

# **Cloudi-Fi integration with Cisco Meraki**

*MX and MR*

## Table of Contents

<b>1. Solution overview</b>	<b>3</b>
<b>2. Importing Cisco Meraki networks into Cloudi-Fi</b>	<b>5</b>
<b>2.1. Enable API access to Meraki portal</b>	<b>5</b>
<b>2.2. Generate the API Key</b>	<b>6</b>
<b>2.3. Import the API key in the Cloudi-Fi portal</b>	<b>6</b>
<b>2.4. Run the wizard to configure your Cloudi-Fi locations</b>	<b>8</b>
<b>2.5. Verify Cloudi-Fi locations creation</b>	<b>10</b>
<b>2.6. Create the Guest SSID (optional / when Manual SSID configuration is selected)</b>	<b>12</b>
<b>2.7. Configure the Splash page in Meraki administration</b>	<b>14</b>
<b>2.8. Prevent Guest users to access your internal networks</b>	<b>16</b>

## 1. Solution overview

This article describes how the Cloudi-Fi solution integrates into Cisco Meraki MX and MR solutions. The joint solution provides a secure, compliant, and customizable Guest Wi-Fi service and enhances Cisco Meraki offer with multiple advantages:

- Compliance with local regulations (Data privacy and Internet provider regulations)
- Enhanced security: Guests profiling allowing seamless integration with profile-based security policies and total visibility of all guest's traffic
- Personalized guests onboarding and optimized user experience with fully customizable captive portals and personalized digital user journey
- Added-value digital services to hotspots and corporate environments

More information here

[Cisco Meraki Marketplace](#)

[Cloudi-Fi and Cisco Meraki demo video](#)

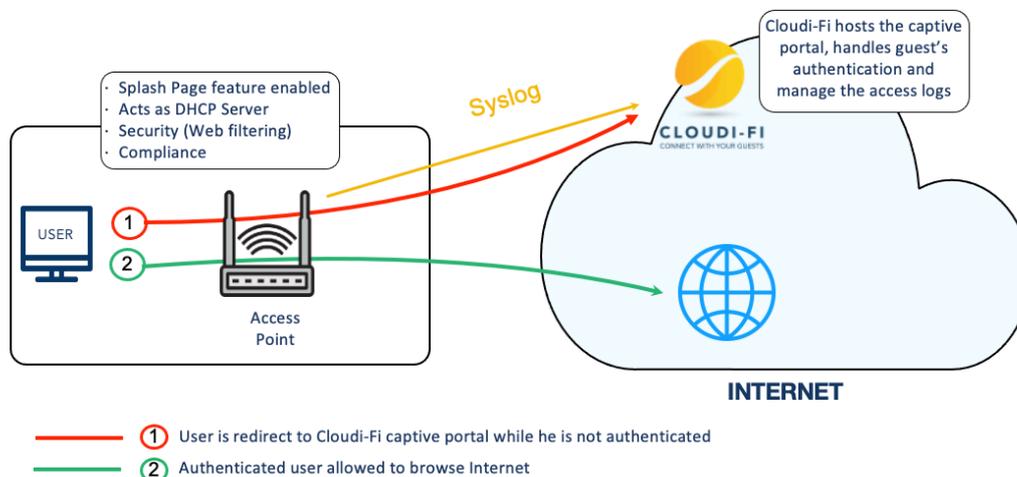
[Cloudi-Fi and Cisco Meraki Deployment Guide](#)

### Solution tested

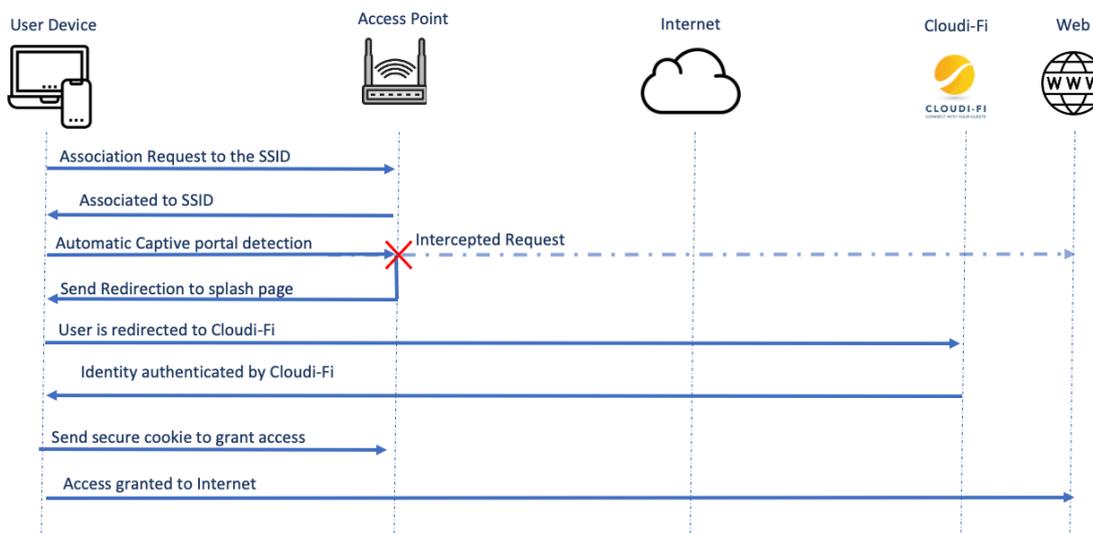
- MR33 with version MR25.13 onward
- MX67W with version MX15.4 onward

The above diagram shows the Cloudi-Fi integration.

