Readme for iOS 7 WebAuth on Cisco Wireless LAN Controller, Release 7.4 MR 2

September, 2013

1 Contents

This document includes the following sections:

2 Background

Wireless Internet Service Provider roaming (WISPr) is a draft protocol that enables users to roam between different wireless service providers. Some devices (For example, Apple iOS devices) have a mechanism using which they can determine if the device is connected to Internet, based on an HTTP WISPr request made to a designated URL. This mechanism is used to allow users to launch the web browser if they need to provide credentials to access Internet, and the actual authentication is done in the background every time the device connects to a new Service set identification (SSID).

Apple introduced an iOS feature to facilitate network access when captive portals are present. This feature detects the presence of a captive portal by sending a web request on connecting to a wireless network and directs the request to http://www.apple.com/library/test/success.html. If a response is received, then the Internet access is assumed to be available and no further interaction is required. If no response is received, then the Internet access is assumed to be blocked by the captive portal and Apples' Captive Network Assistant (CNA) auto-launches the pseudo-browser to request portal login in a controlled window.

2.1 Captive Bypassing on Wireless LAN Controller (WLC)

The captive portal can be hosted on either the WLC or on an external server such as a Cisco Identity Services Engine (ISE). Due to the limited capability of the CNA browser, the content of the page cannot be displayed, and a blank page is shown instead. When the blank page is displayed and the CNA browser is closed, the device disconnects from the wireless network and the user cannot open the full browser page and log in.

The new Captive Portal Bypass feature has been developed to bypass the CNA feature on Apple devices. When this feature is deployed—**`config network web-auth captive-bypass enable`**–the WLC will respond to the URL request with the expected Success page. This response stops the iOS device launching the pseudo browser. The user is then required to launch a full feature browser to request a page for authentication; this will cause a redirect to the ISE and the full feature browser session will allow the Guest authentication process to proceed.

2.2 Changes in iOS 7

With iOS 7, Apple sends web requests to as many as 200 websites leading to the failure of captive bypassing on WLC. Therefore, even after deploying the CLI, the WLC fails to respond to the URL request with the expected success page and this results in the iOS 7 device launching the CNA browser.

Users with a new iOS 7 iPhone, but without an existing iOS Profile or a device-specific certificate installed, may need IT intervention to get the device onboarded to the Enterprise wireless network.

2.3 Results

Figure 1: Results for Captive Portal Testing with iOS 7 with existing Cisco Software

iOS Version	Web Redirect Method			
	Local Web Auth on WLC (WLC Redirect)	*Local Web-Auth with ISE (WLC with External Web-Server)*	*Central Guest Web-Auth with ISE (Guest Flow)*	*CWA ISE BYOD flow On Boarding (Cert Install / iOS Profile Install)*
iOS 7				

3 Workaround

The scenarios represented by a green dot in Figure 1 work successfully. The scenario represented by a red dot in Figure 1 requires that you upgrade your wireless networking infrastructure to the following releases:

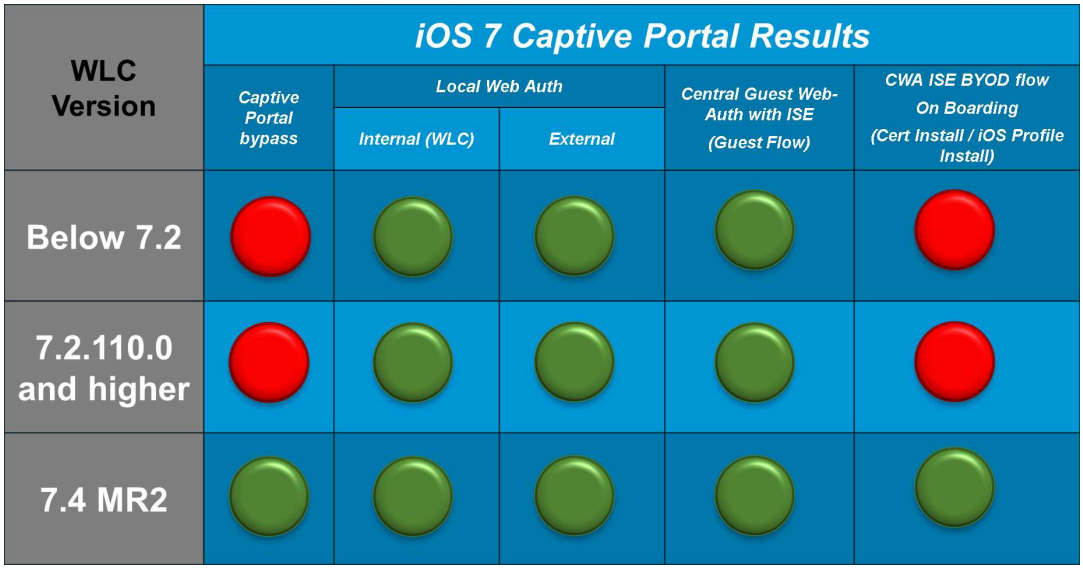
- AireOS 7.4 MR 2 (Cisco 5508 / Cisco 7500 / Cisco 8500 / Cisco 2500 / Wism2 / Virtual Controller)
- IOS-XE 3.2.3 (Cisco WLC 5760 / Cisco Catalyst 3850)
- ISE 1.2 Patch Version 2 (Identity Services Engine)

Note

For iOS 6 users, the experience does not change, as users are not prompted with the pseudo browser.

