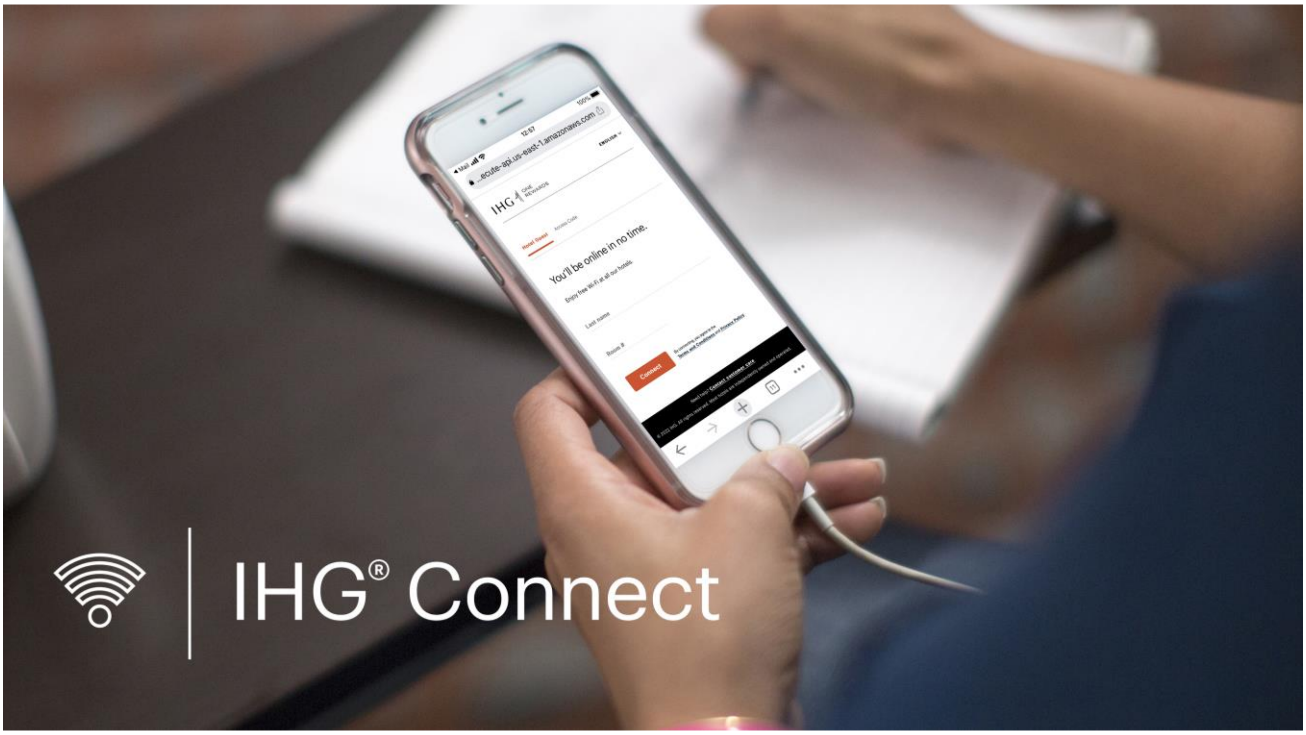
Stay Experience Products
Property, Owner, and Stay Experience (POSE) EMEAA



IHG Connect: Cisco Meraki configuration guide
Version: 4.0 EMEAA

Version Control

Version	Description	Date	Updated by
3.0	▪ Major revision to version 2.3	18th May 2018	Max Sjomin
3.1	▪ Revision page 23	12th July 2018	Max Sjomin
3.2	• Regionalised for EMEAA • Screenshots updated • Dashboard locations updated • New addition: MX Security appliances high availability configuration • RF Profiles added	9th October 2019	Aled Davies Joe Chin
4.0	▪ Rebranded in line with new brand guidelines ▪ Major revisions to configuration guide ▪ New screenshots added ▪ EDGE interface added	December 2022	Joe Chin

1. Introduction

The purpose of the document is to provide the approved IHG Wi-Fi service partners with information needed to configure, manage, and operate a seamless Cisco Meraki network across IHG properties.

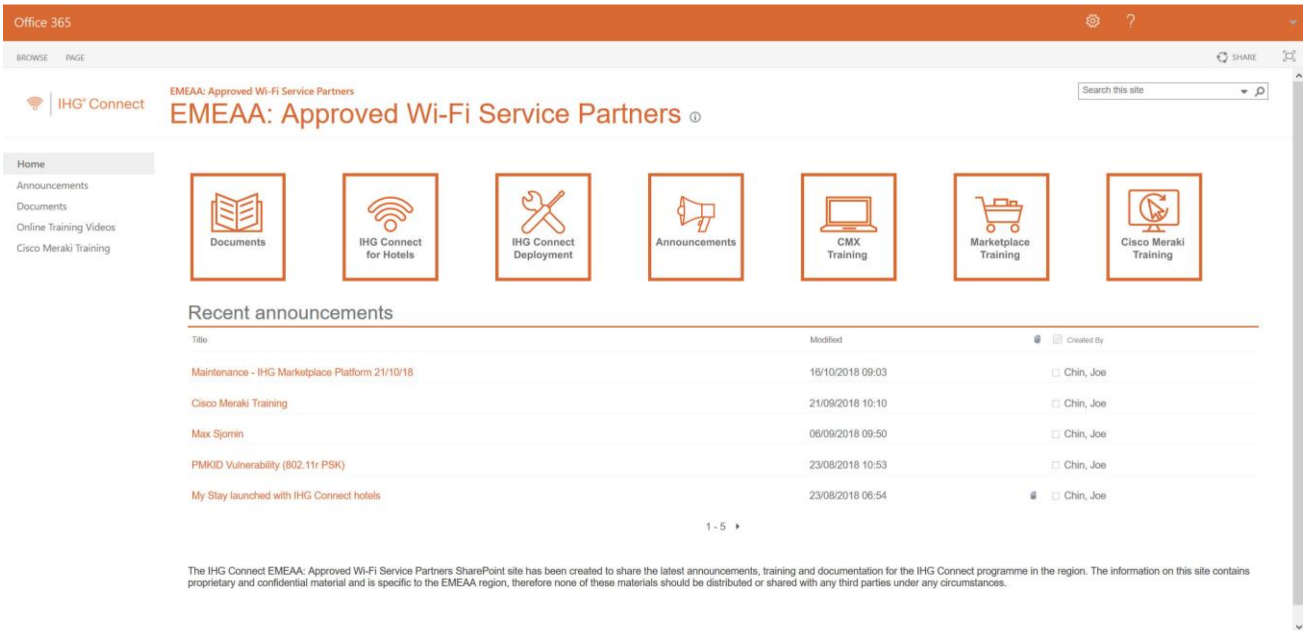
This document details various processes around setting up locations and recommended configuration for the properties.

For help, advice, or assistance with anything in this guide, please contact IHGConnectEMEAA@ihg.com

2. IHG EMEAA network creation process

All partners and hotels must follow the Salesforce process using the IHG Marketplace and the Vendor Portal. **Only** by following this process will a Meraki network be created.

For training and documentation please visit the IHG Connect Approved Wi-Fi Service Partners SharePoint site here or https://ihg.sharepoint.com/sites/euwsps



EMEAA: Approved Wi-Fi Service Partners

EMEAA: Approved Wi-Fi Service Partners

Recent announcements

Title	Modified	Created By
Maintenance - IHG Marketplace Platform 21/10/18	16/10/2018 09:03	Chin, Joe
Cisco Meraki Training	21/09/2018 10:10	Chin, Joe
Max Sjomin	06/09/2018 09:50	Chin, Joe
PMKID Vulnerability (802.11r PSK)	23/08/2018 10:53	Chin, Joe
My Stay launched with IHG Connect hotels	23/08/2018 06:54	Chin, Joe

1 - 5

The IHG Connect EMEAA: Approved Wi-Fi Service Partners SharePoint site has been created to share the latest announcements, training and documentation for the IHG Connect programme in the region. The information on this site contains proprietary and confidential material and is specific to the EMEAA region, therefore none of these materials should be distributed or shared with any third parties under any circumstances.

After you have placed the order for the Meraki hardware, and once the consignment ships you will receive an email from Meraki containing the order number and licence keys; please follow the Marketplace process to request the network set-up. If you require assistance, please email IHGConnectEMEAA@ihg.com

Once the Meraki network is created by IHG, you will be notified by Marketplace and access is automatically granted for the service partner to monitor and start the configuration for the hotel; you can begin the configuration immediately and do not need to wait for the hardware to be delivered.

3. EDGE FIAS Interface

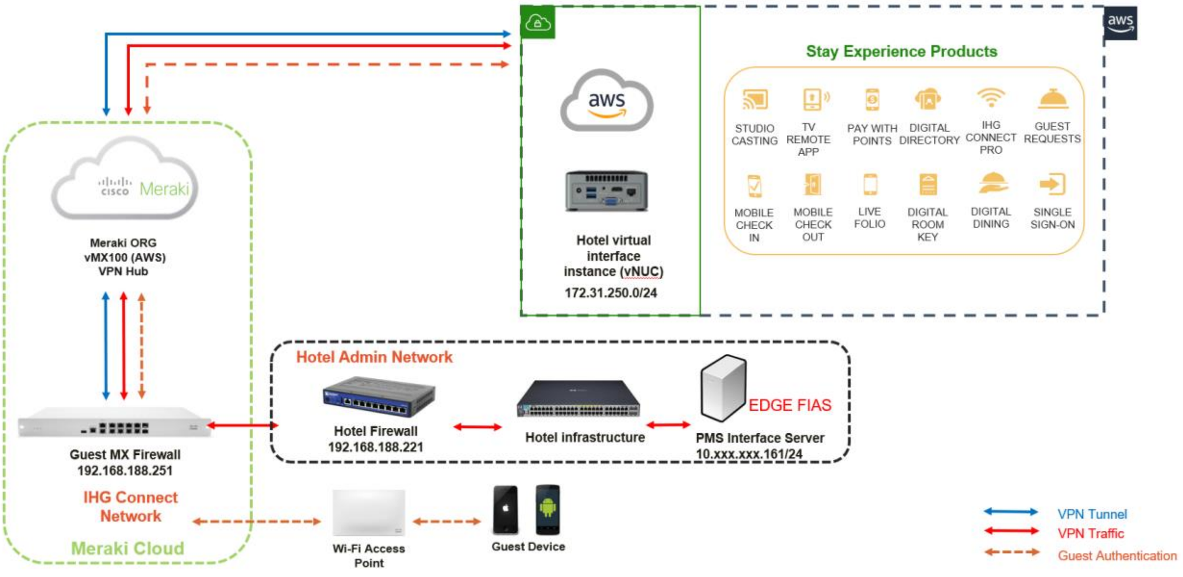
To configure the SSID with the IHG Connect splash page (or Wi-Fi login page), a FIAS interface must be installed in the hotel. **This is a mandatory requirement.**

Summary
The EDGE FIAS interface connects the hotel's Property Management System (PMS) to EDGE services in the AWS cloud. Once connected, guest check-in and check-out messages are sent to the database in AWS. For IHG Connect, this enables the splash page functionality and guest experience.

- Guests can login to the Wi-Fi using their last name and room number.
- IHG ONE REWARDS guests can choose to be remembered and connect automatically on repeat visits or in other IHG Connect Wi-Fi enabled hotels
- Login can also be achieved using an access code.

RADIUS server authentication is enabled on the IHG ONE REWARDS Free WI-FI SSID in the Meraki dashboard and the splash page is configured.

An overview:



To activate the EDGE FIAS interface there are three parts

1. Installation of the FIAS interface.
   This is arranged by the IHG EDGE team. Once the Meraki network task has been completed in IHG Marketplace you should email EDGE.EMEAA@ihg.com and introduce your hotel or IT contact to the team. A PMS licence may be required, along with subnet information to configure services in AWS.

2. Configuration of the IHG Connect network.
   This should be completed by the integration partner as part of the IHG Connect installation. For detailed instructions, please refer to the document IHG EDGE - PMS Interface Hotel Setup guide (EMEAA EDGE Hosted vNUC). You will need to configure VLAN 999 in the Meraki dashboard, assign a port to connect to the admin firewall and add in a static route.

3. Configuration of the admin or back of house firewall.
   The hotel IT or support company should also configure VLAN 999 and configure an interface port on the firewall, add in the required firewall rules and routes and connect the port to the corresponding MX port.

4. Splash page activation
   Once the interface has been installed and all the configuration has been completed, the IHG EDGE team will enable the VPN from the Meraki dashboard to AWS. Once the interface is successfully connected, the team will arrange to activate the splash page.

4. Getting started with the Meraki dashboard

The foundation of any Cisco Meraki network is the Cisco Meraki dashboard – the online management interface that allows administrators to configure, monitor, and manage any Cisco Meraki device from anywhere in the world. The Cisco Meraki dashboard combines the immediacy of on-premise management applications with the simplicity and centralised control of a cloud application.

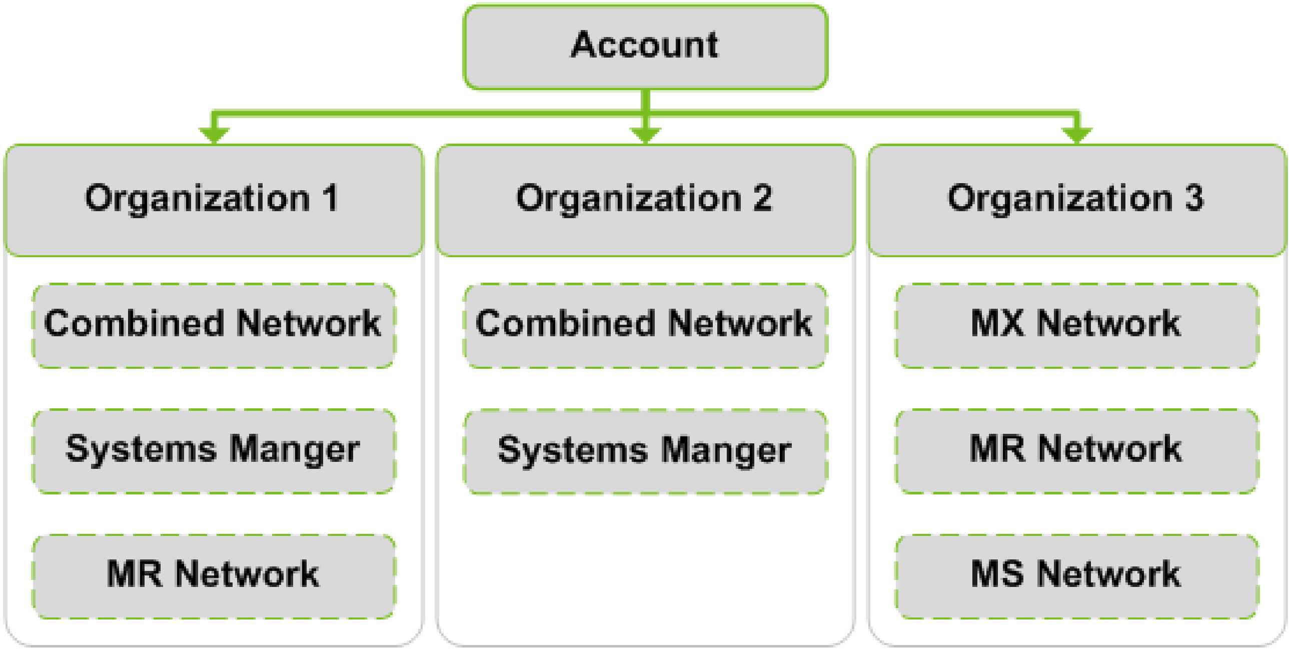
Dashboard Fundamentals

This section covers some basic functionality within the dashboard: the various dashboard views, process around provisioning locations, and dashboard access to the IHG properties.

