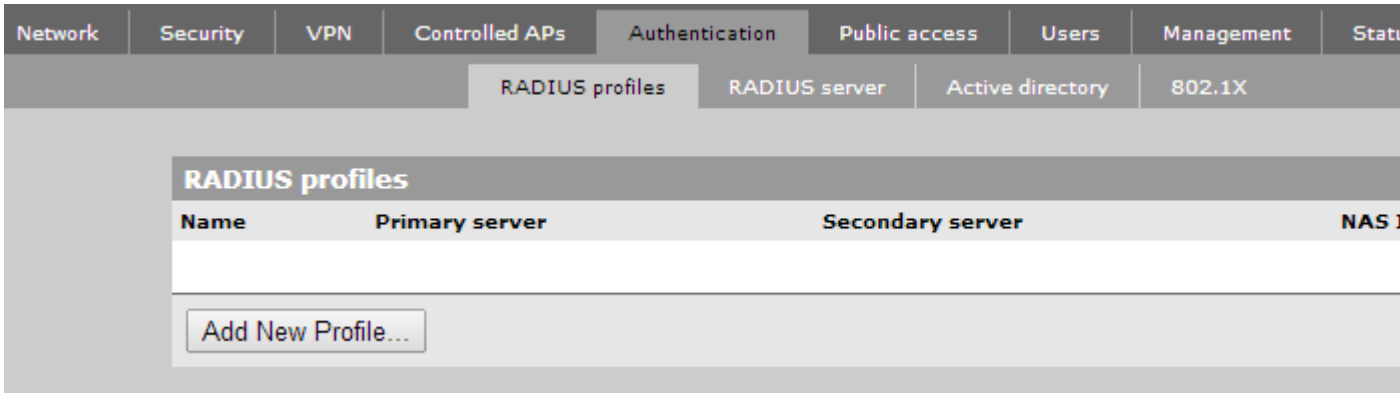
HP (MSM managed)

Modified on: Thu, 26 Feb, 2015 at 11:16 AM

Open a web browser and log in to your HP MSM controller web interface

Click on "**Authentication**" on the top menu

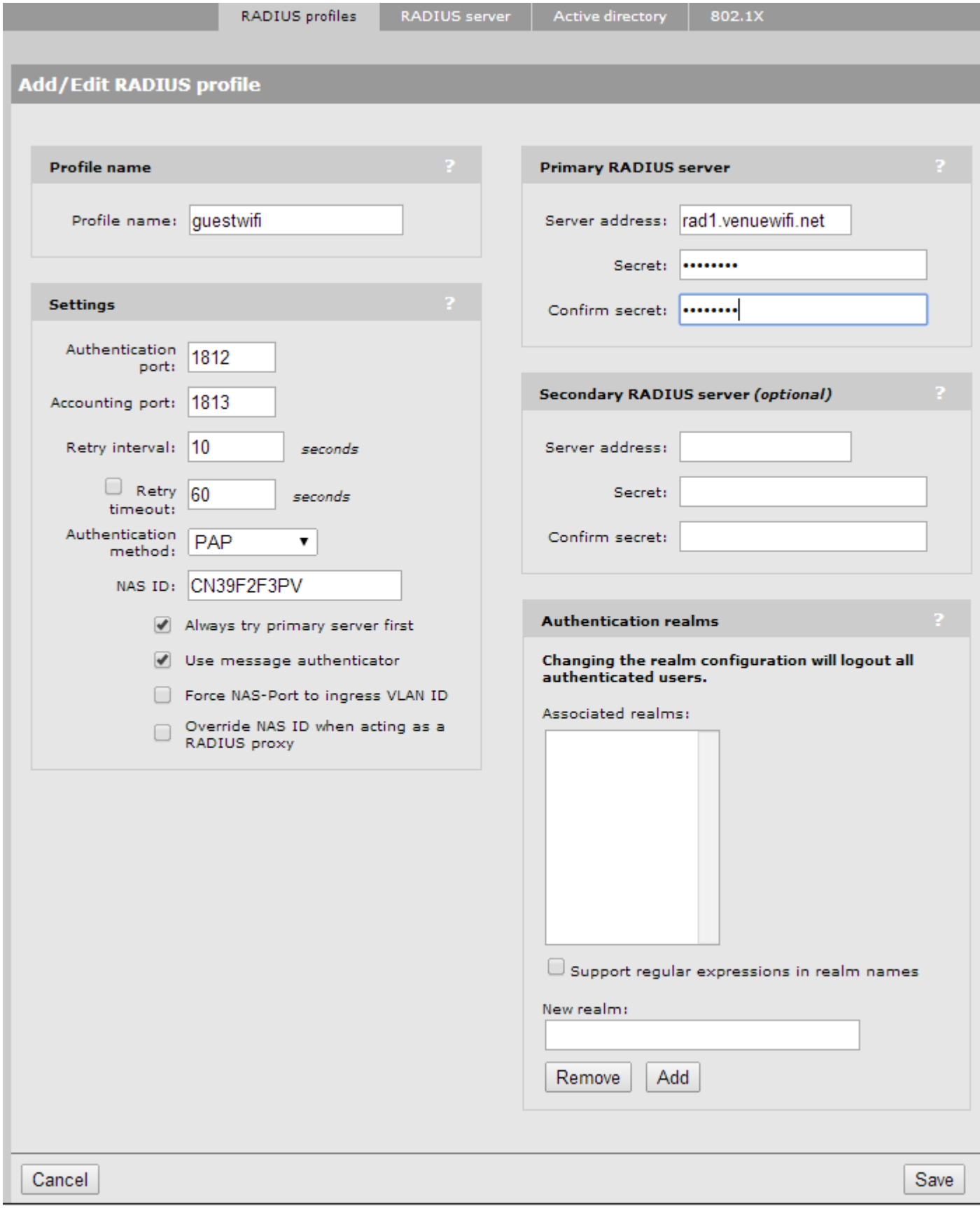
Select "**RADIUS Profiles**" on the top sub menu and then click "**Add New Profile**"



