Cloudi-Fi integration with Cisco Meraki

MX and MR

Table of Contents

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.

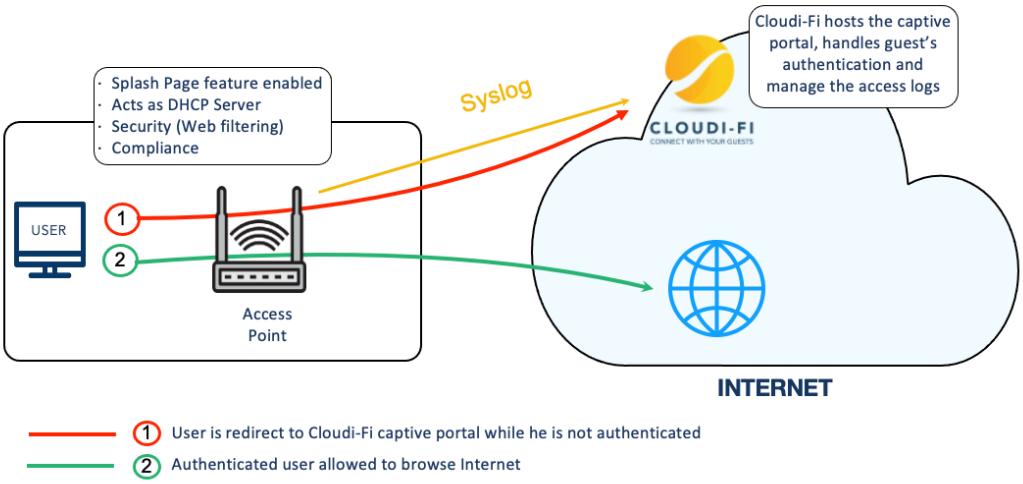


Figure - Configuration Overview

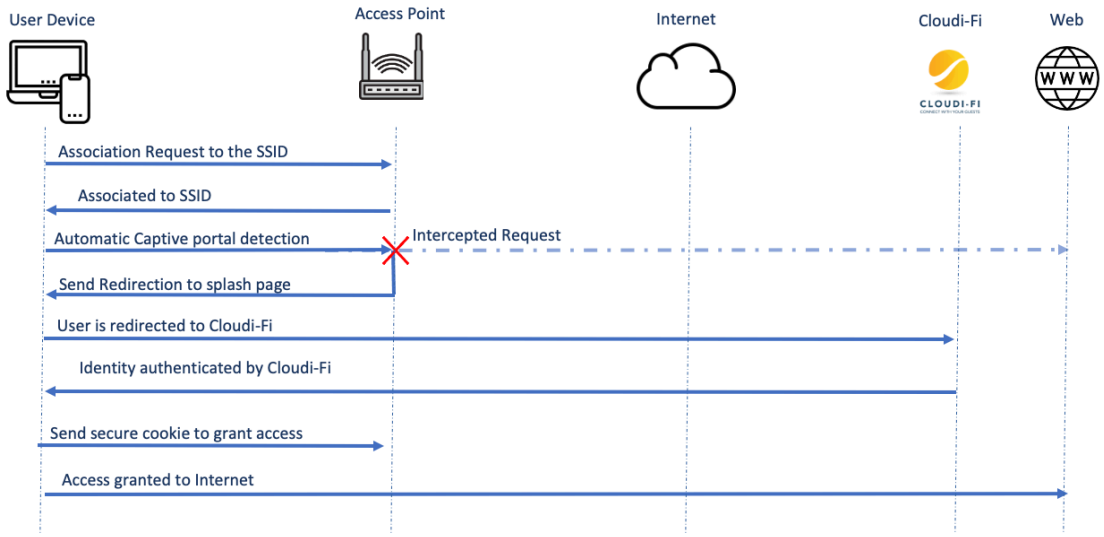


Figure - Authentication workflow

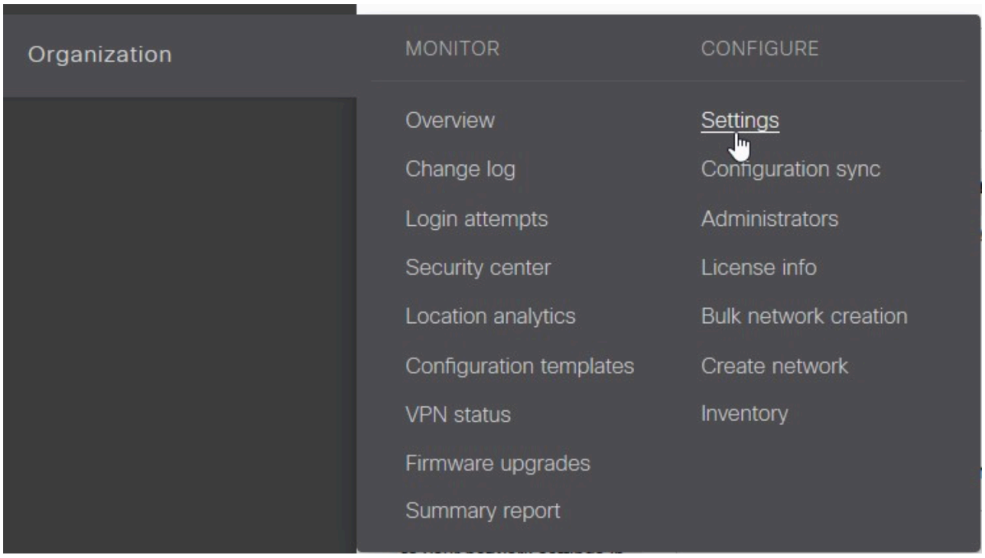
2. Importing Cisco Meraki networks into Cloudi-Fi

