



amigopod

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	3
Audience	3
Document Overview	3
Disclaimer.....	3
Confirming Compatibility	4
Check Plugin Versions	4
Customizing Guest Manager	5
Customize Random Username and Passwords.....	5
Create a Print Template.....	6
Create the Print Template	6
Edit the Print Template.....	6
Customize Create Multi.....	8
Add username_auth the the Field List	8
Create Multiple Accounts	9
Create Multi.....	9
Create Multi Results	9
Print Cards	10
Creating a Web Login Page.....	12
Create a Web Login	12
Testing Authentication	16
WLAN Controller and Access Point setup.....	16
Authenticating.....	16
Troubleshooting.....	17
Invalid username or password.....	17
Logging in timeout	17
WLAN Authentication Failure	17

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**.

- ➔ Customization
 - ➔ Guest Self-Registration
 - ➔ Print Templates
 - ➔ Customize Forms & Views
 - ➔ Customize Fields
 - ➔ **Customize Guest Manager**
 - ➔ Customize Email Receipt
 - ➔ Customize SMS Receipt
- Hotspot Manager
- Reporting Manager
- Advertising Services Administrator
- RADIUS Services
- SMS Services
- Support Services
- CRM Services
- Test Skin
- Logout

* Username Type:	Random letters and digits <input type="button" value="v"/> <small>The method used to generate random account usernames.</small>
* Username Length:	8 <input type="button" value="v"/> <small>The length, in characters, of generated account usernames.</small>
* Random Password Type:	A password matching the password complexity requirements <input type="button" value="v"/> <small>The method used to generate a random account password.</small>
* Random Password Length:	8 <input type="button" value="v"/> <small>Number of characters to include in randomly-generated account passwords.</small>
* Password Complexity:	At least one digit <input type="button" value="v"/> <small>Password complexity to enforce for manually-entered guest passwords. Requires the random password type 'A password matching the password complexity requirements' and the field validator 'NwaIsValidPasswordComplexity' for manual password entry.</small>
* Minimum Password Length:	8 <input type="button" value="v"/> <small>The minimum number of characters that a guest password must contain.</small>

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.

* Expiration Options:	<div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;"> <ul style="list-style-type: none"> 12 12 hours 16 16 hours 20 20 hours 24 1 day 48 2 days 72 3 days 96 4 days 120 5 days 144 6 days 168 1 week 336 2 weeks <li style="border: 1px solid red;">8736 1 year </div> <p><small>The available options to select from when choosing the expiration time of a guest account. Expiration times are specified in hours.</small></p>
* Lifetime Options:	<div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;"> <ul style="list-style-type: none"> 60 1 hour 120 2 hours 180 3 hours 240 4 hours 360 6 hours 480 8 hours 720 12 hours 1440 1 day 2880 2 days 4320 3 days 10080 1 week </div> <p><small>The available options to select from when choosing the lifetime of a guest account. Lifetime values are specified in minutes.</small></p>

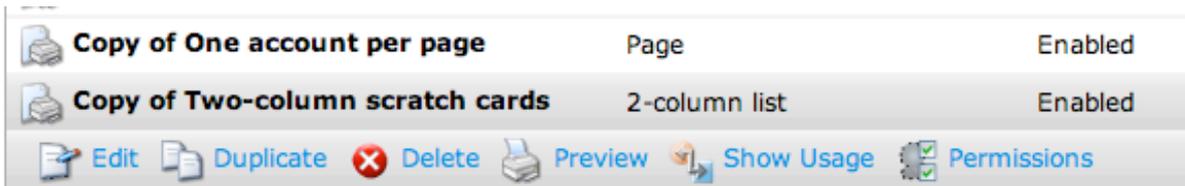
Our accounts will be created with an expiration of 1 year and a lifetime of 4 hours. By default the expiration list does not have a value for 1 year. We have added 8736 (24 * 365) as an additional value.

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.

