Ruckus ZoneDirector 1100

Functionality and hotspot service setting is different while using ZoneDirector compared to the use of access control in StandAlone mode separate AP. Hotspot is controlled by the controller, but user authentication is tied to a single AP, therefore, in the AP groups defined by the controller it is not possible to roam freely.

Tested on ZoneDirector 1100 and ZoneFlex 7982.

> Recommended version of firmware both device is 9.8.1.0.101 or newest.

Controller setting process

AAA servers

First of all it is necessary to set the authentication service of radius server. For each of the sites it is needed to select correct radius server. Radius servers, both primary and backup, can be set in one step. Especially it is necessary to set the authentication access (auth) and accounting access (ACC). See **Configure tab / AAA Servers / Authentication / Accounting Servers**. Here we create a new record for the authentication service with the following parameters:

Name	enter unique name for this authentication method
Type	select **RADIUS**
Auth Method	set **PAP**
Backup RADIUS	check **Enable Backup RADIUS support**
First Server	
IP Address	enter IP address of primary server due to the location
Port	leave default setting **1812**
Shared Secret	enter **socifi**
ConfirmSecret	enter **socifi**
SecondServer	
IP Address	enter IP address of secondary server due to the location
Port	leave default setting **1812**
Shared Secret	enter **socifi**
ConfirmSecret	enter **socifi**
Retry Policy	
Request Timeout	**3** seconds
Max Number of Retries	**2** times
Max Number of Consecutive Drop Packets	**1**
Reconnect Primary	**5** minutes

Select RADIUS server according to your location:

For North America:

> **RADIUS Server 1**
> **rad-us-1.socifi.com** or IP address: **54.83.207.11**

RADIUS Server 2
rad-eu-2.socifi.com or IP address: **54.246.95.103**

For South America:

RADIUS Server 1
rad-sa-1.socifi.com or IP address: **54.232.188.193**

RADIUS Server 2
rad-eu-2.socifi.com or IP address: **54.246.95.103**

For Europe:

RADIUS Server 1
rad-eu-1.socifi.com or IP address: **54.228.255.173**

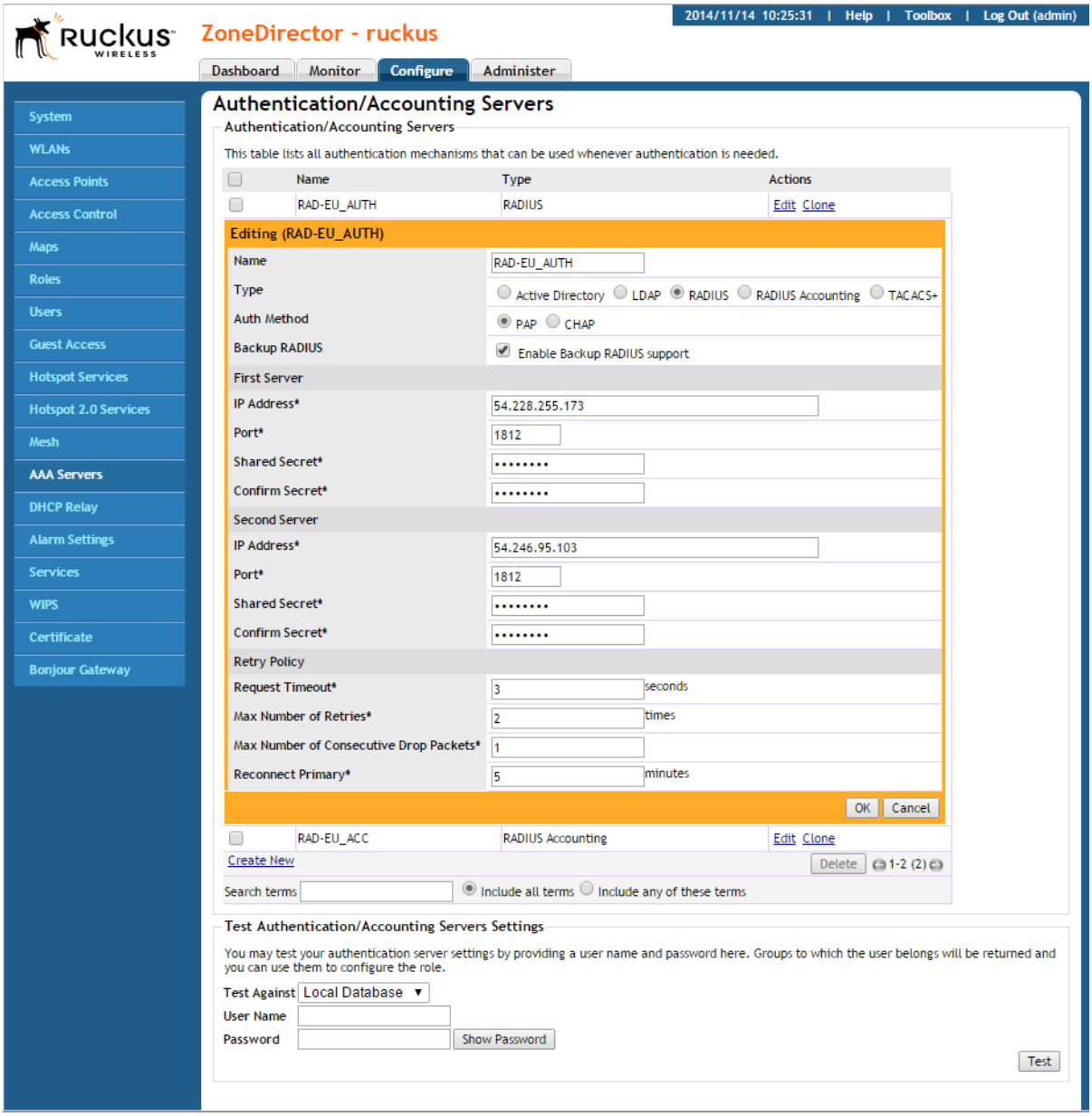
RADIUS Server 2
rad-eu-2.socifi.com or IP address: **54.246.95.103**