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

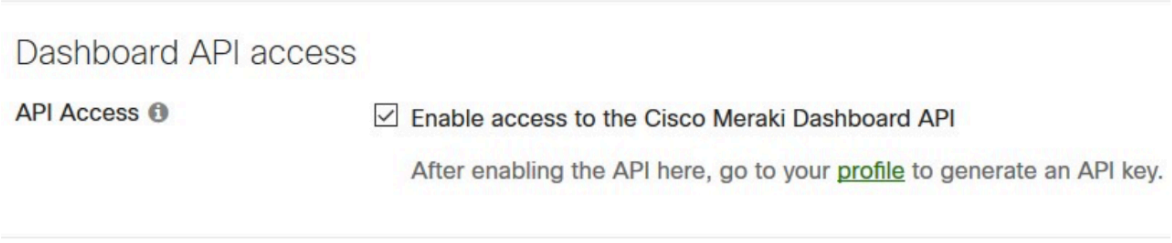
- Meraki API enablement
- Use Cloudi-Fi wizard to import any existing Meraki network
- Configure Meraki SSID and Splash page manually (optional)

2.1. Enable API access to Meraki portal

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

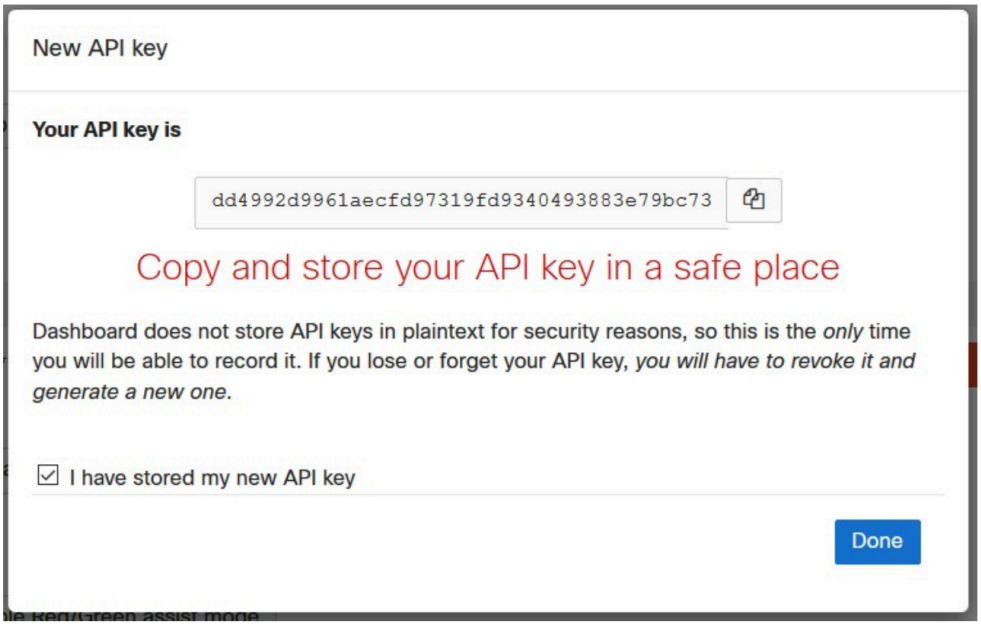


Tick the box « Enable access to the Cisco Meraki Dashboard API and save changes.



2.2. Generate the API Key

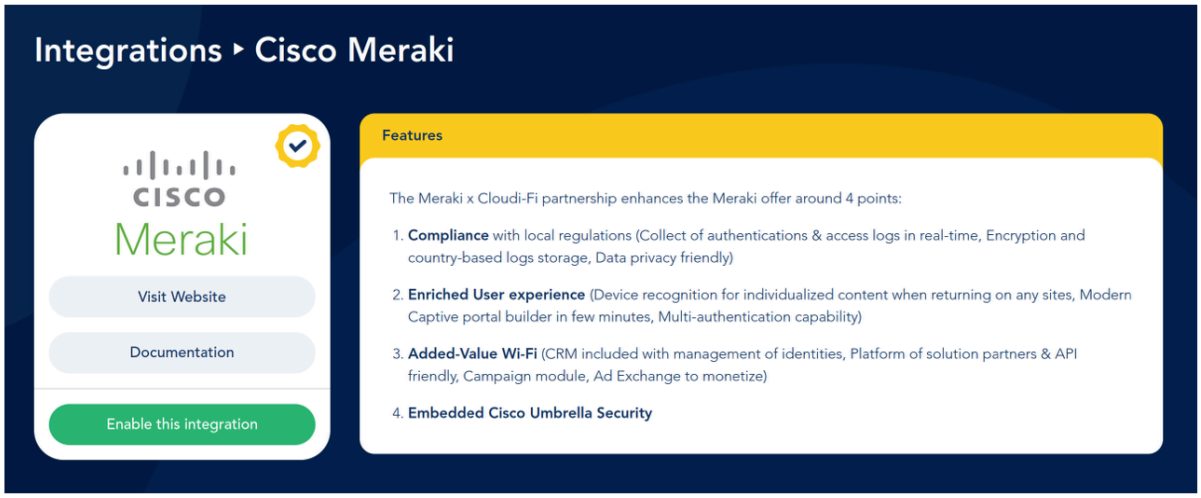
Edit your profile and scroll down to the « API access » section.
Click on Generate a new API key and save it on your workstation.
Tick the box to confirm that you saved the key and click on Done.



