

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

How to configure WLC doing Web—Auth using NGS as central WebServer.....	1
Idea:.....	1
Setup:.....	2
Requirement:	2
WLC Configuration:.....	3
NGS Configuration:.....	4
Trouble shooting	12
Appendix - Customizing login page:	14

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.

The screenshot shows the Cisco WLC configuration interface in a Windows Internet Explorer browser. The page title is 'WLANs > Edit'. The 'Security' tab is selected, showing the following configuration:

Profile Name	Webauth
Type	WLAN
SSID	Webauth
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	Web-Auth[WPA + WPA2][Auth(PSK)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface	management
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

Foot Notes:

- 1 CKIP is not supported by 10xx model APs
- 3 H-REAP Local Switching is not supported with IPsec, CRANITE authentication
- 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
- 5 Client HFP is not active unless WPA2 is configured
- 6 Learn Client IP is configurable only when HREAP Local Switching is enabled
- 7 WMM and open or AES security should be enabled to support higher 11n rates

The screenshot displays the Cisco WLC GUI in Internet Explorer. The main content area shows the 'Clients > Detail' page for a client named 'roger'. The page is divided into several sections: Client Properties, AP Properties, Security Information, and Quality of Service Properties. Several values are circled in red to highlight specific configuration details.

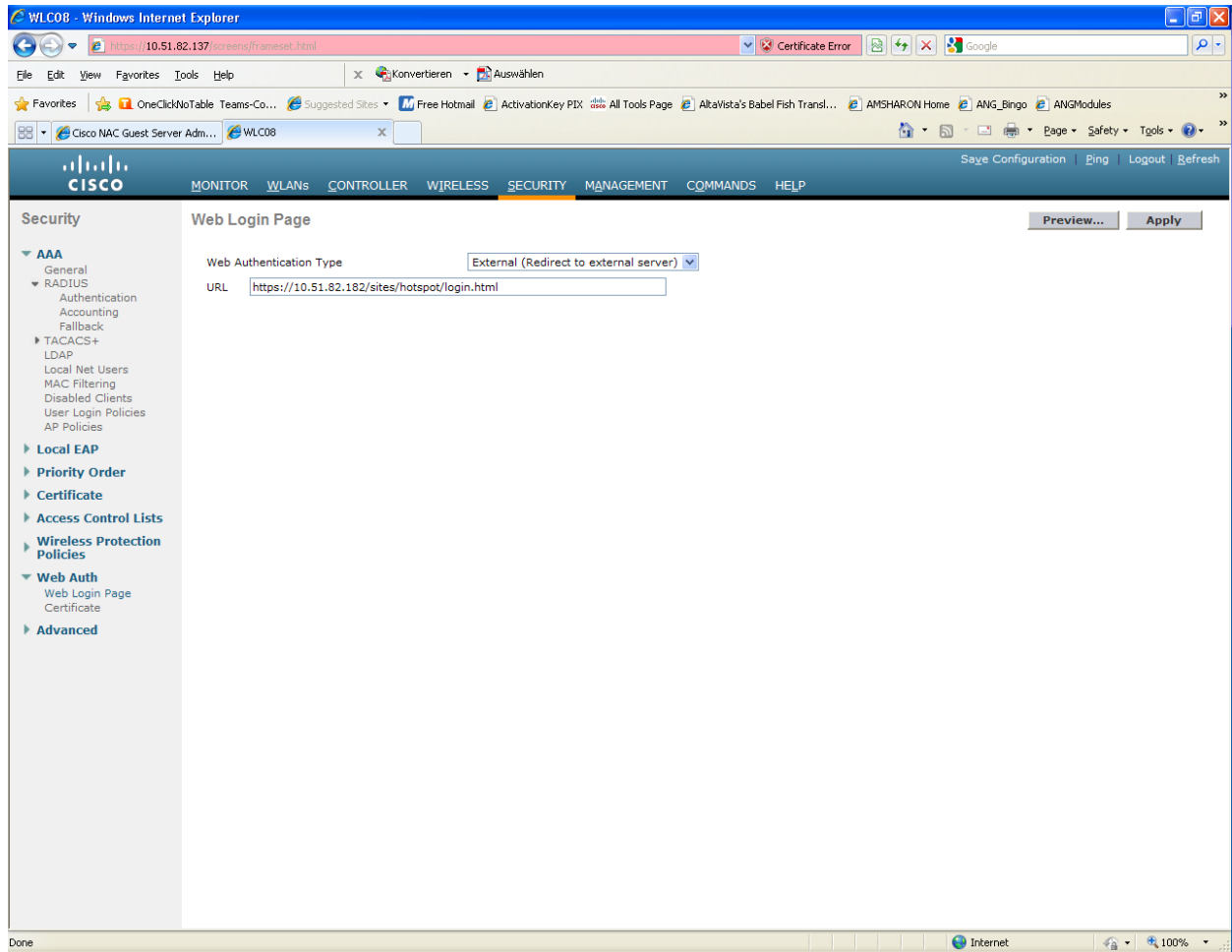
Client Properties		AP Properties	
MAC Address	00:40:96:b1:1c:5f	AP Address	00:1f:ca:83:b3:70
IP Address	10.0.108.140	AP Name	chtac-LAP1130-04
Client Type	Regular	AP Type	802.11a
User Name	roger	WLAN Profile	Webauth
Port Number	1	Status	Associated
Interface	management	Association ID	1
VLAN ID	108	802.11 Authentication	Open System
CCX Version	CCXv5	Reason Code	0
E2E Version	Not Supported	Status Code	0
Mobility Role	Local	CF Pollable	Not Implemented
Mobility Peer IP Address	N/A	CF Poll Request	Not Implemented
Policy Manager State	RUN	Short Preamble	Not Implemented
Management Frame Protection	No	PBCC	Not Implemented
		Channel Agility	Not Implemented
		Timeout	1800
		WEP State	WEP Enable

