157
	Boot Loader - 1.0.0 Build 3090
	IAP Driver - 1.5.0 Build 2036
Integration:	HTTP Captive Portal

Amigopod was deployed locally on the LAN interface of the Xirrus Array as a dedicated appliance. Amigopod VMWare image, or virtual appliance solution, can also be used successfully.

Xirrus Array IP Address	192.168.1.104
Internet Gateway Address	192.168.1.1
amigopod IP Address	192.168.1.103
amigopod RADIUS port	Auth 1812 Acc 1813 (*default settings*)

The following diagram provides a high level overview of the test topology:


amigopod
Amigopod – Xirrus Array Integration Topology
Amigopod
Visitor Management Appliance
Default Gateway
192.168.1.105/24
Internet
192.168.1.1/24
Xirrus Array redirect wireless users to
Amigopod hosted Web-login page
ABGN4
ABGN1
ABGN3
ABGN2
Xirrus Array XN4
192.168.1.104/24
Wireless clients connect to Amigopod SSID
Legend
Gigabit Eternet
Fast Enternet
Web Portal
RADIUS

Integration

Although the Xirrus Array supports both internal and external Captive portal functionality, this integration guide will focus on the later (external) as the internal Captive portal dictates the use of the internal Login Page resident on the Array itself. The Login page is very basic and doesn't allow for significant customization as is possible with the amigoPod Web Logins feature.

Note: Cisco now allow for fully customized Captive portal pages to be uploaded to the Array and managed via templates on the Cisco WCS management platform 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 Xirrus Array's ability to define and reference external RADIUS servers for the authentication and accounting of visitor accounts. In the standalone Xirrus Array Guest provisioning solution the local database in each Array 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.

Xirrus Array Configuration

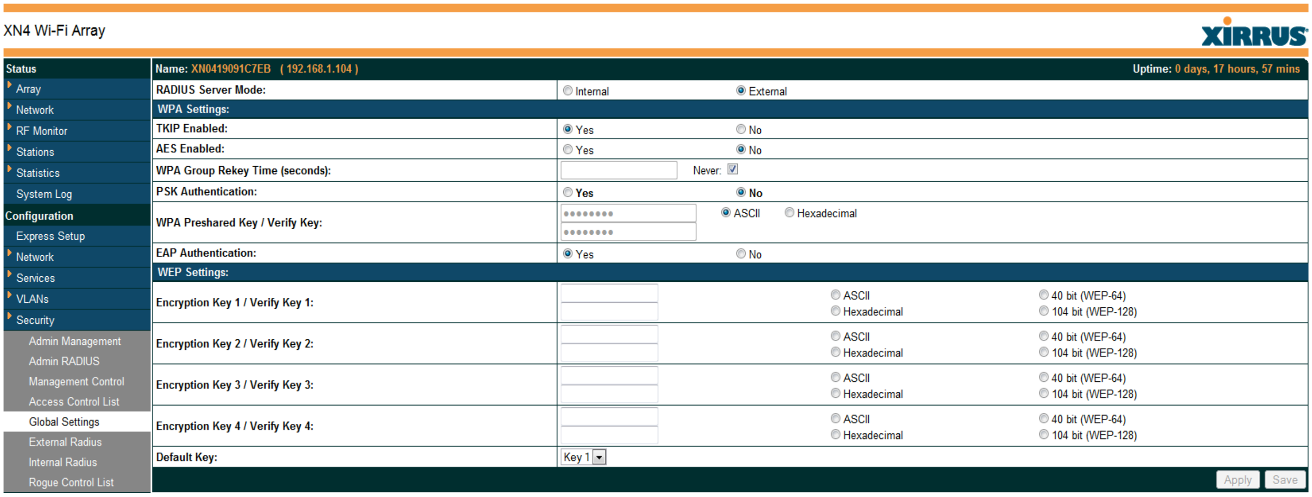
The following configuration procedure assumes that the Xirrus Array has been powered up and a basic IP configuration has been applied through the CLI to allow the administrator to access the Web User Interface. The following table again reviews the IP Addressing used in the test environment but this would be replaced with the site specific details of each customer deployment:

Xirrus Array Address	192.168.1.104
Internet Gateway Address	192.168.1.1
amigopod IP Address	192.168.1.105
amigopod RADIUS port	Auth 1812 Acc 1813 (default settings)

Note: Although the amigopod is communicating with the Xirrus Array via the 192.168.1.x subnet there will be typically several other IP Addresses allocated to the Array on various interface such as the *Service Interface, Management Interface.* Some of these addresses will be visible in the following screenshots and this note is made to hopefully avoid any confusion among the various addresses on the WLC and that the 192.168.1.x subnet was simply the chosen subnet for the deployment of amigopod in this test environment. Site specific issues will drive this topology in all cases and this configuration is only provided as a guide to the high level configuration steps.

Step 1 - Create RADIUS Authentication Server Instance

In order for the Xirrus Array to successfully authenticate the guest users that will be provisioned on the amigopod appliance, a RADIUS Server needs to be enabled on the Array. From the *Security→Global Settings* menu option, click the ‘External’ button at the top middle of the screen.



Name: XN0419091C7EB (192.168.1.104)

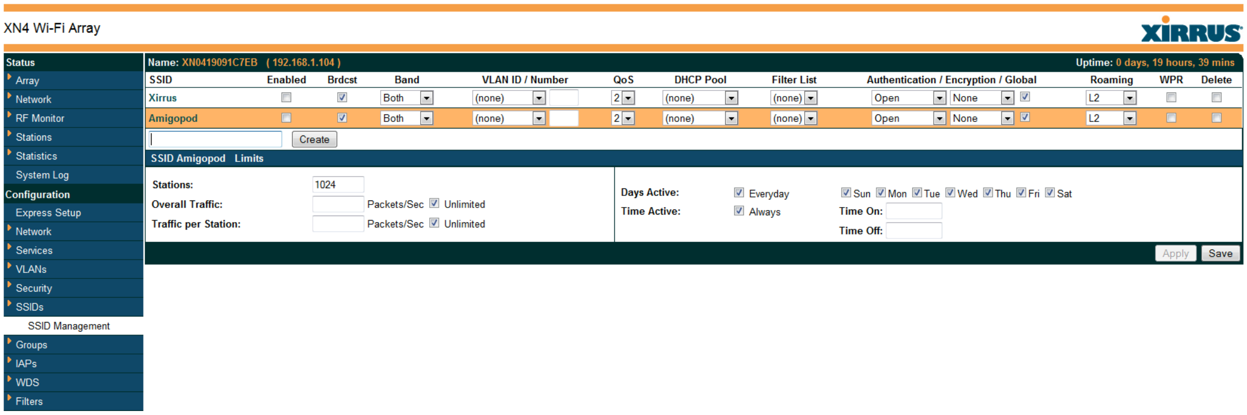
Uptime: 0 days, 17 hours, 57 mins

RADIUS Server Mode:	○ Internal	● External	
WPA Settings:			
TKIP Enabled:	● Yes	○ No	
AES Enabled:	○ Yes	● No	
WPA Group Rekey Time (seconds):		Never: ☑	
PSK Authentication:	○ Yes	● No	
WPA Preshared Key / Verify Key:	•••••••• ••••••••	● ASCII	○ Hexadecimal
EAP Authentication:	● Yes	○ No	
WEP Settings:			
Encryption Key 1 / Verify Key 1:		○ ASCII ○ Hexadecimal	○ 40 bit (WEP-64) ○ 104 bit (WEP-128)
Encryption Key 2 / Verify Key 2:		○ ASCII ○ Hexadecimal	○ 40 bit (WEP-64) ○ 104 bit (WEP-128)
Encryption Key 3 / Verify Key 3:		○ ASCII ○ Hexadecimal	○ 40 bit (WEP-64) ○ 104 bit (WEP-128)
Encryption Key 4 / Verify Key 4:		○ ASCII ○ Hexadecimal	○ 40 bit (WEP-64) ○ 104 bit (WEP-128)
Default Key:	Key 1		

Click the *Apply* Apply and the *Save* Save button (immediately after) to save changes.

