

Amigopod URL Persistence Tech Note

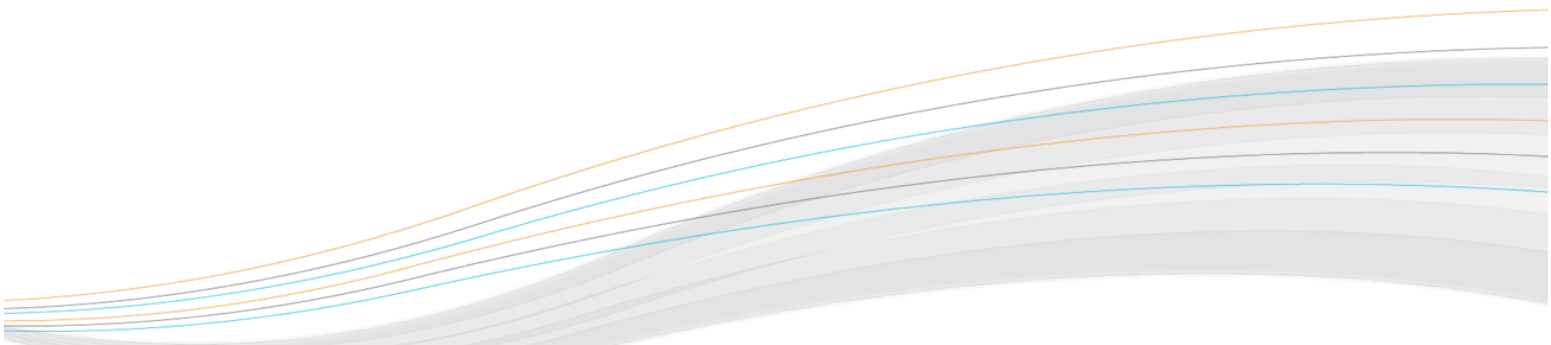


Table of Contents

1. Problem Definition.....	3
2. Work Around Configuration	3
3. Summary.....	7

1. Problem Definition

When the Aruba Controller is configured to host its own internal Captive Portal page, the wireless/wired user's originally requested URL is captured as part of the redirect process. Once the user has successfully logged in the web session is then forwarded onto their original destination.

This is typically the homepage of the default browser or the page they attempted to access immediately before being redirected to the Aruba Controller Captive Portal page.

Unfortunately an issue has been discovered in ArubaOS when the Captive Portal profile is configured to redirect users to an externally hosted Web Login page such as those found in Amigopod deployments. The ability to automatically redirect a user to their originally requested URL is currently not supported in this configuration.

This document serves to demonstrate a workaround to achieve the same result in the interim until a resolution is found to the ArubaOS handling of External Captive Portal configurations.

2. Work Around Configuration

The following steps are to be performed on both the ArubaOS configuration and the Amigopod to restore the functionality of automatically redirecting to the user's originally requested URL.

It is assumed that you have already configured a successful integration between the Amigopod and your Aruba controller and these additional steps will build on that existing configuration.

Create Captive Portal Profile

One of the key features of Amigopod is the ability to host the branded Web Login or Captive Portal pages on the Amigopod appliance. The Captive Portal profile allows us to configure both the Login and optionally Welcome Pages to be hosted by Amigopod.

Security > Authentication > L3 Authentication

Servers AAA Profiles L2 Authentication **L3 Authentication** User Rules Advanced

Captive Portal Authentication Profile

- default
 - Guest-Auth-CP
 - Server Group default
- WISPr Authentication Profile
- VPN Authentication Profile
- Stateful NTLM Authentication Profile
- VIA Authentication Profile
- VIA Connection Profile
- VIA Web Authentication

Captive Portal Authentication Profile > Guest-Auth-CP Show Reference Save As Reset

Default Role	guest	Default Guest Role	guest
Redirect Pause	10 sec	User Login	<input checked="" type="checkbox"/>
Guest Login	<input type="checkbox"/>	Logout popup window	<input checked="" type="checkbox"/>
Use HTTP for authentication	<input type="checkbox"/>	Logon wait minimum wait	5 sec
Logon wait maximum wait	10 sec	logon wait CPU utilization threshold	60 %
Show FQDN	<input type="checkbox"/>	Use CHAP (non-standard)	<input type="checkbox"/>
Login page	https://10.0.20.60/Arub	Welcome page	60/Aruba_welcome.php
Show Welcome Page	<input checked="" type="checkbox"/>	Proxy Server Configuration	
Add switch IP address in the redirection URL	<input type="checkbox"/>	Allow only one active user session	<input type="checkbox"/>
Show the acceptable use policy page	<input type="checkbox"/>		

For example, we could set these pages to the following:

- **Login Page:** https://<Amigopod IP Address or FQDN>/Aruba_login.php
- **Welcome Page:** https://<Amigopod IP Address or FQDN>/Aruba_welcome.php

These URLs will be defined on the Amigopod in a later step as part of the Web Login configuration.

It is the configuration of the Welcome Page in the Captive Portal Profile to point to another Amigopod hosted page that will allow us to control the user experience.

Configure Web Login Page to perform Automatic Redirect

Creating a new Web Login from the Amigopod RADIUS Services → Web Logins will display the following page.