Security Information	
Security Policy Completed	Yes
Policy Type	WPA
Encryption Cipher	TKIP-MIC
EAP Type	N/A
NAC State	Access

Quality of Service Properties	
WMM State	Enabled
U-APSD Support	Disabled
QoS Level	Silver
Diff Serv Code Point (DSCP)	disabled

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:

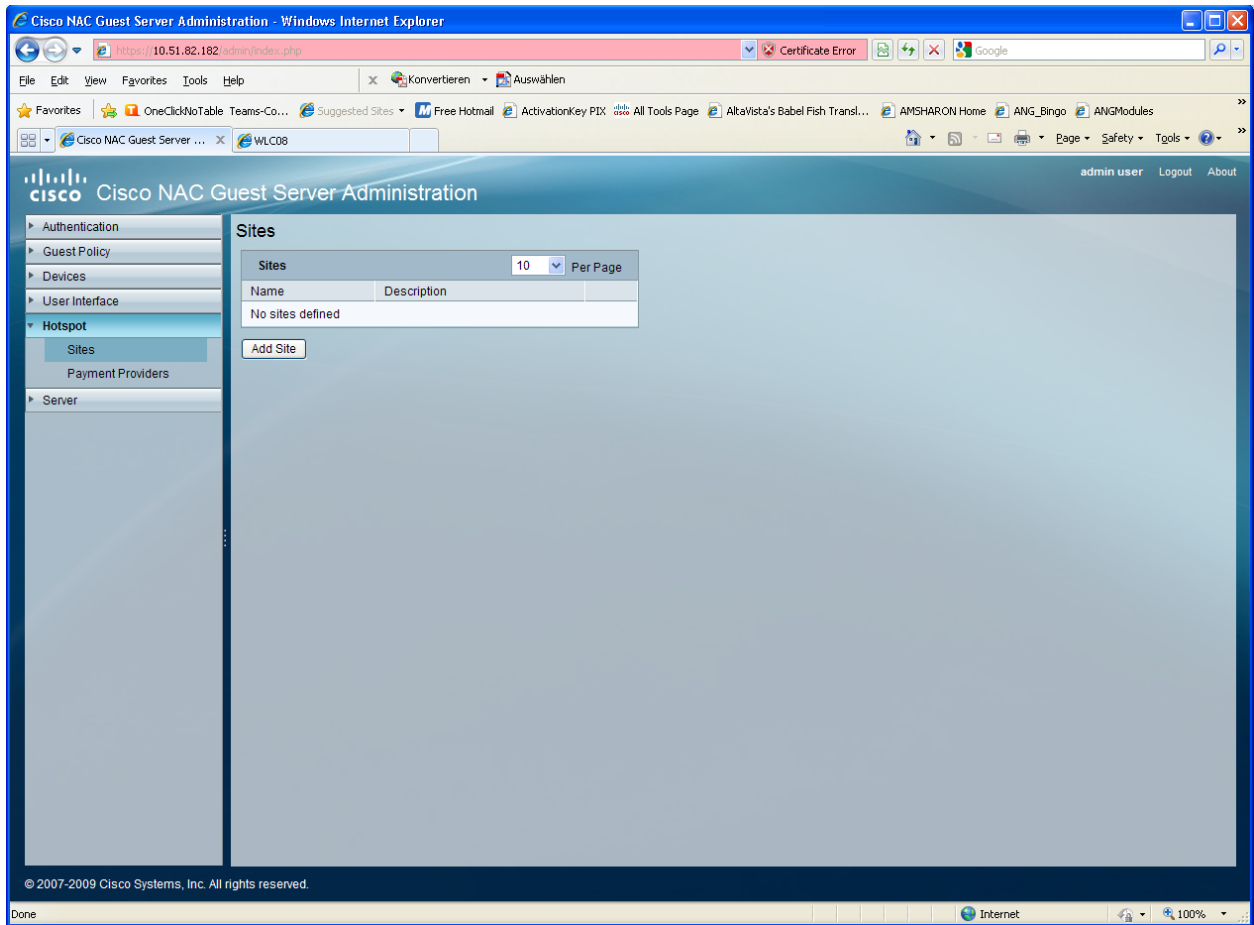
- 1.) You need to create the files required on NGS to have login page

