D-Link DSA-3600 Integration Guide

Revision	0.9
Date	15th December 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 D-Link Multi-Service Business Gateways and the amigopod appliance to create a fully integrated Visitor Management solution. The solution leverages the captive portal functionality built into the D-Link DSA-3600. D-Link uses the terminology of User Login Pages 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 D-Link User Login Pages 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 D-Link Gateways that have been tested with the amigopod solution by either a partner or the vendor directly

Vendor	Products	amigopod verified	Partner Verified
D-Link Building Networks for People	DSA-3600	Yes – 3.50.00	

Test Environment

The test environment referenced throughout this integration guide is based on a D-Link DSA-3600 Multi-Service Business Gateway. Although this low end hardware platform has been used, the testing and therefore this procedure is valid for all DSA hardware variants from D-Link as it is the DSA software that is providing the integration points with amigopod.

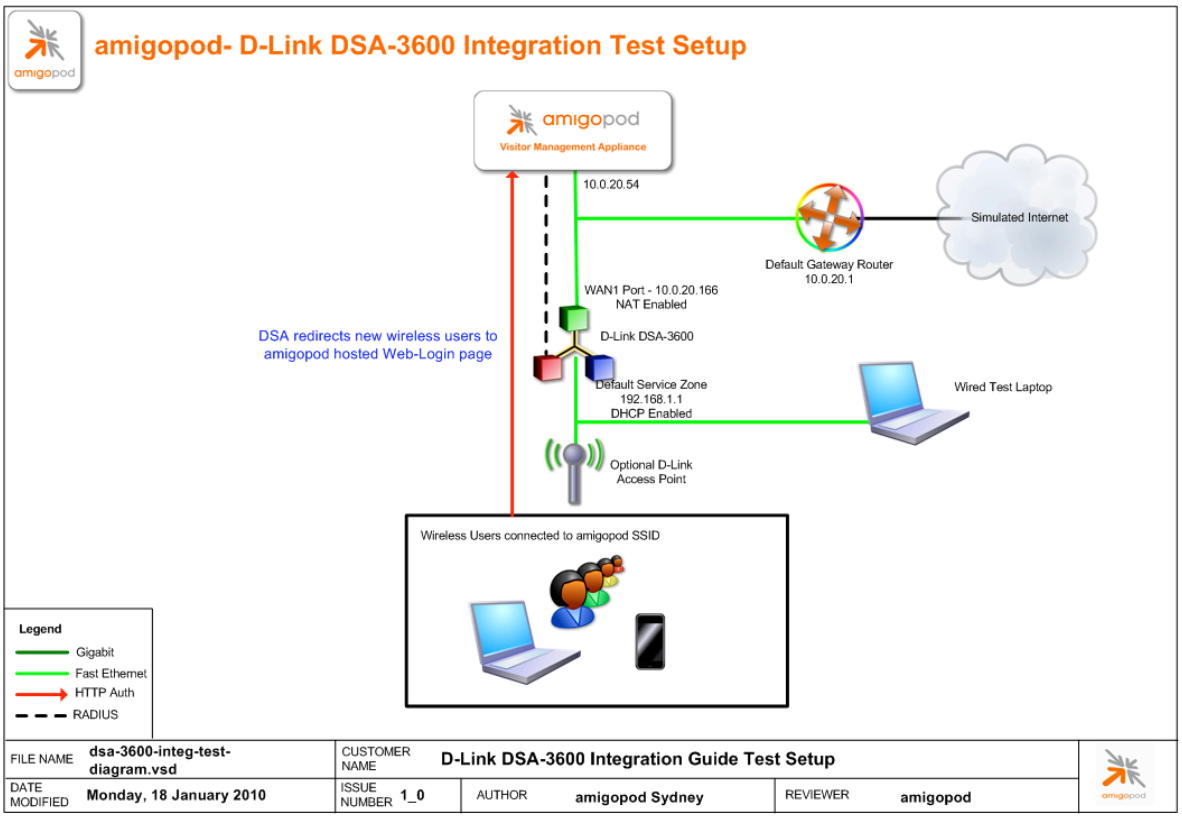
The following table shows the software versions used during the integration testing. This document will be updated in the future if changes in either amigopod or D-Link subsequent releases affect the stability of this integration. It is advised that the customer always check for the latest integration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

Date Tested:	December 2009
AmigoPod Version:	Kernel→2.0.20, Radius Services→ 2.0.20
Plugins Required:	Standard build only
DSA Version:	3.50.00
Integration:	HTTP Captive Portal

Amigopod was deployed locally on the WAN1 interface of the D-Link DSA3600 Gateway 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.

DSA WAN1 IP Address	10.0.20.166
DSA Default Service Zone IP Address	192.168.1.1
Internet Gateway Address	10.0.20.1
amigopod IP Address	10.0.20.54
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 D-Link DSA-3600 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: D-Link now allows for customised Captive portal pages to be uploaded onto the gateway 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 DSA-3600's ability to define and reference external RADIUS servers for the authentication and accounting of visitor accounts. In the standalone D-Link ONDEMAND Guest provisioning solution the local database in each gateway 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:

DSA WAN1 IP Address	10.0.20.166
DSA Default Service Zone IP Address	192.168.1.1
Internet Gateway Address	10.0.20.1
amigopod IP Address	10.0.20.54
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 D-Link DSA-3600 Gateway

In order for the D-Link DSA-3600 to authenticate users it needs to be able to communicate with the amigopod RADIUS instance. This step configures the amigopod NAS definition for the D-Link DSA-3600 Gateway. The RADIUS key used here needs to be configured exactly the same as what will be configured on the DSA-3600 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 D-Link DSA-3600 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 D-Link DSA-3600 Gateway, set the *NAS Type* as *Other NAS* 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 *dlink_login* as the name and the resulting URL in this lab environment will be:

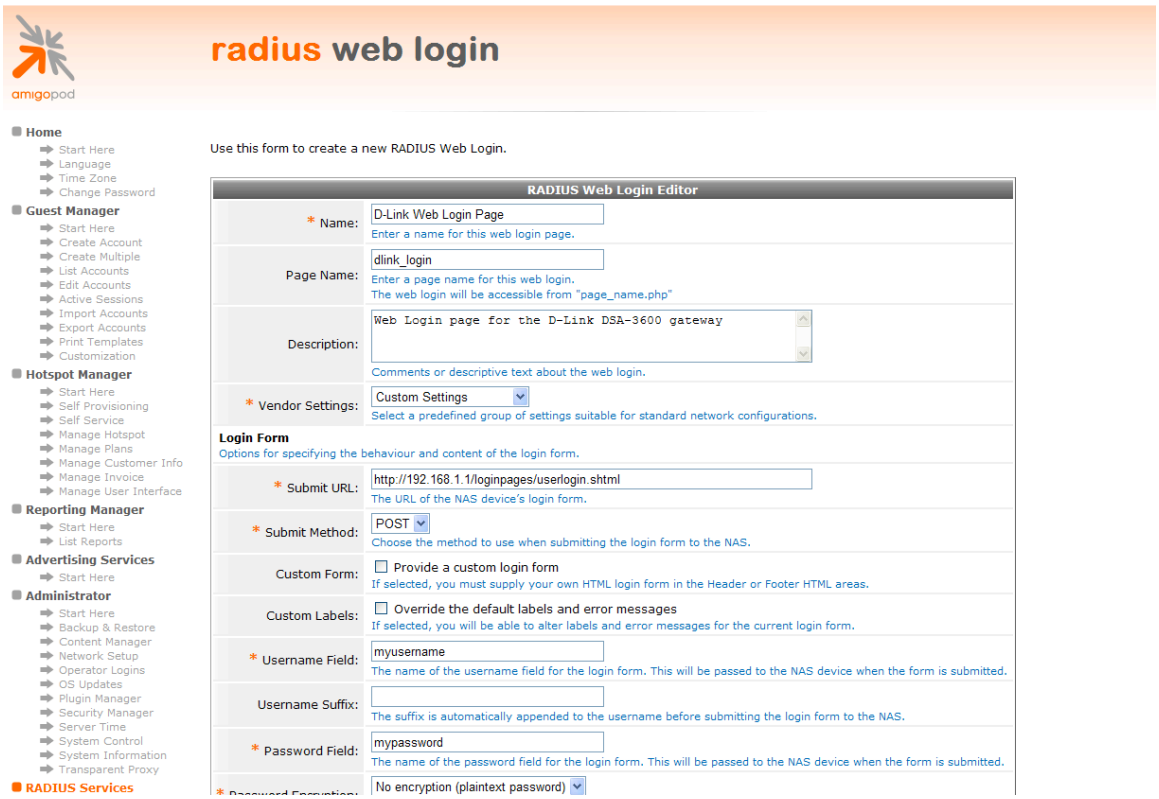
http://10.0.20.54/dlink_login.php

The *Submit URL* is made up of the Service Zone IP Address of the D-Link DSA-3600 and a URL suffix defined by D-Link to be:

/loginpages/userlogin.shtml

In the Lab network design, the Default Service Zone is being used for the basis of all subsequent configurations and therefore the default IP address used by D-Link on this interface is *192.168.1.1.* Depending on your network design, the remaining Service Zones such as *SZ1-SZ4* may also be used and your submit URL should be updated to reflect these changes.

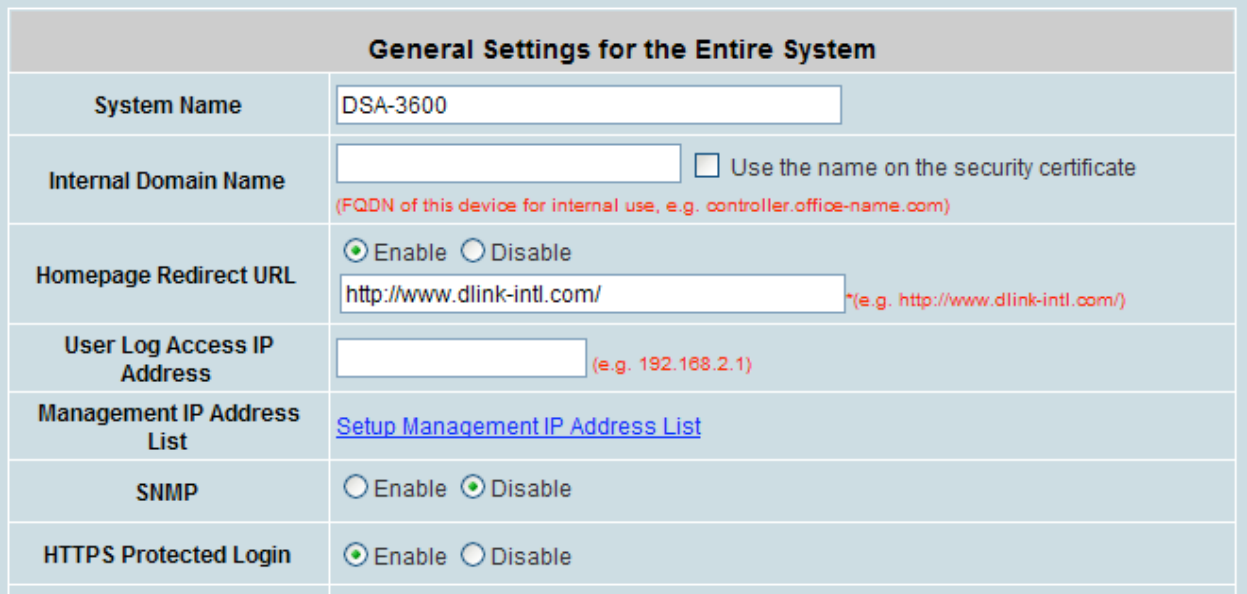
Ensure the *Submit Method* is set to POST.



By default the D-Link DSA-3600 uses port 80 for unsecured HTML authentication and 443 for secure HTML authentication. Via the *System→General* settings on the D-Link DSA-3600 all we login traffic can be configured to use HTTPS (port 443) and therefore provide secure encryption for the username and password traffic being sent over the wireless network.

Note: To avoid receiving browser warnings regarding self signed certificates, trusted root issued certificates should be deployed on both the D-Link DSA-3600 and the amigopod in production environments.

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 above shows the default setting of port 80 (ie. http) being used.



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 *D-Link Web 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 Custom Pages settings on the D-Link DSA-3600 gateway. An example of the URL is shown below:

http://10.0.20.54/dlink_login.php

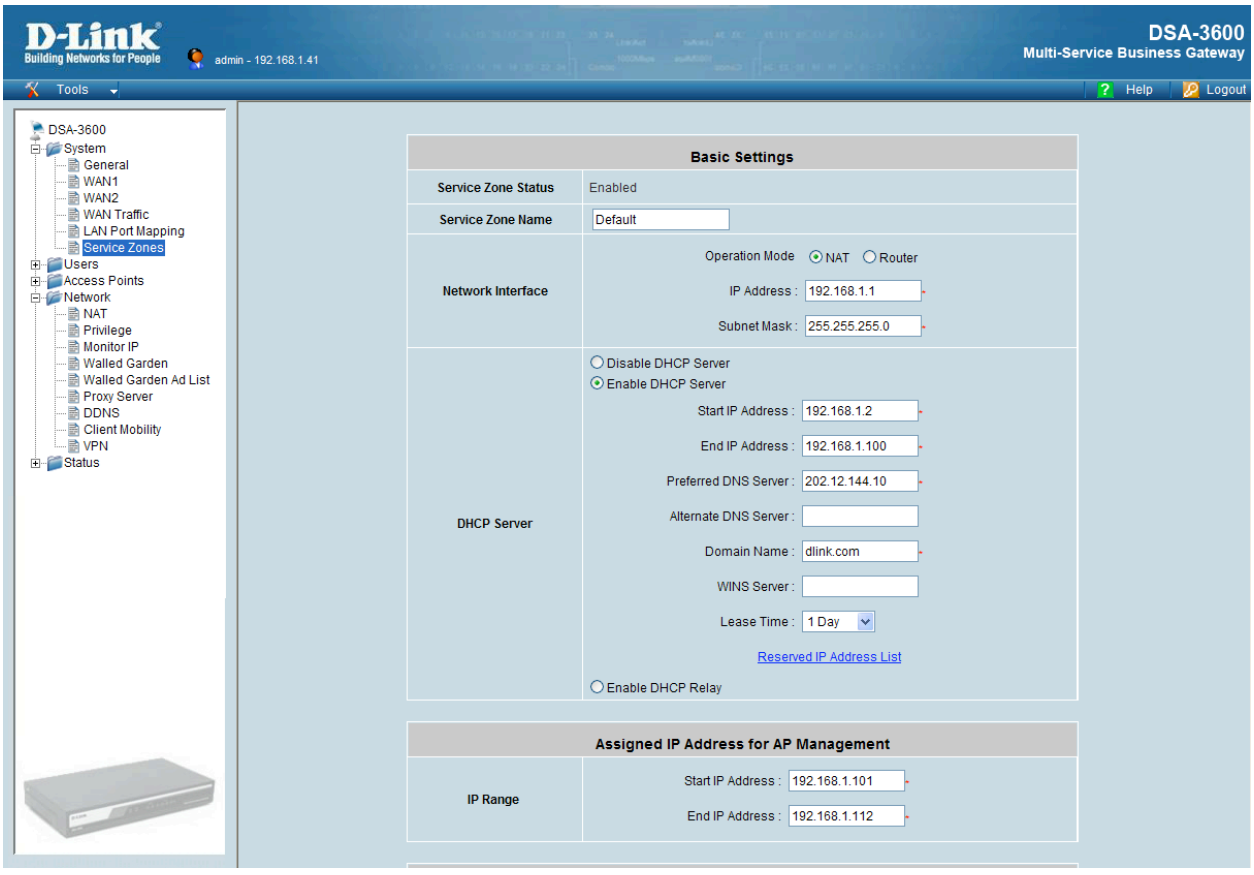
D-Link DSA-3600 Configuration

The following configuration procedure assumes that the D-Link DSA-3600 has been powered up and a basic IP configuration has been applied through the steps detailed in the Quick Install 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:

DSA WAN1 IP Address	10.0.20.166
DSA Default Service Zone IP Address	192.168.1.1
Internet Gateway Address	10.0.20.1
amigopod IP Address	10.0.20.54
amigopod RADIUS port	Auth 1812 Acc 1813 (default settings)

Depending on your network design the D-Link DSA-3600 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.