Enter the following information:

- **Profile Name**: guestwifi
- **Authentication port**: 1812
- **Accounting port**: 1813
- **Authentication method**: PAP
- **Server address**: *insert radius_server here*
- **Secret**: *insert radius_secret here*
- **Confirm secret**: As above

Click on **Save**


RADIUS profiles
RADIUS server
Active directory
802.1X
Add/Edit RADIUS profile
Profile name
Profile name: guestwifi
Settings
Authentication port: 1812
Accounting port: 1813
Retry interval: 10 seconds
Retry timeout: 60 seconds
Authentication method: PAP
NAS ID: CN39F2F3PV
Always try primary server first
Use message authenticator
Force NAS-Port to ingress VLAN ID
Override NAS ID when acting as a RADIUS proxy
Primary RADIUS server
Server address: rad1.venuewifi.net
Secret:
Confirm secret:
Secondary RADIUS server (optional)
Server address:
Secret:
Confirm secret:
Authentication realms
Changing the realm configuration will logout all authenticated users.
Associated realms:
Support regular expressions in realm names
New realm:
Remove
Add
Cancel
Save

On the left menu, under Network Tree, click "**VSCs**" and then click "**Add New VSC Profile**". Set the correct settings:

Under **Global**:

- **Profile Name**: Free WiFi
- **Use Controller for**: Tick both Authentication and Access control

Under **Access Control**:

- **Present session and welcome page**: Ticked

Under **Virtual AP**:

- **Name (SSID)**: Free WiFi (or whatever you want)
- **Broadcast name (SSID)**: Ticked

Under **HTML-based user logins**:

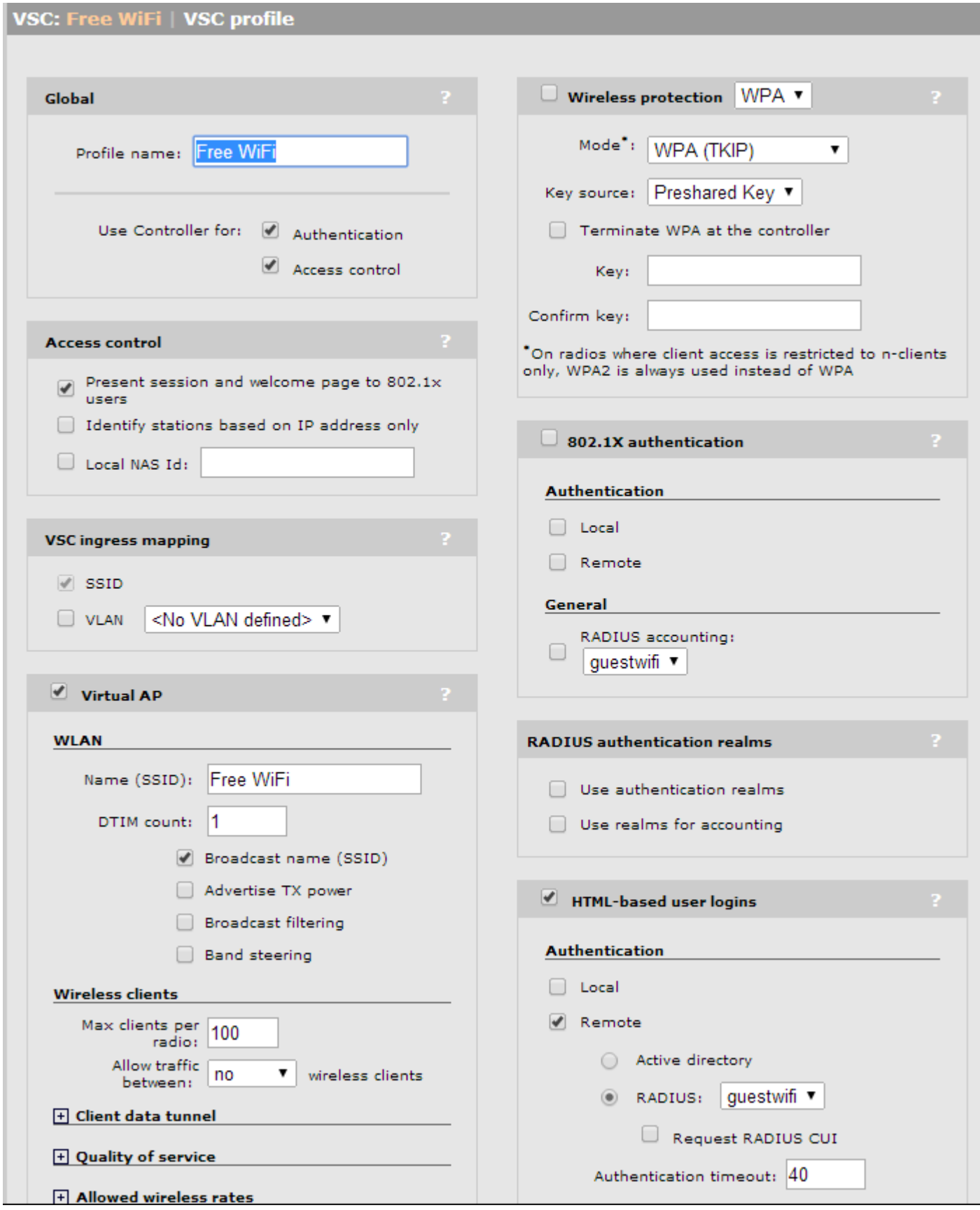
- **HTML-based user logins**: Ticked
- **Authentication**: Remote
- **RADIUS**: guestwifi
- **RADIUS accounting**: Ticked; choose guestwifi

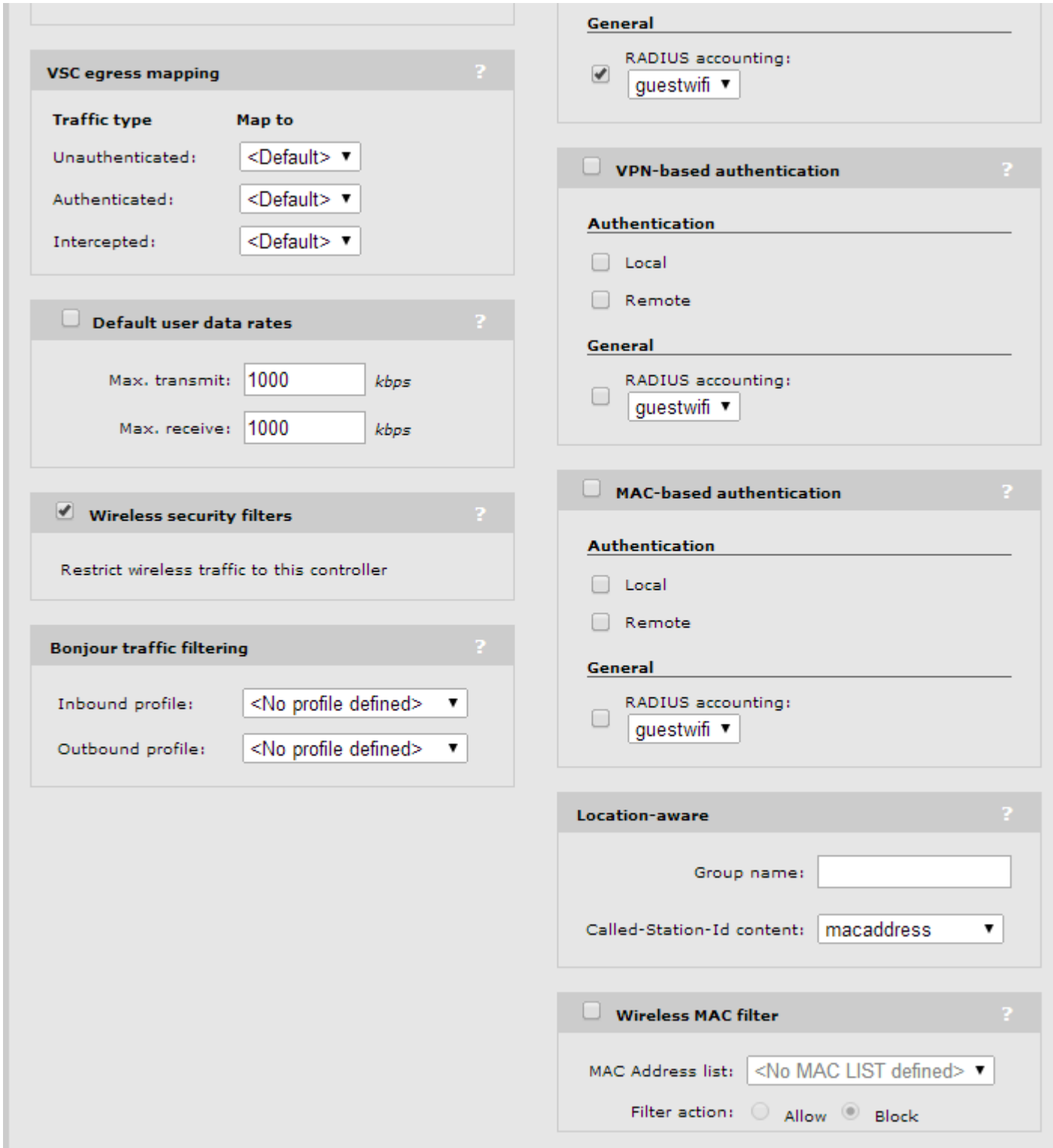
Under **Location-aware**:

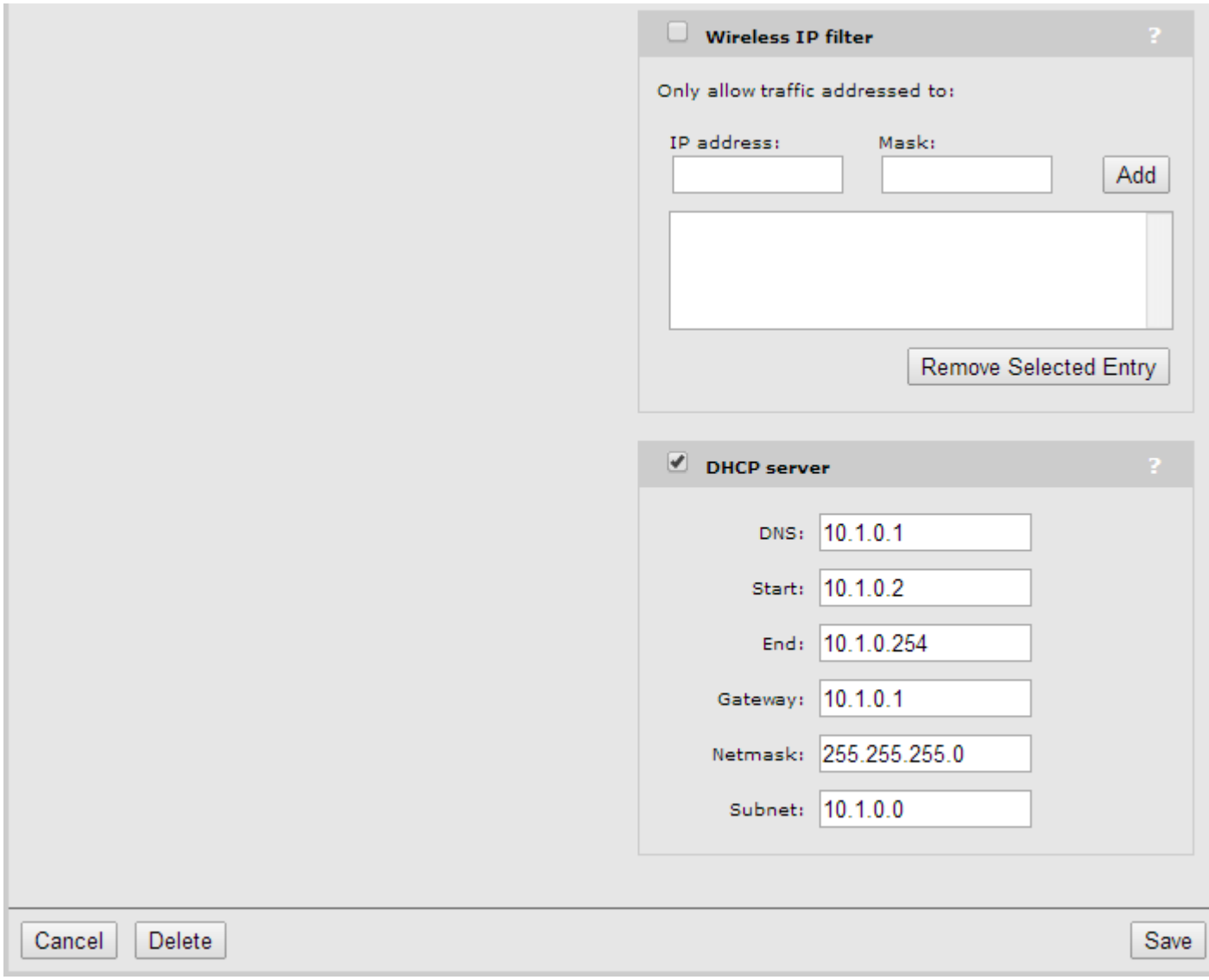
- **Called-Station-Id content**: macaddress