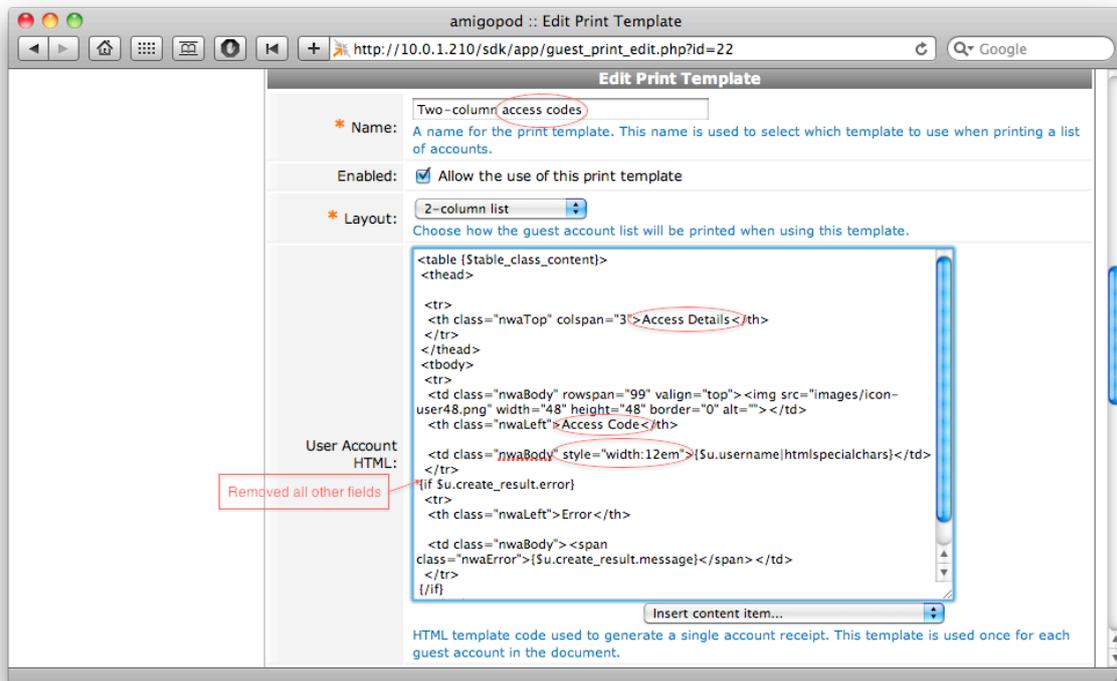
Create the Print Template

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"></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>

```

Two-column access codes 2-column list **Enabled**

[Edit](#)
[Duplicate](#)
[Delete](#)
[Preview](#)
[Show Usage](#)
[Permissions](#)

Access Details			Access Details		
	Access Code	user0		Access Code	user1

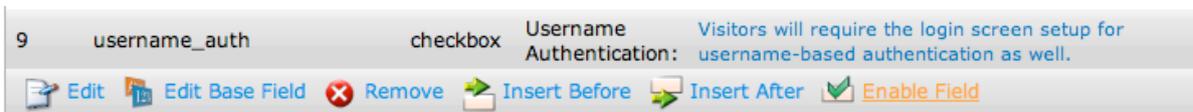
Customize Create Multi

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.

Use this form to add a new field to the form **create_multi**.

Form Field Editor

* Field Name:
Select the field definition to attach to the form.

Form Display Properties
These properties control the user interface displayed for this field.

Field: **Enable this field**
When checked, the field will be included as part of the form.

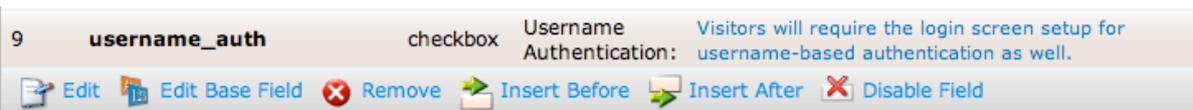
* Rank:
Number indicating the relative ordering of user interface fields, which are displayed in order of increasing rank.

* User Interface:
The kind of user interface element to use when entering or editing this field.

Label:
Label for this field to display on the form.

Description:
Descriptive text for this field, displayed with the user-interface element.

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.

amigopod :: Create Accounts

http://10.0.1.210/sdk/app/create_multi.php

Create multiple guest accounts, each with a randomly-assigned username and password.

Account usernames will have 8 random letters and digits.
Account passwords will be 8 characters long, and adhere to the current complexity requirements.

Create Guest Accounts

* Number of Accounts: 10
Number of visitor accounts to create.