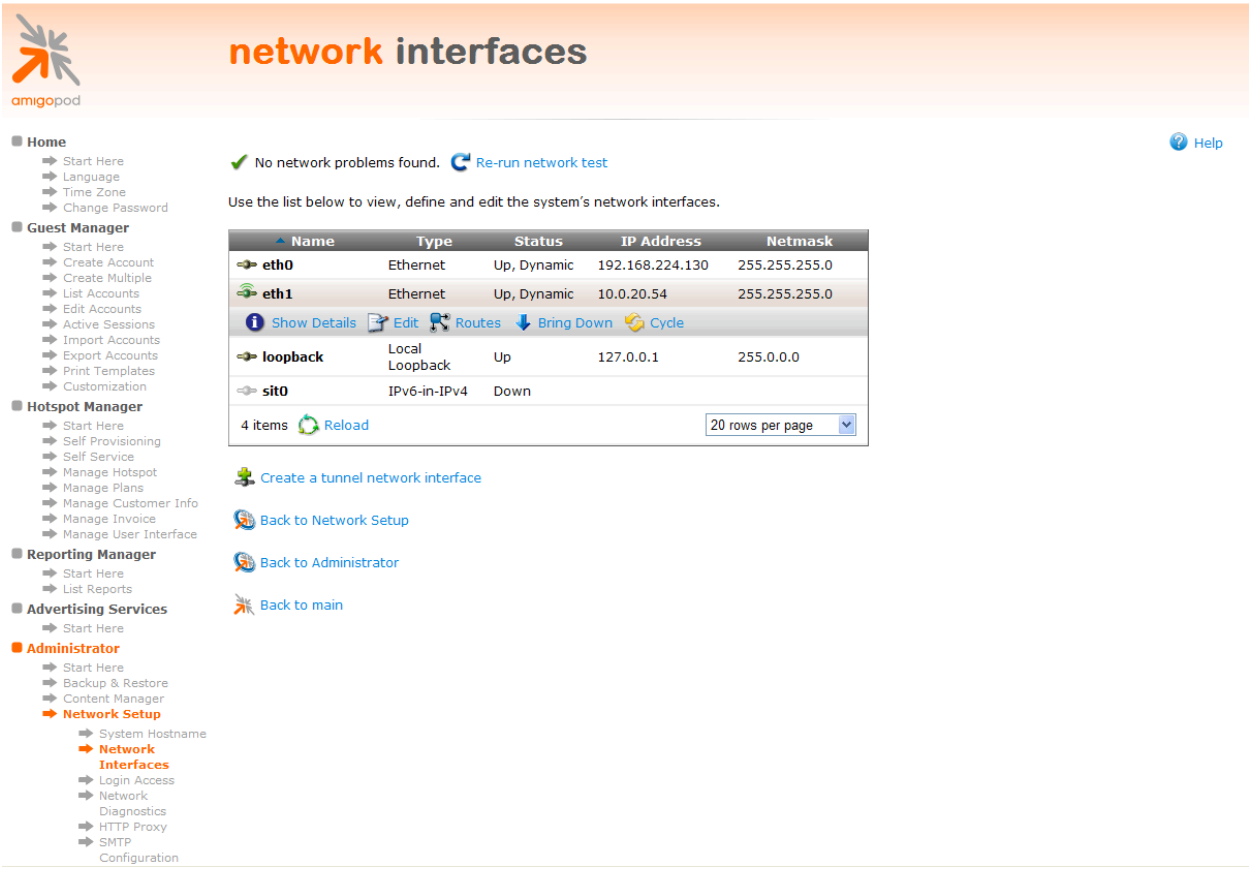
If NAT is required in your network design, the DSA NAT settings can be found under *System→Service Zones→Default→Configure* as shown below:



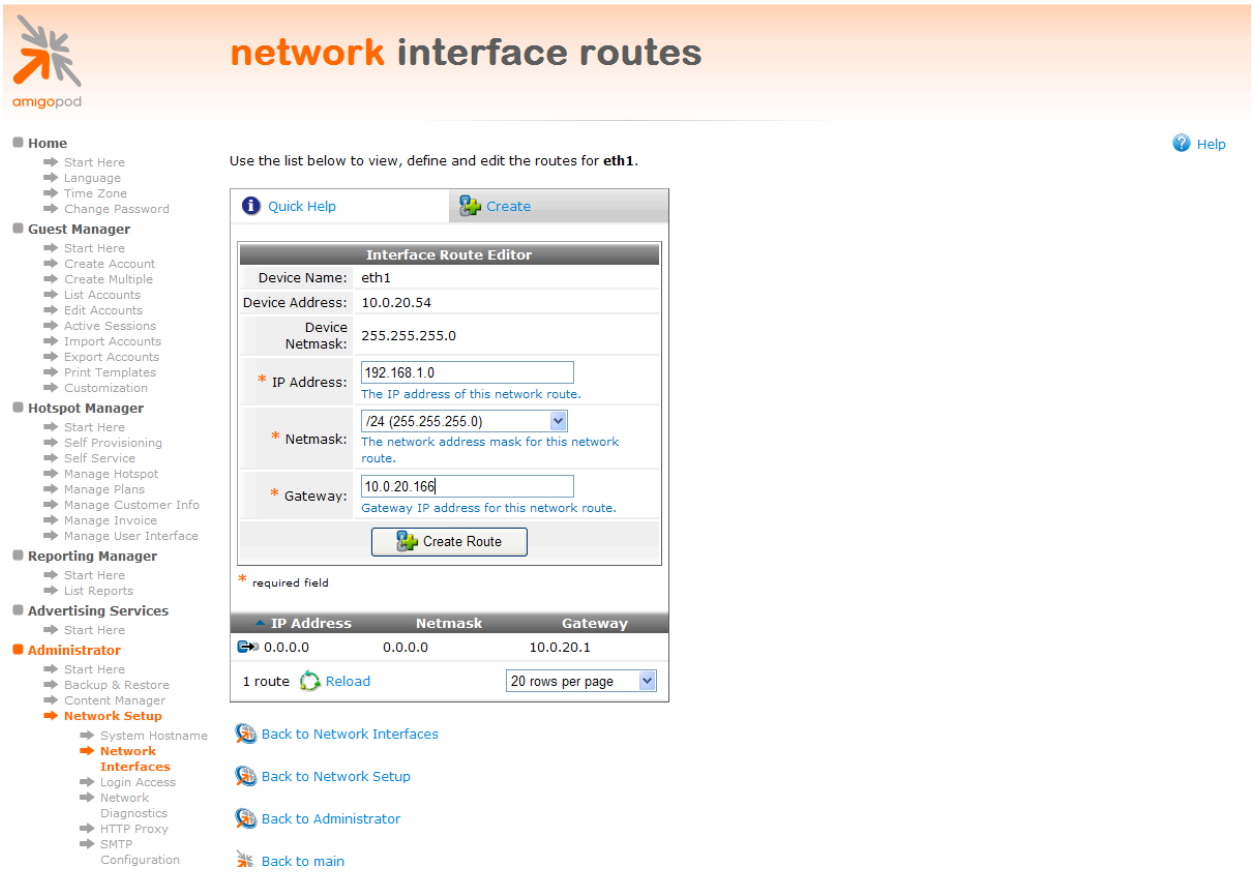
If your design requires the use of other Service Zones than the *Default* Service Zone then the NAT settings for these zones will also have to be updated.

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 *WAN1 port* of the DSA 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:

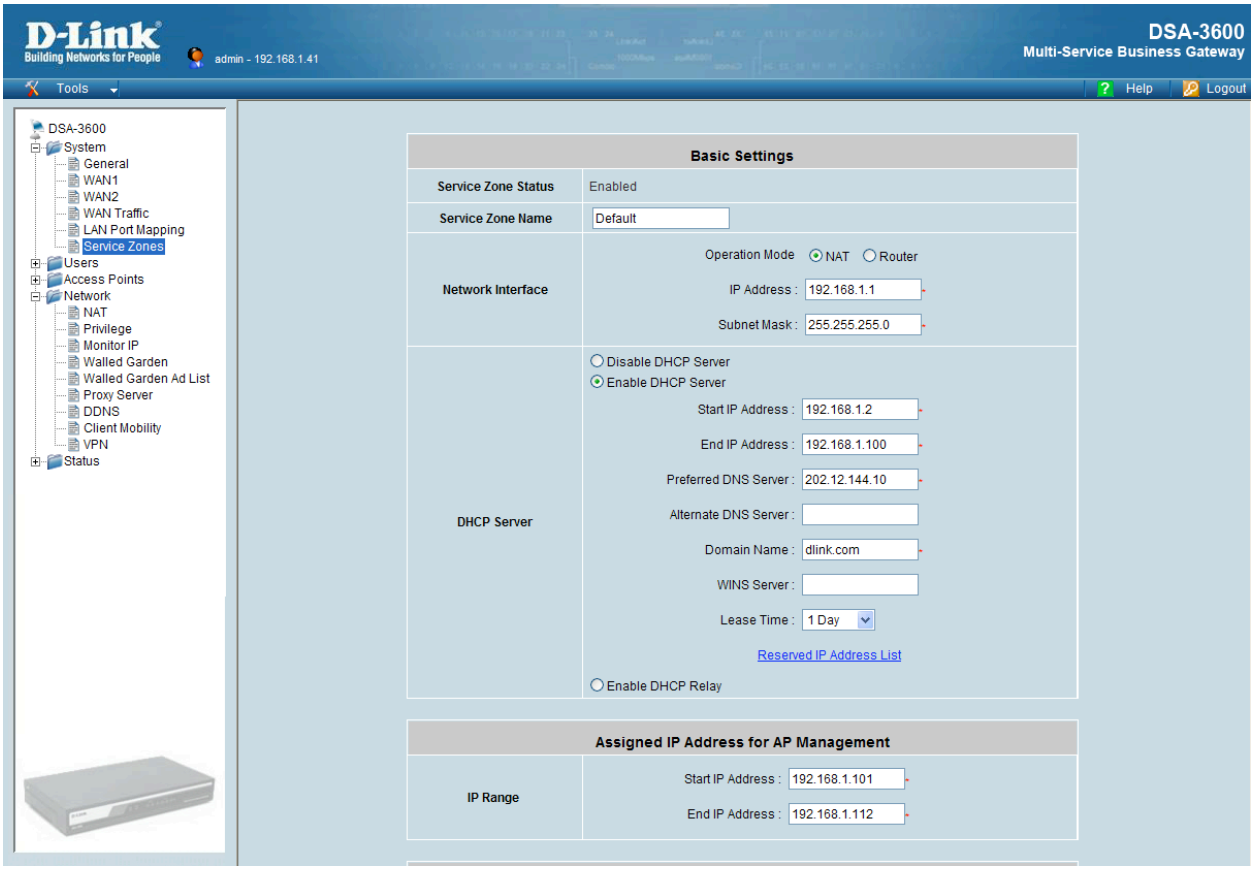


Click on the *Routes* option and add in the details for your IP address range allocated to the *LAN port* on the DSA as shown below:



Step 1 – Enable DHCP on LAN port

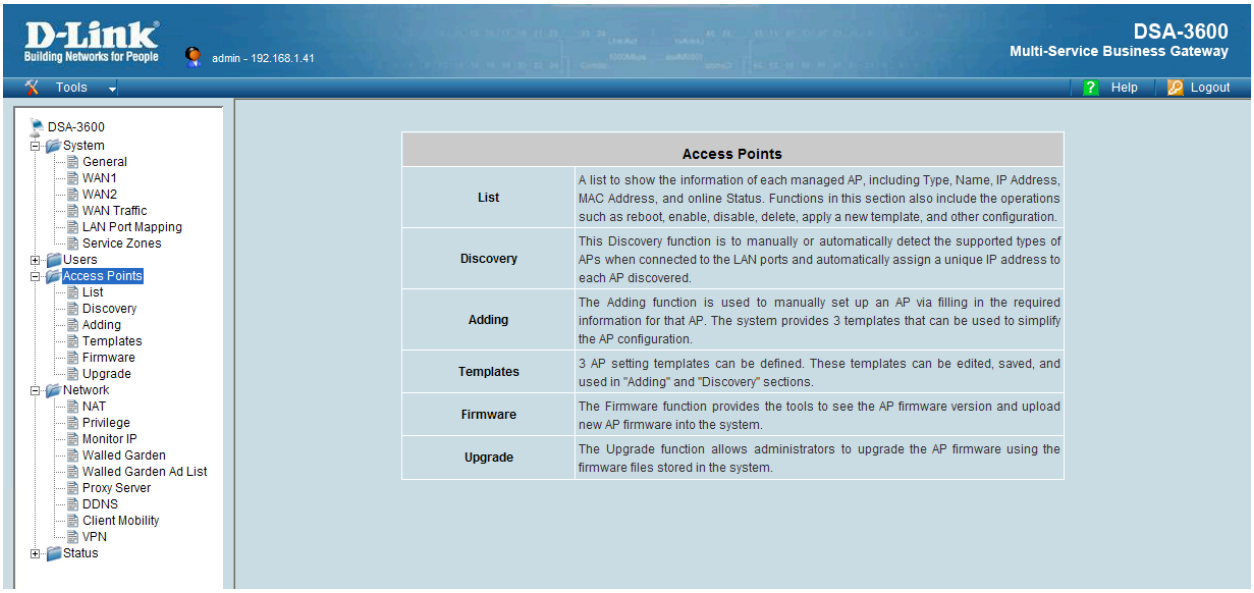
In our Lab environment DHCP needs to be enabled on the *Default Service Zone* to provide IP addresses to both downstream D-Link Access Points and any wired clients connected to this interface of the DSA-3600. This is configured again under *System→Service Zones→Default→Configure* as shown in the following screen shot:



Step 2 – Install Managed D-Link Access Points (Optional)

Although the D-Link DSA-3600 range of gateways is designed primarily for the centralized control of D-Link Access Points, the gateway can be equally used for providing Access Control in pure wired environments.

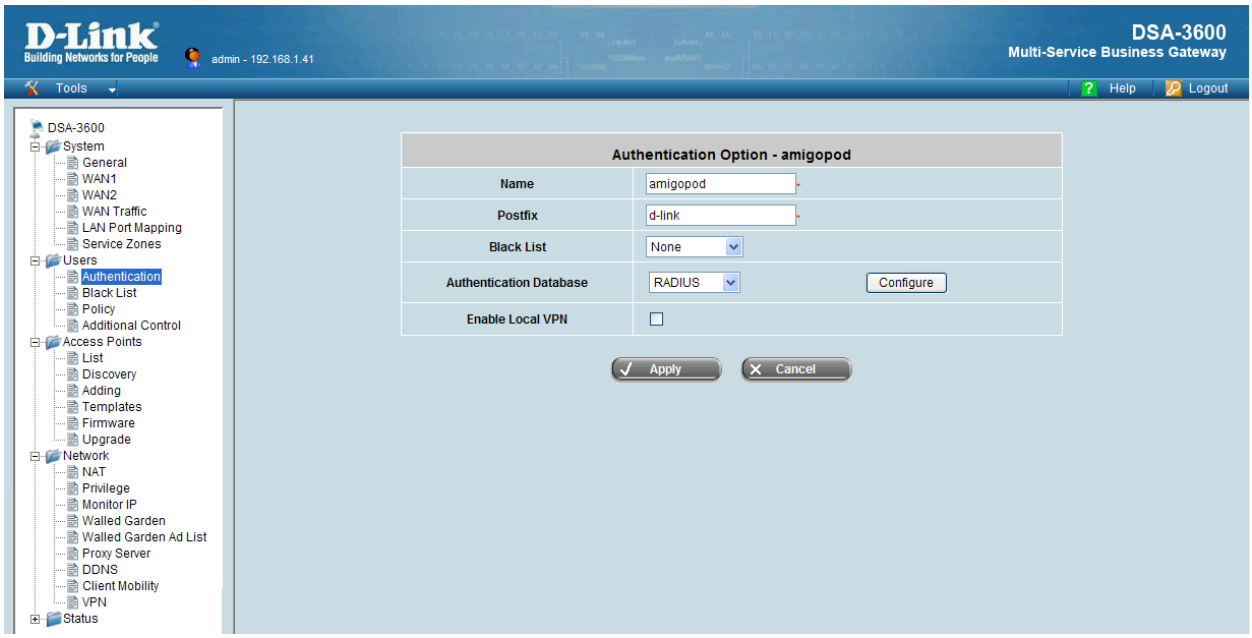
The many different methods of configuring the D-Link Access Points is covered extensively in the D-Link DSA-3600 User Guide in Chapters 4.3 and is therefore considered outside of the scope of this Integration guide. Please refer to the D-Link User Guide for further information on these topics and the best method for configuring your wireless environment.



For the lab environment used through the rest of this document, the DSA-3600 will be used and configured as a wired Access Controller and the test client will be attached directly to the LAN ports of the DSA.

