HP ProCurve MSM Integration Guide

Revision 0.9

Date 22 August 2009

amigopod Head Office

amigopod Pty Ltd
Suite 101
349 Pacific Hwy
North Sydney, NSW 2060
Australia

ABN 74 124 753 420

Web www.amigopod.com

Phone +61 2 8669 1140

Fax +61 7 3009 0329

Table of Contents

Introduction

This document outlines the configuration process on both the HP Pro Curve MultiService Controllers and the amigopod appliance to create a fully integrated Visitor Management solution. The solution leverages the captive portal functionality built into the HP ProCurve MSM. HP ProCurve uses the terminology of HTML Authentication to refer to their internal captive portal functionality and it can be generally defined as follows:

Captive portal 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, Captive 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 HP ProCurve HTML Authentication 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.

The following table outlines the HP ProCurve MSM appliances that have been tested with the amigopod solution by either a partner or the vendor directly.

Vendor	Products	amigopod verified	Partner Verified
ProCurve Networking by HP	MSM710, MSM750	Yes – 5.2.6.2	

Test Environment

The test environment referenced throughout this integration guide is based on a HP ProCurve MSM710. Although this low end hardware platform has been used, the testing and therefore this procedure is valid for all hardware variants from HP ProCurve as it is the MSM software that is providing the integration points with amigopod.

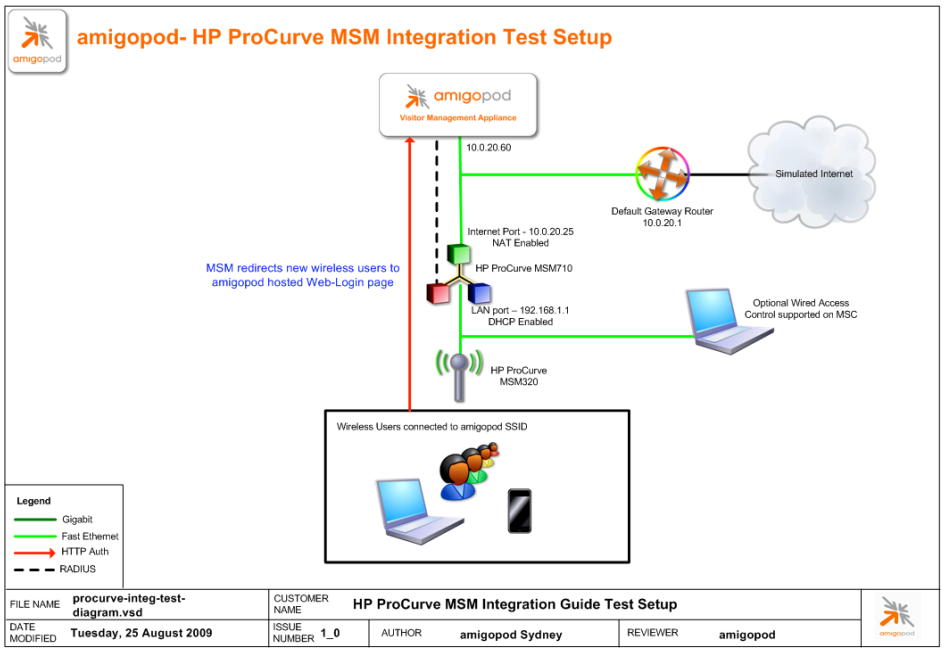
The following table shows the software versions used during the integration testing. This document will be updated in the future if changes in either amigopod or HP ProCurve subsequent releases affect the stability of this integration. It is advised that the customer always check for the latest integration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

Date Tested:	August 2009
AmigoPod Version:	Kernel→2.0, Radius Services→ 2.0.1
Plugins Required:	Standard build only
MSM Version:	5.2.6.2-01-7148
Integration:	HTTP Captive Portal

Amigopod was deployed locally on the LAN interface of the HP ProCurve controller as a VMWare image running on a test laptop. Although the VMWare image has been used the integration is equally valid for the amigopod appliance and self installing DVD deployment variants.

MSM710 IP Address	10.0.20.25
Internet Gateway Address	10.0.20.1
amigopod IP Address	10.0.20.60
amigopod RADIUS port	Auth 1812 Acc 1813 (default settings)

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



Integration

Although the HP ProCurve MSM710 supports both internal and external Captive portal functionality, this integration guide will focus on the later as the internal HTML Authentication 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: HP ProCurve now allows for customised Captive portal pages to be cached on the controller but this process requires a significant amount of web design and javascript 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 MSM's ability to define and reference external RADIUS servers for the authentication and accounting of visitor accounts. In the standalone HP ProCurve 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.

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

MSM710 IP Address	10.0.20.25
Internet Gateway Address	10.0.20.1
amigopod IP Address	10.0.20.60
amigopod RADIUS port	Auth 1812 Acc 1813 (default settings)

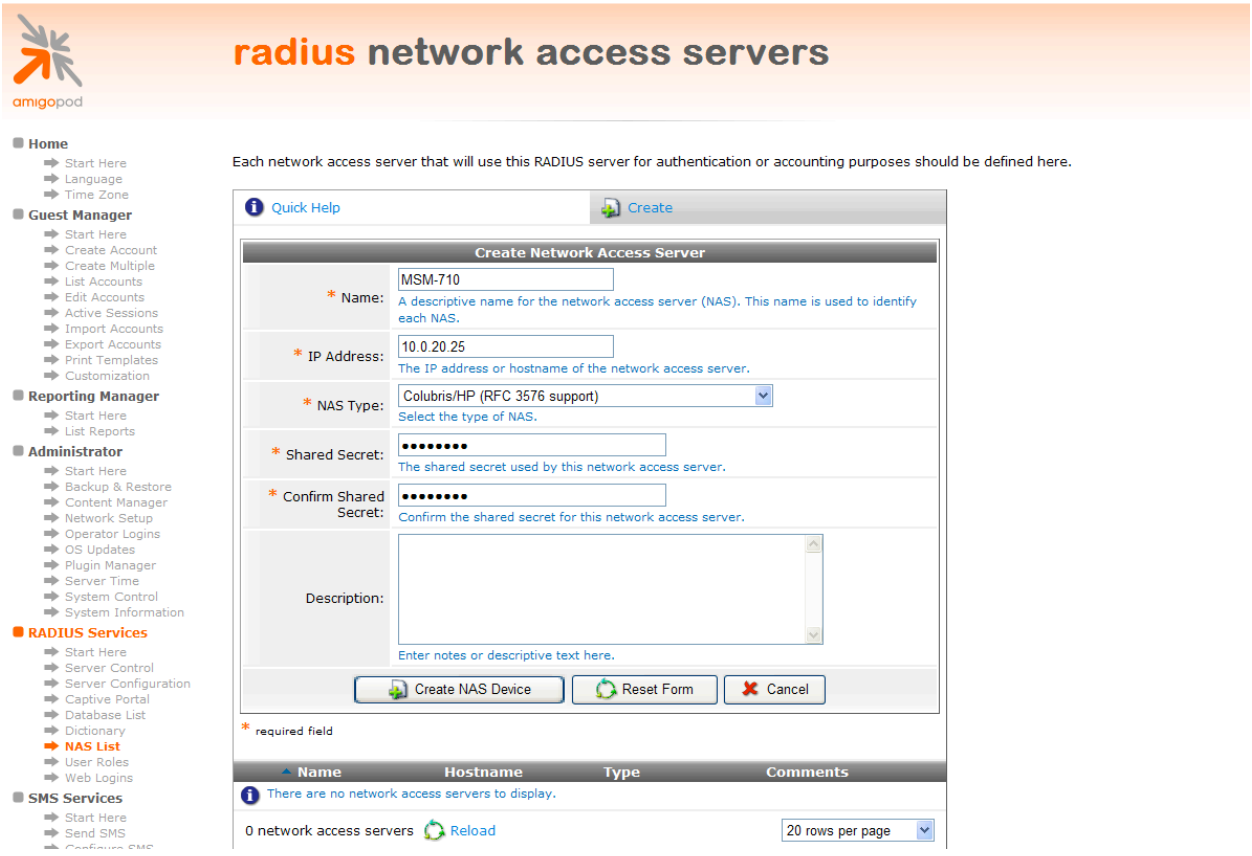
Please refer to the amigopod Quick Start Guide for more information on the basic configuration of the amigopod software.

Step 1 – Create RADIUS NAS for HP ProCurve Controller

In order for the HP ProCurve controller to authenticate users it needs to be able to communicate with the amigopod RADIUS instance. This step configures the amigopod NAS definition for the HP ProCurve Controller. The RADIUS key used here needs to be configured exactly the same as what will be configured on the MSM for the RADIUS transactions to be successful.

For simplicity we will use a shared secret of ***wireless***. Please note this as it will be required in the first step of the HP ProCurve configuration.

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 HP ProCurve Controller, set the *NAS Type* as *Colubris/HP* (*RFC 3576 Support)* and enter the key of *wireless* in the *Shared Secret* 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 effect.

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

Step 3 – Create a Web-Login Page

From the *RADIUS Services→Web Logins* page select the *Create New Web Login page* option at the bottom of the page. From the *RADIUS Web* Login page enter a name and description of the Web Login page you are creating.

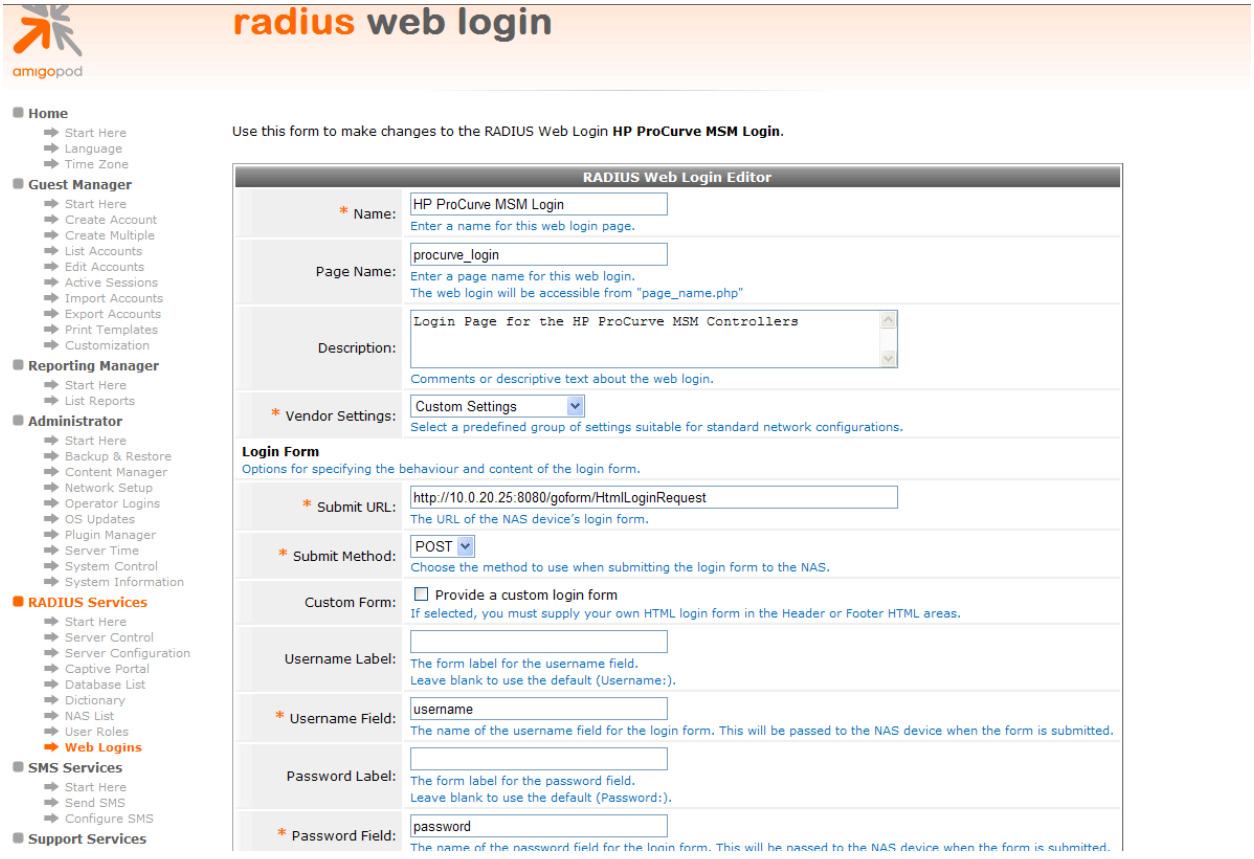
Optionally you can set a preferred page name that will make up the Web Login URL. In this example we have chosen to use *procurve_login* as the name and the resulting URL in this lab environment will be:

http://10.0.20.60/procurve_login.php

The *Submit URL* is made up of the IP Address of the HP ProCurve MSM, the port number used for HTTP authentication and a URL suffix defined by HP ProCurve to be:

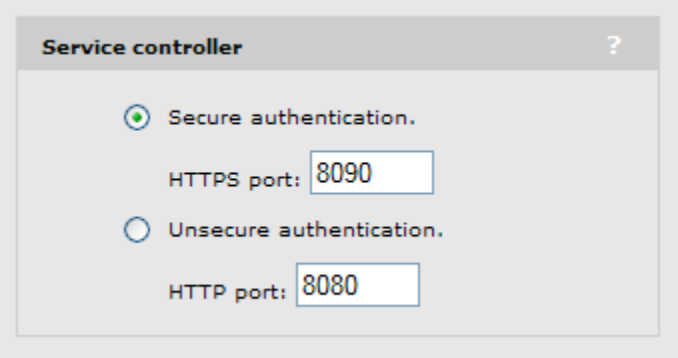
/goform/HtmlLoginRequest

Ensure the *Submit Method* is set to POST.



By default the HP ProCurve MSM710 uses port 8080 for unsecured HTML authentication and 8090 for secure HTML authentication. Depending on your sites use of Proxy Servers these ports may not be appropriate and may need to be modified. These settings can be reviewed in the MSM configuration under *Service Controller→Public Access→Access Control.* The defaults are shown below in the screenshot from the HP ProCurve MSM Web Management Tool.

This setting has been mentioned at this point of the configuration process as it affects the *Submit URL* that needs to be set in the Web Login configuration shown above. The example shows the default setting of port 8080 being used. Note the <IP-address:port-number> syntax used in URLs above.



The decision to use either secure (https) or non-secure (http) authentication will be determined by what sort of Guest Access you intend to provide. If you are providing credit card based billable Guest Access then the expectation would be that all transactions would be secure and protected by a https session. On the other hand if you are running a Free Hotspot this may not be as much of a concern.

Make sure you select the *Skin* that you would like presented as the branding for the Captive Portal page and set the Title of the Web Login so it is displayed correctly in the user's browser.

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 - Review to Web Login Captive Portal page

Returning to the *Web Logins* page, select the *HP ProCurve MSM Login* entry and Click the *Test* button and in a new window the configured captive portal page will be displayed as shown below:

Click the Back button in the web browser to return to the amigopod configuration screen.

