Access Code Logins

Unified Visitor Management

amigopod Technical Note

Revision 1.0

30 September 2010

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

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

Australia & Pacific
+61 2 8669 1140

http://www.amigopod.com

Table of Contents

Introduction

This technical note explains the creation of bulk accounts and a login page that require a single access code for access to the network.

This method of authentication can be convenient for short-term access where security does not play as important of a role as security.

The accounts will be valid for 1 year, or 4 hours after the account first logs on.

NOTE The default username and password based authentication remains the preferred and recommend deployment for guest access.

Audience

This document is intended for network administrators and system integrators deploying an amigopod-based visitor management solution.

Basic familiarity with the amigopod Visitor Management Appliance is assumed. For in-depth information about the features and functions of the amigopod appliance, refer to the amigopod Deployment Guide.

Document Overview

The first section of the document explains configuring guest manager to create multiple accounts with the ability to login in with only the username. We will refer to this as an **Access Code**.

The next section will explain creating a web login that only requires the access code for entry onto the system

Finally, we will show you how to test the authentication.

Disclaimer

The topics of network design, security architectures and visitor access are complex subjects, and no single document can hope to cover all of the possible combinations of network equipment, network design, deployment requirements, and device configurations, nor can all the possible security implications for a particular recommendation be covered.

Therefore, while you read this document, it is best to consider it as a guide to developing your own understanding of the network design topics covered, and as a basis for further investigation.

Confirming Compatibility

Check Plugin Versions

Access Code logins requires the following plugin versions:

- amigopod RADIUS Services 3.0.4 or later
- GuestManager Plugin 3.0.3

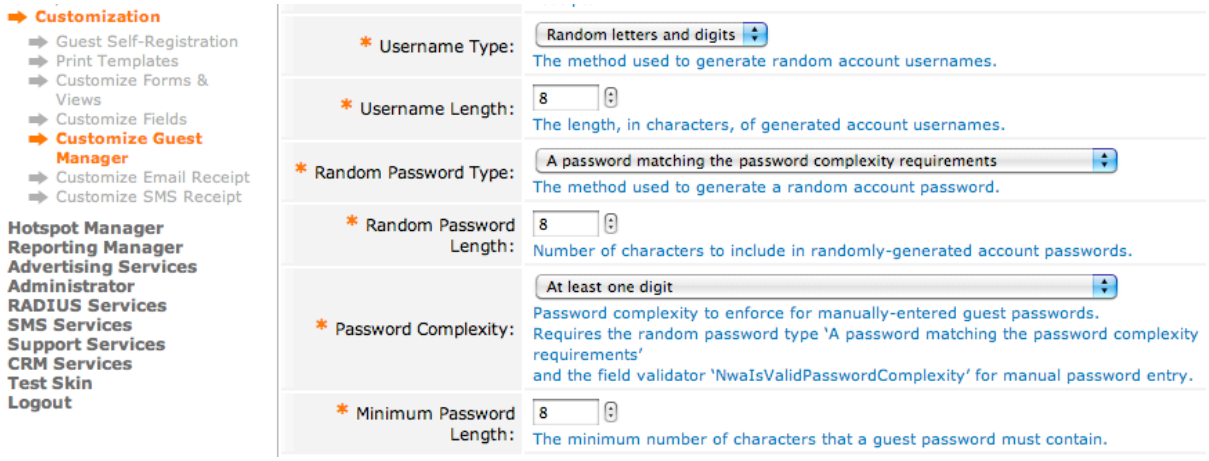
To verify you have the correct plugin versions installed, navigate to **Administrator** > **Plugin Manager** > **Manage Plugins** and check the version number in the list.

Use the **Update Plugins** link to download and install updated plugins.