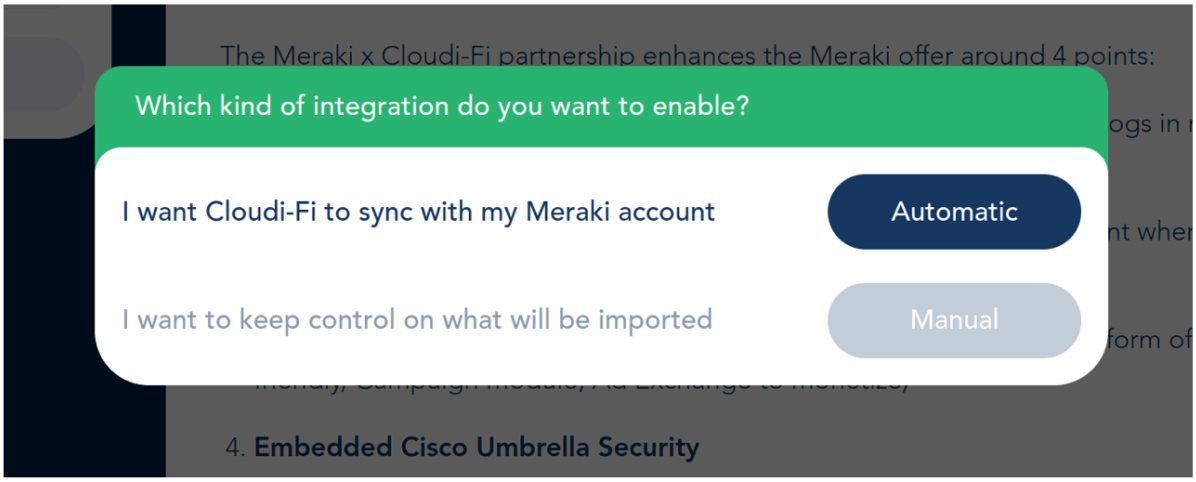
2.3. Import the API key in the Cloudi-Fi portal

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

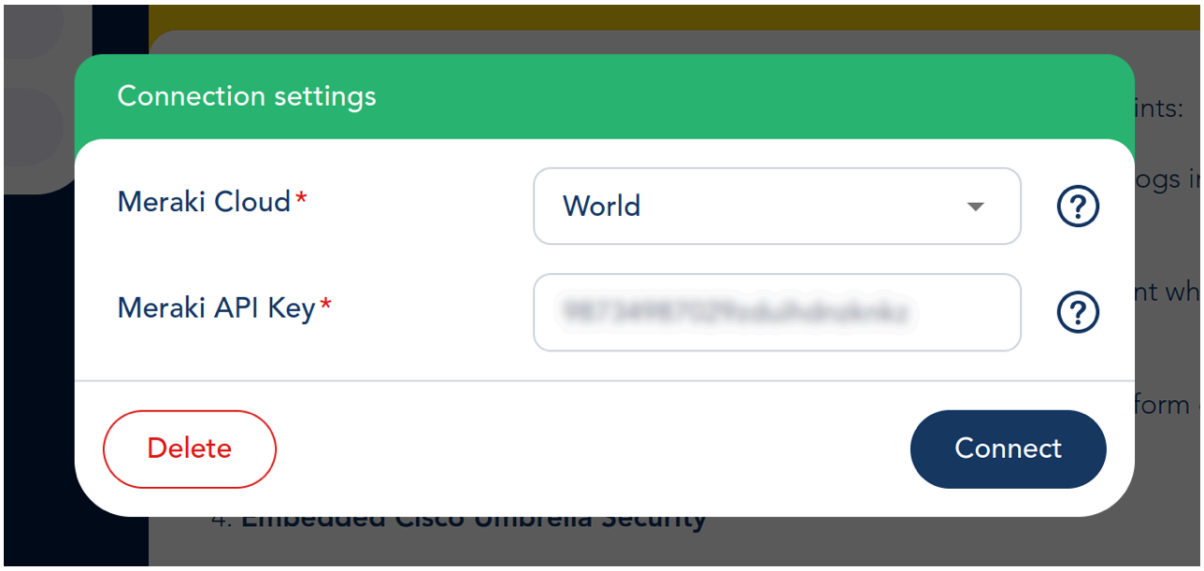
From the Meraki integration screen, create a new Activation by clicking on "Enable this activation" button.



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.



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

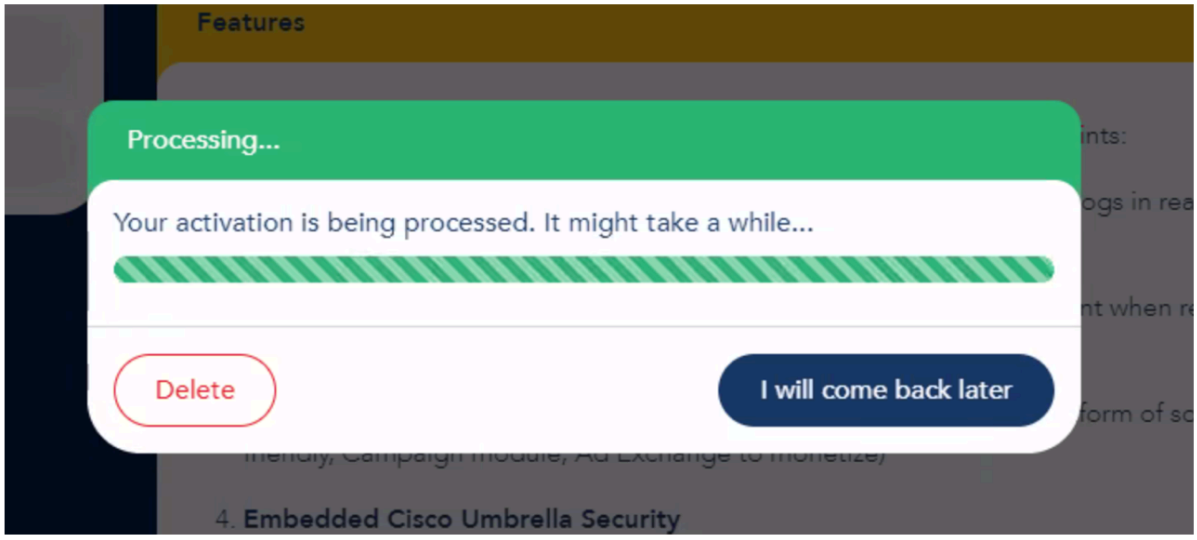


It could be useful to create multiple activation if you have devices connected to different Meraki Clouds.

