How to configure WLC doing Web—Auth using NGS as central WebServer

Idea:

Based on
http://www.cisco.com/en/US/docs/security/nac/guestserver/configuration_guide/20/g_hotspots.html

Customized authentication pages—Allow guest portal pages to be located on the Guest Server instead of on each captive portal device, providing a centralized location for configuration and display.

NOTE:

You need latest patched code for the hotspots feature due to bug id *CSCtd45002*

Copy the patch to the NGS /guest/www and extract:

```
unzip -o CSCtd45002.zip -d /
```

Set permissions for copied files:

```
chown apache:apache /guest/www/html/sponsor/api/SitesJsonApi.class.php
chmod 755 /guest/www/html/sponsor/api/SitesJsonApi.class.php
chown -R apache:apache /guest/www/html/sites/
chmod -R 755 /guest/www/html/sites/
```

IMPORTANT: After applying the patch, make sure you clear the browser cache before attempting to re-authenticate.

This is not a official Cisco document and you use it on your own risk.

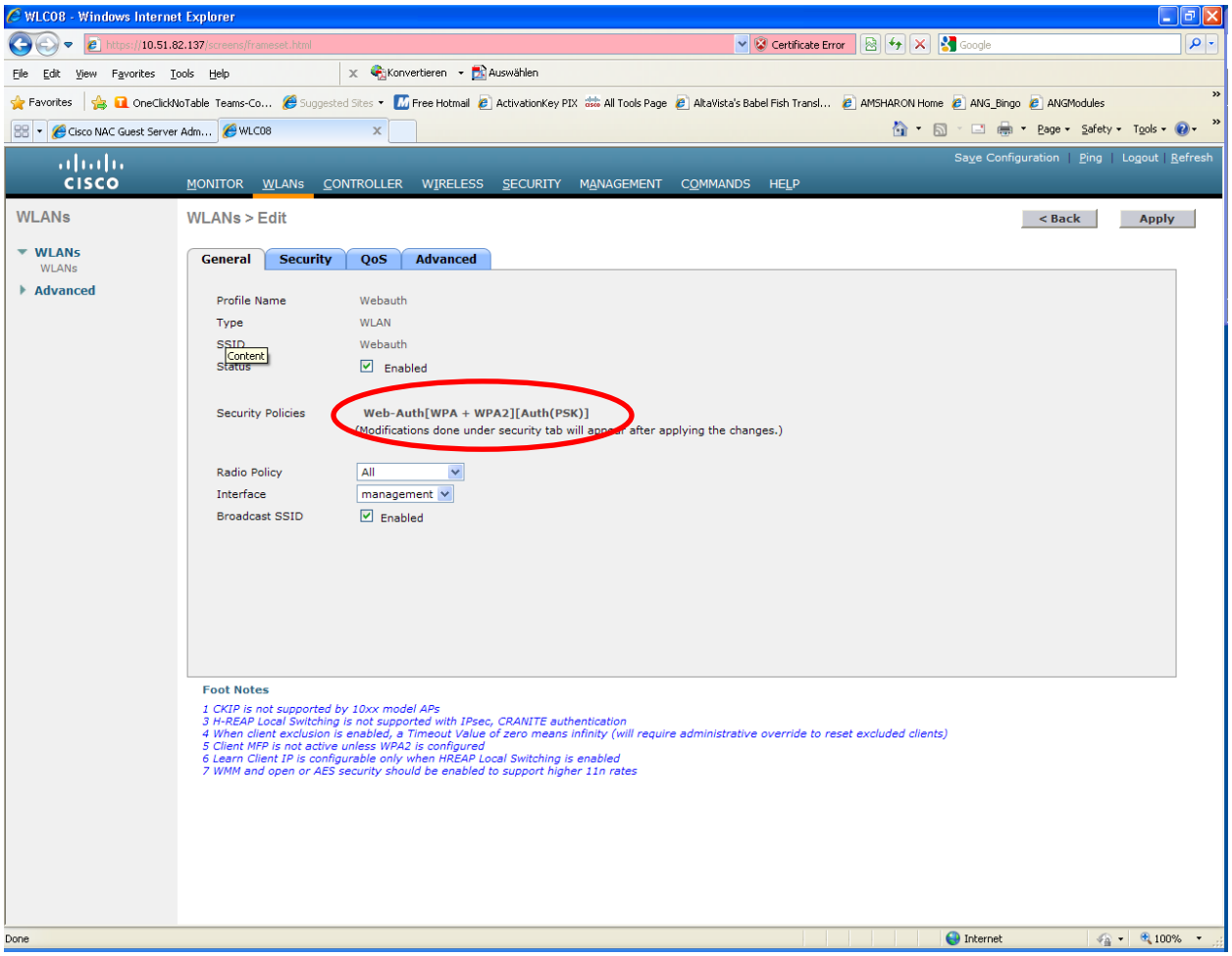
Setup:

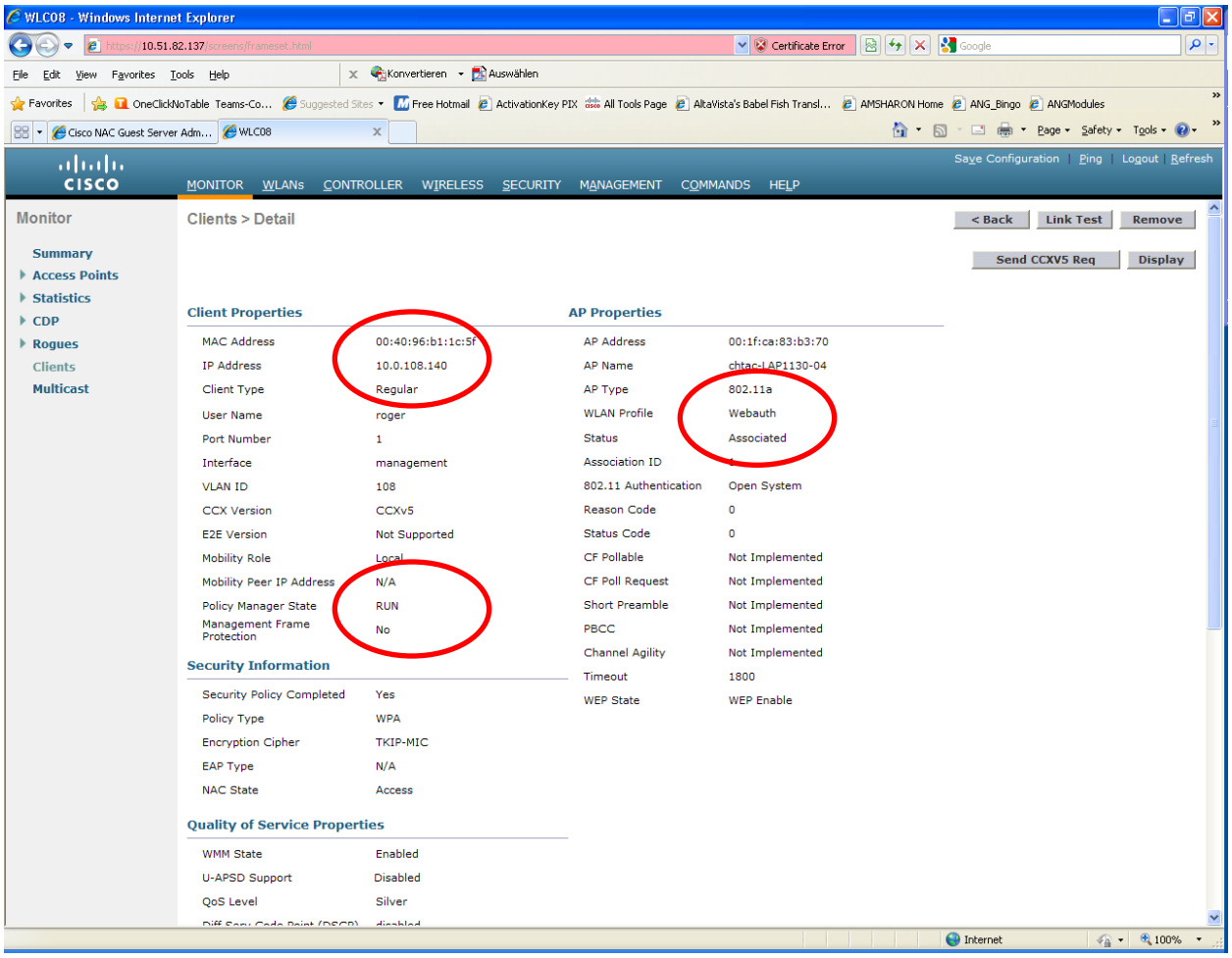
WirelessClient)))Webauth(((LAP----WLC-----NGSv2.0.1

Requirement:

WLC configure with SSID (Webauth) using already Webauthentication in conjunction to other security if needed, with local login page running on WLC.

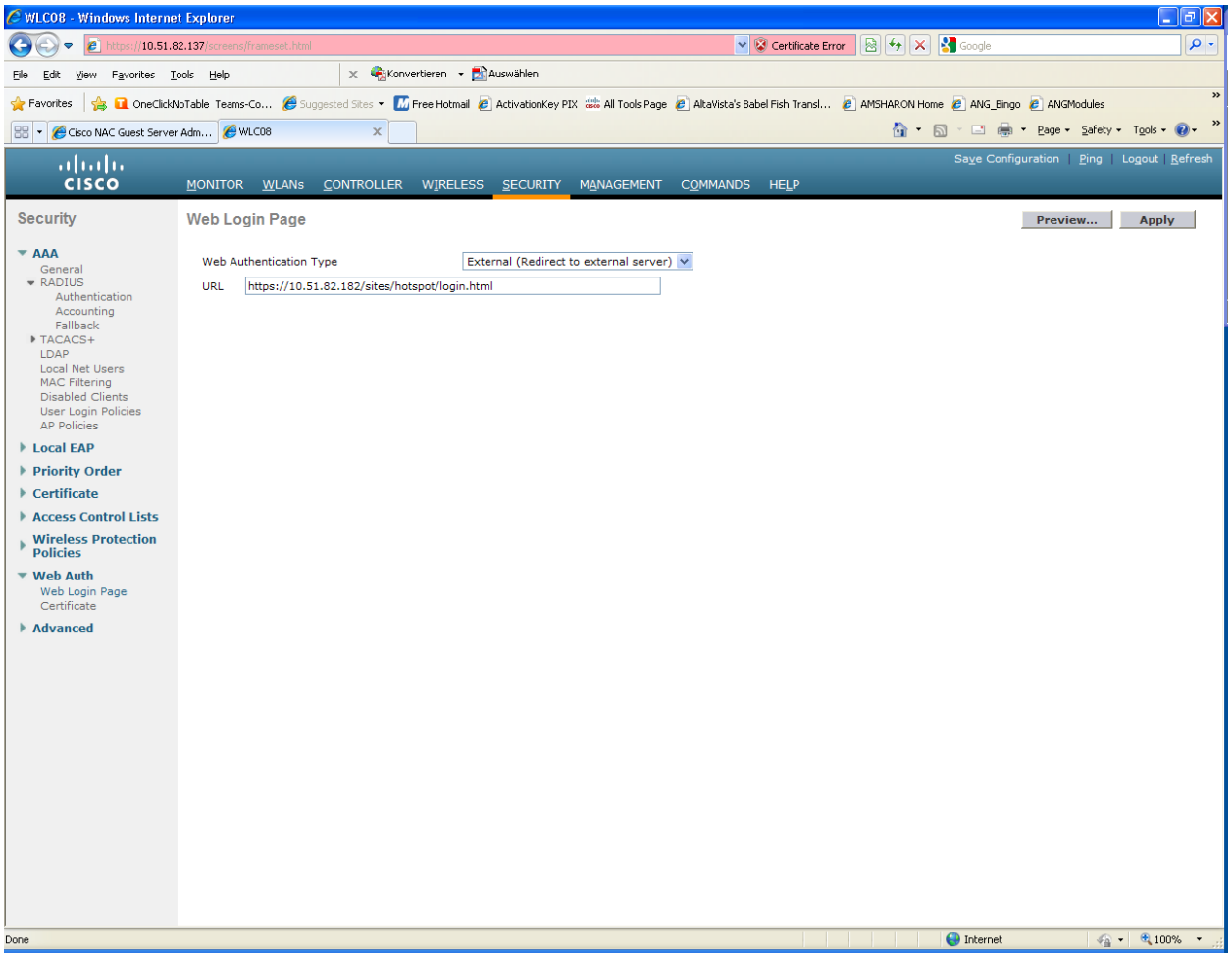
Verify on WLC Client associated and authenticated using Webauth local on WLC with local user.





WLC Configuration:

1.) WLC need to point to NGS for Webauthentication.
NGS is acting as Webserver.