Step 2 - Create an SSID and Configure/Enable Web Page Redirect

In order for the Xirrus Array to successfully redirect guest users to the web porta hosted by the Amigopod appliance and forward accounting data associated with traffic being generated by guest users, an SSID need to be created and Web Portal Redirect needs to be enabled and configured; along with a RADIUS definition. From the *SSIDs→SSID Management* menu option, edit the existing SSID (*default is Xirrus*) or create a new one, by typing the name of the SSID and clicking on the 'Create' Create button. In this example, we've created an SSID called 'Amigopod'.



Name: XN0419091C7EB (192.168.1.104) Uptime: 0 days, 19 hours, 39 mins

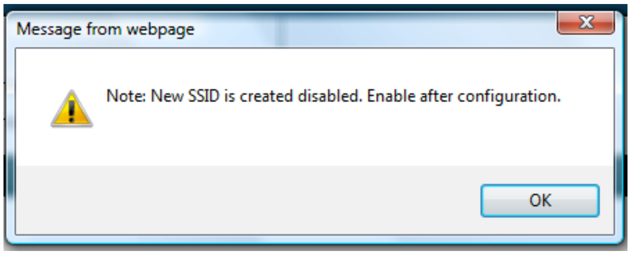
SSID	Enabled	Brdcst	Band	VLAN ID / Number	QoS	DHCP Pool	Filter List	Authentication / Encryption / Global	Roaming	WPR	Delete
Xirrus	□	☑	Both	(none)	2	(none)	(none)	Open / None / ☑	L2	□	□
Amigopod	□	☑	Both	(none)	2	(none)	(none)	Open / None / ☑	L2	□	□

SSID Amigopod Limits

Stations: 1024
Overall Traffic: Packets/Sec ☑ Unlimited
Traffic per Station: Packets/Sec ☑ Unlimited

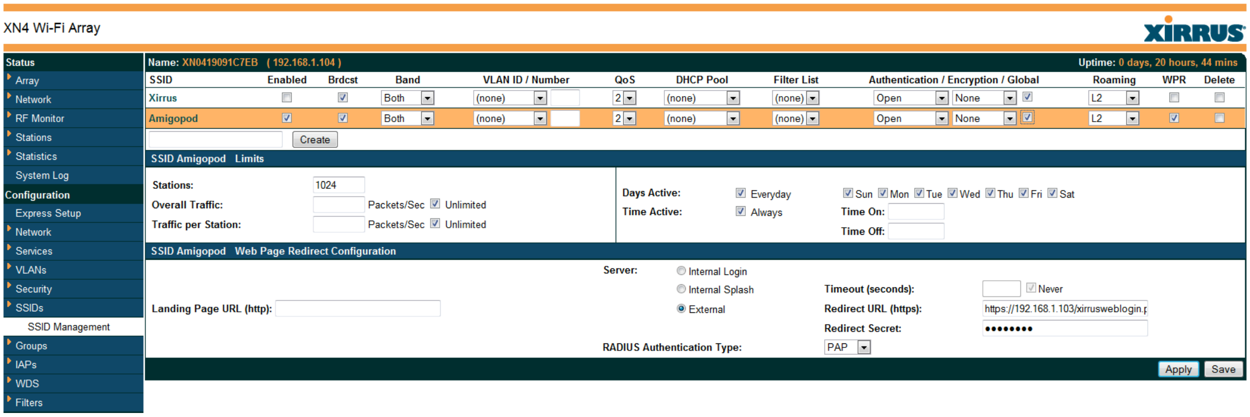
Days Active: ☑ Everyday ☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat
Time Active: ☑ Always Time On:
Time Off:

Note: When the 'Create' button is depressed, the following message will appear; as all newly created SSIDs are disabled by default.



Note: New SSID is created disabled. Enable after configuration.

Enable the WPR feature by clicking in the WPR check box. This will cause the 'SSID Amigopod Web Page Redirect Configuration' section to appear (*see illustration on the following page*). Enable the external RADIUS function for the SSID by clicking on the 'External' circle. In the 'Redirect URL' field, type in the address, for example; http://192.168.1.103/xirrusweblogin.php. Type in the 'Redirect Secret' after entering in the Redirect URL.



Name: XN0419091C7EB (192.168.1.104) Uptime: 0 days, 20 hours, 44 mins

SSID	Enabled	Brdcst	Band	VLAN ID / Number	QoS	DHCP Pool	Filter List	Authentication / Encryption / Global	Roaming	WPR	Delete
Xirrus	☐	☑	Both	(none)	2	(none)	(none)	Open None ☑	L2	☐	☐
Amigopod	☑	☑	Both	(none)	2	(none)	(none)	Open None ☑	L2	☑	☐

SSID Amigopod Limits

Stations: 1024
Overall Traffic: Packets/Sec ☑ Unlimited
Traffic per Station: Packets/Sec ☑ Unlimited
Days Active: ☑ Everyday ☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat
Time Active: ☑ Always Time On: Time Off:

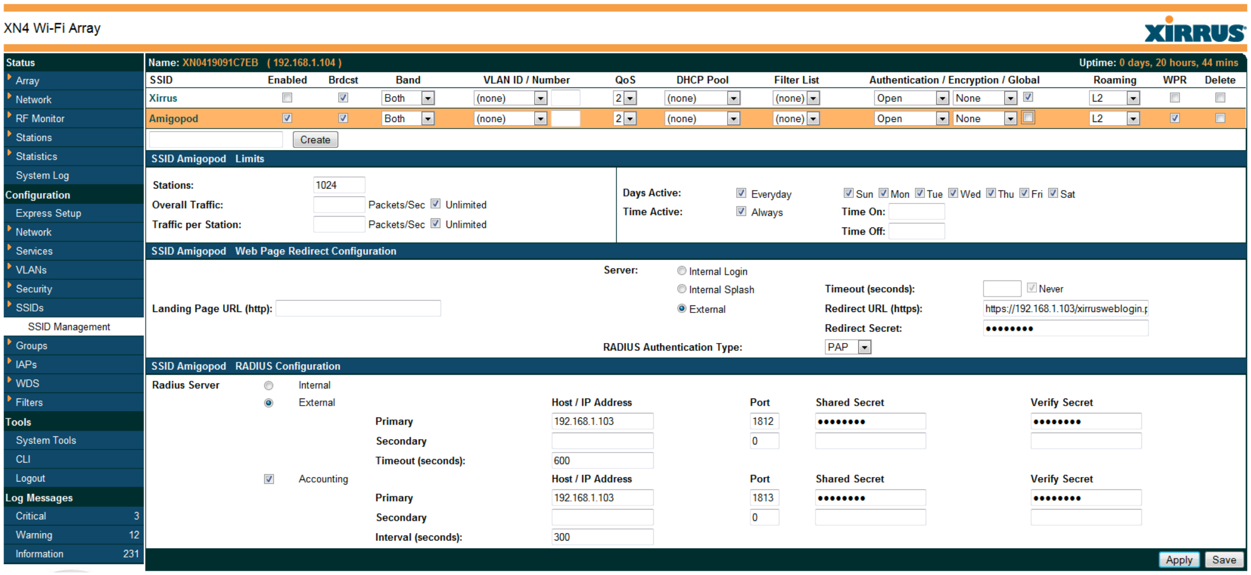
SSID Amigopod Web Page Redirect Configuration

Landing Page URL (http):
Server: ○ Internal Login ○ Internal Splash ● External
Timeout (seconds): ☑ Never
Redirect URL (https): https://192.168.1.103/xirrusweblogin.p
Redirect Secret: ••••••••
RADIUS Authentication Type: PAP

Click on the ‘Save’ button (*bottom right*).

