

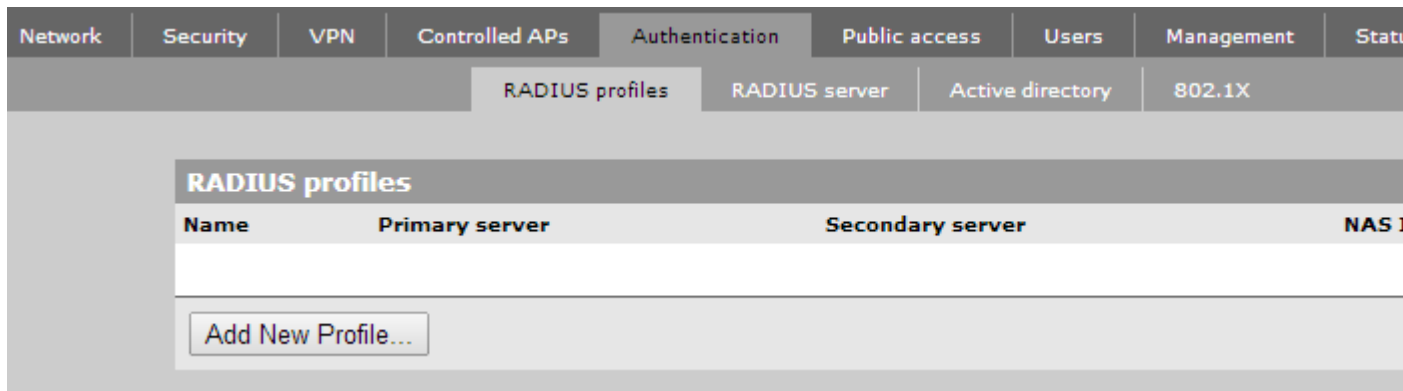
HP (MSM managed)

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**

Add/Edit RADIUS profile

Profile name ?

Profile name:

Settings ?

Authentication port: Accounting port: Retry interval: seconds Retry timeout: secondsAuthentication method: NAS ID:

- 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: 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

Global ?

Profile name:

- 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

Virtual AP ?

WLAN

Name (SSID):

DTIM count:

- Broadcast name (SSID)
- Advertise TX power
- Broadcast filtering
- Band steering

Wireless clients

Max clients per radio:

Allow traffic between: wireless clients

+ Client data tunnel

+ Quality of service

+ Allowed wireless rates

Wireless protection ?

Mode*:

Key source:

- 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:

RADIUS authentication realms ?

- Use authentication realms
- Use realms for accounting

HTML-based user logins ?

Authentication

- Local
- Remote
 - Active directory
 - RADIUS:
 - Request RADIUS CUI

Authentication timeout:

VSC egress mapping ?

Traffic type	Map to
Unauthenticated:	<Default> ▼
Authenticated:	<Default> ▼
Intercepted:	<Default> ▼

Default user data rates ?

Max. transmit: kbps
Max. receive: kbps

Wireless security filters ?

Restrict wireless traffic to this controller

Bonjour traffic filtering ?

Inbound profile: <No profile defined> ▼
Outbound profile: <No profile defined> ▼

General

RADIUS accounting:
 ▼

VPN-based authentication ?

Authentication

Local
 Remote

General

RADIUS accounting:
 ▼

MAC-based authentication ?

Authentication

Local
 Remote

General

RADIUS accounting:
 ▼

Location-aware ?

Group name:

Called-Station-Id content: ▼

Wireless MAC filter ?

MAC Address list: <No MAC LIST defined> ▼

Filter action: Allow Block

Wireless IP filter ?

Only allow traffic addressed to:

IP address: Mask:

DHCP server ?

DNS:

Start:

End:

Gateway:

Netmask:

Subnet:

Click on **Save**

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

Security | VPN | Controlled APs | Authentication | **Public access** | Users | Management | Status | Tools

Access control | Web server | Web content | Payment services | Billing records | Attributes

Access control ?

Click on **Save**

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

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

Security | VPN | Controlled APs | Authentication | **Public access** | Users | Management | Status | Tools

Access control | Web server | **Web content** | Payment services | Billing records | Attributes

Manage public access web site content ?

Site options ?

Allow subscription plan purchases

Allow creation of user accounts

Limit to new accounts in sec.

Detete user accounts when

Invalid/expired for hours

Not activated after hours

Display the Free Access option

Free accounts are valid for mins

Support a local Welcome page

Use frames when presenting ads

HTML authentication: ▼

FIPS compliant operation

Redirect users to the Login page via:

HTTP

HTTPS

Site file archive ?

Save current site files to archive

Overwrite current site files from archive

Archive name: No file chosen

FTP server ?