- The Guest connects to Internet through an open SSID configured on the Cisco Meraki equipment
- A splash page or captive portal pops up immediately on its device and is directly redirected to Cloudi-Fi portal while he/she is not authenticated.
- Cloudi-Fi hosts the captive portal, handles guest’s authentication, and manages the access logs.
- The guest is invited to authenticate with his/her preferred method.
- Once authenticated, the user is allowed to browse Internet.



**Figure - Configuration Overview**



**Figure - Authentication workflow**

## 2. Importing Cisco Meraki networks into Cloudi-Fi

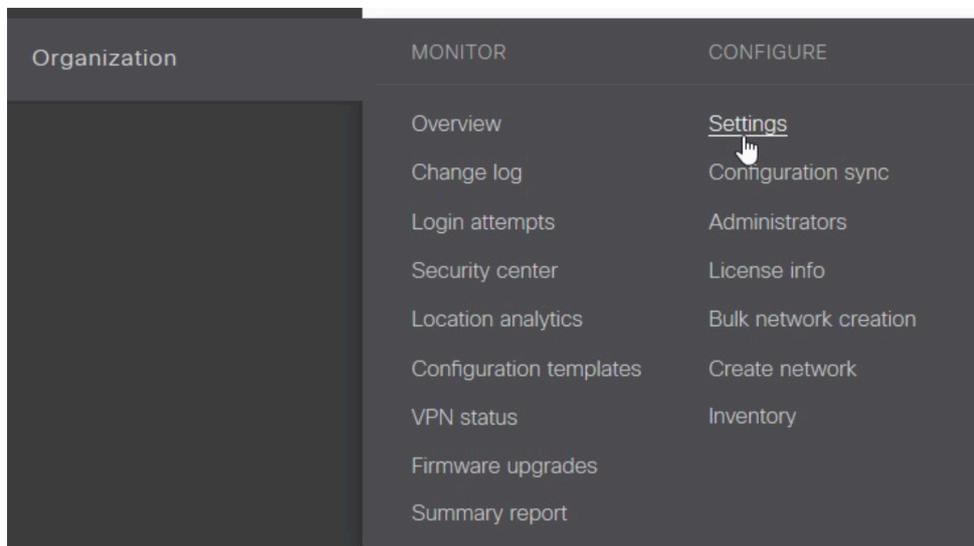
The goal of this is to enable splash page directly in your Meraki MR/MX.

Summary:

- Meraki API enablement
- Use Cloudi-Fi wizard to import any existing Meraki network
- Configure Meraki SSID and Splash page manually (optional)

### 2.1. Enable API access to Meraki portal

Go to Meraki administration page, go to Organization > Settings Menu,



Tick the box « Enable access to the Cisco Meraki Dashboard API and save changes.

---

#### Dashboard API access

API Access ⓘ

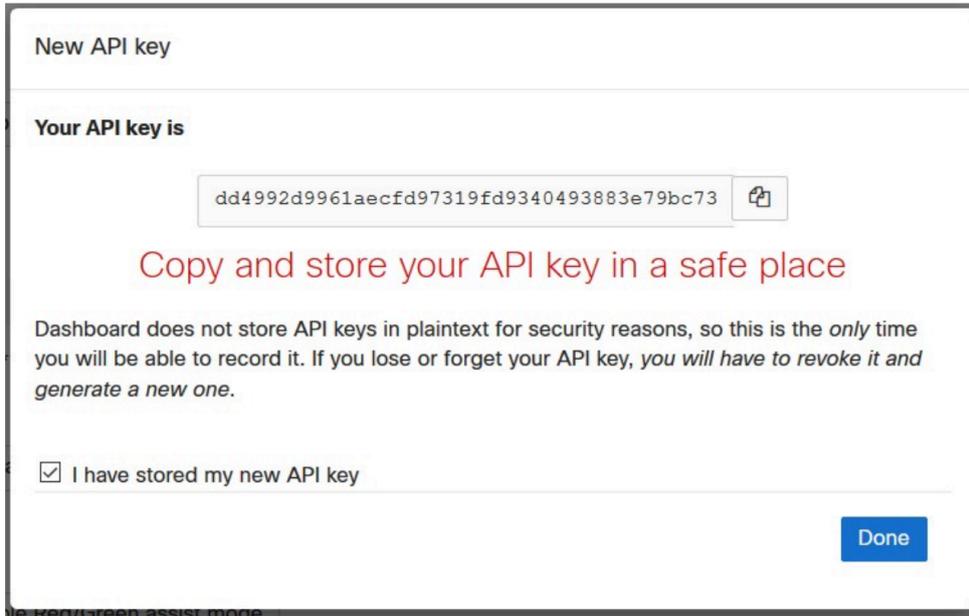
Enable access to the Cisco Meraki Dashboard API

After enabling the API here, go to your [profile](#) to generate an API key.