Step 3 – RADIUS Configuration

To configure the RADUIS Server, uncheck the ‘Global’ box; the SSID Amigopod RADIUS Configuration section should appear. Click the ‘External’ circle and click the ‘Accounting’ box. Enter the IP Address of your Amigopod appliance and the Port Numbers (*note, the same IP Address can be used for both the RADIUS and Accounting Servers*). Next, enter the ‘Shared Secret’, and verify by typing it a second time in the ‘Verify Secret’ field (*do this for both the RADUS and Accounting Servers*). Finally, enable the SSID by clicking on the ‘Enable’ box next to the SSID name.



Name: XN0419091C7EB (192.168.1.104) Uptime: 0 days, 20 hours, 44 mins

SSID	Enabled	Brdcst	Band	VLAN ID / Number	QoS	DHCP Pool	Filter List	Authentication / Encryption / Global	Roaming	WPR	Delete
Xirrus	☐	☑	Both	(none)	2	(none)	(none)	Open None ☑	L2	☐	☐
Amigopod	☑	☑	Both	(none)	2	(none)	(none)	Open None ☐	L2	☑	☐

SSID Amigopod Limits

Stations: 1024
Overall Traffic: Packets/Sec ☑ Unlimited
Traffic per Station: Packets/Sec ☑ Unlimited
Days Active: ☑ Everyday ☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat
Time Active: ☑ Always Time On: Time Off:

SSID Amigopod Web Page Redirect Configuration

Landing Page URL (http):
Server: ○ Internal Login ○ Internal Splash ● External
Timeout (seconds): ☑ Never
Redirect URL (https): https://192.168.1.103/xirrusweblogin.p
Redirect Secret: ••••••••
RADIUS Authentication Type: PAP

SSID Amigopod RADIUS Configuration

Radius Server ○ Internal

		Host / IP Address	Port	Shared Secret	Verify Secret
● External	Primary	192.168.1.103	1812	••••••••	••••••••
	Secondary		0		
	Timeout (seconds):	600			
☑ Accounting		Host / IP Address	Port	Shared Secret	Verify Secret
	Primary	192.168.1.103	1813	••••••••	••••••••
	Secondary		0		
	Interval (seconds):	300			

Apply and Save your configuration by clicking on the ‘Apply’ and ‘Save’ button.

Amigopod Configuration

The following configuration procedure assumes that the amigopod software or appliance has been powered up and a basic IP configuration has been applied through the setup wizard to allow the administrator to access the Web User Interface. 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:

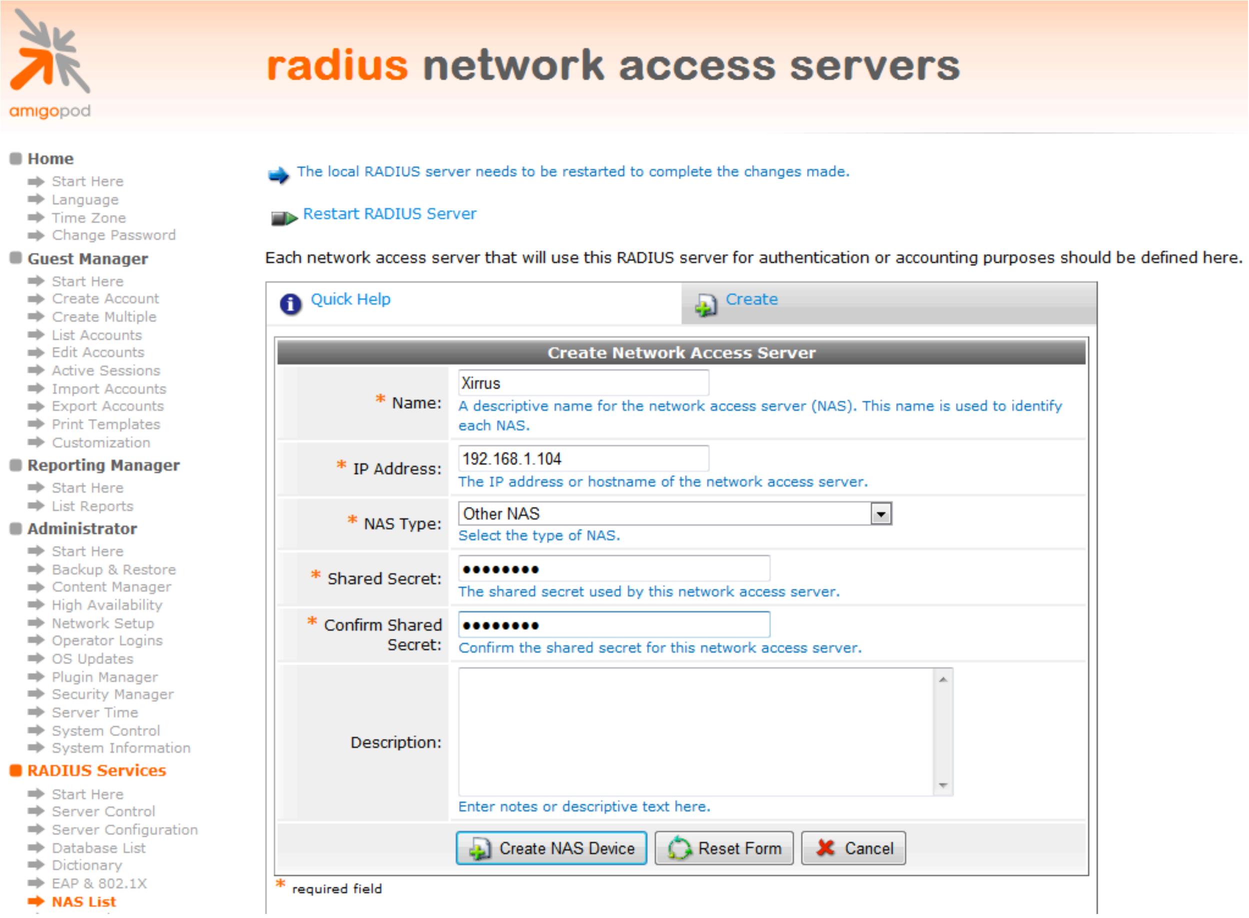
Xirrus Array Address	192.168.1.104
Internet Gateway Address	192.168.1.1
amigopod IP Address	192.168.1.103
amigopod RADIUS port	Auth 1812 Acc 1813 (default settings)

Please refer to the amigopod Quick Start Guide for more information on the basic configuration of the amigopod software.

Step1 - Create RADIUS NAS for Xirrus Array

In order for the Xirrus Array to authenticate users it needs to be able to communicate with the amigopod RADIUS instance. Back in Step 3 of the Xirrus Array configuration, a RADIUS server definition was created. This step configures the amigopod NAS definition for the Xirrus Array. The RADIUS key used in Step 3 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 Name and IP Address of the Xirrus Array, leave the *NAS Type* as *Other NAS* and enter the key from Step 3 in the *Shared Secret* field.



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.

Create Network Access Server

* Name:	Xirrus A descriptive name for the network access server (NAS). This name is used to identify each NAS.
* IP Address:	192.168.1.104 The IP address or hostname of the network access server.
* NAS Type:	Other NAS Select the type of NAS.
* Shared Secret:	•••••••• The shared secret used by this network access server.
* Confirm Shared Secret:	•••••••• Confirm the shared secret for this network access server.
Description:	Enter notes or descriptive text here.