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

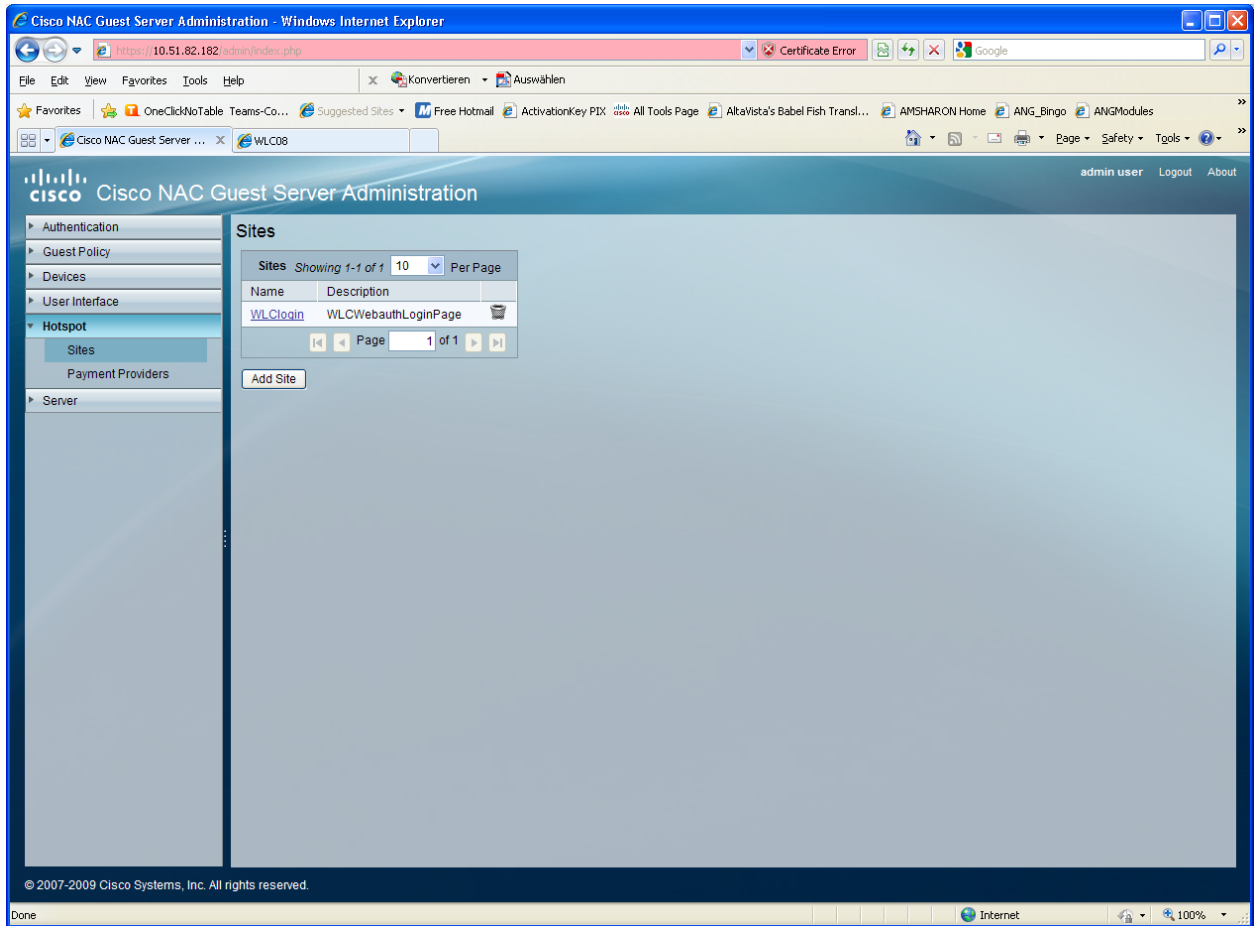
```
<html>
<head>
</head>
<body>
  <script type="text/javascript"
  src="/sites/js/ngs_wlc_login.js"></script>
</body>
</html>
```