---

## 2.2. Generate the API Key

Edit your profile and scroll down to the « API access » section.  
Click on Generate a new API key and save it on your workstation.  
Tick the box to confirm that you saved the key and click on Done.



New API key

Your API key is

dd4992d9961aecfd97319fd9340493883e79bc73

Copy and store your API key in a safe place

Dashboard does not store API keys in plaintext for security reasons, so this is the *only* time you will be able to record it. If you lose or forget your API key, *you will have to revoke it and generate a new one.*

I have stored my new API key

Done

## 2.3. Import the API key in the Cloudi-Fi portal

Go to Cloudi-Fi administration UI > Settings > Integrations >  
Select "Meraki" in the integration list.

From the Meraki integration screen, create a new Activation by clicking on "Enable this activation" button.

### Integrations > Cisco Meraki



Visit Website

Documentation

Enable this integration

#### Features

The Meraki x Cloudi-Fi partnership enhances the Meraki offer around 4 points:

1. **Compliance** with local regulations (Collect of authentications & access logs in real-time, Encryption and country-based logs storage, Data privacy friendly)
2. **Enriched User experience** (Device recognition for individualized content when returning on any sites, Modern Captive portal builder in few minutes, Multi-authentication capability)
3. **Added-Value Wi-Fi** (CRM included with management of identities, Platform of solution partners & API friendly, Campaign module, Ad Exchange to monetize)
4. **Embedded Cisco Umbrella Security**

As of today, only Automatic synchronization mode is available. A manual mode will be added for companies which don't want to share an API key. Click on Automatic to continue.

The Meraki x Cloudi-Fi partnership enhances the Meraki offer around 4 points:

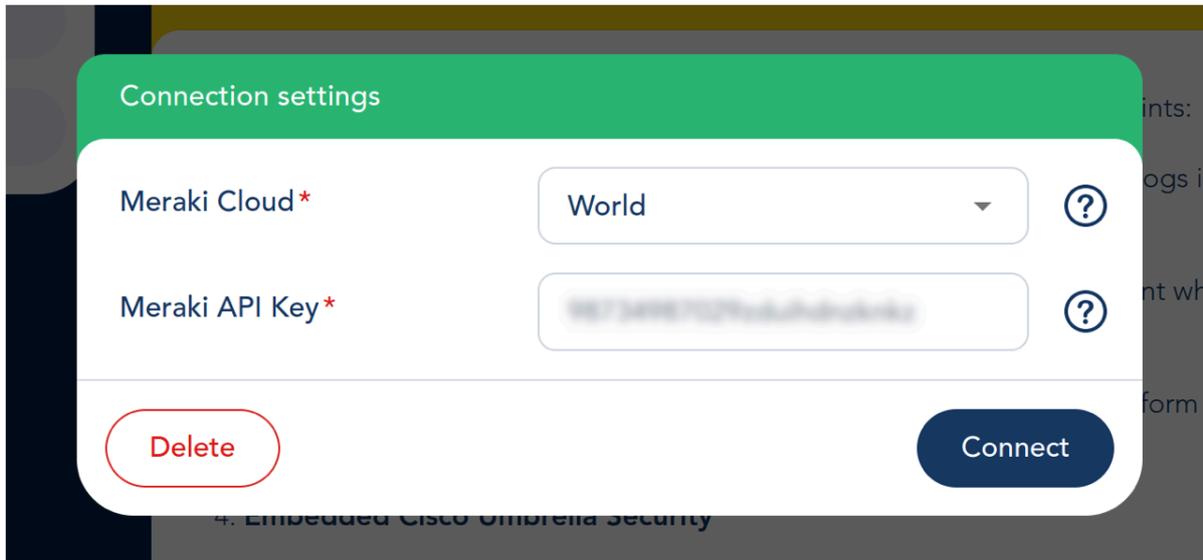
Which kind of integration do you want to enable?

I want Cloudi-Fi to sync with my Meraki account  Automatic

I want to keep control on what will be imported  Manual

4. **Embedded Cisco Umbrella Security**

- ( 1 ) Select Meraki cloud ( World or China )
- ( 2 ) Paste the API key generated on the Meraki portal