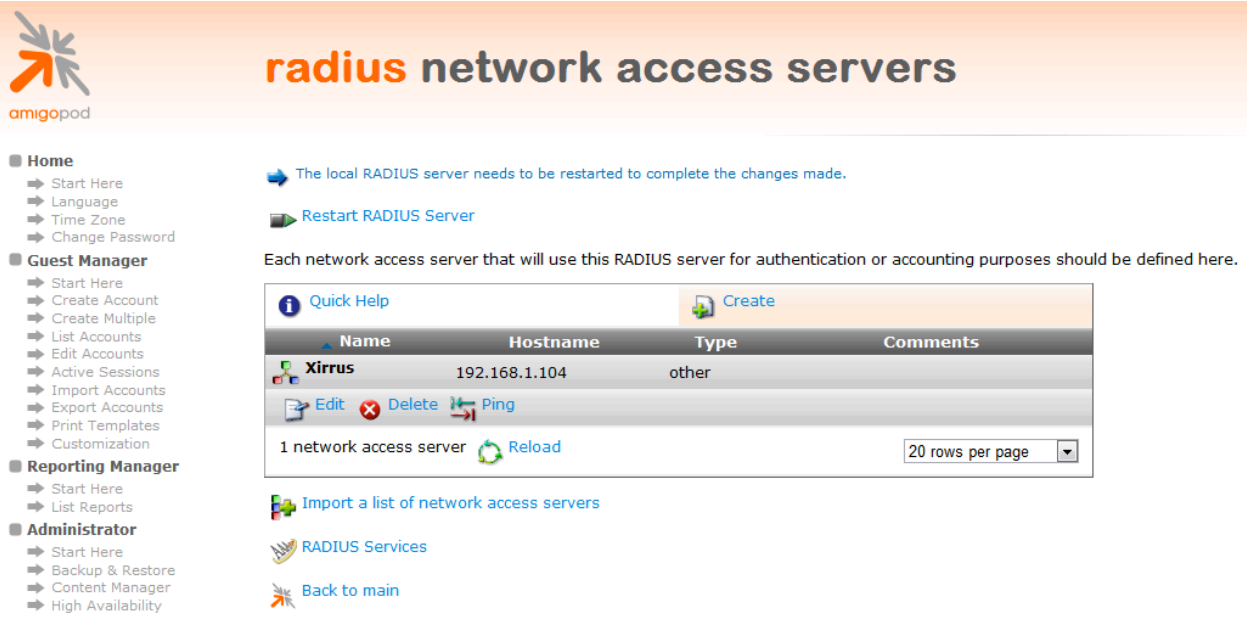
* required field

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.



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

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

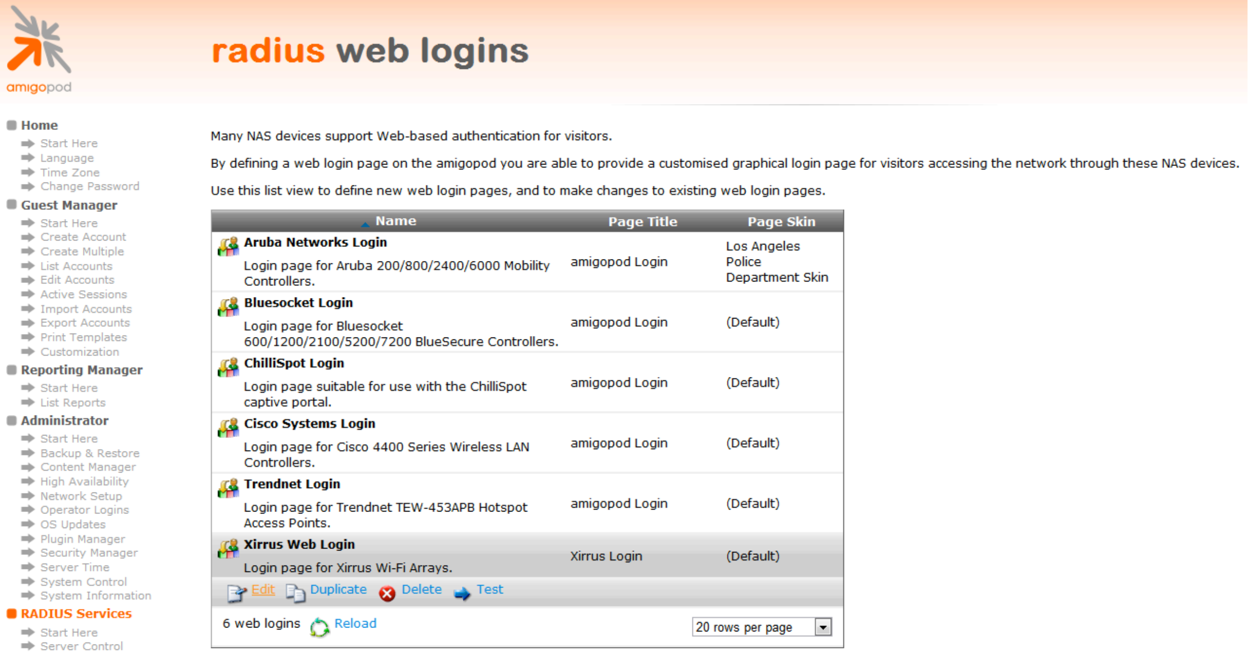
Name	Hostname	Type	Comments
Xirrus	192.168.1.104	other	

1 network access server

Step 3 - Configure Xirrus Array Web Logins Page

By default the amigopod comes pre-configured with Web Login templates (*RADIUS Services→ Web Logins*) for all the major wireless manufactures. The Xirrus 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 installed; as shown below:

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



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.

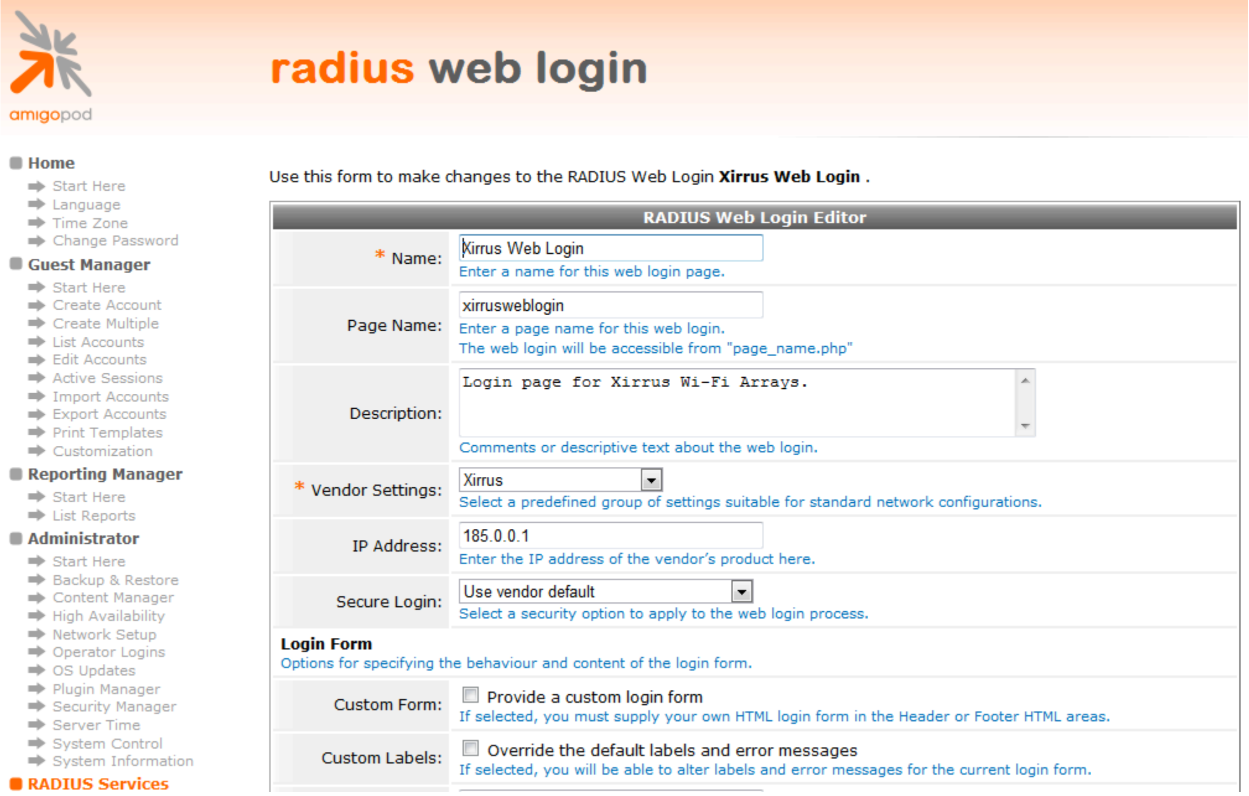
Use this list view to define new web login pages, and to make changes to existing web login pages.