b.) Creat Hotspot Site

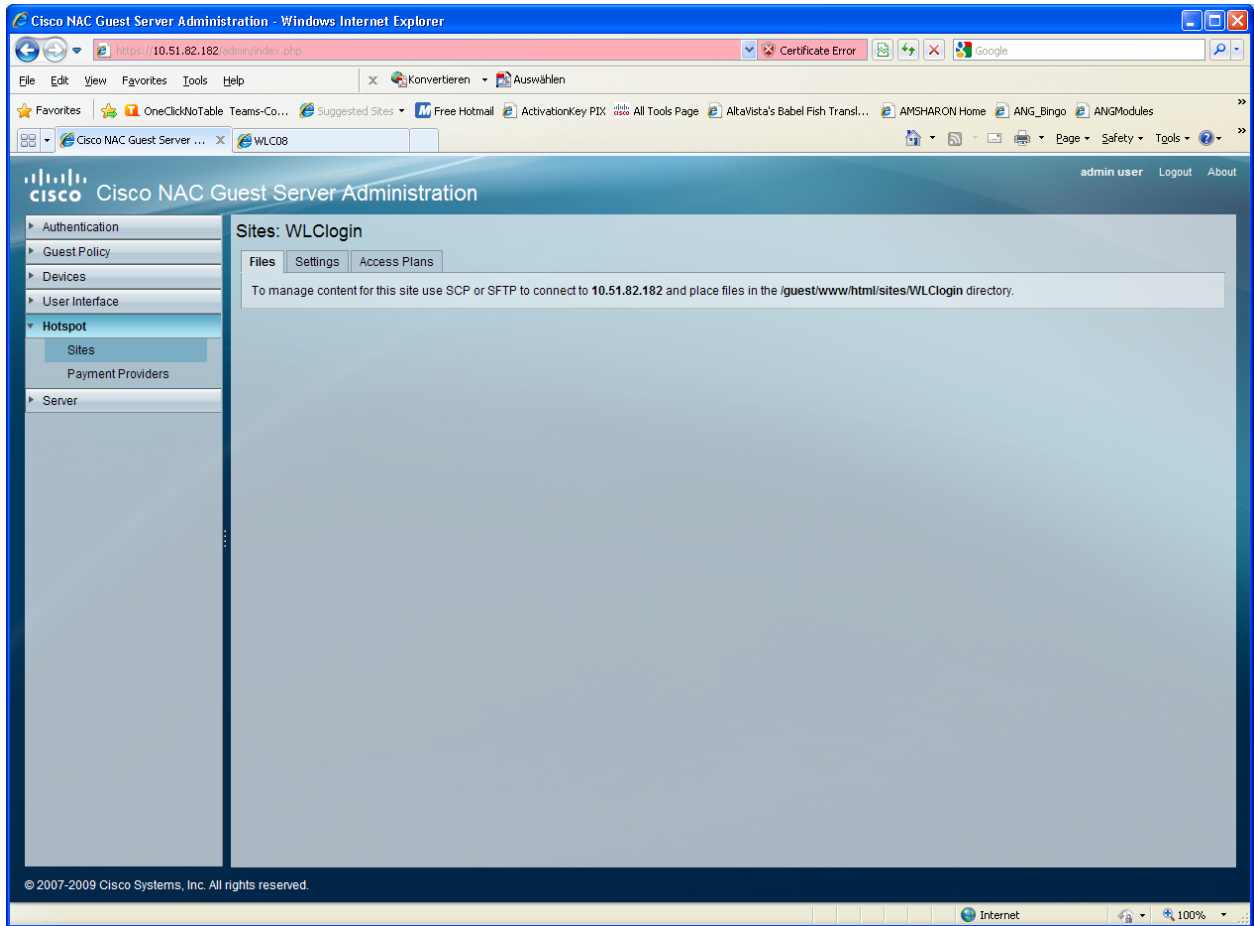


The screenshot shows the Cisco NAC Guest Server Administration web interface in a Windows Internet Explorer browser. The browser's address bar displays the URL `https://10.51.82.182/admin/index.php`. The interface features a navigation menu on the left with categories: Authentication, Guest Policy, Devices, User Interface, Hotspot, and Server. The 'Hotspot' category is expanded, showing sub-items: Sites, Payment Providers, and Server. The main content area is titled 'Sites' and contains a table with columns 'Name' and 'Description'. The table is currently empty, with the text 'No sites defined' displayed below it. An 'Add Site' button is located below the table. The interface also includes a 'Per Page' dropdown menu set to '10'. The footer of the page contains the copyright notice '© 2007-2009 Cisco Systems, Inc. All rights reserved.' and the text 'Done'.