Step 3- Create RADIUS Definition for amigopod

From the *Users→Authentication* screen click the *Server 3 RADIUS Auth* option. In the following screen be sure to enter and confirm the following details:

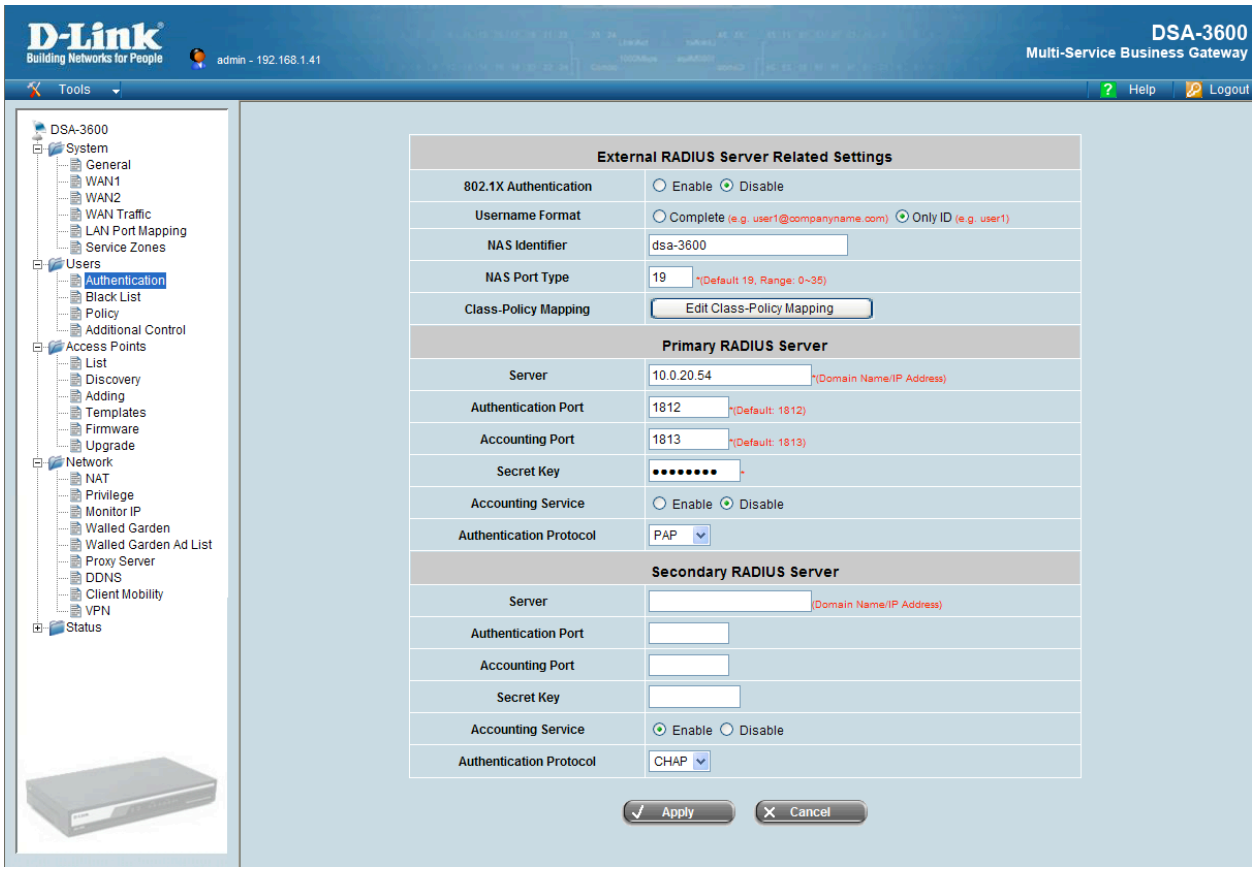


- Enter a descriptive name for the *Name*
- An identifier that will be appended to the end of any authenticated usernames in the *Postfix* field

Next to the *Authentication Database* option click on the *Configure* button as shown in the above screenshot.

- Under *Primary RAIUS Server* enter the IP address of the amigopod
- Confirm the default setting of 1812 & 1813 for the *Authentication & Accounting Port*
- Select *PAP* for the *Authentication Protocol*
- Enter the Shared Secret recorded in Step 1 of the amigopod config as the *Secret Key* ie. ***wireless***
- Enable the *Accounting Service* if you wish to receive session statistics and be able to leverage the amigopod *Guest Manager→Active Sessions* display.

Be sure to save the changes by clicking on the *Apply* button on the bottom left 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***.

The *User→Authentication* table should now look something like the following screenshot:

Authentication Settings		
Auth Option	**Auth Database**	**Postfix**
Server 1	LOCAL	local
Server 2	POP3	pop3
amigopod	RADIUS	d-link
Server 4	LDAP	ldap
On-demand User	ONDEMAND	ondemand
SIP	SIP	N/A

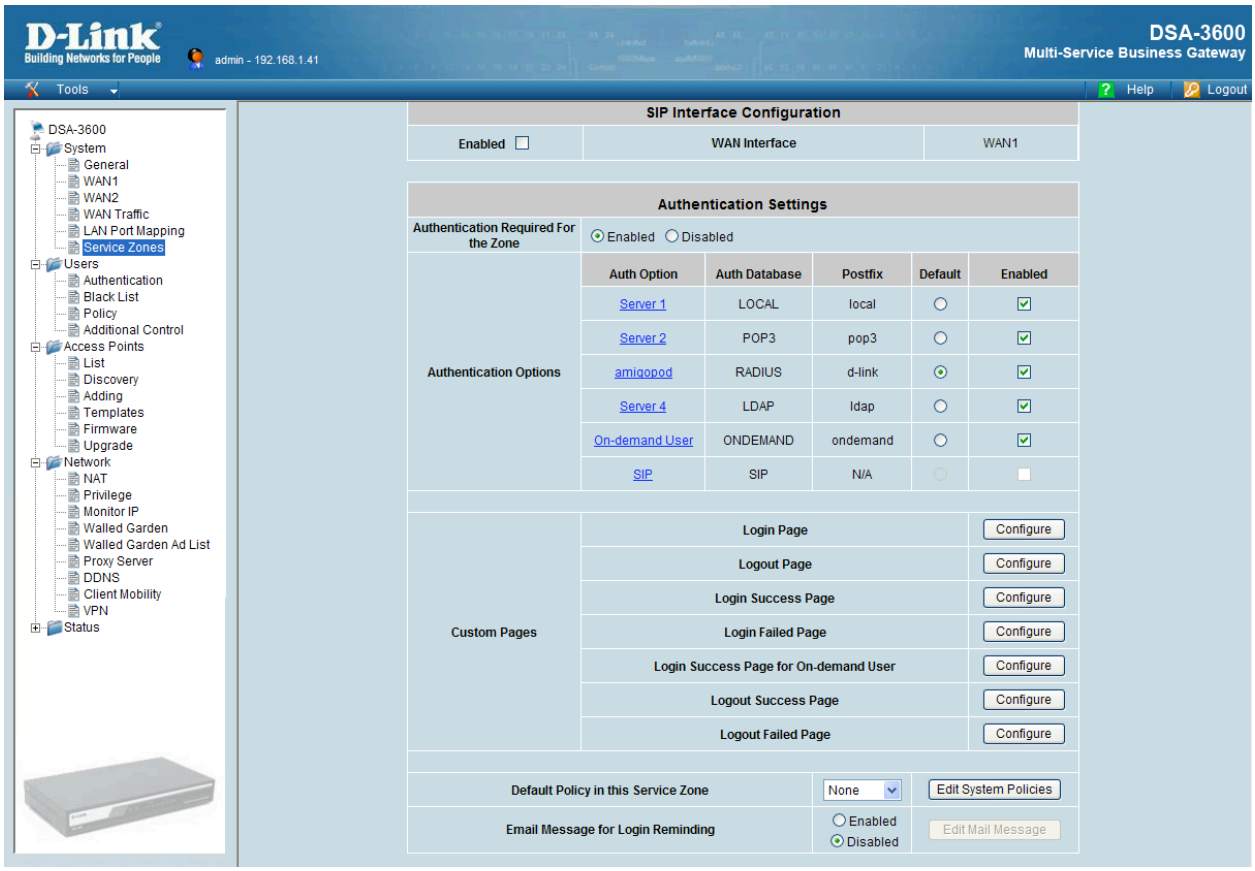
Step 4 – Enable Authentication on Default Service Zone

In order for the DSA to be able to intercept and redirect any new Guest users to the amigopod hosted Web Login page, the gateway must have *Authentication Required* enabled for the Security Zone in question. By default the following table displays the factory configured Security Zones and their disabled authentication state:

Click on the Configure button for the Default Security Zone shown above and scroll down to the *Authentication Settings* section.

Firstly make sure the *Authentication Required For the Zone* option is *Enabled.*

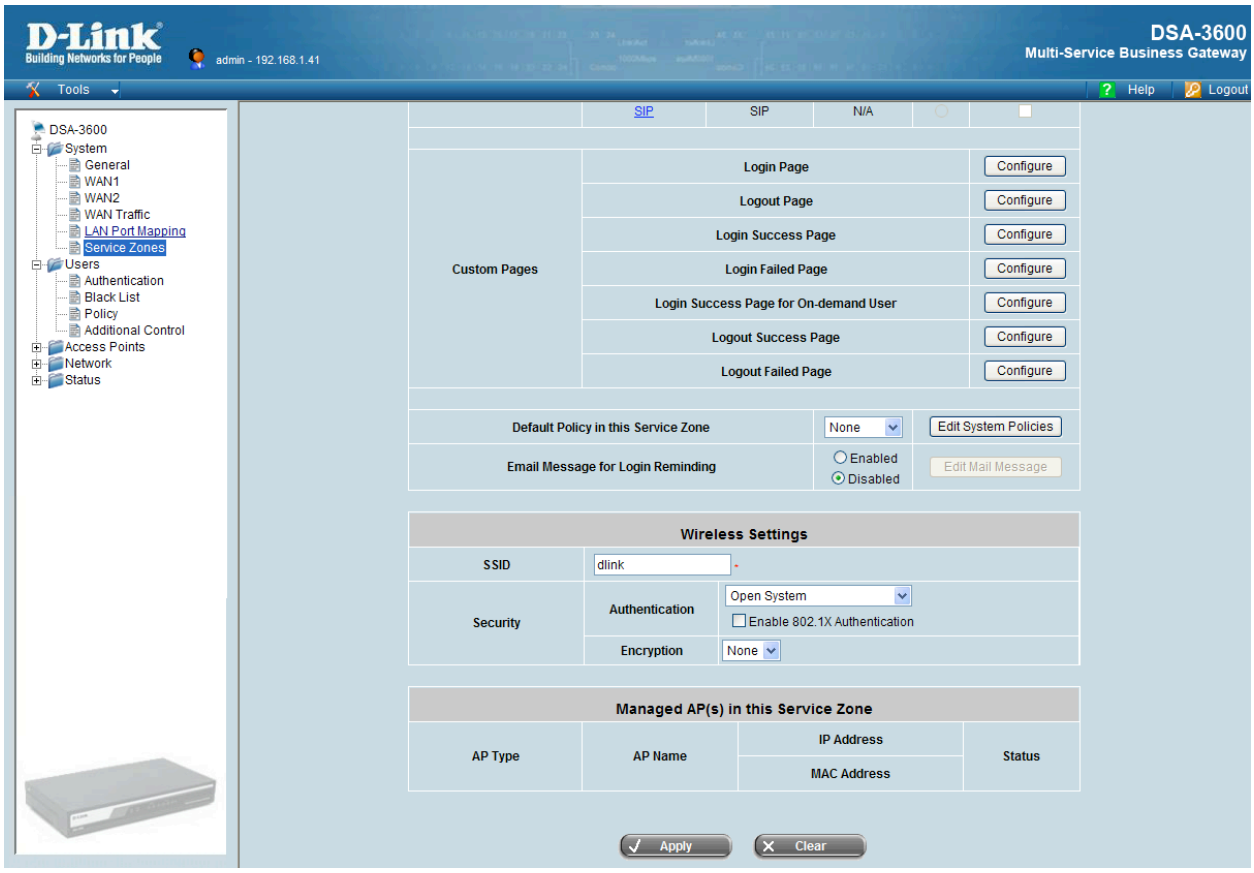
Next, under the *Authentication Options* section immediately below ensure the radio button in the *Default* column for *RADIUS Auth Database* is checked and enabled.



Scroll to the bottom of the page and click the *Apply* button to save the changes so far.

Step 5 – Define Login Page External Destination

Returning to the *System→Service Zones→Default* configuration section, scroll down to the *Custom Pages* part of the configuration page as shown below:



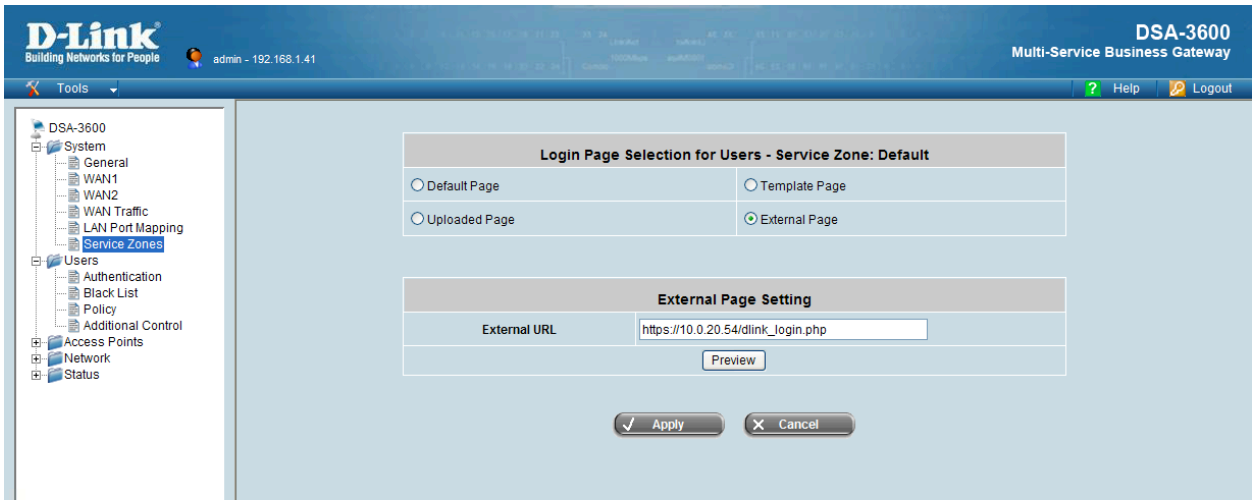
There are various configuration options on this screen allow the Pages displayed during the Login and Logout procedures support by the DSA-3600 to be either customised on the Gateway itself or redirected to an external host such as the amigopod.

In order for the DSA-3600 to redirect new Guest users to the amigopod Web Login page we need to define an External *Login Page* 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://10.0.20.54/dlink_login.php

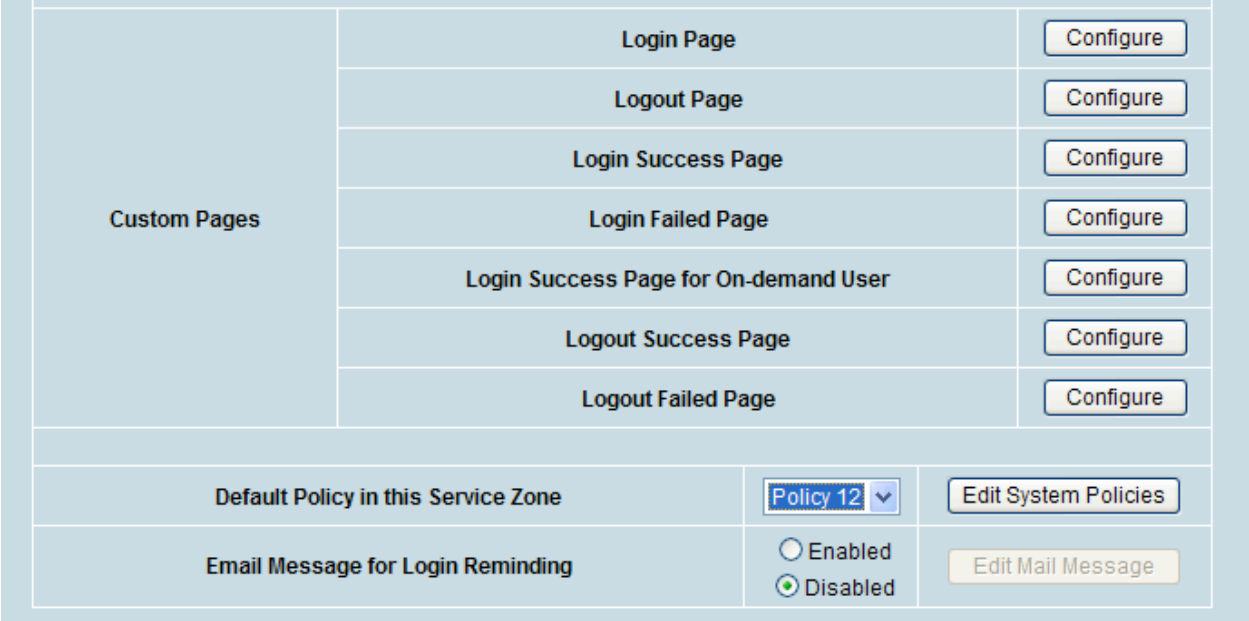
From the *Custom Pages* configuration section click on the *Configure* button and select the *External Page* radio button as shown below:



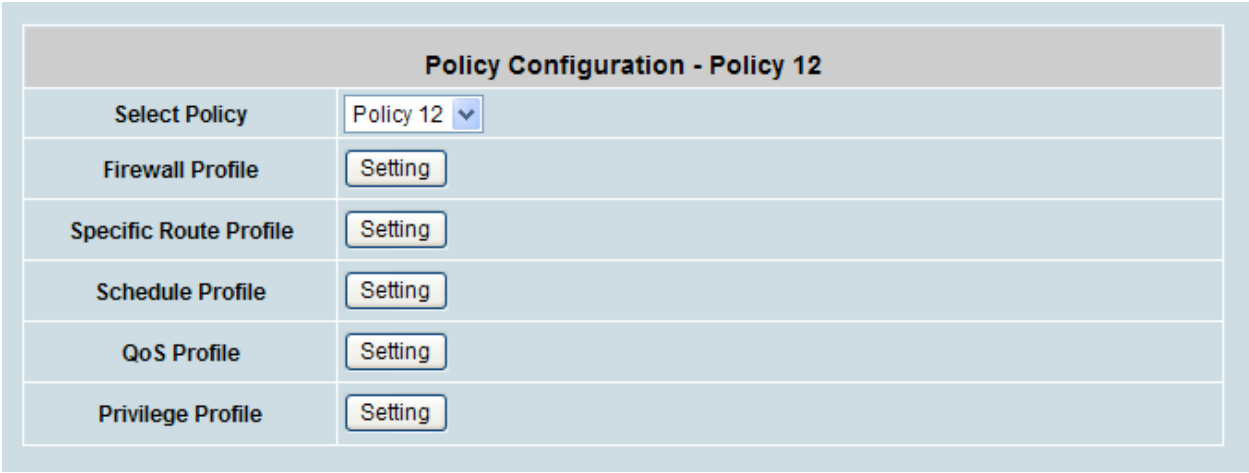
Enter the URL from the previous step and click the *Apply* button to commit the changes to the *Default Security Zone*.