The basic structure of dashboard consists of two levels:

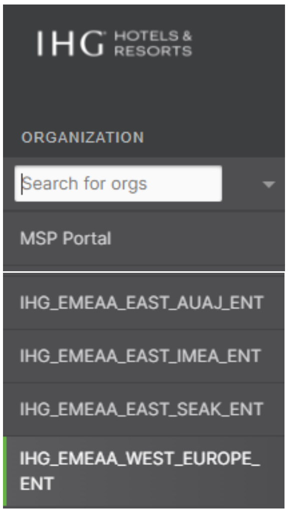
- **Networks (Hotels)** - contains Cisco Meraki devices, their configurations, statistics, and any client-device information. Think of a network as a container for devices, primarily determined by what type of devices it will contain. Multiples of the same network type can exist within an organisation. All IHG Networks are 'Combined Networks' containing MX, MS, and MR devices

- **Organisations** - A collection of networks that are all part of a single organisational entity, such as a company. Administrator accounts can then access multiple organisations and the networks they contain, as long as an account exists in each organisation with the same e-mail address. IHG currently does not allow Integrators Organisational access. Currently, access is restricted to the Networks (Hotels) only



3.1 Access & permissions

When an account has access to multiple organisations, logging into that account will present the administrator with a page where a starting organisation can be selected. Example below:



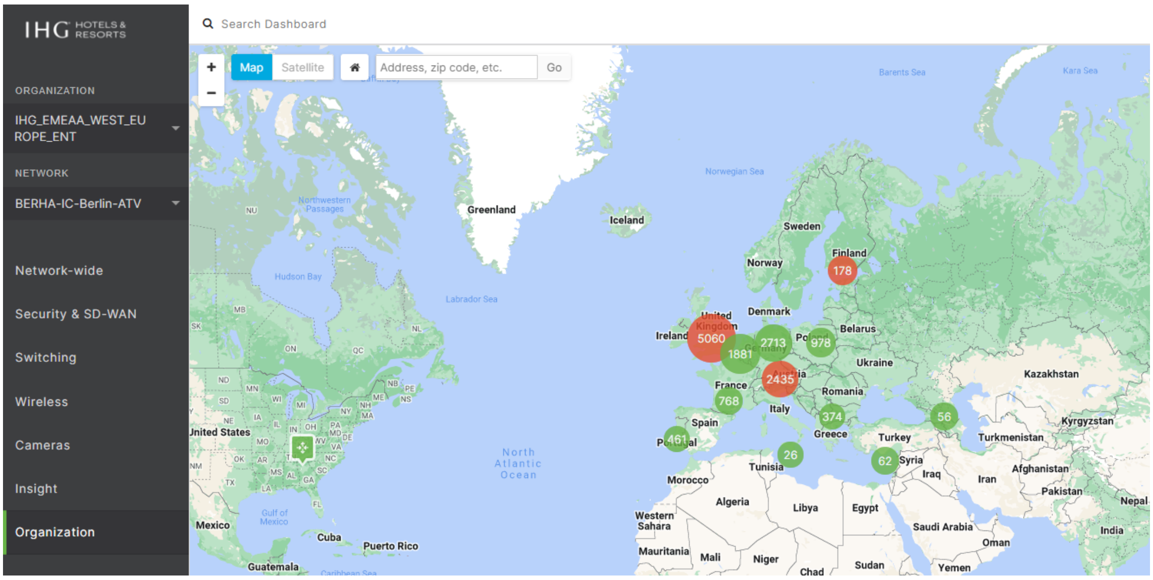
To change organisations later, make selection in the upper left corner of Dashboard.
The access available to each individual network or organisation will be dependent on the permissions configuration.

For more information on permissions, refer to the Meraki article on Managing Administrators

https://documentation.meraki.com/zGeneral_Administration/Managing_Dashboard_Access/Managing_Dashboard_Administrators_and_Permissions

3.2 The organisation view

After an administrator, has created a dashboard account and logged in, a screen similar to the one below will be displayed:



NB: IHG service partners do not have access to the Organization tab.

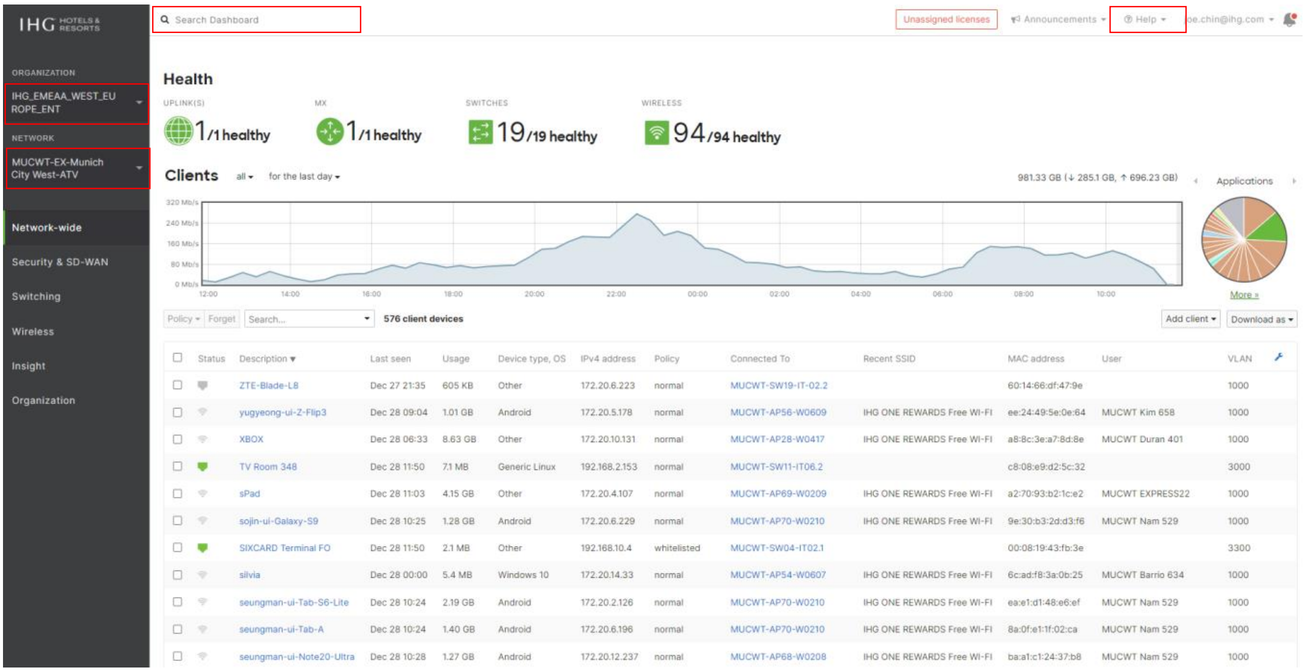
This page is called the **Organization** -> **Overview** page and displays all networks that are running within an organisation.

Within Dashboard there is an idea of organisations and networks. A network is generally thought of as one geographic site. So, for IHG, each hotel would be a network and all of the properties/networks would be a part of an IHG Organisation or ORG.

IHG has an Organisational view to all hotels while the service partners have network (Hotel) level views.

3.3 The network view

Once an administrator selects a particular network, they will be sent to the relevant Health page for that particular hotel or network.



Health

UPLINK(S) 1/1 healthy — MX 1/1 healthy — SWITCHES 19/19 healthy — WIRELESS 94/94 healthy

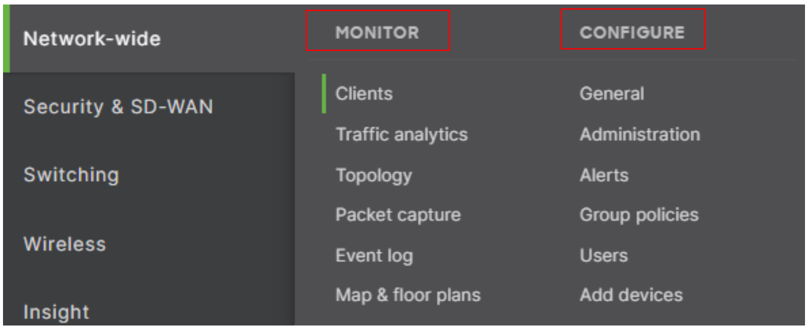
Clients all for the last day — 981.33 GB (↓ 285.1 GB, ↑ 696.23 GB)

576 client devices

Status	Description ▾	Last seen	Usage	Device type, OS	IPv4 address	Policy	Connected To	Recent SSID	MAC address	User	VLAN
	ZTE-Blade-L8	Dec 27 21:35	605 KB	Other	172.20.6.223	normal	MUCWT-SW19-IT-02.2		60:14:66:df:47:9e		1000
	yugyeong-ui-Z-Flip3	Dec 28 09:04	1.01 GB	Android	172.20.5.178	normal	MUCWT-AP56-W0609	IHG ONE REWARDS Free WI-FI	ee:24:49:5e:0e:64	MUCWT Kim 658	1000
	XBOX	Dec 28 06:33	8.63 GB	Other	172.20.10.131	normal	MUCWT-AP28-W0417	IHG ONE REWARDS Free WI-FI	a8:8c:3e:a7:8d:8e	MUCWT Duran 401	1000
	TV Room 348	Dec 28 11:50	7.1 MB	Generic Linux	192.168.2.153	normal	MUCWT-SW11-IT06.2		c8:08:e9:d2:5c:32		3000
	sPad	Dec 28 11:03	4.15 GB	Other	172.20.4.107	normal	MUCWT-AP69-W0209	IHG ONE REWARDS Free WI-FI	a2:70:93:b2:1c:e2	MUCWT EXPRESS22	1000
	sojin-ui-Galaxy-S9	Dec 28 10:25	1.28 GB	Android	172.20.6.229	normal	MUCWT-AP70-W0210	IHG ONE REWARDS Free WI-FI	9e:30:b3:2d:d3:f6	MUCWT Nam 529	1000
	SIXCARD Terminal FO	Dec 28 11:50	2.1 MB	Other	192.168.10.4	whitelisted	MUCWT-SW04-IT02.1		00:08:19:43:fb:3e		3300
	silvia	Dec 28 00:00	5.4 MB	Windows 10	172.20.14.33	normal	MUCWT-AP54-W0607	IHG ONE REWARDS Free WI-FI	6c:ad:f8:3a:0b:25	MUCWT Barrio 634	1000
	seungman-ui-Tab-S6-Lite	Dec 28 10:24	2.19 GB	Android	172.20.2.126	normal	MUCWT-AP70-W0210	IHG ONE REWARDS Free WI-FI	ea:e1:d1:48:e6:ef	MUCWT Nam 529	1000
	seungman-ui-Tab-A	Dec 28 10:24	1.40 GB	Android	172.20.6.196	normal	MUCWT-AP70-W0210	IHG ONE REWARDS Free WI-FI	8a:0f:e1:1f:02:ca	MUCWT Nam 529	1000
	seungman-ui-Note20-Ultra	Dec 28 10:28	1.27 GB	Android	172.20.12.237	normal	MUCWT-AP68-W0208	IHG ONE REWARDS Free WI-FI	ba:a1:c1:24:37:b8	MUCWT Nam 529	1000

Notice in the screenshot that there are six primary tabs to the left side of the screen: Network-wide, Security & SD-WAN, Switching, Wireless, Insight and Organization. These tabs will vary according to the products purchased by the hotel.

The menu list for each tab is usually split into two sections, *Monitor* and *Configure*:



The options under *Monitor* allow you to view features, perform troubleshooting or network analytics and under *Configure*, the ability to change the configuration settings.

The Organization tab allows you to view and change Organisation-wide settings.

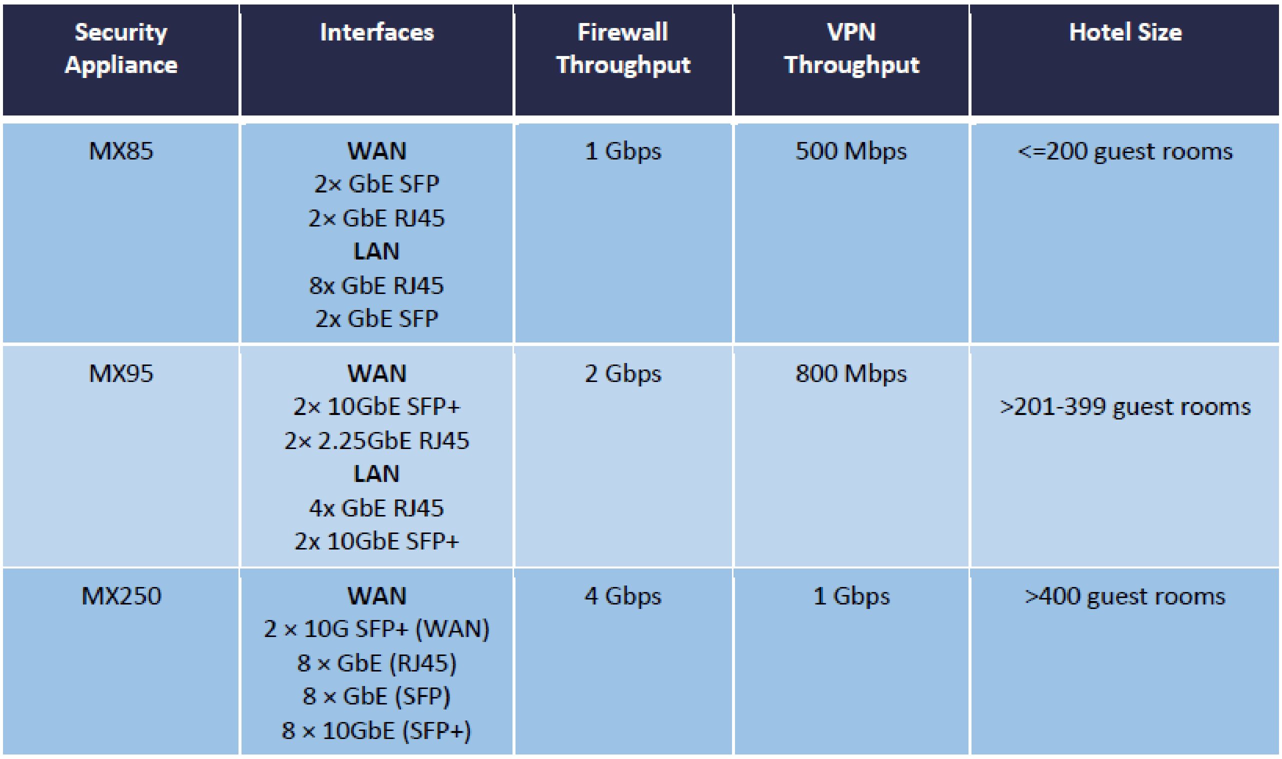
The Help option at the top, allows you to search the Meraki knowledge base.

Finally, there's a search option at the top, giving you the ability to search the dashboard of the selected network for a client device, an AP, switch etc.

5. Configuring the MX security appliance

5.1 IHG Connect MX sizing guide

The latest sizing guide can be found on the IHG Connect Approved Wi-Fi Service Partners SharePoint site here or https://ihg.sharepoint.com/sites/euwsps



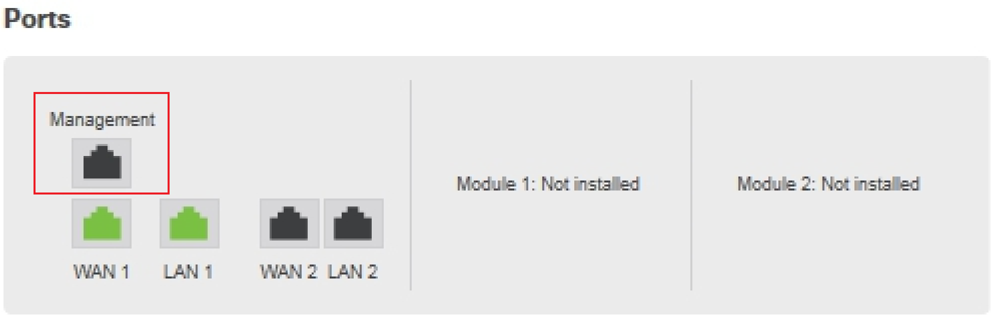
Security Appliance	Interfaces	Firewall Throughput	VPN Throughput	Hotel Size
MX85	**WAN** 2× GbE SFP 2× GbE RJ45 **LAN** 8x GbE RJ45 2x GbE SFP	1 Gbps	500 Mbps	<=200 guest rooms
MX95	**WAN** 2× 10GbE SFP+ 2× 2.25GbE RJ45 **LAN** 4x GbE RJ45 2x 10GbE SFP+	2 Gbps	800 Mbps	>201-399 guest rooms
MX250	**WAN** 2 × 10G SFP+ (WAN) 8 × GbE (RJ45) 8 × GbE (SFP) 8 × 10GbE (SFP+)	4 Gbps	1 Gbps	>400 guest rooms

NB: One enterprise licence is required for two MX firewalls (in a HA pair/warm spare setup).