⇒ Add Site → file the form → Create Site

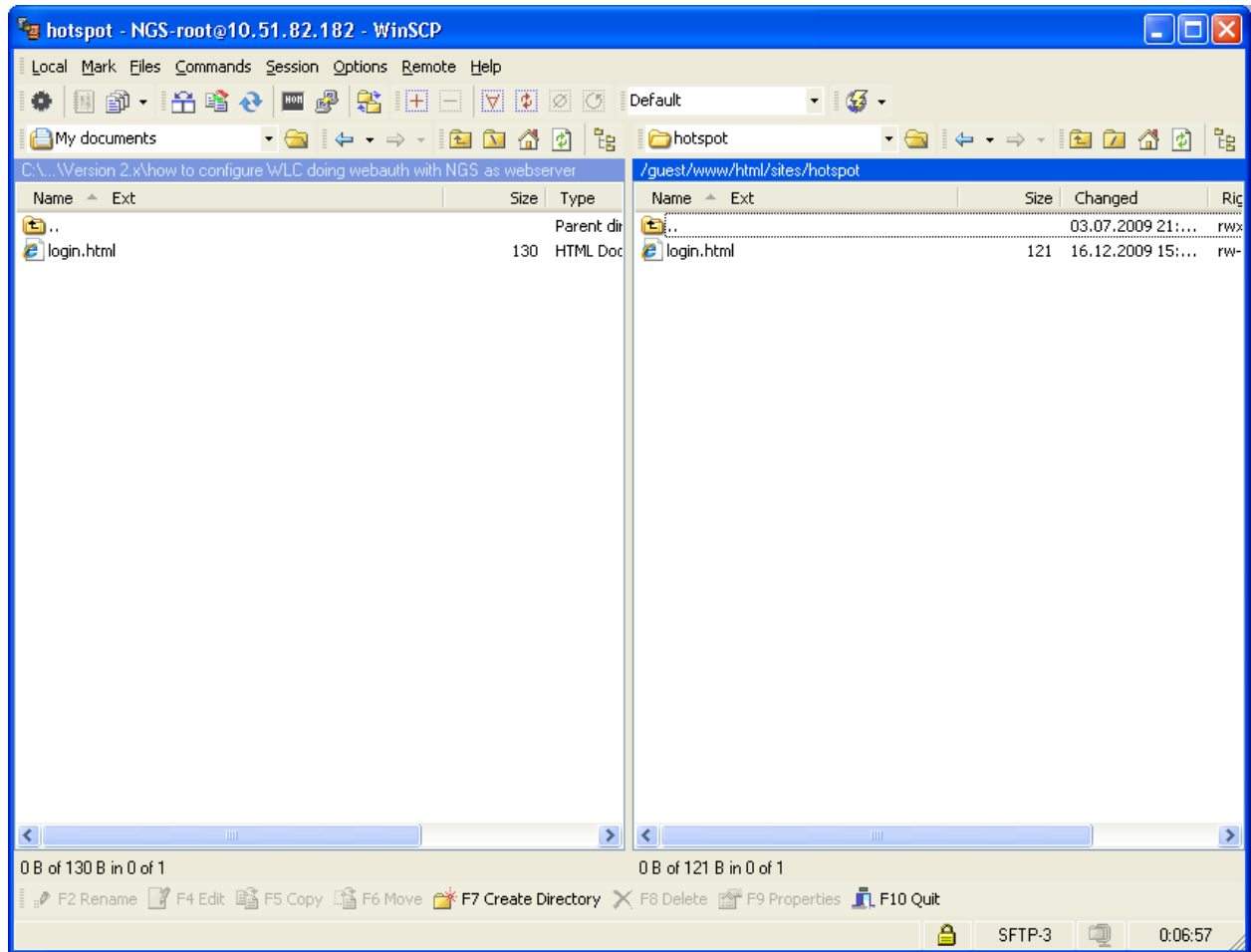


c.) Upload the login.html file to NGS



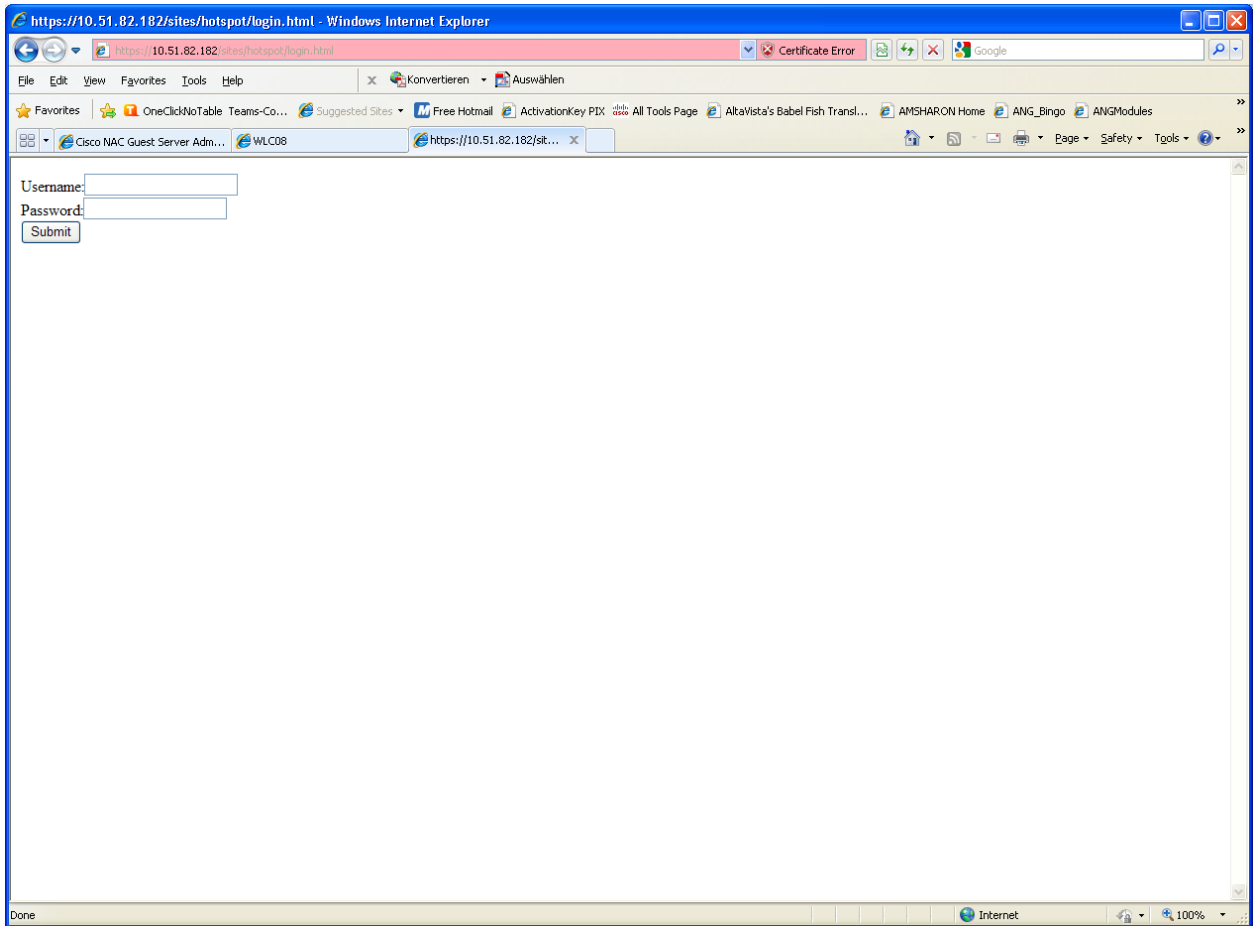
To manage content for this site use SCP or SFTP to connect to **10.51.82.182** and place files in the **/guest/www/html/sites/WLClogin** directory.