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 Web Portal settings on the HP ProCurve controller. An example of the URL is shown below:

http://10.0.20.60/procurve_login.php

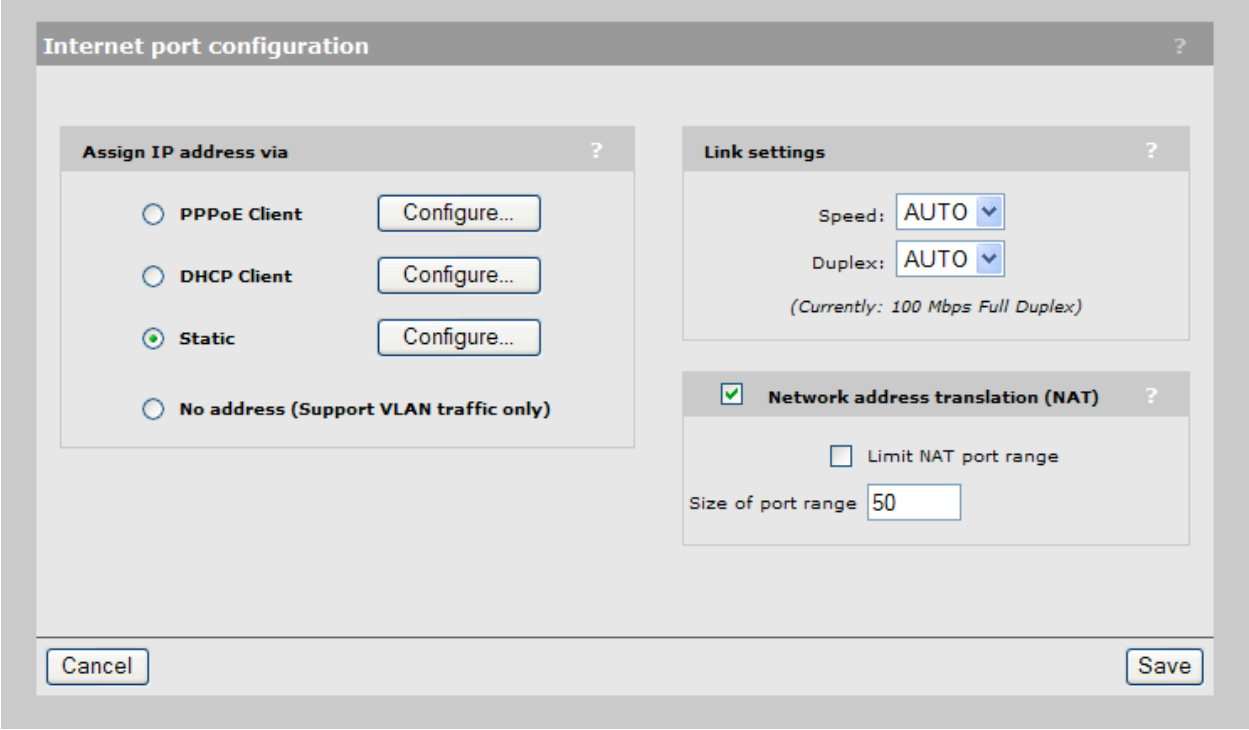
HP ProCurve MSM Configuration

The following configuration procedure assumes that the HP ProCurve MSM710 has been powered up and a basic IP configuration has been applied through the steps detailed in the Getting Started Chapter of the HP ProCurve Admin Guide. 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:

MSM710 IP Address	10.0.20.25
Internet Gateway Address	10.0.20.1
amigopod IP Address	10.0.20.60
amigopod RADIUS port	Auth 1812 Acc 1813 (default settings)

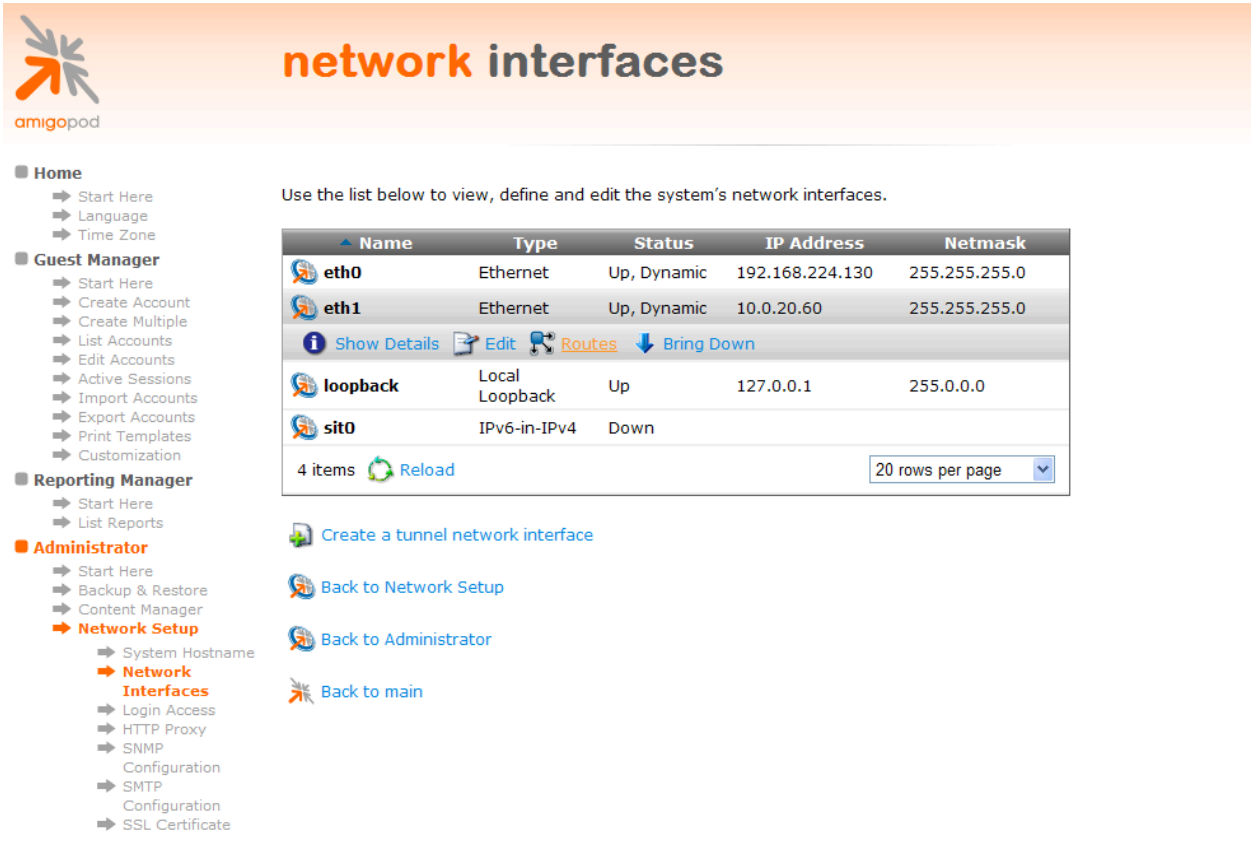
Depending on your network design the MSM710 may need to be configured to perform Network Address Translation (NAT) on the *Internet* port. As can be seen from the previous Lab Topology diagram, to simplify our lab routing environment NAT has been enabled.

If NAT is required in your network design, the MSM NAT settings can be found under *Service Controller→Network→Internet Port* as shown below:

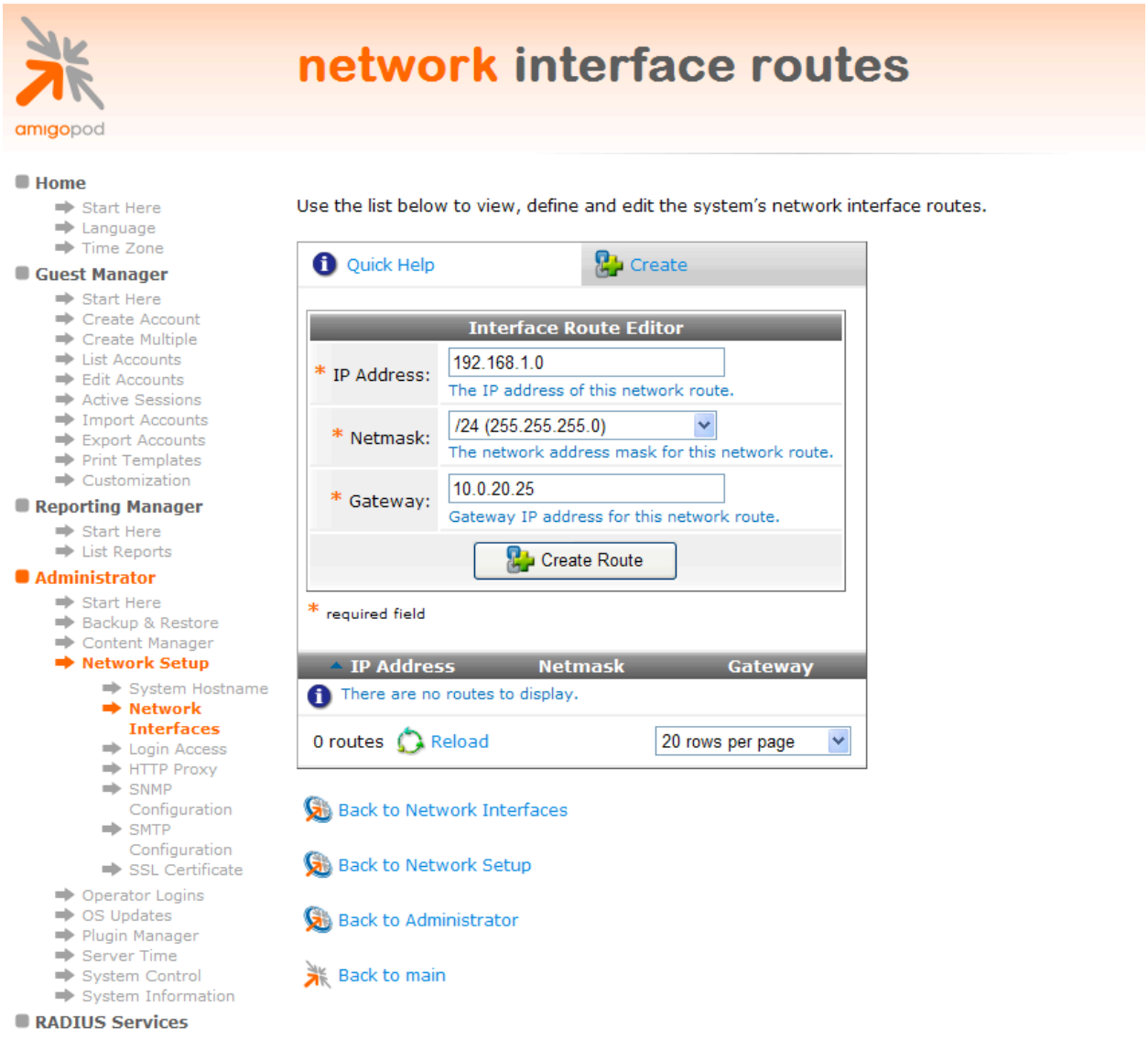


If you intend to run your network in a routed environment you will either need to update your routing tables on the default gateway router that is servicing the network the *Internet port* of the MSM is connected to and / or add a static route to the amigopod configuration.

To add a static route to your amigopod install, browse to the *Administrator→Network Interfaces* menu option and select your active Ethernet adaptor. In our case *eth1* is connected to the local lab network as shown below:

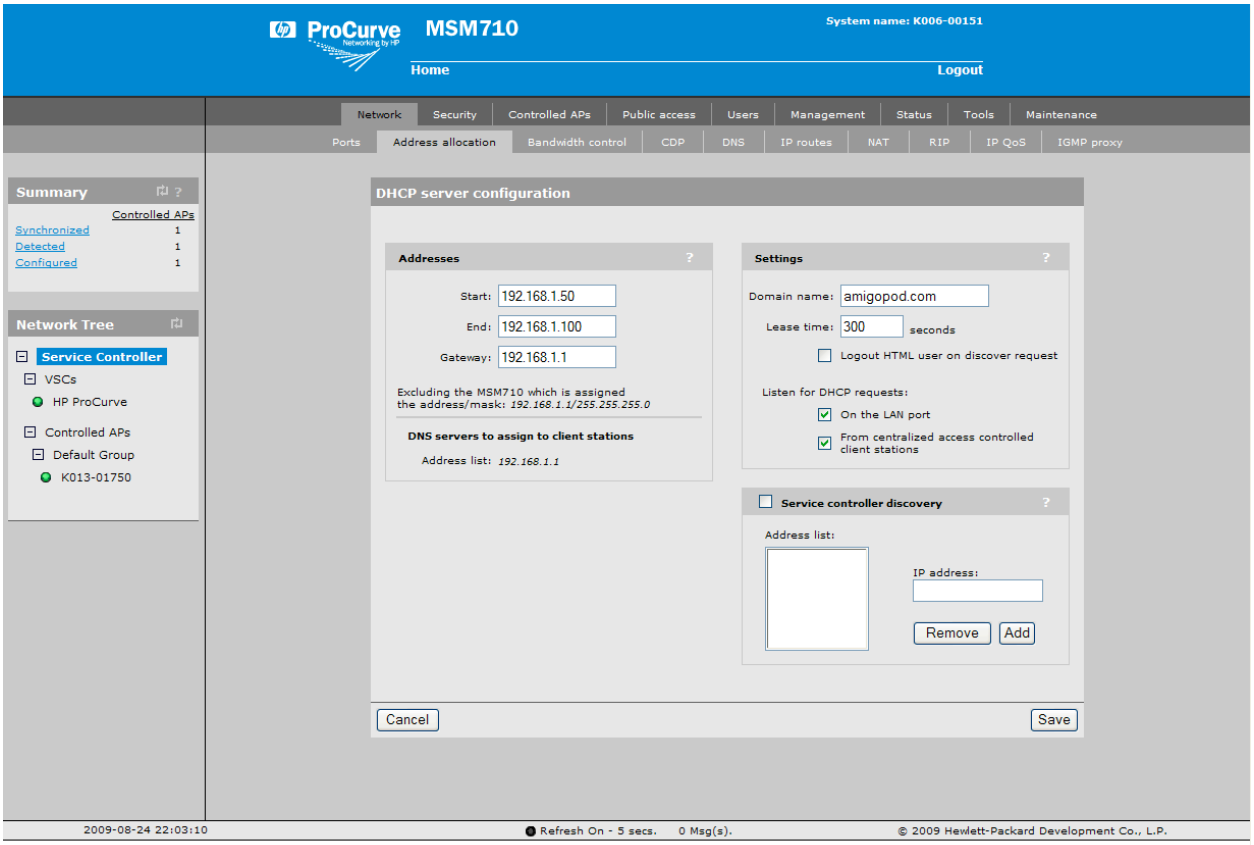


Click on the *Routes* option and add in the details for your IP address range allocated to the *LAN port* on the MSM as shown below:



Step 1 – Enable DHCP on LAN port

In our Lab environment DHCP needs to be enabled on the *LAN port* to provide IP addresses to both the MAP-320 and any wired clients connected to this interface of the MSM710. This is configured under *Service Controller→Networks→Address Allocation* as shown in the following screen shot:

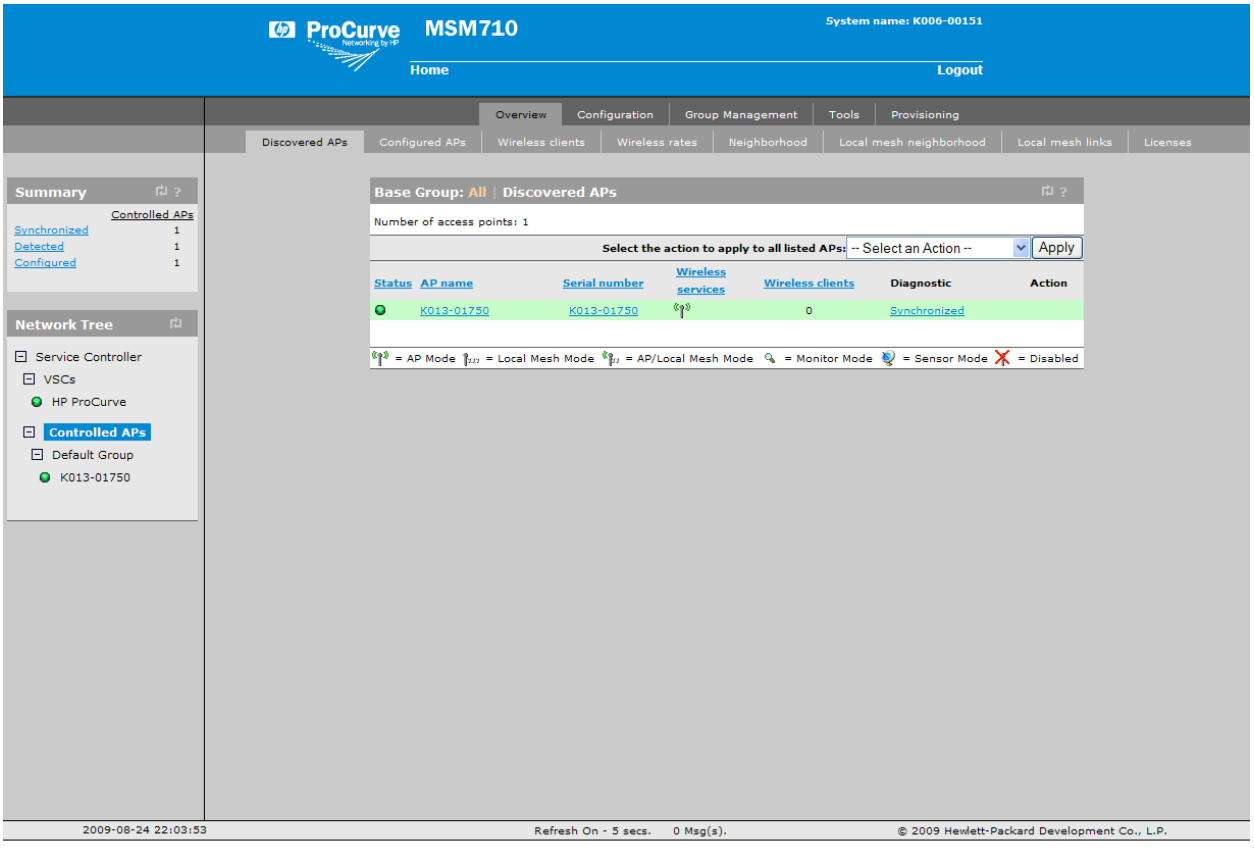


Step 2 – Install HP ProCurve MultiService Access Point (Optional)

Although the HP ProCurve MSM range of controllers are designed primarily for the centralized control of HP ProCurve MulitService Access Points, the controller can be equally used for providing Access Control in pure wired environments.