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

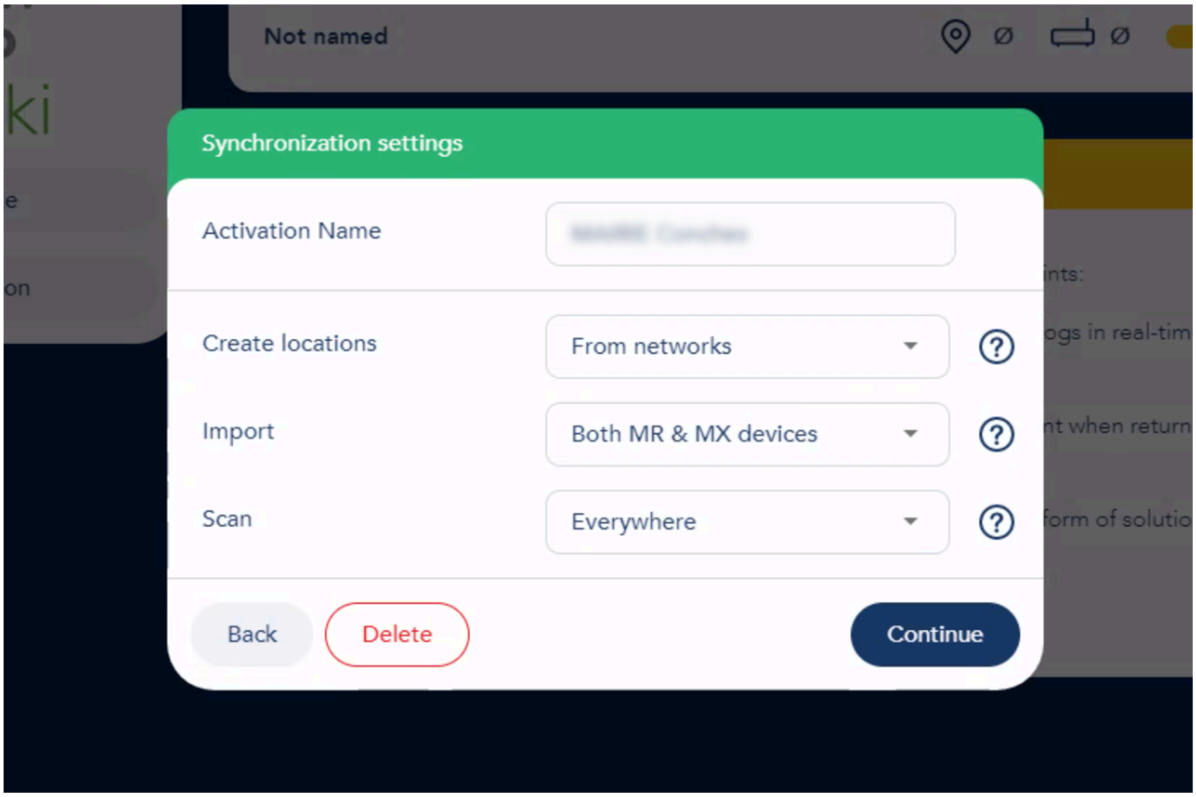
The wizard is used to automatically import Meraki networks. They will be available as Cloudi-Fi locations.