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>

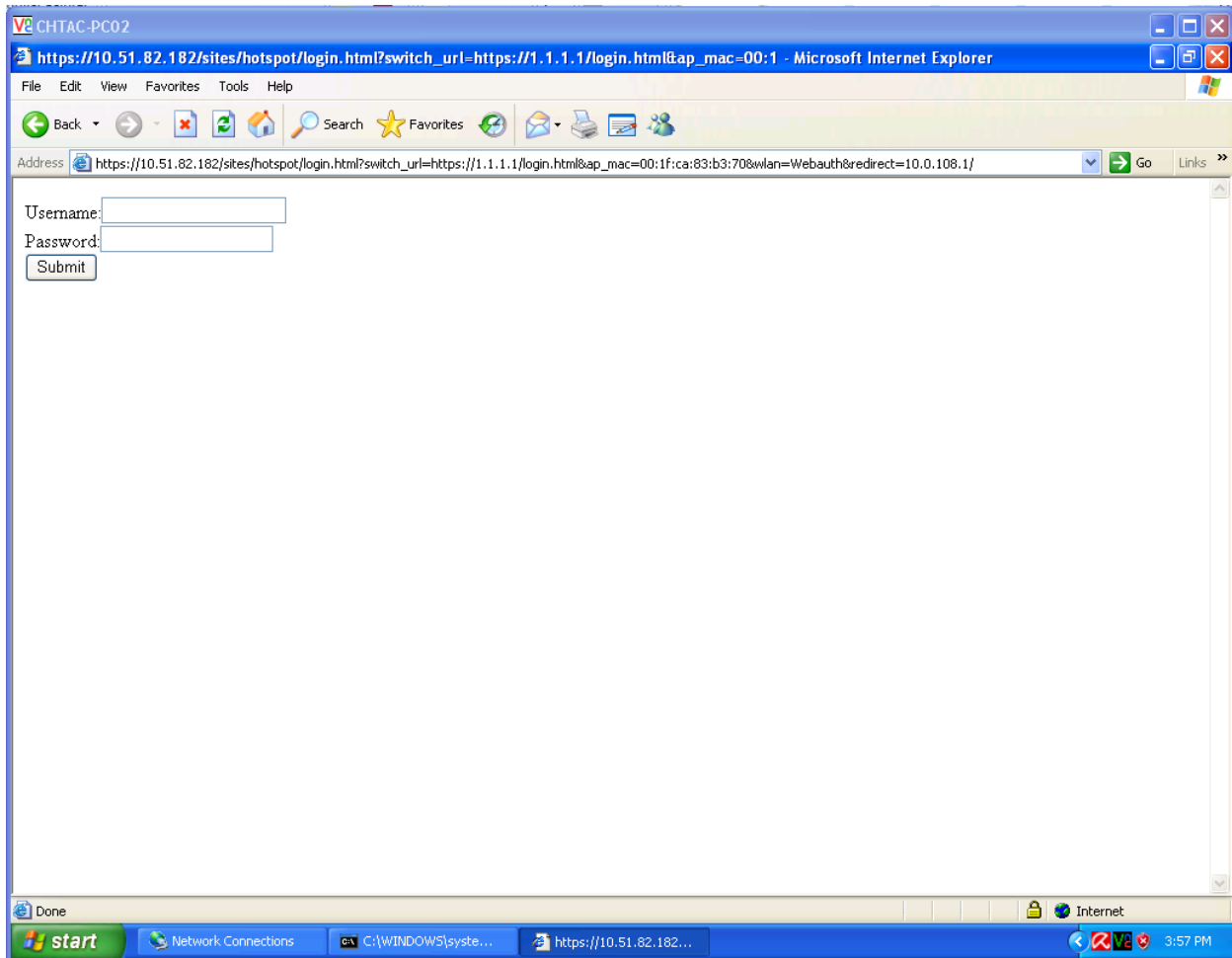


Do new deauthentication with the Wireless Client :

>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 AlkaVista's Babel Fish Transl... AMSHARON Home ANG_Bingo ANGMModules

Cisco MAC Guest Server Adm... WLC08 https://10.51.82.182/sites/h...

