

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.

2014/11/14 10:25:31 | Help | Toolbox | Log Out (admin)

ruckus WIRELESS ZoneDirector - ruckus

Dashboard | Monitor | **Configure** | Administer

System
WLANs
Access Points
Access Control
Maps
Roles
Users
Guest Access
Hotspot Services
Hotspot 2.0 Services
Mesh
AAA Servers
DHCP Relay
Alarm Settings
Services
WIPS
Certificate
Bonjour Gateway

Authentication/Accounting Servers

Authentication/Accounting Servers

This table lists all authentication mechanisms that can be used whenever authentication is needed.

<input type="checkbox"/>	Name	Type	Actions
<input type="checkbox"/>	RAD-EU_AUTH	RADIUS	Edit Clone

Editing (RAD-EU_AUTH)

Name:

Type: Active Directory LDAP RADIUS RADIUS Accounting TACACS+

Auth Method: PAP CHAP

Backup RADIUS: Enable Backup RADIUS support

First Server

IP Address*:

Port*:

Shared Secret*:

Confirm Secret*:

Second Server

IP Address*:

Port*:

Shared Secret*:

Confirm Secret*:

Retry Policy

Request Timeout*: seconds

Max Number of Retries*: times

Max Number of Consecutive Drop Packets*:

Reconnect Primary*: minutes

<input type="checkbox"/>	Name	Type	Actions
<input type="checkbox"/>	RAD-EU_ACC	RADIUS Accounting	Edit Clone

[Create New](#) 1-2 (2)

Search terms: Include all terms Include any of these terms

Test Authentication/Accounting Servers Settings

You may test your authentication server settings by providing a user name and password here. Groups to which the user belongs will be returned and you can use them to configure the role.

Test Against:

User Name:

Password:

... 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


ZoneDirector - ruckus
2014/11/14 10:27:31 | [Help](#) | [Toolbox](#) | [Log Out \(admin\)](#)

Dashboard

Monitor

Configure

Administer

- System
- WLANS
- Access Points
- Access Control
- Maps
- Roles
- Users
- Guest Access
- Hotspot Services
- Hotspot 2.0 Services
- Mesh
- AAA Servers
- DHCP Relay
- Alarm Settings
- Services
- WIPS
- Certificate
- Bonjour Gateway

Authentication/Accounting Servers

This table lists all authentication mechanisms that can be used whenever authentication is needed.

Name	Type	Actions
<input type="checkbox"/> RAD-EU_AUTH	RADIUS	Edit Clone
<input type="checkbox"/> RAD-EU_ACC	RADIUS Accounting	Edit Clone

Editing (RAD-EU_ACC)

Name:

Type: Active Directory LDAP RADIUS RADIUS Accounting TACACS+

Backup RADIUS: Enable Backup RADIUS Accounting support

First Server

IP Address*:

Port*:

Shared Secret*:

Confirm Secret*:

Second Server

IP Address*:

Port*:

Shared Secret*:

Confirm Secret*:

Retry Policy

Request Timeout*: seconds

Max Number of Retries*: times

Max Number of Consecutive Drop Packets*:

Reconnect Primary*: minutes

[Create New](#) 1-2 (2)

Search terms: Include all terms Include any of these terms

Test Authentication/Accounting Servers Settings

You may test your authentication server settings by providing a user name and password here. Groups to which the user belongs will be returned and you can use them to configure the role.

Test Against: ▼

User Name:

Password:

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


ZoneDirector - ruckus
2014/11/14 10:29:39 | [Help](#) | [Toolbox](#) | [Log Out \(admin\)](#)

Dashboard

Monitor

Configure

Administer

- System
- WLANS
- Access Points
- Access Control
- Maps
- Roles
- Users
- Guest Access
- Hotspot Services
- Hotspot 2.0 Services
- Mesh
- AAA Servers
- DHCP Relay
- Alarm Settings
- Services
- WIPS
- Certificate
- Bonjour Gateway

Hotspot Services

Hotspot Services

Name	Login Page	Start Page	WISPr Smart Client Support	Actions
<input type="checkbox"/>	Socifi Captive portal	http://connect.socifi.com/	The user's intended page	Enabled Edit Clone

Editing (Socifi Captive portal)

Name:

Redirection

WISPr Smart Client Support: None Enabled Only WISPr Smart Client allowed

Smart Client HTTP Secure: HTTPS HTTP

Login Page*: Redirect unauthenticated user to for authentication.