Username Authentication: Allow visitor access using their username only
Visitors will require the login screen setup for username-based authentication as well.

* Account Role: Guest
Role to assign to this visitor account.

Account Activation: Now
Select an option for changing the activation time of this account.

Account Expiration: Account expires after...
Select an option for changing the expiration time of this account.

Expires After: 1 year
Amount of time before this visitor account will expire.

* Expire Action: Delete and logout at specified time
Select an option for controlling the expiration of this account. Note that a logout can only occur if the NAS is RFC-3576 compliant.

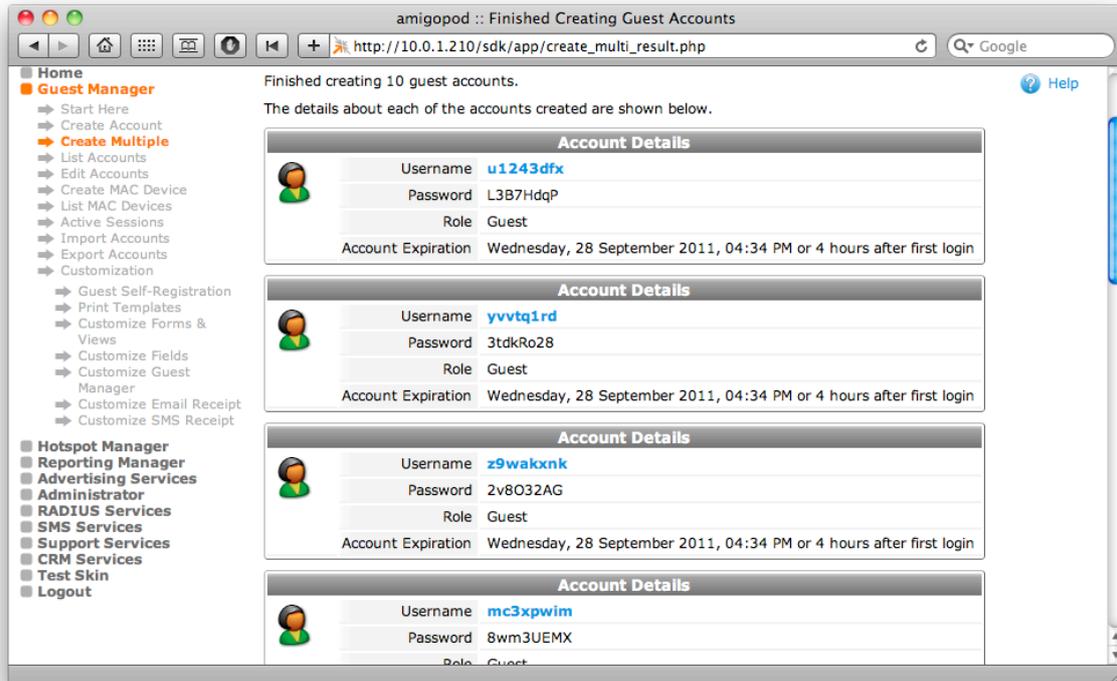
Account Lifetime: 4 hours
The amount of time after the first login before the visitor account will expire and be deleted.