Save Configuration Ping Logout Refresh

CISCO MONITOR WLANs CONTROLLER WIRELESS **SECURITY** MANAGEMENT COMMANDS HELP

Security

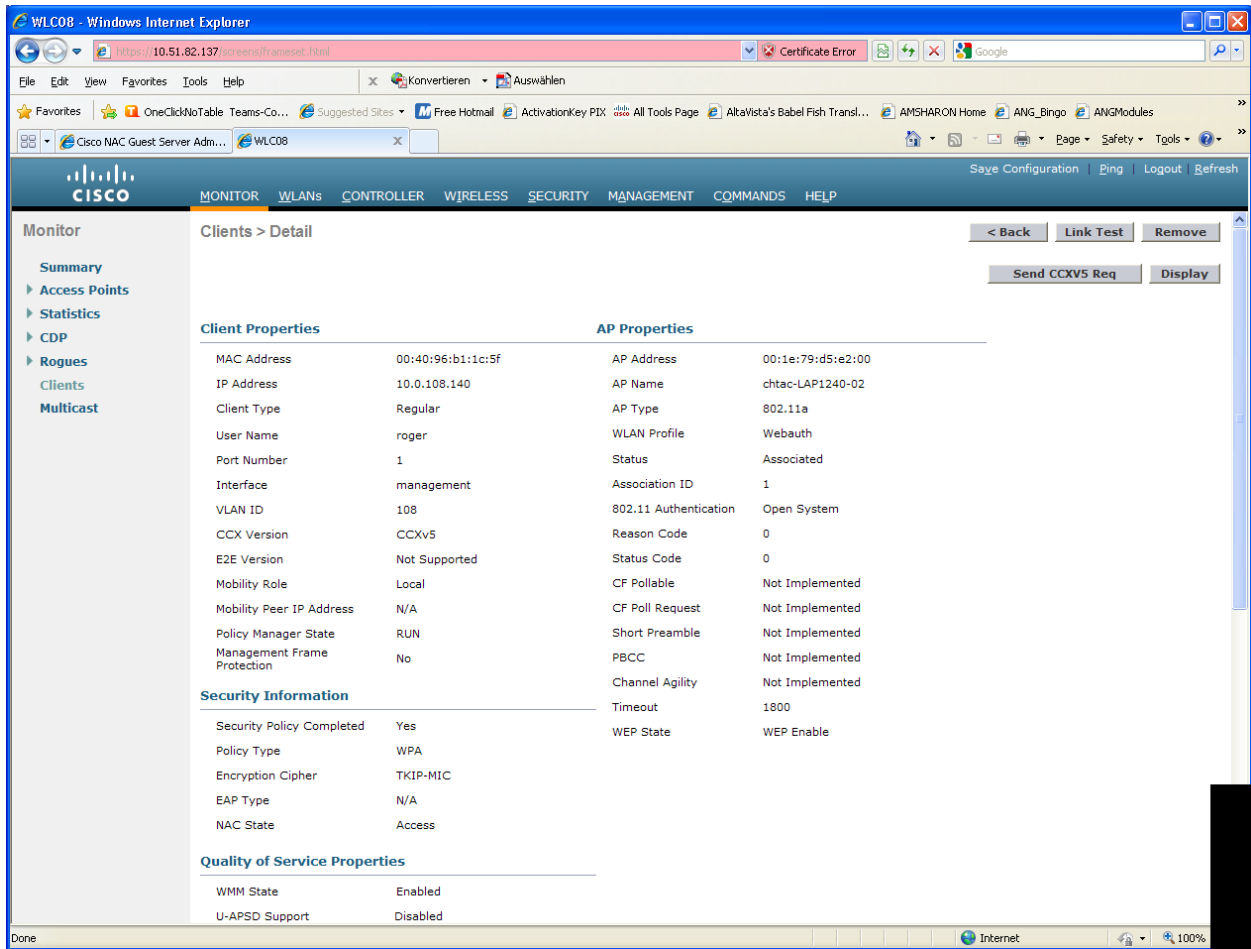
- AAA
 - General
 - RADIUS
 - Authentication
 - Accounting
 - Fallback
 - TACACS+
 - LDAP
 - Local Net Users
 - MAC Filtering
 - Disabled Clients
 - User Login Policies
 - AP Policies
- Local EAP
- Priority Order
- Certificate
- Access Control Lists
- Wireless Protection Policies
- Web Auth
- Advanced

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 PLUMBFASPATH: 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&image=&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>