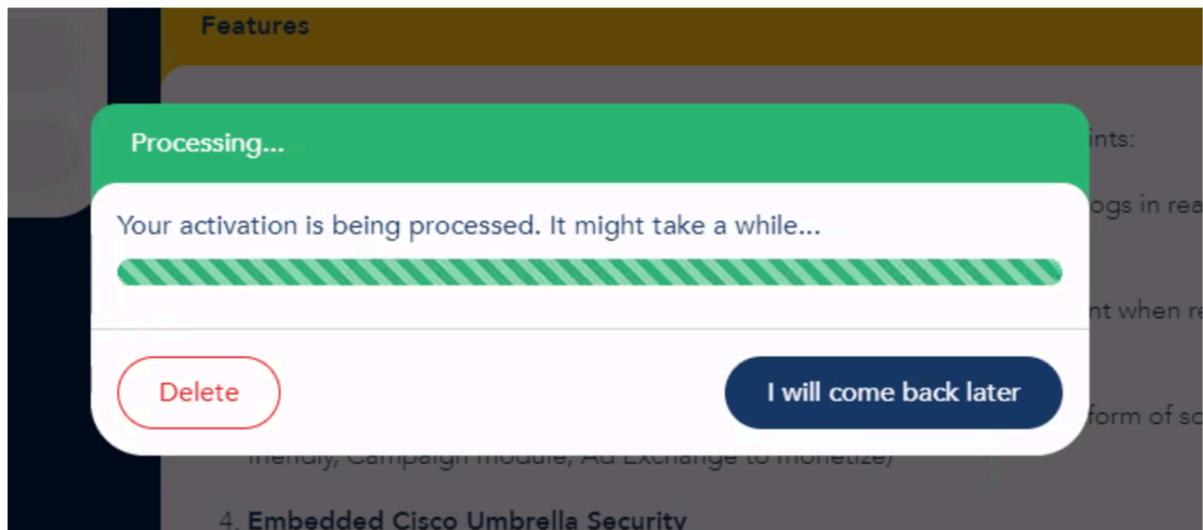


It could be useful to create multiple activation if you have devices connected to different Meraki Clouds.

## 2.4. Run the wizard to configure your Cloudi-Fi locations

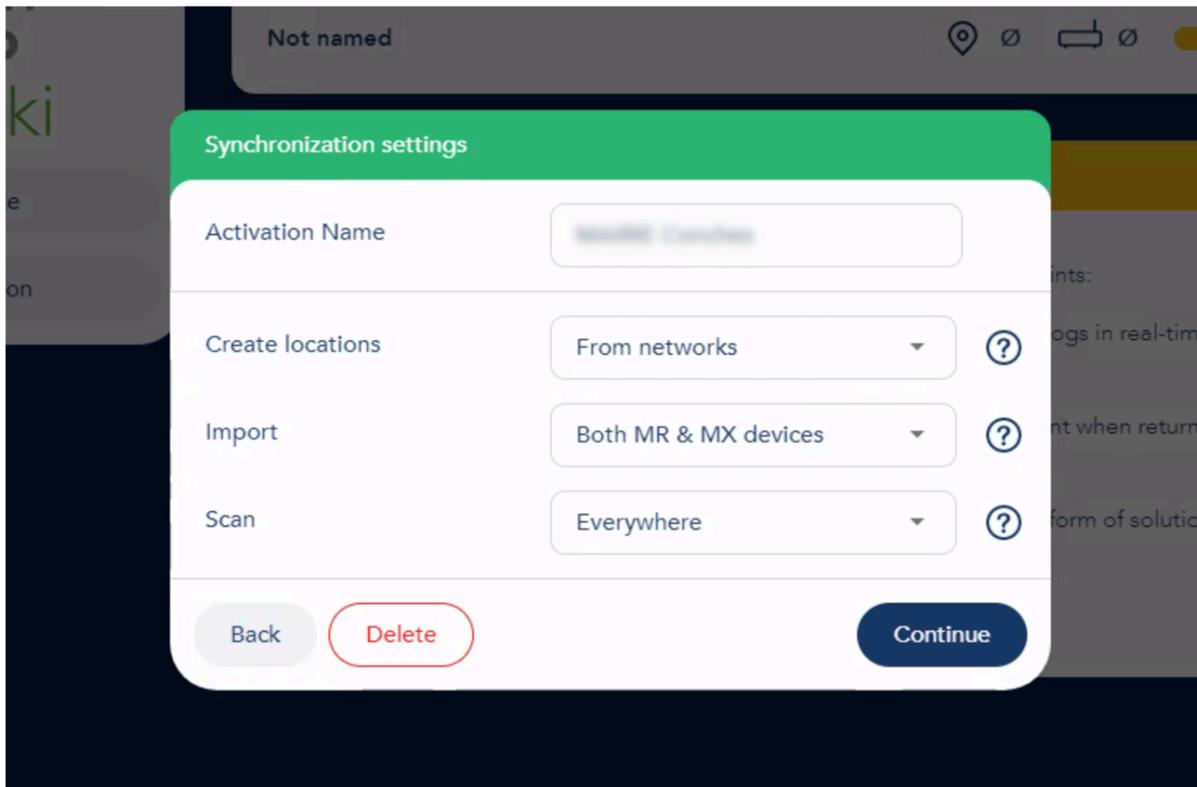
The wizard is used to automatically import Meraki networks. They will be available as Cloudi-Fi locations.

- Click on connect to start the synchronization process.
- The wizard will directly retrieve networks and devices details from Meraki.

