ClearPass Guest

App Note: Apple Captive Network Assistant Bypass with Guest

Introduction

This document describes the process for leveraging the ClearPass Guest captive portal to bypass the Captive Network Assistant (web sheet) that is displayed on iOS devices such as iPhone®, iPad®, and more recently, OS X® machines running Lion (10.7) and above.

The Captive Network Assistant web sheet is displayed on these platforms when a device connects to a Wi-Fi network that has been configured with open security, such as those typically found in guest access networks or public hotspots.

The benefit of this Apple® feature is to prompt users automatically to login to the detected captive portal network without the need to explicitly open a web browser. This type of login is useful on mobile devices where many of the common applications are not browser-based and these applications would otherwise fail to connect without the successful browser-based authentication. Examples of these non-browser-based applications are email, social networking applications, corporate VPNs, and media streaming.

The Apple operating systems detect the presence of a network that has captive portal enabled by attempting to request a web page from various web servers registered by Apple. This HTTP GET process retrieves a simple success.html file from the Apple web servers and the operating system uses the successful receipt of this file to assume that it is connected to an open network without the requirement for captive portal authentication.

If the success.html file is not received, the operating system conversely assumes that a captive portal is in place and presents the web sheet automatically to prompt the user to perform a web authentication task.

When the web authentication has completed successfully, the web sheet window displays a “Done” button which allows the user to close the web sheet and continue using their mobile device in an authenticated state.

Also, if the user chooses to cancel the web sheet before successfully authenticating to the network, the Wi-Fi connection to the open network is dropped automatically, which prevents any further interaction via the full browser or other applications.

The following examples of these web sheet sessions are from a Mac OS X Lion laptop, an iPad, and an iPhone.