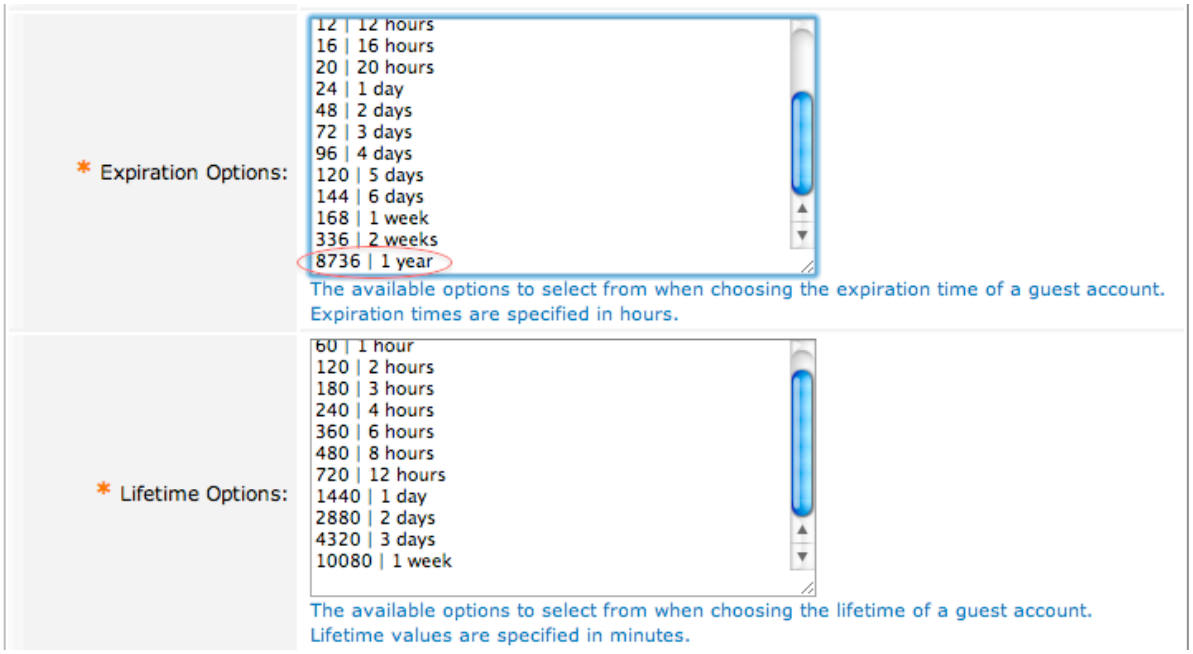
Customizing Guest Manager

Customize Random Username and Passwords

In this example we will set the random usernames and passwords to be a mix of letters and digits. Navigate to **Guest Manager > Customization > Customize Guest Manager**.



We have chosen an **8** character **Random letters and digits** username, and a **Password Complexity** of digits for the password. Note that the generator matching the complexity will also include a mix of upper and lower case letters.



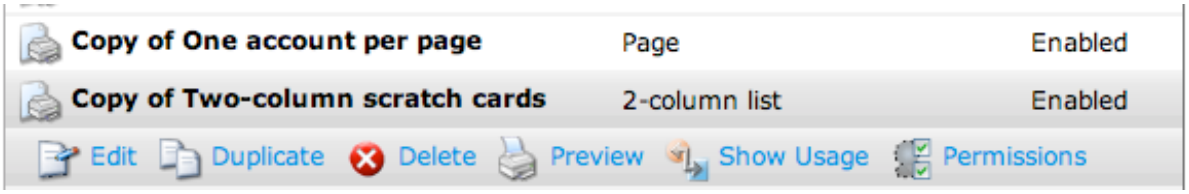
Our accounts will be created with an expiration of 1 year and a lifetime of 4 hours. By default the expiration list does not have a value for 1 year. We have added 8736 (24 * 365) as an additional value.

Create a Print Template

By default, the print templates include username, password, expiration, as well as other options. For the purpose of access codes, we only want the username presented.

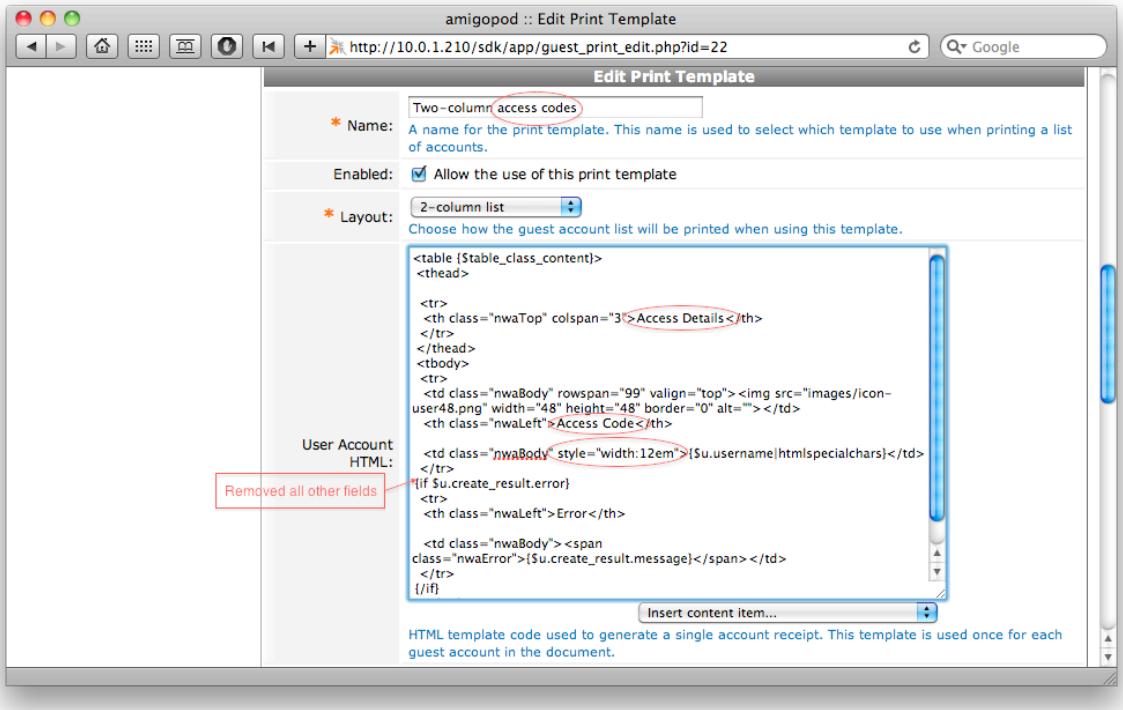
Create the Print Template

We will base our print template off one of the existing scratch card templates. Navigate to **Guest Manager > Customization > Print Templates** and select **Two-column scratch cards** and click **Duplicate**.