Under **DHCP server**:

- **DNS**: 10.1.0.1
- **Start**: 10.1.0.2
- **End**: 10.1.0.254
- **Gateway**: 10.1.0.1
- **Netmask**: 255.255.255.0
- **Subnet**: 10.1.0.0

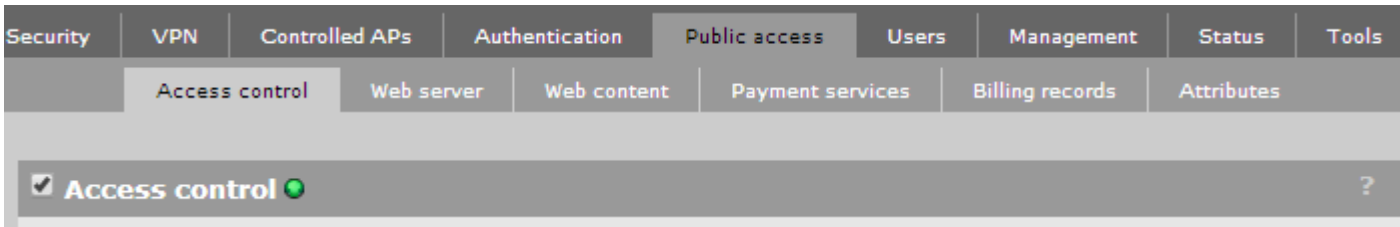

VSC: Free WiFi | VSC profile
Global
Profile name: Free WiFi
Use Controller for: Authentication
Access control
Access control
Present session and welcome page to 802.1x users
Identify stations based on IP address only
Local NAS Id:
VSC ingress mapping
SSID
VLAN <No VLAN defined>
Virtual AP
WLAN
Name (SSID): Free WiFi
DTIM count: 1
Broadcast name (SSID)
Advertise TX power
Broadcast filtering
Band steering
Wireless clients
Max clients per radio: 100
Allow traffic between: no wireless clients
Client data tunnel
Quality of service
Allowed wireless rates
Wireless protection WPA
Mode*: WPA (TKIP)
Key source: Preshared Key
Terminate WPA at the controller
Key:
Confirm key:
*On radios where client access is restricted to n-clients only, WPA2 is always used instead of WPA
802.1X authentication
Authentication
Local
Remote
General
RADIUS accounting:
guestwifi
RADIUS authentication realms
Use authentication realms
Use realms for accounting
HTML-based user logins
Authentication
Local
Remote
Active directory
RADIUS: guestwifi
Request RADIUS CUI
Authentication timeout: 40


General
RADIUS accounting:
guestwifi
VSC egress mapping
Traffic type
Map to
Unauthenticated:
<Default>
Authenticated:
<Default>
Intercepted:
<Default>
VPN-based authentication
Authentication
Local
Remote
General
RADIUS accounting:
guestwifi
Default user data rates
Max. transmit:
1000
kbps
Max. receive:
1000
kbps
MAC-based authentication
Authentication
Local
Remote
General
RADIUS accounting:
guestwifi
Wireless security filters
Restrict wireless traffic to this controller
Bonjour traffic filtering
Inbound profile:
<No profile defined>
Outbound profile:
<No profile defined>
Location-aware
Group name:
Called-Station-Id content:
macaddress
Wireless MAC filter
MAC Address list:
<No MAC LIST defined>
Filter action:
Allow
Block