Figure 1: *Captive network assistant on Mac OS X*

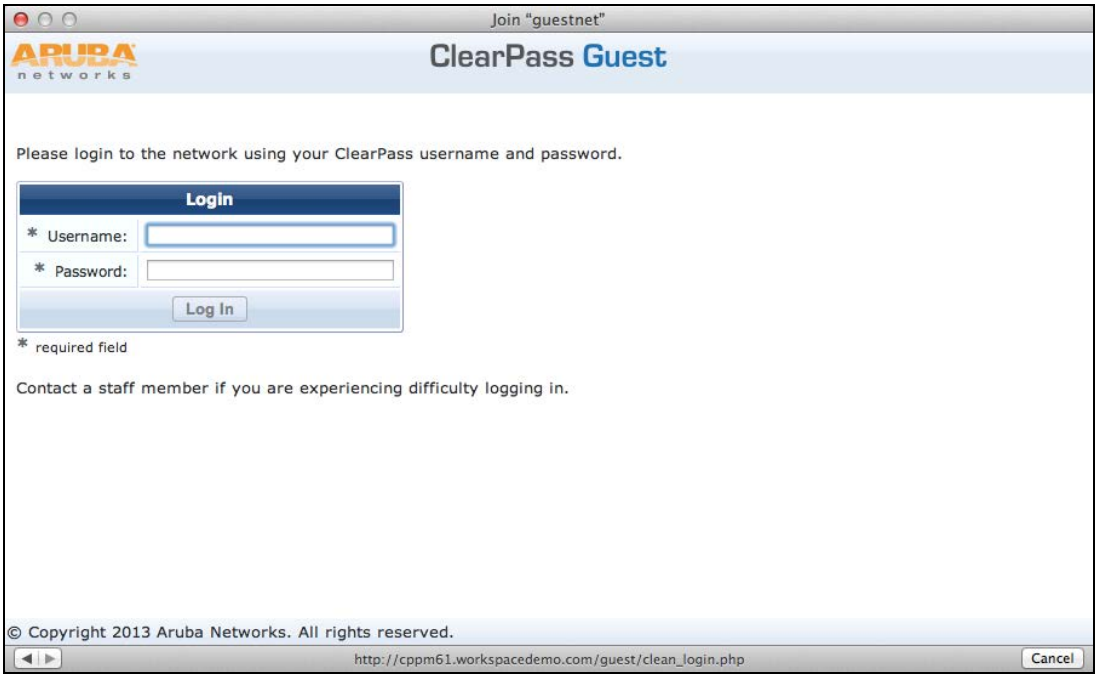


Figure 2: *Captive network assistant on iPad*

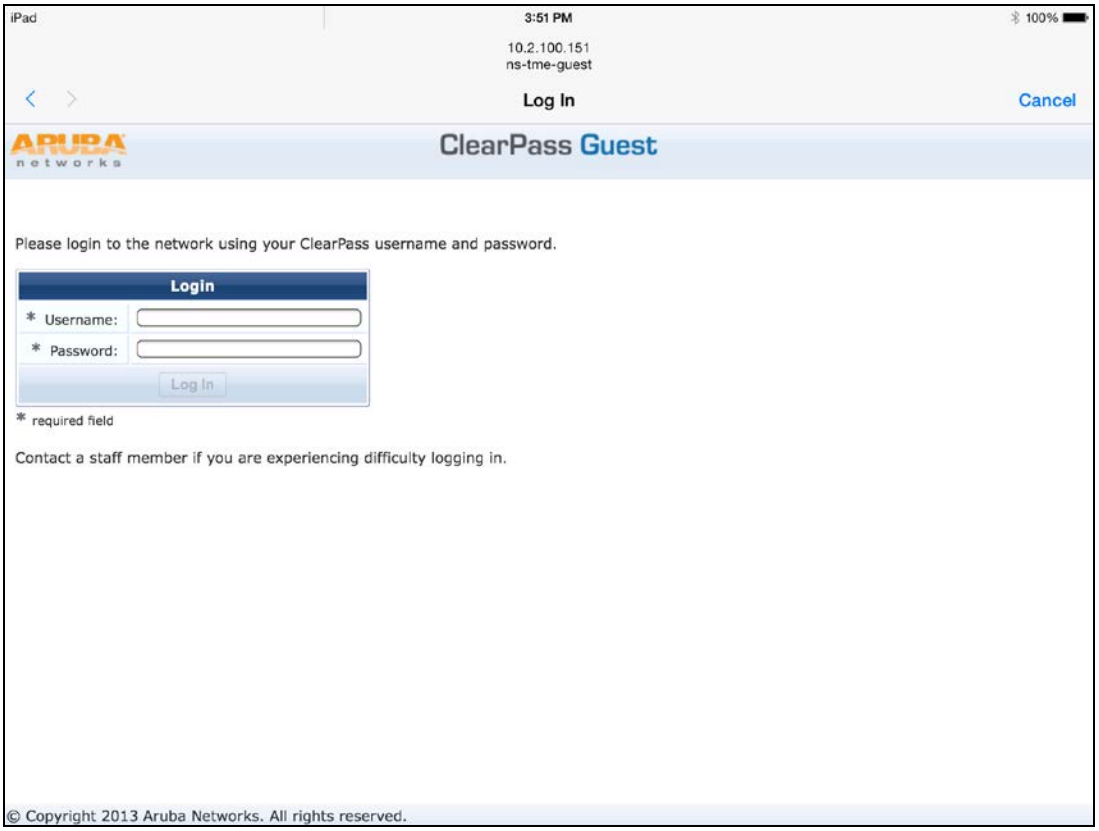
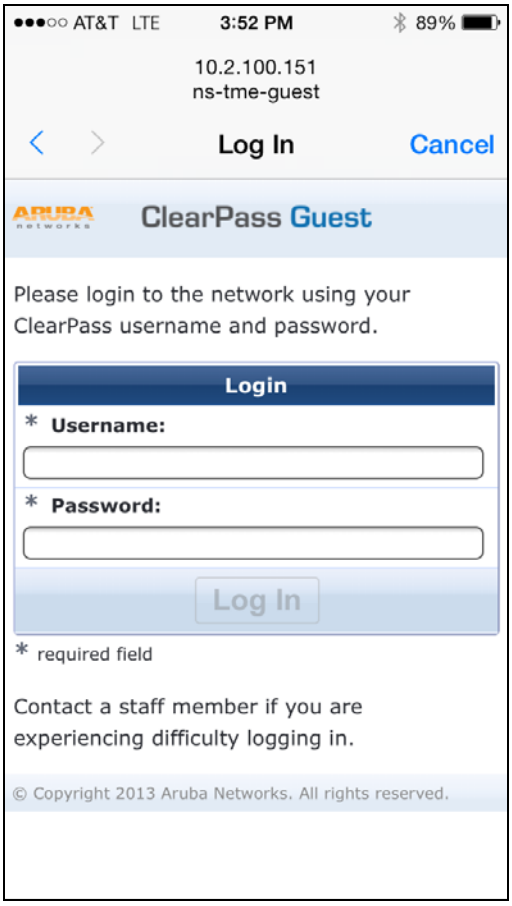