For Asia-Pacific

RADIUS Server 1
rad-ap-1.socifi.com or IP address: **54.251.105.182**

RADIUS Server 2
rad-eu-2.socifi.com or IP address: **54.246.95.103**

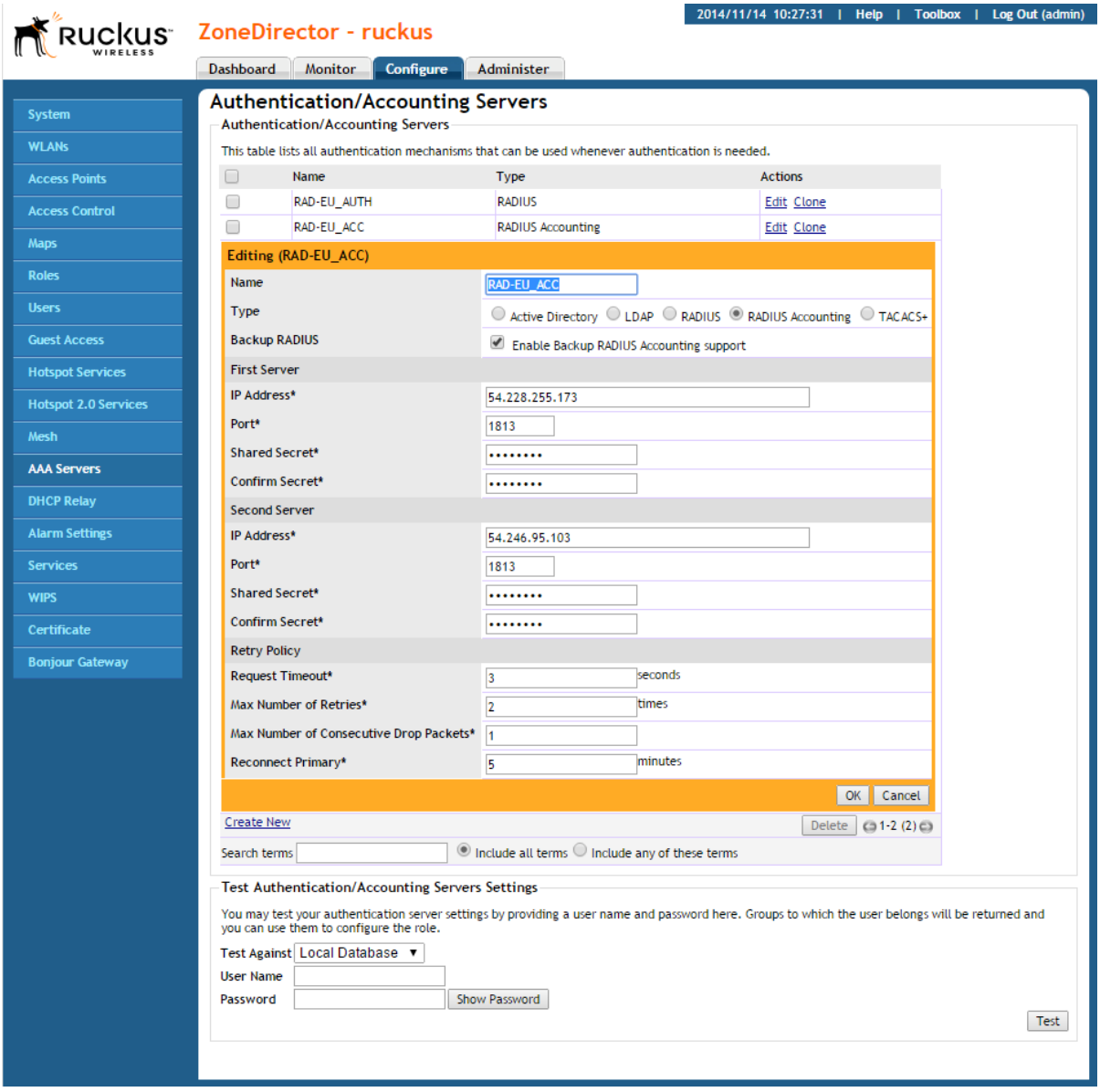
Note: please always use the server pair as suggested. The **rad-eu-2.socifi.com** should be always used as the Secondary server.



... and new record for Accounting service with following parameters:

Name	enter unique name for this accounting method
Type	select **RADIUS Accounting**
Backup RADIUS	check **Enable Backup RADIUS support**
First Server	
IP Address	enter IP address of primary server due to the location
Port	leave default setting **1813**
Shared Secret	enter **socifi**
ConfirmSecret	enter **socifi**
SecondServer	
IP Address	enter IP address of secondary server due to the location
Port	leave default setting **1813**

Shared Secret	enter **socifi**
ConfirmSecret	enter **socifi**
Retry Policy	
Request Timeout	**3** seconds
Max Number of Retries	**2** times
Max Number of Consecutive Drop Packets	**1**
Reconnect Primary	**5** minutes

