

# Cisco Meraki AP / MX / Z1

Modified on: Mon, 21 Sep, 2015 at 10:59 AM

Open a web browser and log in to your Meraki dashboard at <https://dashboard.meraki.com>

Click on "Configure" on the left menu

Click "Access Control" on the left menu and configure with the below settings:

## Access control

SSID:

### Network access

- Association requirements
- Open (no encryption)  
Any user can associate
  - Pre-shared key with   
Users must enter a passphrase to associate
  - MAC-based access control (no encryption)  
RADIUS server is queried at association time
  - WPA2-Enterprise with   
User credentials are validated with 802.1X at association time

- 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
  - Sign-on with   
Users must enter a username and password before being allowed on the network
  - Sign-on with SMS Authentication <sup>BETA</sup>  
Users enter a mobile phone number and receive an authorization code via SMS.  
After a trial period of 25 texts, you will need to connect with your Twilio account on the [Network-wide settings](#) page.
  - Billing (paid access)  
Users choose from various pay-for-access options, or an optional free tier
  - Systems Manager Sentry <sup>Ⓜ</sup>  
Only devices with Systems Manager can access this network

RADIUS for splash page

#	Host	Port	Secret	Status	Actions
1	<input type="text" value="radius.groplabs.net"/>	<input type="text" value="1812"/>	<input type="text" value="....."/>	Show secret	<input type="button" value="⊕"/> <input type="button" value="✕"/> <input type="button" value="Test"/>

[Add a server](#)

RADIUS accounting

RADIUS accounting servers

#	Host	Port	Secret	Status	Actions
1	<input type="text" value="radius.groplabs.net"/>	<input type="text" value="1813"/>	<input type="text" value="....."/>	Show secret	<input type="button" value="⊕"/> <input type="button" value="✕"/>

[Add a server](#)

IP addresses

The Meraki cloud must be able to communicate with your RADIUS servers via the Internet.

**Please make sure that:**

- Your RADIUS servers have public IP addresses (i.e., they are reachable on the Internet).
- Your firewall, if any, allows incoming traffic to your RADIUS servers.
- You whitelist the following IP addresses as clients on your RADIUS server: 46.165.249.11, 64.156.192.245, 72.249.183.161, 74.50.56.181.

Failover policy

If none of your RADIUS servers are reachable, should clients be allowed to use the network?

- Deny access
- Allow access

Load balancing policy

- Strict priority order
- Round robin

- **Association Requirements:** Open (no encryption)
- **Splash page:** Sign-on with my RADIUS server

- **RADIUS for splash page:**

click **Add a Server** and add:

**Host:** \*insert radius\_server here\*

**Port:** 1812

**Secret:** \*insert radius\_secret here\*

click **Add a Server** again and add:

**Host:** \*insert radius\_server2 here\*

**Port:** 1812

**Secret:** \*insert radius\_secret here\*

**Note:** When you enter the radius server you may see an error: *"Host for RADIUS is not a valid IP address."* This is an expected error message, the field prefers an IP address but will still work with a domain name in this field.

- **RADIUS accounting:** RADIUS accounting is enabled
- **RADIUS accounting servers:**

click **Add a Server** and add:

**Host:** \*insert radius\_server here\*

**Port:** 1813

**Secret:** \*insert radius\_secret here\*

click **Add a Server** again and add:

**Host:** \*insert radius\_server2 here\*

**Port:** 1813

**Secret:** \*insert radius\_secret here\*

**Note:** You may not see the option to set up the RADIUS accounting. If this is the case please raise a Meraki support case via **Help** -> **Cases** -> **New Case** asking them: "Please can you enable RADIUS accounting on my account"

**Note 2:** The Meraki MX/Z1 does not support accounting, so please skip this step.

Network access control <sup>ⓘ</sup> Disabled: do not check clients for antivirus software ▼

---

Assign group policies by device type <sup>ⓘ</sup> Disabled: do not assign group policies automatically ▼

---

Captive portal strength <sup>ⓘ</sup> Block all access until sign-on is complete ▼

Walled garden <sup>ⓘ</sup> Walled garden is enabled ▼

Walled garden ranges

```

*.*insert_access_domain_here*
*.meraki.com
www.google.com
www.google.co.uk
*.google-analytics.com
*.venuewifi.com
*.openweathermap.org

*.cloudfront.net

```

[What do I enter here?](#)

Simultaneous logins <sup>ⓘ</sup> Allow simultaneous devices per user ▼

Controller disconnection behavior <sup>ⓘ</sup> Login attempts on this SSID will be processed by the Meraki Cloud Controller. What should happen to new clients if your Internet uplink is down or the controller is otherwise unreachable?