Figure 3: *Captive network assistant in iPhone*



The web sheet can be identified easily by the lack of a URL bar at the top of the screen and typical menu bar items.

For many customers, this behavior of their Apple wireless devices will be acceptable and a great usability enhancement for their user community.

However for some guest access or public access designs, the use of this web sheet and the lack of ability to control the entire web authentication user experience are not desirable.

For these customer scenarios, ClearPass Guest includes a method of bypassing the display of the web sheet on the Mac OS X Lion or iOS devices. The main driver for this implementation is to restore the ability to control the user experience and support the enrollment of mobile devices using protocols such as SCEP for certificate provisioning.

NOTE: The Captive Network Assistant on Apple devices will not be displayed in the event that the captive portal destination is deployed with a self-signed server certificate. It appears that the web sheet will consider a server with a self-signed certificate untrustworthy and will not attempt to assist the user logging in and they will be forced to interact with the captive portal environment using the native Safari browser.

The following table lists the current software versions that were tested for this guide.

Table 1: *Aruba Software Versions*

Product	Version
ArubaOS™ (mobility controllers)	6.1*
Aruba Instant (Aruba Instant APs)	3.4.0.2
AmigopodOS	3.9.9
ClearPass Guest (ClearPass Policy Manager)	6.1, 6.2

NOTE: Although the testing in this document was performed using ArubaOS 6.1 there are no new 6.1 features leveraged in this guide. Amigopod 3.9.9, ClearPass Guest 6.1, and 6.2 were updated to support some of the enhancements in the iOS7 release made available on the September 18, 2013.

The terms Amigopod and ClearPass Guest can be used interchangeably within the context of this Application Note as the Captive Network Assistant Bypass functionality is equally applicable to both platforms.

Reference Material

This guide assumes a working knowledge of Aruba products. This guide is based on the network detailed in the *Aruba Campus Wireless Networks VRD* and the *Base Designs Lab Setup for Validated Reference Design.* These guides are available for free at http://www.arubanetworks.com/vrd.

The complete suite of Aruba technical documentation is available for download from the Aruba support site. These documents present complete, detailed feature and functionality explanations outside the scope of the VRD series. The Aruba support site is located at: https://support.arubanetworks.com/. This site requires a user login and is for current Aruba customers with support contracts.

Implementation

In a typical ClearPass Guest deployment integrating with an ArubaOS controller, the captive portal profile is configured to redirect all unauthenticated users to the external captive portal page hosted on ClearPass Guest.