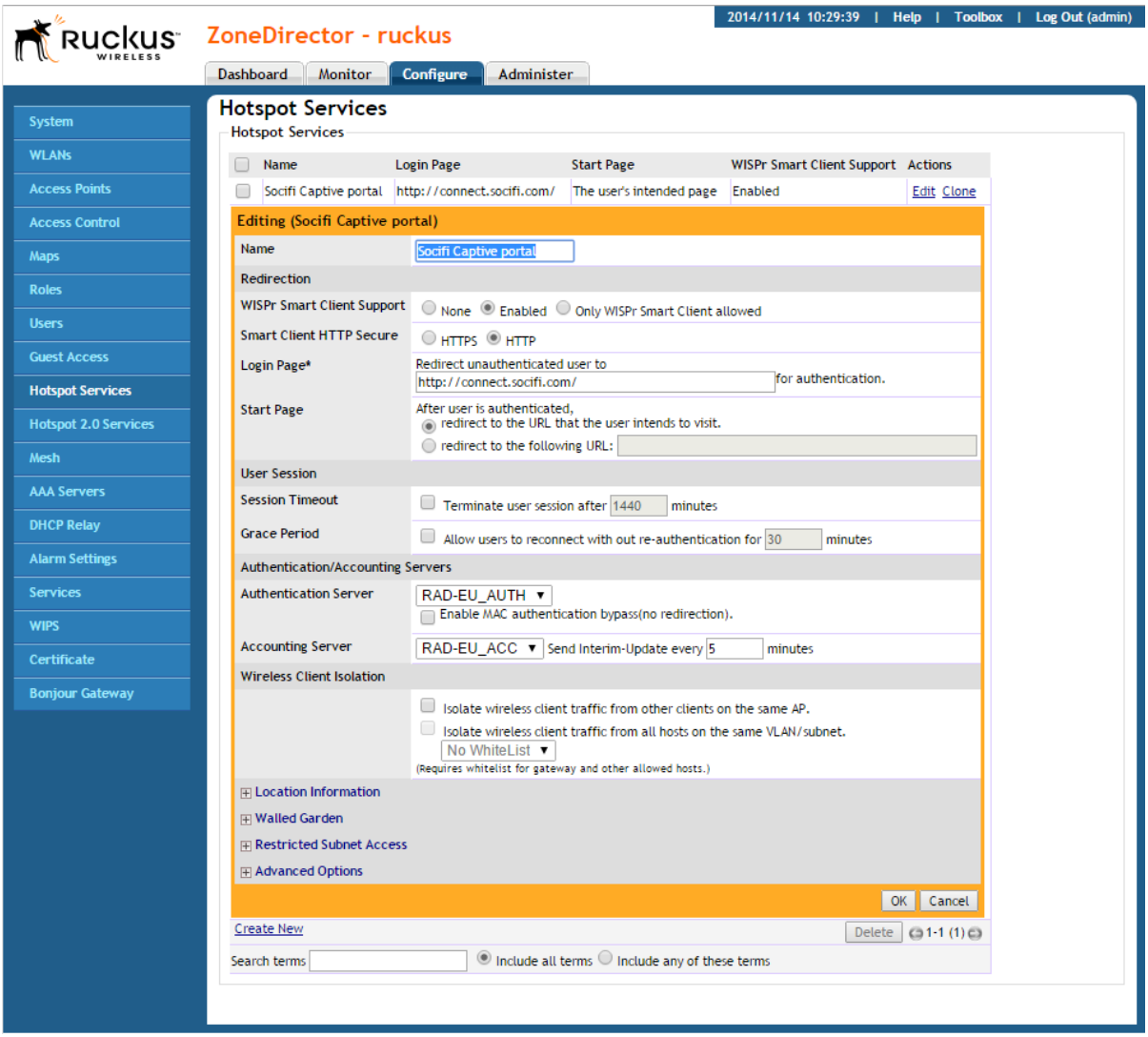


Hotspot

Hotspot service settings are set in the tab **Configure / Hotspot Services / Hotspot Services.** Here we create a new record and enter following parameters:

Name	call it e.g. **Socifi Captive portal**

Redirection	
WISPr Smart Client Support	select **Enabled**
Smart Client HTTP Secure	select **HTTP**
Login Page	enter **http://connect.socifi.com/** *(remember to use end symbol "/")*
Start Page	set **redirect to the URL that the user intends to visit**
User Session	
Session Timeout	leave **unchecked**
Grace Period	leave **unchecked**
Authentication/Accounting Servers	
Authentication Server	select our entered ***AUTH server***, selection ***Enable MAC authentication bypass (no redirection)*** leave **turned off** due to your needs
Accounting Server	select our entered ***ACC server*** and selection ***Send Interim-Update every*** enter **5** minutes
Wireless Client Isolation	both selection leave turned off due to your needs



Walled Garden

In Walled Garden setting, which is located in the hotspot settings, need to be entered all necessary domains individually and in shape *.domain.net.

Enter following **Walled garden ranges:**

```
*.socifi.com
*.bam.nr-data.net
*.js-agent.newrelic.com
*.1e100.net
*.google-analytics.com
*.facebook.com
*.akamaihd.net
*.akamai.net
*.edgecastcdn.net
twitter.com
*.twitter.com
*.twimg.com
*.fastly.net
```

Want to Allow Google+ login ?

The new **Allow login through social networks** does not include the **Google login**. The reason is that some Android based devices **are not redirected** to the Captive Portal when the user gets connected to WiFi network. In case you'd like to add it you need to do following:

1. Check if your hotspot allows DNS names in the Walled garden. Some hotspots can use IP addresses only. See: Why DNS-based Walled Garden (and not IP-based)
2. Allow Google+ login: Settings > Brand > Authentication > Allow login through social networks
3. Send request for enabling Google+ login to support@socifi.com or through SOCIFI Dashboard.
4. Add these walled garden domain into existing list:

Google+ Login DNS's

Please adopt same format your Walled garden is already using e.g. with or without the asterisk, separated by comma or space etc.