The many different methods of configuring the *Controlled APs, AP Groups, Virtual Service Community (VSC)* is covered extensively in the HP ProCurve Admin Guide in Chapters 4 & 5 and is therefore considered outside of the scope of this Integration guide. Please refer to the HP ProCurve Admin Guide for further information on these topics and the best method for configuring your wireless environment.

For the lab environment used through the rest of this document, a single MSM320 will be used and configured via the default AP Group and default VSC. As can be seen from the screenshot below the MSM320 has been successfully detected, configured and synchronized with the MSM710 and is available to start serving wireless clients.

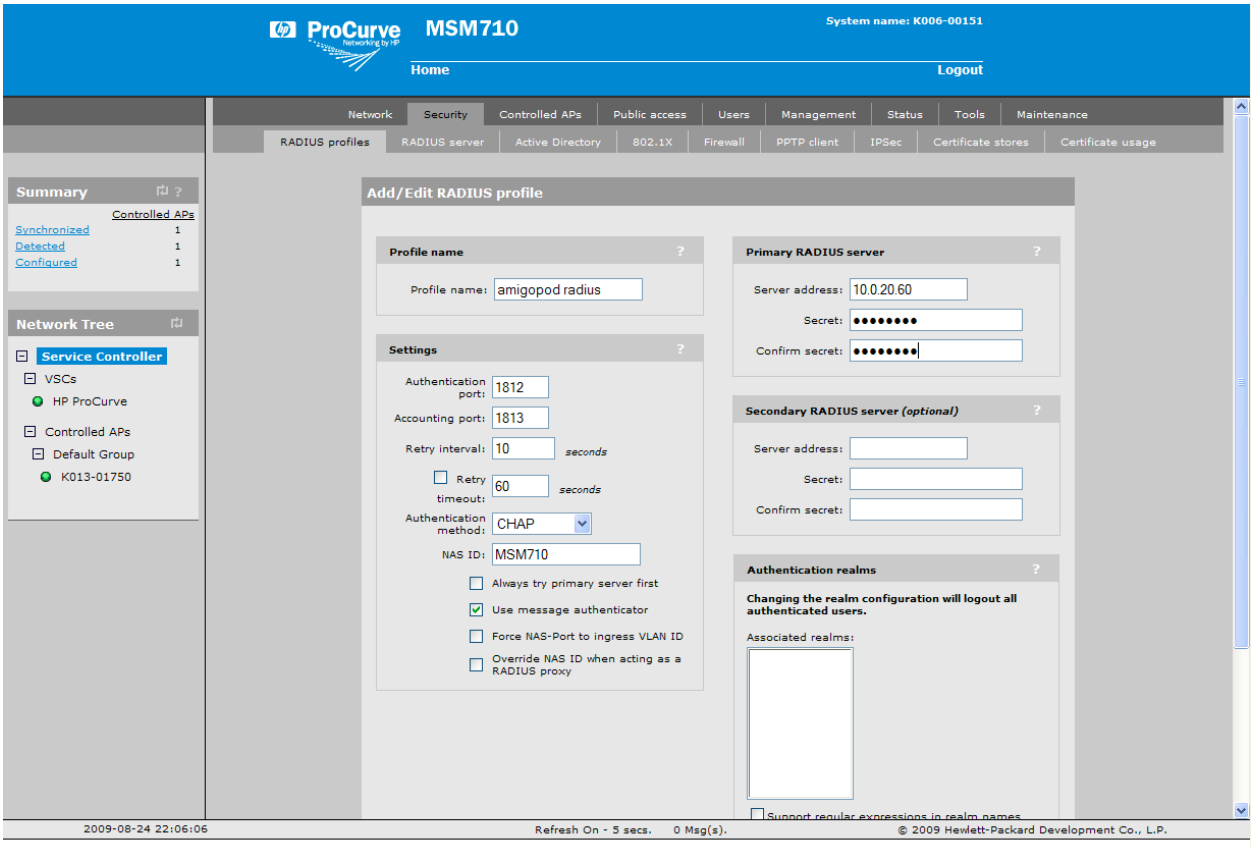


Step 3- Create RADIUS Definition for amigopod

From the *Service Controller→Security→RADIUS Profiles* screen click the *Add New Profile …* button. In the following screen be sure to enter and confirm the following details:

- Enter a descriptive name for the *Profile Name*
- Confirm the default setting of 1812 & 1813 for the *Authentication & Accounting Port*
- Select CHAP for the *Authentication Method*
- Enter a descriptive name for the *NAS ID*
- Under *Primary RAIUS Server* enter the IP address of the amigopod & the *Secret*
- The remaining defaults should be adequate for most installs.

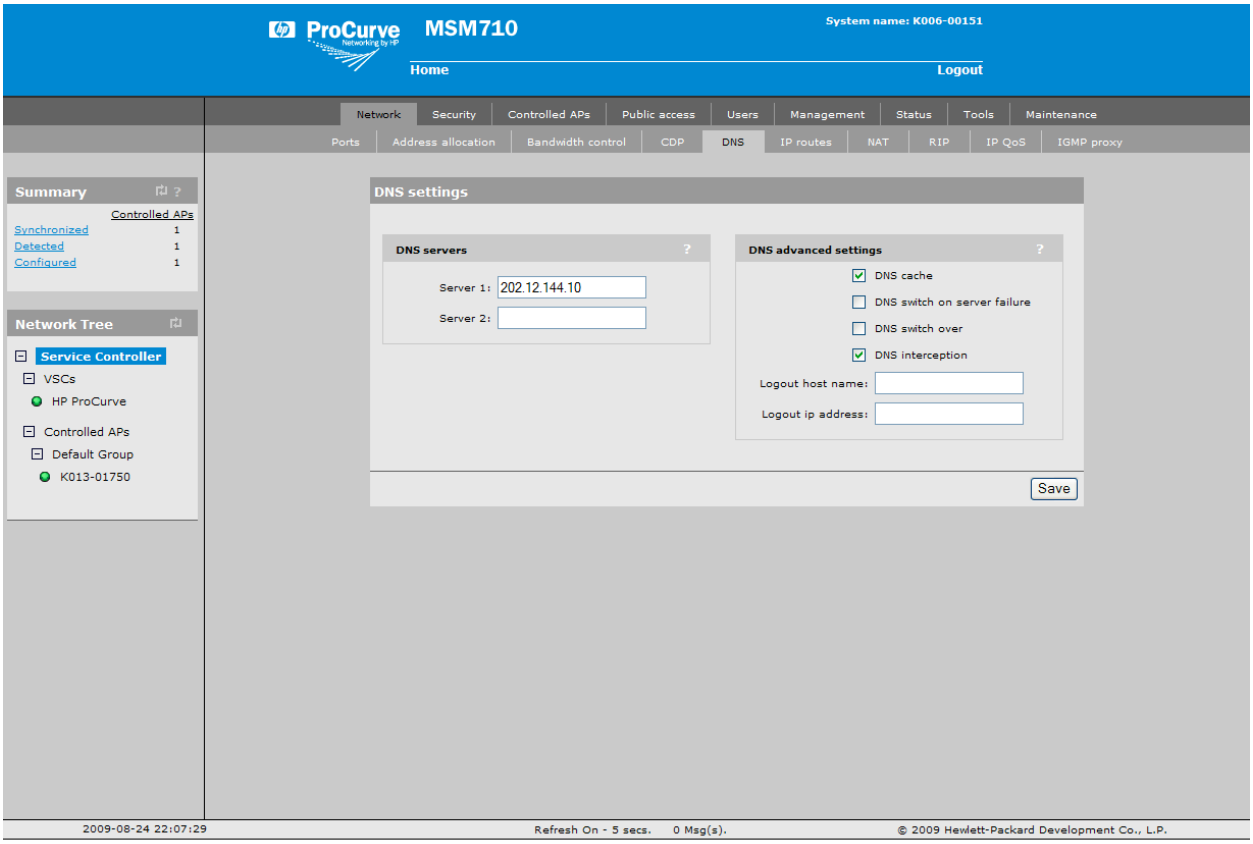
Be sure to Save the changes by clicking on the *Save* button on the bottom right hand side of the page.



Note: The *Secret* above needs to be the same as the one defined in Step 1 of the amigopod configuration. For example, ***wireless***.

Step 4 – DNS Proxy & Interception configuration

In order for the MSM to be able to intercept and redirect any new Guest users to the amigopod hosted Web Login page, the controller must get involved in the DNS resolution process of these users. The MSM DNS configuration allows the definition of upstream DNS servers along with the enablement of *DNS Proxy* & *DNS Interception* required to perform these redirects as shown in the screen capture below:



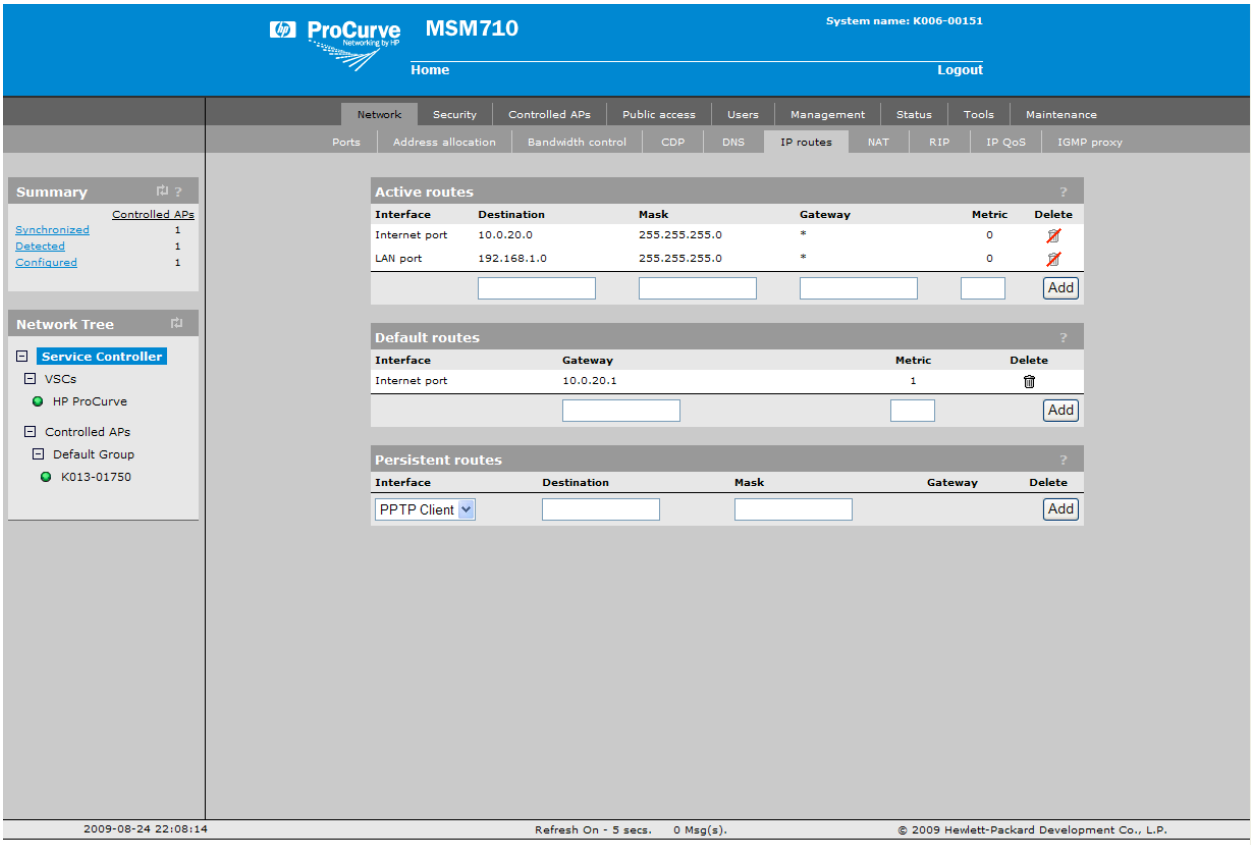
Without the *DNS Proxy* feature enabled attempts by Guest users to resolve globally unknown hosts and domain names typically used in corporate Intranet environments would fail. This DNS resolution failure would lead to the Guest user's browser never attempting a HTTP transaction and hence the MSM would not be able to redirect the client's session to the amigopod Web Login page.

Based on this you can see the DNS configuration is a critical component in the successful user experience for Guest access.

Step 5 - Add Default Route for MSM

As with all Layer 3 networking devices, the MSM needs to be configured or learn via a Dynamic routing protocol is gateway to use for all non local traffic. Without this default route in place the Guest users will not be able to access the Internet.

As shown in the screen capture below a simple *Default Route* has been added to MSM config by accessing the *IP Routes* configuration page under *Service Controller→Network.*

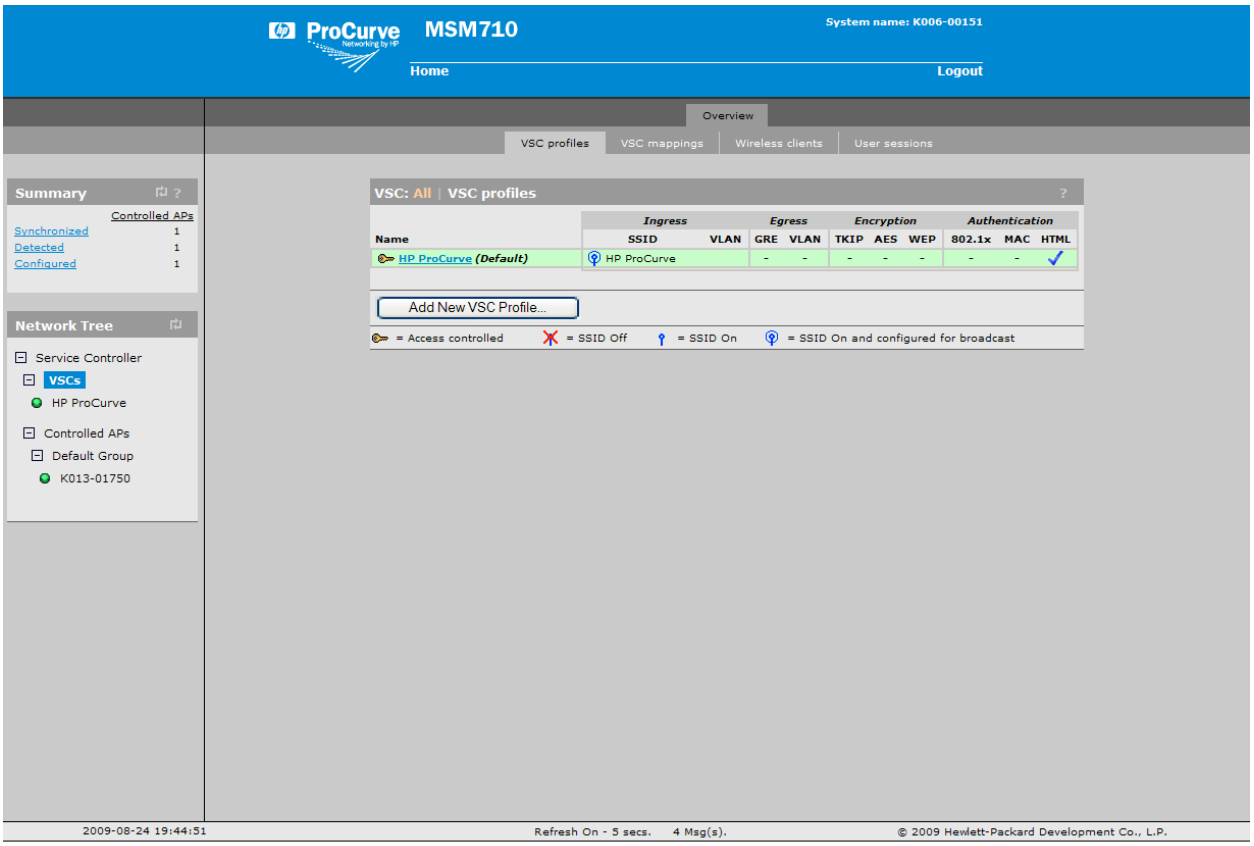


Step 6 – Configure the Default VSC

A Virtual Service Community is defined by HP ProCurve as a collection of configuration settings that define key operating characteristics of the service controller and controlled APs. In most cases. A VSC is used to define the characteristics of a wireless network.