⇨ 10.51.82.182 is the NGS ip address.
URL: https://<ngsip>/sites/hotspot/login.html

NGS Configuration:

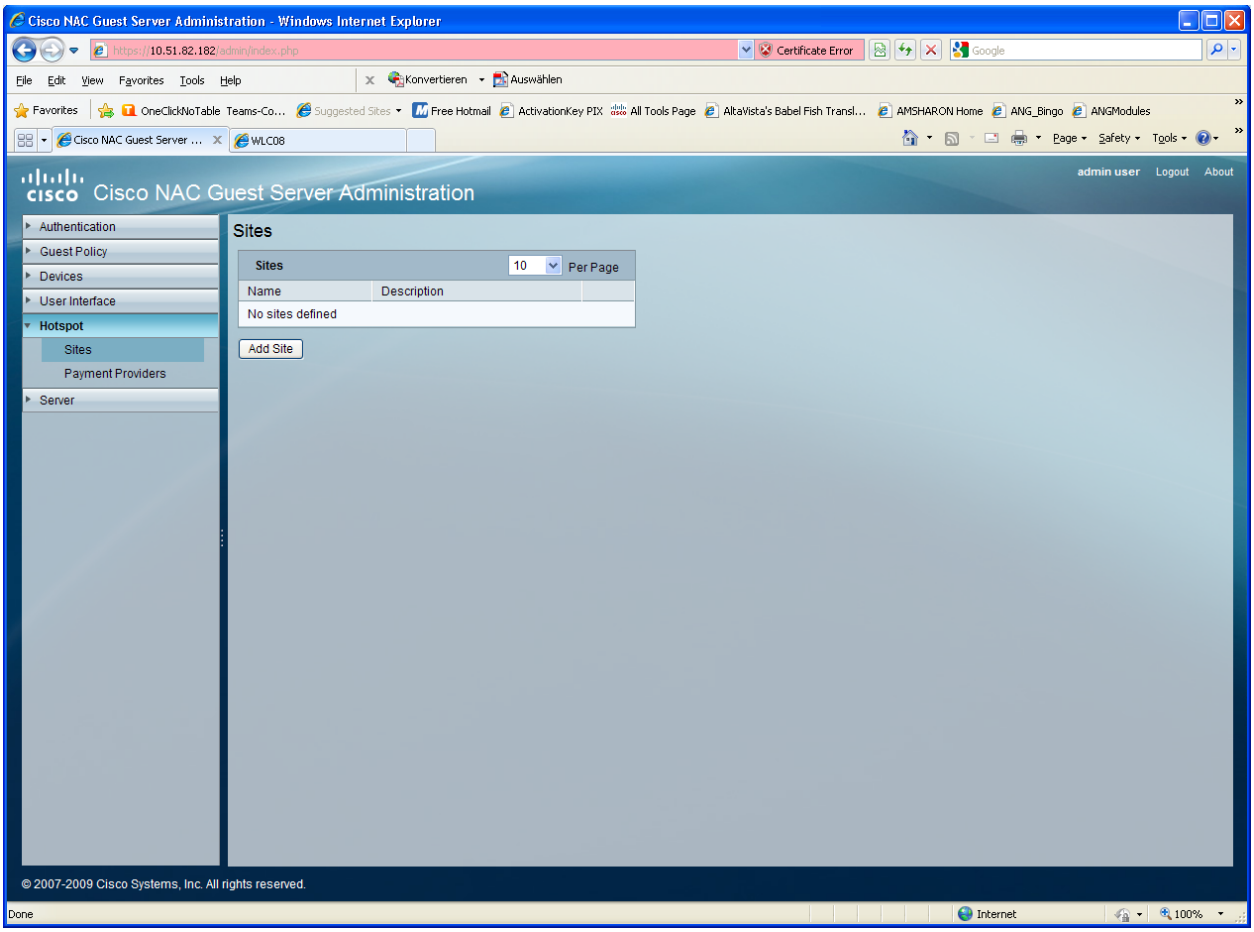
1.) You need to create the files required on NGS to have login page

http://www.cisco.com/en/US/docs/security/nac/guestserver/configuration_guide/20/g_hotspots.html#wp1073046

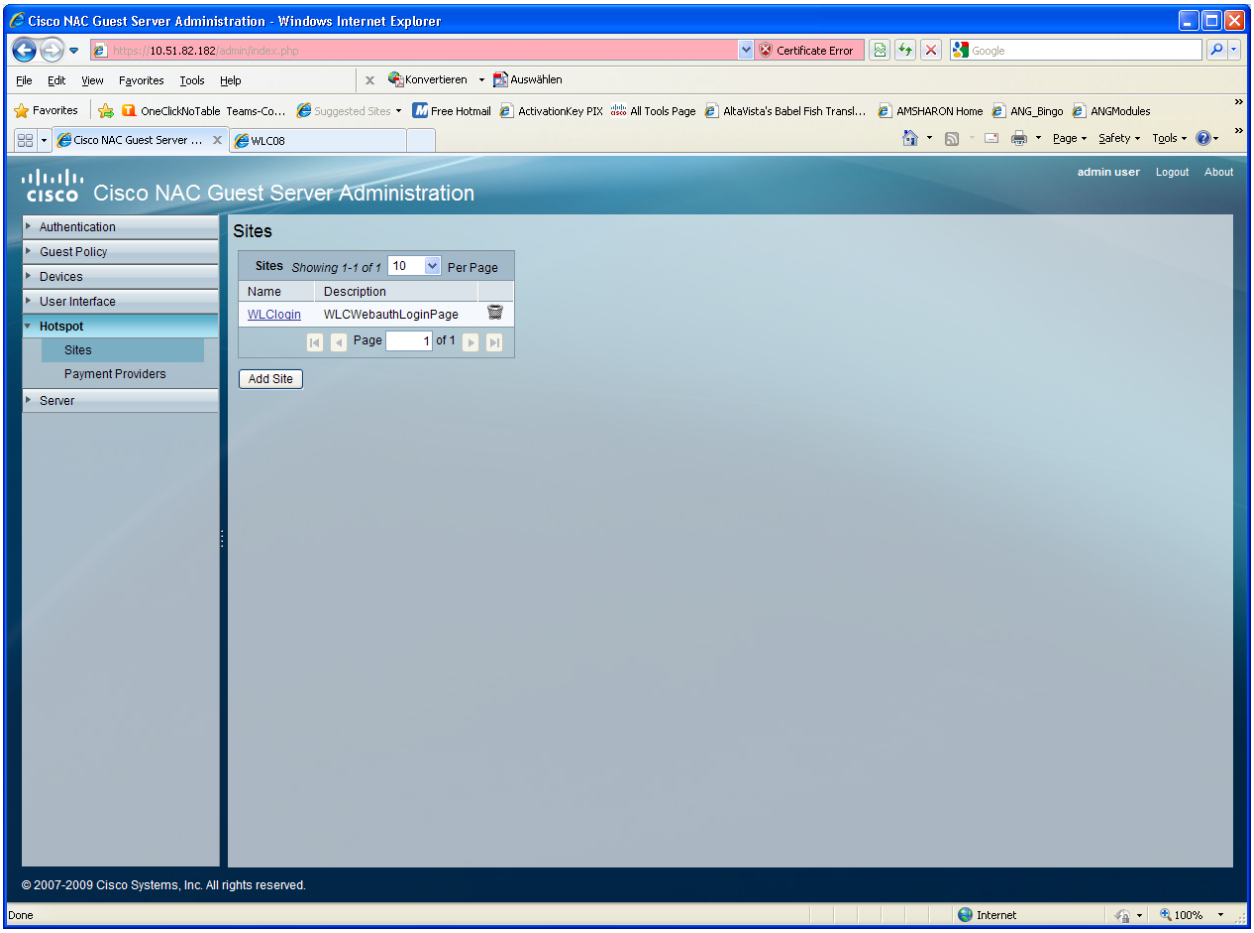
a.) Create a file called login.html with the following html code below to add the Login widget to a page

```
<html>
<head>
</head>
<body>
        <script type="text/javascript"
src="/sites/js/ngs_wlc_login.js"></script>
</body>
<html>
```