Name	Page Title	Page Skin
Aruba Networks Login Login page for Aruba 200/800/2400/6000 Mobility Controllers.	amigopod Login	Los Angeles Police Department Skin
Bluesocket Login Login page for Bluesocket 600/1200/2100/5200/7200 BlueSecure Controllers.	amigopod Login	(Default)
ChilliSpot Login Login page suitable for use with the ChilliSpot captive portal.	amigopod Login	(Default)
Cisco Systems Login Login page for Cisco 4400 Series Wireless LAN Controllers.	amigopod Login	(Default)
Trendnet Login Login page for Trendnet TEW-453APB Hotspot Access Points.	amigopod Login	(Default)
Xirrus Web Login Login page for Xirrus Wi-Fi Arrays.	Xirrus Login	(Default)

Please note the Xirrus Login template assumes the Virtual Interface address is the default setting of 185.0.0.1.

The Virtual Interface IP address is used only in communications between the Array and wireless clients. It never appears as the source or destination address of a packet that goes out a distribution system port and onto the switched network. For the system to operate correctly, the virtual interface IP address must be set (it cannot be 0.0.0.0), and no other device on the network can have the same address as the virtual interface. Therefore, the virtual interface must be configured with an unassigned and unused gateway IP address, such as 1.1.1.1. The virtual interface IP address is not pingable and should not exist in any routing table in your network. In addition, the virtual interface cannot be mapped to a backup port.

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 **Xirrus Web Login** .

RADIUS Web Login Editor

* Name:	Xirrus Web Login Enter a name for this web login page.
Page Name:	xirrusweblogin Enter a page name for this web login. The web login will be accessible from "page_name.php"
Description:	Login page for Xirrus Wi-Fi Arrays. Comments or descriptive text about the web login.
* Vendor Settings:	Xirrus Select a predefined group of settings suitable for standard network configurations.
IP Address:	185.0.0.1 Enter the IP address of the vendor's product here.
Secure Login:	Use vendor default Select a security option to apply to the web login process.

Login Form
Options for specifying the behaviour and content of the login form.

Custom Form:	☐ Provide a custom login form If selected, you must supply your own HTML login form in the Header or Footer HTML areas.
Custom Labels:	☐ Override the default labels and error messages If selected, you will be able to alter labels and error messages for the current login form.

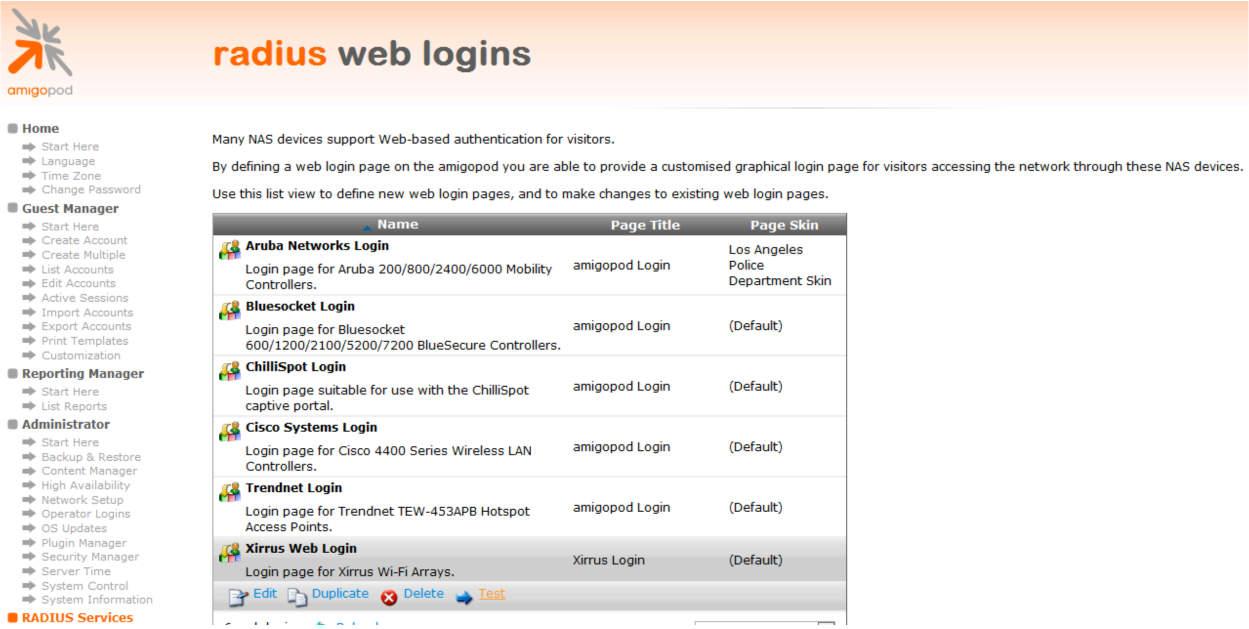
Modify the sample HTML in the *Header HTML,* and *Login Message* section to customize for your local environment. In addition add the following html script to the Footer section:

```
<script><!--
{literal}
var frm = document.forms[0];
if (frm.res && frm.res.value == 'success') {
  if (frm.userurl && frm.userurl.value != '') {
    window.location.href=frm.userurl.value;
  } else if (frm.redirurl && frm.redirurl.value != '') {
    window.location.href=frm.redirurl.value;
  }
}
{/literal}

//-->
</script>
```

Click the *Save Changes* button to commit the changes.

Step 3 - Confirm External Captive Portal URL

The URL that needs to be configured in the Xirrus Array External Captive Portal section covered in Step 3 can be confirmed by clicking on the test button shown on the screen below under the *RADIUS Services → Web Logins* screen:



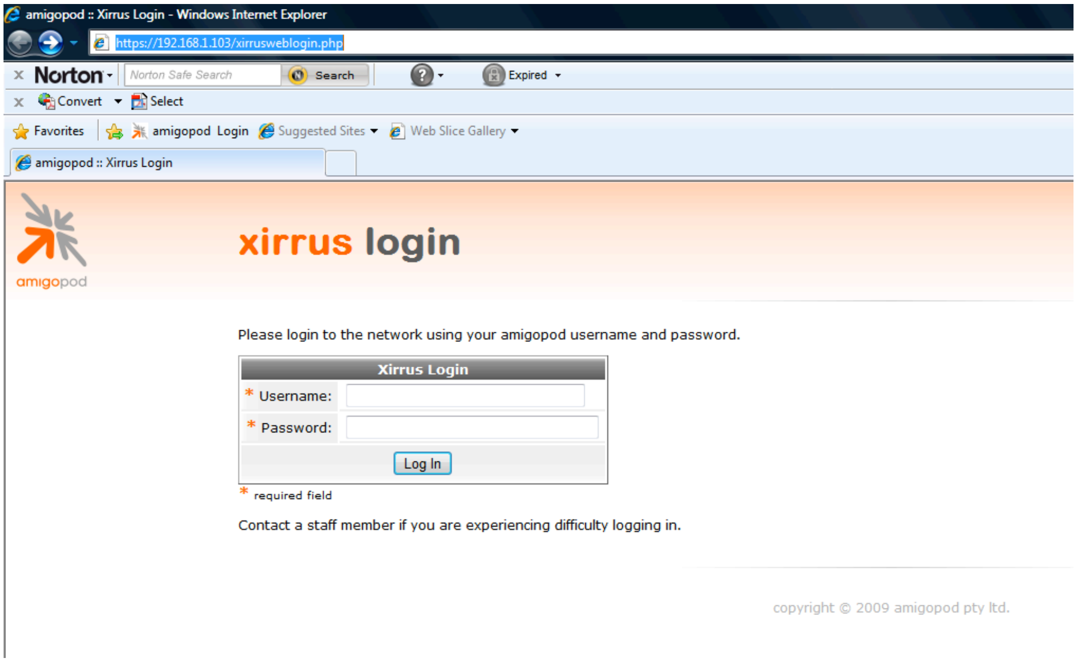
Many NAS devices support Web-based authentication for visitors.