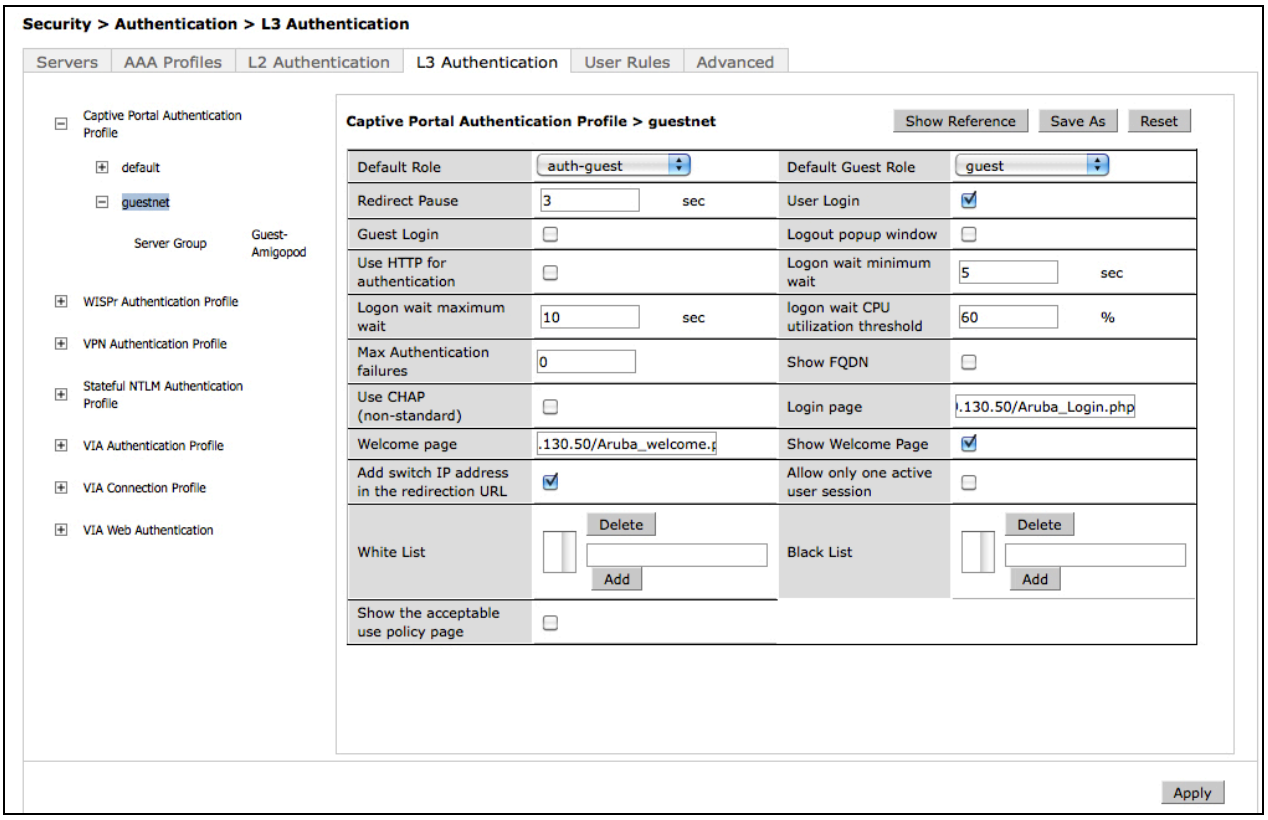
The following CLI and Web UI examples show a typical configuration of the captive portal profile. The login-page is set to point directly to the ClearPass Guest hosted Web Login page.

```
http://10.169.130.50/Aruba_Login.php
```

Captive Portal Profile Configuration

```
aaa authentication captive-portal "guestnet"
   default-role auth-guest
   redirect-pause 3
   no logout-popup-window
   login-page http://10.169.130.50/Aruba_Login.php
   welcome-page http://10.169.130.50/Aruba_welcome.php
   switchip-in-redirection-url
```

Figure 4: *Captive portal profile configuration*



ClearPass Guest has implemented a new embedded URL within the portal configuration that is designed to address the issue of bypassing the mini browser discussed previously. This new page is available on the following URL:

ClearPass Guest 3.9.9:
`http://<ClearPass Guest IP or FQDN>/landing.php/<intended web login name>`