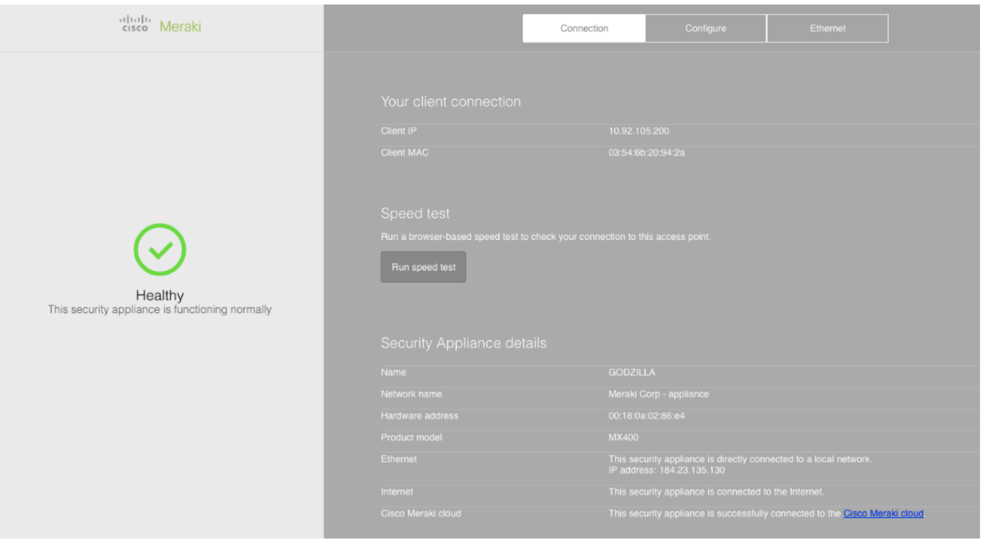
5.2 Local status & configuration

The Meraki MX appliance includes a local status and configuration interface that allows you to view information about WAN connectivity and traffic statistics, as well as apply IP configuration settings to the WAN port(s) and modify the speed and duplex settings of all ports on the appliance.

The first step in making a hotel active is to access the local interface by connecting a computer to the management port of the MX appliance.



You should receive an IP address from DHCP. Once your computer has an IP address, navigate to either http://wired.meraki.com or http://setup.meraki.com in your web browser. This will bring up the status portion of the local interface:



Healthy
This security appliance is functioning normally

Your client connection

Client IP	10.92.105.200
Client MAC	03:54:6b:20:94:2a

Speed test

Run a browser-based speed test to check your connection to this access point.

Security Appliance details

Name	GODZILLA
Network name	Meraki Corp - appliance
Hardware address	00:18:0a:02:86:e4
Product model	MX400
Ethernet	This security appliance is directly connected to a local network. IP address: 184.23.135.130
Internet	This security appliance is connected to the Internet.
Cisco Meraki cloud	This security appliance is successfully connected to the Cisco Meraki cloud.

Next, select the ‘Configure’ tab at the top of the screen and statically assign an available public WAN IP Address to the Internet 1 interface. If there are two Internet connections terminating on the MX, toggle LAN 2 to Internet 2 and statically set the secondary public WAN IP address to Internet 2.

5.3 MX security appliance naming convention

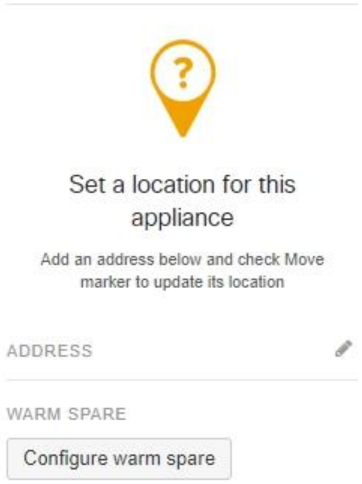
Configure name for each MX security appliance using naming convention as per example below:

Hotel Code – SA Security Appliance – Appliance Number

```
Primary: BERHA-SA-01
Spare:   BERHA-SA-02
```

NB, naming conventions must be limited to 40 characters and contain only:
Alphabet: A-Z (no special alphabet characters like á é í ó ú ü ä ö ñ etc. are allowed either)
Numeric: 0-9
Special characters: / - _ ( ) [ ]

Please navigate to **Security & SD-WAN -> Monitor -> Appliance Status**



Set a location for this appliance

Add an address below and check Move marker to update its location

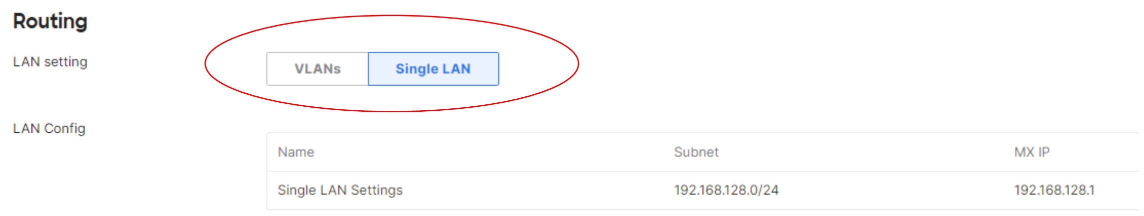
5.4 Addressing & VLANs configuration

1. VLANs 2000 and below are reserved for IHG use. Currently 100, 999, 1000 and 1050.
2. Guest/Integrator networks should use 192.168.128.0/17 which allows integrators to use 192.168.128.1 through 192.168.255.254. IHG reserves 10.0.0.0/8, 172.16.0.0/10 and 192.168.188.0/24 subnets as we are currently using them.

To enable and configure VLANs and IP addressing schemes, first browse to the appropriate network using the drop-down box at the top of the dashboard.
To enable VLANs:

Navigate to **Security & SD-WAN -> Configure -> Addressing & VLANs**

Under the option *Routing*, under the LAN setting, select VLANs



Routing

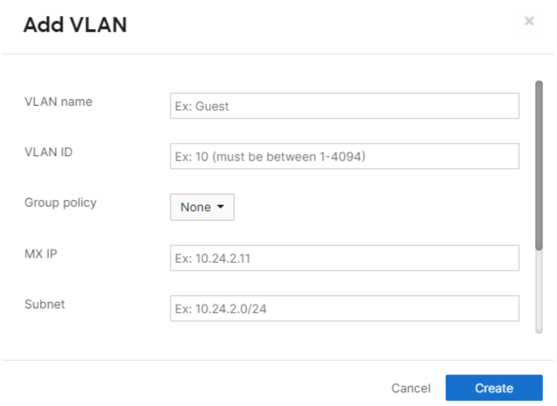
LAN setting: VLANs | Single LAN

LAN Config

Name	Subnet	MX IP
Single LAN Settings	192.168.128.0/24	192.168.128.1

NB: The option for Single VLAN is enabled by default.

After VLANs have been enabled you can add additional ones by clicking 'Add VLAN'.



Add VLAN

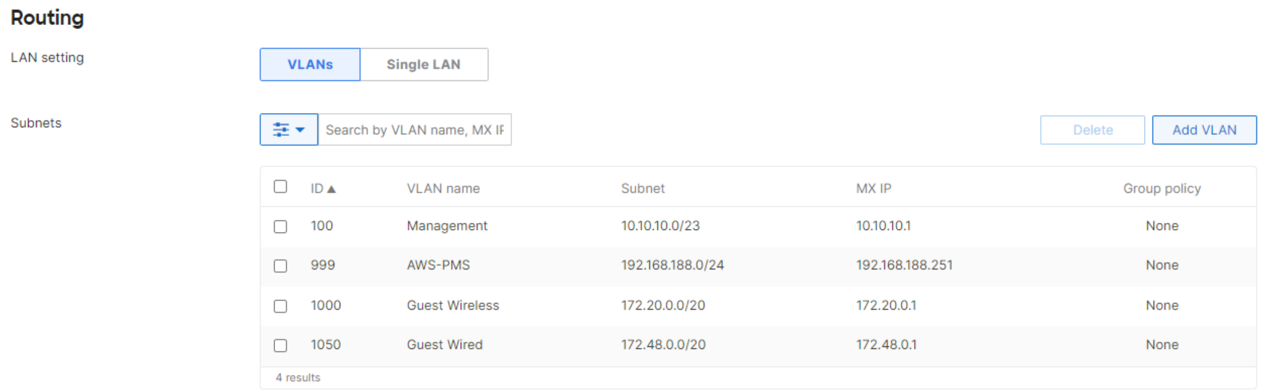
VLAN name	Ex: Guest
VLAN ID	Ex: 10 (must be between 1-4094)
Group policy	None ▾
MX IP	Ex: 10.24.2.11
Subnet	Ex: 10.24.2.0/24

The Name is a description of the VLAN, the VLAN ID is the VLAN number, the Subnet is the network expressed using CIDR notation, and the Appliance LAN IP is the local MX VLAN interface IP.

A VLAN can be removed by checking the appropriate box and selecting delete.

Click here or https://documentation.meraki.com/MX-Z/Networks_and_Routing/Configuring_VLANs_on_the_MX_Security_Appliance for more detailed information about settings on Addressing & VLANs.

1. Navigate to **Security & SD-WAN -> Configure -> Addressing & VLANs**
2. Select Add a Local VLAN and add the following:
3. VLAN 100 for Management (IHG Standard)
4. VLAN 999 for AWS-PMS (IHG Standard for EDGE)
5. VLAN 1000 for Guest Wireless (IHG Standard)
6. VLAN 1050 for Guest Wired (IHG Standard)



Routing

LAN setting

Subnets

	ID ▲	VLAN name	Subnet	MX IP	Group policy
☐	100	Management	10.10.10.0/23	10.10.10.1	None
☐	999	AWS-PMS	192.168.188.0/24	192.168.188.251	None
☐	1000	Guest Wireless	172.20.0.0/20	172.20.0.1	None
☐	1050	Guest Wired	172.48.0.0/20	172.48.0.1	None

4 results

IP addressing

Subnet	VLAN	Name
10.10.10.0/23	100	Management
192.168.188.0/24	999	EDGE-PMS
172.20.0.0/20	1000	Guest Wireless
172.48.0.0/20	1050	Guest Wired

Please use the following guide for the IP addressing scheme for any additional subnets/network services:

Netmask: 255.255.240.0 = 20 **Wildcard: 0.0.15.255**	**Netmask: 255.255.254.0 = 23** **Wildcard: 0.0.1.255**	**Netmask: 255.255.255.0 = 24** **Wildcard: 0.0.0.255**
Network: 192.168.128.0/20 Broadcast: 192.168.143.255 Host Min: 192.168.128.1 Host Max: 192.168.143.254 **Hosts/Net: 4094 (VLAN 3128)**	Network: 192.168.192.0/23 Broadcast: 192.168.193.255 Host Min: 192.168.192.1 Host Max: 192.168.193.254 **Hosts/Net: 510 (VLAN 3192)**	Network: 192.168.200.0/24 Broadcast: 192.168.200.255 Host Min: 192.168.200.1 Host Max: 192.168.200.254 **Hosts/Net: 254 (VLAN 3200)**
Network: 192.168.144.0/20 Broadcast: 192.168.159.255 Host Min: 192.168.144.1 Host Max: 192.168.159.254 **Hosts/Net: 4094 (VLAN 3144)**	Network: 192.168.194.0/23 Broadcast: 192.168.195.255 Host Min: 192.168.194.1 Host Max: 192.168.195.254 **Hosts/Net: 510 (VLAN 3194)**	Network: 192.168.201.0/24 Broadcast: 192.168.201.255 Host Min: 192.168.201.1 Host Max: 192.168.201.254 **Hosts/Net: 254 (VLAN 3201)**
Network: 192.168.160.0/20 Broadcast: 192.168.175.255 Host Min: 192.168.160.1 Host Max: 192.168.175.254 **Hosts/Net: 4094 (VLAN 3160)**	Network: 192.168.196.0/23 Broadcast: 192.168.197.255 Host Min: 192.168.196.1 Host Max: 192.168.197.254 **Hosts/Net: 510 (VLAN 3196)**	Network: 192.168.202.0/24 Broadcast: 192.168.202.255 Host Min: 192.168.202.1 Host Max: 192.168.202.254 **Hosts/Net: 254 (VLAN 3202)**
	Network: 192.168.198.0/23 Broadcast: 192.168.199.255 Host Min: 192.168.198.1 Host Max: 192.168.199.254 **Hosts/Net: 510 (VLAN 3198)**	Network: 192.168.203.0/24 Broadcast: 192.168.203.255 Host Min: 192.168.203.1 Host Max: 192.168.203.254 **Hosts/Net: 254 (VLAN 3203)**

NB: The voice VLAN tag must be removed from the phone when a MR30H/MR36H or MR36H access point (port 1) is being used to connect IP phones in the guest rooms.

5.5 MX per port VLAN configuration

1. Navigate to **Security & SD-WAN -> Configure -> Addressing & VLANs**
2. Scroll down to Per-port VLAN Settings

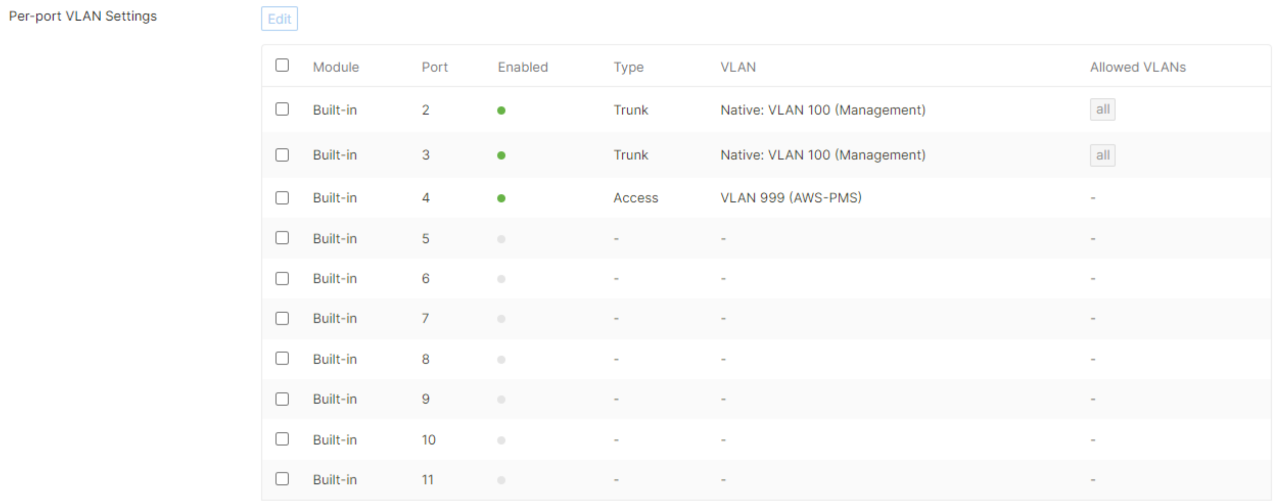
The uplink ports to the switches will be configured as a trunk port to carry the VLANs that were configured in the previous step. Changes can be made to the MX LAN ports under **Per-port VLAN configuration** by selecting the check box beside the port number or by selecting multiple ports and clicking the **Edit** button.

NB: some ports are used for internet connections and will not be displayed in the per-port VLAN settings; this is dependent on the model of MX device.

3. Select the port or multiple ports using the check box and clicking edit
4. Ensure a Native VLAN is defined for each active port
5. Specify a port for the EDGE interface and assign VLAN 999
6. As a security measure, all other ports must be disabled

The **Type** determines if the LAN port is an access or trunk port. When connecting the MX to a switch that will carry multiple VLANs select trunk from the drop-down list. Traffic without an 802.1Q tag will be dropped by default unless a native VLAN is defined from the Native VLAN field.

You can specify specific VLANs that the trunk port will allow from **Allowed VLANs** or choose to allow all VLANs to pass on the link. Click here or https://documentation.meraki.com/MX-Z/Networks_and_Routing/Configuring_VLANs_on_the_MX_Security_Appliance for more information about per-port VLAN configuration options.