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

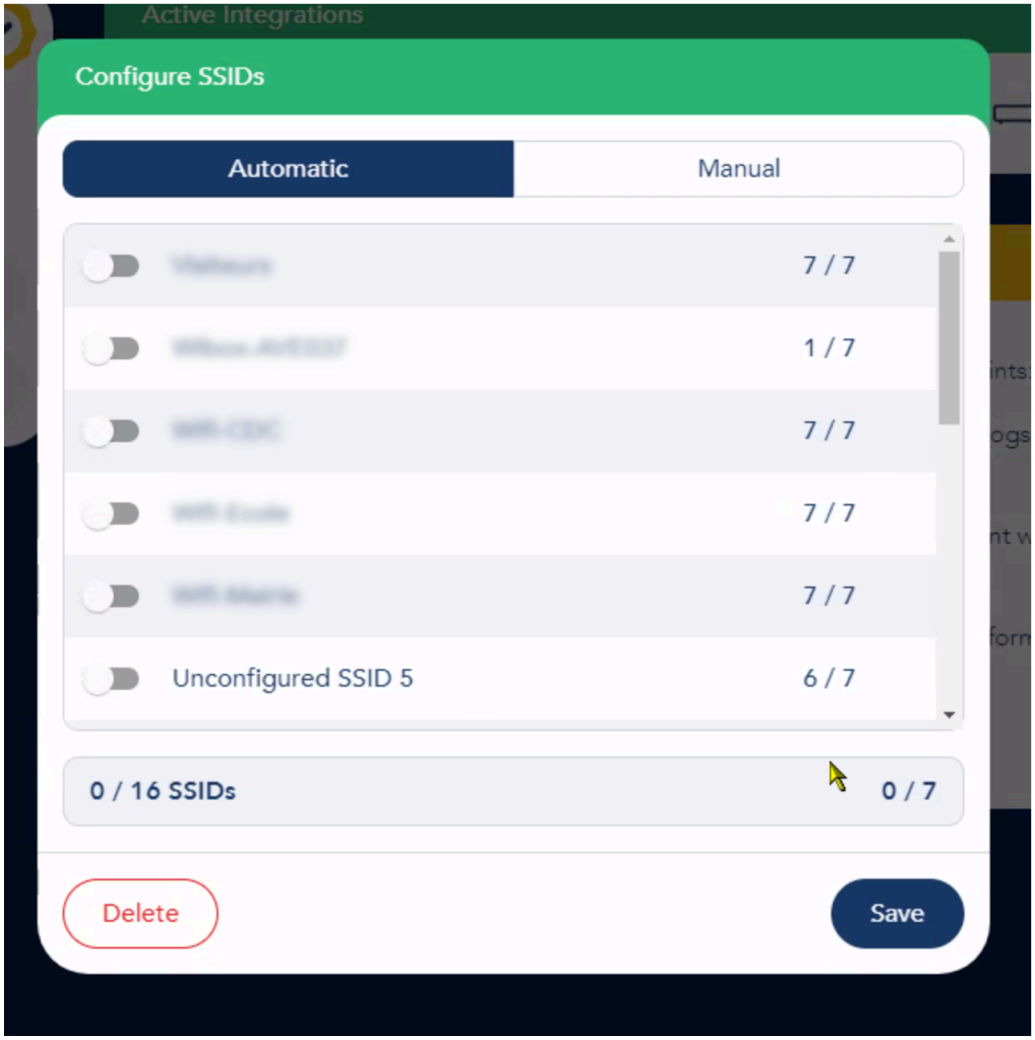


- Define the synchronization target on the following screen by choosing the device type to import (MX / MR)

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

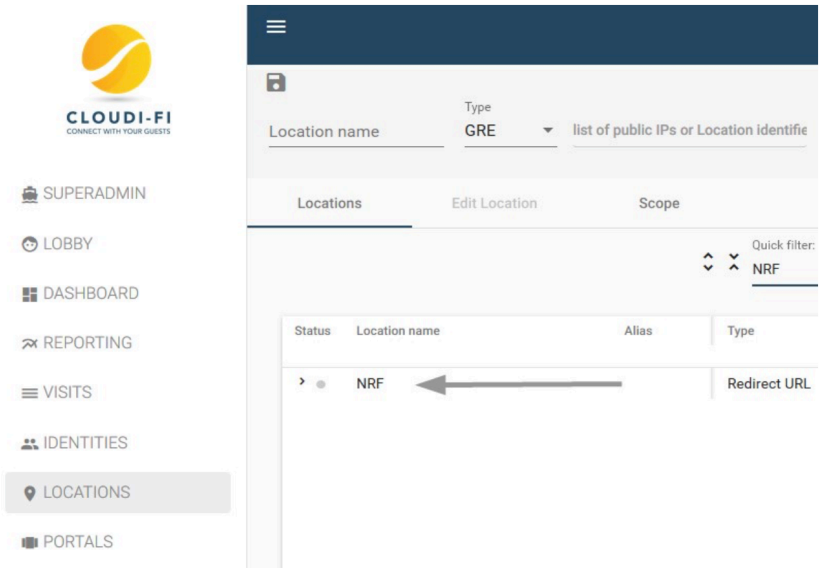


- The last step allows you to enable Cloudi-Fi on a chosen SSID. If you don't want to let Cloudi-Fi change your Meraki configuration you can select "Manual" in order to get information required to setup your Meraki Splash page / ACLs with Cloudi-Fi.