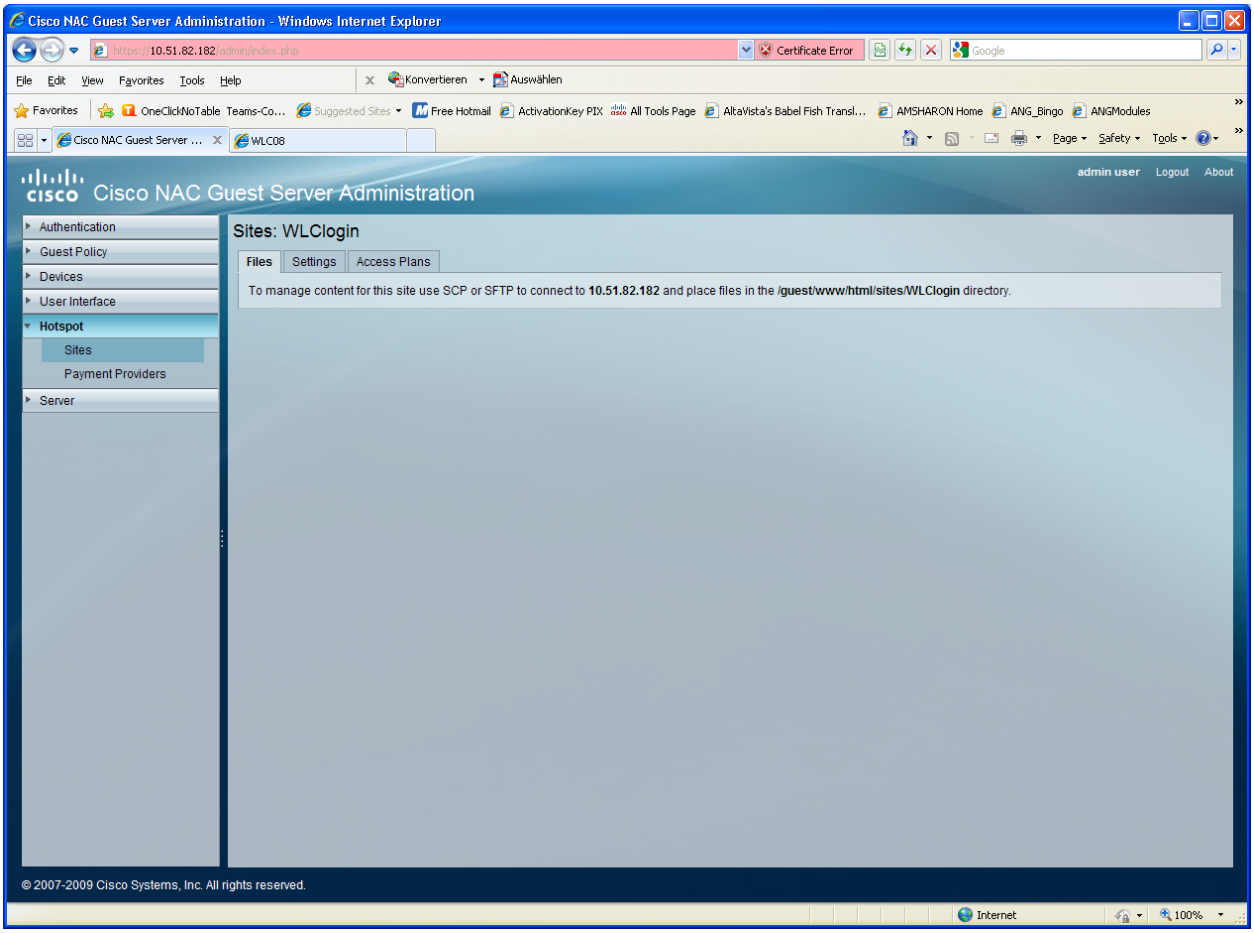
b.) Creat Hotspot Site



⇨ Add Site ➔file the form ➔Create Site

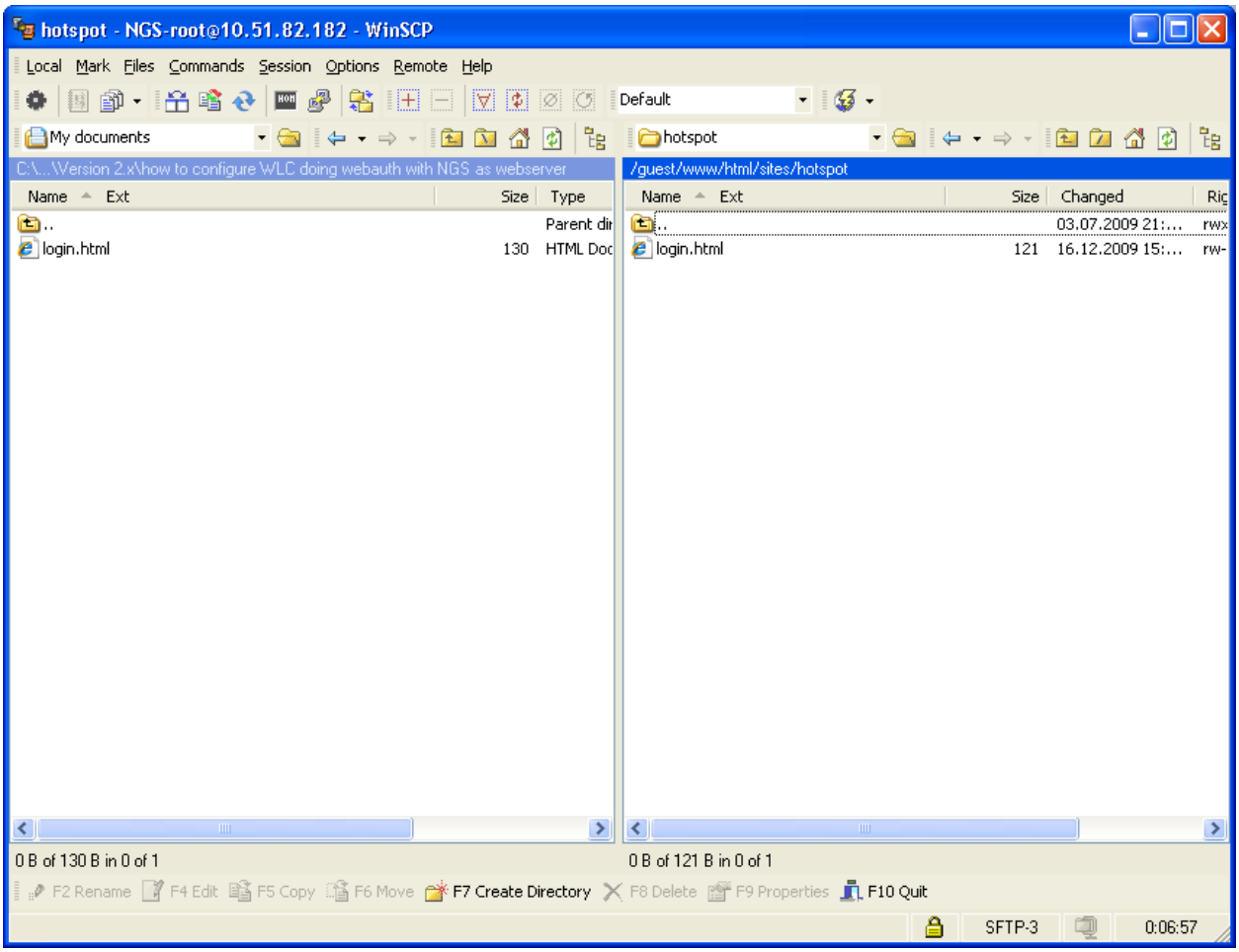


c.) Upload the login.html file to NGS