Per-port VLAN Settings

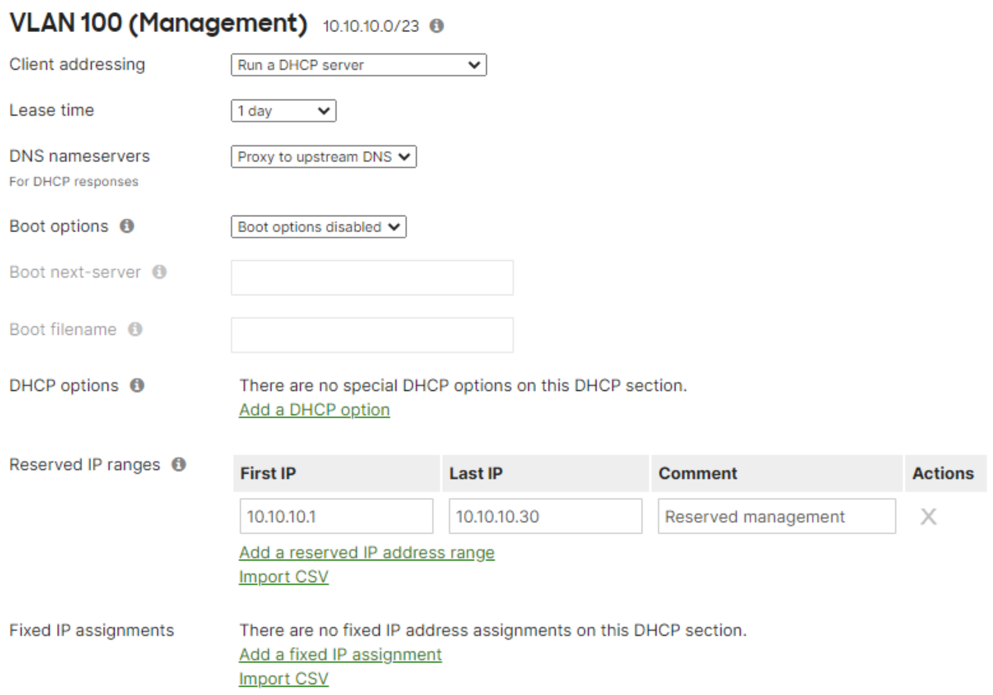
□	Module	Port	Enabled	Type	VLAN	Allowed VLANs
□	Built-in	2	●	Trunk	Native: VLAN 100 (Management)	all
□	Built-in	3	●	Trunk	Native: VLAN 100 (Management)	all
□	Built-in	4	●	Access	VLAN 999 (AWS-PMS)	-
□	Built-in	5	○	-	-	-
□	Built-in	6	○	-	-	-
□	Built-in	7	○	-	-	-
□	Built-in	8	○	-	-	-
□	Built-in	9	○	-	-	-
□	Built-in	10	○	-	-	-
□	Built-in	11	○	-	-	-

5.6 DHCP configuration

To configure DHCP on the MX Security Appliance, navigate to
Security & SD-WAN -> Configure -> DHCP, and refer to the section for the desired VLAN/subnet.

MX devices and switches should have static IP addresses assigned in reserved range VLAN 100. If more than 30 addresses are required, then increase the reserved range accordingly.
Access points will use DHCP in VLAN 100.

Configure VLAN 100, 999, 1000 and 1050 as per the screenshots below:



VLAN 100 (Management) 10.10.10.0/23

Client addressing: Run a DHCP server

Lease time: 1 day

DNS nameservers
For DHCP responses: Proxy to upstream DNS

Boot options: Boot options disabled

Boot next-server:

Boot filename:

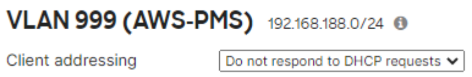
DHCP options: There are no special DHCP options on this DHCP section.
Add a DHCP option

Reserved IP ranges:

First IP	Last IP	Comment	Actions
10.10.10.1	10.10.10.30	Reserved management	X

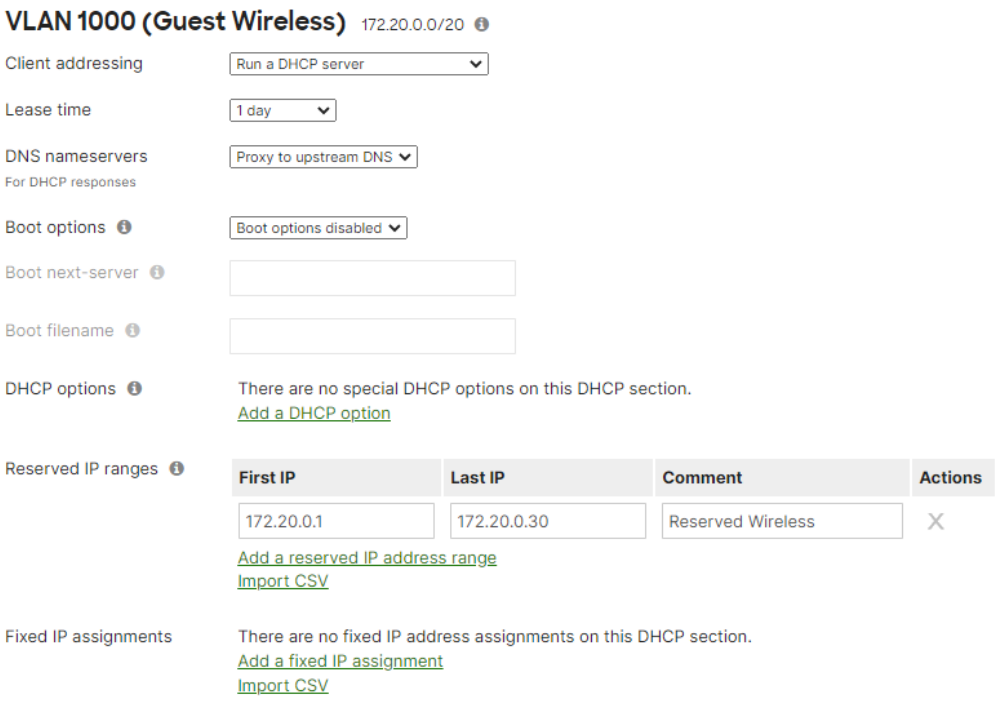
Add a reserved IP address range
Import CSV

Fixed IP assignments: There are no fixed IP address assignments on this DHCP section.
Add a fixed IP assignment
Import CSV



VLAN 999 (AWS-PMS) 192.168.188.0/24

Client addressing: Do not respond to DHCP requests



VLAN 1000 (Guest Wireless) 172.20.0.0/20

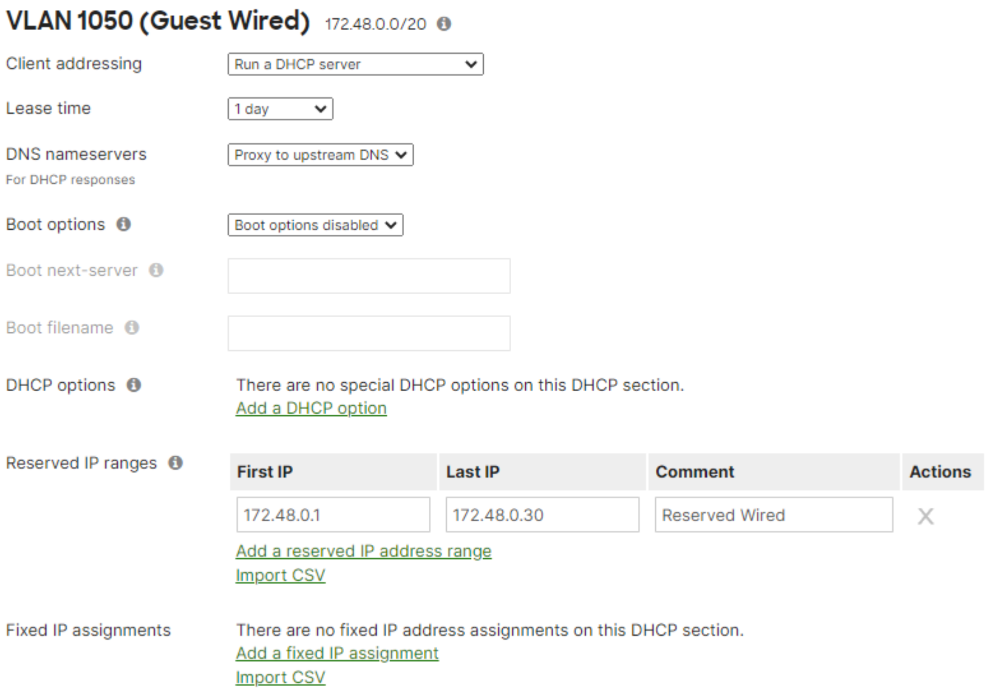
Client addressing	Run a DHCP server
Lease time	1 day
DNS nameservers For DHCP responses	Proxy to upstream DNS
Boot options	Boot options disabled
Boot next-server	
Boot filename	
DHCP options	There are no special DHCP options on this DHCP section. Add a DHCP option

Reserved IP ranges

First IP	Last IP	Comment	Actions
172.20.0.1	172.20.0.30	Reserved Wireless	X

Add a reserved IP address range
Import CSV

Fixed IP assignments: There are no fixed IP address assignments on this DHCP section.
Add a fixed IP assignment
Import CSV



VLAN 1050 (Guest Wired) 172.48.0.0/20

Client addressing	Run a DHCP server
Lease time	1 day
DNS nameservers For DHCP responses	Proxy to upstream DNS
Boot options	Boot options disabled
Boot next-server	
Boot filename	
DHCP options	There are no special DHCP options on this DHCP section. Add a DHCP option

Reserved IP ranges

First IP	Last IP	Comment	Actions
172.48.0.1	172.48.0.30	Reserved Wired	X

Add a reserved IP address range
Import CSV

Fixed IP assignments: There are no fixed IP address assignments on this DHCP section.
Add a fixed IP assignment
Import CSV

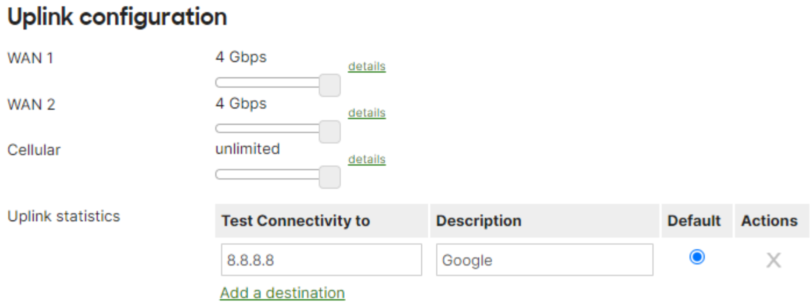
Click **Save.**

5.7 WAN load sharing

The MX Security Appliance has two uplinks with a tertiary cellular uplink capability. On the MX, link aggregation can be enabled to use both uplinks for all traffic.

By default, link aggregation is disabled and all traffic will use the primary uplink (defaults to Internet/WAN 1) to forward traffic to the internet unless it is overridden by an uplink preference. The uplink will only fail over to the secondary uplink in the event that the primary uplink can no longer reach the internet.

These settings can be changed in **Security & SD-WAN -> Configure -> SD-WAN & Traffic Shaping**



Uplink configuration

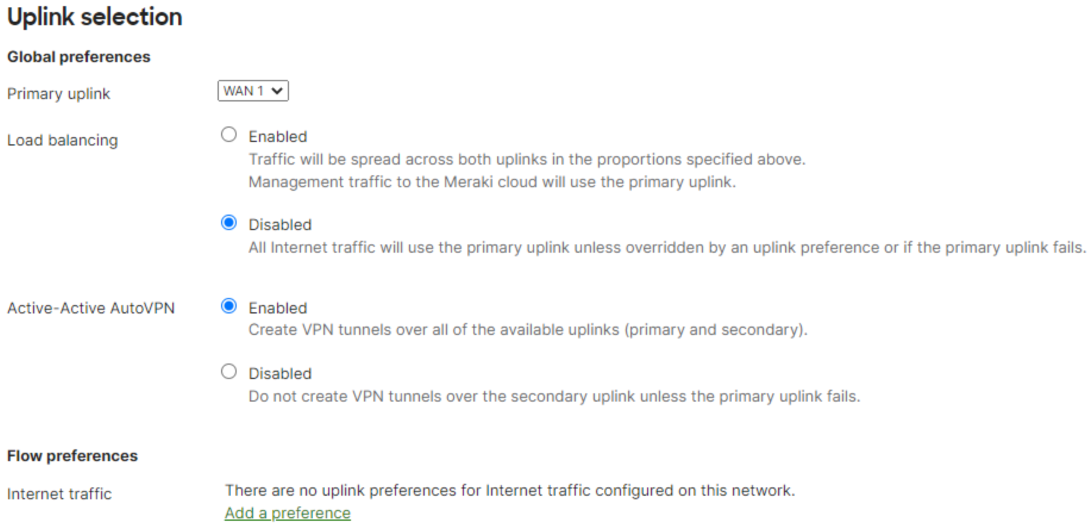
WAN 1	4 Gbps	details
WAN 2	4 Gbps	details
Cellular	unlimited	details

Uplink statistics

Test Connectivity to	Description	Default	Actions
8.8.8.8	Google	●	X

Add a destination

NB: The first LAN port of MX devices without a dedicated Internet/WAN 2 port can be toggled between **LAN** *and* **Internet***, through* **Uplink configuration** *tab on the* **Local status** page*.*



Uplink selection

Global preferences

Primary uplink: WAN 1

Load balancing:
○ Enabled
Traffic will be spread across both uplinks in the proportions specified above.
Management traffic to the Meraki cloud will use the primary uplink.
● Disabled
All Internet traffic will use the primary uplink unless overridden by an uplink preference or if the primary uplink fails.

Active-Active AutoVPN:
● Enabled
Create VPN tunnels over all of the available uplinks (primary and secondary).
○ Disabled
Do not create VPN tunnels over the secondary uplink unless the primary uplink fails.

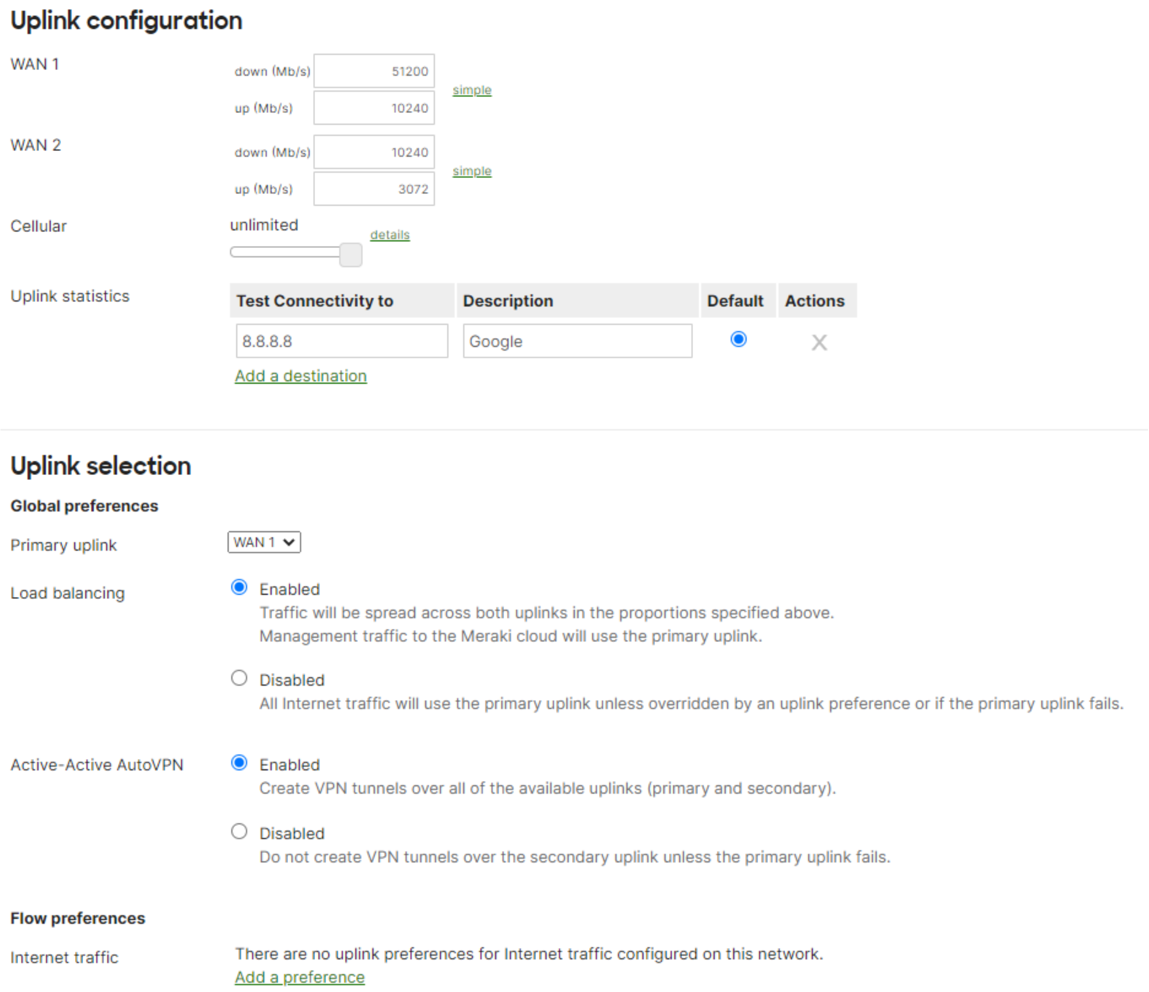
Flow preferences

Internet traffic: There are no uplink preferences for Internet traffic configured on this network.
Add a preference

Ensure that the radio button is set to 'Enabled' to turn on link aggregation and either adjust the slider bars or set the configuration manually by clicking the details link next to the side bar.

to the speeds supported by each uplink, of manually add a specific number to the uplinks in Mbps by clicking on the 'Details' button just to the right of the slider. The MX will now distribute data streams to each uplink in the ratio specified by the slider bars.