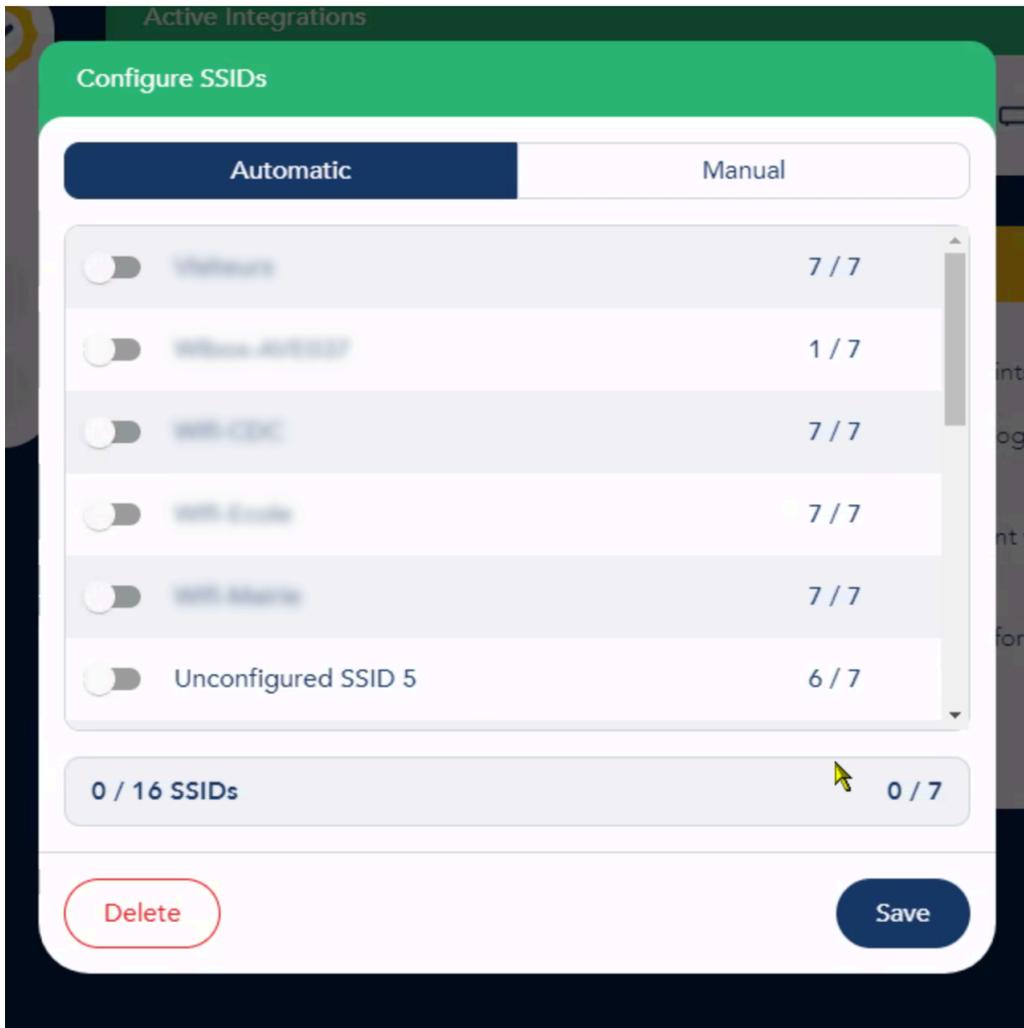


- Define the synchronization target on the following screen by choosing the device type to import ( MX / MR )

- Restrict synchronized Networks or Devices by selecting Networks or Tags to sync in the Scan section

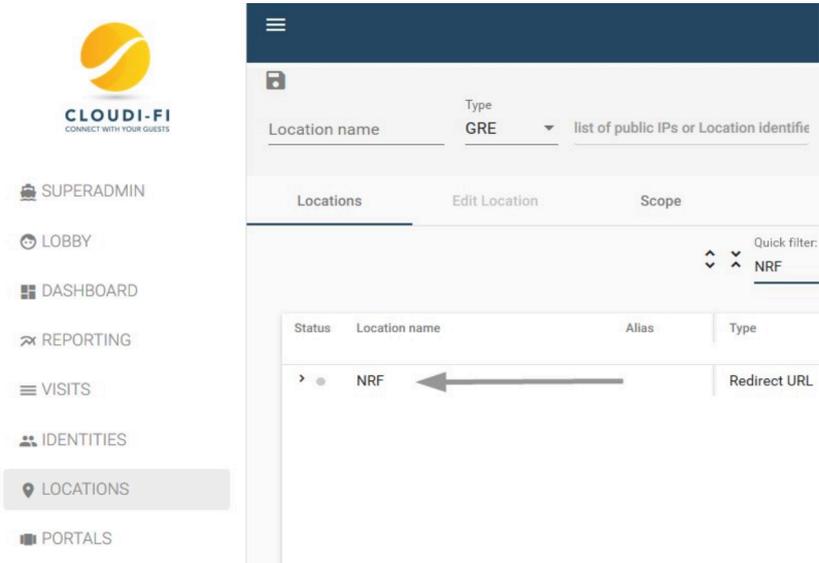


- The last step allows you to enable Cloudi-Fi on a chosen SSID. If you don't want to let Cloudi-Fi change your Meraki configuration you can select "Manual" in order to get information required to setup your Meraki Splash page / ACLs with Cloudi-Fi.