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
Aruba Networks Login Login page for Aruba 200/800/2400/6000 Mobility Controllers.	amigopod Login	Los Angeles Police Department Skin
Bluesocket Login Login page for Bluesocket 600/1200/2100/5200/7200 BlueSecure Controllers.	amigopod Login	(Default)
ChilliSpot Login Login page suitable for use with the ChilliSpot captive portal.	amigopod Login	(Default)
Cisco Systems Login Login page for Cisco 4400 Series Wireless LAN Controllers.	amigopod Login	(Default)
Trendnet Login Login page for Trendnet TEW-453APB Hotspot Access Points.	amigopod Login	(Default)
Xirrus Web Login Login page for Xirrus Wi-Fi Arrays.	Xirrus Login	(Default)

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



https://192.168.1.103/xirrusweblogin.php

Please login to the network using your amigopod username and password.

Xirrus Login

* Username:

* Password:

Log In

* required field

Contact a staff member if you are experiencing difficulty logging in.

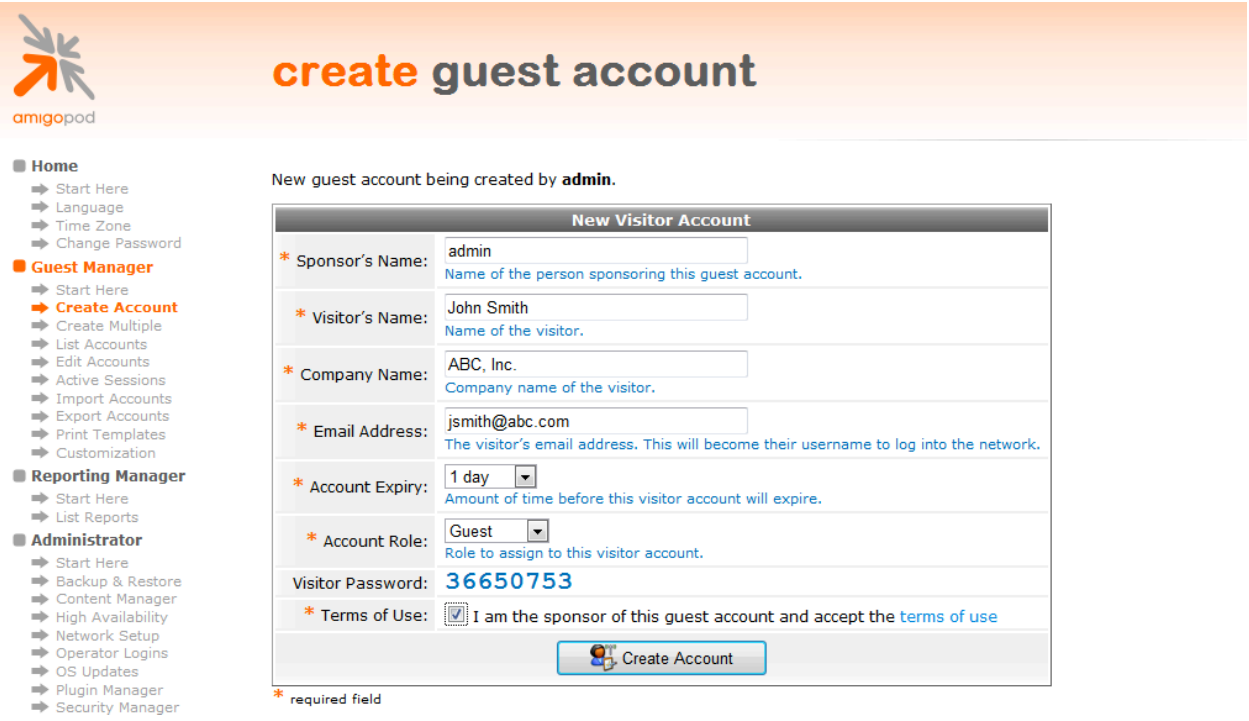
copyright © 2009 amigopod pty ltd.

Note: The URL presented in the web browser after the *Test* button has been clicked will be required in the configuration of the captive portal settings on the Xirrus Array. An example of the URL is shown below:

http://192.1668.1.103/xirrusweblogin.php

Step 4 - Create a test 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.



New guest account being created by **admin**.

New Visitor Account

* Sponsor's Name:	admin Name of the person sponsoring this guest account.
* Visitor's Name:	John Smith Name of the visitor.
* Company Name:	ABC, Inc. Company name of the visitor.
* Email Address:	jsmith@abc.com The visitor's email address. This will become their username to log into the network.
* Account Expiry:	1 day Amount of time before this visitor account will expire.
* Account Role:	Guest Role to assign to this visitor account.
Visitor Password:	36650753
* Terms of Use:	☑ I am the sponsor of this guest account and accept the terms of use

* required field

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.