Edit the Print Template

We need to replace Username for Access Code, as well as remove the extraneous data.



The exact text is provided below.

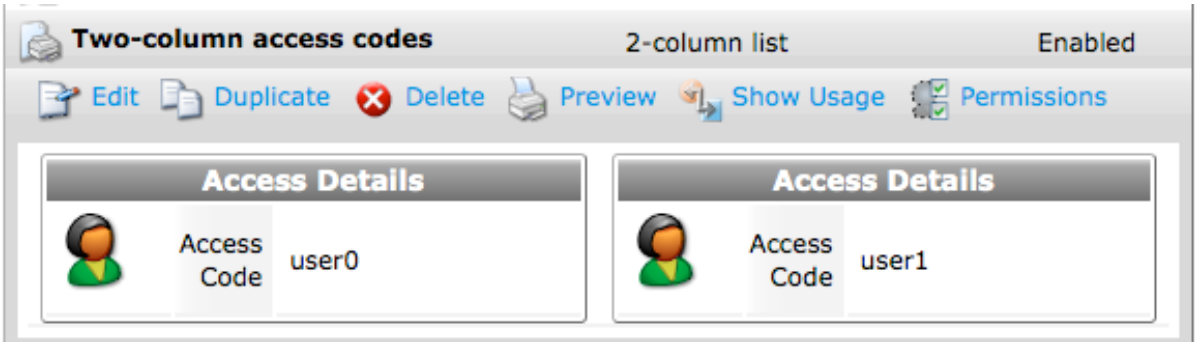
```
<table {$table_class_content}>
 <thead>

  <tr>
   <th class="nwaTop" colspan="3">Access Details</th>
```

```
  </tr>
 </thead>
 <tbody>
  <tr>
   <td class="nwaBody" rowspan="99" valign="top"><img
src="images/icon-user48.png" width="48" height="48" border="0"
alt=""></td>
   <th class="nwaLeft">Access Code</th>

   <td class="nwaBody"
style="width:12em">{$u.username|htmlspecialchars}</td>
  </tr>
 {if $u.create_result.error}
  <tr>
   <th class="nwaLeft">Error</th>

   <td class="nwaBody"><span
class="nwaError">{$u.create_result.message}</span></td>
  </tr>
 {/if}
 </tbody>
</table>
```



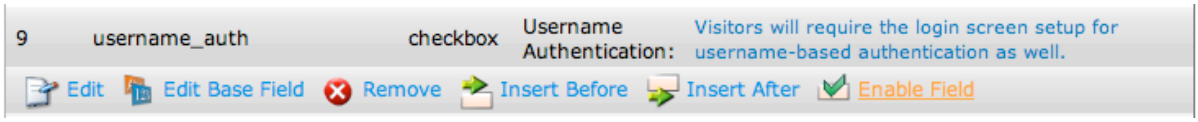
Customize Create Multi

Create Multi is the screen used to generate accounts with random usernames and passwords. We need to modify it to add a flag to accounts to allow the access-code based authentication.

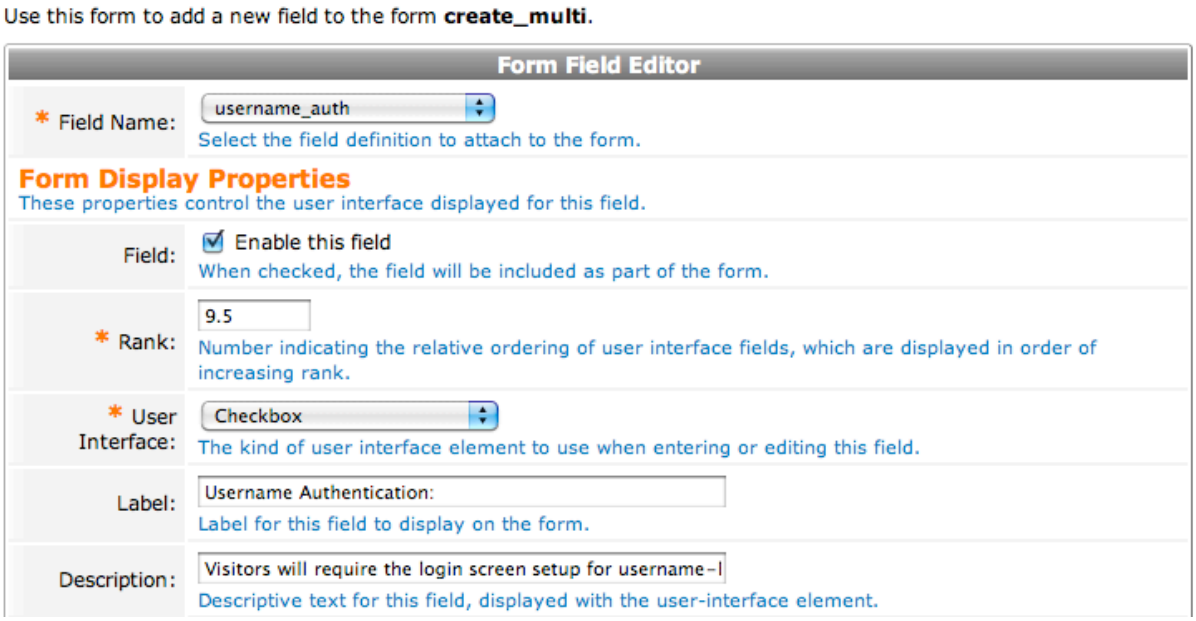
Add username_auth the the Field List

Navigate to **Guest Manager > Customization > Customize Forms & Views** and select **create_multi** and then click **Edit Fields**. Look for a field named **username_auth**.