Create Accounts

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

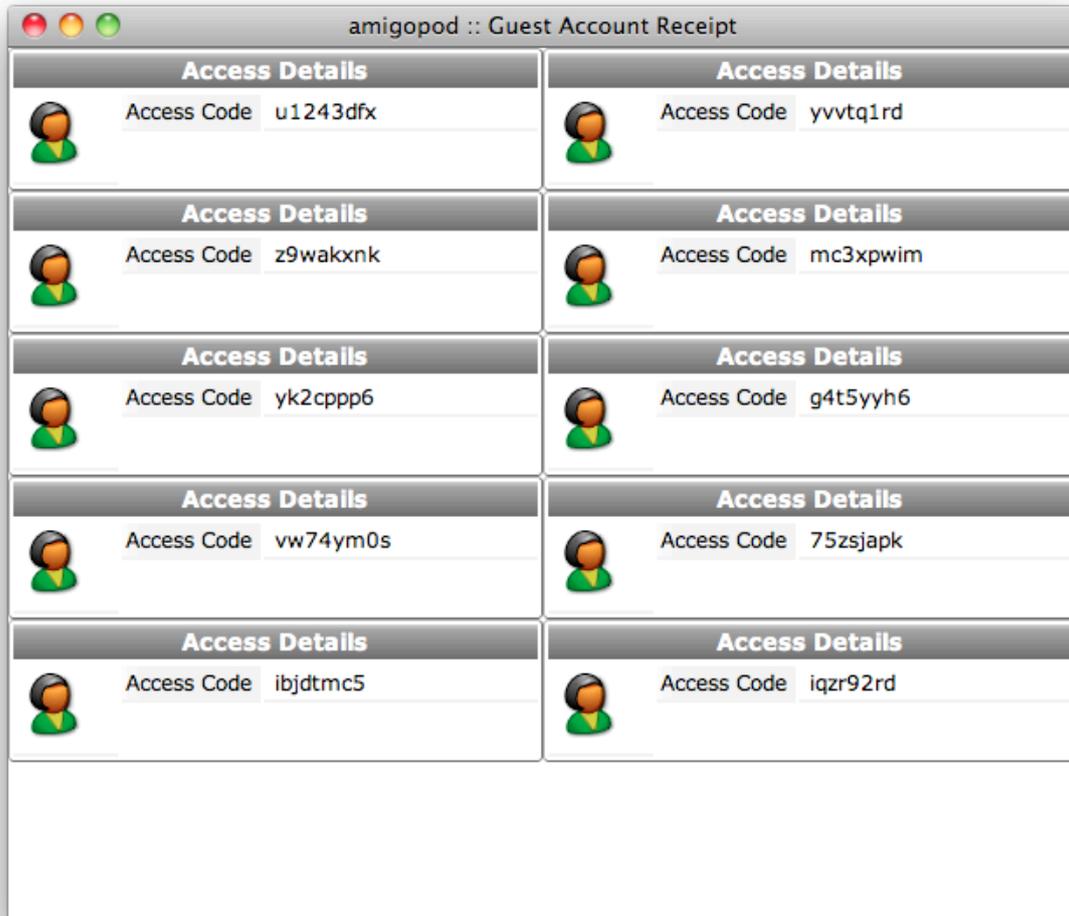
After clicking Create Accounts, the results page will be displayed with a list of accounts. If a large number of accounts are created at one time they may not all be displayed at the same time. This will not effect the printing action



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.

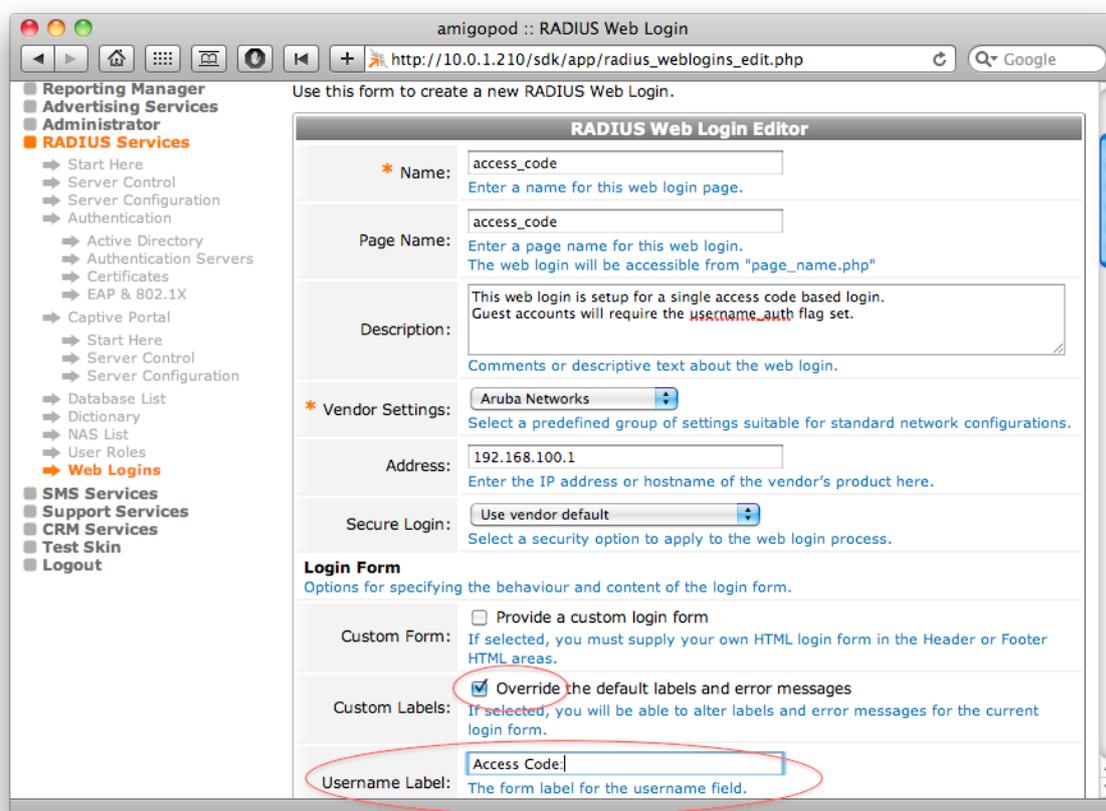
Creating a Web Login Page

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.