Step 6 – Apply Access Policy to all Guest Users (Optional)

Following on directly from the *Custom Pages* configuration above, the administrator can chose to apply a blanket policy definition to all Guest Users of this Service Zone by selecting a Policy in the *Default Policy in this Service Zone* option shown below.



Policies are covered extensively in the D-Link User Guide for the DSA-3600 in Chapter 4.2.3 and are therefore considered outside the scope of this Integration Guide. Nonetheless Policies for controlling the user experience with attributes such as *Firewall Rules*, *QoS Profiles*, *Schedules* and *Specific Routes* can all be invoked using this powerful tool.



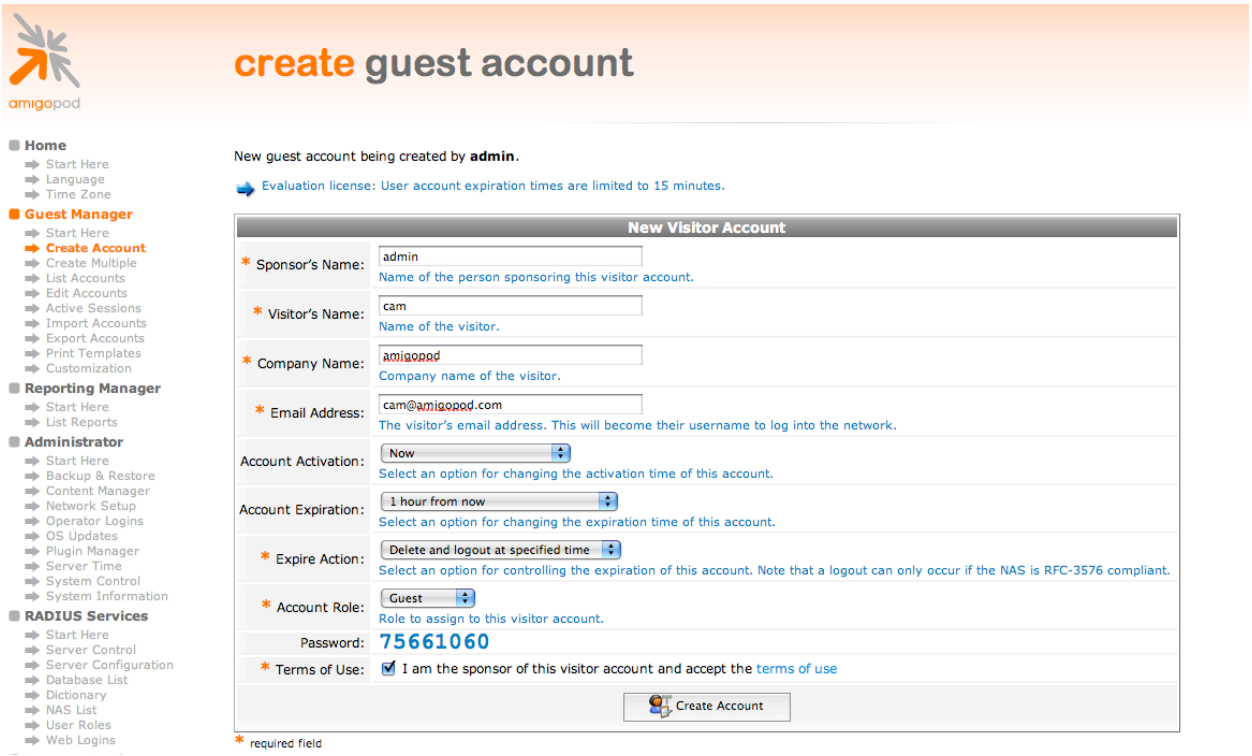
Please see *Appendix A* for more details on how these Policies can be invoked per user by integration with the amigopod *User Roles* functionality.

Testing the Configuration

Now that the configuration of both the D-Link DSA-3600 Gateway 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.

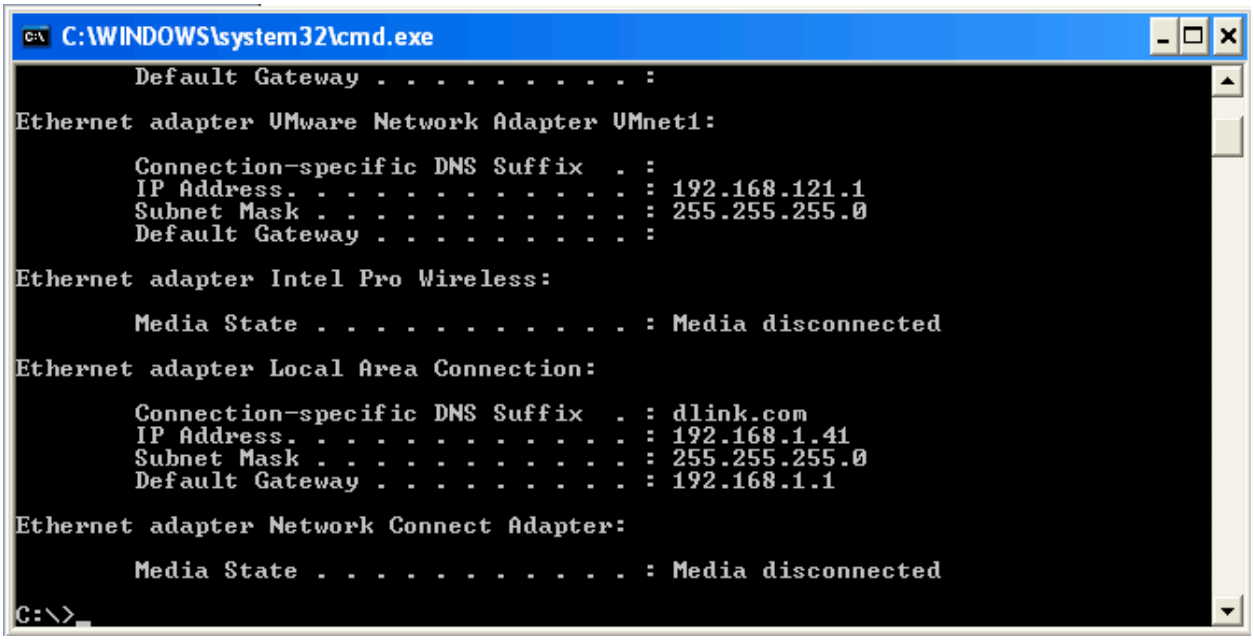
For simplicity during our testing we took this option and changed the username to ***cam*** and password to ***wireless.*** All subsequent screenshots and debugs will reflect this change.

Step 2 - Confirm DHCP IP Address received

Assuming our test laptop is connected to the LAN1 port on the back of the DSA-3600 we should successfully receive an IP address via DHCP.

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 DSA-3600 Gateway

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 – Launch Web Browser and login

When the web browser on the test laptop is launched the DSA will automatically capture the session and redirect the user to the amigopod hosted login page as shown below (which was defined in the *Custom Pages→Login Page*)

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

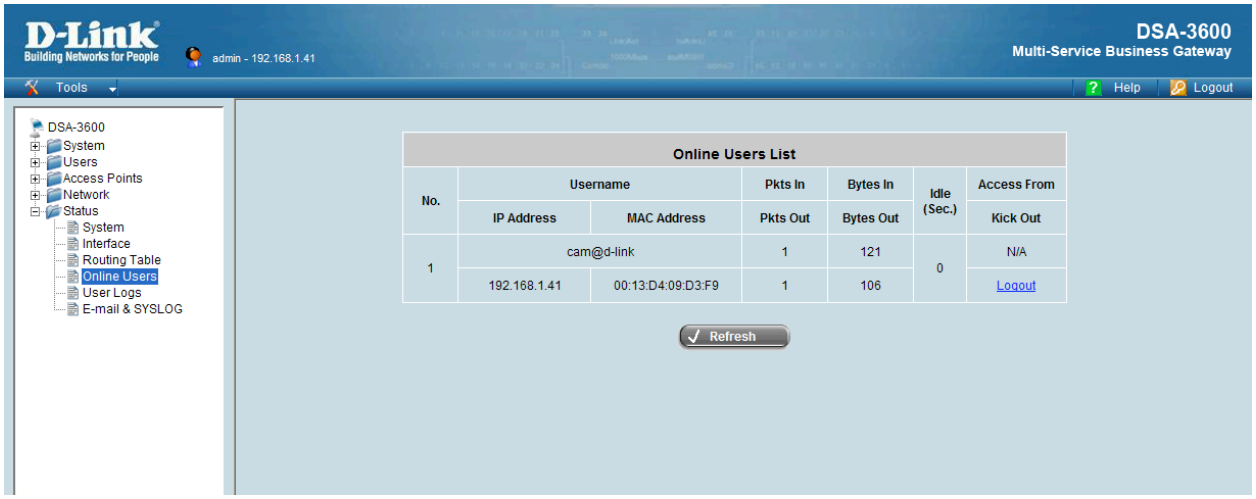
At this point the test user should be successfully authenticated and allowed to transit through the controller and onto the Internet or Corporate network.

Note: If the web browser fails to redirect check that the DNS server configured in the base DSA-3600 configuration 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 DSA-3600 controller to redirect. Other situations that can cause issues with the captive portal include but are not limited to:

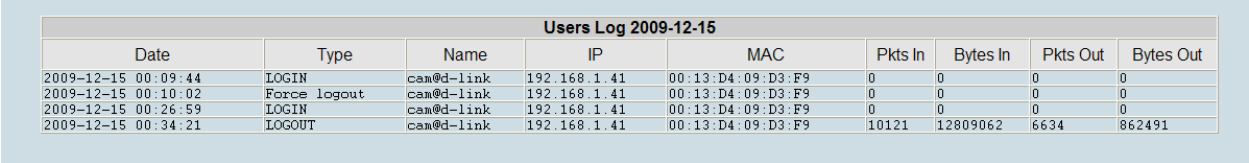
- Web browser home page set to intranet site not available in current DNS
- Proxy Server configuration in browser using non standard HTTP ports

Step 4 – Confirm the login successful from DSA-3600

From the *Status→Online Users* menu option 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 *Kick Out* column of the table shown below:



You can also check the *Status→User Logs* option to display a table of successful Login and Logout transactions and summaries of traffic transmitted in each session as shown below:



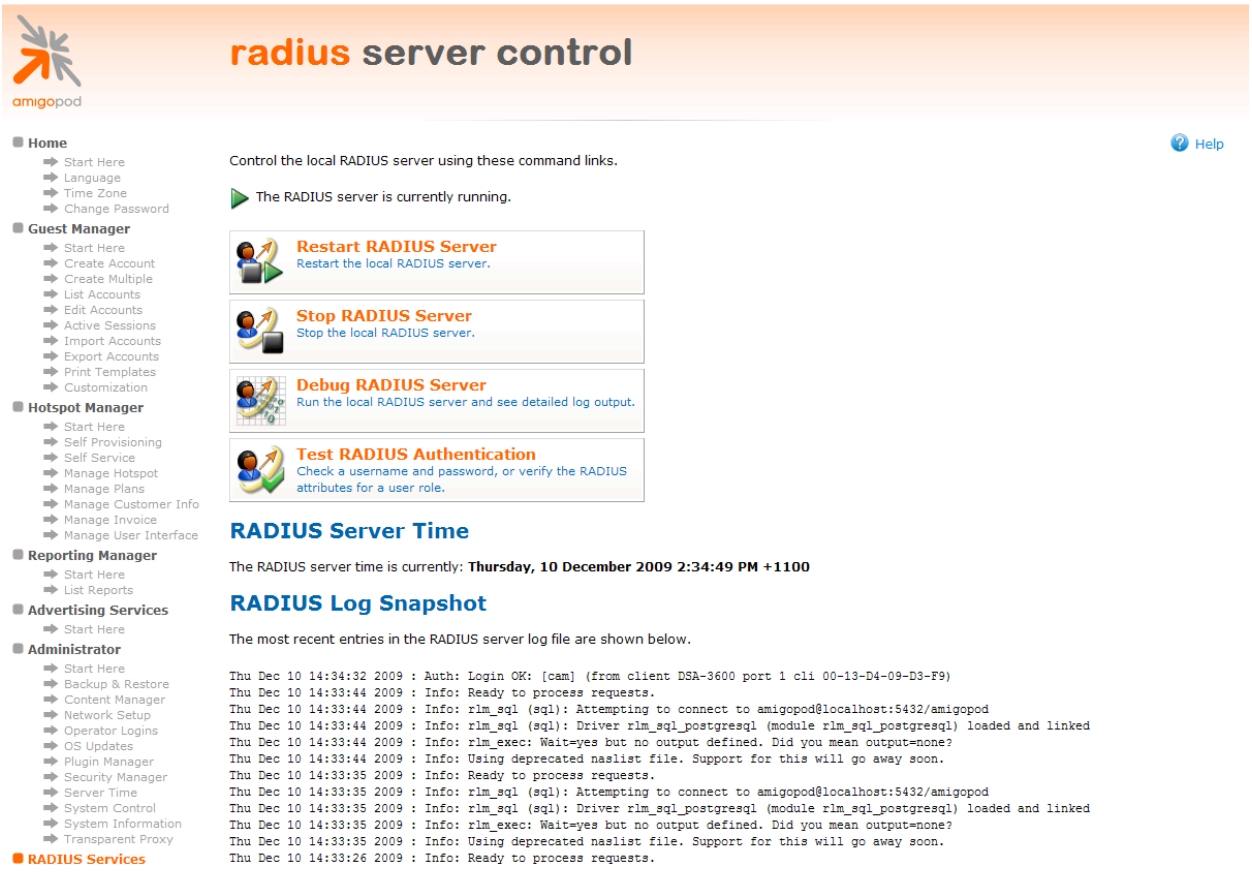
Users Log 2009-12-15

Date	Type	Name	IP	MAC	Pkts In	Bytes In	Pkts Out	Bytes Out
2009-12-15 00:09:44	LOGIN	cam@d-link	192.168.1.41	00:13:D4:09:D3:F9	0	0	0	0
2009-12-15 00:10:02	Force logout	cam@d-link	192.168.1.41	00:13:D4:09:D3:F9	0	0	0	0
2009-12-15 00:26:59	LOGIN	cam@d-link	192.168.1.41	00:13:D4:09:D3:F9	0	0	0	0
2009-12-15 00:34:21	LOGOUT	cam@d-link	192.168.1.41	00:13:D4:09:D3:F9	10121	12809062	6634	862491

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*.