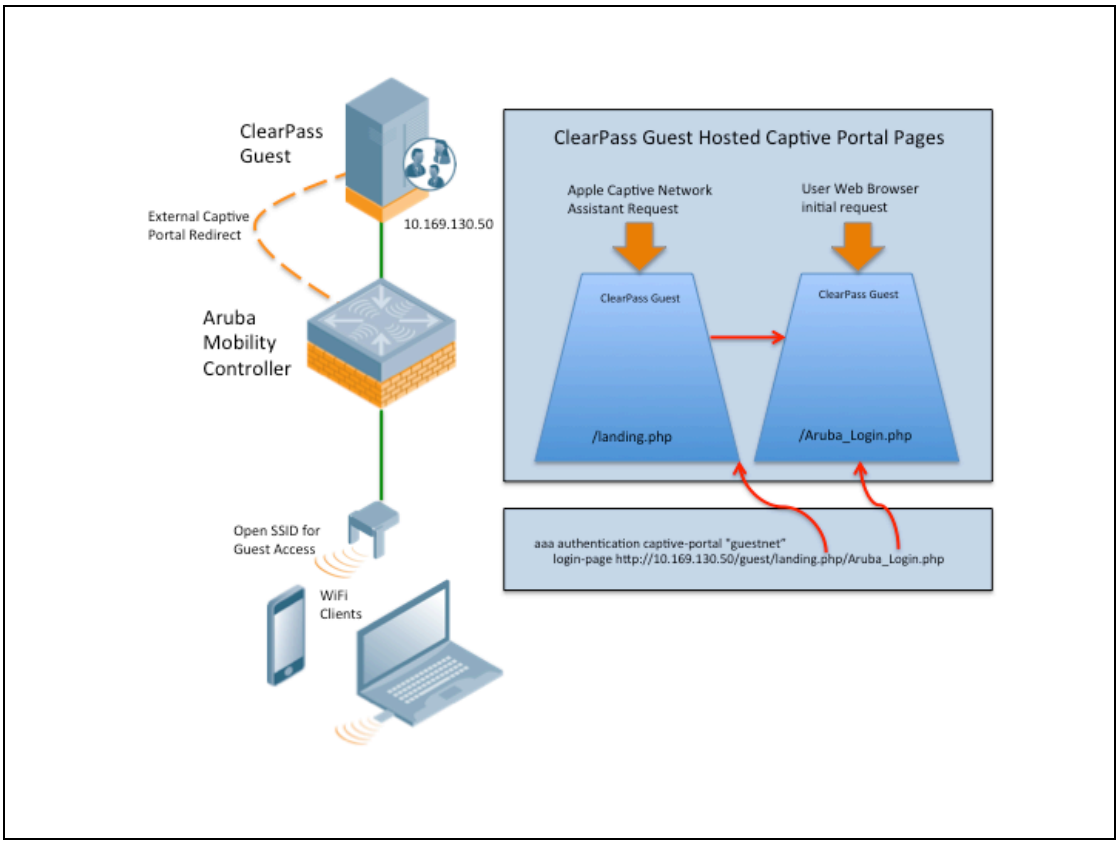
ClearPass Guest 6.0 or later:
`http://<ClearPass Guest IP or FQDN>/guest/landing.php/<intended web login name>`

The new web page includes the logic to detect the presence of an iOS device or Mac OS X machine being redirected as part of the captive portal configuration on an Aruba controller. If these devices are detected, their initial request to the Apple registered web sites is served locally from the ClearPass Guest web server, which emulates the environment of an open connection to the Internet. When the response from the Apple web sites is emulated, the iOS device or Mac OS X machine no longer initiates the Captive Network Assistant and the user can launch their local browser manually as desired.

Now that the devices are able to open the local browser, any attempt to access the Internet is redirected again to the ClearPass Guest captive portal page. This new function differentiates between this web browser request and the previous Captive Network Assistant request and forwards the session onto the configured ClearPass Guest Web Login page.

ClearPass Guest can host multiple Web Login pages, so a simple method has been provided to configure the Web Login page that should be used without requiring any additional configuration on ClearPass Guest. This definition of the Web Login page simply can be specified as part of the captive portal profile configuration on the Aruba controller.