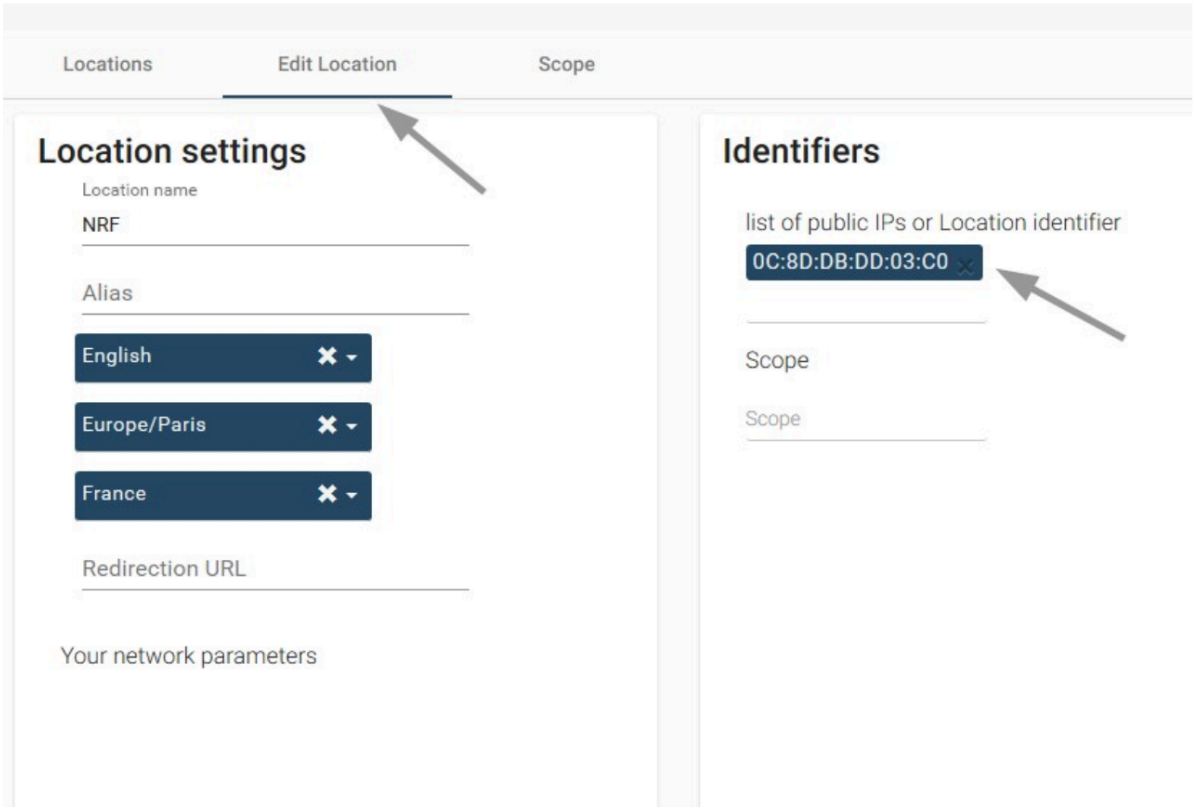


2.5. Verify Cloudi-Fi locations creation

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



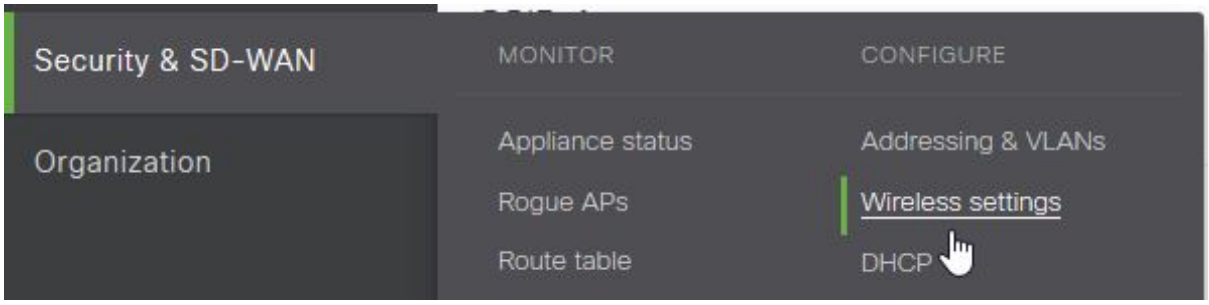
If you edit the location, you can see that the Wizard has automatically imported the MAC-addresses of the Meraki devices. This parameter is used to identify the location.



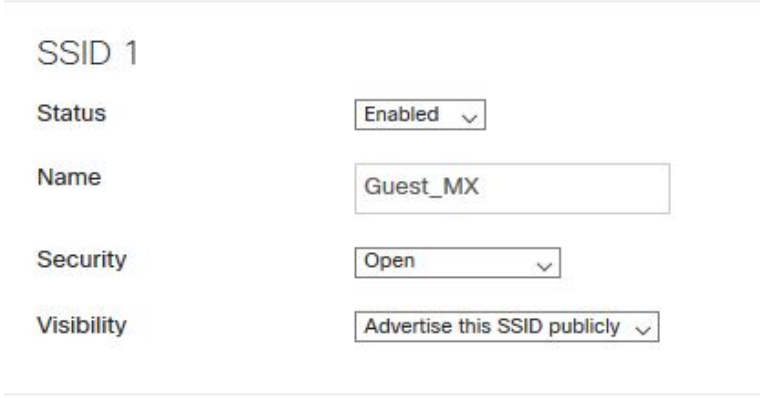
2.6. Create the Guest SSID (optional / when Manual SSID configuration is selected)

Note that menus are differents between MR and MX devices

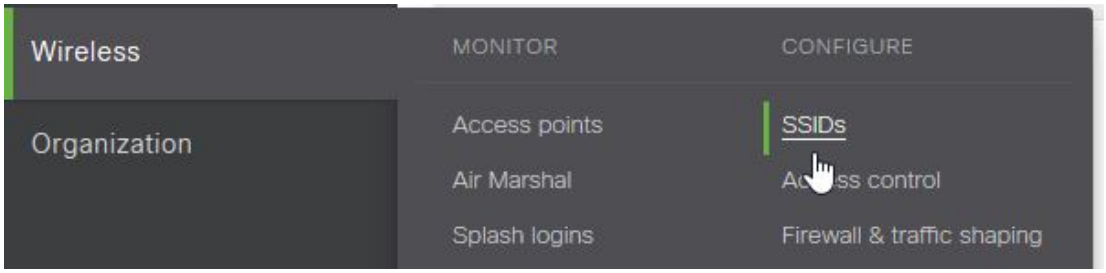
For MX devices, go to Security & SD-WAN > Wireless settings



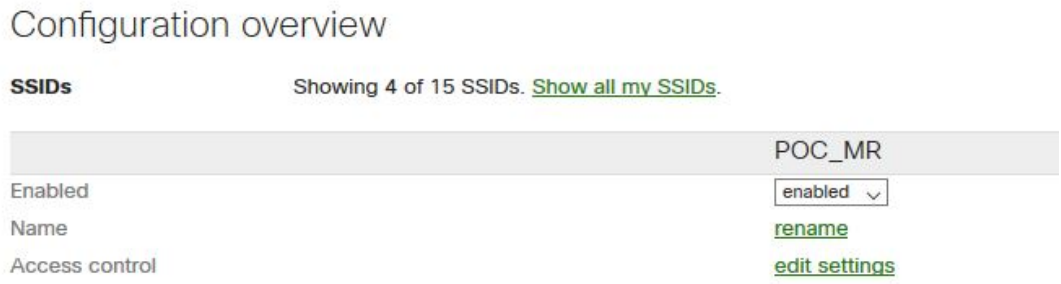
Enable an available SSID, fill a name and choose Security : Open