URL Params HMAC tag ?

HMAC tag required

HMAC tag secret:

Confirm HMAC tag secret:

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.

Public access attribute

Attribute ?

Name: ACCESS-LIST

Value:

Syntax: listname[,OPTIONAL],action,protocol,address,port[,account[,interval]]

Placeholders: ---

Cancel Delete Save

- **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&hpamac=%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
<ul style="list-style-type: none"> • Name: ACCESS-LIST • Value: guestwifi,ACCEPT,all,*facebook.com,all <ul style="list-style-type: none"> • Name: ACCESS-LIST • Value: guestwifi,ACCEPT,all,*fbcdn.net,all <ul style="list-style-type: none"> • Name: ACCESS-LIST • Value: guestwifi,ACCEPT,all,*akamaihd.net,all <ul style="list-style-type: none"> • Name: ACCESS-LIST • Value: guestwifi,ACCEPT,all,*connect.facebook.net,all 	<ul style="list-style-type: none"> • Name: ACCESS-LIST • Value: guestwifi,ACCEPT,all,*twitter.com,all <ul style="list-style-type: none"> • Name: ACCESS-LIST • Value: guestwifi,ACCEPT,all,*twimg.com,all

LinkedIn	Google	Instagram
<ul style="list-style-type: none"> • Name: ACCESS-LIST • Value: guestwifi,ACCEPT,all,*linkedin.com,all <ul style="list-style-type: none"> • Name: ACCESS-LIST • Value: guestwifi,ACCEPT,all,*licdn.com,all <ul style="list-style-type: none"> • Name: ACCESS-LIST • Value: guestwifi,ACCEPT,all,*licdn.net,all 	<ul style="list-style-type: none"> • Name: ACCESS-LIST • Value: guestwifi,ACCEPT,all,*googleusercontent.com,all <ul style="list-style-type: none"> • Name: ACCESS-LIST • Value: guestwifi,ACCEPT,all,*googleapis.com,all <ul style="list-style-type: none"> • Name: ACCESS-LIST • Value: guestwifi,ACCEPT,all,*accounts.google.com,all <ul style="list-style-type: none"> • Name: ACCESS-LIST • Value: guestwifi,ACCEPT,all,*gstatic.com,all 	<ul style="list-style-type: none"> • Name: ACCESS-LIST • Value: guestwifi,ACCEPT,all,*instagram.com,all

You should then see a list, similar to:

Configured attributes			?		
Attribute	Value	Action			
ACCESS-LIST	guestwifi,ACCEPT,all,*facebook.com...	↑	↓	🗑️	
ACCESS-LIST	guestwifi,ACCEPT,all,api.twitter.c...	↑	↓	🗑️	
ACCESS-LIST	guestwifi,ACCEPT,all,*linkedin.com...	↑	↓	🗑️	
ACCESS-LIST	guestwifi,ACCEPT,all,*cloudfront.n...	↑	↓	🗑️	
ACCESS-LIST	guestwifi,ACCEPT,all,connect.faceb...	↑	↓	🗑️	
ACCESS-LIST	guestwifi,ACCEPT,all,*licdn.com,all	↑	↓	🗑️	
ACCESS-LIST	guestwifi,ACCEPT,all,*licdn.net,all	↑	↓	🗑️	
ACCESS-LIST	guestwifi,ACCEPT,all,*twimg.com,all	↑	↓	🗑️	
ACCESS-LIST	guestwifi,ACCEPT,all,*fbcdn.net,all	↑	↓	🗑️	
ACCESS-LIST	guestwifi,ACCEPT,all,*akamaihd.net...	↑	↓	🗑️	
ACCESS-LIST	guestwifi,ACCEPT,all,*openweatherm...	↑	↓	🗑️	
ACCESS-LIST	guestwifi,ACCEPT,all,*google.com,a...	↑	↓	🗑️	
ACCESS-LIST	guestwifi,ACCEPT,all,*google.co.uk...	↑	↓	🗑️	
ACCESS-LIST	guestwifi,ACCEPT,all,*googleapis.c...	↑	↓	🗑️	
ACCESS-LIST	guestwifi,ACCEPT,all,*googleuserco...	↑	↓	🗑️	
ACCESS-LIST	guestwifi,ACCEPT,all,*gstatic.com,...	↑	↓	🗑️	
USE-ACCESS-LIST	guestwifi			🗑️	
WELCOME-URL	http://test.net/access/?res=success			🗑️	
LOGIN-URL	http://test.net/access/?login_url=...			🗑️	
VSA-WISPR-ACCESS-PROCEDURE	1.0			🗑️	

[Add New Attribute...](#)

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.