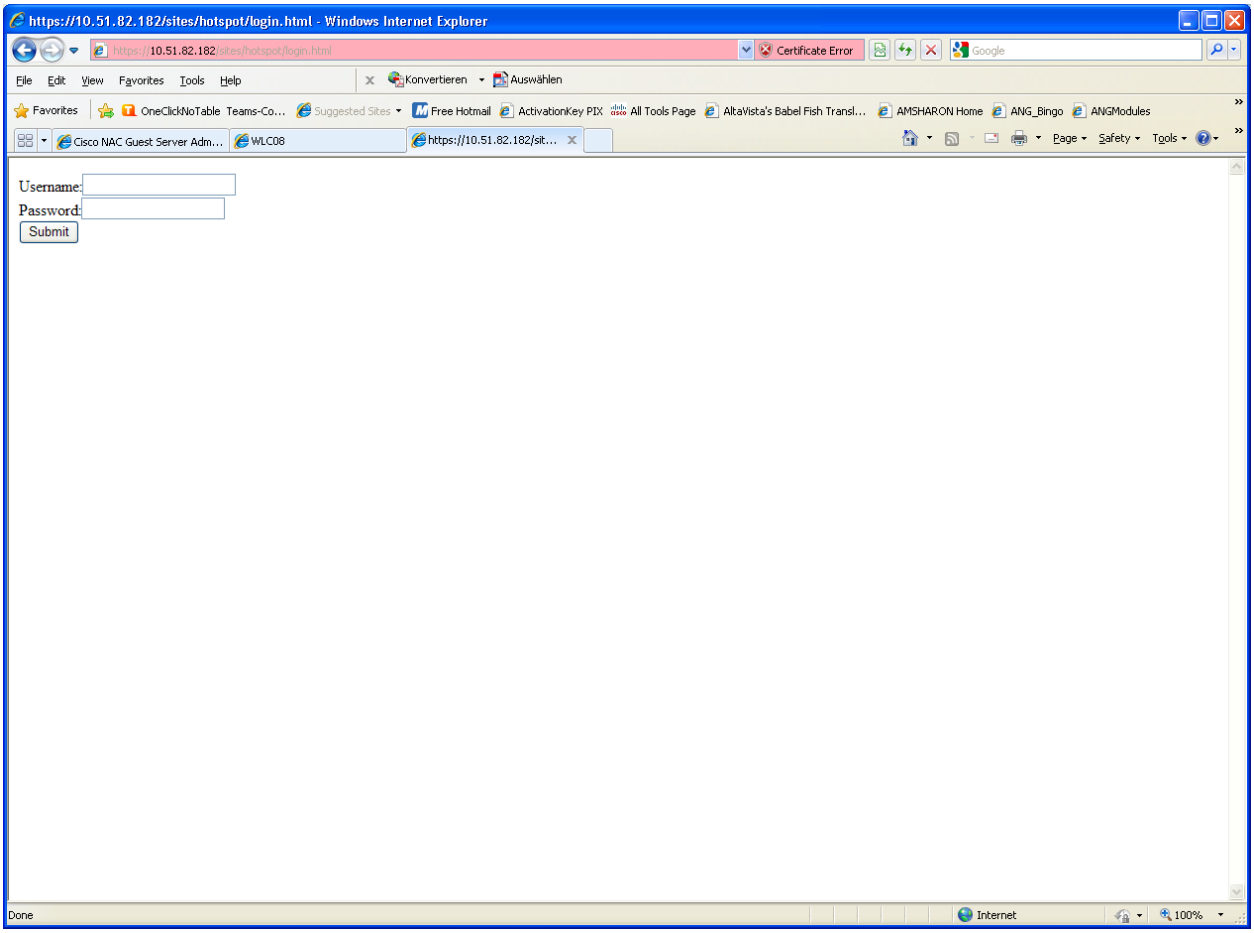
To manage content for this site use SCP or SFTP to connect to **10.51.82.182** and place files in the **/guest/www/html/sites/WLClogin** directory.