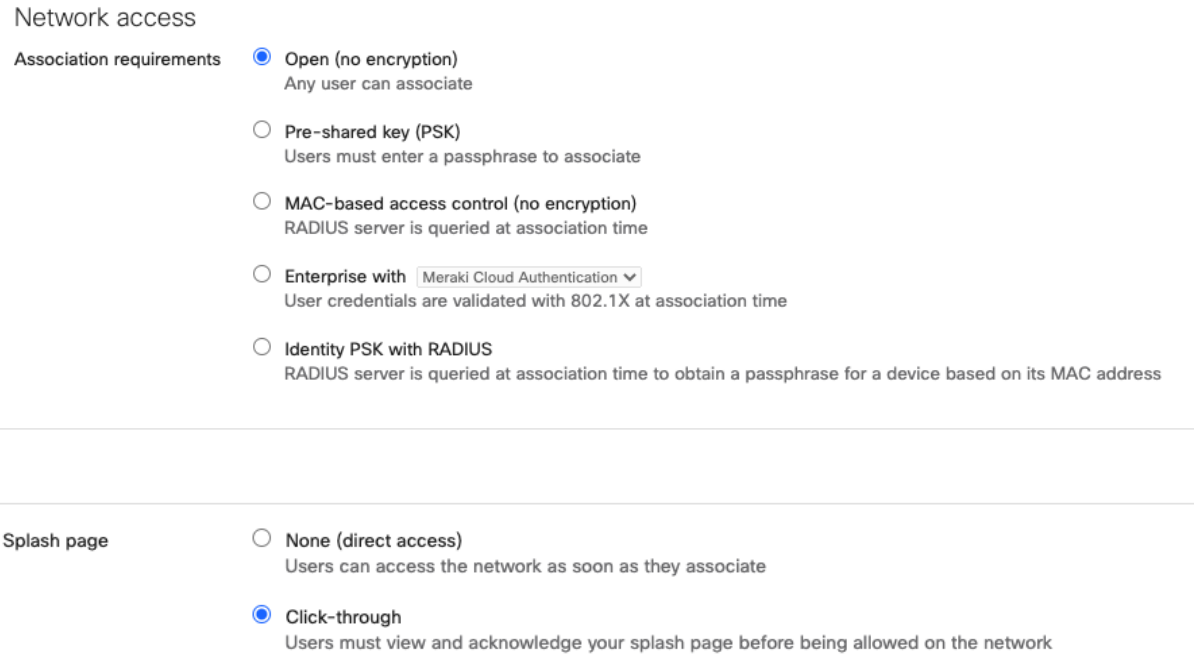
For MR devices, go to Wireless > SSIDs



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



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

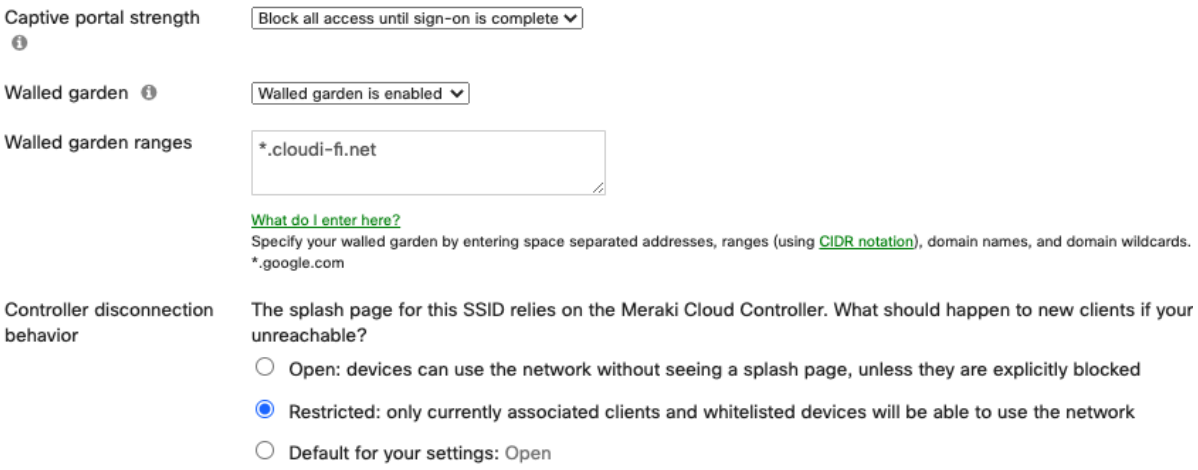


You also have to authorize unauthenticated users to access to "cloudi-fi.net" domain in order to allow them to access to the Cloudi-Fi captive portal.

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

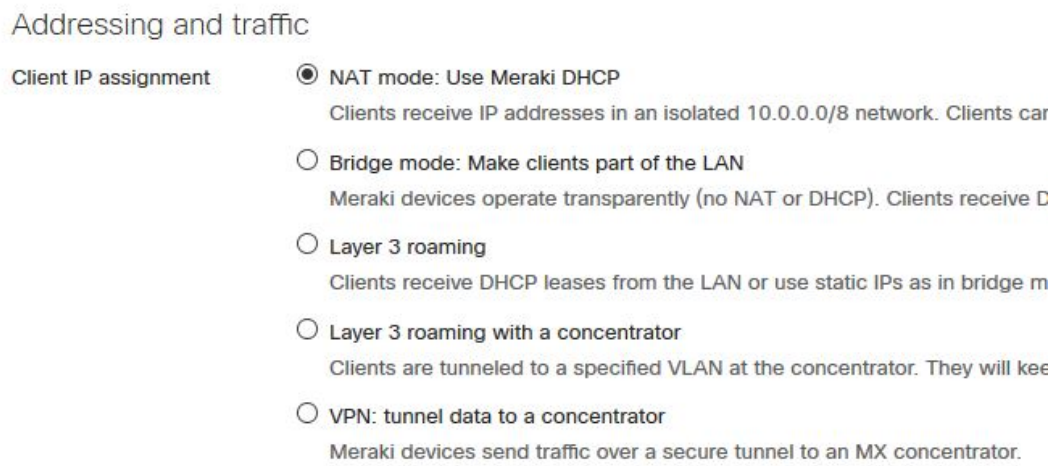
In the Walled garden ranges, add *.cloudi-fi.net

Depending the authentification 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.