For Cisco Meraki, Ruckus, Xirrus

```
*.googleapis.com
*.googleusercontent.com
*.gstatic.com
*.accounts.youtube.com
*.apis.google.com
*.accounts.google.com
*.l.google.com
```

For Open Mesh

```
googleapis.com,googleusercontent.com,gstatic.com,accounts.youtube.com,apis.google
.com,accounts.google.com,l.google.com
```

For Mikrotik

```
/ip hotspot walled-garden
add dst-host=*.googleapis.com
add dst-host=*.googleusercontent.com
add dst-host=*.gstatic.com
add dst-host=*.accounts.youtube.com
add dst-host=*.apis.google.com
add dst-host=*.accounts.google.com
add dst-host=*.l.google.com
```

For DD-WRT

```
googleapis.com googleusercontent.com gstatic.com accounts.youtube.com
apis.google.com accounts.google.com l.google.com
```

At the end we recommend adding your local Google domain into the Walled garden list. For example google.co.uk for United Kingdom, google.com.sg for Singapore etc.

Related pages:

The Splash Page is not triggered when Android devices connect to WiFi

twitter.com (Yes, twice. Once with and once without the asterisk)

If you have **Ruckus** equipment it's necessary to add extra IP ranges to Walled Garden, see the following article

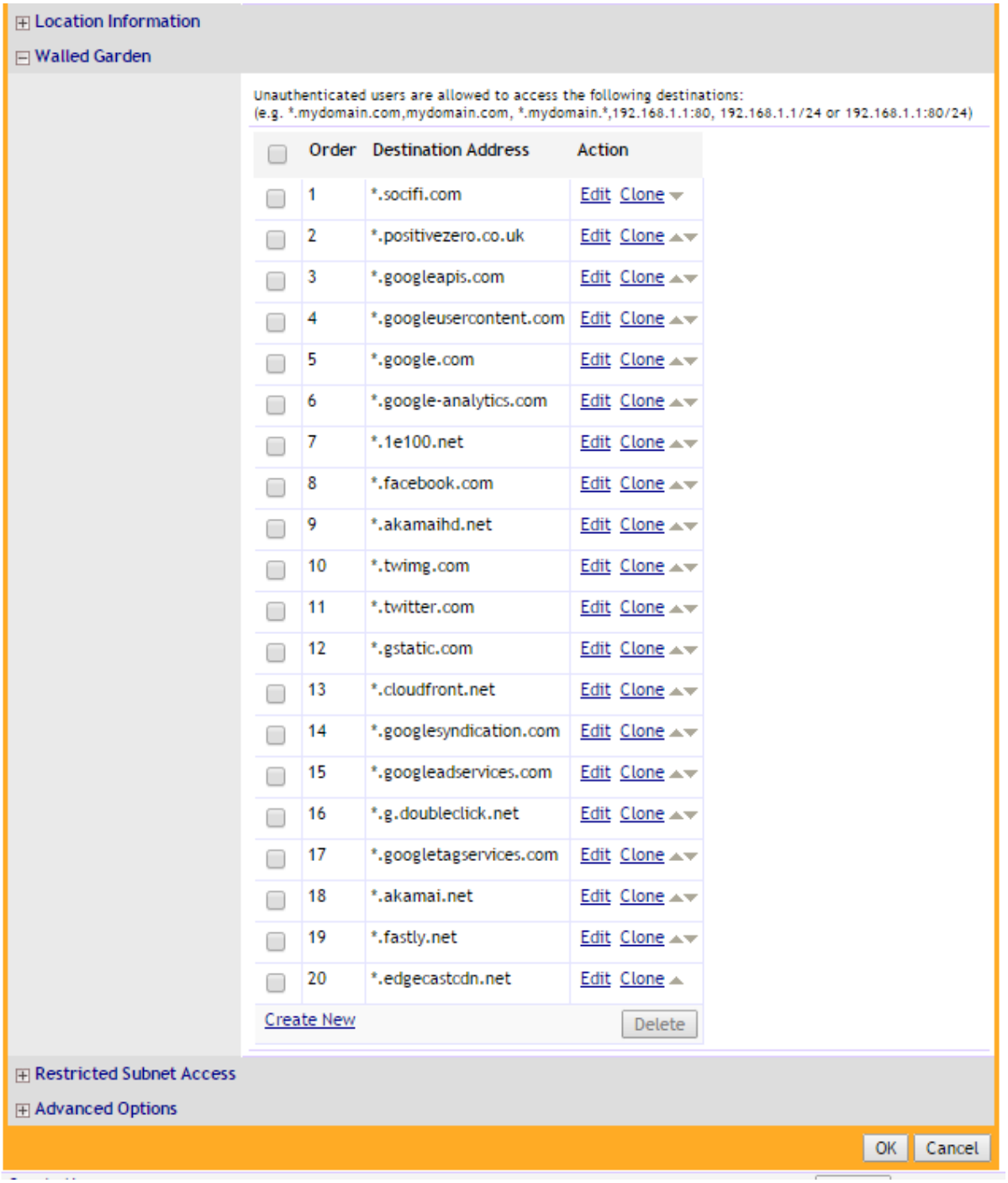
Due to Ruckus firmware behavior end-user devices might not be able to reach some (mainly CDN and cloud) domains from walled garden list. This can cause wrong rendering of the captive portal.

As a workaround you have to add all static IPs to adjust firmware behavior and be able to start monetizing your network immediately.