Open: devices can use the network without signing in, unless they are explicitly blocked

Restricted: only currently associated clients and whitelisted devices will be able to use the network

Default for your settings: Restricted

---

Bandwidth limit controls <sup>ⓘ</sup> The Per-device bandwidth limit <sup>ⓘ</sup> and Total SSID bandwidth limit <sup>ⓘ</sup> controls moved to the [Firewall and traffic shaping page](#). Choose a default per-device bandwidth limit. Your RADIUS server can override this value. [Explain more...](#)

Whitelist & blocked <sup>ⓘ</sup> [Whitelisted](#) and [blocked](#) devices are set on the clients page. The default block message moved to [Network-wide settings](#).

---

**Addressing and traffic**

Client IP assignment <sup>ⓘ</sup>

NAT mode: Use Meraki DHCP  
Clients receive IP addresses in an isolated 10.0.0.0/8 network. Clients cannot communicate with each other, but they may communicate with devices on the wired LAN if the [SSID firewall settings](#) permit.

Bridge mode: Make clients part of the LAN  
Meraki devices operate transparently (no NAT or DHCP). Clients receive DHCP leases from the LAN or use static IPs. Use this for shared printers, file sharing, and wireless cameras.

VPN: tunnel data to a concentrator  
Meraki devices send traffic over a secure tunnel to an MX or VM concentrator.

Layer 3 roaming <sup>beta</sup>  
Clients are tunneled to a specified VLAN at the concentrator. They will keep the same IP address when roaming between APs.

VLAN tagging <sup>ⓘ</sup> Don't use VLAN tagging ▼  
Bridge mode only

- **Enable data-carrier detect:** Disabled
- **Captive portal strength:** Block all access until sign-on is complete
- **Walled garden:** Walled garden is enabled

**Note:** You may see an error saying the walled garden entry is invalid. If this is the case please raise a Meraki support case via **Help -> Cases -> New Case** ask them, "Please can you enable domain based walled garden support".

- **Walled garden ranges - Copy and paste the list below**

\*.\*insert\_access\_domain\_here\*

\*.meraki.com

www.google.com

www.google.co.uk

\*.google-analytics.com

\*.venuewifi.com

\*.openweathermap.org

\*.cloudfront.net

If you wish to support social network logins, you also need to add the domains below for each network you plan to support

Facebook	Twitter	LinkedIn	Google	Instagram
*.facebook.com *.fbcdn.net	*.twitter.com	*.linkedin.com	*.googleusercontent.com	
*.akamaihd.net	*.twimg.com	*.licdn.net *.licdn.com	*.googleapis.com *.accounts.google.com *.gstatic.com	*.instagram.com
*.connect.facebook.net				

**Note :** The Meraki MX/Z1 does not support the Client IP assignment or DNS settings, so please skip this step.

- **Client IP assignment NAT mode: Meraki DHCP**

Content filtering <sup>?</sup>  
NAT mode only

Custom DNS ▼

DNS Servers

208.67.222.222  
208.67.220.220

(one xx.xx.xx.xx IP address per line - max 2 servers)

Bonjour forwarding <sup>?</sup>  
Bridge mode only

Disable Bonjour Forwarding ▼

---

Wireless options

Legacy 11b operation <sup>?</sup>

Disable legacy 11b bitrates (1, 2, & 5.5 Mbps) ▼

Save Changes or [cancel](#)

(Please allow 1-2 minutes for changes to take effect.)

- **Content filtering:** Custom DNS:
- **DNS Servers:**

208.67.222.222  
208.67.220.220

Click on "Save Changes"

Click on "Splash page" on the left and configure with the below settings:



## Splash page

SSID:

Splash pages on this SSID are enabled because custom RADIUS authentication is configured.

### Official themes ?

- Fluid (mobile friendly) new
- Classic
- Plain

### Custom themes ?

[Create something new](#)

### Custom splash URL

Or provide a URL where users will be redirected:

[What is this?](#)

### Customize your page

Message

Splash logo

No logo

[Upload a logo](#)

Splash language

### Splash behavior

Splash frequency

[What is this?](#)

Where should users go after the splash page?

- The URL they were trying to fetch
- A different URL:

- **Custom splash URL:** \*insert access\_url here\*
- **Where should users go after the splash page?:**  
**A Different URL:** \*insert redirect\_url here\*

Click: **Save**