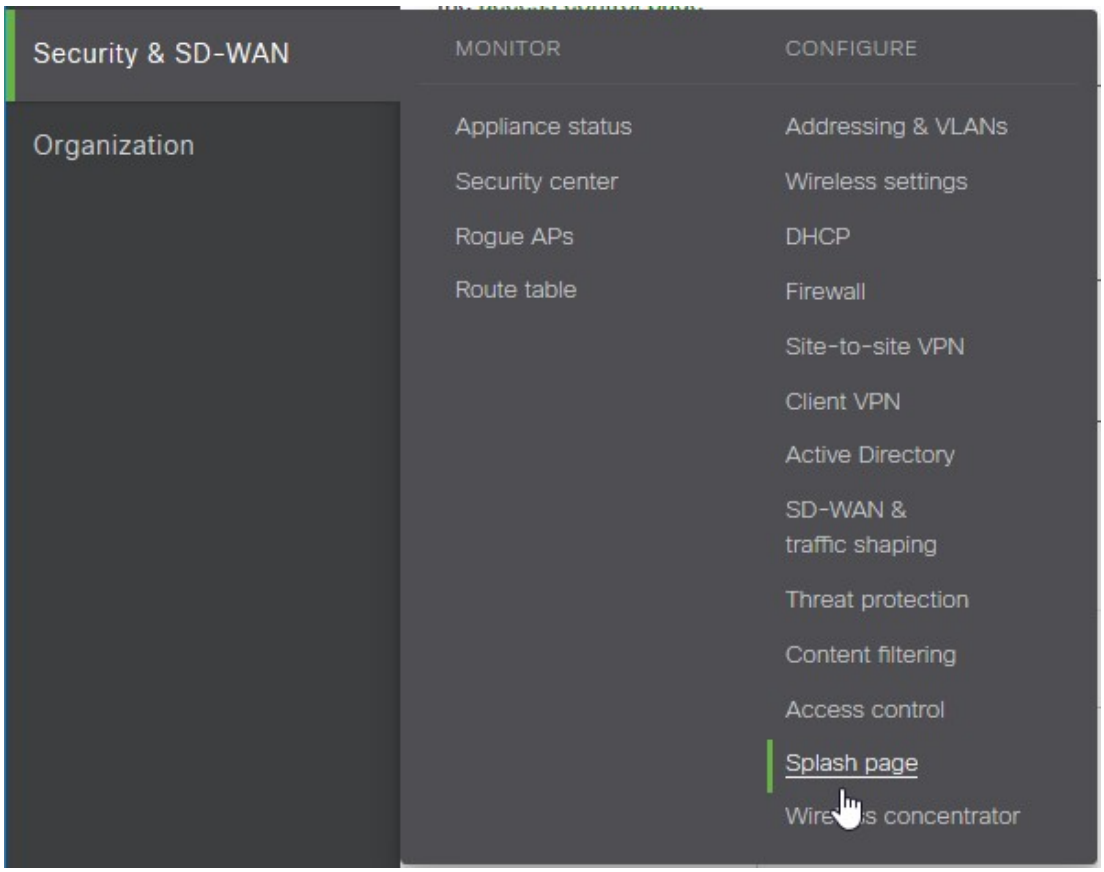
For MR and MX: Configure how WiFi clients will retrieve an IP:
This settings depends of your network architecture, for instance if you already have a DHCP server and dedicated DHCP range for Guest users.

For an easy deployement, 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.

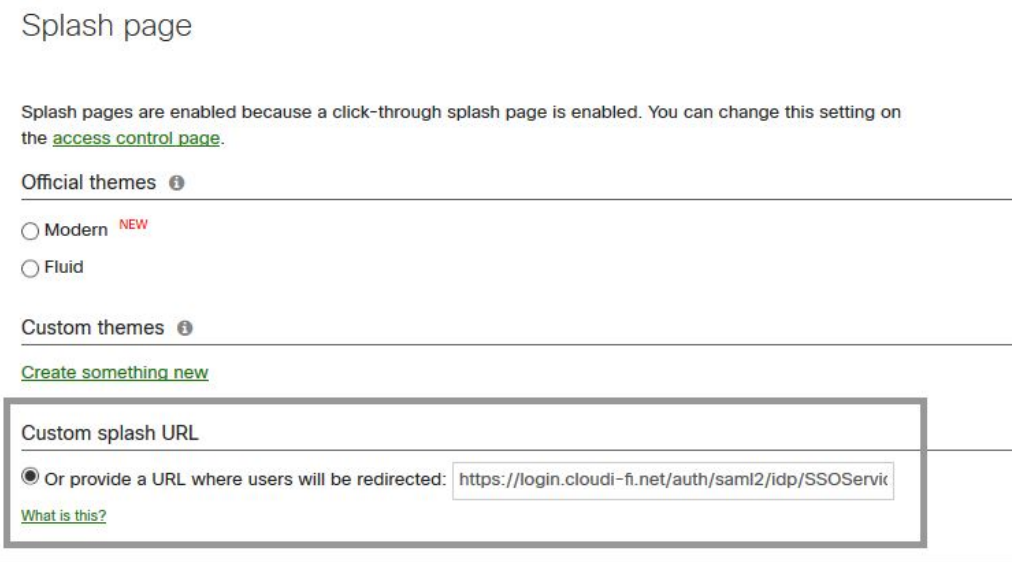


2.7. Configure the Splash page in Meraki administration

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



2.8. Prevent Guest users to access your internals 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