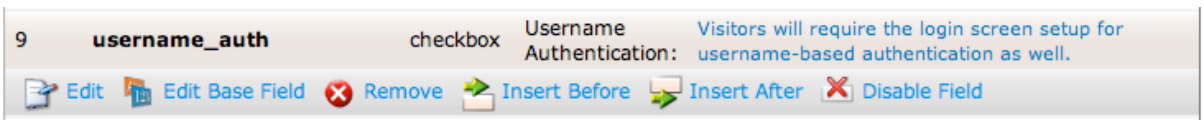
If the field exists, but is not bolded and enabled, click **Enable Field**.



If the field does not exist, select a field that does (num_accounts) and select **Insert After**. Select **username_auth** from the **Field Name** dropdown and allow the page to refresh. The defaults should be acceptable, but feel free to customize the label or description.



Once the field is enabled or inserted, you should see it bolded in the list of fields.

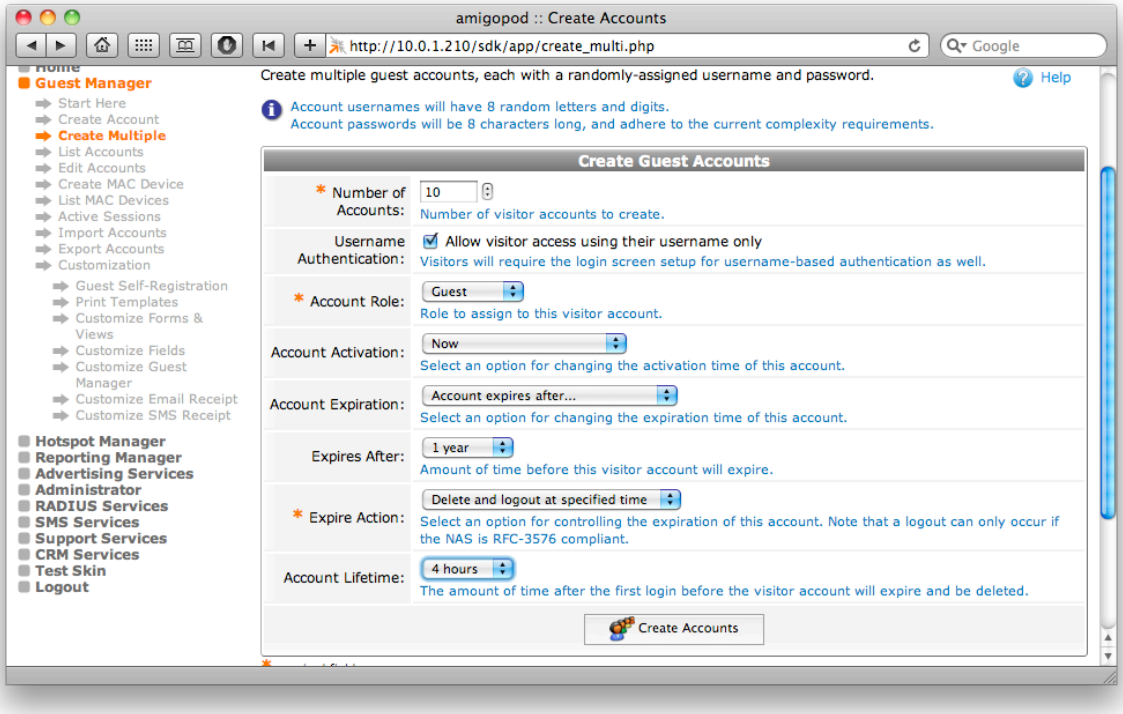


Create Multiple Accounts

With the account generation customized, we can now create our accounts.