Using WinSCP



⇨ Note: path /guest/www/html/sites/hotspot – maybe needs to be created to copy the file login.html there.

Verify the login.html is working -> https://10.51.82.182/sites/hotspot/login.html

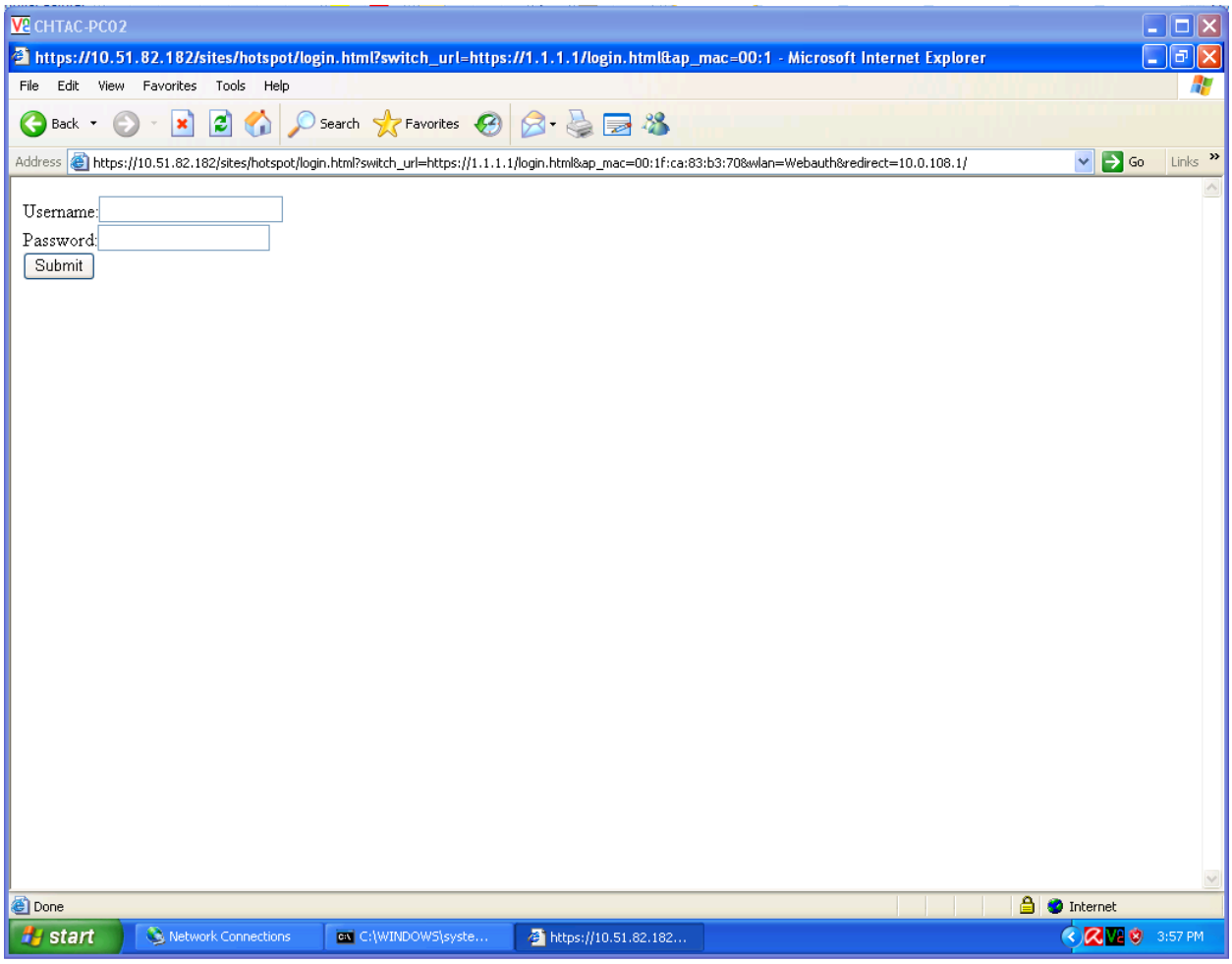


Do new deauthentication with the Wireless Client :

>Show client summary

00:40:96:b1:1c:5f chtac-LAP1130-04 Associated 2 No 802.11a 1 No

>Config client deauthenticate 00:40:96:b1:1c:5f



⇨ Note this is the login page now running on NGS.

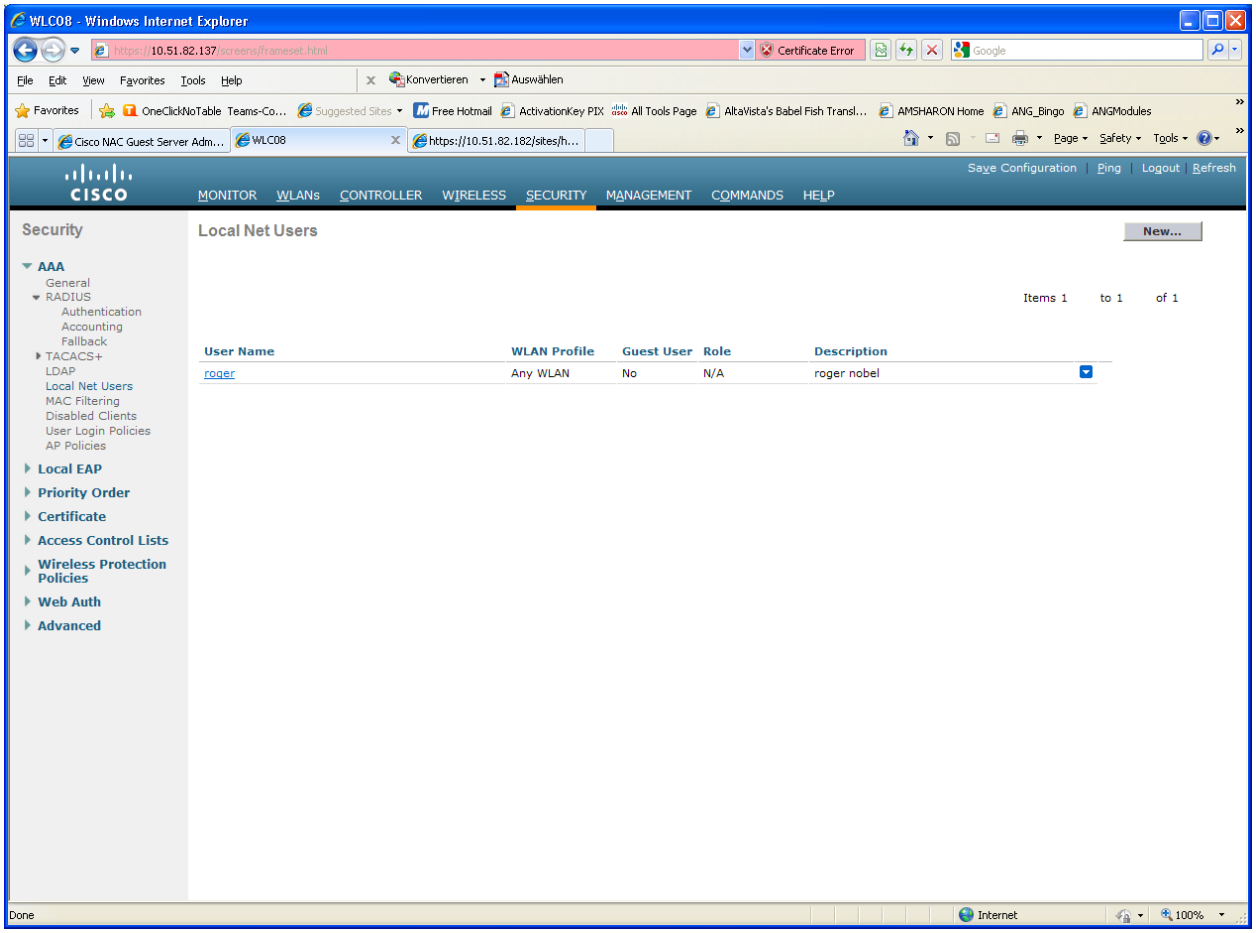
d.) Now since this is only the login page redirect and give back user credential to WLC, you would have to configure as well authentication method on WLC e.g using AAA server (Radius) or local database for user credential verification.