Start Page: After user is authenticated,
 redirect to the URL that the user intends to visit.
 redirect to the following URL:

User Session

Session Timeout: Terminate user session after minutes

Grace Period: Allow users to reconnect with out re-authentication for minutes

Authentication/Accounting Servers

Authentication Server:
 Enable MAC authentication bypass(no redirection).

Accounting Server: Send Interim-Update every minutes

Wireless Client Isolation

Isolate wireless client traffic from other clients on the same AP.
 Isolate wireless client traffic from all hosts on the same VLAN/subnet.

(Requires whitelist for gateway and other allowed hosts.)

[Location Information](#)

Walled Garden

Restricted Subnet Access

Advanced Options

[Create New](#) 1-1 (1)

Search terms: Include all terms Include any of these terms

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
*.le100.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>)

Location Information

Walled Garden

Unauthenticated users are allowed to access the following destinations:
(e.g. *.mydomain.com,mydomain.com, *.mydomain.*,192.168.1.1:80, 192.168.1.1/24 or 192.168.1.1:80/24)

<input type="checkbox"/>	Order	Destination Address	Action
<input type="checkbox"/>	1	*.socifi.com	Edit Clone ▼
<input type="checkbox"/>	2	*.positivezero.co.uk	Edit Clone ▲▼
<input type="checkbox"/>	3	*.googleapis.com	Edit Clone ▲▼
<input type="checkbox"/>	4	*.googleusercontent.com	Edit Clone ▲▼
<input type="checkbox"/>	5	*.google.com	Edit Clone ▲▼
<input type="checkbox"/>	6	*.google-analytics.com	Edit Clone ▲▼
<input type="checkbox"/>	7	*.1e100.net	Edit Clone ▲▼
<input type="checkbox"/>	8	*.facebook.com	Edit Clone ▲▼
<input type="checkbox"/>	9	*.akamaihd.net	Edit Clone ▲▼
<input type="checkbox"/>	10	*.twimg.com	Edit Clone ▲▼
<input type="checkbox"/>	11	*.twitter.com	Edit Clone ▲▼
<input type="checkbox"/>	12	*.gstatic.com	Edit Clone ▲▼
<input type="checkbox"/>	13	*.cloudfront.net	Edit Clone ▲▼
<input type="checkbox"/>	14	*.googlesyndication.com	Edit Clone ▲▼
<input type="checkbox"/>	15	*.googleadservices.com	Edit Clone ▲▼
<input type="checkbox"/>	16	*.g.doubleclick.net	Edit Clone ▲▼
<input type="checkbox"/>	17	*.googletagmanager.com	Edit Clone ▲▼
<input type="checkbox"/>	18	*.akamai.net	Edit Clone ▲▼
<input type="checkbox"/>	19	*.fastly.net	Edit Clone ▲▼
<input type="checkbox"/>	20	*.edgecastcdn.net	Edit Clone ▲

[Create New](#) [Delete](#)

Restricted Subnet Access

Advanced Options

OK Cancel

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


ZoneDirector - ruckus
2014/11/14 10:36:44 | Help | Toolbox | Log Out (admin)

Dashboard

Monitor

Configure

Administer

System

WLANs

Access Points

Access Control

Maps

Roles

Users

Guest Access

Hotspot Services

Hotspot 2.0 Services

Mesh

AAA Servers

DHCP Relay

Alarm Settings

Services

WIPS

Certificate

Bonjour Gateway

WLANs

This table lists your current WLANs and provides basic details about them. Click Create New to add another WLAN, or click Edit to make changes to an existing WLAN.