The VSC configuration can be accessed from the left hand pane of the Management Tool by clicking on the + sign next to the *Service Controller* option. You will then be able to see the default VSC available on the controller.

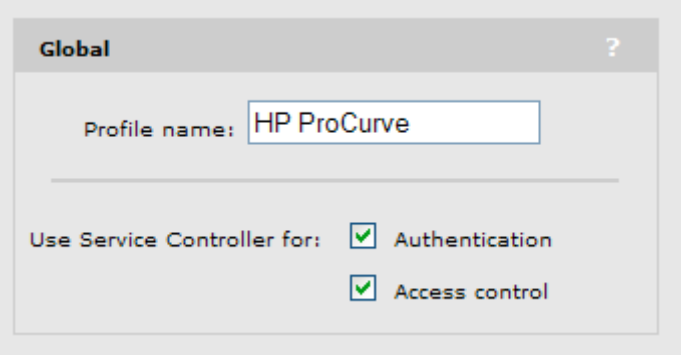
As you can see from the default settings shown below, both the VSC name and SSID for the wireless is set to *HP ProCurve*. Obviously if the MSM is being used to control wired traffic only access then the SSID is of little interest.



There are several other configuration settings within the VSC that are critical to the functioning of this Guest access design. To make these changes enter into the default VSC configuration by clicking on the *HP ProCurve* option below the VSC container.

VSC Global Configuration

Under the *Global* Configuration the name of the VSC can be changed to suit your deployment. In our case we are going to leave it as the default of *HP ProCurve Networks.* More importantly the options of both *Authentication* & *Access Control* need to be enabled to support the HTML based authentication required for Guest Access.



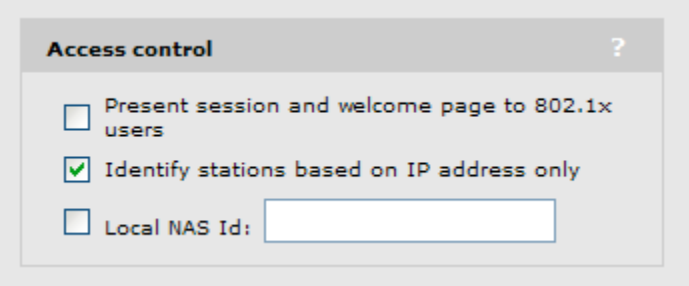
For more information on both of these options please refer to the HP ProCurve Admin Guide Chapter 5 on VSCs.

VSC Access Control Configuration

Under the *Access Control* section there is a critical option that often needs to be enabled in a wired authentication model. The *Identify stations based on IP address only* is useful when the MSM is not deployed with direct Layer 2 adjacency to the Guest Users.

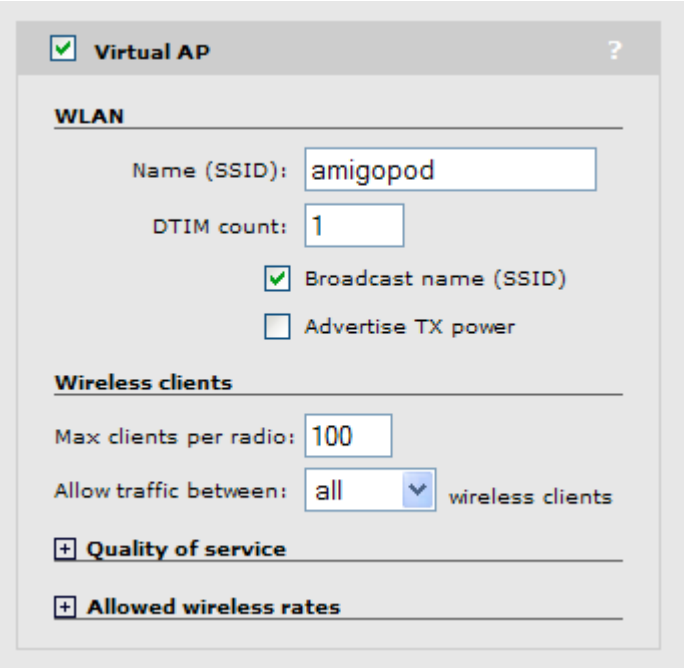
For example, if your MSM was deployed in the centre of a routed Layer 3 network and some Guest traffic was arriving on the MSM LAN port after traversing these routed connections, all Layer 2 MAC address visibility would be lost. Essentially the Layer 2 rewrite functionality of the routers would make all Guest Users appear to be coming from the same MAC address (the router's outbound interface) and therefore the MSM would not be able to differentiate between them from security or session control.

Therefore is feature is extremely powerful in these centralized or highly routed designs.

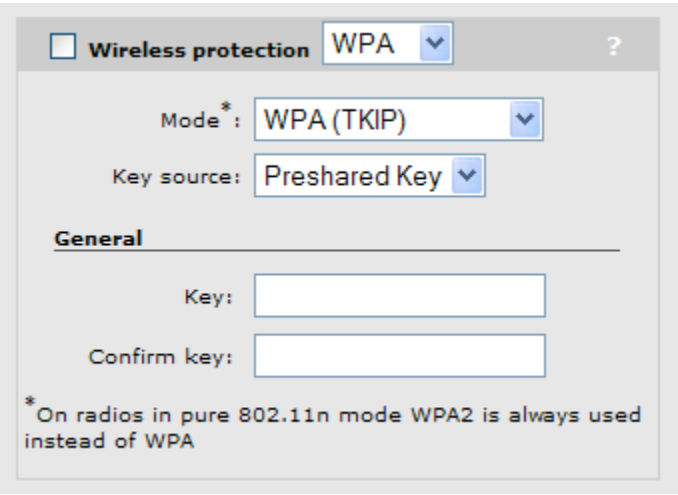


VSC Virtual AP Configuration

Under the *Virtual AP* configuration all of the wireless specific settings can be modified to suit your deployment. For our simple test environment we will only be modifying the SSID to be *amigopod*. All other defaults will be left as is and will need to be modified for each design based on site specific criteria.

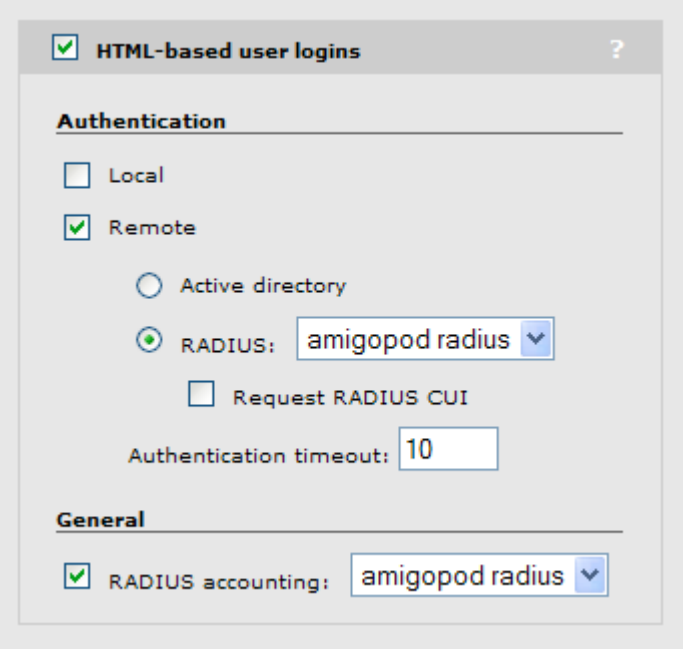


To keep the Guest Access example simple, we have also elected to not enable any of the *Wireless Protection* features in the test environment. Again depending on your environment and wireless design this may not be an appropriate setting for Guest Wireless Access.



VSC HTML Based User Logins Configuration

Under the *HTML Based User Logins Configuration* section the *Authentication* option must be set to *Remote* and configured to point as the *RADIUS* entry created in the previous step above. Also the *RADIUS Accounting* option must also be configured to point at the amigopod RADIUS definition created previously as shown below:

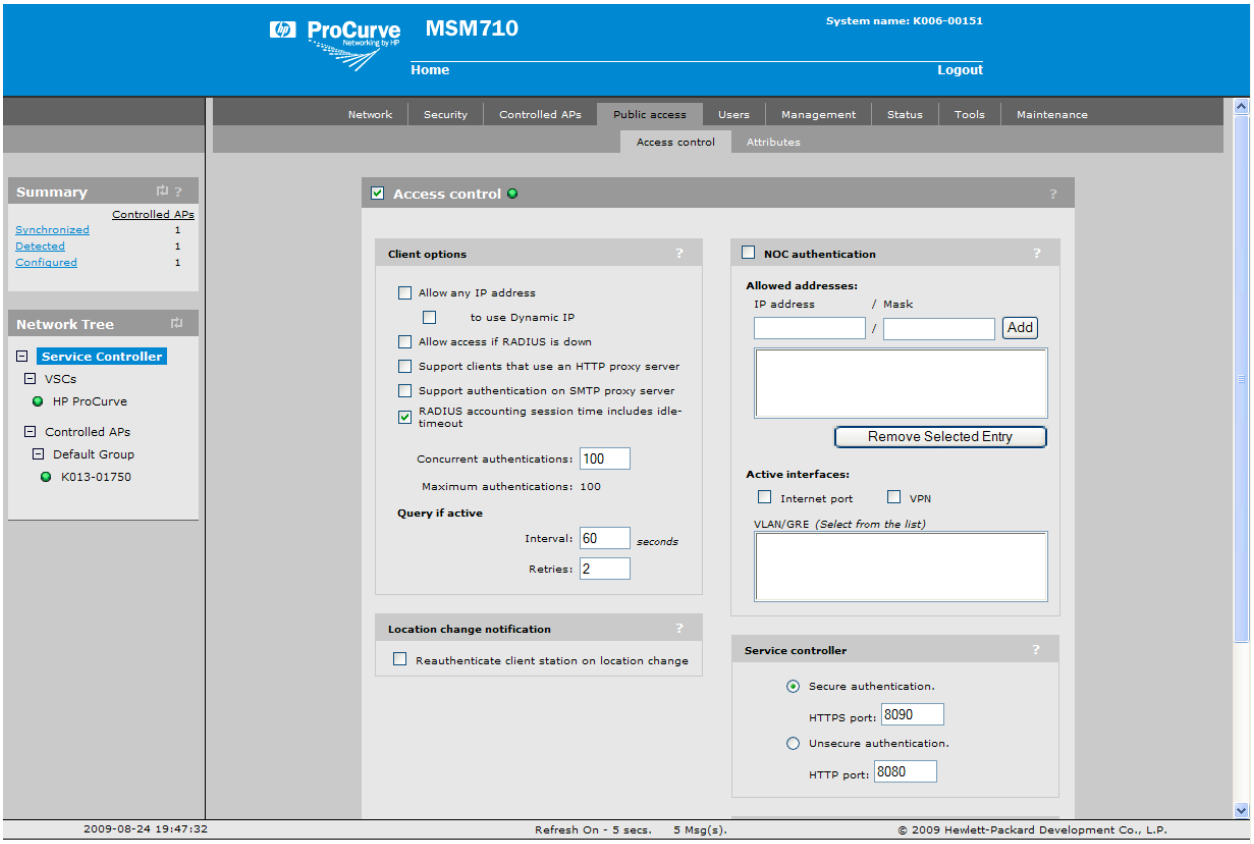


All remaining *VSC* configuration options can be left as their defaults.

Be sure to save all of these changes by clicking on the *Save* button at the bottom right hna sie of the screen.

Step 7 – Public Access Configuration

Returning to the *Service Controller* configuration section of the Management Tool, select the *Public Access* menu option and the following screen will be displayed.

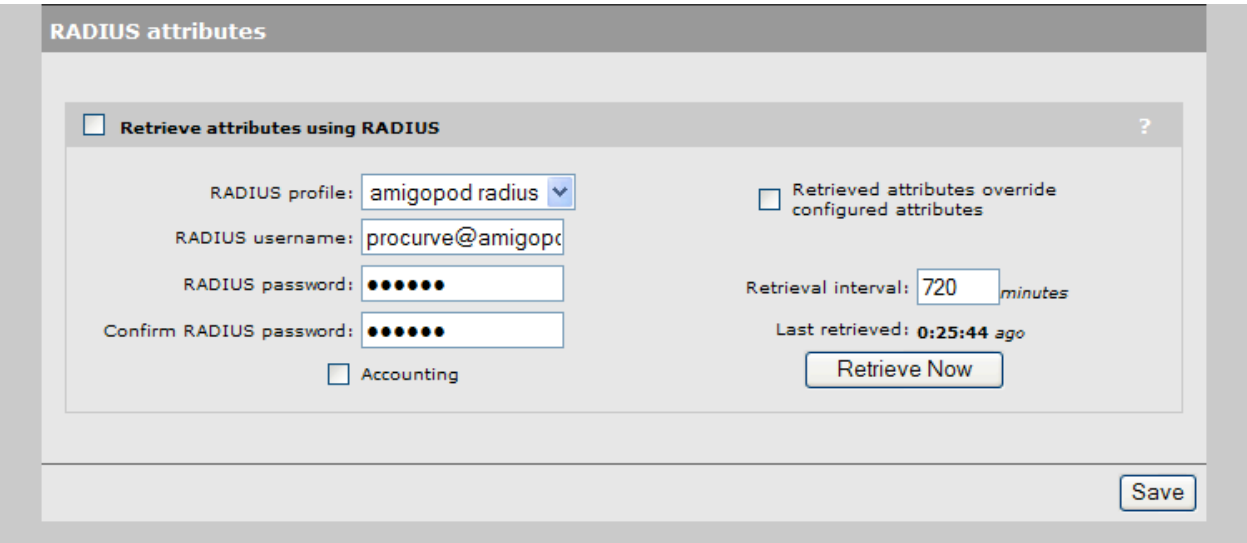


There are various configuration options on this screen that will be unique to your deployment design including the *Secure* & *Unsecure authentication* ports mentioned in Step 3 of the amigopod configuration. Please refer to the HP ProCurve Network Access Guide for more information on the *Client Options* & *NOC authentication* features to see if they are applicable for your network design.

Step 8 – Public Access Attributes

Under the *Public Access→Attributes* configuration screen is where all of the major integration points between the MSM and amigopod (excluding the RADIUS configuration already covered) are setup. These *Attributes* can either being configured manually directly on this screen or be dynamically provisioned via RADIUS in a larger centralized management configuration.

For the simplicity of the test environment we will configure the attributes locally through this configuration page but an example of the RADIUS account that could be defined on the amigopod will be included in Appendix A of this document. In the screen capture below you can see the settings required to retrieve the *Public Access Attributes* configuration from the external amigopod defined RADIUS server.