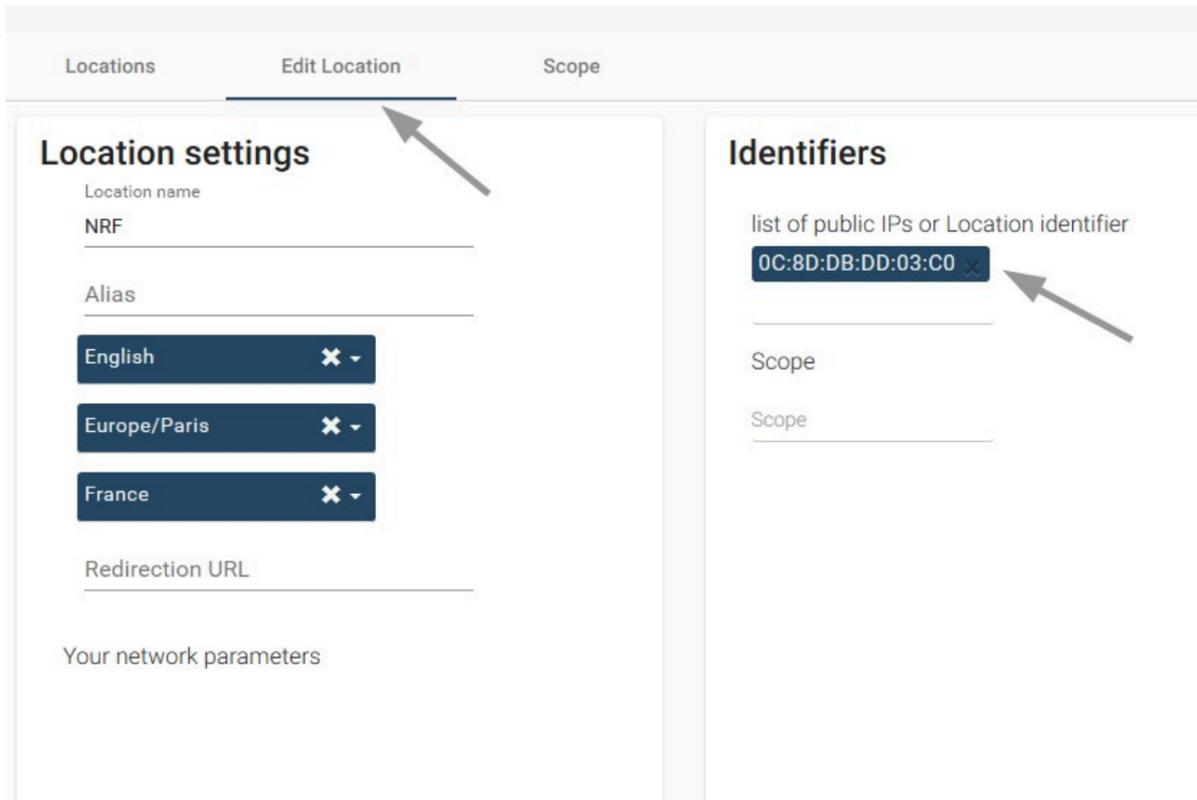
## 2.5. Verify Cloudi-Fi locations creation

Verify that Meraki networks are successfully imported as Cloudi-Fi locations in the LOCATIONS menu :



The screenshot shows the Cloudi-Fi admin interface. On the left is a sidebar with navigation options: SUPERADMIN, LOBBY, DASHBOARD, REPORTING, VISITS, IDENTITIES, LOCATIONS (highlighted), and PORTALS. The main content area shows a 'Locations' table with columns for Status, Location name, Alias, and Type. A table entry for 'NRF' is shown with an arrow pointing to it. Above the table, there are tabs for 'Locations', 'Edit Location', and 'Scope'. A 'Quick filter' dropdown is set to 'NRF'.

If you edit the location, you can see that the Wizard has automatically imported the MAC-addresses of the Meraki devices. This parameter is used to identify the location.

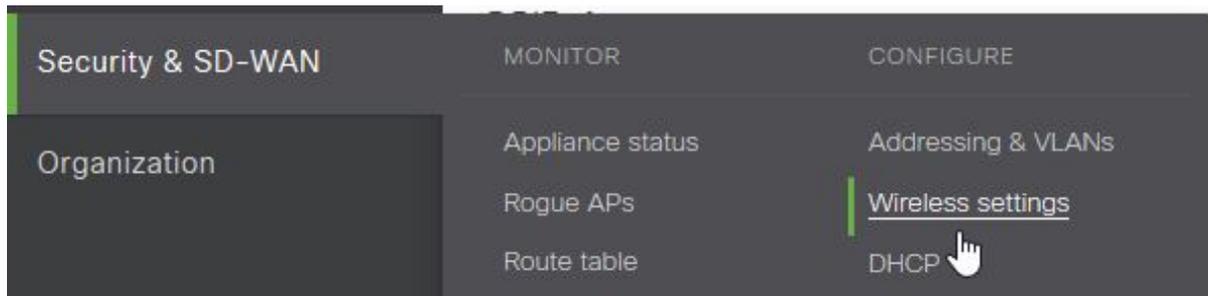


The screenshot shows the 'Edit Location' form for the 'NRF' location. The form is divided into two main sections: 'Location settings' and 'Identifiers'. In the 'Location settings' section, the 'Location name' is 'NRF'. The 'Alias' section contains three dropdown menus: 'English', 'Europe/Paris', and 'France'. The 'Redirection URL' field is empty. In the 'Identifiers' section, the 'list of public IPs or Location identifier' field contains the MAC address '0C:8D:DB:DD:03:C0', which is highlighted with an arrow. Below this field are two 'Scope' fields, both of which are empty.