<input type="checkbox"/>	Name	ESSID	Description	Authentication	Encryption	Actions
<input type="checkbox"/>	Socifi@free	Socifi@free	Socifi@free	Open	None	Edit Clone

Editing (Socifi@free)

General Options

Name/ESSID* ESSID

Description

WLAN Usages

Type

- Standard Usage (For most regular wireless network usages.)
- Guest Access (Guest access policies and access control will be applied.)
- Hotspot Service (WISPr)
- Hotspot 2.0
- Autonomous

Authentication Options

Method Open 802.1x EAP MAC Address 802.1x EAP + MAC Address

Fast BSS Transition Enable 802.11r FT Roaming (Recommended to enable 802.11k Neighbor-list Report for assistant.)

Encryption Options

Method WPA2 WPA-Mixed WEP-64 (40 bit) WEP-128 (104 bit) None

Options

Hotspot Services

Priority High Low

Advanced Options

[Create New](#) 1-1 (1)

Search terms Include all terms Include any of these terms

WLAN Groups

This table lists your current WLAN groups and provides basic details about them. Click Create New to add another WLAN group, or click Edit to make changes to an existing WLAN group.

<input type="checkbox"/>	Name	Description	Actions
<input type="checkbox"/>	Default	Default WLANs for Access Points	Edit Clone

[Create New](#) 1-1 (1)

Search terms Include all terms Include any of these terms

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

DHCP Server

If a DHCP server does not exist on your network, you can enable this function to provide DHCP service to clients.

Enable DHCP server

Starting IP*

Number of IPs*

Lease Time

DHCP Option 43 (Layer 3 discovery protocol for AP to find ZoneDirector)

To view all IP addresses that have been assigned by the DHCP server, [click here](#)