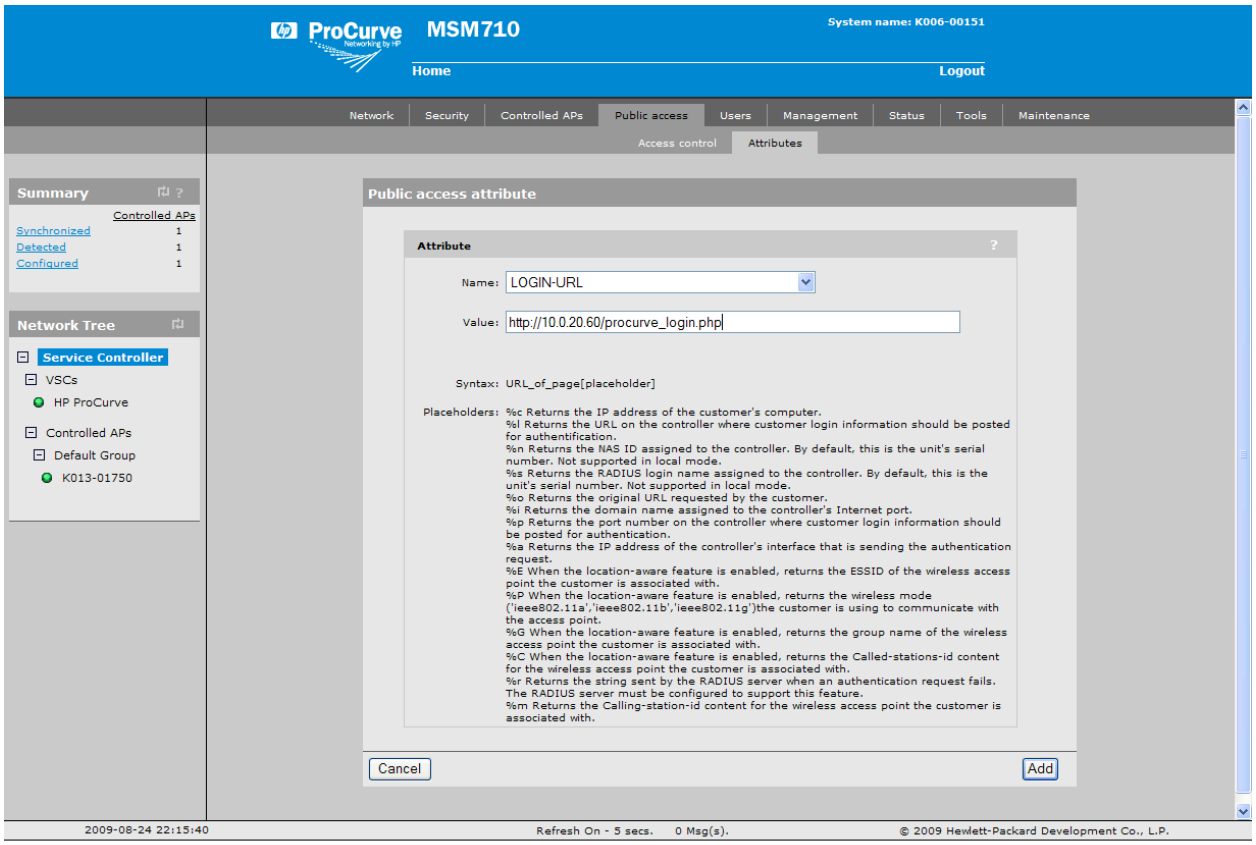
Define Login URL destination

In order for the MSM to redirect new Guest users to the amigopod Web Login page we need to define a *LOGIN-URL* that points to the Web Login page we defined in Step 4 of the amigopod configuration above.

For reference the URL we defined in the previous configuration of this integration guide was:

http://10.0.20.60/procurve_login.php

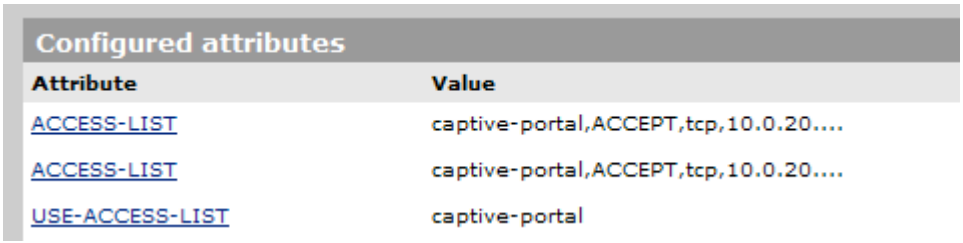
From the *Public Access→Attributes* configuration page click on the *Add New Attribute …* button and select *LOGIN-URL* the drop-down box as shown below:



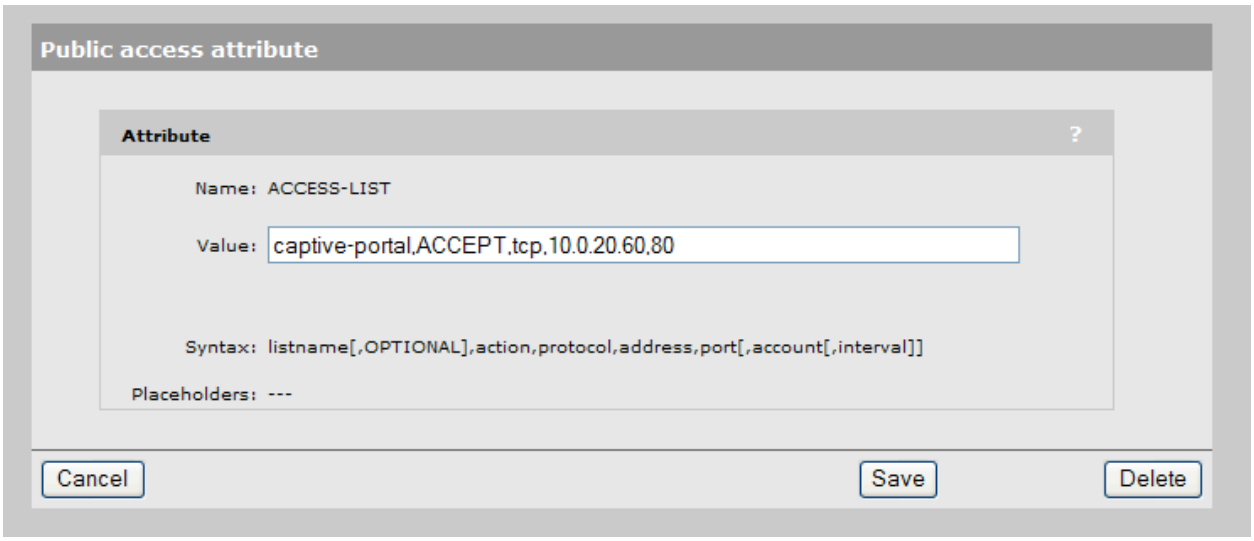
Enter the URL from the previous step and click the *Save* button to commit the changes to the *Public Access Attributes.*

Access List Configuration

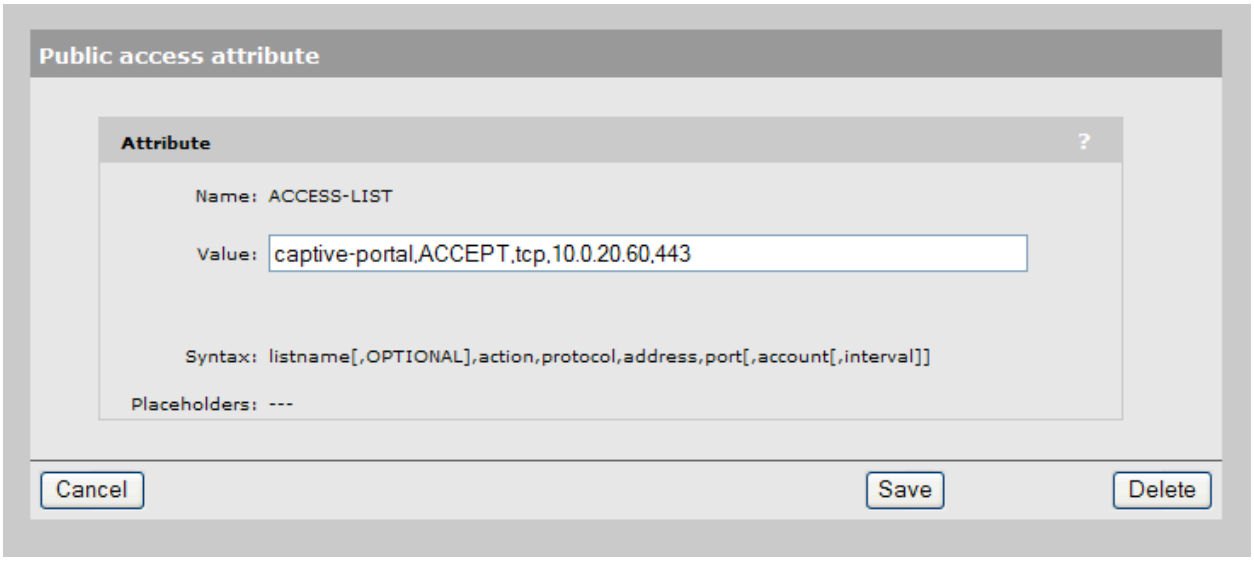
An Access List must be defined and enabled to permit the HTTP authentication traffic reaching the amigopod Web Login interface. The following screenshot shows the entries created in our lab environment to permit both HTTP (port 80) and HTTPS (port 443) traffic to the amigopod from unauthenticated Guest users:



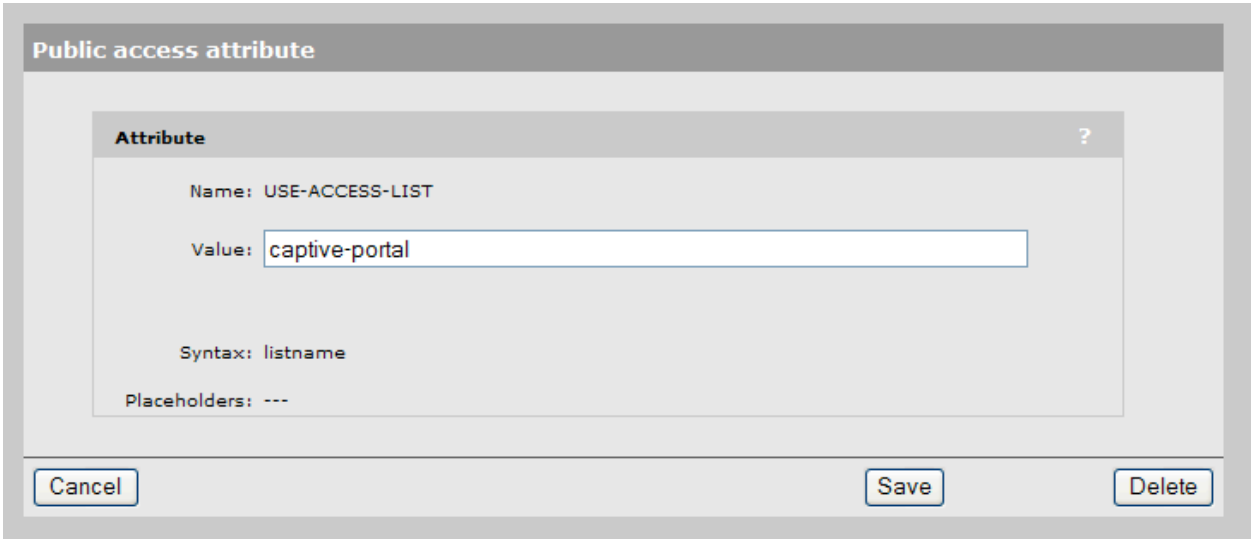
Firstly we need to permit HTTP traffic to the amigopod. In this example we have used *captive-portal* as the name for the Access List.



Optionally we have added support for HTTPS in event that we might want to configure secure login pages to protect username and password credentials or potentially credit card details in a Hotspot configuration.



Finally now that we have created the Access List we need to apply it so it takes affect on the *Public Access* interface.



(Optional) User Experience Customisation

Referring to the HP ProCurve Network Access Guide there are several other attributes that can be changed to influence the user experience for your Guest users.

In particular you might wish to investigate the following in more detail:

- LOGO
- TRANSPORT-PAGE
- SESSION-PAGE
- FAIL-PAGE

Modified versions of these pages can be hosted on the amigopod by uploading your site specific versions via the *Administrator→Content Manager* menu option. Once uploaded to the amigopod you can reference these files in the /public directory of the amigopod.

For example, if you wished to change the logo displayed on the default transport and session pages you would update the *LOGO* attribute to equal:

```
http://<IP address of amigopod>/public/<name of new logo file>
```

(Optional) Modify default user session limits

Again referencing the HP ProCurve Network Access Guide you may also want to set some default constraints around your Guest Access sessions. These defaults can be applied or individually defined per user on the amigopod based on the returned RADIUS attributes defined in *RADIUS Services→User Roles.*

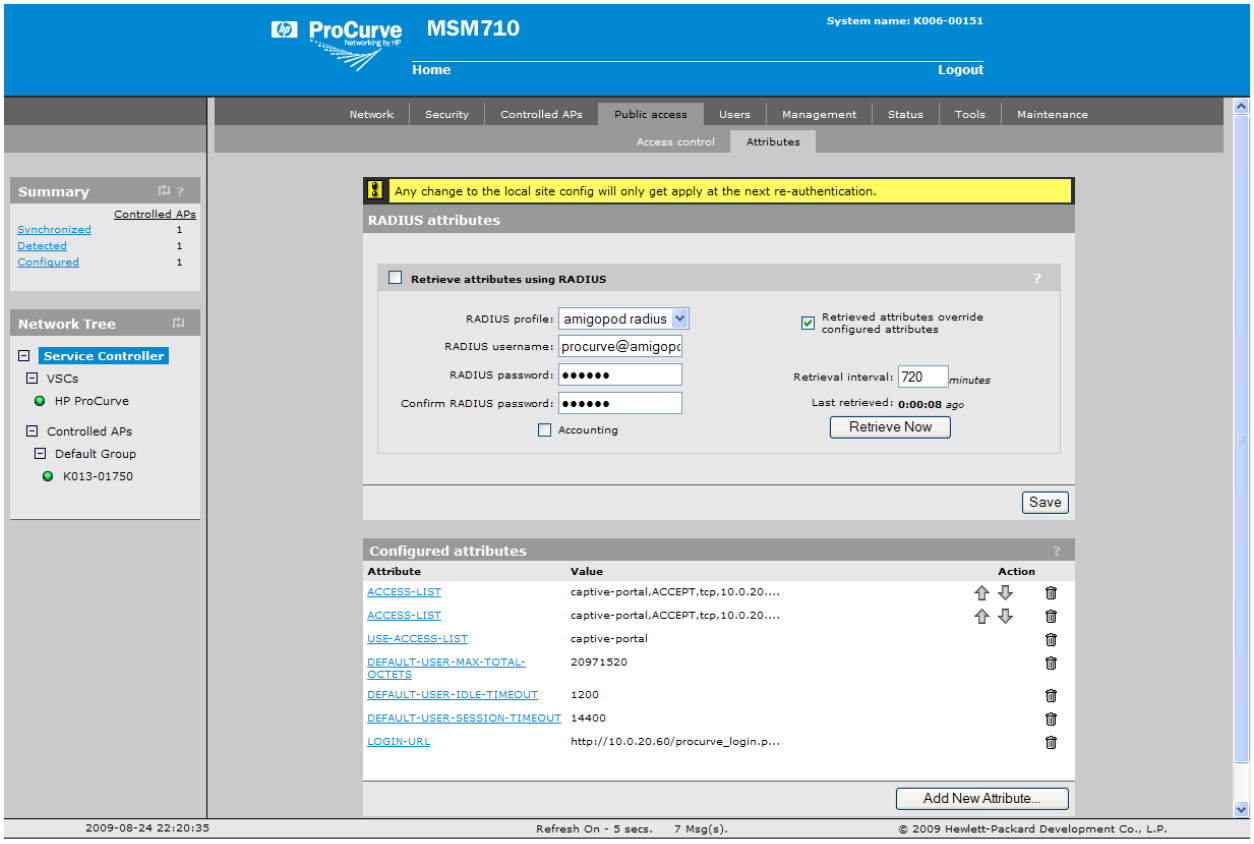
Below are some examples of attributes that can control the Guest user's session and some sample settings which can be modified to suit your deployment.

DEFAULT-USER-MAX-TOTAL-OCTETS	20971520
DEFAULT-USER-IDLE-TIMEOUT	1200
DEFAULT-USER-SESSION-TIMEOUT	14400

In the above example the user's session will be subject to the following constraints assuming more specific user based constraints haven't been applied by amigopod configured user attributes:

- 20Mb of total traffic (1024 octets * 1024(MB) * 20)
- Idle timeout of 20mins
- Session timeout of 4 hours

Once all of these changes have been completed you should be left with an *Attributes* page looking something like the following one.