4 User Experience with iOS 7 Devices without Deploying the Latest 7.4 MR 2 Code

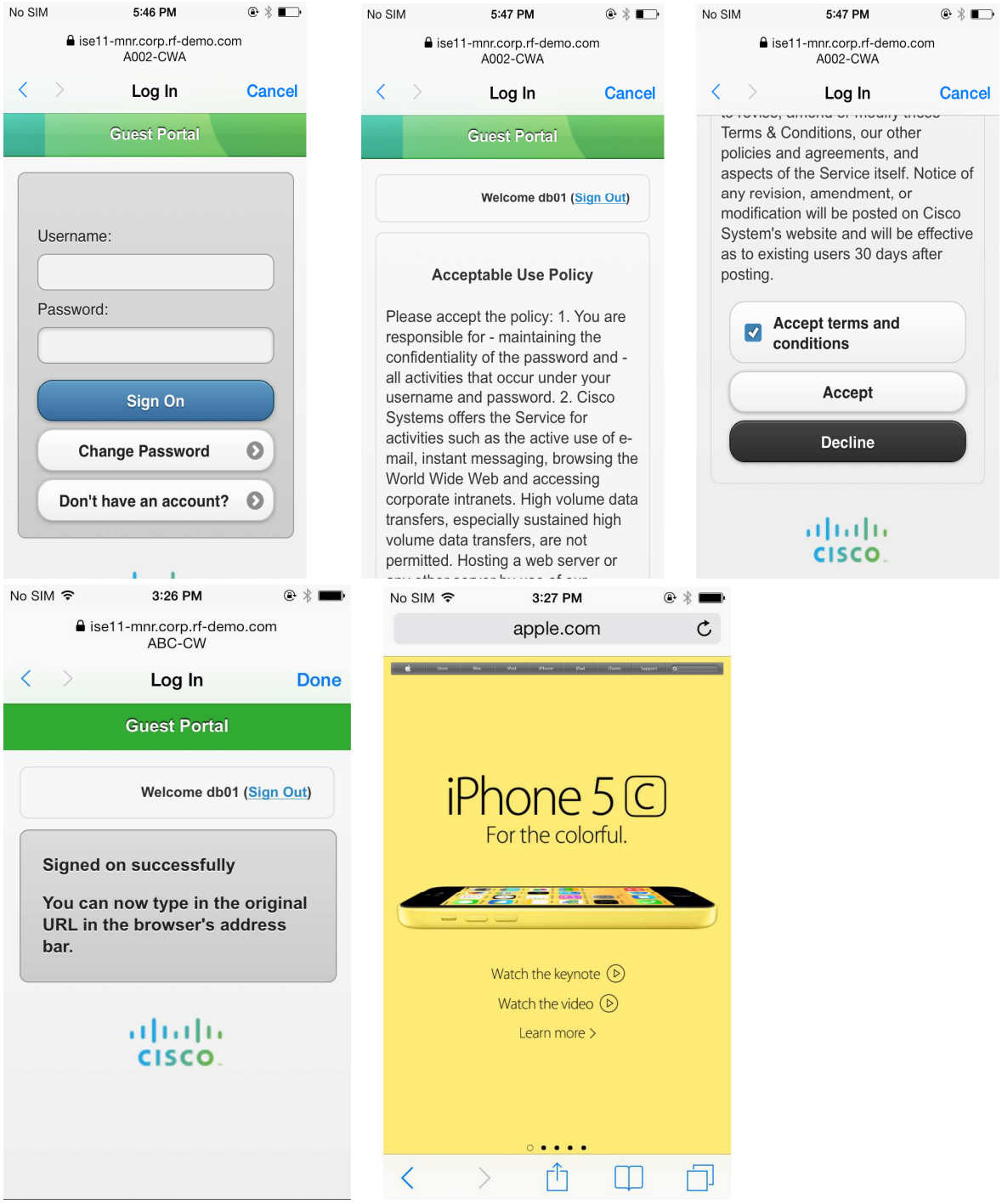
Figure 2: WLC Captive Portal Results



4.1 Local WebAuth and Central WebAuth Use Case

With iOS 7, the CNA browser launches to request the guest credentials.

Figure 3: End User Experience with iOS 7 Device using Captive Portal



4.2 ISE BYOD On-Boarding Flow (with Certificate Installation)

While onboarding a new iOS 7 device, the ISE redirects the CNA browser to register the device on the ISE, and install the Root CA certificate. However, the CNA cannot go beyond this, resulting in the iOS device disconnecting itself from the network.

Figure 4: End User Experience for iOS 7 trying to OnBoard and Install a Certificate on a New Device.