Create Multi

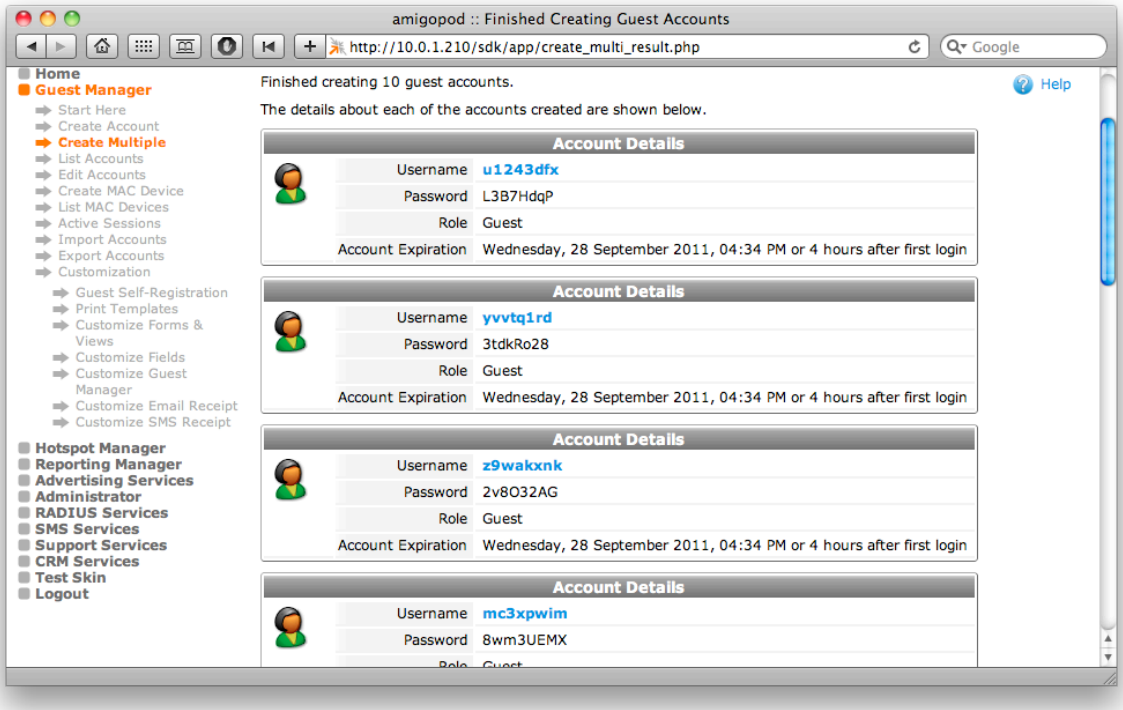
Navigate to **Guest Manager > Create Multi** (or select **Use this form** from the previous fields list). We will create 10 accounts that will expire in 1 year, or 4 hours after they first log in, whichever comes first.



NOTE Note that the Username Authentication field we added must be selected. Otherwise if the username is entered on the login screen, the authentication will be denied.

Create Multi Results

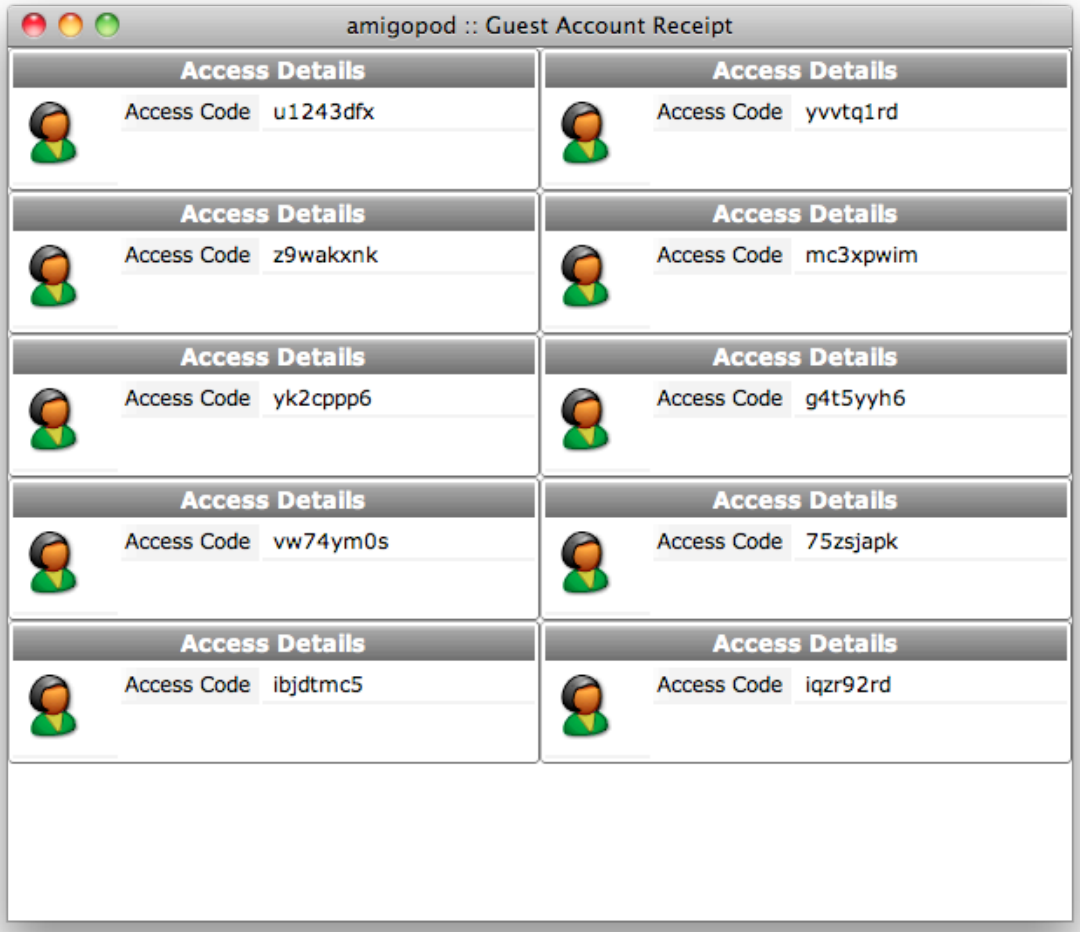
After clicking Create Accounts, the results page will be displayed with a list of accounts. If a large number of accounts are created at one time they may not all be displayed at the same time. This will not effect the printing action



Confirm that the accounts settings are as you expected with respect to letters and digits in the username and password, expiration, and role.

