Secure Hotspot Demonstration

**************************** NOTICE
****

USE AT YOUR OWN RISK. ANY CODE, SCRIPT, OR INFORMATION CONTAINED HEREIN (“MATERIAL”) IS NOT SUPPORTED BY RUCKUS WIRELESS, INC. ("RUCKUS") AND IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. RUCKUS AND ITS LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. RUCKUS RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

IN NO EVENT SHALL RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL.

Ruckus offers no technical support for the Material.

**************************** NOTICE
****

This software provides a simple example of captive portal web coding necessary to implement the Ruckus Secure Hotspot functionality. It includes the following:

CONTENTS:

1. A simple login page (HTML and JavaScript)
2. Python scripts to:
    - authenticate user-provided credentials against ZD
    - generate a D-PSK for the user device
    - retrieve the newly created D-PSk
    - display the key information (manual client configuration)
    - download the Zero-IT script (automatic client configuration)

INSTALLATION:

1. Configure web server for Javascript, Python and CGI
2. Extract .html, .js, CSS and image files into the web server htdocs directory or equivalent
3. Files must be readable/executable by the web server daemon account
4. Extract .py scripts into cgi-bin directory or equivalent
5. Edit first line of Python scripts to point to the local pathname of the Python binary
6. Scripts must be readable/executable by the web server daemon account
7. Edit the odpsk-restricted and odpsk-unrestricted files to:
    - change northbound interface password to match ZD configuration (default is = testme123)
    - change the name of the secure SSID to match ZD configuration (default = secure-dpsk)
    - change D-PSK expiration if desired (default =)
    - change port number of ZD URL if desired (default is 443)

8. Edit the odpskcommon.py file to change the variable server_loc to the actual document root for your server

Client web browsers must support JavaScript.

CAVEATS:

The included files are heavily commented - please check there first for clarifications.
This code has been tested against the following environment:

- Apache 2 web server (Linux Fedora 17)
- Python 2.7
- Web browsers:
    - Mac OS: Chrome X.X, Safari Y.Y
    - iOS: Safari Z.Z
    - Windows: ...
    - Android ...

KNOWN ISSUES:

1. Full error handling and logging are not supported
2. HTML pages are not formatted for mobile devices
3. Python 3 is not guaranteed to be backwards-compatible with included 2.7 scripts