For example, if uplink 1 is set to 50Mbps down and 10 Mbps up whereas uplink 2 has 10Mbps down and 3 Mbps up, then for every 6 data streams 5 would go over uplink 1 and 1 stream would go over uplink 2.



Uplink configuration

WAN 1 — down (Mb/s) 51200, up (Mb/s) 10240 — simple

WAN 2 — down (Mb/s) 10240, up (Mb/s) 3072 — simple

Cellular — unlimited — details

Uplink statistics

Test Connectivity to	Description	Default	Actions
8.8.8.8	Google	●	×

Add a destination

Uplink selection

Global preferences

Primary uplink: WAN 1

Load balancing

● Enabled
Traffic will be spread across both uplinks in the proportions specified above.
Management traffic to the Meraki cloud will use the primary uplink.

○ Disabled
All Internet traffic will use the primary uplink unless overridden by an uplink preference or if the primary uplink fails.

Active-Active AutoVPN

● Enabled
Create VPN tunnels over all of the available uplinks (primary and secondary).

○ Disabled
Do not create VPN tunnels over the secondary uplink unless the primary uplink fails.

Flow preferences

Internet traffic: There are no uplink preferences for Internet traffic configured on this network.
Add a preference

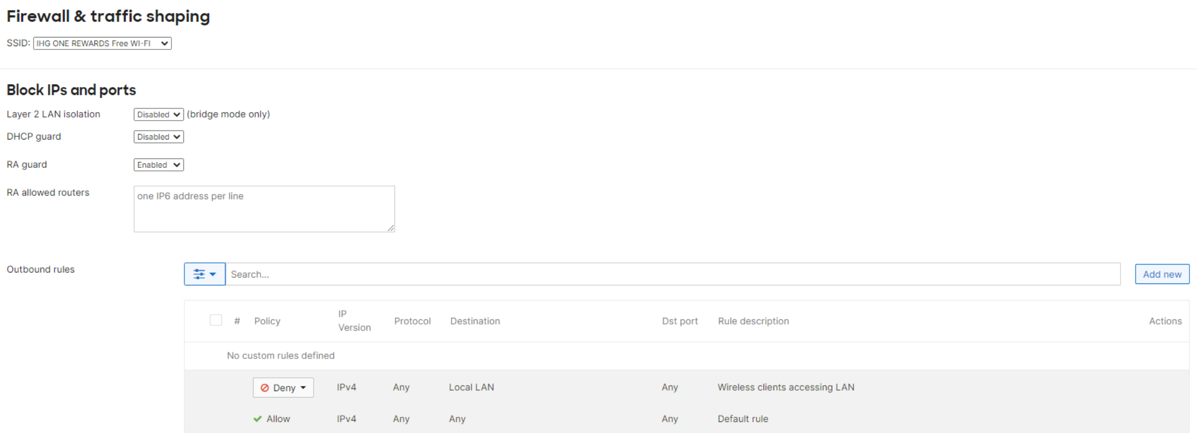
Flow preferences supersede the ratio defined for link aggregation. The MX first checks to see if the stream satisfies the conditions defined by the uplink rules sequentially. If it does, it sends the data out over the uplink defined by the rule, if it does not then it relegates the stream to the link aggregation ratio.

When aggregation is enabled, clients are not restricted to using a single uplink at a time. The traffic is divvied out on a per connection basis, so a client may have one connection go over Internet 1 and another connection go over Internet 2. Because the router doesn't know how much traffic each connection will use, it treats them all equally when spreading them over the internet uplinks even though some connections may end up using more traffic than others. Therefore, if there are only one or two high bandwidth connections, then it's possible that they may get put on the slower link, so the slower link would be using more bandwidth than the faster link. It is not recommended to use WAN aggregation when the links have very different bandwidths. Example: 100MB circuit 1, 10MB circuit 2.

5.8 Firewall & traffic shaping per client

Navigate to Wireless > Configure > Firewall & traffic shaping.

Select the SSID from drop down menu “IHG ONE REWARDS Free WI-FI”
Add a Deny Policy (Wireless clients accessing LAN) in the Outbound rules Section.



Firewall & traffic shaping

SSID: IHG ONE REWARDS Free WI-FI

Block IPs and ports

Layer 2 LAN isolation: Disabled (bridge mode only)

DHCP guard: Disabled

RA guard: Enabled

RA allowed routers: one IP6 address per line

Outbound rules

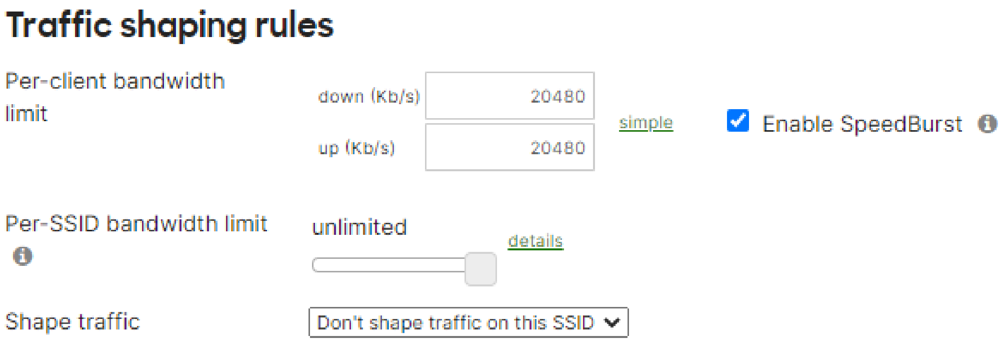
□	#	Policy	IP Version	Protocol	Destination	Dst port	Rule description	Actions
		No custom rules defined						
		⊘ Deny	IPv4	Any	Local LAN	Any	Wireless clients accessing LAN	
		✓ Allow	IPv4	Any	Any	Any	Default rule	

Traffic shaping rules

Bandwidth limits must be applied per client on each client device’s total network traffic (incoming / outgoing). The minimum limit on the throughput is 20 kb/s. Click **Details** or **Simple** to switch between two possible modes:

- **Simple**: Single setting that applies to both upload and download traffic throughput. Move the slider control right or left to set the limits.
- **Details**: Allows you to set different limits on upload and download throughput. Enter the limits manually in kb/s. You can also use this mode to create more-precise per-client limits than in simple mode.

Set the Per-client bandwidth to 20 Mbps (20480 Kb/s) and check the box Enable **SpeedBurst**.
Enabling SpeedBurst will allow guests a better user experience during periods when bandwidth is available.



Traffic shaping rules

Per-client bandwidth limit: down (Kb/s) 20480, up (Kb/s) 20480 ☑ Enable SpeedBurst

Per-SSID bandwidth limit: unlimited

Shape traffic: Don't shape traffic on this SSID

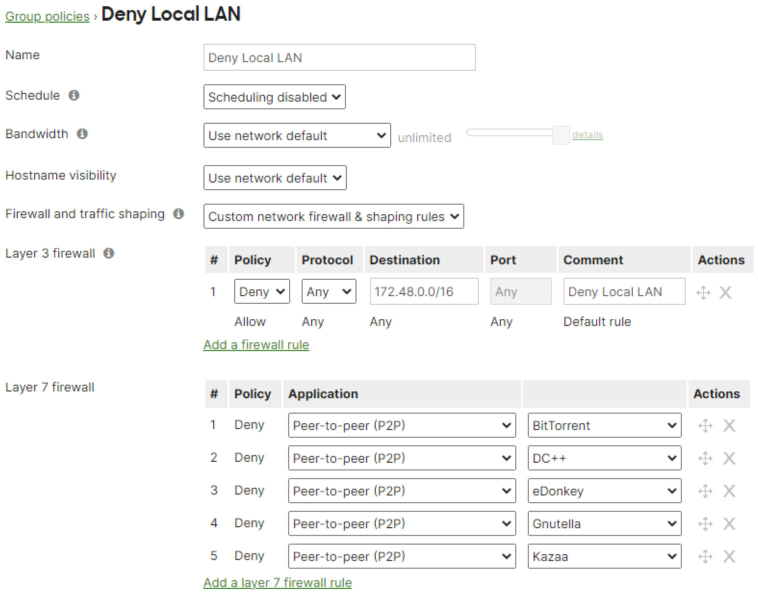
DO NOT limit the Per-SSID bandwidth limit or activate the Shape traffic option.

5.9 Group policies L3 firewall rules for wired & wireless clients

Group policies define a list of rules, restrictions, and other settings, that can be applied to devices to change how they are treated by the network. Group policies can be used on wireless and security appliance networks and can be applied through several manual and automated methods. We are going to create group policies to apply Layer 3 Firewall rules on a per VLAN basis to deny communication between clients on the Guest Network.

1. Navigate to **Network-wide -> Configure -> Group policies**
2. Click **Add a group** and create two new policies Deny Local LAN and Deny Local WLAN
3. Scroll down to Firewall and traffic shaping and select **Custom network firewall & shaping rules**
4. Create a Layer 3 Firewall policy denying access to any destination containing IP Addresses obtained by LAN guests clients on the network as per the below:

Create two Group Policies, Deny Local LAN and Deny Local WLAN. Set the Layer 3 Firewall policy denying access to any destination containing IP Addresses obtained by WLAN guests clients on the network and add Layer 7 firewall rules to block P2P applications like in the examples below.



Group policies › **Deny Local LAN**

Name	Deny Local LAN
Schedule	Scheduling disabled
Bandwidth	Use network default — unlimited — details
Hostname visibility	Use network default
Firewall and traffic shaping	Custom network firewall & shaping rules

Layer 3 firewall

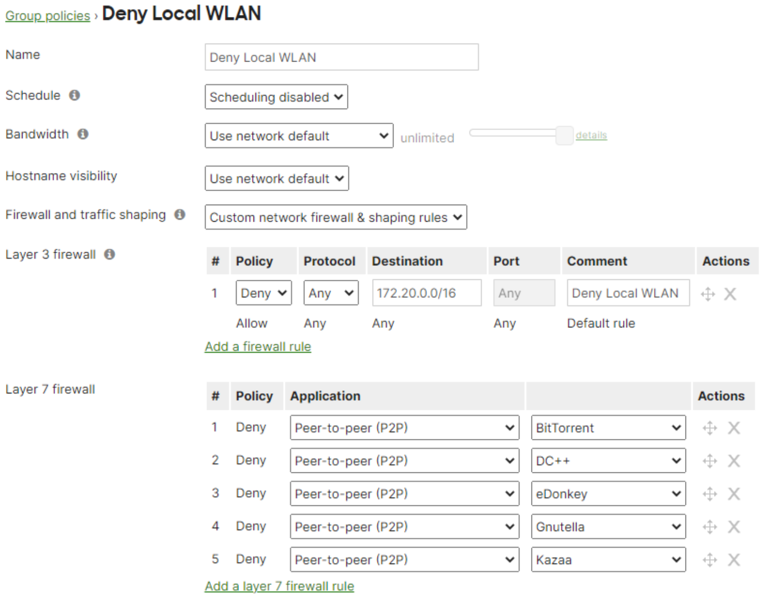
#	Policy	Protocol	Destination	Port	Comment	Actions
1	Deny	Any	172.48.0.0/16	Any	Deny Local LAN	✥ ✕
	Allow	Any	Any	Any	Default rule	

Add a firewall rule

Layer 7 firewall

#	Policy	Application		Actions
1	Deny	Peer-to-peer (P2P)	BitTorrent	✥ ✕
2	Deny	Peer-to-peer (P2P)	DC++	✥ ✕
3	Deny	Peer-to-peer (P2P)	eDonkey	✥ ✕
4	Deny	Peer-to-peer (P2P)	Gnutella	✥ ✕
5	Deny	Peer-to-peer (P2P)	Kazaa	✥ ✕

Add a layer 7 firewall rule



Group policies › **Deny Local WLAN**

Name	Deny Local WLAN
Schedule	Scheduling disabled
Bandwidth	Use network default — unlimited — details
Hostname visibility	Use network default
Firewall and traffic shaping	Custom network firewall & shaping rules

Layer 3 firewall

#	Policy	Protocol	Destination	Port	Comment	Actions
1	Deny	Any	172.20.0.0/16	Any	Deny Local WLAN	✥ ✕
	Allow	Any	Any	Any	Default rule	

Add a firewall rule

Layer 7 firewall

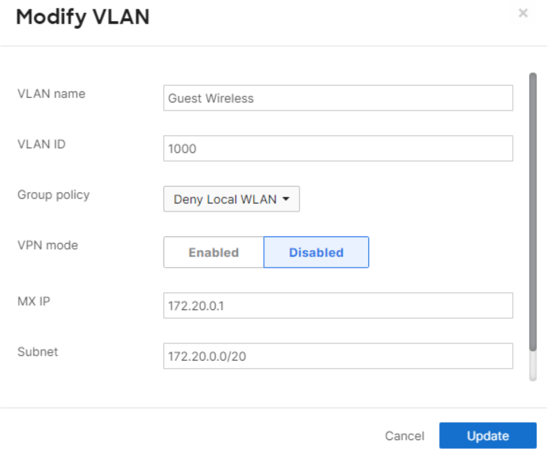
#	Policy	Application		Actions
1	Deny	Peer-to-peer (P2P)	BitTorrent	✥ ✕
2	Deny	Peer-to-peer (P2P)	DC++	✥ ✕
3	Deny	Peer-to-peer (P2P)	eDonkey	✥ ✕
4	Deny	Peer-to-peer (P2P)	Gnutella	✥ ✕
5	Deny	Peer-to-peer (P2P)	Kazaa	✥ ✕

Add a layer 7 firewall rule

Next, we need to add the group policies to the appropriate VLAN.

Navigate to **Security & SD-WAN-> Configure -> Addressing and VLANs**

Select VLAN 1000 and apply the Deny Local WLAN policy, and update.



Modify VLAN

VLAN name: Guest Wireless

VLAN ID: 1000

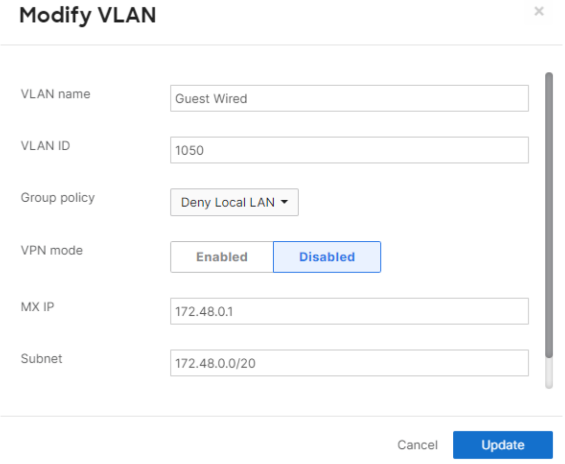
Group policy: Deny Local WLAN

VPN mode: Disabled

MX IP: 172.20.0.1

Subnet: 172.20.0.0/20

Do the same for VLAN 1050 and apply the Deny Local LAN policy and update/save.