Print Cards

Select the new print template from the dropdown at the bottom of the table. A new window or tab will open with the cards.



NOTE Your method of printing and delivery to the customer should define the print template used in production. If you have a label printer, or cards, they should be tested prior to the creation of the actual accounts.

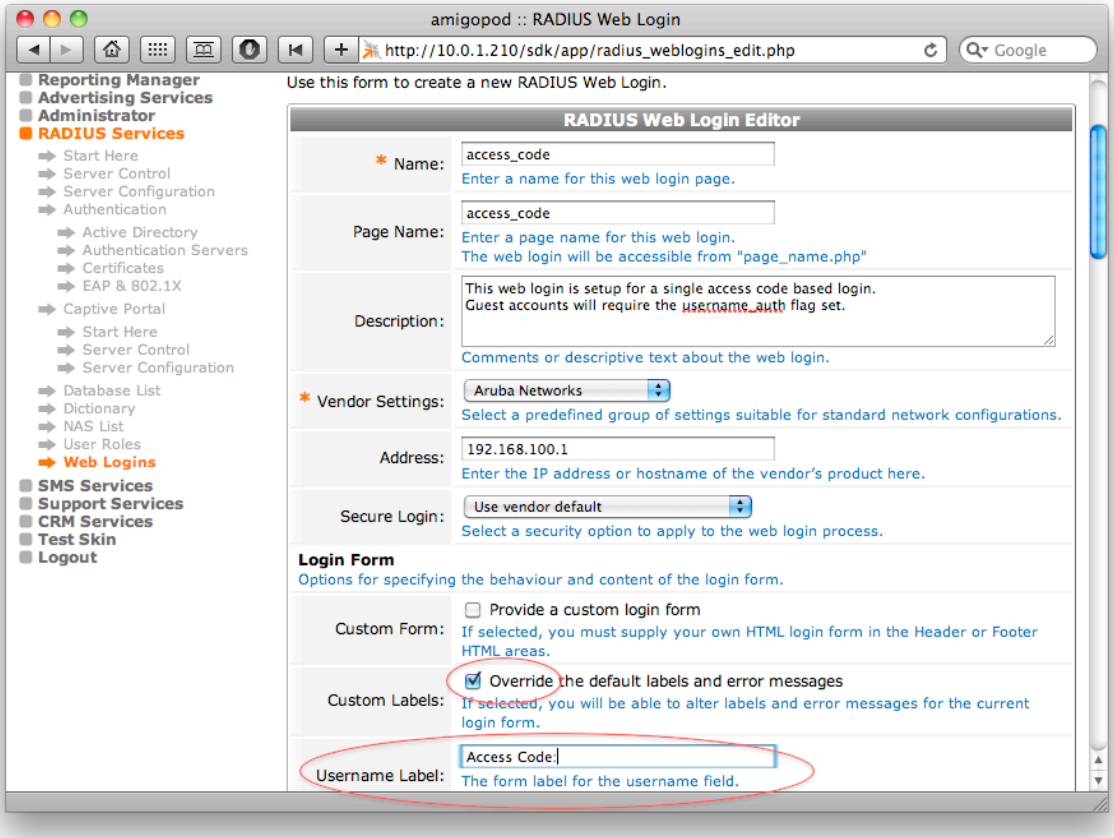
Creating a Web Login Page

The web login will need to be customized to hide the password, and check for accounts with the username_auth flag set.