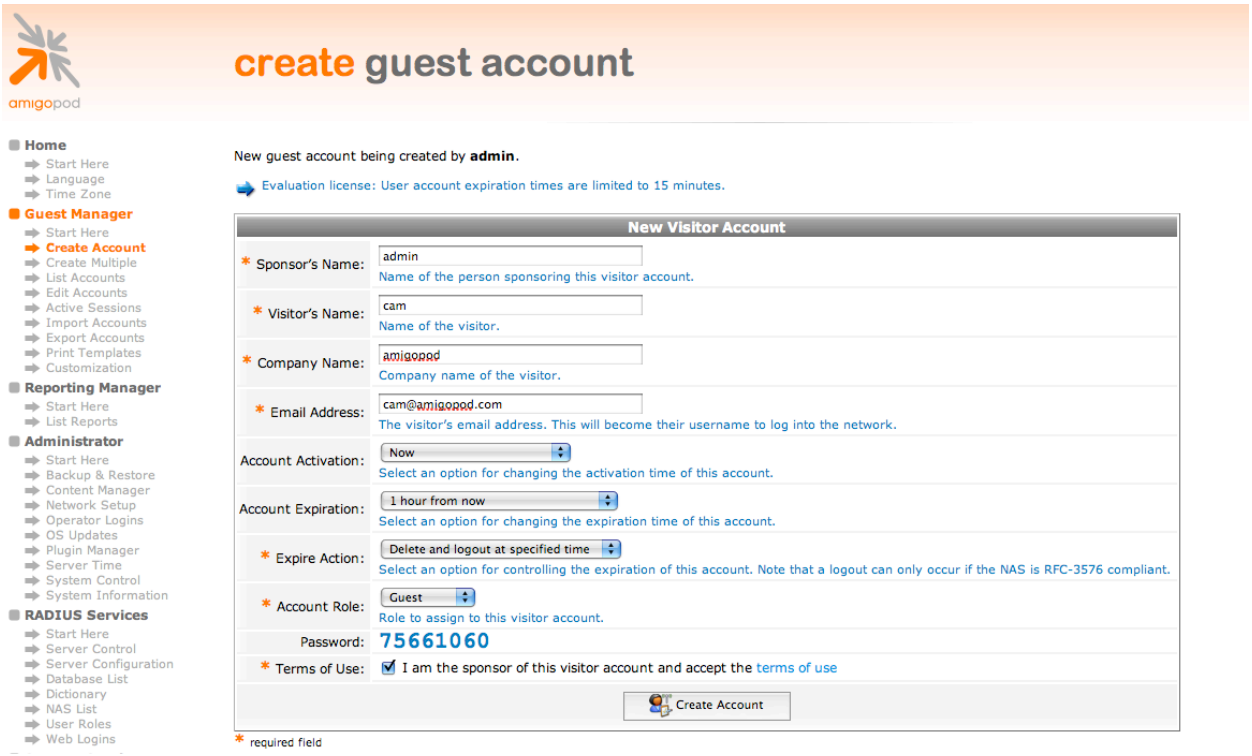
Click the *Save* button for these changes to be committed to the *Public Access* configuration.

Testing the Configuration

Now that the configuration of both the HP ProCurve Controller and the amigopod solution is complete, the following steps can be followed to verify the setup.

Step 1 – 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.



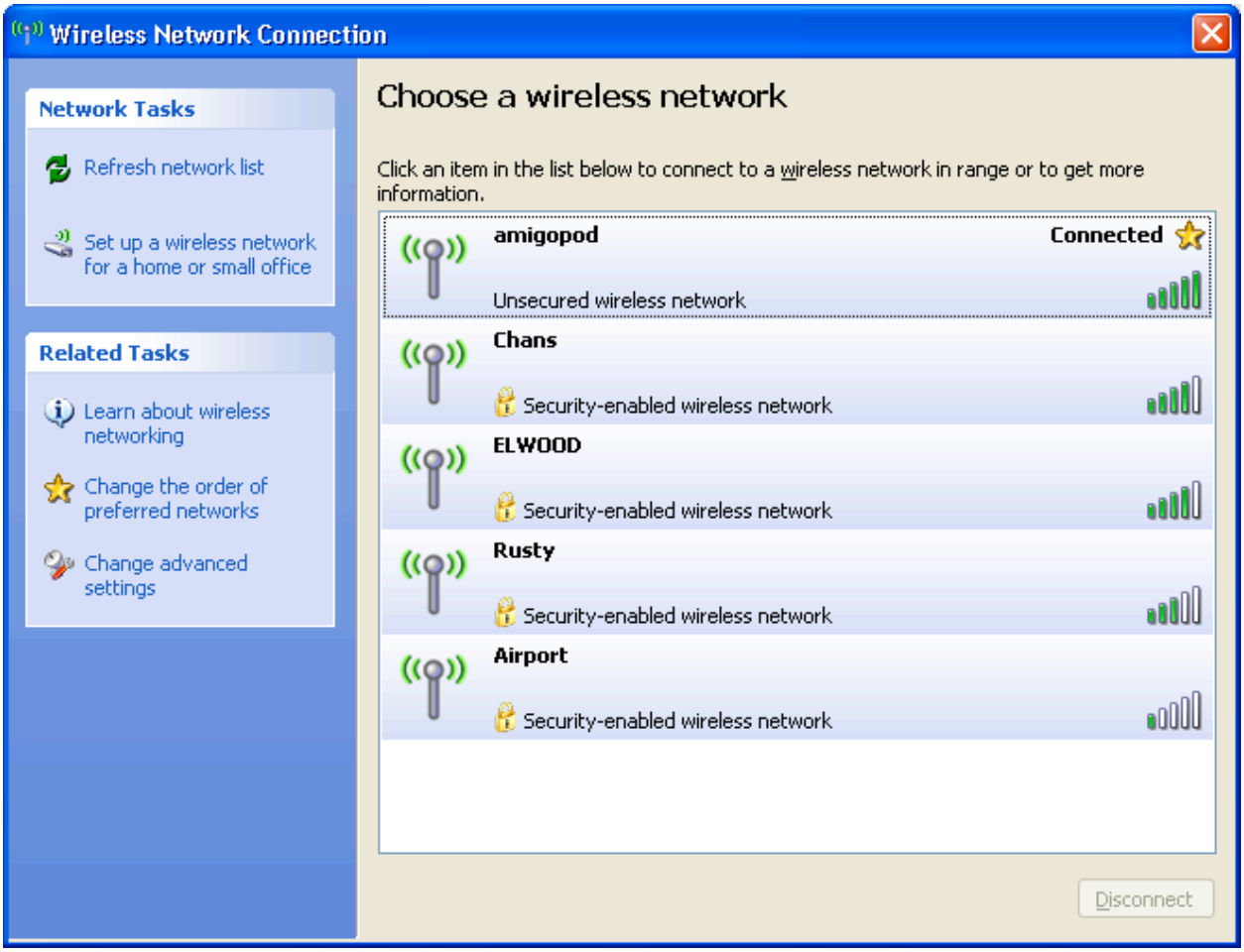
Note: Make note of the randomly generated *Visitor Password* as this will be required during the integration testing. If this password is proving difficult to remember during testing you can use the *List guest accounts* option on the screen to then edit the account and change the password to a more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

For simplicity during our testing we took this option and changed the username to ***cam*** and password to ***wireless.*** All subsequent screenshots and debugs will reflect this change.

Step 2 - 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 HP ProCurve Controller and potentially source a second wireless test device to see if the problem is laptop specific.



Step 2 – Confirm DHCP IP Address received

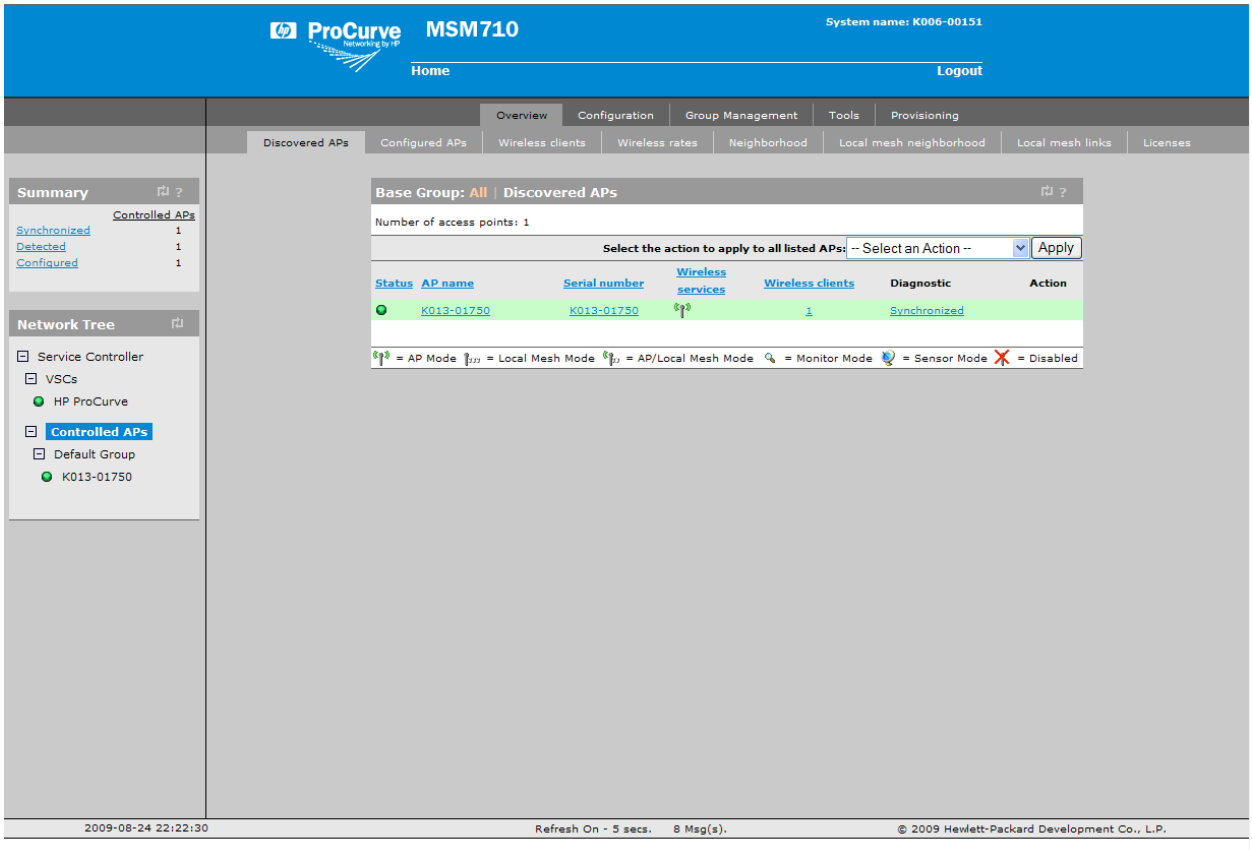
Using the Windows Command Prompt or equivalent in the chosen operating system, confirm that a valid IP Address has been received from the DHCP server configured on the HP ProCurve Controller.

Issue the *ipconfig* command from the Windows Command Prompt to display the IP information received from the DHCP process. By checking on the Wireless adaptor you should be able to confirm an IP Address in the range of *192.168.1.x* has been received.

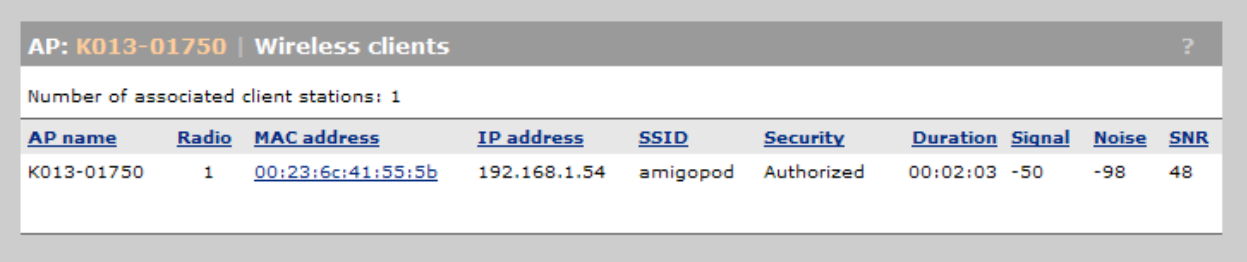
Note: On Mac OS X and Linux operating system variants use a Terminal window and enter the *ifconfig* command to display the same information.

Step 3 – Confirm session detected by HP ProCurve Controller

Once you have received an IP address, the HP ProCurve controller should have entry shown under the *Controlled APs* section of the Management Tool as shown below:



By clicking on the entry for *Wireless Clients* on the screen shown above you will be presented with a more detailed view of the wireless client's statistics along with the IP address allocated via DHCP.



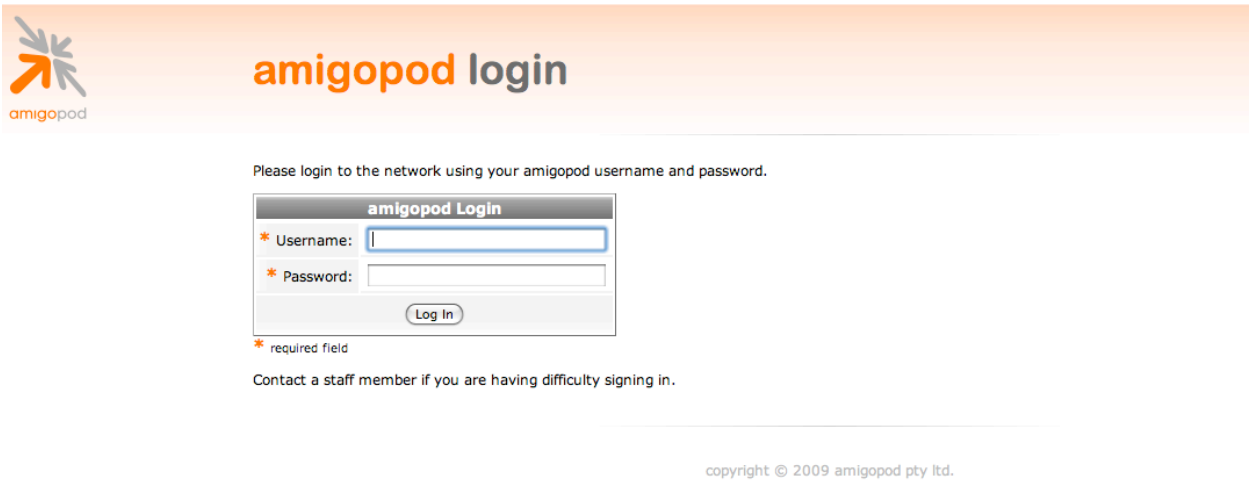
AP: K013-01750 | Wireless clients

Number of associated client stations: 1

AP name	Radio	MAC address	IP address	SSID	Security	Duration	Signal	Noise	SNR
K013-01750	1	00:23:6c:41:55:5b	192.168.1.54	amigopod	Authorized	00:02:03	-50	-98	48

Step 4 – Launch Web Browser and login

When the web browser on the test laptop is launched the MSM will automatically capture the session and redirect the user to the amigopod hosted login page as shown below (which was defined in the *Public Access LOGIN-URL*)



Enter the test user details entered and recorded in Step 1 above and click the *Login* button.