Work-around solution is to add the following IP ranges to the Walled Garden List:

```
54.182.0.0/16
54.192.0.0/16
54.230.0.0/16
54.239.128.0/18
54.239.192.0/19
54.240.128.0/18
204.246.164.0/22
204.246.168.0/22
204.246.174.0/23
204.246.176.0/20
205.251.192.0/19
205.251.249.0/24
205.251.250.0/23
205.251.252.0/23
205.251.254.0/24
216.137.32.0/19
```

Actual list of Amazon CloudFront (CDN) IPs is here: http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/LocationsOfEdgeServers.html (direct link to IPs list in JSON format: https://ip-ranges.amazonaws.com/ip-ranges.json)

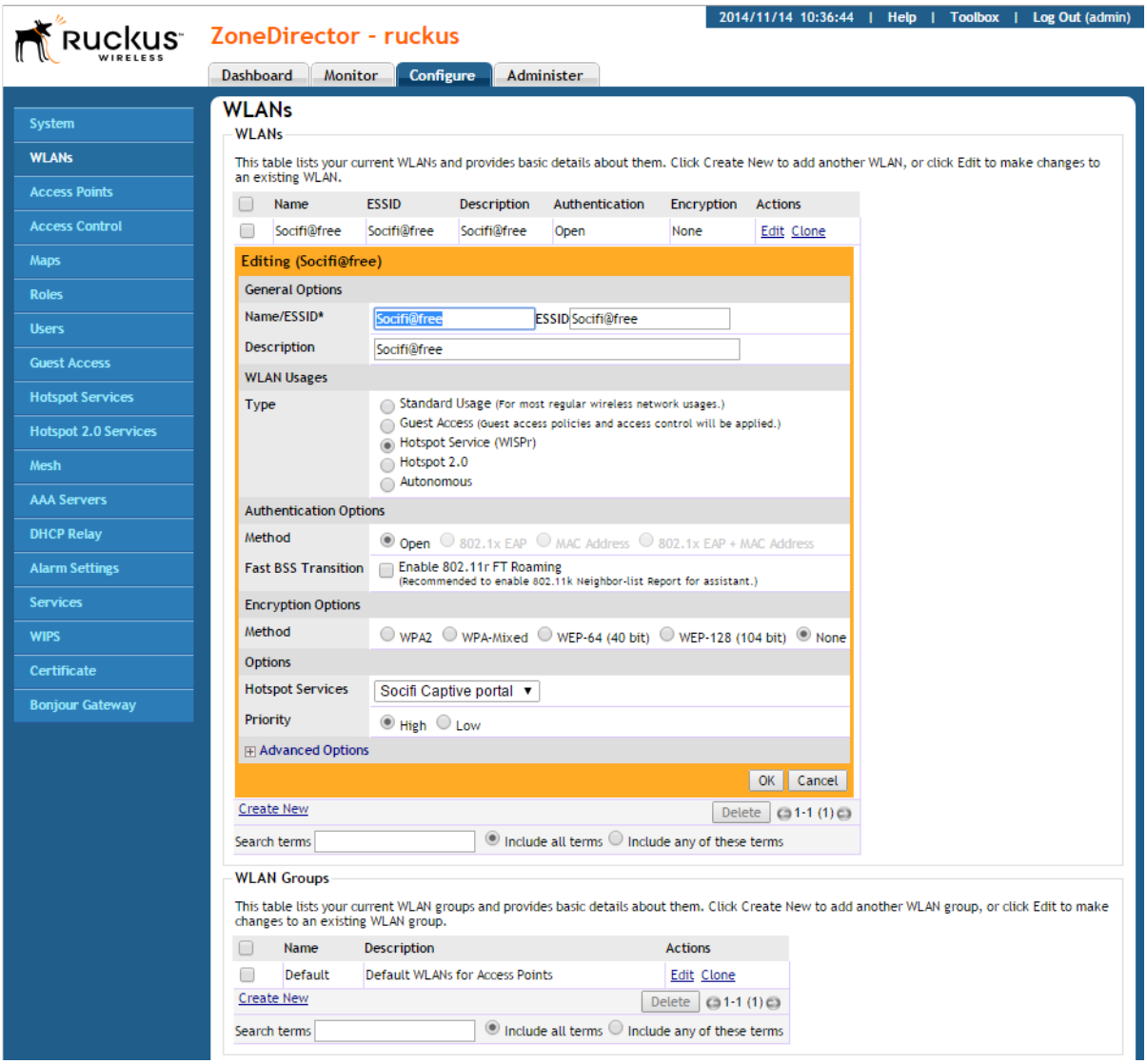


WLan

In WLan setting, located in tab **Configure / WLANs / WLans**, select chosen record and make the following adjustment of parameters:

Name	enter appropriate record name
ESSID	enter ESSID, under which the network will presented
Description	network description
WLAN Usages	
Type	select **Hotspot Service (WISPr)**

Authentication Options	
Method	leave default **Open**
Fast BSS transition	due to your needs leave **unchecked**
Encryption Options	
Method	select **None**
Options	
Hotspot Services	choose defined name of the service (see above)
Priority	High