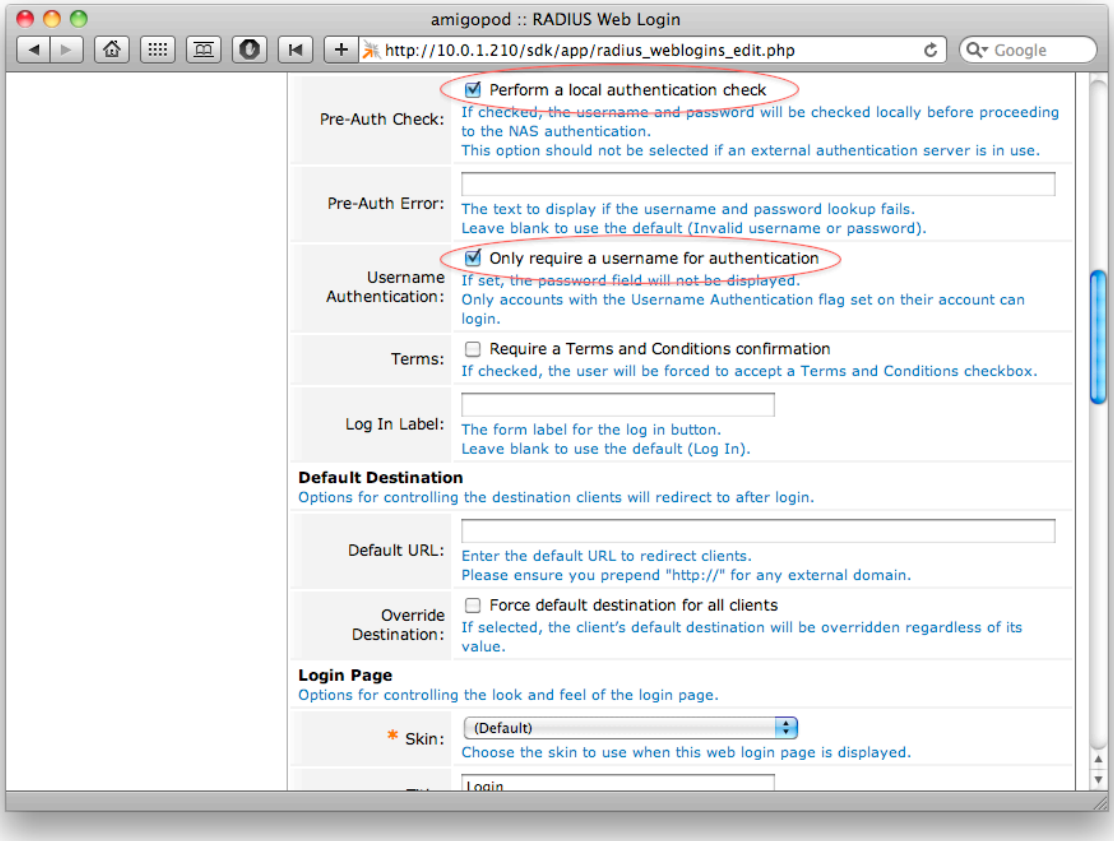
Create a Web Login

Navigate to **RADIUS Services > Web Logins** and **click Create a new web login page** at the bottom of the table.

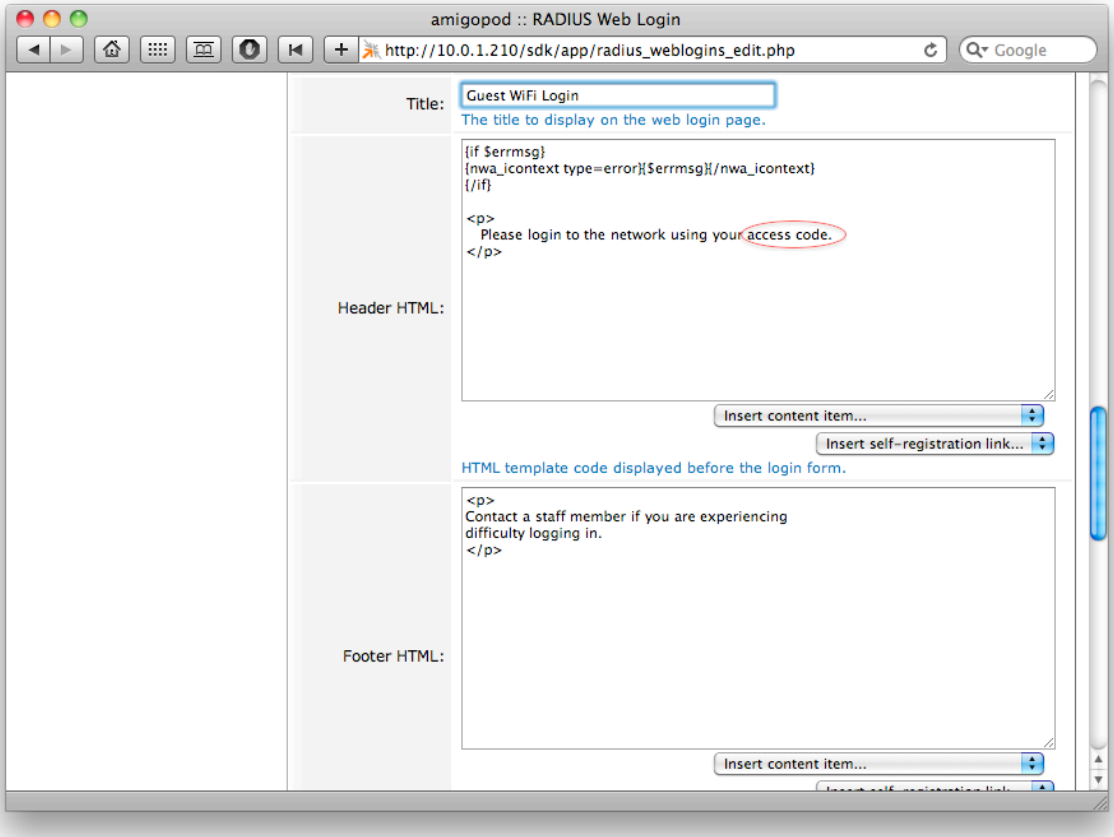
In our example we will create a page called **access_codes** that has been customized to our liking.



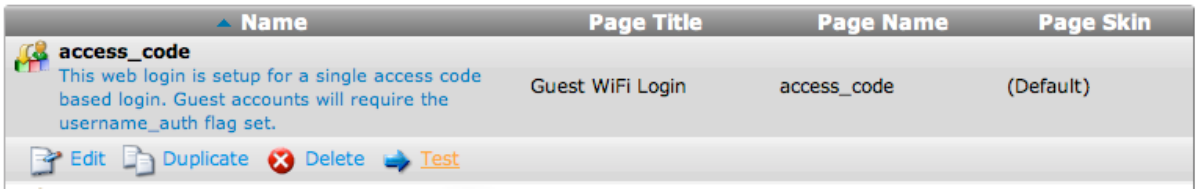
In order to provide access-code based authentication, we must also enable the Pre-Auth Check.