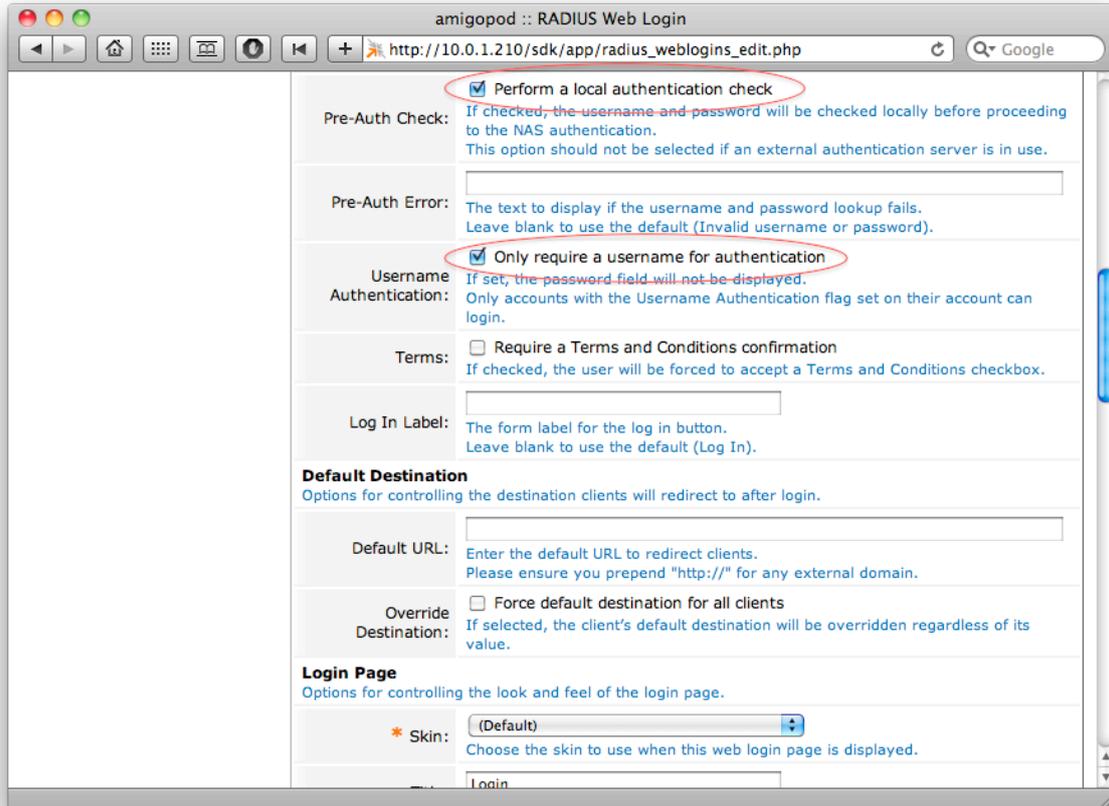


The screenshot shows a web browser window titled "amigopod :: RADIUS Web Login" with the URL "http://10.0.1.210/sdk/app/radius_weblogins_edit.php". The page displays the "RADIUS Web Login Editor" form. The form fields are as follows:

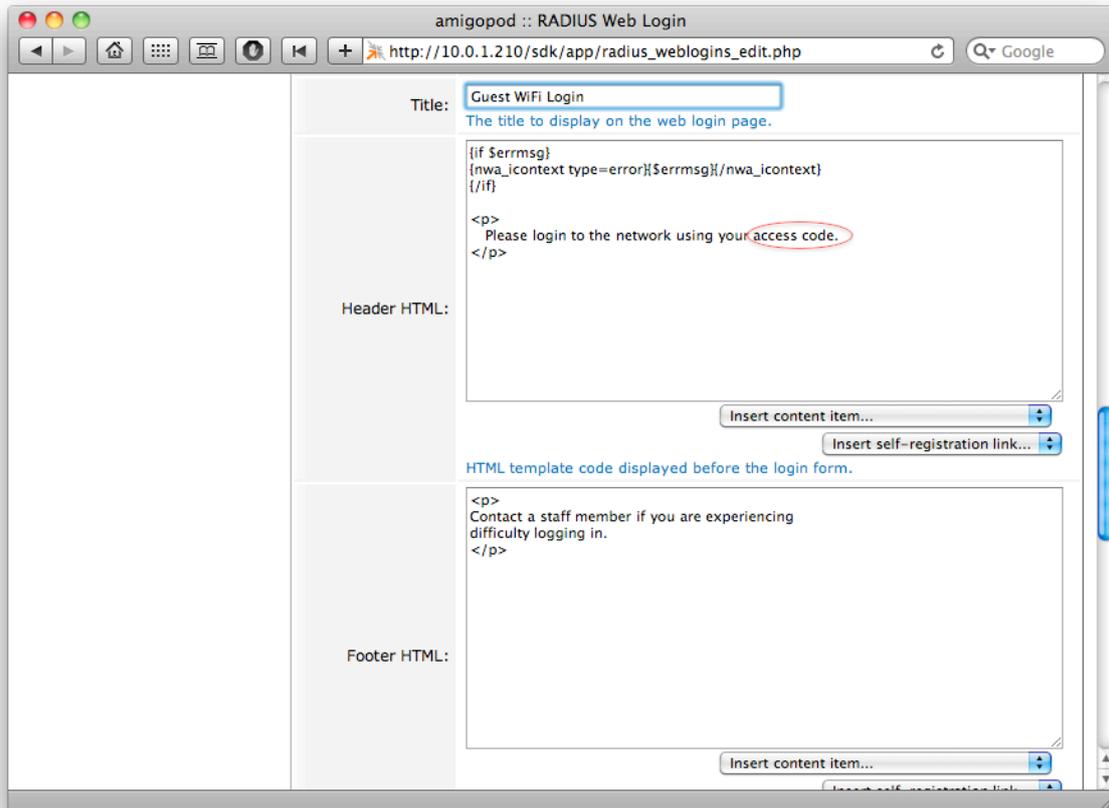
- Name:** access_codes
- Page Name:** access_codes
- Description:** This web login is setup for a single access code based login. Guest accounts will require the `username_auth` flag set.
- Vendor Settings:** Aruba Networks
- Address:** 192.168.100.1
- Secure Login:** Use vendor default
- Custom Form:** Provide a custom login form
- Custom Labels:** Override the default labels and error messages
- Username Label:** Access Code|

Red circles highlight the "Override the default labels and error messages" checkbox and the "Access Code|" text in the Username Label field.

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.