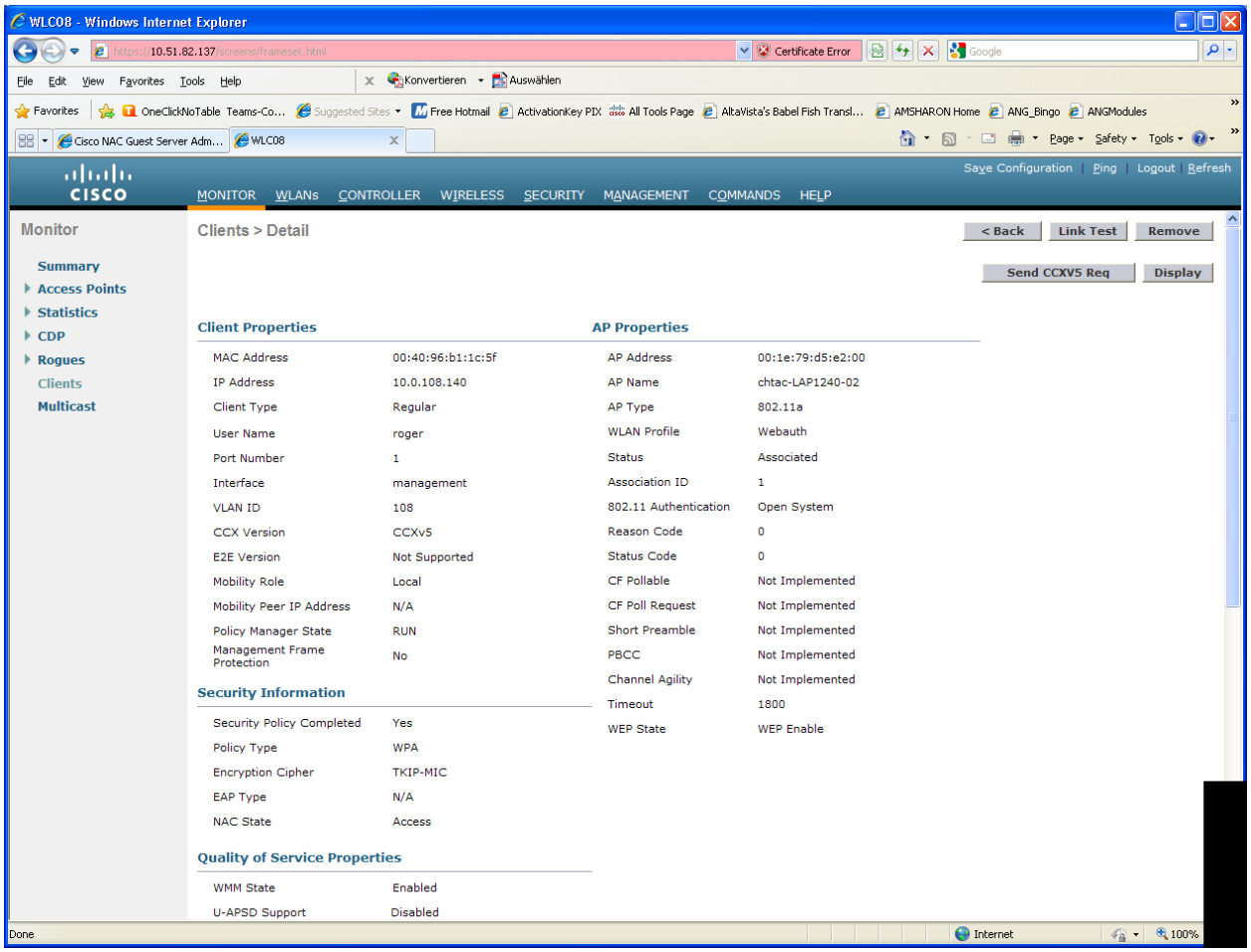
There is a possibility to use again the NGS to act as AAA server (Radius). You can follow on the link below.

Wireless LAN Controller (WLC) and NAC Guest Server (NGS) Integration Guide
http://www.cisco.com/en/US/products/ps6366/products_tech_note09186a00809d6b9a.shtml

For simplification I have a local user already per this document requirement above.

Now login with user credential and “Submit”.