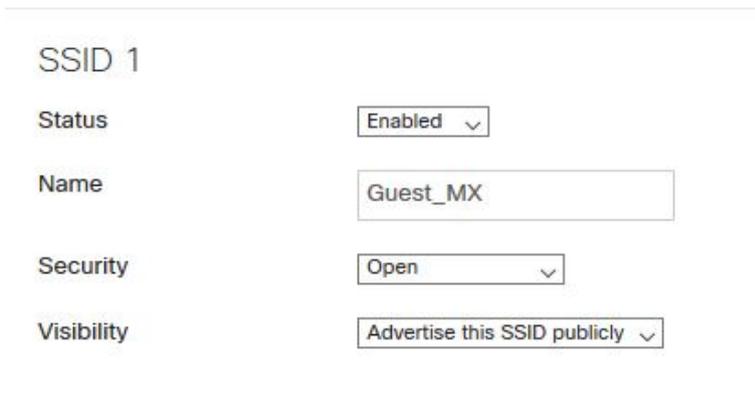
## 2.6. Create the Guest SSID (optional / when Manual SSID configuration is selected)

Note that menus are different between MR and MX devices

For MX devices, go to Security & SD-WAN > Wireless settings



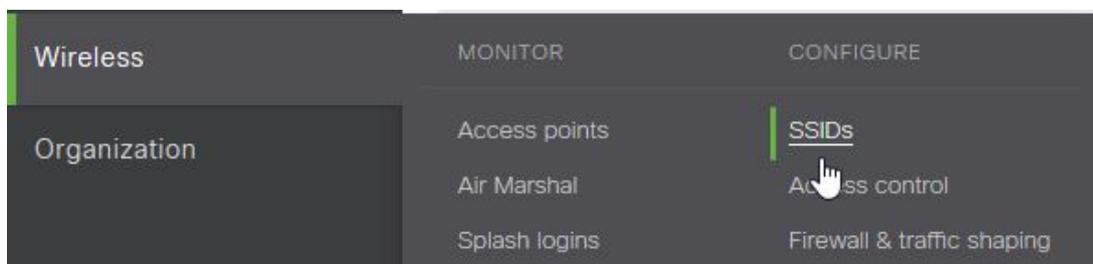
Enable an available SSID, fill a name and choose Security : Open



The screenshot shows the configuration form for 'SSID 1'. The form includes the following fields:

- Status: Enabled (dropdown menu)
- Name: Guest\_MX (text input field)
- Security: Open (dropdown menu)
- Visibility: Advertise this SSID publicly (dropdown menu)

For MR devices, go to Wireless > SSIDs



Enable an available SSID, fill a name and save changes.

## Configuration overview

**SSIDs** Showing 4 of 15 SSIDs. [Show all my SSIDs.](#)

POC_MR	
Enabled	<input type="checkbox"/> enabled <span>▼</span>
Name	<a href="#">rename</a>
Access control	<a href="#">edit settings</a>

Then go to Wireless > Access control and select "Open (no encryption)" in Association requirement And select "Click-through" method for the Splash page

### Network access

- Association requirements**
- Open (no encryption)**  
Any user can associate
  - Pre-shared key (PSK)**  
Users must enter a passphrase to associate
  - MAC-based access control (no encryption)**  
RADIUS server is queried at association time
  - Enterprise with** Meraki Cloud Authentication ▼  
User credentials are validated with 802.1X at association time
  - Identity PSK with RADIUS**  
RADIUS server is queried at association time to obtain a passphrase for a device based on its MAC address

- Splash page**
- None (direct access)**  
Users can access the network as soon as they associate
  - Click-through**  
Users must view and acknowledge your splash page before being allowed on the network

You also have to authorize unauthenticated users to access to "cloudi-fi.net" domain in order to allow them to access to the Cloudi-Fi captive portal.

- For MX devices, go to Security & SD-WAN > Access control
- For MR devices, go to Wireless > Access control

In the Walled garden ranges, add \*.cloudi-fi.net

Depending the authentication methods you have enabled on your captive portal, you may have to add additional domains in the Walled garden ranges.

Cloudi-Fi support will provide you the needed extra domains.

---

**Captive portal strength** Block all access until sign-on is complete

**Walled garden** Walled garden is enabled

**Walled garden ranges** \*.cloudi-fi.net

[What do I enter here?](#)  
Specify your walled garden by entering space separated addresses, ranges (using [CIDR notation](#)), domain names, and domain wildcards.  
\*.google.com

**Controller disconnection behavior** The splash page for this SSID relies on the Meraki Cloud Controller. What should happen to new clients if your unreachable?

- Open: devices can use the network without seeing a splash page, unless they are explicitly blocked
- Restricted: only currently associated clients and whitelisted devices will be able to use the network
- Default for your settings: Open

For MR and MX: Configure how WiFi clients will retrieve an IP:  
This settings depends of your network architecture, for instance if you already have a DHCP server and dedicated DHCP range for Guest users.