The screenshot displays the 'RADIUS Web Login Editor' interface. It contains several configuration fields:

- Name:** 'Aruba Networks Welcome' (with a hint: 'Enter a name for this web login page.')
- Page Name:** 'Aruba_welcome' (with a hint: 'Enter a page name for this web login. The web login will be accessible from "page_name.php"').
- Description:** 'Login page for Aruba 200/800/2400/6000 Mobility Controllers.' (with a hint: 'Comments or descriptive text about the web login.')
- Vendor Settings:** 'Aruba Networks' (with a hint: 'Select a predefined group of settings suitable for standard network configurations.').
- Address:** '10.0.20.58' (with a hint: 'Enter the IP address or hostname of the vendor's product here.').
- Secure Login:** 'Use vendor default' (with a hint: 'Select a security option to apply to the web login process.').

Below these fields is a section titled 'Login Form' with the subtitle 'Options for specifying the behaviour and content of the login form.' It includes four checkboxes:

- Custom Form:** ☒ Provide a custom login form. (Hint: 'If selected, you must supply your own HTML login form in the Header or Footer HTML areas.')
- Custom Labels:** ☐ Override the default labels and error messages. (Hint: 'If selected, you will be able to alter labels and error messages for the current login form.')
- Pre-Auth Check:** ☐ Perform a local authentication check. (Hint: 'If checked, the username and password will be checked locally before proceeding to the NAS authentication. This option should not be selected if an external authentication server is in use.')
- Terms:** ☐ Require a Terms and Conditions confirmation. (Hint: 'If checked, the user will be forced to accept a Terms and Conditions checkbox.')

The *Page Name* field is what defines the URL that will be hosted on the Amigopod appliance. For example in the previous step we configured the Welcome Page of the Captive Portal Profile to be the following URL:

`https://<Amigopod IP Address or FQDN>/Aruba_welcome.php`

As you can see the screenshot has got the `Aruba_welcome` name defined – there is no need to include the `.php` extension as this will be automatically appended.

The IP Address field is largely irrelevant as we are going to use the Custom Form option to override the default Web Login capabilities and just perform the automatic redirect.

Login Form Options for specifying the behaviour and content of the login form.	
Custom Form:	<input checked="" type="checkbox"/> Provide a custom login form If selected, you must supply your own HTML login form in the Header or Footer HTML areas.
Custom Labels:	<input type="checkbox"/> Override the default labels and error messages If selected, you will be able to alter labels and error messages for the current login form.
* Password Encryption:	<div>No encryption (plaintext password)</div> Choose the type of password encryption to use when submitting the login form.
Pre-Auth Check:	<input type="checkbox"/> Perform a local authentication check If checked, the username and password will be checked locally before proceeding to the NAS authentication. This option should not be selected if an external authentication server is in use.
Terms:	<input type="checkbox"/> Require a Terms and Conditions confirmation If checked, the user will be forced to accept a Terms and Conditions checkbox.
Default Destination Options for controlling the destination clients will redirect to after login.	
Default URL:	<div></div> Enter the default URL to redirect clients. Please ensure you prepend "http://" for any external domain.
Override Destination:	<input type="checkbox"/> Force default destination for all clients If selected, the client's default destination will be overridden regardless of its value.
Login Page Options for controlling the look and feel of the login page.	
* Skin:	<div>(Default)</div> Choose the skin to use when this web login page is displayed.
Title:	<div>Aruba Networks</div> The title to display on the web login page.
Header HTML:	<div> <pre><h2> Welcome to Aruba Networks </h2> <meta http-equiv="refresh" content="5; URL={\$extra_fields.url escape}"> <p> Redirecting you to {\$extra_fields.url escape}, please wait... </p></pre> </div>

Given the *Provide a custom login form* is checked as shown above, only the contents of the *Header and Footer HTML* will be presented to the user. The example in the screenshot provides some basic formatting and a redirecting message to the user. Additionally, there is a small code snippet that actually performs the automatic redirect for us. This is shown in text format below:

```
<meta http-equiv="refresh" content="5;
URL={$extra_fields.url|escape}">
```

```
<p>
```

```
Redirecting you to {$extra_fields.url|escape}, please wait...
```

```
</p>
```

Amigopod has an internal set of variables (\$extra_fields) for each user session and the code leverages this to extract the user's originally requested URL and then automatically redirect to this destination after a configurable number of seconds.

The example above pauses for 5 seconds before initiating the redirect (highlighted in yellow). This value can be changed to 0 if you would prefer this page to never be displayed to the end users.

3. Summary

Although the default operation of the ArubaOS Captive Portal Profile does not support the automatic redirection of a user's originally requested URL, this simple workaround of hosting a second page on the Amigopod as the Welcome Page destination provides the same end user experience.

Aruba Networks

1344 Crossman Ave.

Sunnyvale, CA 94089-1113

Phone: +1-408-227-4500

Fax: +1-408-227-4550

[Get Directions »](#)

General Inquiries:

info@arubanetworks.com

© 2010 Aruba Networks, Inc. AirWave®, Aruba Networks®, Aruba Mobility Management System®, Bluescanner, For Wireless That Works®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFprotect®, The All Wireless Workplace Is Now Open For Business, Green Island, and The Mobile Edge Company® are trademarks of Aruba Networks, Inc. All rights reserved. Aruba Networks reserves the right to change, modify, transfer, or otherwise revise this publication and the product specifications without notice. While Aruba uses commercially reasonable efforts to ensure the accuracy of the specifications contained in this document, Aruba will assume no responsibility for any errors or omissions. Note: All scaling metrics outlined in this document are maximum supported values. The scale may vary depending upon the deployment scenario and features enabled.