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:

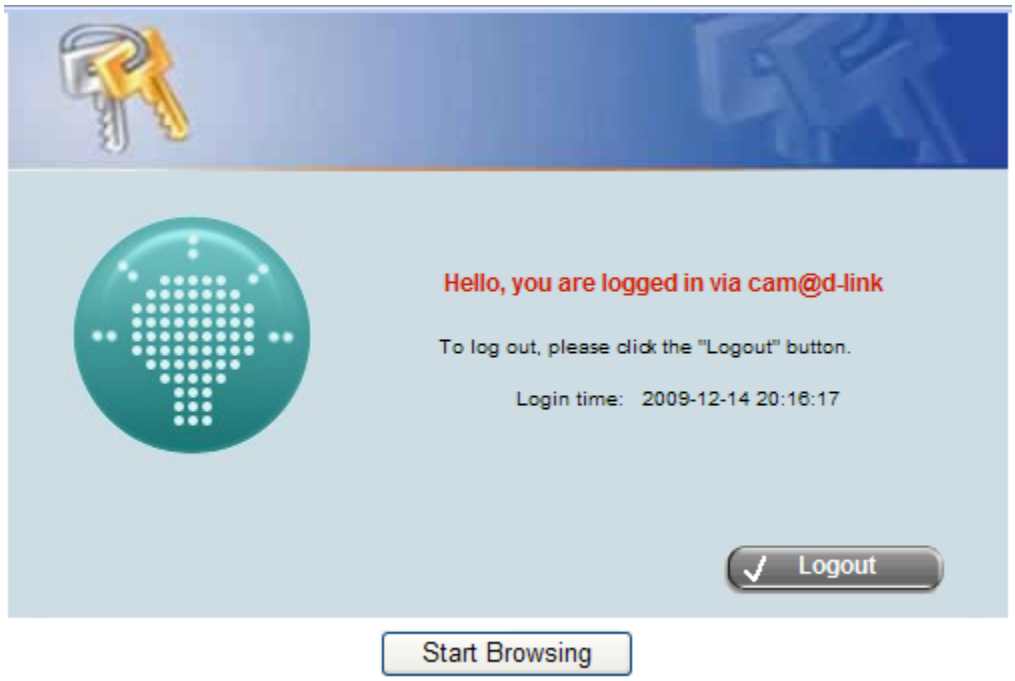
```
Ready to process requests.
rad_recv: Access-Request packet from host 10.0.20.166:1027, id=80, length=127
Service-Type = Call-Check
NAS-Identifier = "dsa-3600"
NAS-Port = 1
NAS-Port-Id = "Controlled"
NAS-Port-Type = Wireless-802.11
NAS-IP-Address = 10.0.20.166
```

```
User-Name = "cam"
User-Password = "wireless"
Called-Station-Id = "00-15-E9-DB-22-0B"
Calling-Station-Id = "00-13-D4-09-D3-F9"
rlm_sql (sql): Reserving sql socket id: 3
rlm_sql_postgresql: query: SELECT id, UserName, Attribute, Value, Op FROM radcheck
WHERE Username='cam' 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' 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' 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' 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
Exec-Program: /usr/bin/php /opt/amigopod/www/amigopod_request.php 2 4
Exec-Program-Wait: value-pairs: Reply-Message = "Employee",
Exec-Program: returned: 0
Login OK: [cam] (from client DSA-3600 port 1 cli 00-13-D4-09-D3-F9)
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', 'wireless', '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 80 to 10.0.20.166 port 1027
Reply-Message = "Employee"
rad_recv: Accounting-Request packet from host 10.0.20.166:1027, id=124, length=145
Service-Type = Call-Check
NAS-Identifier = "dsa-3600"
NAS-Port = 1
NAS-Port-Id = "Controlled"
NAS-Port-Type = Wireless-802.11
NAS-IP-Address = 10.0.20.166
User-Name = "cam"
Acct-Status-Type = Start
Acct-Session-Id = "1260793628"
```

```
Acct-Delay-Time = 0
Acct-Authentic = RADIUS
Called-Station-Id = "00-15-E9-DB-22-0B"
Calling-Station-Id = "00-13-D4-09-D3-F9"
Framed-IP-Address = 192.168.1.41
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('1260793628', 'd065a0a421bdf720',
'cam', '', '10.0.20.166', ??'Controlled', 'Wireless-802.11', ('2009-12-10
14:36:46'::timestamp - '0'::interval), 'RADIUS', '', ??'00-15-E9-DB-22-0B', '00-13-D4-
09-D3-F9', 'Call-Check', '', ??'192.168.1.41', '0', (SELECT roledef.name FROM
useraccount LEFT JOIN roledef ON useraccount.role_id=roledef.id WHERE
useraccount.username='cam'))
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 124 to 10.0.20.166 port 1027
```

Step 7 – Check User Experience

The following Login Success page will be displayed within the test laptop browser to confirm the successful authentication and also provide the opportunity for the user to explicitly logout:



This page can be changed from the default branding through either the use of the Internal Templates configure within the *Custom Pages→Login Success Page* or by following some of the Advanced amigopod configuration guidelines in *Appendix B.*

Appendix A - Per User Policy Definition via RADIUS

As mentioned in the *Service Zone* configuration section of the D-Link DSA-3600 configuration, RADIUS attributes can be used to trigger Per-User policy definitions used to drive the Guest access user experience.

In this case we will use the amigopod RADIUS technology to manage the Per-User policy configuration and it 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 D-Link to extend their functionality and apply policies based on their value-add features.

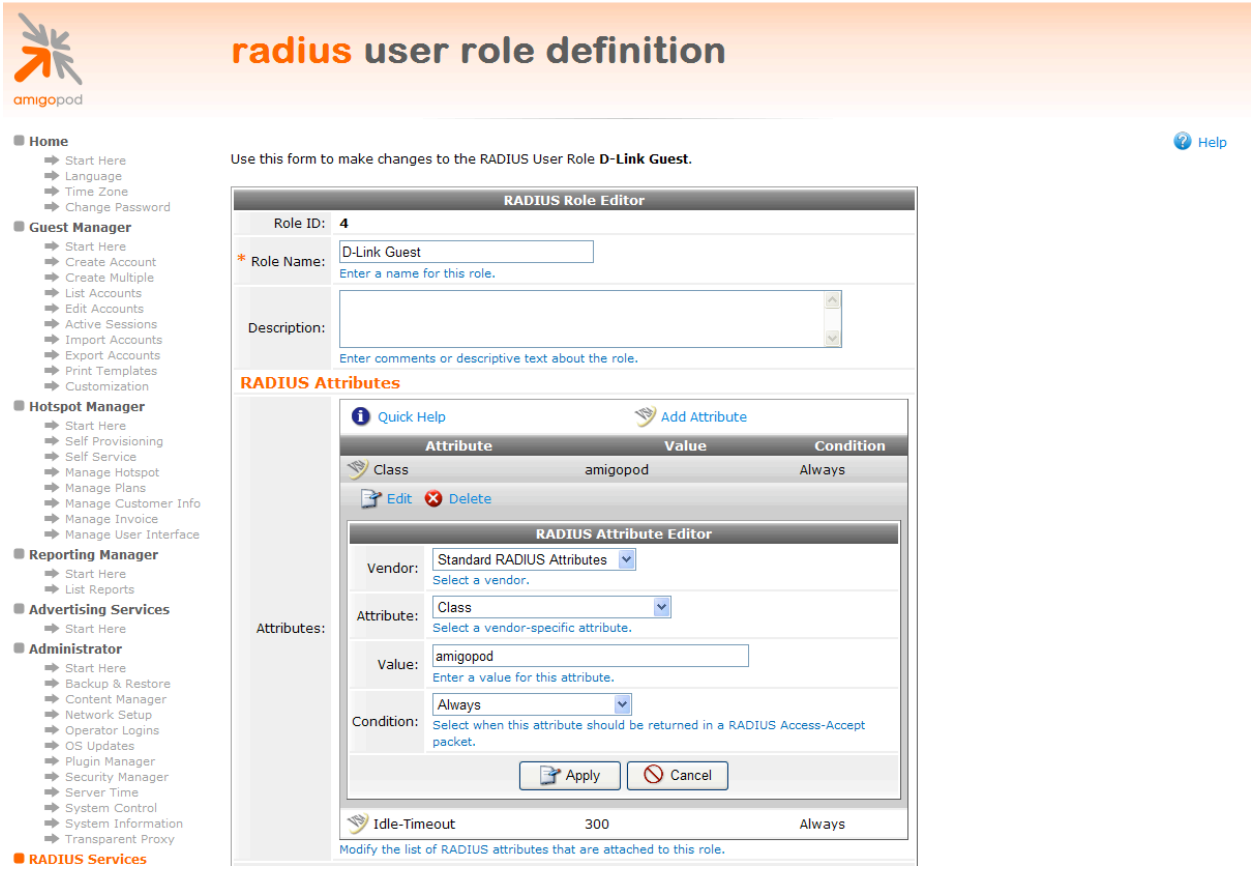
Amigopod has an extensive RADIUS dictionary of vendors and includes the full list of supported VSAs from D-Link. For more details on the definition and use of the D-Link VSA attributes please refer to the latest D-Link Application Note discussed in *Appendix C*.

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 RADIUS Attributes
- Define a test user that is part of this role to test out any *Policy* elements that have been configured.

Create D-Link Specific 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 *D-Link Guest.*

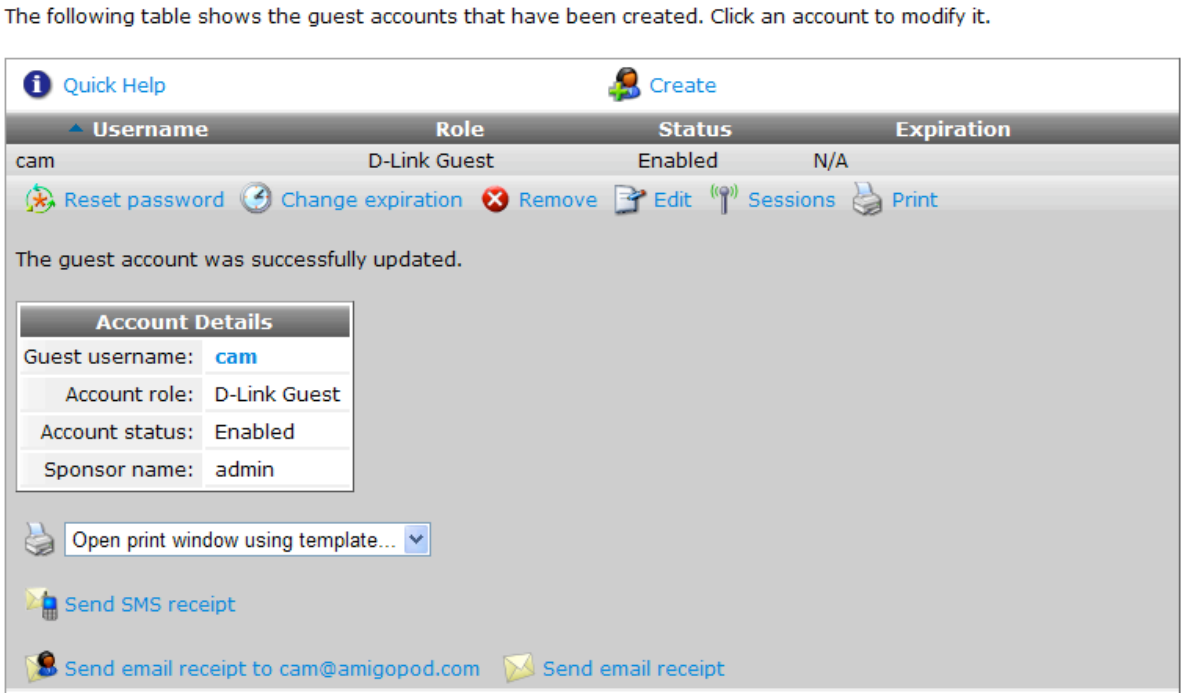


As you can see we have added the 2 attributes that are part of the Standard RADIUS dictionary in *Idle-Timeout & Class.*

D-Link has defined that a RADIUS ACCEPT message returned from the RADIUS that include the Standard RADIUS attribute of Class will be used to determine the *Policy* that should be applied to the user session in question.

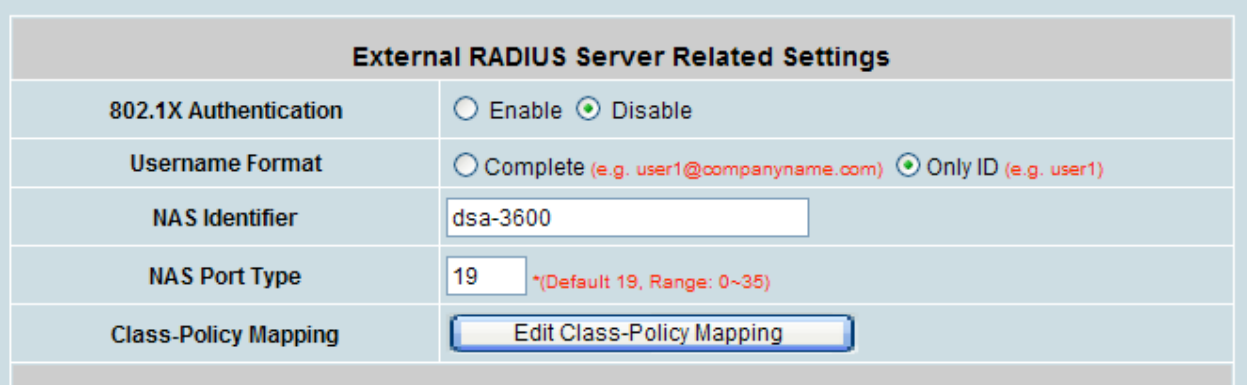
Create Test D-Link user

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 *D-Link Guest.* The following screen capture shows our RADIUS user known as *cam* and the User Role has been set to *D-Link Guest* as discussed.

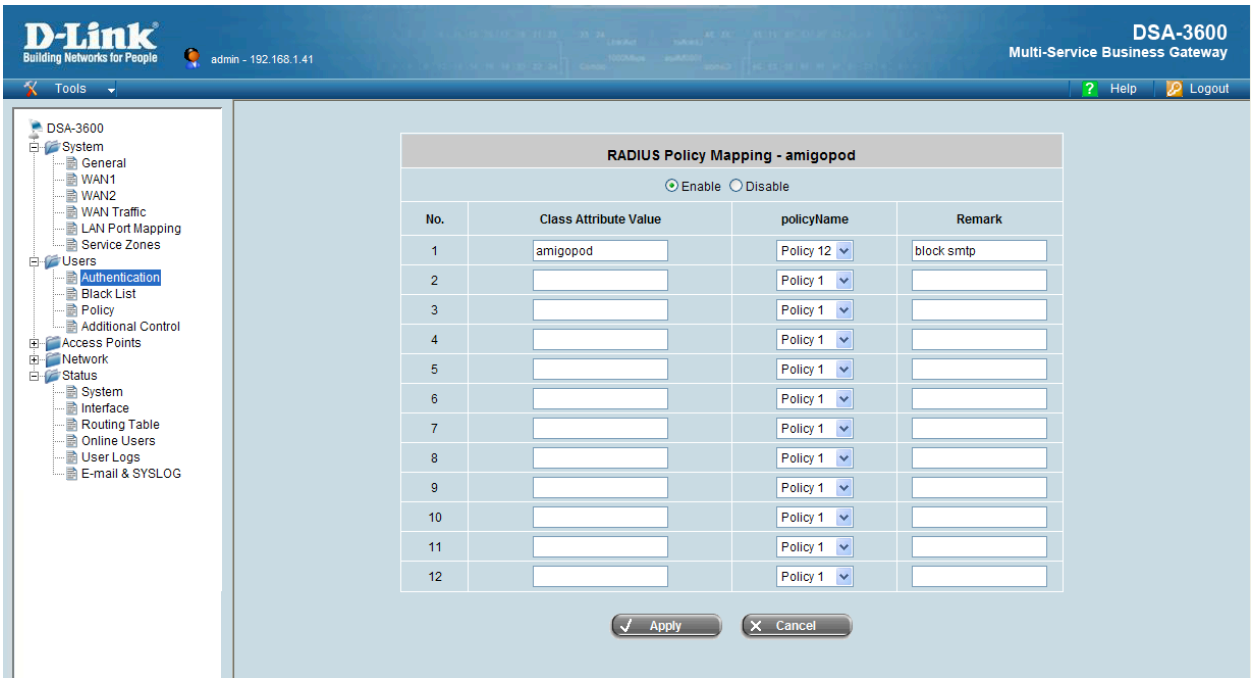


Enable Class-Mapping on the DSA-3600

Returning to the DSA-3600 configuration for User Authentication, navigate to the Users→Authentication→RADIUS→Configure section and you will find the *Edit Class-Policy Mapping* button.