Modify VLAN

VLAN name: Guest Wired

VLAN ID: 1050

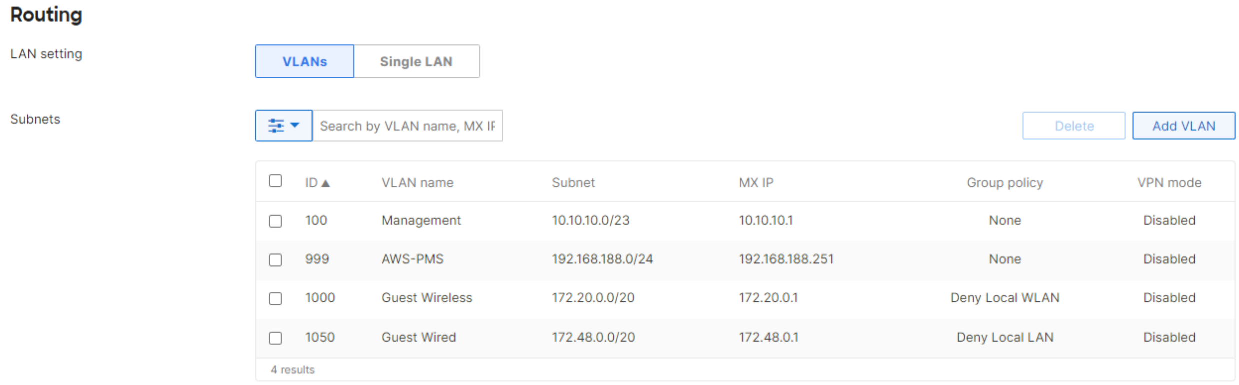
Group policy: Deny Local LAN

VPN mode: Disabled

MX IP: 172.48.0.1

Subnet: 172.48.0.0/20

You’ll notice that the group policies have been added to the VLANs.



Routing

LAN setting: VLANs

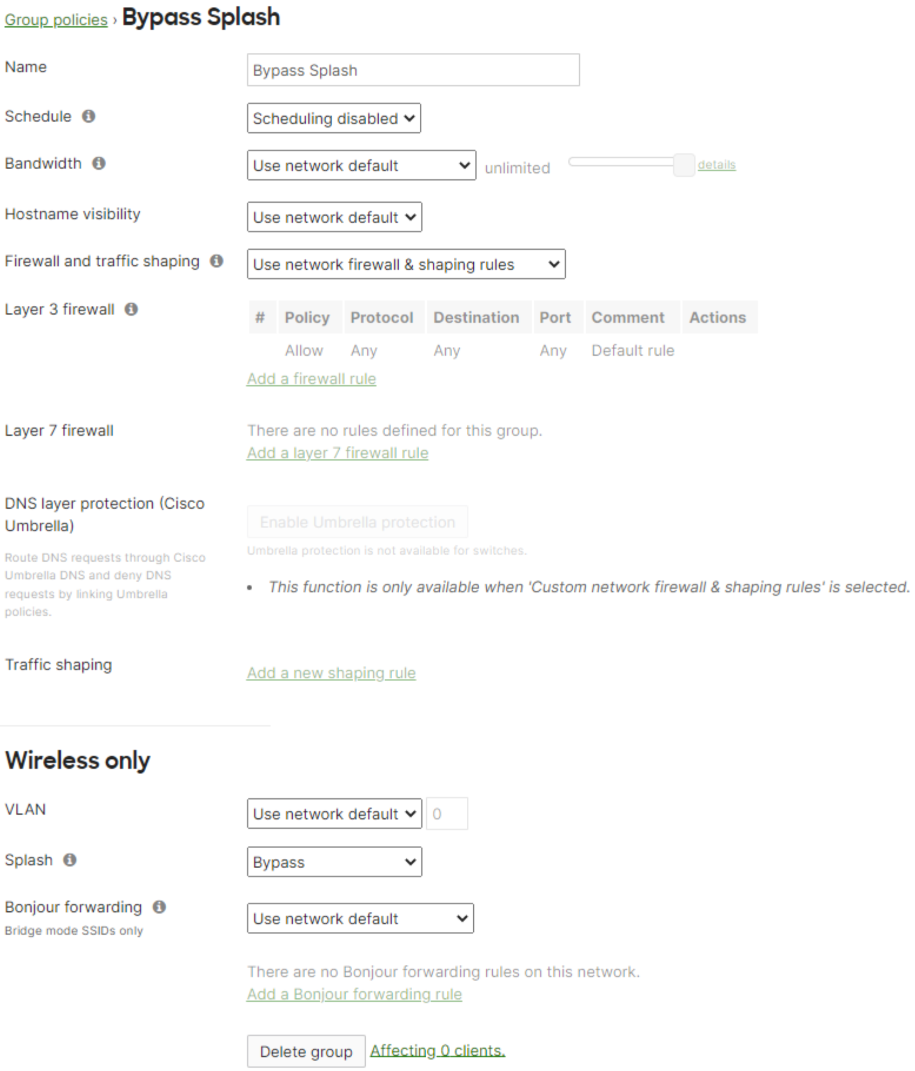
Subnets

	ID ▲	VLAN name	Subnet	MX IP	Group policy	VPN mode
☐	100	Management	10.10.10.0/23	10.10.10.1	None	Disabled
☐	999	AWS-PMS	192.168.188.0/24	192.168.188.251	None	Disabled
☐	1000	Guest Wireless	172.20.0.0/20	172.20.0.1	Deny Local WLAN	Disabled
☐	1050	Guest Wired	172.48.0.0/20	172.48.0.1	Deny Local LAN	Disabled

4 results

From a guest perspective, there may be instances when a certain device cannot connect to the Wi-Fi as it may not have browser functionality to initiate the login. Therefore, we need to create another group policy which can be applied to a guest device, like an Xbox for example, which will give them connectivity while adhering to configured firewall and traffic shaping rules. We never *Whitelist* devices as we relinquish all control over them.

1. Navigate to **Network-wide -> Configure -> Group policies**
2. Click *Add a group* to create a new policy
3. Name it Bypass Splash, then scroll down to the Wireless only section and change Splash to Bypass.



Group policies › **Bypass Splash**

Name	Bypass Splash
Schedule	Scheduling disabled
Bandwidth	Use network default — unlimited — details
Hostname visibility	Use network default
Firewall and traffic shaping	Use network firewall & shaping rules

Layer 3 firewall

#	Policy	Protocol	Destination	Port	Comment	Actions
	Allow	Any	Any	Any	Default rule	

Add a firewall rule

Layer 7 firewall: There are no rules defined for this group. Add a layer 7 firewall rule

DNS layer protection (Cisco Umbrella)

Route DNS requests through Cisco Umbrella DNS and deny DNS requests by linking Umbrella policies.

Enable Umbrella protection

Umbrella protection is not available for switches.

- *This function is only available when 'Custom network firewall & shaping rules' is selected.*

Traffic shaping: Add a new shaping rule

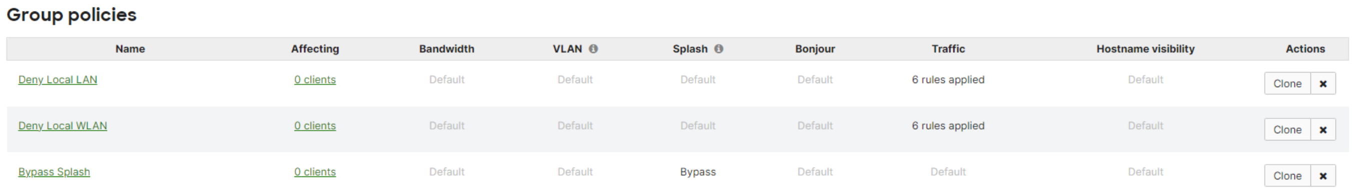
Wireless only

VLAN	Use network default — 0
Splash	Bypass
Bonjour forwarding Bridge mode SSIDs only	Use network default

There are no Bonjour forwarding rules on this network.
Add a Bonjour forwarding rule

4. Save changes.

Now all three policies have been created.



Group policies

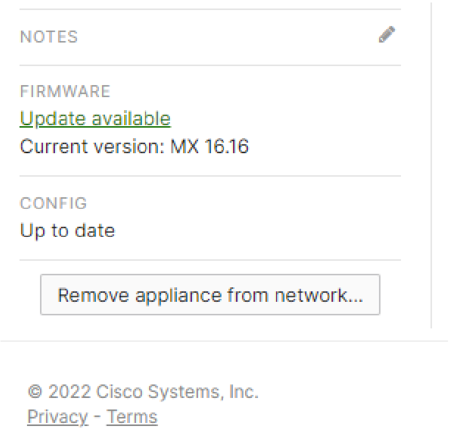
Name	Affecting	Bandwidth	VLAN	Splash	Bonjour	Traffic	Hostname visibility	Actions
Deny Local LAN	0 clients	Default	Default	Default	Default	6 rules applied	Default	Clone ✖
Deny Local WLAN	0 clients	Default	Default	Default	Default	6 rules applied	Default	Clone ✖
Bypass Splash	0 clients	Default	Default	Bypass	Default	Default	Default	Clone ✖

5.10 Check & upgrade MX firmware

To ensure the MX performs optimally, immediately following installation, it is recommended that a firmware upgrade is facilitated prior to going live.

First, check if the connected MX firmware is up to date.

Security & SD-WAN -> Monitor -> Appliance status -> Firmware



NOTES

FIRMWARE
Update available
Current version: MX 16.16

CONFIG
Up to date

Remove appliance from network...

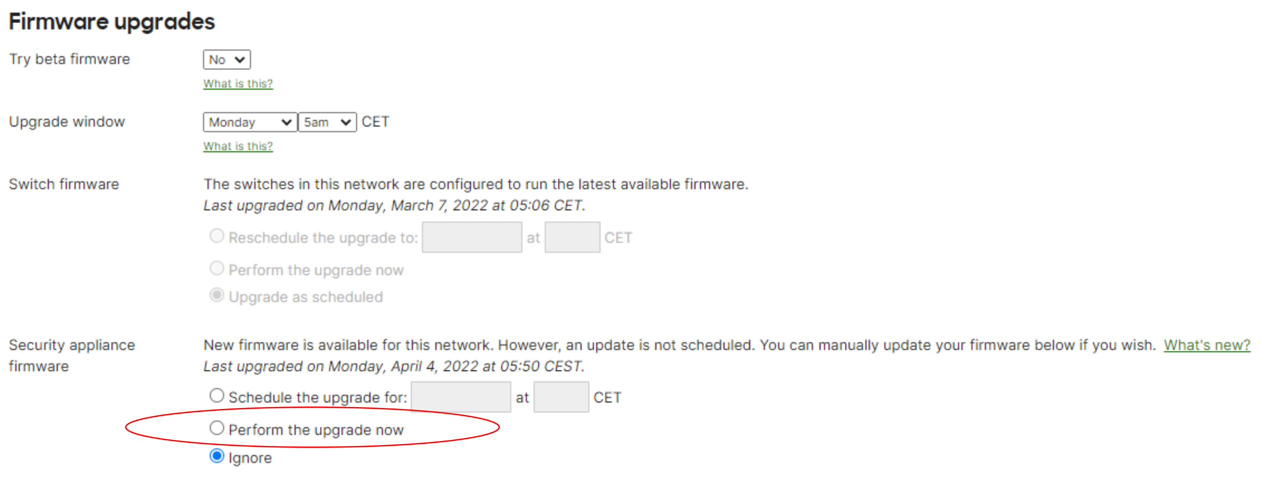
© 2022 Cisco Systems, Inc.
Privacy - Terms

The firmware will either be up to date and state the version or state Update available.

If an update is available, click the hyperlink or navigate to

Network-wide -> Configure -> General

In the section for Firmware upgrades, for the Security Appliance, select *Perform the upgrade now* and click Save. The update will be performed immediately.



Firmware upgrades

Try beta firmware: No
What is this?

Upgrade window: Monday 5am CET
What is this?

Switch firmware: The switches in this network are configured to run the latest available firmware.
Last upgraded on Monday, March 7, 2022 at 05:06 CET.
○ Reschedule the upgrade to: at CET
○ Perform the upgrade now
● Upgrade as scheduled

Security appliance firmware: New firmware is available for this network. However, an update is not scheduled. You can manually update your firmware below if you wish. What's new?
Last upgraded on Monday, April 4, 2022 at 05:50 CEST.
○ Schedule the upgrade for: at CET
○ Perform the upgrade now
● Ignore

5.10 MX security appliances high availability (warm spare) configuration

In a single ISP one router approach, connect both MX security appliances directly to the router ports.

Where there is only one router port available, the use of an 8-port WAN internet breakout switch is required. For example, the MS120-8.

Should you have two different ISP routers, each MX device should be connected to a separate port on the ISPs router. The connectivity should allow for full redundancy.

The below configuration example uses only one ISP.

1. The primary and secondary MX security appliances must be the same models and running the same firmware version. HA or Warm Spare setup requires only one Meraki licence.

2. The MX devices will require one public IP address each, to configure basic connectivity and other networking parameters on these devices.

3. Using a laptop, connect an ethernet cable from the machine to the management port on the MX device.

4. Open a browser window on the laptop and access the MXs built-in web service by browsing to http://setup.meraki.com NB: you do not have to be connected to the Internet to reach this address.

5. Click **Uplink configuration** under the **Local status** tab. The default credentials are the device serial number as the username, with a blank password.

6. Choose **Static** for the **IP Assignment** option.

7. Enter the IP address, subnet mask, default gateway IP and DNS server information.

8. Verify that the primary MX device has been added to the newly created network in the IHG Connect organisation and you can see it in the dashboard.

9. From the **Appliance status** page, select the **Configure warm spare** option.

10. Click **Enable**, then select the secondary MX under the device serial dropdown. If you don’t see it listed, verify that the secondary device was in the original order and has been claimed in the IHG Connect organisation. For assistance, please email IHGConnectEMEAA@ihg.com.

11. Choose the **MX uplink IP** option and click **Update**. Save the changes.

12. It may take a few minutes to sync between the two MX devices and you’ll notice that the status will change for the PRIMARY MX as **Current master** and the SPARE MX as ***Passive ready.***

More information can be found on the Meraki website.
https://documentation.meraki.com/MXZ/Deployment_Guides/NAT_Mode_Warm_Spare_(NAT_HA)

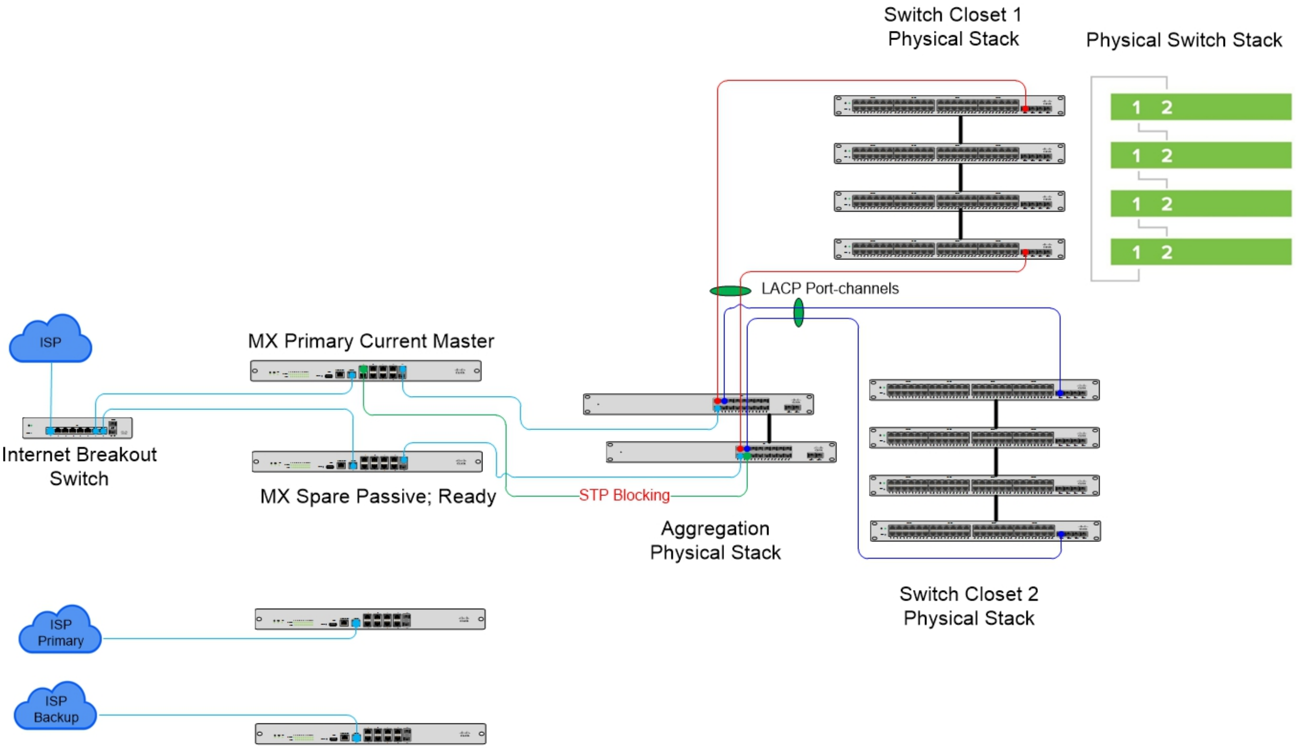
6. MS switch configuration

6.1 Network design & hardware specification

To avoid situations where legacy, unmanaged switches sit between the Guest Network and the ISP, IHG Connect requires an 8 port Cisco Meraki switch to terminate the Guest Network and the Hotel's Back Office Network and connect directly to ISP managed router.