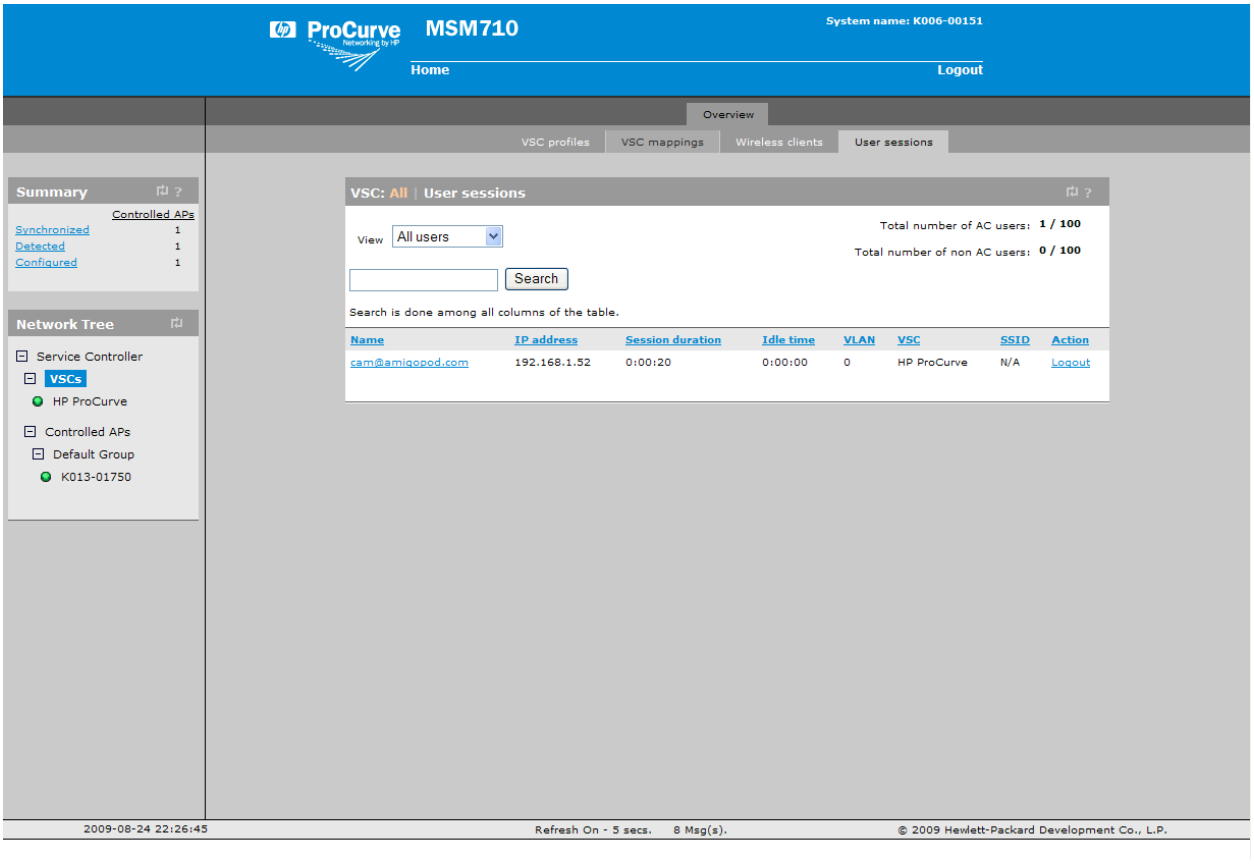
At this point the test user should be successfully authenticated and allowed to transit through the controller and onto the Internet or Corporate network.

Note: If the web browser fails to redirect check that the DNS server configured in the base Trapeze configured defined before Step 1 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 HP ProCurve controller 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

Step 5 - Confirm the login successful from MSM

From the *VSC→User Sessions* tab you will be able to monitor the number and details of authenticated Guest access sessions at any given time. From this interface you also have to option to *Logout* a user from the *Action* column of the table shown below:



Step 6 - 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, *cam@amigopod.com*.

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

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. The following output is an example from the RADIUS debugs for this transaction:

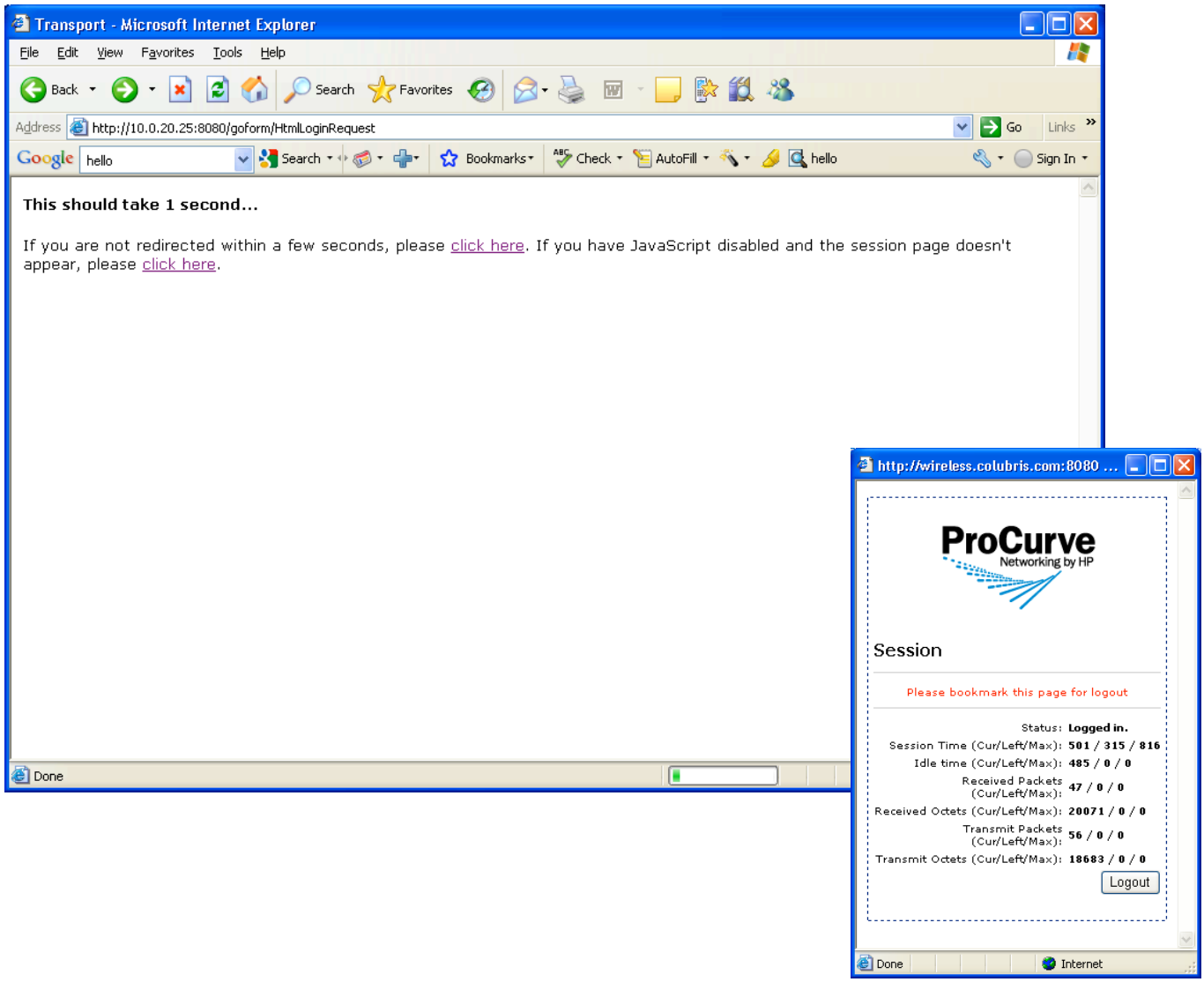
```
Ready to process requests.
rad_recv: Access-Request packet from host 10.0.20.25:32771, id=34, length=220
Acct-Session-Id = "0f5b51ca"
NAS-Port = 1
NAS-Port-Type = Wireless-802.11
User-Name = "cam@amigopod.com"
Calling-Station-Id = "00-0A-E4-04-68-FD"
Called-Station-Id = "00-03-52-09-14-C5"
Framed-IP-Address = 192.168.1.52
```

```
CHAP-Password = 0x2204f280159f4832107bd2c8ad87f36ccb
CHAP-Challenge = 0xe9c9d7c59c932a46d5f4db2a02dfd124
NAS-Identifier = "MSM710"
NAS-IP-Address = 10.0.20.25
Framed-MTU = 1496
Connect-Info = "HTTPS"
Service-Type = Framed-User
Colubris-AVPair = "vsc-name=HP ProCurve"
Message-Authenticator = 0x3967060fe0ff01cfc5b0661e2f2c51b4
rlm_chap: Setting 'Auth-Type := CHAP'
rlm_sql (sql): Reserving sql socket id: 3
rlm_sql_postgresql: query: SELECT id, UserName, Attribute, Value, Op FROM radcheck
WHERE Username='cam@amigopod.com' ORDER BY id
rlm_sql_postgresql: Status: PGRES_TUPLES_OK
rlm_sql_postgresql: affected rows =
rlm_sql_postgresql: query: SELECT radgroupcheck.id, radgroupcheck.GroupName,
radgroupcheck.Attribute, radgroupcheck.Value,radgroupcheck.Op ??FROM radgroupcheck,
usergroup WHERE usergroup.Username = 'cam@amigopod.com' AND usergroup.GroupName =
radgroupcheck.GroupName ??ORDER BY radgroupcheck.id
rlm_sql_postgresql: Status: PGRES_TUPLES_OK
rlm_sql_postgresql: affected rows =
rlm_sql_postgresql: query: SELECT id, UserName, Attribute, Value, Op FROM radreply
WHERE Username='cam@amigopod.com' ORDER BY id
rlm_sql_postgresql: Status: PGRES_TUPLES_OK
rlm_sql_postgresql: affected rows =
rlm_sql_postgresql: query: SELECT radgroupreply.id, radgroupreply.GroupName,
radgroupreply.Attribute, radgroupreply.Value, radgroupreply.Op ??FROM
radgroupreply,usergroup WHERE usergroup.Username = 'cam@amigopod.com' AND
usergroup.GroupName = radgroupreply.GroupName ??ORDER BY radgroupreply.id
rlm_sql_postgresql: Status: PGRES_TUPLES_OK
rlm_sql_postgresql: affected rows =
rlm_sql (sql): Released sql socket id: 3
rlm_chap: login attempt by "cam@amigopod.com" with CHAP password
rlm_chap: Using clear text password wireless for user cam@amigopod.com authentication.
rlm_chap: chap user cam@amigopod.com authenticated succesfully
Exec-Program: /usr/bin/php /opt/amigopod/www/amigopod_request.php 2 16
Exec-Program-Wait: value-pairs: Reply-Message = "Guest", Session-Timeout = 610,
Exec-Program: returned: 0
Login OK: [cam@amigopod.com] (from client MSM-710 port 1 cli 00-0A-E4-04-68-FD)
rlm_sql (sql): Processing sql_postauth
rlm_sql (sql): Reserving sql socket id: 2
rlm_sql_postgresql: query: INSERT INTO radpostauth (username, pass, reply, authdate)
VALUES ('cam@amigopod.com', 'Chap-Password', 'Access-Accept', NOW())
rlm_sql_postgresql: Status: PGRES_COMMAND_OK
rlm_sql_postgresql: affected rows = 1
rlm_sql (sql): Released sql socket id: 2
Sending Access-Accept of id 34 to 10.0.20.25 port 32771
Reply-Message = "Guest"
Session-Timeout = 610
```

```
rad_recv: Accounting-Request packet from host 10.0.20.25:32771, id=198, length=142
User-Name = "cam@amigopod.com"
NAS-Port = 1
NAS-Port-Type = Wireless-802.11
NAS-Identifier = "MSM710"
NAS-IP-Address = 10.0.20.25
Acct-Status-Type = Start
Calling-Station-Id = "00-0A-E4-04-68-FD"
Called-Station-Id = "00-03-52-09-14-C5"
Event-Timestamp = "Aug 25 2009 13:28:20 EST"
Acct-Delay-Time = 0
Acct-Session-Id = "0f5b51ca"
Acct-Authentic = RADIUS
Framed-IP-Address = 192.168.1.52
rlm_sql (sql): Reserving sql socket id: 1
rlm_sql_postgresql: query: INSERT INTO radacct ??(AcctSessionId, AcctUniqueId,
UserName, Realm, NASIPAddress, NASPortId, NASPortType, AcctStartTime, AcctAuthentic,
??ConnectInfo_start, CalledStationId, CallingStationId, ServiceType, FramedProtocol,
FramedIPAddress, AcctStartDelay, RoleName) ??VALUES('0f5b51ca', '3215f3890fa69871',
'cam@amigopod.com', '', '10.0.20.25', ??'1', 'Wireless-802.11', ('2009-08-25
13:28:19'::timestamp - '0'::interval), 'RADIUS', '', ??'00-03-52-09-14-C5', '00-0A-E4-
04-68-FD', '', '', ??'192.168.1.52', '0', (SELECT roledef.name FROM useraccount LEFT
JOIN roledef ON useraccount.role_id=roledef.id WHERE
useraccount.username='cam@amigopod.com'))
rlm_sql_postgresql: Status: PGRES_COMMAND_OK
rlm_sql_postgresql: affected rows = 1
rlm_sql (sql): Released sql socket id: 1
Sending Accounting-Response of id 198 to 10.0.20.25 port 32771
```

Step 7 - Check User Experience

After successful login the user web browser should be displayed with a *Transport* page informing them that they are about to be redirected to their original requested page and also the *Session* pop-up box should be displayed as shown below:



Appendix A – Public Access RADIUS configuration

As mentioned in the Public Access section of the HP ProCurve configuration guide, all the *Attributes* required to drive the Guest access user experience can be centrally administered from a RADIUS server.

In this case we will use the amigopod RADIUS technology to manage the Public Access configuration and will be implemented using amigopod *User Roles.*

As with all amigopod deployments, *User Roles* can be configured to implement a wireless policy for each user once they have been authenticated. These roles definitions can be made up of both Standard RADIUS attributes as per RFC 2865 and also Vendor Specific Attributes (VSA) that enable vendors such as HP ProCurve to extend their functionality and apply policies based on their value-add features.

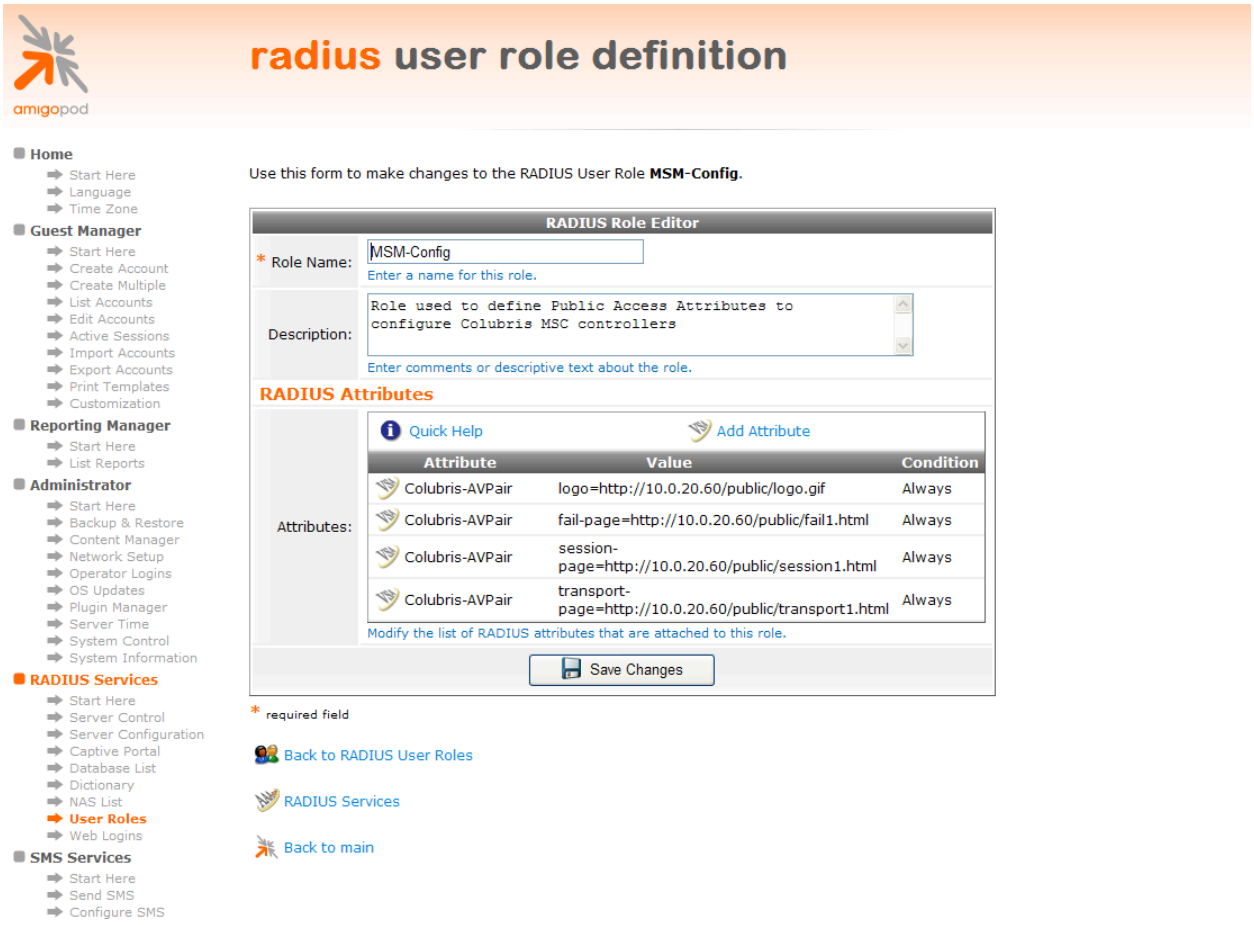
Amigopod has an extensive RADIUS dictionary of vendors and includes the full list of supported VSAs from HP ProCurve / Colubris. For more details on the definition and use of the Colubris VSA attributes please refer to the latest HP ProCurve Network Access Guide.