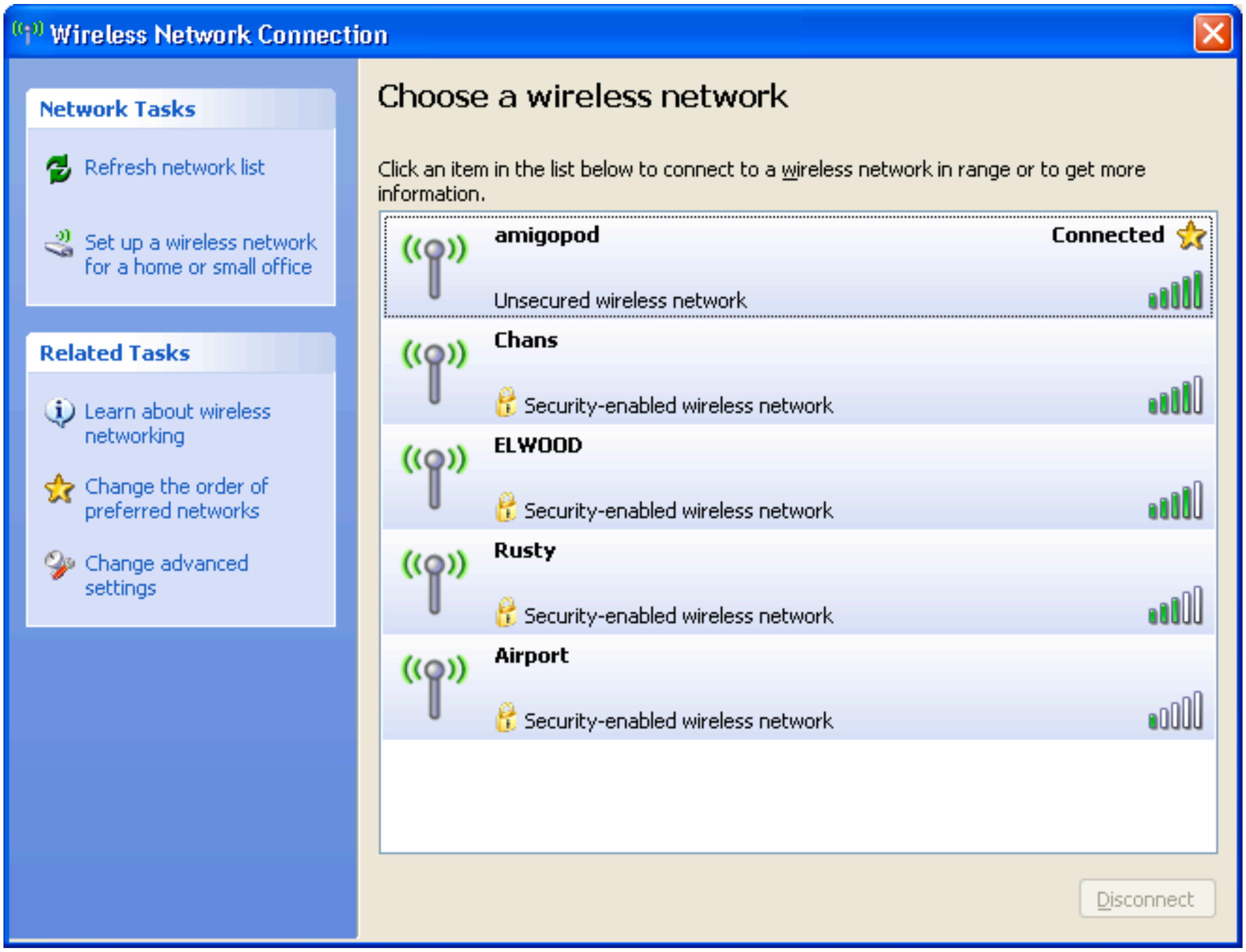
Testing the Configuration

Now that the configuration of both the Xirrus Array and the amigopod appliance is complete, the following steps can be followed to verify the configuration.

Step 1 - Connect to the amigopod wireless network

Using a test laptop with a compatible 802.11 based wireless card attempt to connect to the advertised *amigopod* wireless network. The screen capture below shows the interface used on a Windows XP SP2 based laptop. Although the process differs from laptop to laptop depending on the wireless card drivers installed and different operating systems in use, the basic premise of connecting to the unsecured Guest Wireless 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.

Note: If the *Amigopod* wireless network is not visible from the test laptop, double check the configuration of the Xirrus Array and potentially source a second wireless test device to see if the problem is laptop specific.



Wireless Network Connection
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Disconnect

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

amigopod — Connected — Unsecured wireless network

Chans — Security-enabled wireless network

ELWOOD — Security-enabled wireless network

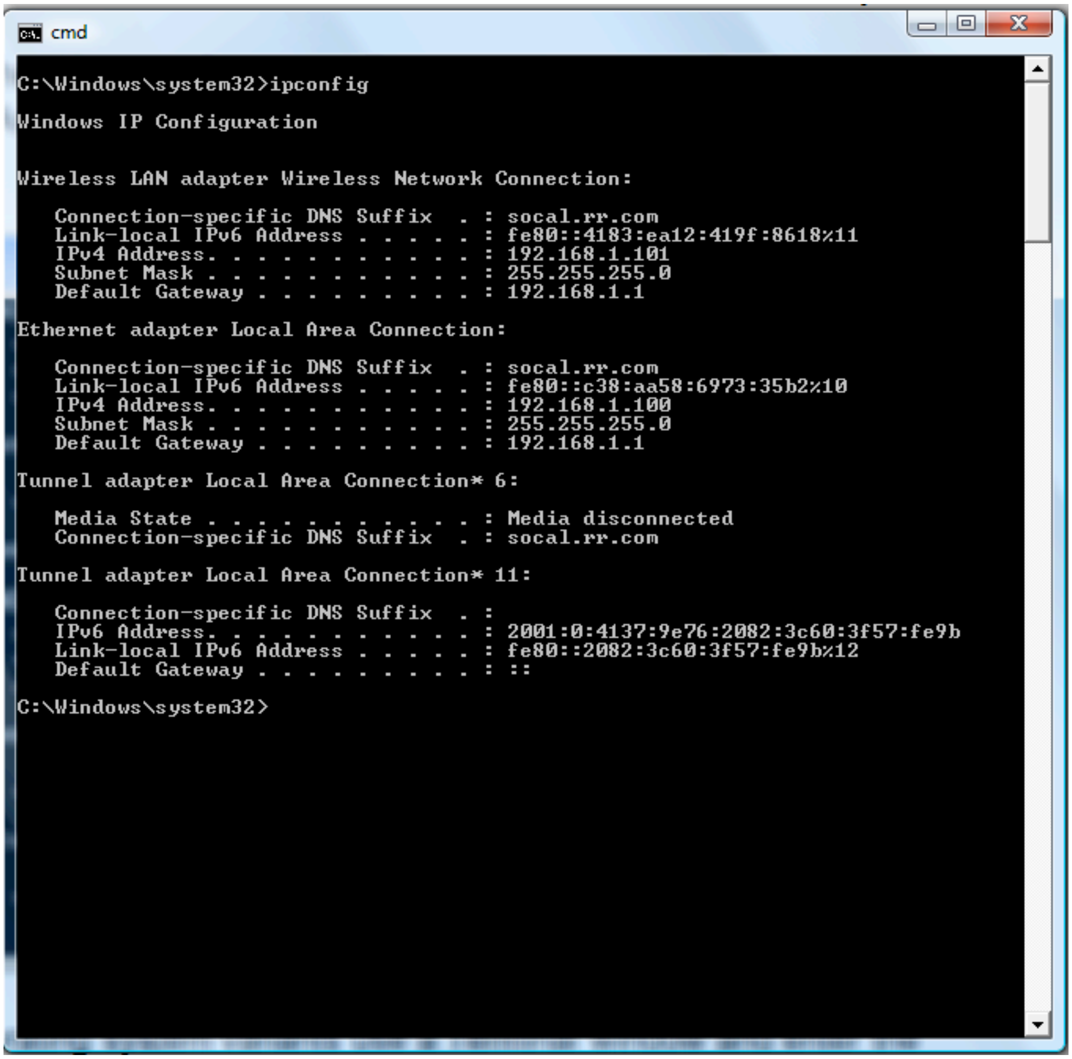
Rusty — Security-enabled wireless network

Airport — Security-enabled wireless network

Step 2 – 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 Xirrus Array.

Issue the *ipconfig* command from the Windows Command Prompt to display the IP information received from the DHCP process. As illustrated below on the Wireless adapter an IP Address of *192.168.1.101* has been received.