Click on **Save**

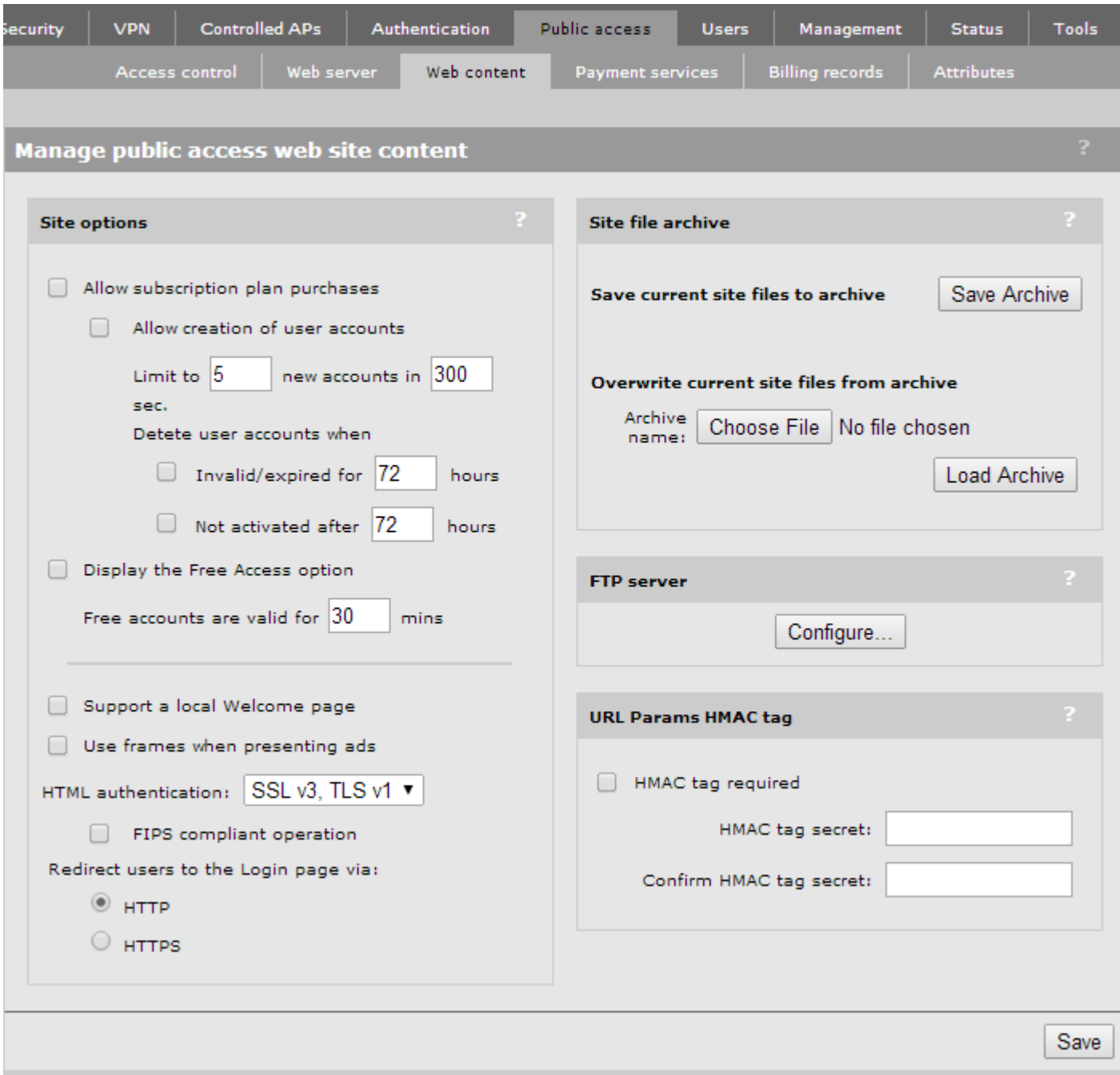
Next, click on **Public access** at the top, and ensure that "**Access Control**" is ticked.



Click on **Save**

Next, click on the "Web content" tab, and enter the following:

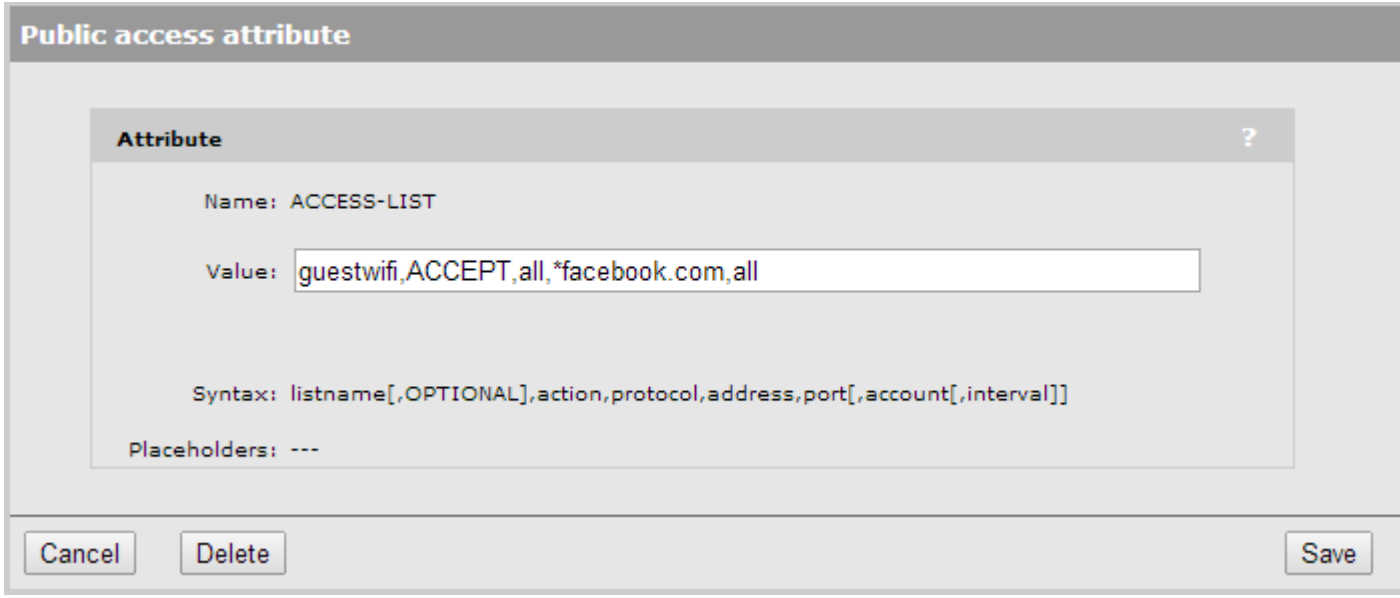
- **Support a local Welcome page**: Unticked
- Redirec**t users to the login page via**: HTTP



Click on **Save**

Next, click on **Attributes** at the top, and then under **Configure Attributes** click on **Add New Attribute**

IMPORTANT: You will need to add the below attributes one by one until you have them all listed.



- **Name:** USE-ACCESS-LIST
- **Value:** guestwifi

- **Name:** ACCESS-LIST
- **Value:** guestwifi,ACCEPT,all,**insert access_domain here*,all

- **Name:** ACCESS-LIST
- **Value:** guestwifi,ACCEPT,all,*cloudfront.net,all

- **Name:** ACCESS-LIST
- **Value:** guestwifi,ACCEPT,all,www.google.com,all

- **Name:** ACCESS-LIST
- **Value:** guestwifi,ACCEPT,all,www.google.co.uk,all

- **Name:** ACCESS-LIST
- **Value:** guestwifi,ACCEPT,all,*openweathermap.org,all

- **Name:** ACCESS-LIST
- **Value:** guestwifi,ACCEPT,all,*google-analytics.com,all

- **Name:** ACCESS-LIST
- **Value:** guestwifi,ACCEPT,all,*venuewifi.com,all

- **Name:** LOGIN-URL
- **Value:** *insert access_url here*?login_url=%l&hpapmac=%C&client_mac=%m