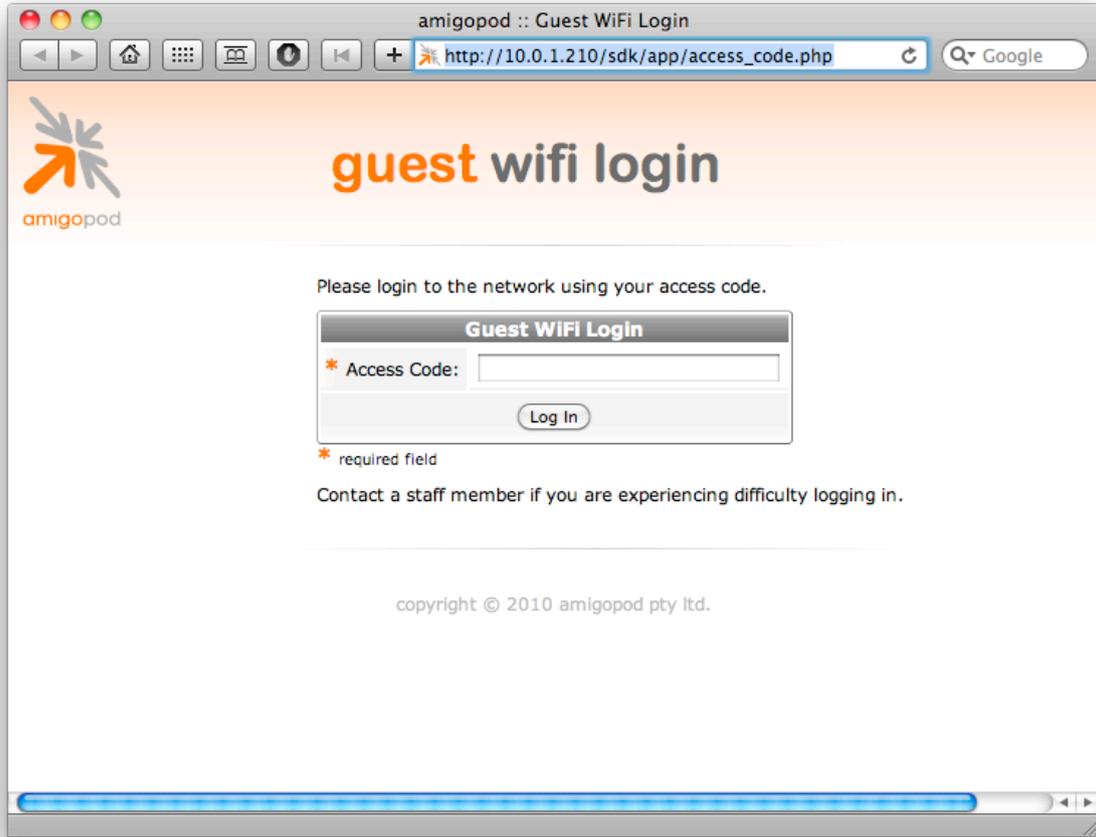


Click **Save Changes** to create the web login.

Name	Page Title	Page Name	Page Skin
access_code This web login is setup for a single access code based login. Guest accounts will require the username_auth flag set.	Guest WiFi Login	access_code	(Default)

[Edit](#)
[Duplicate](#)
[Delete](#)
[Test](#)

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



Testing Authentication