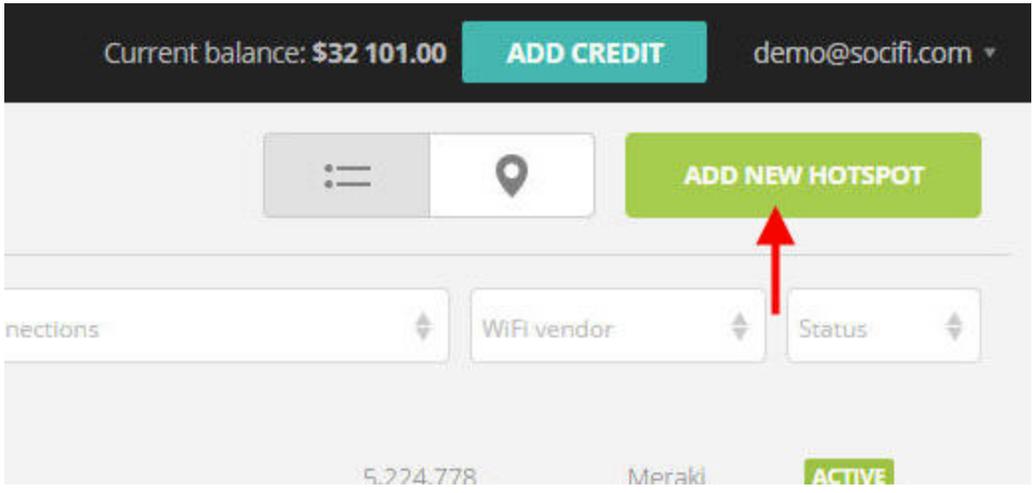
Add a new devices to SOCIFI Dashboard

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

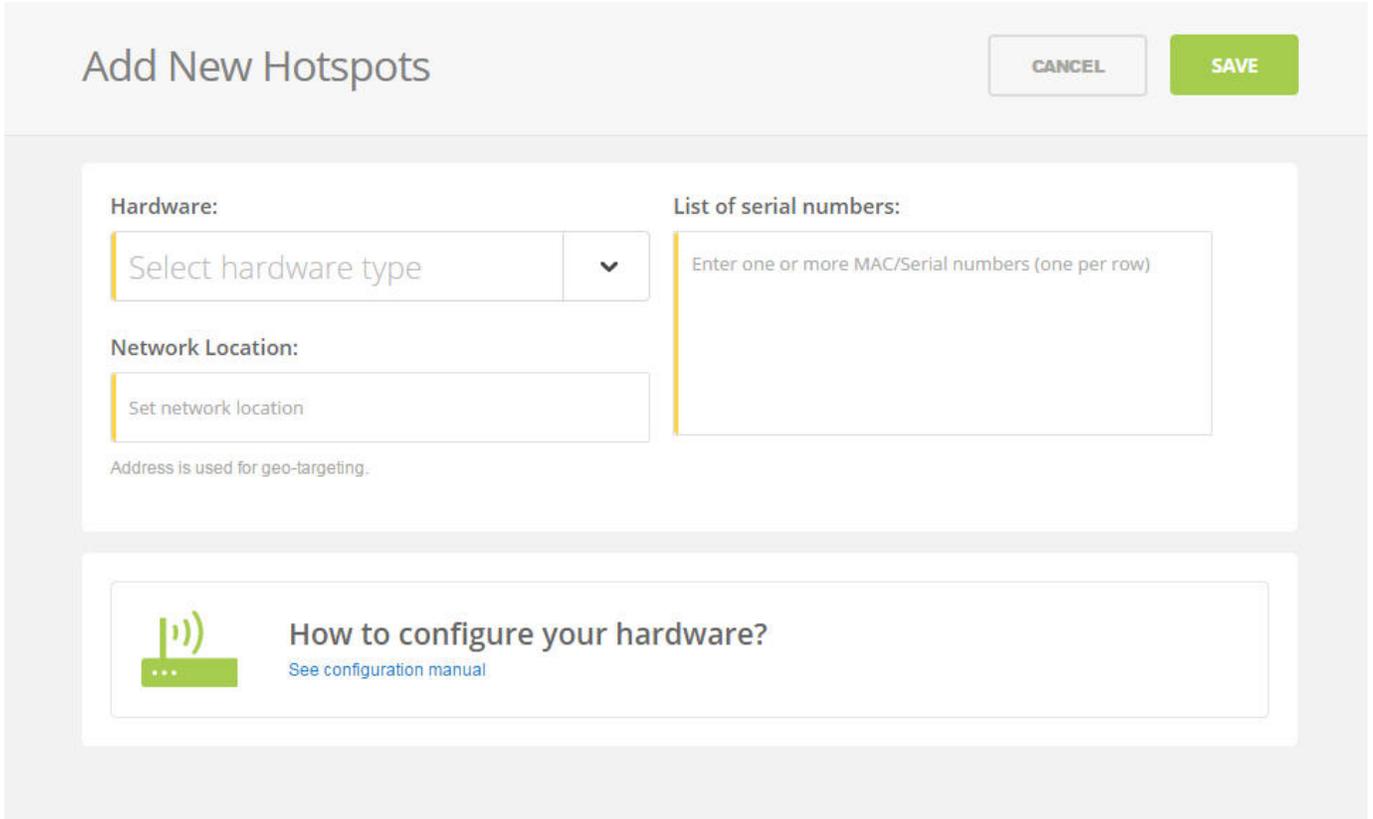
The screenshot shows the SOCIFI Dashboard interface. At the top, there is a navigation bar with the SOCIFI logo, a user profile for 'Old Winery Restaurant', and a current balance of '\$32 101.00'. A green 'ADD CREDIT' button and the email 'demo@socifi.com' are also visible. On the left, a sidebar contains navigation icons for 'Dashboard', 'Campaigns', 'Hotspots', and 'Settings'. The main content area displays a table of hotspots under the 'All brands' filter. The table has columns for 'MAC / Name', 'Network Location', 'Connections', 'WiFi vendor', and 'Status'. Two hotspots are listed, both with a status of 'ACTIVE'.