In order to setup up this centrally controlled RADIUS configuration of the Public Access interface there are two steps within the amigopod configuration that need to be addressed:

- Create a *User Role* with the desired Colubris VSAs
- Define a user that will be used by the MSM to retrieve the Public Access configuration

Create the MSM Configuration User Role

The following screenshot from the amigopod *RADIUS Services → Users Roles* shows how several RADIUS attributes have been added to a new role called *MSM-Config.*



As you can see we have added the 4 attributes that HP ProCurve define as part of their Customising the Public Access Interface in their Network Access Guide (Chapter 3). To prove that the RADIUS download of the Public Access configuration worked we wanted to simply change the logo displayed on the *Session* and *Transport* pages but it is a HP ProCurve requirement that all 4 attributes are configured.

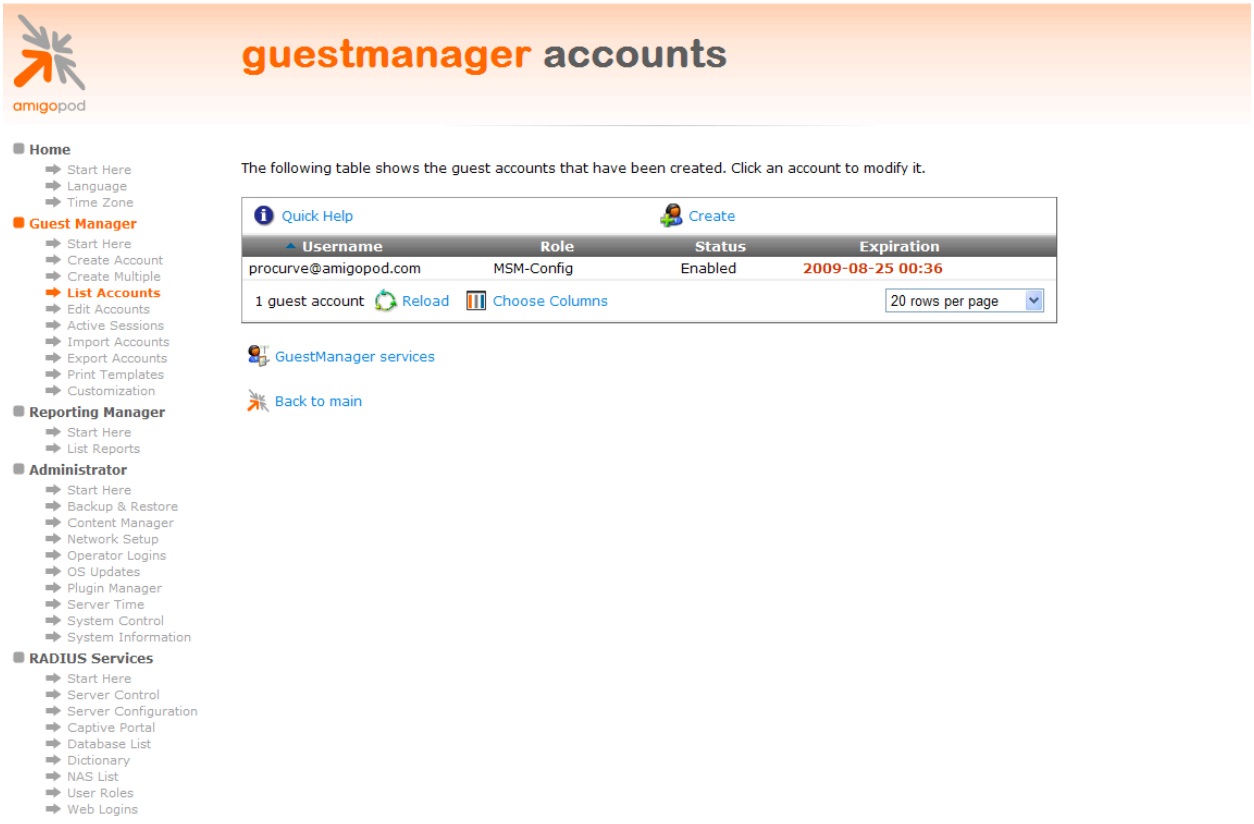
- LOGO
- TRANSPORT-PAGE
- SESSION-PAGE
- FAIL-PAGE

In order to meet this requirement we uploaded the default *transport.hml, session.html* and *fail.html.* These default pages can be found on the HP ProCurve documentation CD under *public_access/Internal_Pages.zip*.

We also uploaded an amigopod logo in gif format and resized it to match the default pixel size of 194 *100px. This was renamed to *logo.gif* in the amigopod *Content Manager* to be consistent with the HP ProCurve default naming convention.

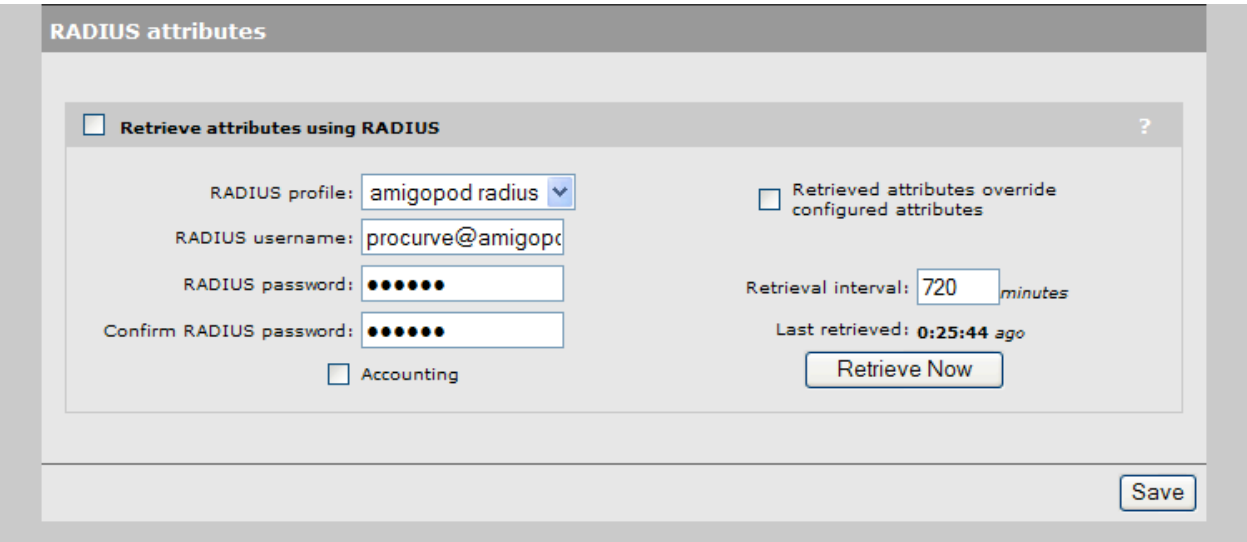
Create MSM Configuration user

The next step is to create a RADIUS user that can be configured to return all of the above attributes defined in the User Role *MSM-Config.* The following screen capture shows our new RADIUS user known as procurve@amigopod.com and the User Role has been set to *MSM-Config* as discussed.



This account should be configured to never expire if you intend to configure the HP ProCurve to perform regular checks of the RADIUS hosted Public Access configuration.

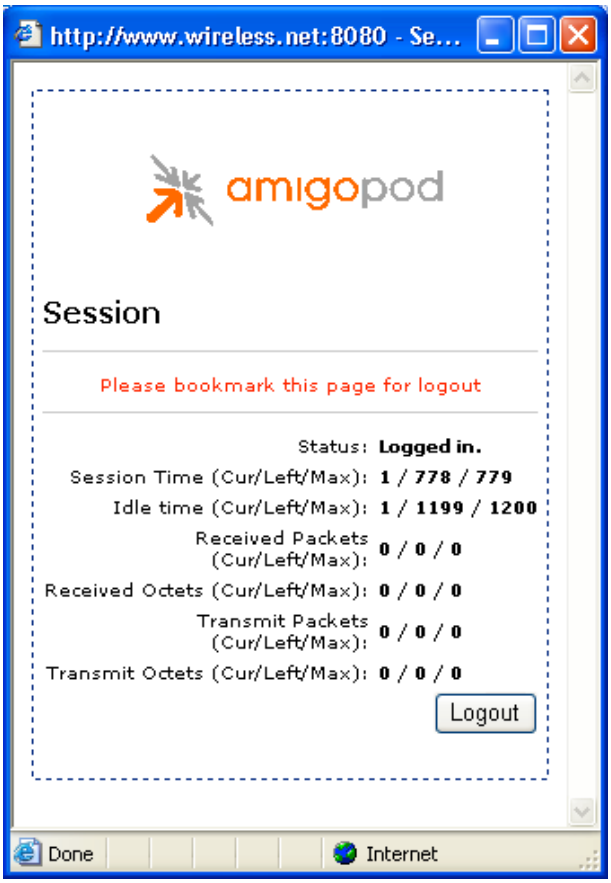
You will recall from Step 8 of the HP ProCurve configuration that under *Service Controller→Public Access→Attributes* is where you can then configure the details of this new RADIUS used that will be used to retrieve the Public Access configuration.

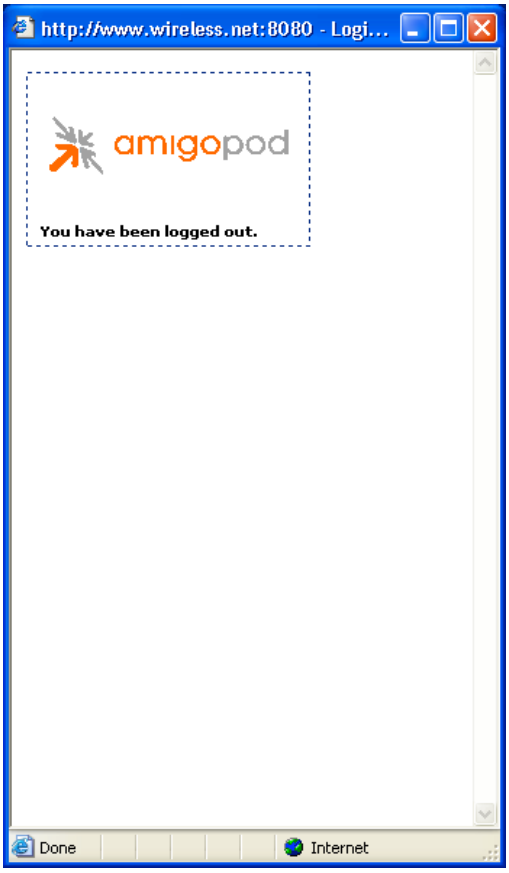


Depending on the frequency of the changes to your configuration you may wish to either leverage the *Retrieve Now* option or check the *Retrieve attributes using RADIUS* option at the top left to check for changes automatically.

Test Result

After making these changes and getting the Test laptop to login again via the Web Login interface we were presented with the following session and logout pages as expected:





Detailed RADIUS Debug

Also the following RADIUS debug successfully shows the Public Access account authentication to the amigopod RADIUS engine and retrieving the 4 new Public Access attributes that make up the *MSM-Config* User Role.

```
Ready to process requests.
rad_recv: Access-Request packet from host 10.0.20.25:32771, id=136, length=199
Acct-Session-Id = "3f06b417"
NAS-Port = 0
NAS-Port-Type = Wireless-802.11
User-Name = "procurve@amigopod.com"
Calling-Station-Id = "00-03-52-09-14-C5"
Called-Station-Id = "00-03-52-09-14-C5"
Framed-IP-Address = 192.168.1.1
CHAP-Password = 0x88e6ef16942ad21c9599d43d6fe8cc0944
CHAP-Challenge = 0xf67f882cd53a1476654bbbe91bdf5a2d
NAS-Identifier = "colubris"
NAS-IP-Address = 10.0.20.25
Framed-MTU = 1496
Connect-Info = "HTTPS"
Service-Type = Administrative-User
Message-Authenticator = 0xbe139e880c7e2bfa2a0c2a885211ed4a
rlm_chap: Setting 'Auth-Type := CHAP'
rlm_sql (sql): Reserving sql socket id: 3
rlm_sql_postgresql: query: SELECT id, UserName, Attribute, Value, Op FROM radcheck
WHERE Username='procurve@amigopod.com' ORDER BY id
rlm_sql_postgresql: Status: PGRES_TUPLES_OK
rlm_sql_postgresql: affected rows =
rlm_sql_postgresql: query: SELECT radgroupcheck.id, radgroupcheck.GroupName,
radgroupcheck.Attribute, radgroupcheck.Value,radgroupcheck.Op ??FROM radgroupcheck,
usergroup WHERE usergroup.Username = 'procurve@amigopod.com' AND usergroup.GroupName =
radgroupcheck.GroupName ??ORDER BY radgroupcheck.id
rlm_sql_postgresql: Status: PGRES_TUPLES_OK
rlm_sql_postgresql: affected rows =
rlm_sql_postgresql: query: SELECT id, UserName, Attribute, Value, Op FROM radreply
WHERE Username='procurve@amigopod.com' ORDER BY id
rlm_sql_postgresql: Status: PGRES_TUPLES_OK
rlm_sql_postgresql: affected rows =
rlm_sql_postgresql: query: SELECT radgroupreply.id, radgroupreply.GroupName,
radgroupreply.Attribute, radgroupreply.Value, radgroupreply.Op ??FROM
radgroupreply,usergroup WHERE usergroup.Username = 'procurve@amigopod.com' AND
usergroup.GroupName = radgroupreply.GroupName ??ORDER BY radgroupreply.id
rlm_sql_postgresql: Status: PGRES_TUPLES_OK
rlm_sql_postgresql: affected rows =
rlm_sql (sql): Released sql socket id: 3
rlm_chap: login attempt by "procurve@amigopod.com" with CHAP password
```

```
rlm_chap: Using clear text password wireless for user procurve@amigopod.com
authentication.
rlm_chap: chap user procurve@amigopod.com authenticated succesfully
Exec-Program: /usr/bin/php /opt/amigopod/www/amigopod_request.php 2 15
Exec-Program-Wait: value-pairs: Colubris-AVPair =
"logo=http://10.0.20.60/public/logo.gif", Colubris-AVPair = "fail-
page=http://10.0.20.60/public/fail1.html", Colubris-AVPair = "session-
page=http://10.0.20.60/public/session1.html", Colubris-AVPair = "transport-
page=http://10.0.20.60/public/transport1.html", Session-Timeout = 688,
Exec-Program: returned: 0
Login OK: [procurve@amigopod.com] (from client MSM-710 port 0 cli 00-03-52-09-14-C5)
rlm_sql (sql): Processing sql_postauth
rlm_sql (sql): Reserving sql socket id: 2
rlm_sql_postgresql: query: INSERT INTO radpostauth (username, pass, reply, authdate)
VALUES ('procurve@amigopod.com', 'Chap-Password', 'Access-Accept', NOW())
rlm_sql_postgresql: Status: PGRES_COMMAND_OK
rlm_sql_postgresql: affected rows = 1
rlm_sql (sql): Released sql socket id: 2
Sending Access-Accept of id 136 to 10.0.20.25 port 32771
Colubris-AVPair = "logo=http://10.0.20.60/public/logo.gif"
Colubris-AVPair = "fail-page=http://10.0.20.60/public/fail1.html"
Colubris-AVPair = "session-page=http://10.0.20.60/public/session1.html"
Colubris-AVPair = "transport-page=http://10.0.20.60/public/transport1.html"
Session-Timeout = 688
```