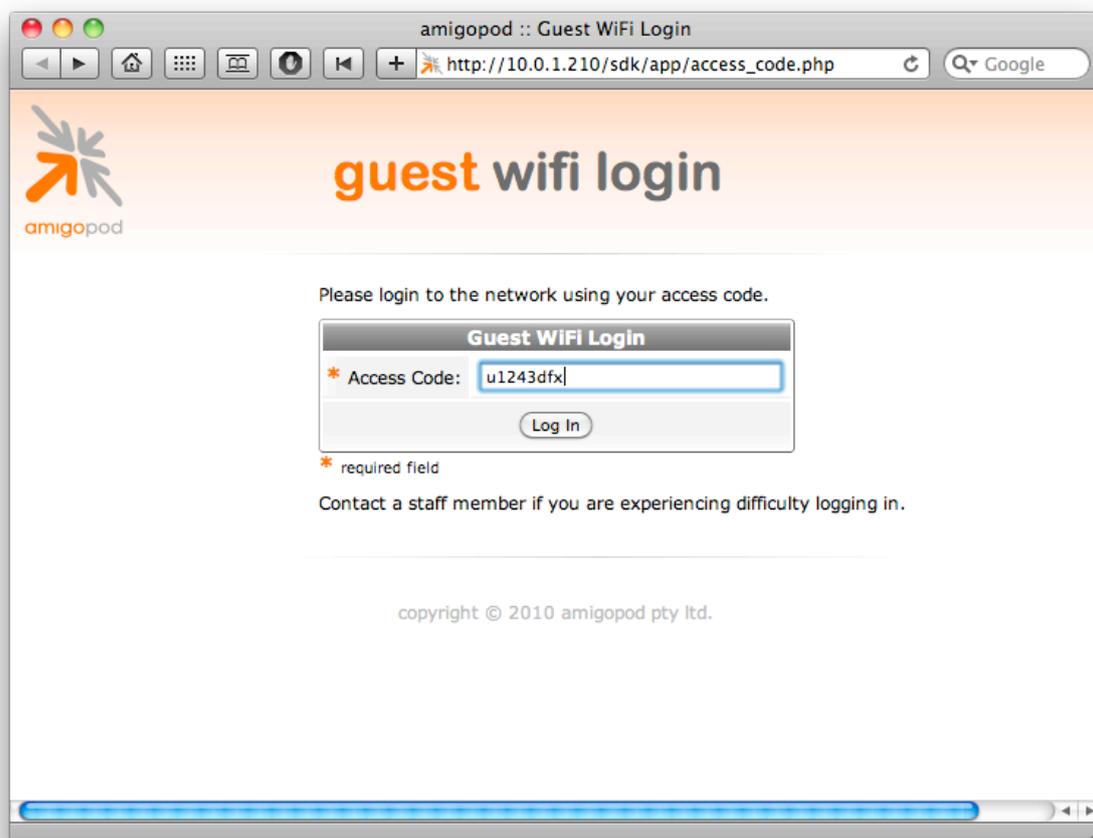
WLAN Controller and Access Point setup

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

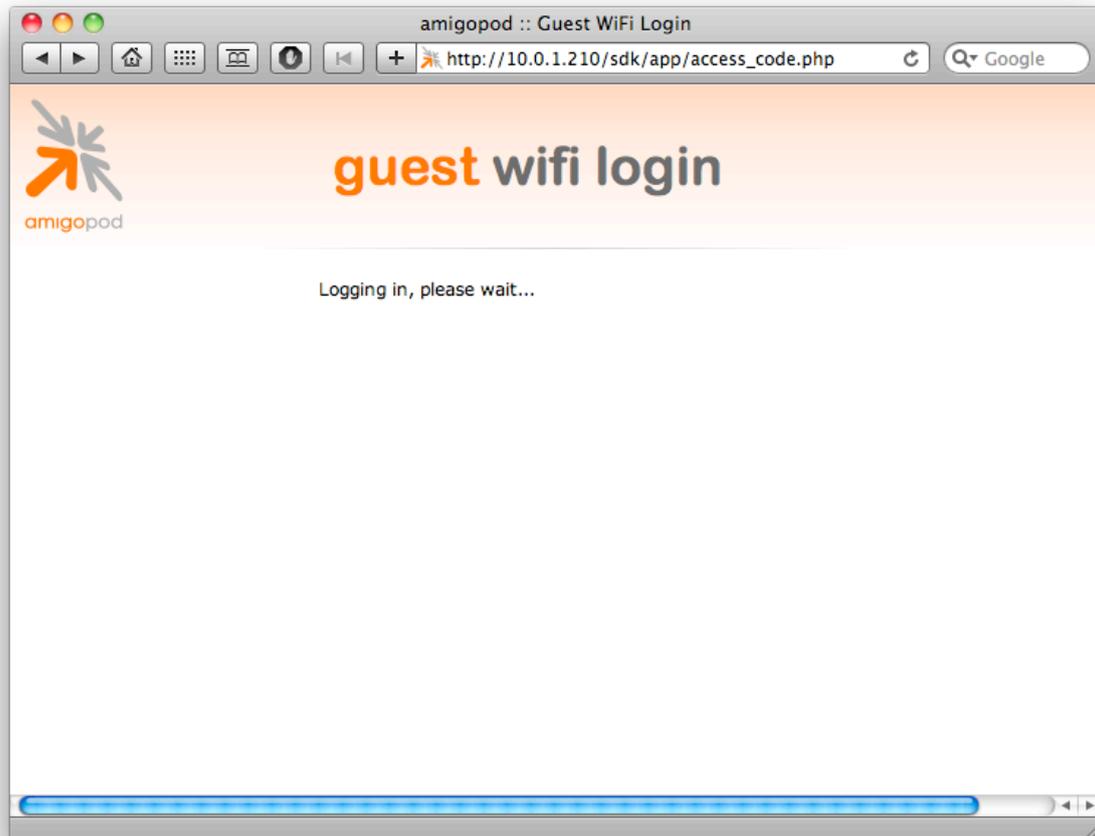
As a proof of concept, some of the below steps can be used without being connected to the WLAN. However the test will not do complete a RADIUS authentication to verify the complete setup.

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.