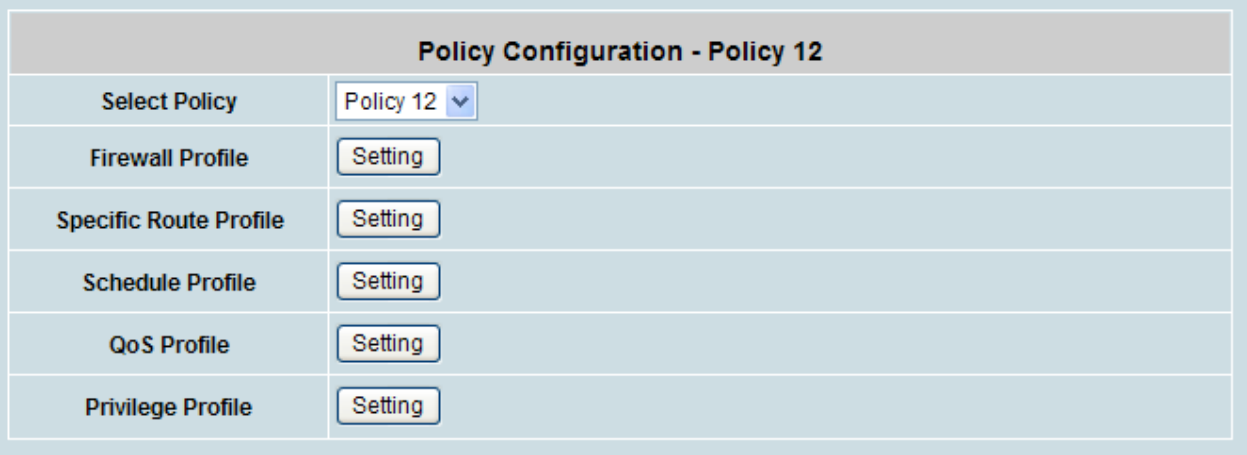


Clicking on this button will display the configuration page shown below:



From this screen enter the same name for the RADIUS Class attribute that was configured in the new amigopod role in the previous section. In this example the RADIUS Class attribute was defined to return *amigopod* as the value. Then select one of the available Policies to influence the user experience.

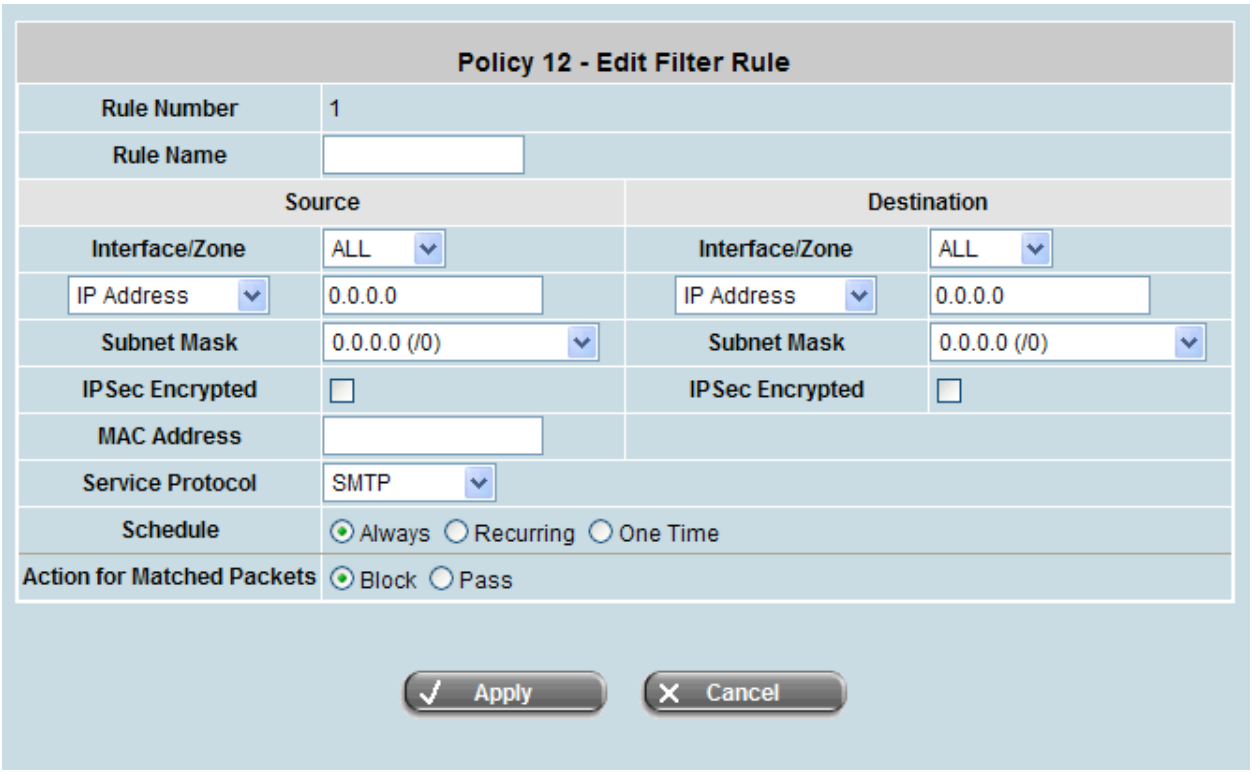
Moving onto the Policy definition steps in this example, chose the Users→Policy menu option and the following configuration screen will be presented:



The details of configuring Policies is covered extensively in the D-Link DSA-3600 Users Guide so any detailed discussion of Policies will not be covered in this document.

In the interests of proving that the *Class Policy Mapping* feature is working as part of the RADIUS authentication process, we have configured the following elements of *Policy 12*:

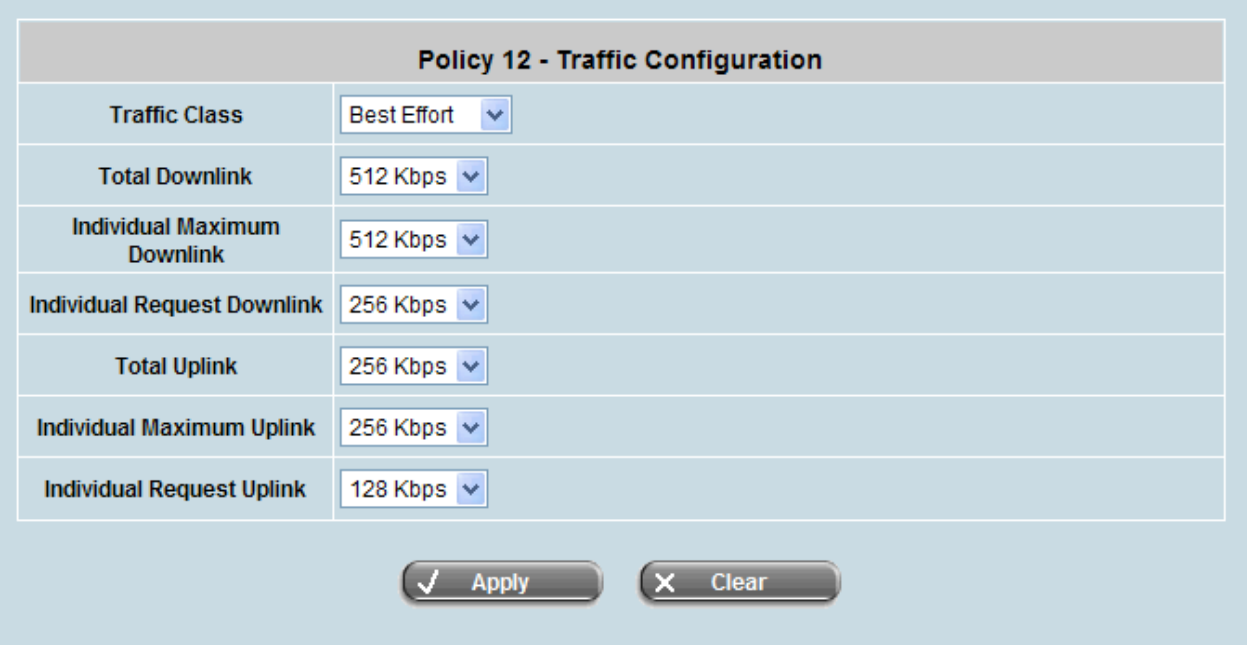
- *Firewall Profile* rule to block SMTP access outbound from the test client
- *QoS Profile* to rate-limit the upstream and downstream bandwidth available to the test client.



As can be seen from the above screenshot, a *Filter Rule* for *Policy 12* has been edited to Block any client traffic trying to access the SMTP *Service Protocol* on any Internet based server. Several other options are available to build granular firewall filters to match your deployment security policy.

Once all required *Firewall Rules* have been edited to match your security policy it is essential to enable the individual rules with the *Active* checkbox as shown below.

Moving onto the *QoS Profile,* the following screenshot details some sample settings of how the *Policy 12* configuration has been modified to constrain the available upstream and downstream client traffic. The *Traffic Class* that is associated with generic Internet access is *Best Effort.*



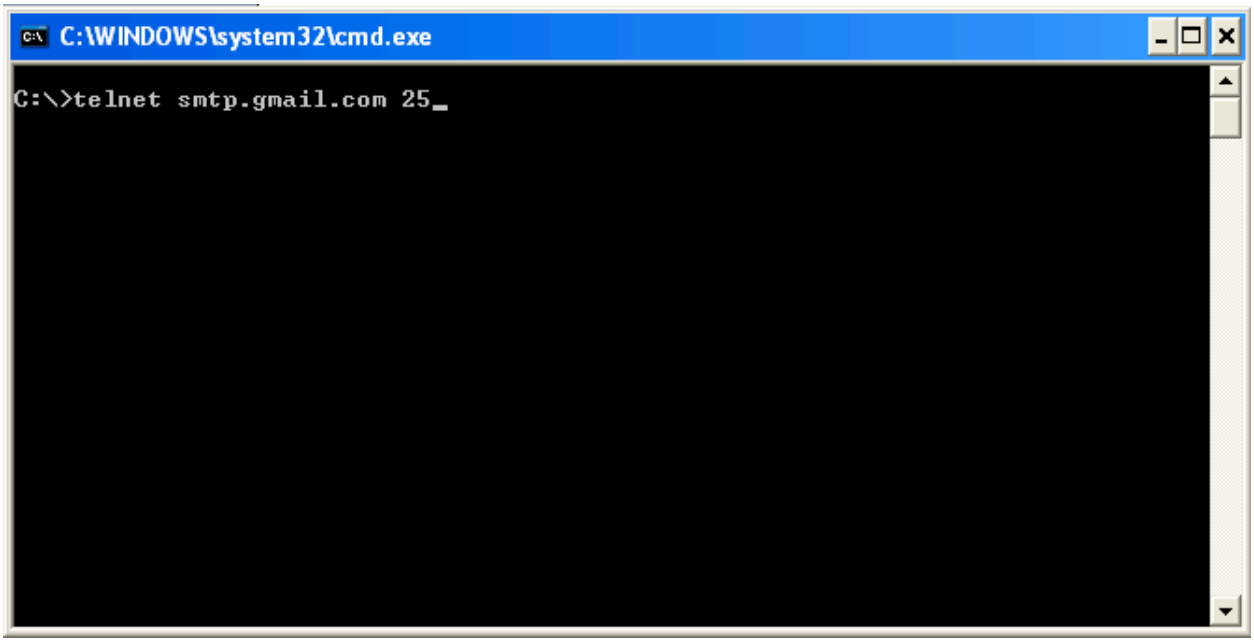
Test Result

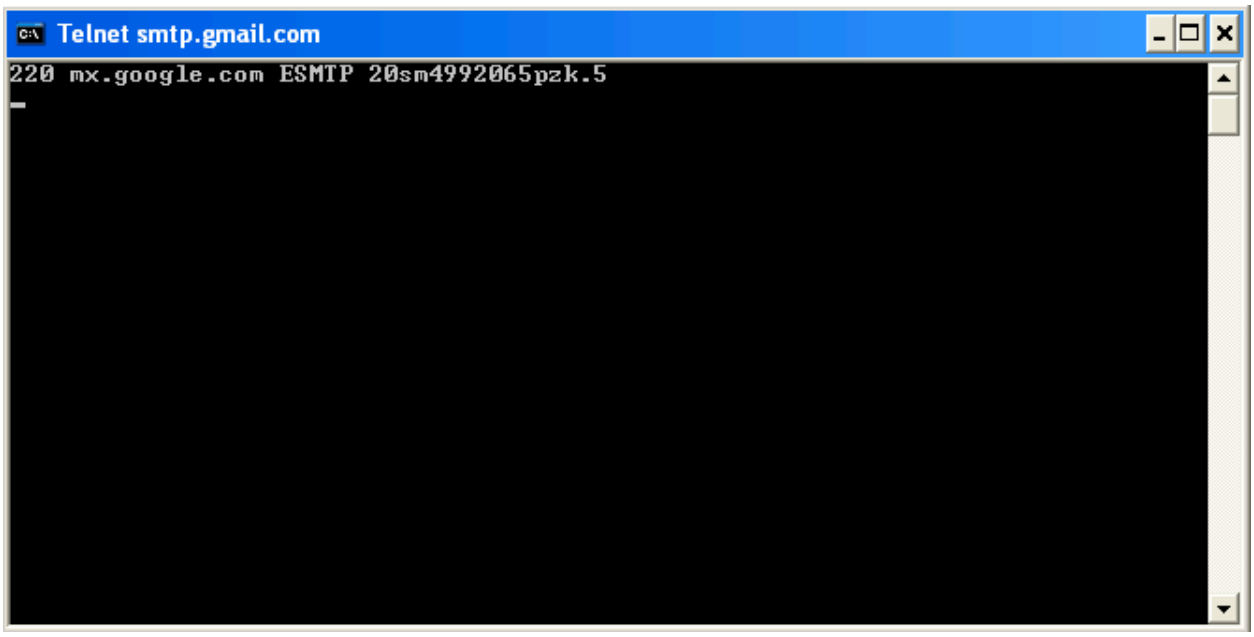
After making these changes to the DSA-3600 configuration, returning to the test laptop you can now test that both the firewalling and bandwidth management controls have been applied. For the changes to take affect you must logout and re-authenticate against the amigopod RADIUS server to apply these policy changes.

In order to demonstrate that both the *Firewalling* and *QoS Profile* settings have been applied the following sections include examples of the user experience prior to the additional constraints being applied.

Before Firewall Policy Applied

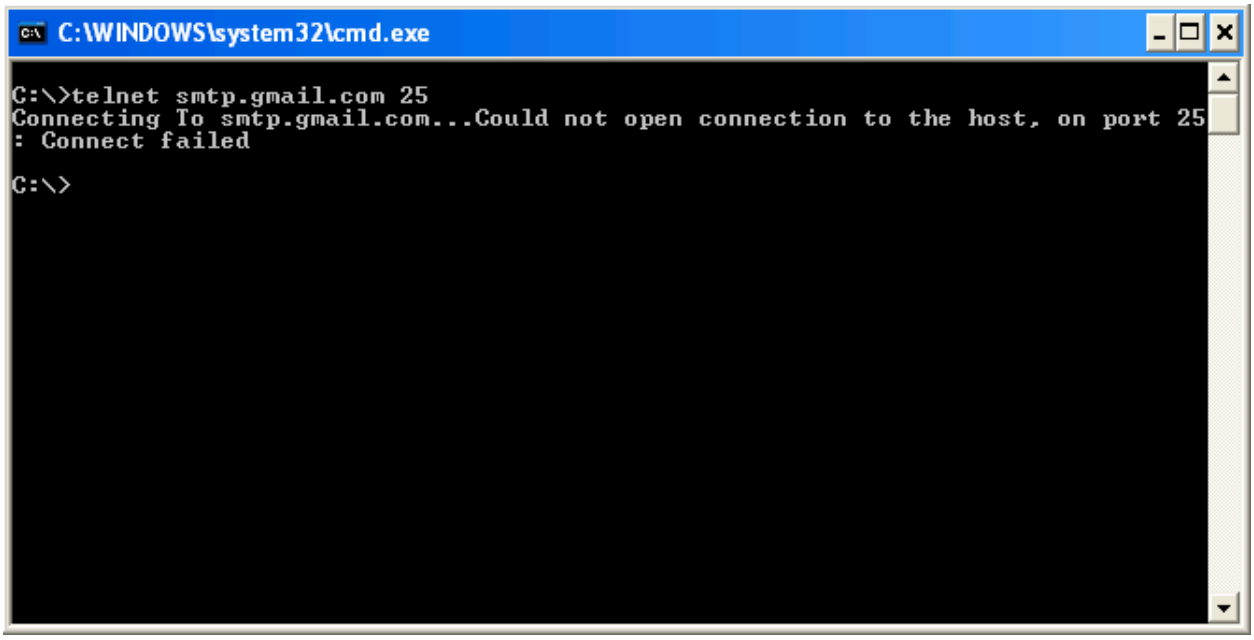
As can be seen from the following screen shots, prior to the new *Firewall* policy being applied the test laptop can successfully connect to an Internet based mail server on port 25 (SMTP).