For an easy deployment, we recommand to use the "**NAT mode**" option.  
The Access-Point will act as DHCP server and all WiFi client will be see outside of the wireless network with the Access Point LAN IP.

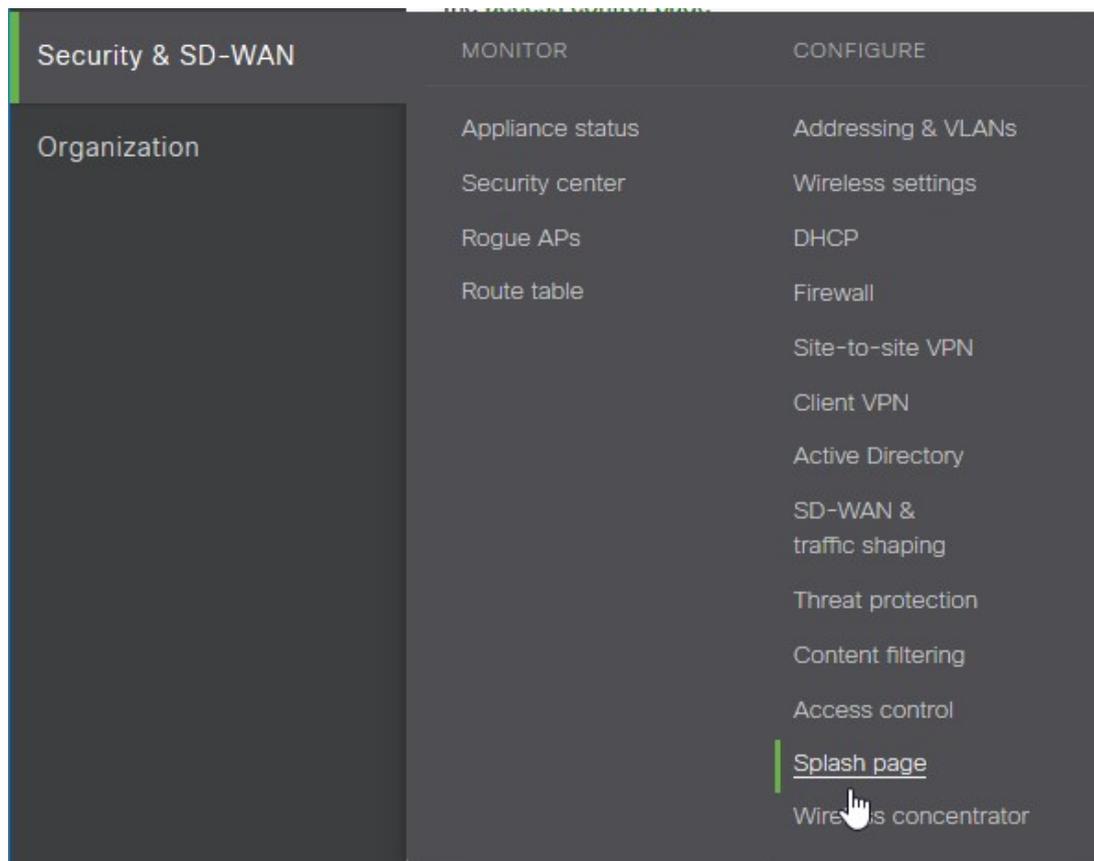
### Addressing and traffic

**Client IP assignment**

- NAT mode: Use Meraki DHCP**  
Clients receive IP addresses in an isolated 10.0.0.0/8 network. Clients can
- Bridge mode: Make clients part of the LAN**  
Meraki devices operate transparently (no NAT or DHCP). Clients receive D
- Layer 3 roaming**  
Clients receive DHCP leases from the LAN or use static IPs as in bridge m
- Layer 3 roaming with a concentrator**  
Clients are tunneled to a specified VLAN at the concentrator. They will kee
- VPN: tunnel data to a concentrator**  
Meraki devices send traffic over a secure tunnel to an MX concentrator.

## 2.7. Configure the Splash page in Meraki administration

On the Meraki Portal,  
For MX devices, go to Security & SD-WAN > Splash page  
For MR devices, go to Wireless > Splash page



Choose to use a Custom splash URL and fill the Cloudi-Fi URL

## Splash page

Splash pages are enabled because a click-through splash page is enabled. You can change this setting on the [access control page](#).

### Official themes ⓘ

- Modern **NEW**
- Fluid

### Custom themes ⓘ

[Create something new](#)

#### Custom splash URL

Or provide a URL where users will be redirected:

[What is this?](#)

## 2.8. Prevent Guest users to access your internal networks

Go to Wireless > Firewall & Traffic Shaping > Select your SSID

And modify the existing rule in order to deny Guest users to access private IP ranges.

Save

---

### Block IPs and ports

Layer 2 LAN isolation Disabled (bridge mode only)

Layer 3 firewall rules ⓘ

#	Policy	Protocol	Destination	Port	Comment	Actions
	<span>Deny</span>	Any	Local LAN	Any	Wireless clients accessing LAN	
	Allow	Any	Any	Any	Default rule	

[Add a layer 3 firewall rule](#)