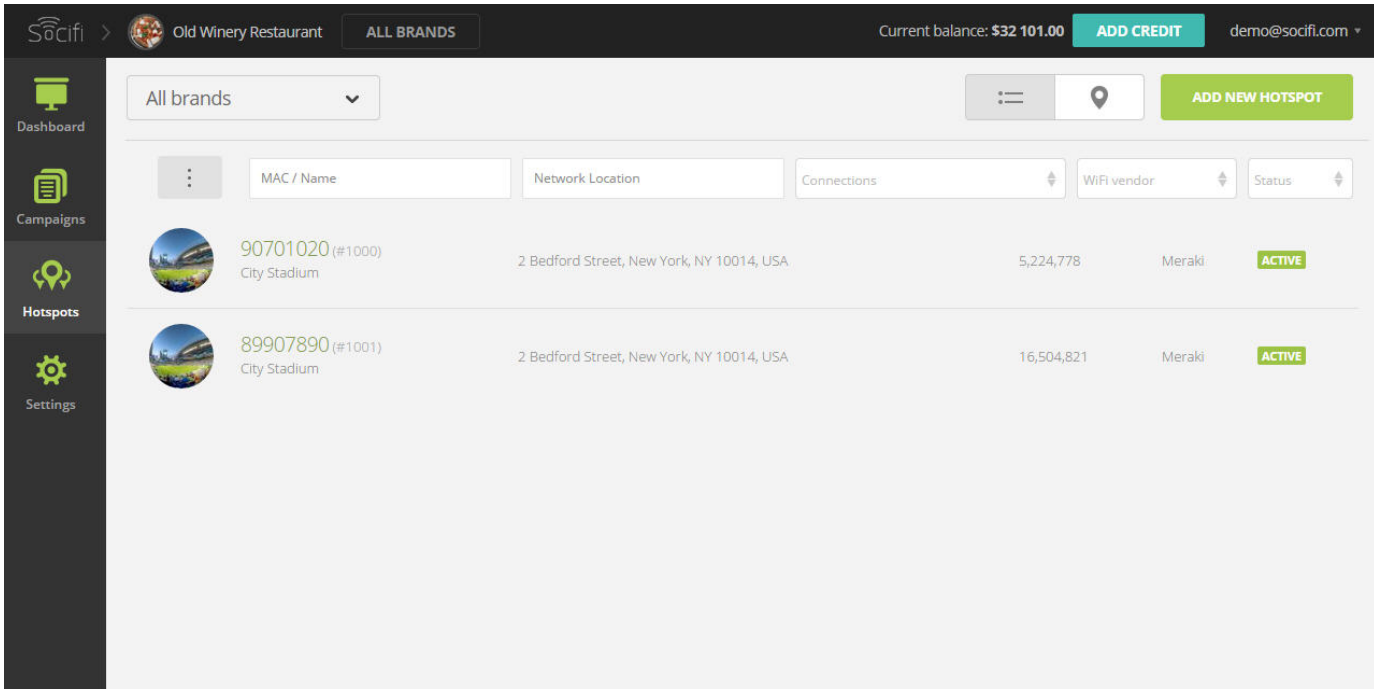
Dhcp services

For the purposes of the Hotspot service it is necessary to permit the allocation of IP addresses to clients using the DHCP server. This option can be found in the tab **Configure / System / DHCP Server**. Make the following adjustments:

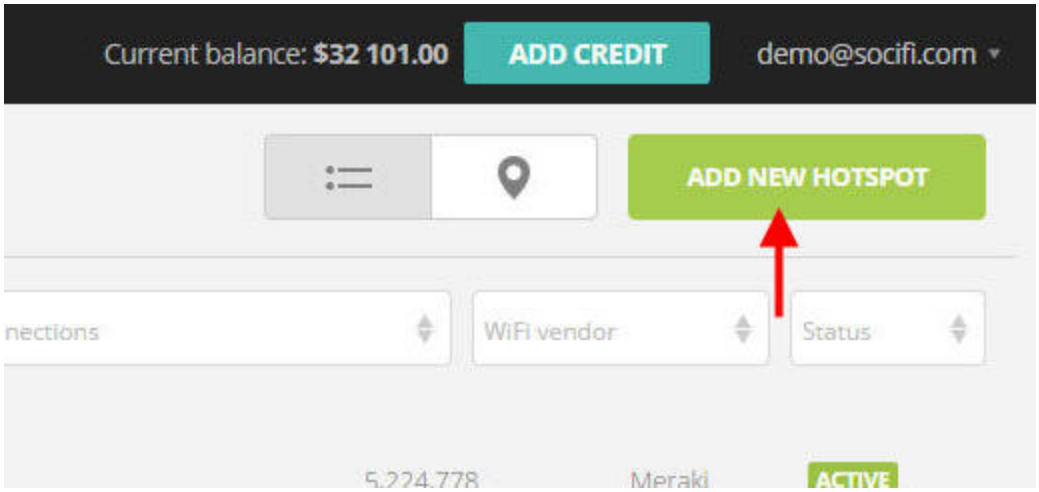
DHCP Server	
	allow service of **Enable DHCP server**
Starting IP	select due to your needs the lowest of the free addresses
Number of IPs	enter required number of addresses that must remain unallocated
Lease Time	select the lowest possible value. In our case **Six hours**
	allow **DHCP Option 43**