NB: an additional switch may not be required if several ports are available directly on the ISP router.

See example diagram below:



1. Use switch stack design as a core and connect uplinks from IDFs 50/50 across core switch stack. Please reference to network design above.

2. Please use LACP Port-channels setup between MDF and IDFs should you have dual links available to the same IDF. Links in red and blue.

3. Connecting switches within the same rack with patch (copper or fibre) cables must be avoided. Please use Meraki stacking cables. Example: 2 x MS210-48FP-HW stacked with 2 x MA-CBL-40G-50CM (Optional 1M or 3M) stacking cables to form a ring.

4. Link between core SW2 and MX1 becomes active (STP) in the event of SW1 failure.

NB: Do not include spare devices when placing an order. You should place a separate order to include all spare devices and no licences.

6.2 Recommended deployment type & hardware specification

Internet Breakout Switch WAN	MDF Core Aggregation switch stack	IDF Switch or Switch Stack
1 x MS120-8FP-FP Copper & Fibre ports in total: 8 x 1GbE 2 x 1GbE SFP	**Deployment type – Copper cable or 1G fibre aggregation.** *Minimal Specification for core switch stack:* 2 x MS210-24P-HW 2 x Stacking Cable MA-CBL-40G-50CM (Optional 1M or 3M) Copper & Fibre ports in total: 48 x 1GbE 8 × 1GbE SFP uplinks or **Deployment type – Copper cable or 1G fibre aggregation.** *Single MDF only, no IDFs. More than 48 1GbE ports required:* 2 x MS210-48FP-HW 2 x Stacking Cable MA-CBL-40G-50CM (Optional 1M or 3M) Copper & Fibre ports in total: 96 x 1GbE 8 × 1GbE SFP uplinks	Depending on number of ports required: *Single switch in rack only:* 1 x MS120-8FP-HW Copper & Fibre ports in total: 8 x 1GbE 2 x 1GbE SFP or 1 x MS120-24P-HW 24 PoE ports Copper & Fibre ports in total: 24 x 1GbE 4 x 1GbE SFP or 1 x MS120-48FP-HW 48 PoE ports Copper & Fibre ports in total: 48 x 1GbE 4 x 1GbE SFP
	Deployment type - 1G fibre aggregation. *Installation requires more than 8 × 1GbE SFP MDF – IDF links:* 2 x MS410–16-HW 2 x Stacking Cable MA-CBL-40G-50CM (Optional 1M or 3M) Fibre ports in total: 32 × 1 GbE SFP Fibre 4 × 10 GbE SFP+ Fibre Note: Core switch stack required with any deployment.	*More than one switch in the same rack and more than 48 copper ports required:* 2 x MS210-48FP-HW 2 x Stacking Cable MA-CBL-40G-50CM (Optional 1M or 3M) Copper & Fibre ports in total: 96 x 1GbE 8 × 1GbE SFP uplinks Note: Stacking capabilities. MS210 can be stacked in combination with 48 and 24 ports models. Same stack compatible with MS225 if available.

NB: Licences, cables, SFP/Copper modules etc. are not included.
Select PoE or non-PoE switch models as per the hotel requirements.

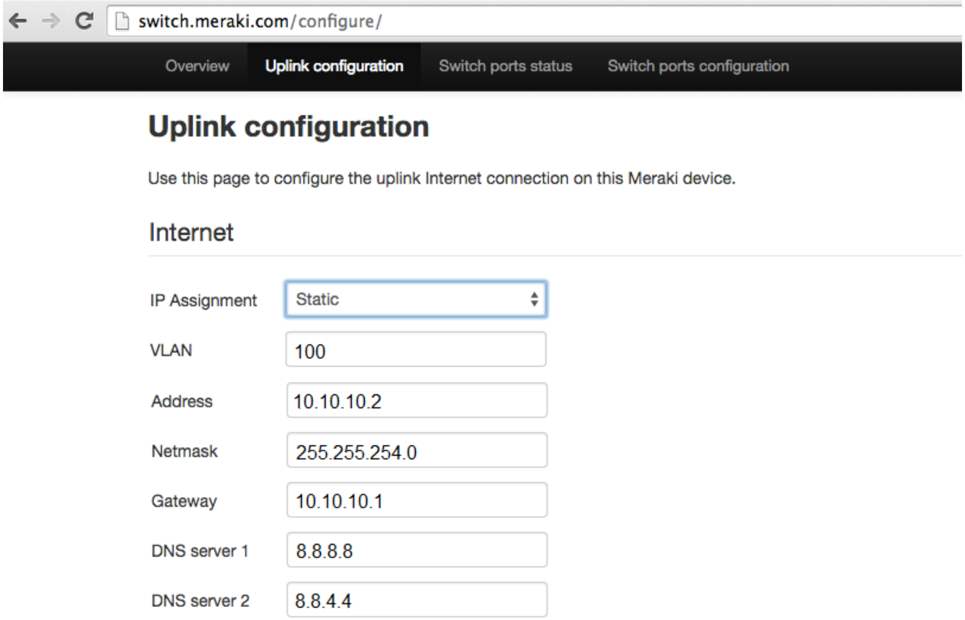
6.3 Assigning a static IP address to the internet breakout switch

1. Connect directly to the Cisco Meraki switch and browse to switch.meraki.com

2. Select **Uplink configuration**

3. Enter a static IP using an IP range from VLAN 100 Management, Subnet Mask, Gateway, and DNS info.

4. Click Save Settings



Uplink configuration

Use this page to configure the uplink Internet connection on this Meraki device.

Internet

IP Assignment	Static
VLAN	100
Address	10.10.10.2
Netmask	255.255.254.0
Gateway	10.10.10.1
DNS server 1	8.8.8.8
DNS server 2	8.8.4.4

NB: Configure ports in VLAN 1 to connect ISP router and MX firewalls in Public IP subnet range provided.

6.4 Configure switch details

Management information for each device can be configured by drilling down on that particular device in the Dashboard.

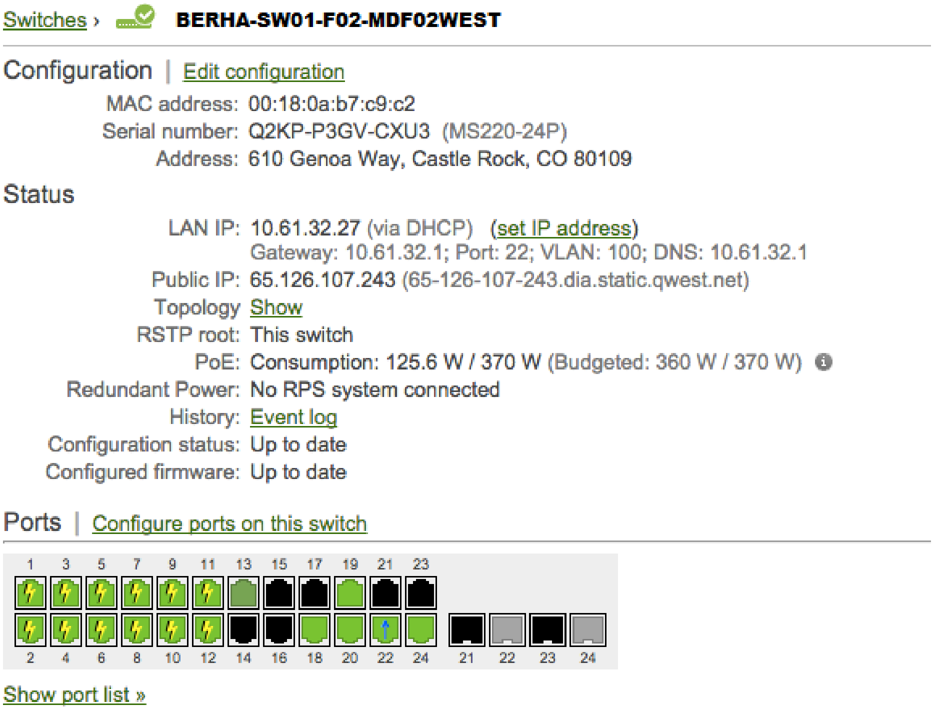
1. Navigate to **Switching -> Monitor -> Switches**
2. Select a switch
3. Click **Edit configuration**
4. Configure the switch name using the following naming convention:

Hotel Code – SW Switch Number F Floor Number – MDF or IDF number and Switch Location

Second Floor:	BERHA-SW01-F02-MDF02WEST
Ground Floor:	BERHA-SW02-F00-MDF03WEST
Basement Level:	BERHA-SW03-F-1-MDF04WEST

NB: naming conventions must be limited to 40 characters and contain only
Alphabet: A-Z (no special alphabet characters like á é í ó ú ü ä ö ñ etc. are allowed)
Numeric: 0-9
Special characters: / - _ ( ) [ ]

1. Enter a physical address of the device for proper placement on Google maps



Switches › BERHA-SW01-F02-MDF02WEST

Configuration | Edit configuration

MAC address: 00:18:0a:b7:c9:c2
Serial number: Q2KP-P3GV-CXU3 (MS220-24P)
Address: 610 Genoa Way, Castle Rock, CO 80109

Status

LAN IP: 10.61.32.27 (via DHCP) (set IP address)
Gateway: 10.61.32.1; Port: 22; VLAN: 100; DNS: 10.61.32.1
Public IP: 65.126.107.243 (65-126-107-243.dia.static.qwest.net)
Topology Show
RSTP root: This switch
PoE: Consumption: 125.6 W / 370 W (Budgeted: 360 W / 370 W)
Redundant Power: No RPS system connected
History: Event log
Configuration status: Up to date
Configured firmware: Up to date

Ports | Configure ports on this switch

Show port list »

Switch power consumption details

These details can be found here or https://documentation.meraki.com/MR/Other_Topics/Calculating_BTU_Consumption_for_Cisco_Meraki_Products

There is also a technical overview in the Cisco Meraki section on the Wi-Fi service partner SharePoint site.

6.5 Global switch setting configuration

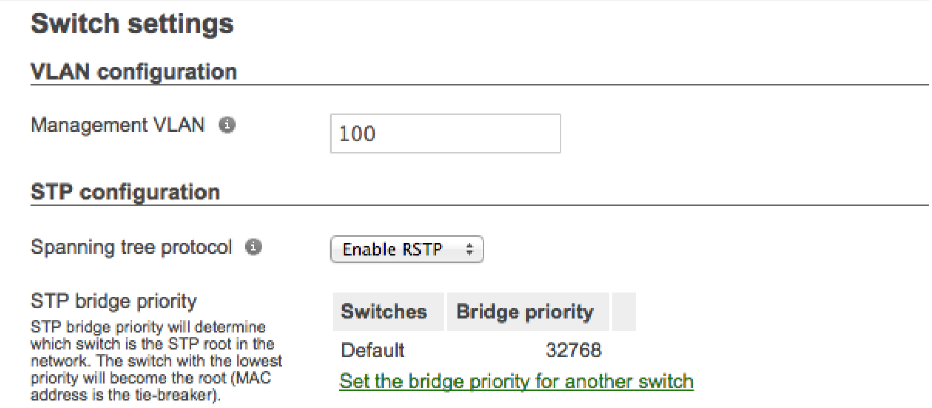
By navigating to the Switch settings tab, you can review the global switch configurations that affect all switches within the Networks/Hotel such as the management VLAN, spanning tree for the switch stack, quality of service, and port mirroring, etc.

The management VLAN should be configured to be VLAN 100, and Rapid Spanning Tree Protocol (RSTP) should be enabled which is the default configuration.

STP bridge priority will determine which switch is the STP root in the network. The switch with the lowest priority will become the root (MAC address is the tiebreaker) which is the default. If you would like to manually specify which of your switches is your root, you can do so by navigating to **Configure -> Switch Settings** and entering a new root bridge rule. For large properties with link redundancy, our recommendation is to configure the aggregation switch downstream of the MX as the STP root.

To set the management VLAN and verify RSTP is enabled:

1. Navigate to **Switch > Configure > Switch Settings**
2. Under VLAN configuration, configure the Management VLAN to 100
3. Under STP configuration, confirm Spanning tree protocol is enabled



Switch settings

VLAN configuration

Management VLAN: 100

STP configuration

Spanning tree protocol: Enable RSTP

STP bridge priority
STP bridge priority will determine which switch is the STP root in the network. The switch with the lowest priority will become the root (MAC address is the tie-breaker).

Switches	Bridge priority
Default	32768

Set the bridge priority for another switch

6.6 Switch port configuration

Meraki's MS switch allows you to configure anything from a single port to thousands of ports through our industry-first, Virtual Stacking technology. Virtual Stacking provides centralised management for up to 10,000 switch ports and unlike traditional stacking, virtually stacked switches do not require a physical connection, can be in different physical locations, and can be of different switch models, thereby simplifying large scale, distributed deployments.

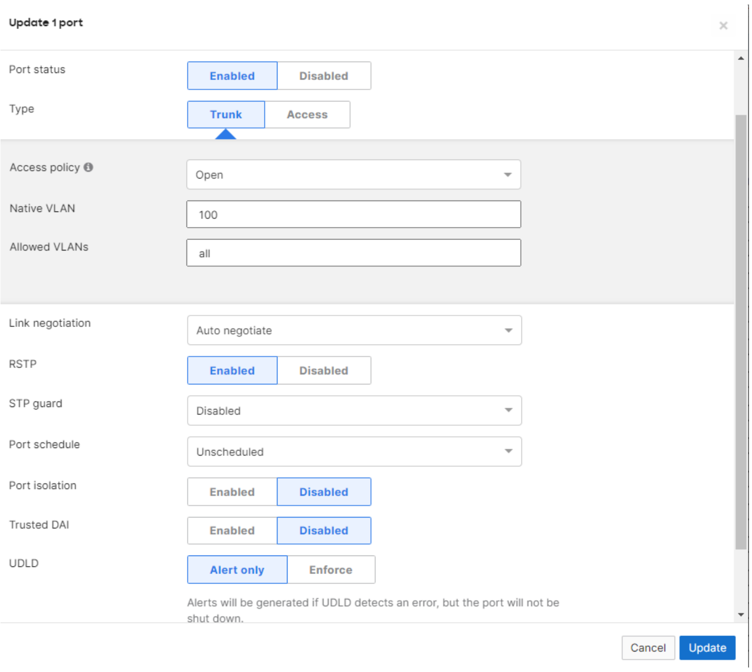
From the Configure>Switch Ports page, you can name your ports, turn ports on/off, enable spanning tree (RSTP), define port types (access/trunk), and specify VLANs. Click here or https://docs.meraki.com/display/MS/Switch+Ports#SwitchPorts-Searchingforports for information on ability to search and filter on multiple ports at time for mass configuration purposes.