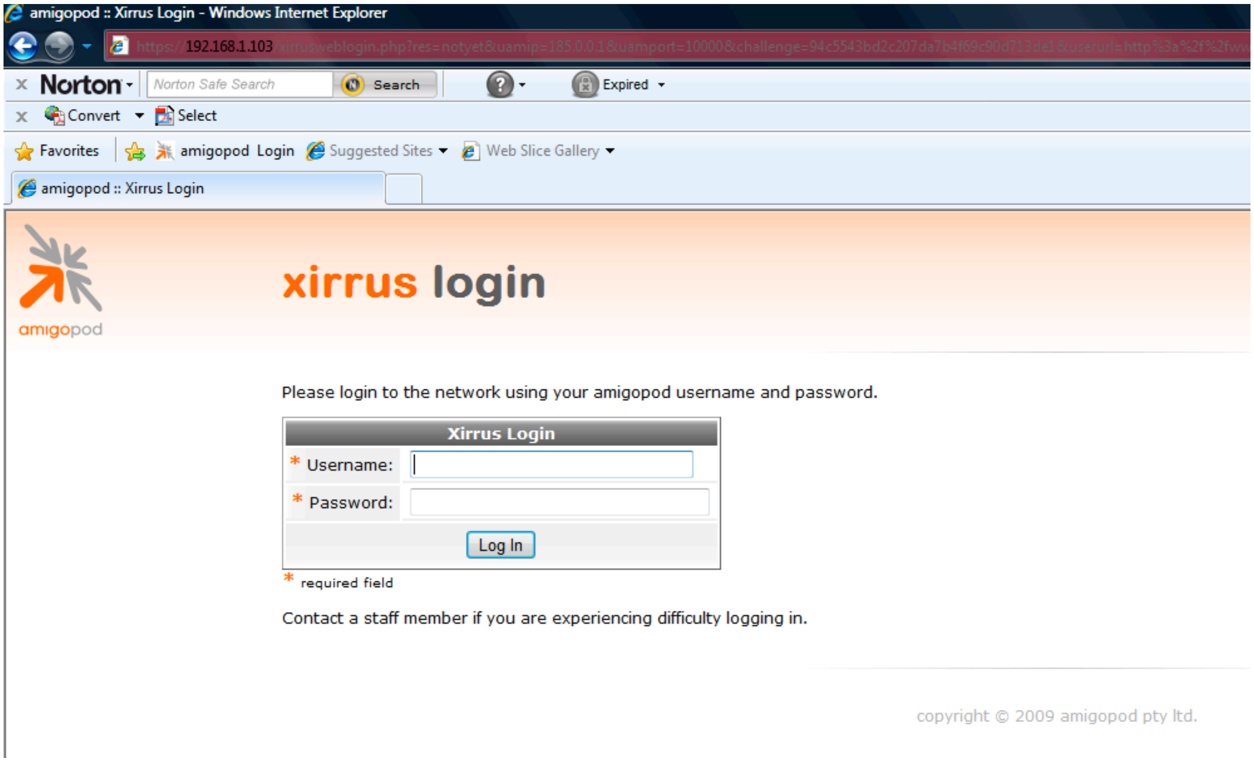


```
C:\Windows\system32>ipconfig

Windows IP Configuration


Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . : socal.rr.com
   Link-local IPv6 Address . . . . . : fe80::4183:ea12:419f:8618%11
   IPv4 Address. . . . . . . . . . . : 192.168.1.101
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : socal.rr.com
   Link-local IPv6 Address . . . . . : fe80::c38:aa58:6973:35b2%10
   IPv4 Address. . . . . . . . . . . : 192.168.1.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Tunnel adapter Local Area Connection* 6:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : socal.rr.com

Tunnel adapter Local Area Connection* 11:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:4137:9e76:2082:3c60:3f57:fe9b
   Link-local IPv6 Address . . . . . : fe80::2082:3c60:3f57:fe9b%12
   Default Gateway . . . . . . . . . : ::

C:\Windows\system32>
```

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

Step 3 - Launch Web Browser and login

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


amigopod :: Xirrus Login - Windows Internet Explorer
https://192.168.1.103/xirrusweblogin.php?res=notyet&uamip=185.0.0.1&uamport=10000&challenge=94c5543bd2c207da7b4f69c90d713de1&userurl=http%3a%2f%2fww
Norton
Norton Safe Search
Search
Expired
Convert
Select
Favorites
amigopod Login
Suggested Sites
Web Slice Gallery
amigopod :: Xirrus Login
amigopod

xirrus login

Please login to the network using your amigopod username and password.

Xirrus Login	
* Username:	
* Password:	
Log In	

* required field

Contact a staff member if you are experiencing difficulty logging in.

copyright © 2009 amigopod pty ltd.

Enter the test user details created in Step 3 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 Array and onto the Internet or Corporate network.

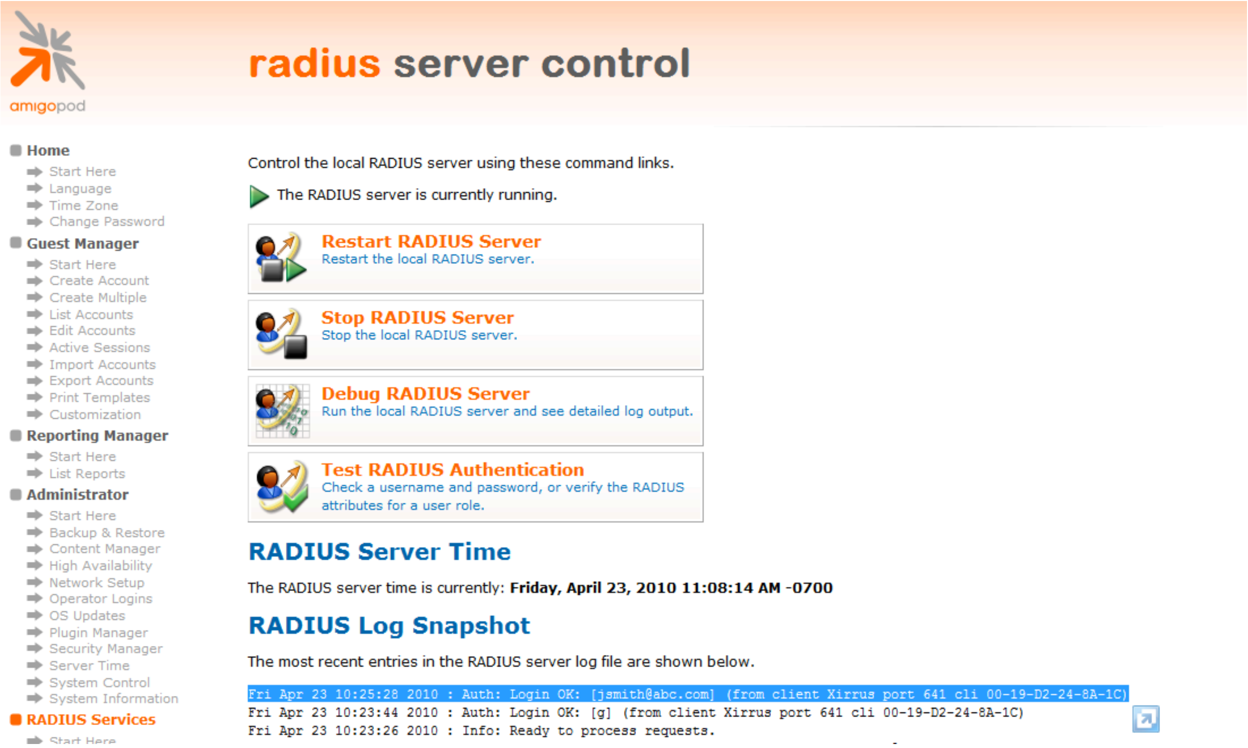
Note: If the web browser fails to redirect check that the DNS server configured in the DHCP Server is available and successfully resolving domain names. Without name resolution working the web browser will never attempt to connect to the website defined in web browser home page and therefore redirection will be unsuccessful. 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

Step 4 - 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, *jsmith@abc.om*

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.



Control the local RADIUS server using these command links.

The RADIUS server is currently running.

RADIUS Server Time

The RADIUS server time is currently: **Friday, April 23, 2010 11:08:14 AM -0700**

RADIUS Log Snapshot

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

```
Fri Apr 23 10:25:28 2010 : Auth: Login OK: [jsmith@abc.com] (from client Xirrus port 641 cli 00-19-D2-24-8A-1C)
Fri Apr 23 10:23:44 2010 : Auth: Login OK: [g] (from client Xirrus port 641 cli 00-19-D2-24-8A-1C)
Fri Apr 23 10:23:26 2010 : Info: Ready to process requests.
```

This is a useful tool to remember when troubleshooting user authentication issues. A more advanced debugging tool is also available from this screen using the *Debug RADIUS Server* button.