WLC08 - Windows Internet Explorer
https://10.51.82.137/screens/frameset.html
Certificate Error
Google
File Edit View Favorites Tools Help
Konvertieren
Auswählen
Favorites
OneClickNoTable Teams-Co...
Suggested Sites
Free Hotmail
ActivationKey PIX
All Tools Page
AltaVista's Babel Fish Transl...
AMSHARON Home
ANG_Bingo
ANGModules
Cisco NAC Guest Server Adm...
WLC08
https://10.51.82.182/sites/h...
Page
Safety
Tools
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security
AAA
General
RADIUS
Authentication
Accounting
Fallback
TACACS+
LDAP
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Local EAP
Priority Order
Certificate
Access Control Lists
Wireless Protection Policies
Web Auth
Advanced
Local Net Users
New...
Items 1 to 1 of 1
User Name
WLAN Profile
Guest User
Role
Description
roger
Any WLAN
No
N/A
roger nobel
Done
Internet
100%



Trouble shooting

(Cisco Controller) >show debug

MAC address 00:40:96:b1:1c:5f

Debug Flags Enabled:
dhcp packet enabled.
dot11 mobile enabled.
dot11 state enabled
dot1x events enabled.
dot1x states enabled.
pem events enabled.
pem state enabled.
pm ssh-appgw enabled.
pm ssh-tcp enabled.
CCKM client debug enabled.

…

*Dec 17 11:15:31.412: 00:40:96:b1:1c:5f Stopping retransmission timer for mobile 00:40:96:b1:1c:5f
*Dec 17 11:15:33.252: 00:40:96:b1:1c:5f 0.0.0.0 DHCP_REQD (7) State Update from Mobility-Incomplete to Mobility-Complete, mobility role=Local, client state=APF_MS_STATE_ASSOCIATED
*Dec 17 11:15:33.252: 00:40:96:b1:1c:5f 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 4072, Adding TMP rule
*Dec 17 11:15:33.252: 00:40:96:b1:1c:5f 0.0.0.0 DHCP_REQD (7) Replacing Fast Path rule
 type = Airespace AP - Learn IP address
 on AP 00:1e:79:d5:e2:00, slot 1, interface = 1, QOS = 0
 ACL Id = 255, Jumbo
*Dec 17 11:15:33.252: 00:40:96:b1:1c:5f 0.0.0.0 DHCP_REQD (7) Successfully plumbed mobile rule (ACL ID 255)
*Dec 17 11:15:33.252: 00:40:96:b1:1c:5f Installing Orphan Pkt IP address 10.0.108.140 for station
*Dec 17 11:15:33.252: 00:40:96:b1:1c:5f 10.0.108.140 DHCP_REQD (7) Change state to WEBAUTH_REQD (8) last state WEBAUTH_REQD (8)
…

*Dec 17 11:15:33.253: 00:40:96:b1:1c:5f 10.0.108.140 WEBAUTH_REQD (8) Successfully plumbed mobile rule (ACL ID 255)

….

*Dec 17 11:15:38.579: 00:40:96:b1:1c:5f DHCP sending REPLY to STA (len 418, port 1, vlan 108)
*Dec 17 11:15:38.579: 00:40:96:b1:1c:5f DHCP transmitting DHCP ACK (5)
*Dec 17 11:15:38.579: 00:40:96:b1:1c:5f DHCP op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0
*Dec 17 11:15:38.579: 00:40:96:b1:1c:5f DHCP xid: 0xb6a95602 (3064550914), secs: 0, flags: 0
*Dec 17 11:15:38.579: 00:40:96:b1:1c:5f DHCP chaddr: 00:40:96:b1:1c:5f
*Dec 17 11:15:38.579: 00:40:96:b1:1c:5f DHCP ciaddr: 10.0.108.140, yiaddr: 10.0.108.140
*Dec 17 11:15:38.579: 00:40:96:b1:1c:5f DHCP siaddr: 0.0.0.0, giaddr: 0.0.0.0
*Dec 17 11:15:38.579: 00:40:96:b1:1c:5f DHCP server id: 1.1.1.1 rcvd server id: 10.0.108.1

Note: Wireless client is associated to LAP (WLC) and did get IP address assigned is now in WEBAUTH_REQD status.

- ⇨ Open IE on WirelessClient and get redirect to login page to fill the username/password and “Submit”

(Cisco Controller) >*Dec 17 11:16:40.631: 00:40:96:b1:1c:5f Username entry (roger) created for mobile
*Dec 17 11:16:40.632: 00:40:96:b1:1c:5f 10.0.108.140 WEBAUTH_REQD (8) Change state to WEBAUTH_NOL3SEC (14) last state WEBAUTH_NOL3SEC (14)

***Dec 17 11:16:40.638: 00:40:96:b1:1c:5f 10.0.108.140 WEBAUTH_NOL3SEC (14) Change state to RUN (20) last state RUN (20)**

*Dec 17 11:16:40.638: 00:40:96:b1:1c:5f Session Timeout is 1800 - starting session timer for the mobile

*Dec 17 11:16:40.639: 00:40:96:b1:1c:5f 10.0.108.140 RUN (20) Reached PLUMBFASTPATH: from line 4675
*Dec 17 11:16:40.639: 00:40:96:b1:1c:5f 10.0.108.140 RUN (20) Replacing Fast Path rule
 type = Airespace AP Client
 on AP 00:1e:79:d5:e2:00, slot 1, interface = 1, QOS = 0
 ACL Id = 255, Jumbo Frames = NO
*Dec 17 11:16:40.639: 00:40:96:b1:1c:5f 10.0.108.140 RUN (20) Successfully plumbed mobile rule (ACL ID 255)
*Dec 17 11:16:40.673: 00:40:96:b1:1c:5f 10.0.108.140 Added NPU entry of type 1, dtlFlags 0x0
*Dec 17 11:16:40.674: 00:40:96:b1:1c:5f Sending a gratuitous ARP for 10.0.108.140, VLAN Id 108

⇨ Webauthentication is successful.

Appendix - Customizing login page:

http://www.cisco.com/en/US/docs/security/nac/guestserver/configuration_guide/20/g_hotspots.html#wp1089039

You can also use ext weblogin page example provide for WLC from CCO.

http://tools.cisco.com/support/downloads/go/PlatformList.x?sftType=Wireless+Lan+Controller+Web+Authentication+Bundle&mdfid=279911269&treeName=Wireless&mdfLevel=Model&url=null&modelName=Cisco+4404+Wireless+LAN+Controller&isPlatform=null&treeMdfId=278875243&modifmdfid=null&imname=&hybrid=Y&imst=N

➔ webauth_bundle.zip -> webauth -> case
- aup.html
- login.html
- yourlogo.jpg

Load the files on same folder on NGS /guest/www/html/sites/hotspot….

- login.html
- aup.html
- yourlogo.jpg

Verify the page by: https://<ngs ip addr>/sites/hotspot/login.html