Figure 5: *Landing page configuration*



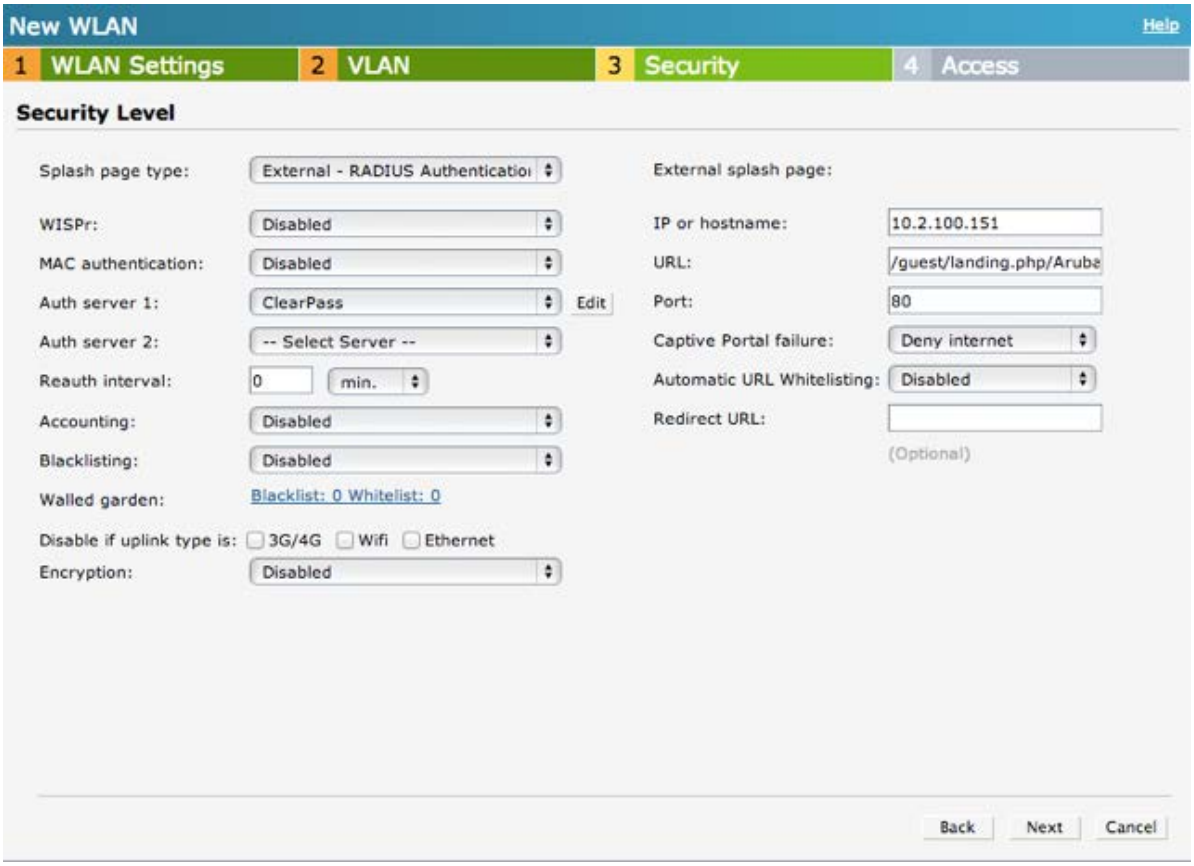
For example, this sample captive portal profile login page configuration links to a ClearPass Guest hosted Web Login page called Aruba_Login as depicted in Figure 5: Landing page configuration.

```
http://<ClearPass IP or FQDN>/guest/landing.php/Aruba_Login.php
```

Aruba Instant Implementation

As of Aruba Instant release 3.4 the same ClearPass Guest implementation can be leveraged in the Splash Page configuration of the Instant AP or cluster. The screenshot below is an example of how the ClearPass Guest landing page can be referenced in the Splash configuration of Aruba Instant.

Figure 6: *Splash configuration in Aruba Instant*



NOTE: The ability to leverage this capability on ClearPass Guest is not compatible with URL based whitelisting on Aruba Instant and therefore this feature should remain disabled if the network deployment requires the bypass of the Captive Network Assistant.

Solution Summary

Based on the proposed configuration in this guide, the combination of an Aruba Wi-Fi network and ClearPass Guest access solution can be used effectively to bypass the Captive Network Assistant technology implemented by Apple in their various Wi-Fi enabled mobile devices.

The need to bypass this web sheet solution for prompting users to perform a web authentication task is driven largely by the customer design and need to control the user experience as guest or public access users authenticate to the network.

By enabling authentication that is based on the client web browser, this solution enables a fully customized web login experience to be developed and presented through the ClearPass Guest portal options.

Some examples of use cases for the browser-based authentication are as follows but certainly not limited to:

- Display of a welcome page to host session statistics, a logout button, and a link to continue to original destination
- Display of an interstitial page to display advertising media before being granted access to the Internet
- Based on browser detection, display a promotional link to a mobile device app from associated App Store for retail applications
- Provide mobile device app-based web authentication for transparent WiFi access in retail application
- ClearPass Onboard environments where the web authentication process is used to push device configurations and client certificates to mobile devices

www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, CA 94089
Phone: 1-800-WIFI-LAN (+800-943-4526)
Fax 408.227.4550