Add a new devices to SOCIFI Dashboard

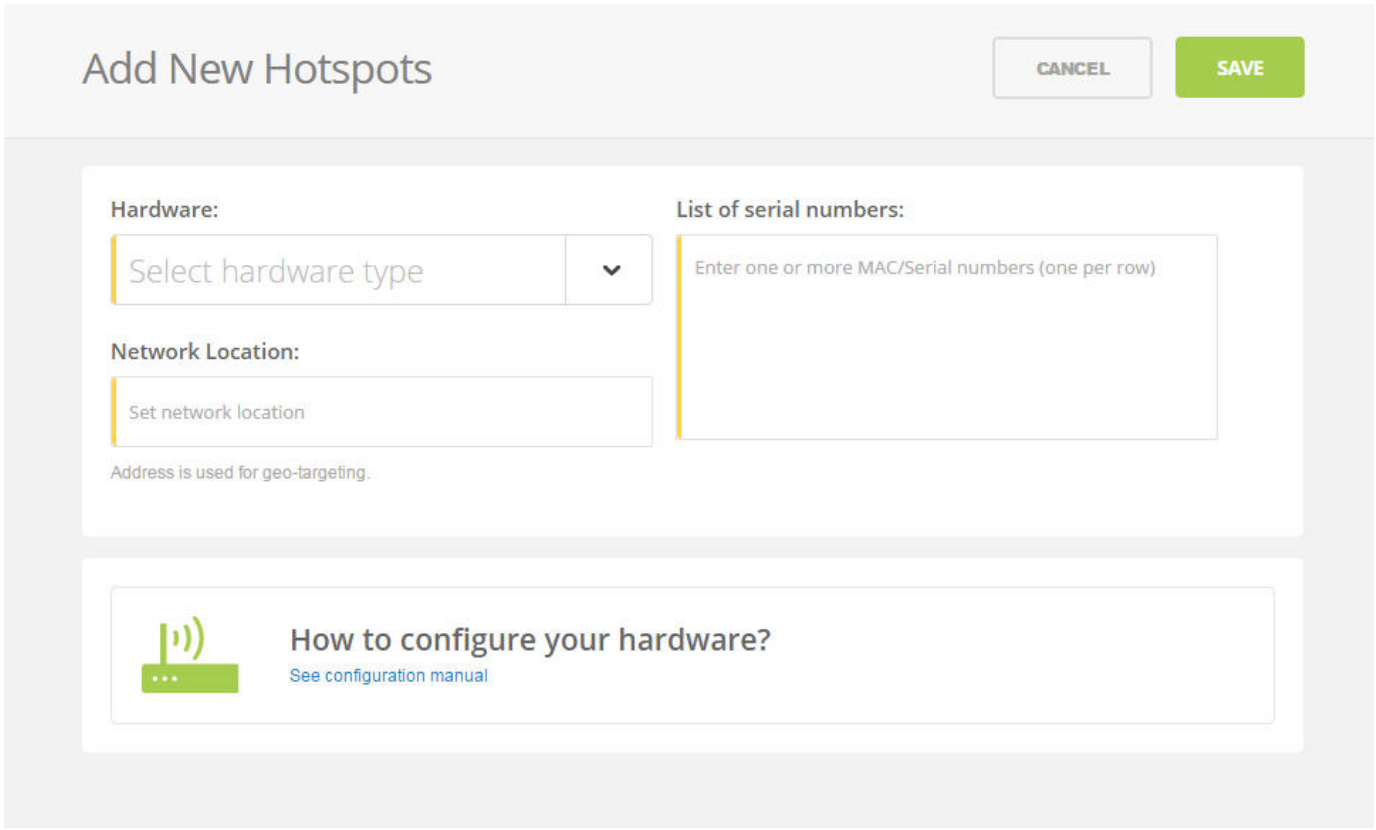
Go to **SOCIFI Dashboard**. After successful login go to "Hotspots" menu tab.



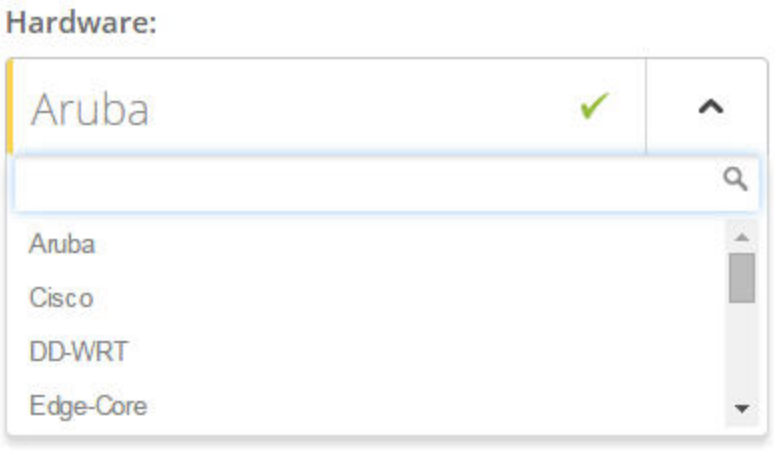
Click on the “**Add a new hotspot**” button located on the top right corner of SOCIFI Dashboard.



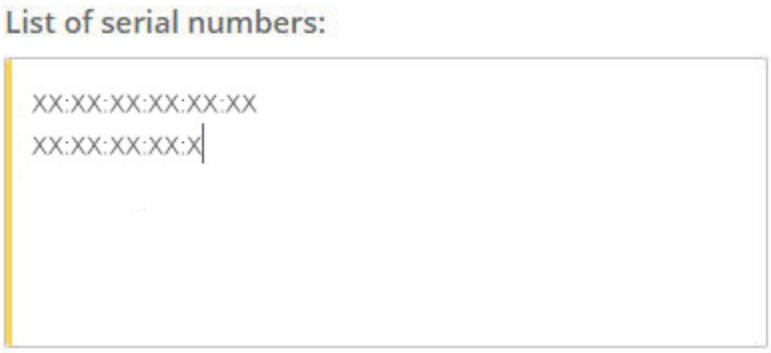
The pop-up window appears



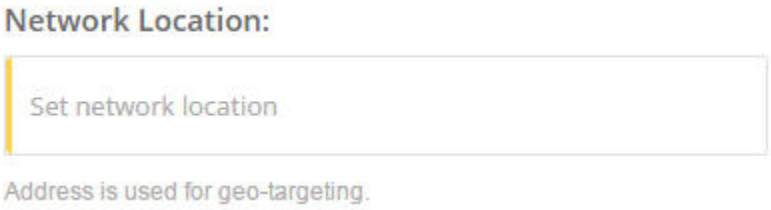
Then select hardware manufacturer.