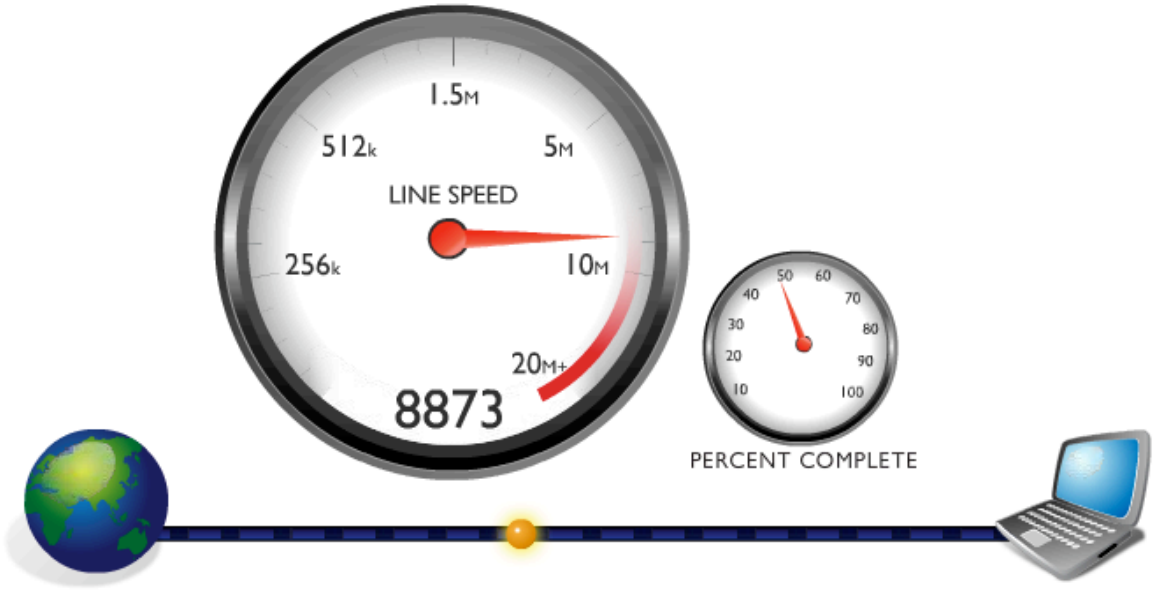
After Firewall Policy Applied

Now that the test user has re-authenticated and the new *Firewall* policy applied, any attempt to connect on port 25 is successfully blocked.



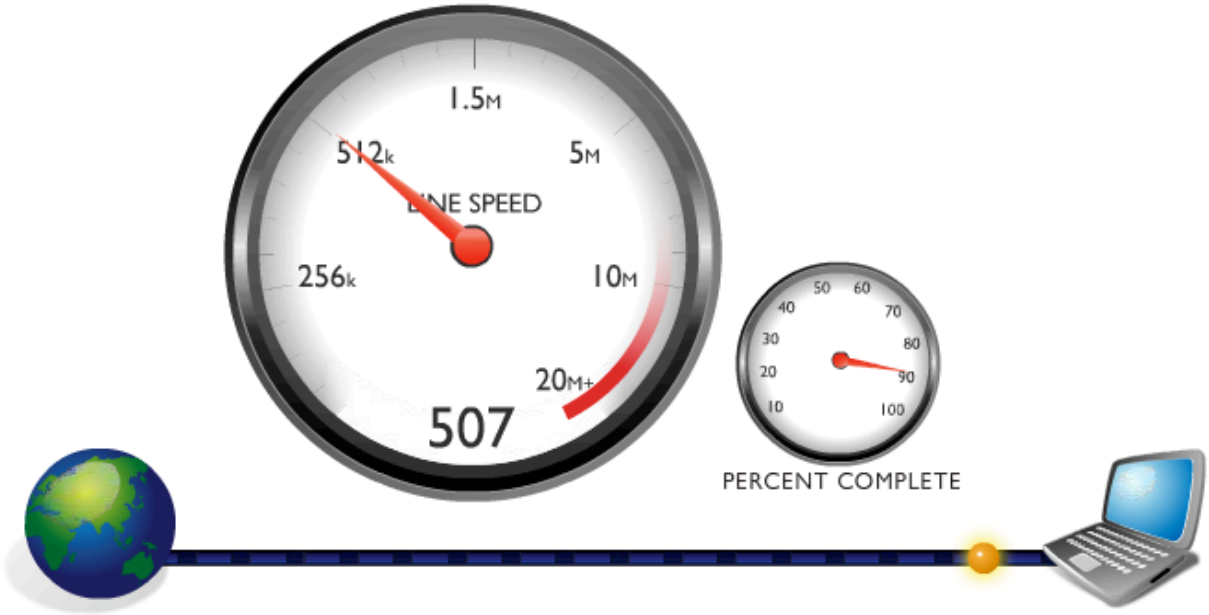
Before QoS Policy Applied

As can be seen from the Internet Speed Test results below that the available downstream bandwidth in the test environment is approaching 9Mbps without any *QoS Profile* applied.



After QoS Policy Applied

As expected after the configured *QoS Profile* is applied the Internet bandwidth has been successfully constrained to 512Kbps



Detailed RADIUS Debug

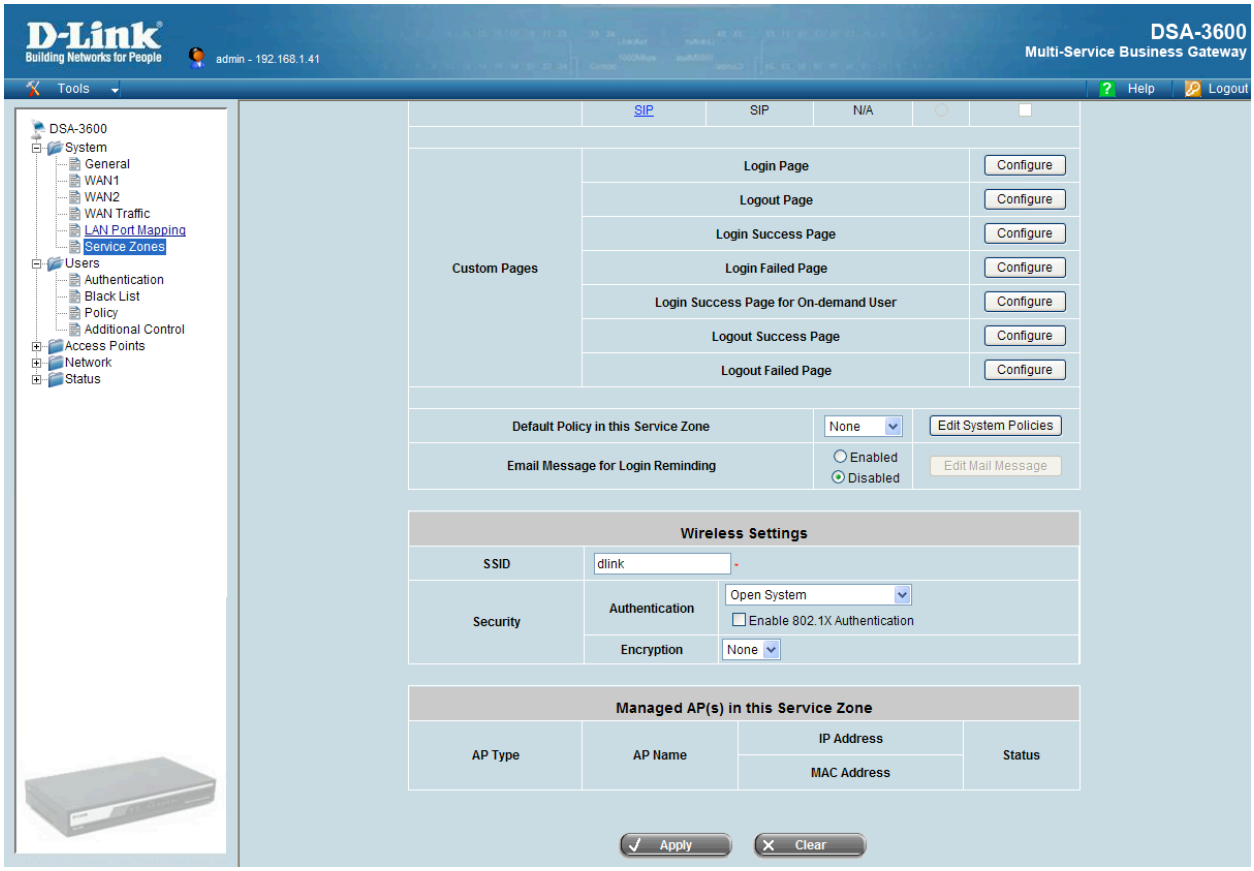
Also the following RADIUS debug successfully shows the additional *Class* attribute being sent back to the DSA-3600 to be applied to the policy configuration.

```
Ready to process requests.
rad_recv: Access-Request packet from host 10.0.20.166:1027, id=150, length=127
Service-Type = Call-Check
NAS-Identifier = "dsa-3600"
NAS-Port = 1
NAS-Port-Id = "Controlled"
NAS-Port-Type = Wireless-802.11
NAS-IP-Address = 10.0.20.166
User-Name = "cam"
User-Password = "wireless"
Called-Station-Id = "00-15-E9-DB-22-0B"
Calling-Station-Id = "00-13-D4-09-D3-F9"
rlm_sql (sql): Reserving sql socket id: 3
rlm_sql_postgresql: query: SELECT id, UserName, Attribute, Value, Op FROM radcheck
WHERE Username='cam' 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' 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' 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' 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
Exec-Program: /usr/bin/php /opt/amigopod/www/amigopod_request.php 2 4
Exec-Program-Wait: value-pairs: Class = "amigopod", Idle-Timeout = 300,
Exec-Program: returned: 0
Login OK: [cam] (from client DSA-3600 port 1 cli 00-13-D4-09-D3-F9)
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', 'wireless', '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 150 to 10.0.20.166 port 1027
Class = 0x616d69676f706f64
Idle-Timeout = 300
rad_recv: Accounting-Request packet from host 10.0.20.166:1027, id=194, length=145
Service-Type = Call-Check
NAS-Identifier = "dsa-3600"
NAS-Port = 1
NAS-Port-Id = "Controlled"
NAS-Port-Type = Wireless-802.11
NAS-IP-Address = 10.0.20.166
User-Name = "cam"
Acct-Status-Type = Start
Acct-Session-Id = "1260795282"
Acct-Delay-Time = 0
Acct-Authentic = RADIUS
Called-Station-Id = "00-15-E9-DB-22-0B"
Calling-Station-Id = "00-13-D4-09-D3-F9"
Framed-IP-Address = 192.168.1.41
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('1260795282', '8e38d415724e4fe1',
'cam', '', '10.0.20.166', ??'Controlled', 'Wireless-802.11', ('2009-12-10
15:04:28'::timestamp - '0'::interval), 'RADIUS', '', ??'00-15-E9-DB-22-0B', '00-13-D4-
09-D3-F9', 'Call-Check', '', ??'192.168.1.41', '0', (SELECT roledef.name FROM
useraccount LEFT JOIN roledef ON useraccount.role_id=roledef.id WHERE
useraccount.username='cam'))
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 194 to 10.0.20.166 port 1027
```

Appendix B - Advanced Customisation

As discussed in the DSA-3600 configuration section, there is support for either customizing internally or redirecting to an external server many of the web pages that make up the user experience. This configuration is performed under the *Custom Pages* section the *Service Zones* configuration as shown below:

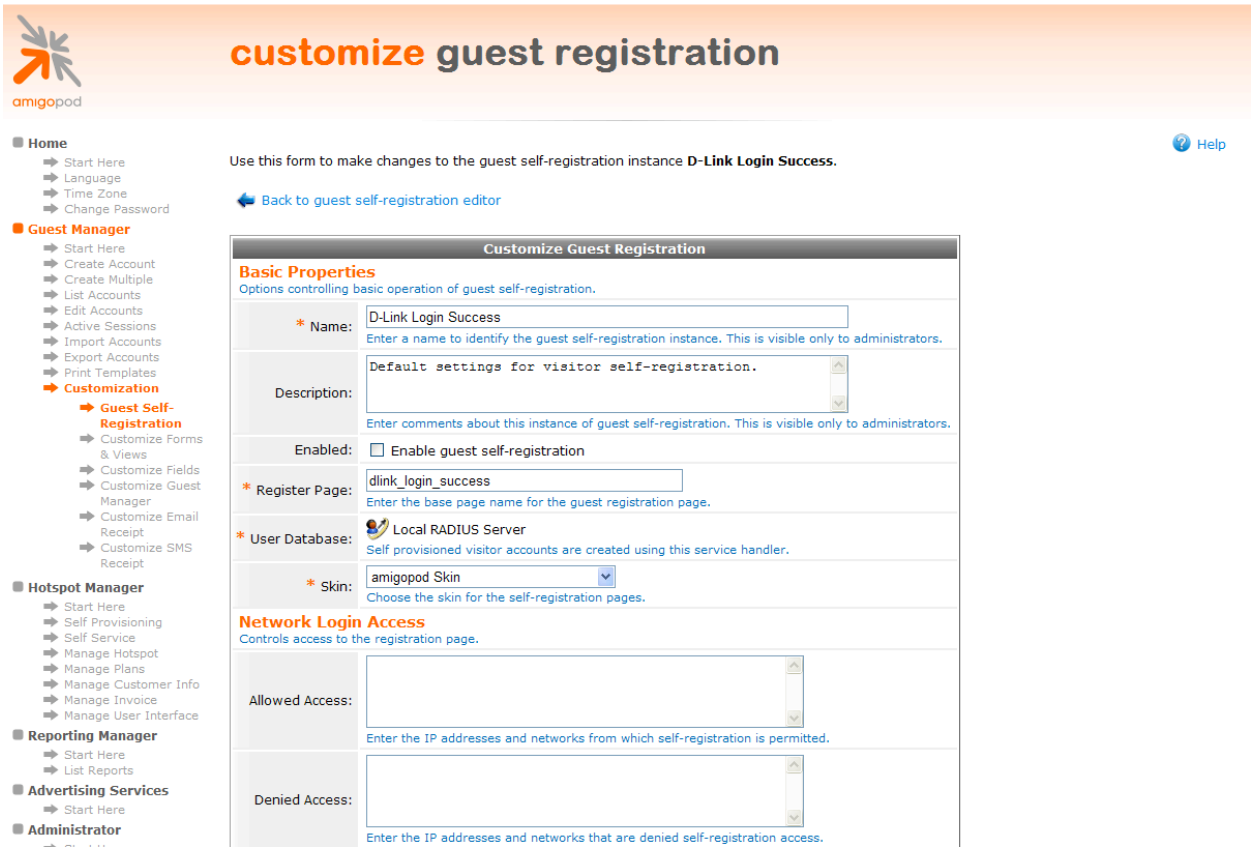


The previous configuration steps detailed the process for redirecting the *Login Page* option to the amigopod hosted *Web Login* to ensure consistent branding for the customer environment.

The following example provides some guidelines on how the remaining pages could be also redirected to amigopod hosted web pages to leverage the amigopod Skin technology for consistent branding.

Amigopod has several options for creating client facing web pages that support the use of the Skin technology for branding. The chosen platform for creating these simple landing pages is the *Guest Self Registration* pages that are available from the *Guest Manager→Customisation* menu option.

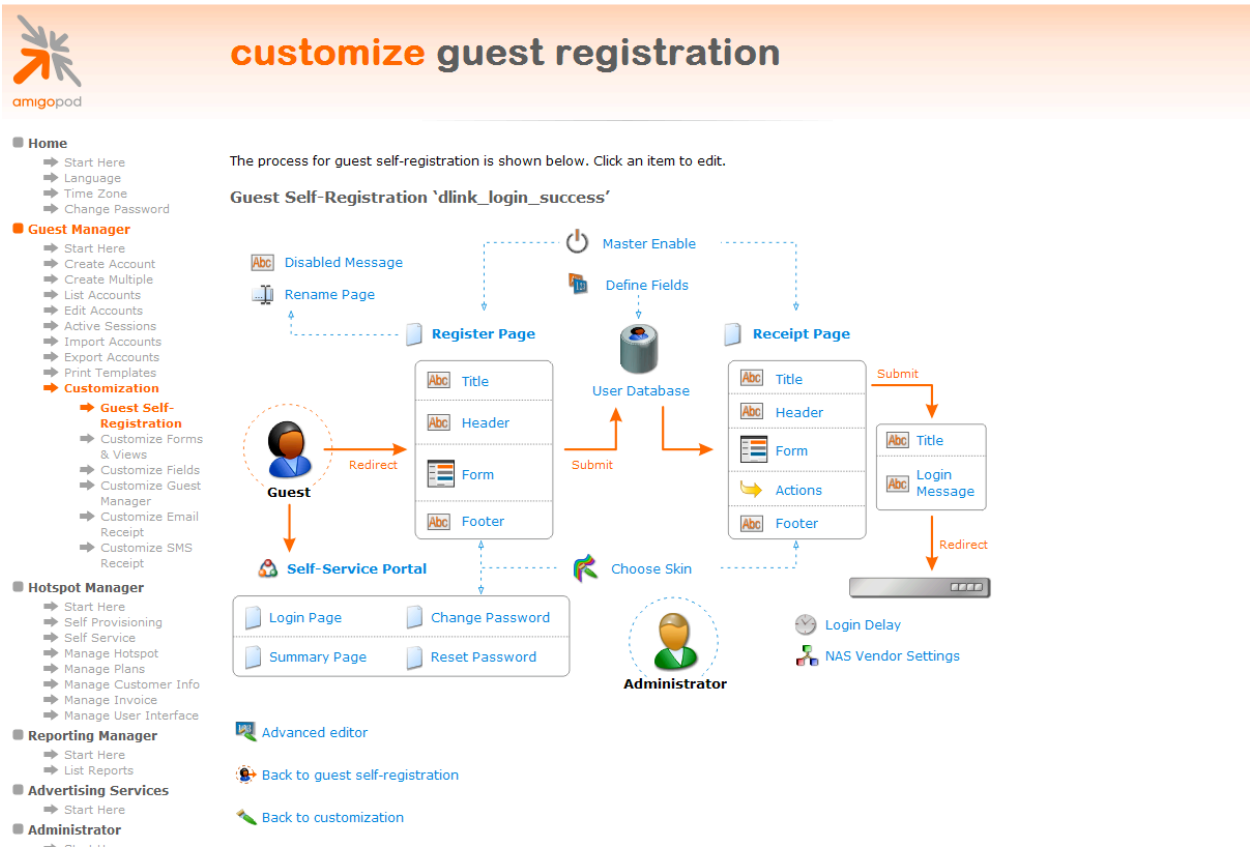
As shown below in the screenshot, fill out a preferred webpage name in the *Register Page* field and also ensure that the self-registration page is left disabled.