We also update the helper text to remove mention of username or password.



Click **Save Changes** to create the web login.



Select Test to open the login page in a new window or tab.


amigopod :: Guest WiFi Login
http://10.0.1.210/sdk/app/access_code.php
Google
amigopod
guest wifi login
Please login to the network using your access code.
Guest WiFi Login
* Access Code:
Log In
* required field
Contact a staff member if you are experiencing difficulty logging in.
copyright © 2010 amigopod pty ltd.

Testing Authentication

WLAN Controller and Access Point setup

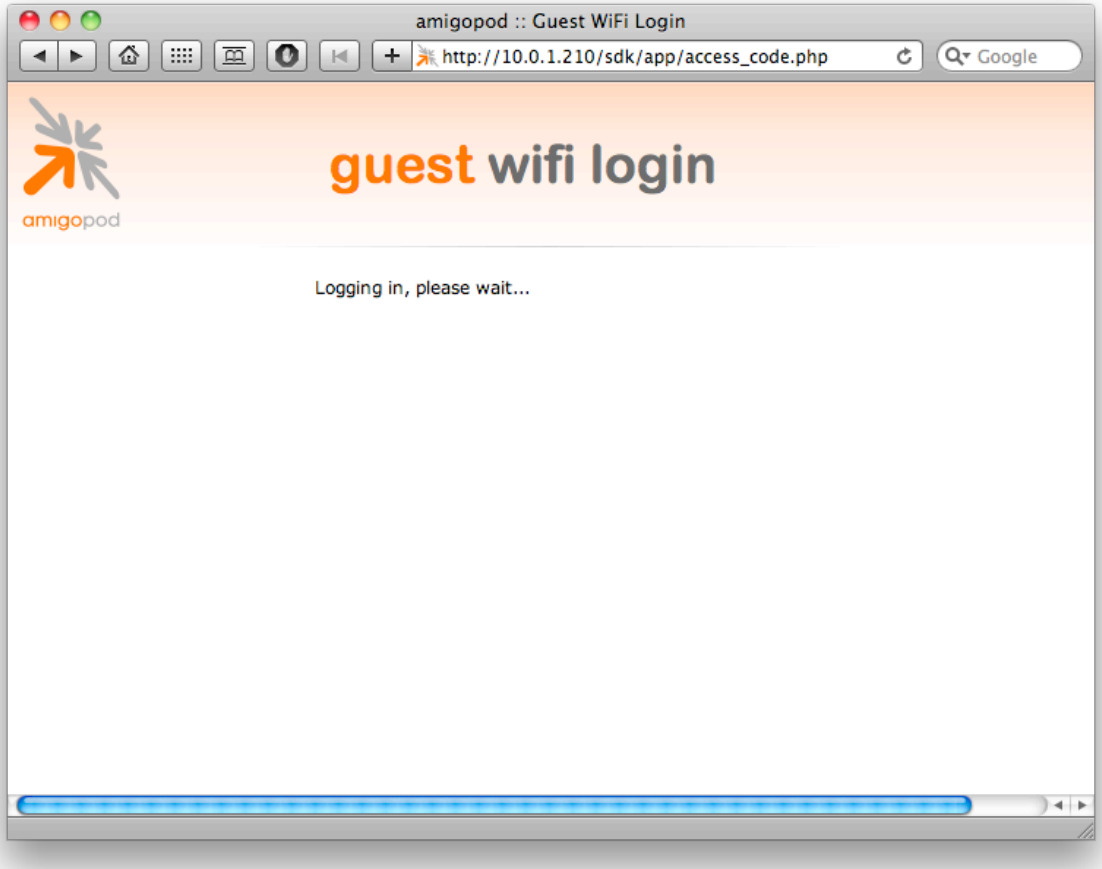
Please refer to your WLAN reference documentation where to configure the external redirection URL. Enter the URL as it appeared when clicking **Test**.

As a proof of concept, some of the below steps can be used without being connected to the WLAN. However the test will not do complete a RADIUS authentication to verify the complete setup.

Authenticating

Connect to the WLAN and open your browser to a web page. You should be redirect to the web login configured above. Enter one of the access codes generated previously.

Select Log In and you should briefly see a logging in message, followed by a successful authentication with the WLAN.



Troubleshooting

Invalid username or password

If you receive the error **Invalid username or password**, it could be due to an username that does not exist, which you can check in the List Accounts list. It could also be due to not selecting **Allow visitor access using their username only** while creating the accounts. To verify the flag, you can add **username_auth** to the **List Accounts** column view (**guest_users**), or the **guest_edit** form, and then edit the user.

Logging in timeout

If you sit on the logging in page until it times out, confirm that you have entered the WLAN settings correctly on the web login page.

WLAN Authentication Failure

If you get an error regarding authentication from the WLAN, ensure your RADIUS settings, especially the shared secret are configured correctly. RADIUS Services > Server Control > Debug RADIUS Server can be very useful in determining errors.