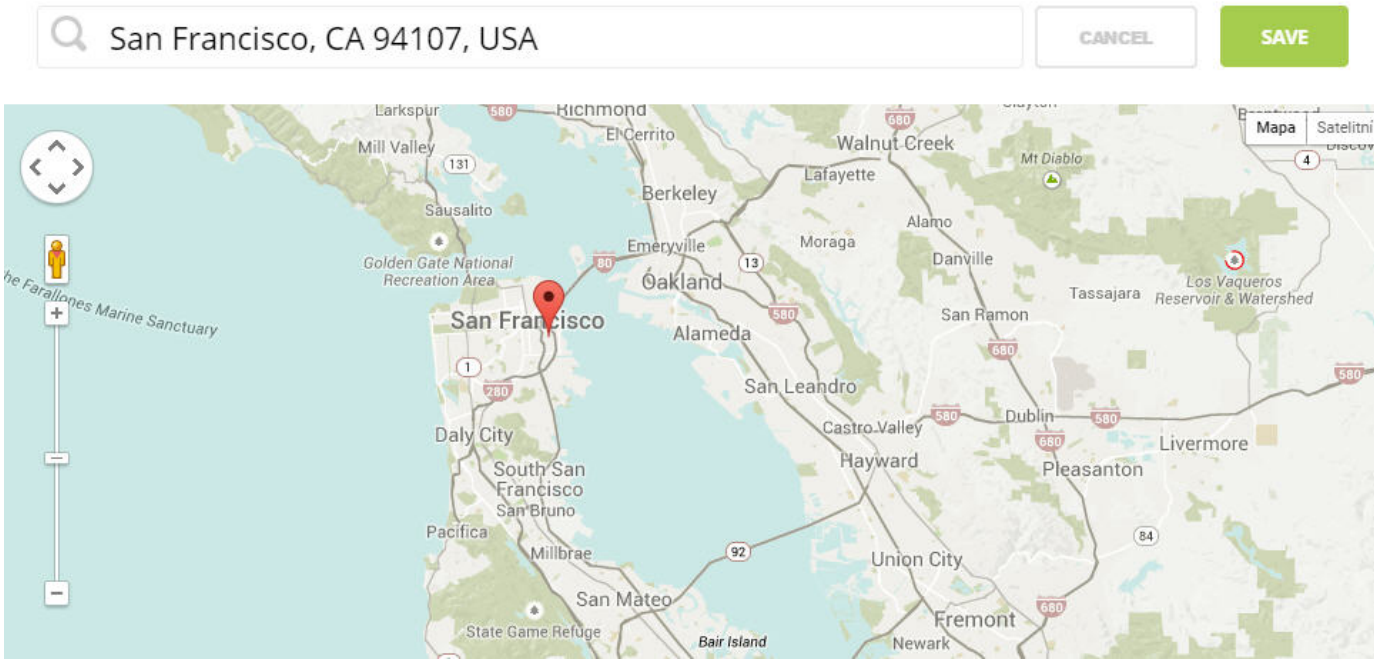
Enter **serial number or MAC address** (depending on the specific equipment manual) of your equipment. You can add multiple hotspots at once.



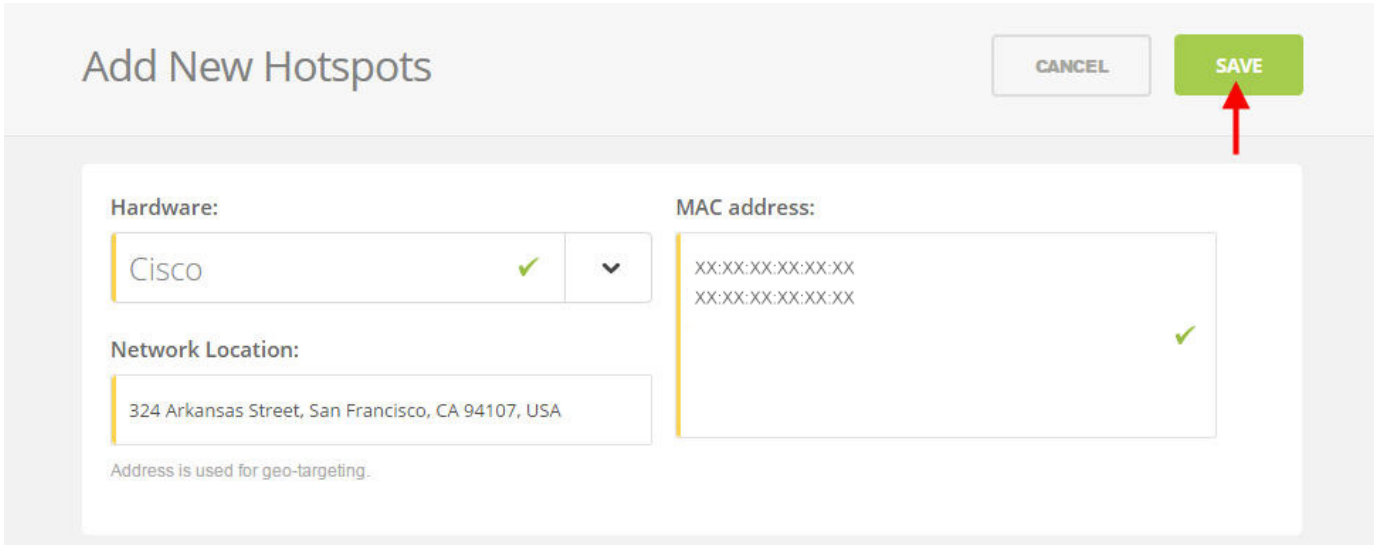
To set Network location, click on the input. The location is essential for correct ad targeting.



In the pop-up window type your place or just move the marker on the map and click on Save button to confirm the selection. This address is used for ad GEO targeting.



Finally click on **Save button**.



New added hotspot is marked as Recently added. After the first user connects to the hotspot via SOCIFI, status get automatically changed into Active in an hour.

Do you need help with configuration of your hardware? Good news, we have configuration guides for all supported devices.