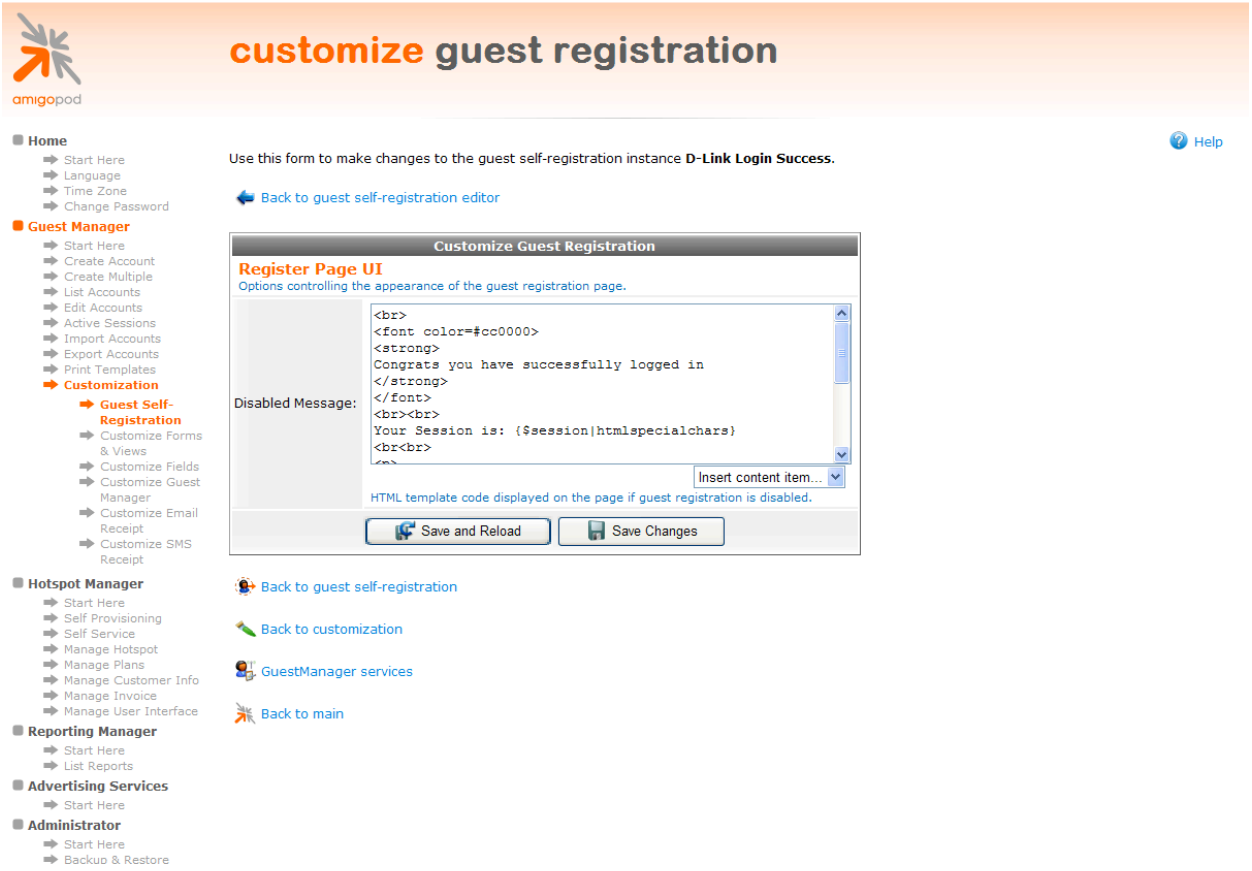
Note: Make note of the URL entered into the *Register Page* above. This URL will be required in the configuration of the Custom Pages settings on the D-Link DSA-3600 gateway. An example of the URL is shown below:

http://10.0.20.54/dlink_login_success.php

Now that the Guest Registration functionality has been disabled in the previous step, clicking on the *Register Page* part of the flow diagram will take you to the *Disable Message* configuration screen. The page will only be displayed whilst the Self Registration page is disabled and provides us with a simple method of configuring a Skin enabled blank web page host on the amigopod.



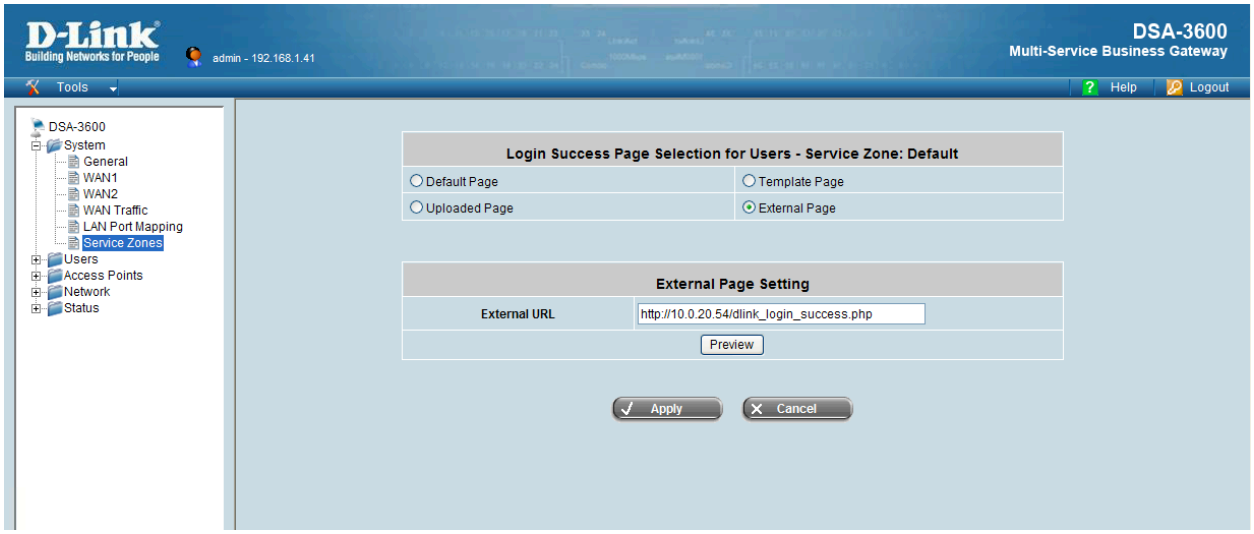
The following screenshot and HTML code extract provide a sample of how these customized pages can be hosted on the amigopod.



Although the sample HTML below is not very aesthetically pleasing, it is the functionality of parsing and using the Session identifier that we are trying to highlight. The Session identifier provides the appropriate unique identifier to allow the Logout button to execute the logout command on the DSA-3600.

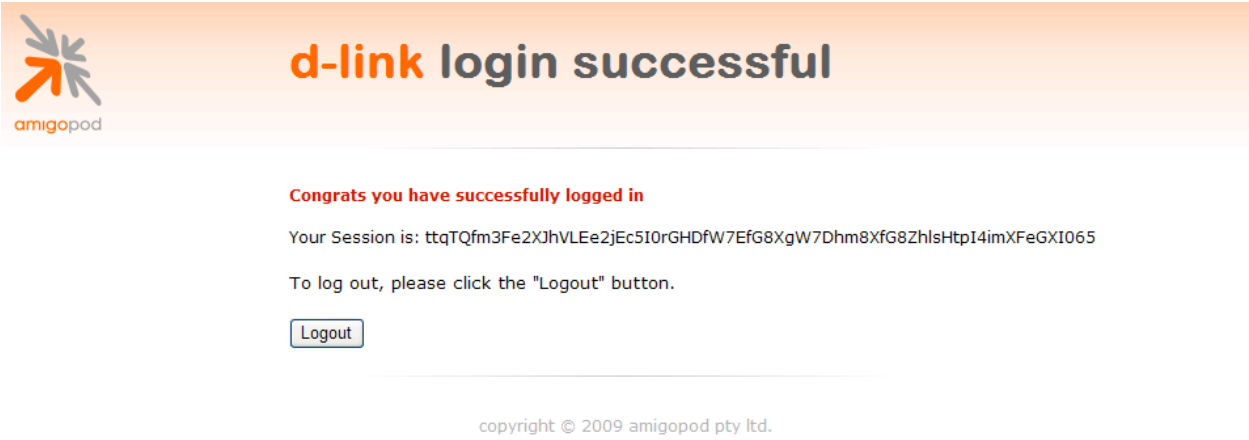
```
<br>
<font color=#cc0000>
<strong>
Congrats you have successfully logged in
</strong>
</font>
<br><br>
Your Session is: {$session|htmlspecialchars}
<br<br>
<p>
<font size="-1">To log out, please click the "Logout" button.
<br><br>
</font>
</p>
<input type=button value="Logout" style='font-
family:Arial;'onClick="window.location.href
('http://192.168.1.1/loginpages/logoff.shtml?session={$session|htmlspecialcha
rs}');">
```

Returning to the DSA-3600 *Custom Pages* configuration, click on the *Login Success Page* option and select the *External Page* radio button as shown below. Enter the URL, noted in the earlier step of creating the Self Registration page and click *Apply* to save the changes.



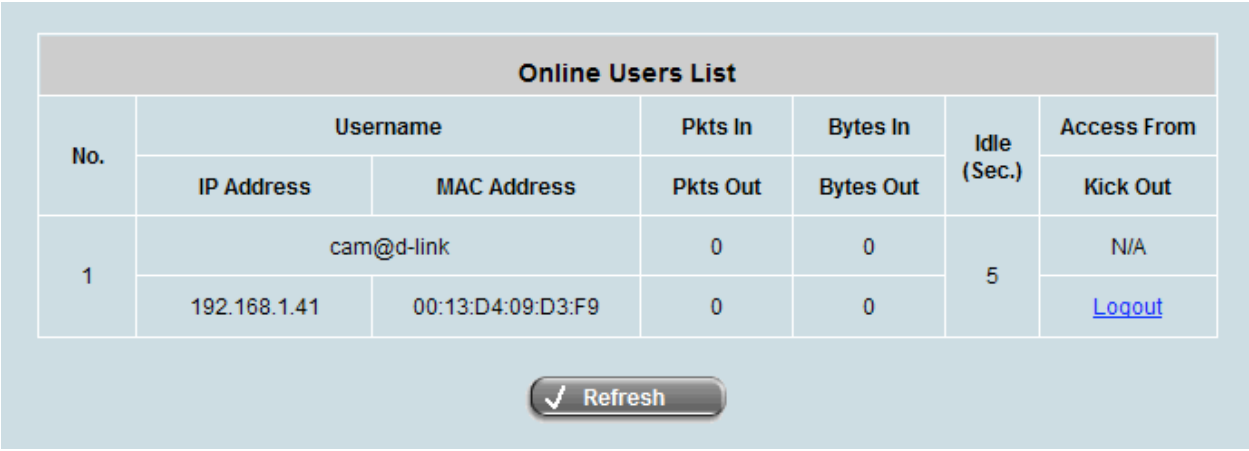
Testing the configuration

After successfully logging in the user experience should have changed from the default Login Success page hosted on the DSA-3600 to the new branded login page on the amigopod as shown below.

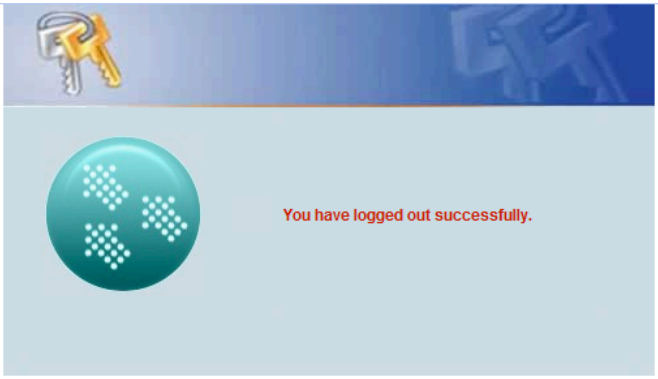


Verify the Logout button works as expected by simply clicking on the Logout button. The Session Identifier is just shown for illustrative and troubleshooting purposes.

Before issuing the Logout command you can verify the active session on the DSA-3600 by going to the *Status→Online Users* menu option as shown below:

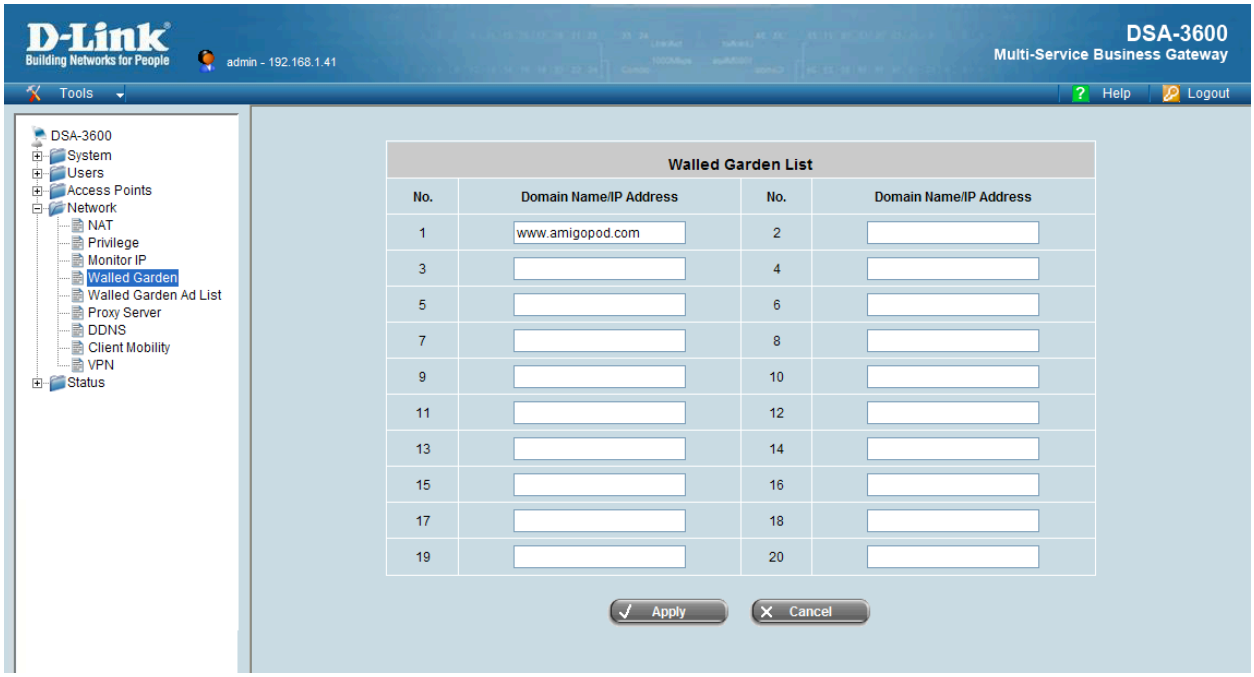


As can be seen the Logout button code worked as expected and the session has been redirected to the standard Logout Success web page hosted on the DSA-3600. The same process as shown here can be applied to each of the *Custom Pages* to achieve a consistent look and feel for the customer deployment.



Optional Walled Garden Access

Additionally from the *Network→Walled Garden* configuration option shown below several websites can be defined that will be served without requiring any user authentication. These sites may include sponsors or support web pages of the Hotspot in question.



Appendix C - Advanced RADIUS VSA Configuration

To be tested in new 3.60.00 firmware update from D-Link