- **Name:** WELCOME-URL

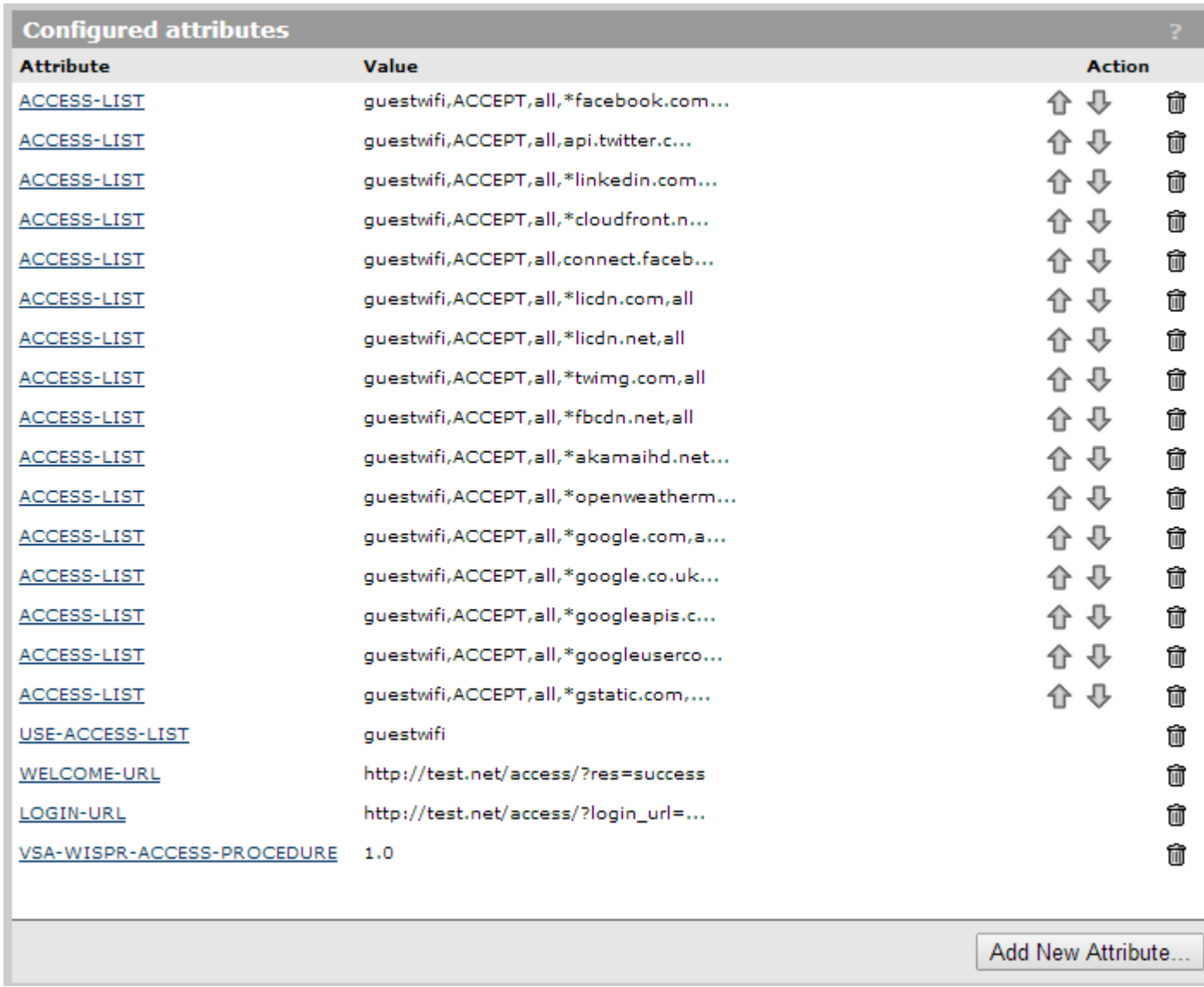
- **Value:** *insert redirect_url here*

If you wish to support social network logins, you also need to add the entries below for each network you plan to support

Facebook	Twitter
• **Name:** ACCESS-LIST • **Value:** guestwifi,ACCEPT,all,*facebook.com,all • **Name:** ACCESS-LIST • **Value:** guestwifi,ACCEPT,all,*fbcdn.net,all • **Name:** ACCESS-LIST • **Value:** guestwifi,ACCEPT,all,*akamaihd.net,all • **Name:** ACCESS-LIST • **Value:** guestwifi,ACCEPT,all,*connect.facebook.net,all	• **Name:** ACCESS-LIST • **Value:** guestwifi,ACCEPT,all,*twitter.com,all • **Name:** ACCESS-LIST • **Value:** guestwifi,ACCEPT,all,*twimg.com,all

LinkedIn	Google	Instagram
• **Name:** ACCESS-LIST • **Value:** guestwifi,ACCEPT,all,*linkedin.com,all • **Name:** ACCESS-LIST • **Value:** guestwifi,ACCEPT,all,*licdn.com,all • **Name:** ACCESS-LIST • **Value:** guestwifi,ACCEPT,all,*licdn.net,all	• **Name:** ACCESS-LIST • **Value:** guestwifi,ACCEPT,all,*googleusercontent.com,all • **Name:** ACCESS-LIST • **Value:** guestwifi,ACCEPT,all,*googleapis.com,all • **Name:** ACCESS-LIST • **Value:** guestwifi,ACCEPT,all,*accounts.google.com,all • **Name:** ACCESS-LIST • **Value:** guestwifi,ACCEPT,all,*gstatic.com,all	• **Name:** ACCESS-LIST • **Value:** guestwifi,ACCEPT,all,*instagram.com,all

You should then see a list, similar to:



To configure the Session Timeout and the Idle Timeout please use the following -

Go to Configuration > Public Access and click on Attributes at the top. Under Configure Attributes click on Add New Attribute and add the two entries:

- Name: DEFAULT-USER-IDLE-TIMEOUT
- Value: 3600

- Name: DEFAULT-USER-SESSION-TIMEOUT
- Value: 86400

You can edit the numerical values to represent the amount of seconds you want to set.

You should now be able to see the SSID broadcasting and connect to it.