MAC / Name	Network Location	Connections	WiFi vendor	Status
90701020 (#1000) City Stadium	2 Bedford Street, New York, NY 10014, USA	5,224,778	Meraki	ACTIVE
89907890 (#1001) City Stadium	2 Bedford Street, New York, NY 10014, USA	16,504,821	Meraki	ACTIVE

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.

Hardware:

 ✓ ^
 🔍
Aruba
Cisco
DD-WRT
Edge-Core

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

List of serial numbers:

```
XX:XX:XX:XX:XX:XX  
XX:XX:XX:XX:XX:XX
```

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

Network Location:

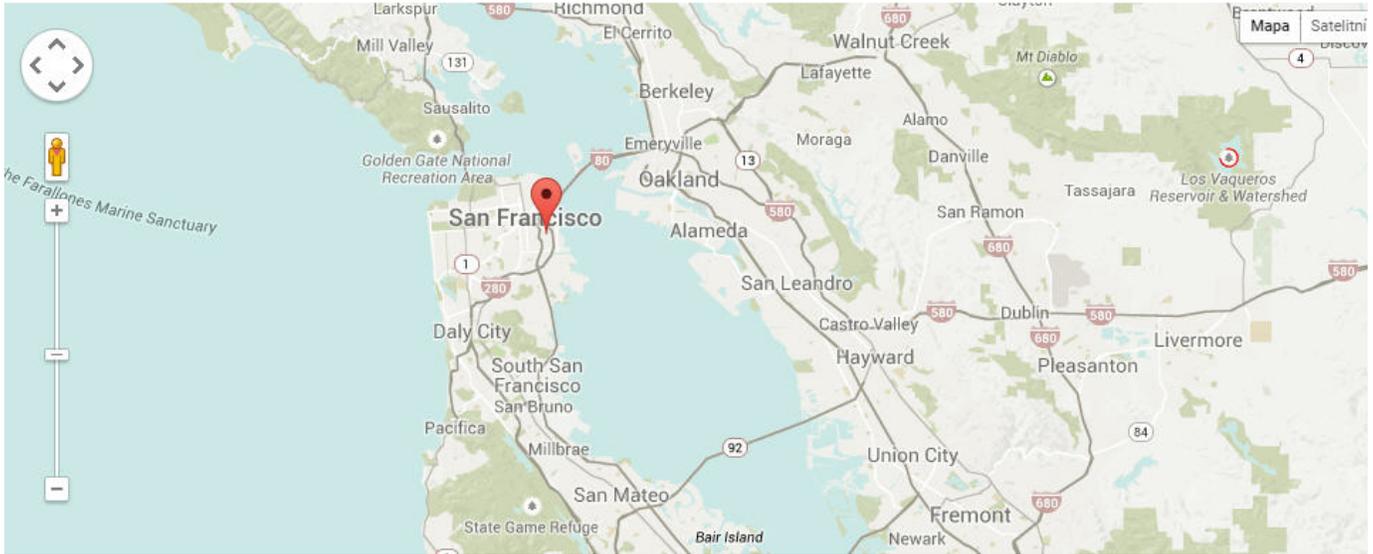
Address is used for geo-targeting.

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.

San Francisco, CA 94107, USA

CANCEL

SAVE



Finally click on **Save button**.

Add New Hotspots

CANCEL

SAVE

Hardware:

Cisco



MAC address:

XX:XX:XX:XX:XX:XX
XX:XX:XX:XX:XX:XX



Network Location:

324 Arkansas Street, San Francisco, CA 94107, USA

Address is used for geo-targeting.

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.



90701020 (#1000)
City Stadium

2 Bedford Street, New York, NY 10014,
USA

5,224,778

Meraki



ACTIVE

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