There should be NO OPEN PORTS on switches. All unused ports must be disabled.

Configuring Switch Interconnect ports

1. Navigate to **Switch > Monitor > Switch ports**
2. Select a port or a range of ports for configuration
3. Click **Edit configuration**
4. Configure as a trunk port with Native VLAN set to 100
5. Insert Name for each connected Switch port

(Please configure allowed VLANs as required per each installation)



Update 1 port

Port status: [✓ Enabled] Disabled

Type: [✓ Trunk] Access

Access policy: Open

Native VLAN: 100

Allowed VLANs: all

Link negotiation: Auto negotiate

RSTP: [✓ Enabled] Disabled

STP guard: Disabled

Port schedule: Unscheduled

Port isolation: Enabled [✓ Disabled]

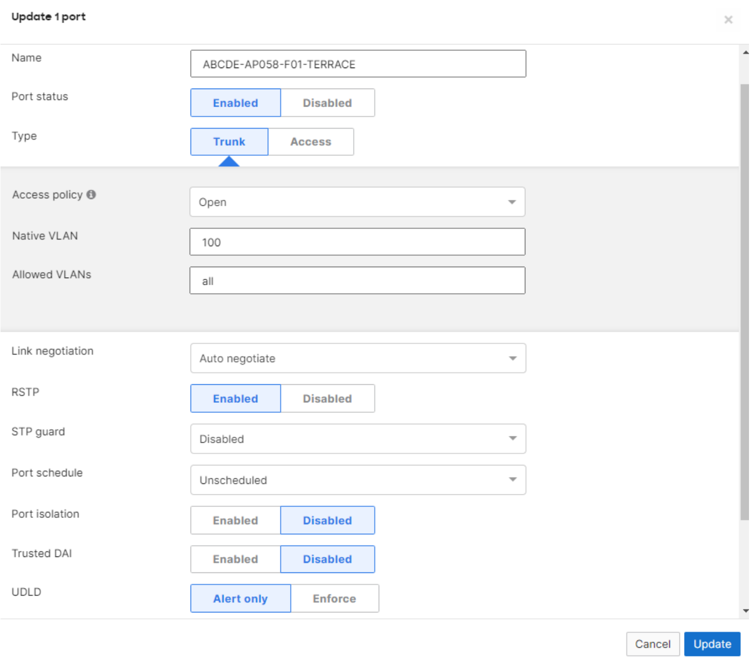
Trusted DAI: Enabled [✓ Disabled]

UDLD: [✓ Alert only] Enforce

Alerts will be generated if UDLD detects an error, but the port will not be shut down.

Configuring switch ports connected to access points

1. Navigate to **Switching -> Monitor -> Switch ports**
2. Select a port or a range of ports for configuration
3. Click **Edit configuration**
4. Configure as a trunk port with Native VLAN set to 100
5. Insert access point name (room/area) for each connected switch port



Update 1 port ×

Name: ABCDE-AP058-F01-TERRACE

Port status: [✓ Enabled] Disabled

Type: [✓ Trunk] Access

Access policy: Open

Native VLAN: 100

Allowed VLANs: all

Link negotiation: Auto negotiate

RSTP: [✓ Enabled] Disabled

STP guard: Disabled

Port schedule: Unscheduled

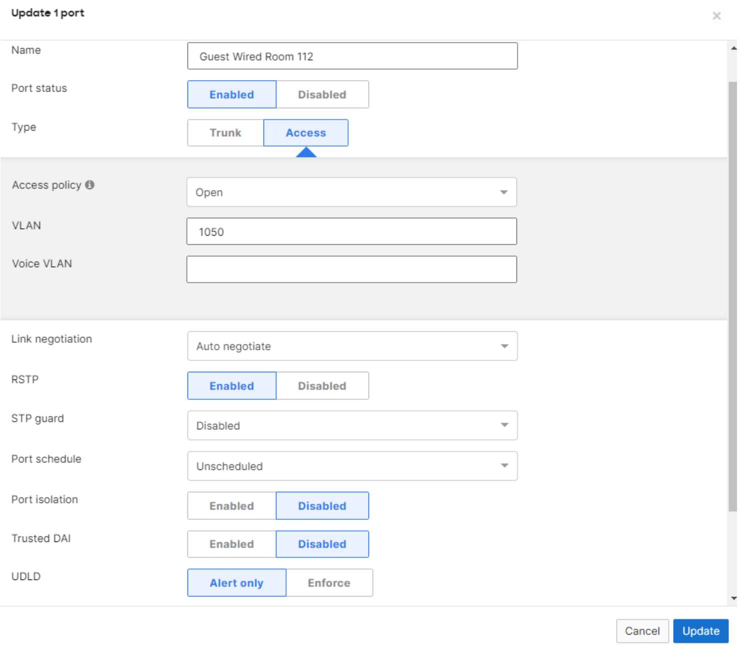
Port isolation: Enabled [✓ Disabled]

Trusted DAI: Enabled [✓ Disabled]

UDLD: [✓ Alert only] Enforce

Configuring switch ports for wired client access

1. Navigate to **Switching -> Monitor -> Switch ports**
2. Select a port or a range of ports for configuration
3. Click Edit configuration
4. Configure as an access port with VLAN set to 1050
5. Insert name for each connected switch port relevant to the wired connection, guest room, business centre etc.



Update 1 port ×

Name: Guest Wired Room 112

Port status: [✓ Enabled] Disabled

Type: Trunk [✓ Access]

Access policy: Open

VLAN: 1050

Voice VLAN:

Link negotiation: Auto negotiate

RSTP: [✓ Enabled] Disabled

STP guard: Disabled

Port schedule: Unscheduled

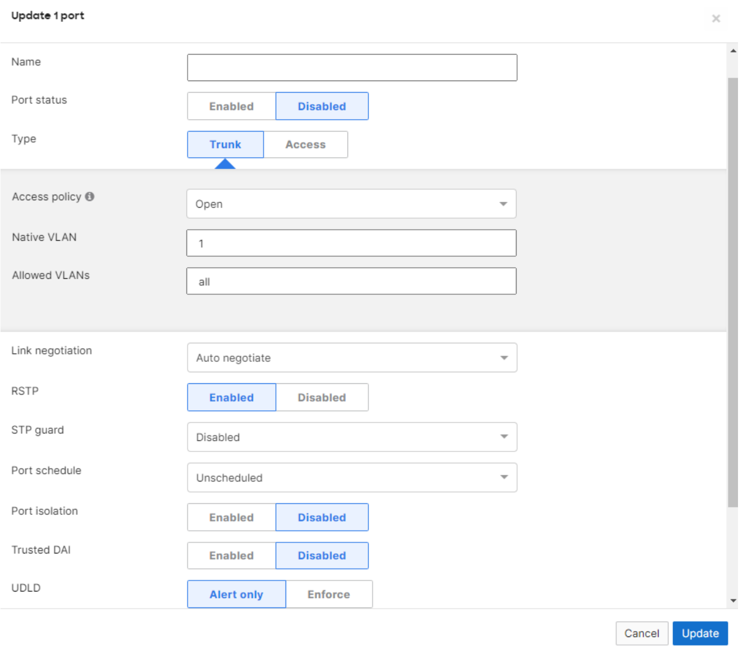
Port isolation: Enabled [✓ Disabled]

Trusted DAI: Enabled [✓ Disabled]

UDLD: [✓ Alert only] Enforce

Configuring switch ports that are spare or not in use

1. All unused or spare ports must be disabled.



Update 1 port

Name:

Port status: Disabled

Type: Trunk

Access policy: Open

Native VLAN: 1

Allowed VLANs: all

Link negotiation: Auto negotiate

RSTP: Enabled

STP guard: Disabled

Port schedule: Unscheduled

Port isolation: Disabled

Trusted DAI: Disabled

UDLD: Alert only

6.7 Restricting traffic with isolated switch ports

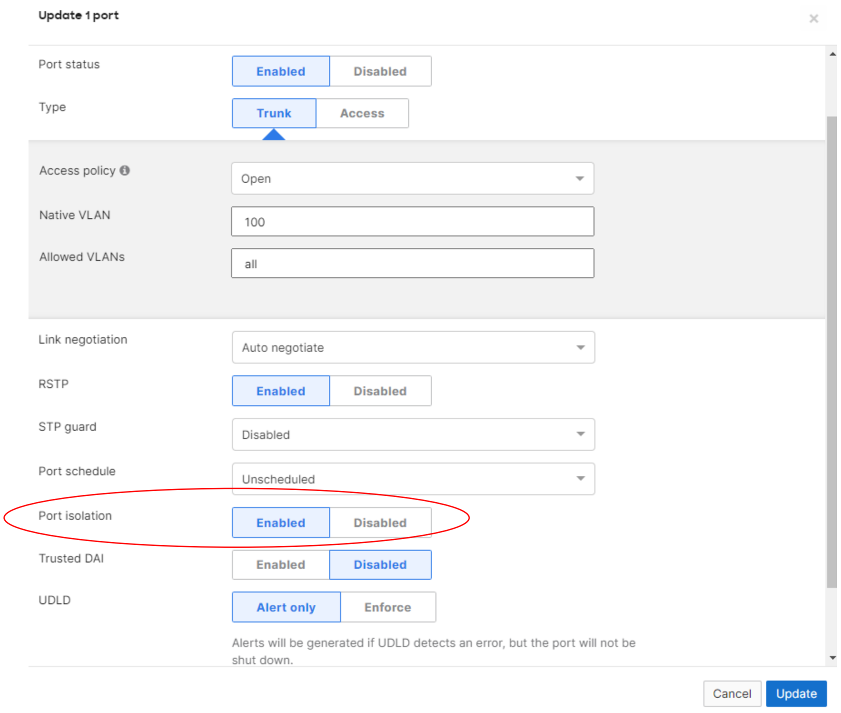
NB: for MS210, MS225, and MS250 series switches, port isolation is only supported on the first 24 ports. Port Isolation is not supported across stack members. Please refer to section 11.1 to restrict guest to guest traffic.

Port isolation allows a network administrator to prevent traffic from being sent between specific ports. This can be configured in addition to an existing VLAN configuration, so even client traffic within the same VLAN will be restricted. This article outlines how to configure isolated ports, as well as best practices and example implementations.

6.8 Configuration for port isolation

Isolated ports can either be configured on a per-port basis, or in bulk. The following instructions explain how to enable isolation in Dashboard:

1. Navigate to the Dashboard network containing the switch/switches to be configured.
2. Select **Configure > Switch ports**.
3. Click the check box on the left of each port.
4. Click the **Edit** button to edit the port configuration.
5. Set Isolation to “enabled” in the configuration window.
6. Select Update to save the configuration.



Update 1 port

Port status [✓ Enabled] Disabled

Type [✓ Trunk] Access

Access policy: Open

Native VLAN: 100

Allowed VLANs: all

Link negotiation: Auto negotiate

RSTP [✓ Enabled] Disabled

STP guard: Disabled

Port schedule: Unscheduled

Port isolation [✓ Enabled] Disabled

Trusted DAI Enabled [✓ Disabled]

UDLD [✓ Alert only] Enforce

Alerts will be generated if UDLD detects an error, but the port will not be shut down.

NB: Isolation can also be enabled/disabled on individual switch ports, on the switch's page in the Meraki dashboard

6.9 Check & upgrade MS firmware

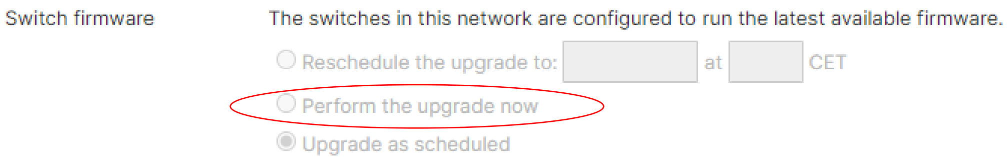
To ensure your MS devices perform optimally immediately following installation, it is recommended that a firmware upgrade is facilitated prior to going live.

1. You can check if the connected MS firmware is up to date by individual switch
   Switching -> Monitor -> Switches -> Select the required switch -> Firmware

2. The firmware will either be **Up to date** and state the version or state **Update available**
   If an update is available navigate to
   Network-wide -> Configure -> General -> Firmware Upgrades

3. There is a section for **Switch firmware,** and you have various scheduling options.

4. Select **Perform the upgrade now** and click **Save changes**, the update will be performed.



Switch firmware

The switches in this network are configured to run the latest available firmware.

○ Reschedule the upgrade to: at CET

○ Perform the upgrade now

● Upgrade as scheduled

7. MR access point configuration

7.1 Meraki access point overview

Most Meraki APs have one Gigabit Ethernet RJ45 port that accepts 802.3at and 802.3af power (labelled “Eth0, PoE”) on the rear of the unit. This port should be used for uplink to WAN connection.

Access point can be powered using either the Meraki AC Adapter, PoE Injector or PoE switch.

If the button is pressed and held for at least five seconds and then released, the access point will reboot and be restored to its original factory settings by deleting all configuration information stored on the unit.

System Status

The access points are equipped with a multi-colour LED light on the front of the unit on the top right to convey information about system functionality and performance. The LED shines through the faceplate of the AP.

- Orange - AP is booting (permanent orange suggests hardware issue)
- Blinking orange - AP can't find uplink
- Rainbow - AP is initializing/scanning
- Blue - AP in Gateway mode with clients
- Blinking blue - AP is upgrading
- Green - AP in Gateway mode with no clients

The MR30H/MR36H features 4x LAN ports labelled 1 through 4. Port 1 may provide 802.3af out to an end device if the MR30H/MR36H is powered via a 802.3at power source. The MR30H/MR36H access point can be powered via PoE using either the Meraki PoE Injector or a PoE switch. The MR30H/MR36H will function in low power mode when powered by a 802.3af power source. While in low power mode, the MR30H/MR36H will disable 802.3af out on the LAN1 port. Despite being in low power mode, the device can still supply full wireless capabilities.

The MR30H/MR36H features four green Ethernet status LEDs near the bottom of the faceplate. When an Ethernet client is connected, the LED will shine through the faceplate.

NB: as most of these switch AP types may be installed in guest rooms the LED lights may cause disturbance to guests, so we recommend that once the installation has been completed successfully the LED lights are disabled.

Network-wide > General -> Device configuration: AP LED Lights = On/Off (run dark)

AP LED lights Off (run dark)

7.2 Check & upgrade firmware

To ensure your access points perform optimally, immediately following installation, it is recommended that firmware upgrade is facilitated prior to mounting.

- Attach the access point to a PoE switch with an active Internet connection.

- The access point will turn on and the LED will glow solid orange. If the unit does not require a firmware upgrade, the LED will turn either green (no clients associated) or blue (clients associated) within thirty seconds.

* If the unit requires an upgrade, the LED will begin blinking orange until the upgrade is complete, at which point the LED will turn solid green or blue. You should allow at least a few minutes for the firmware upgrade to complete, depending on the speed of your internet connection.

7.3 Verify device functionality & test network coverage

1. Check LEDs
2. The power LED should be solid green (or blue if clients are connected). If it is flashing blue, the firmware is automatically upgrading and the LED should turn green when the upgrade is completed (normally within a few minutes).
   NB: The MR30H/MR36H must have an active route to the Internet to check and upgrade its firmware.
3. Verify access point connectivity
4. Use any 802.11 client device to connect to the MR30H/MR36H and verify proper connectivity using the client’s web browser.
5. Check network coverage
6. Confirm that you have good signal strength throughout your coverage area. You can use the signal strength meter on a laptop, smart phone, or another wireless device.

7.4 Optimise the mounting location

A good mounting location is important to getting the best performance out of the access point. You should always follow the Meraki installation guide when mounting access points as it may vary by model and best practises.

Keep the following in mind:

1. The device should have unobstructed line of sight to most coverage areas.
2. Power over Ethernet supports a maximum cable length of 100 m or 300 ft.
3. Please check if wall plates for the MR30H/MR36H are required. MA-MNT-MR-H2

NB: The MR30H/MR36H access point has a lower output compared with the MR33. The MR30H/MR36H should only be used if the hotel is installing an AP in every room or if the switching functionality on the AP is required.

7.5 Access point placement. Best practice.

Typically, hotel owners want to place access points in hallways, but having them in the rooms is better when it comes to performance. Installing access points in the hallways are typically better protected from guest tampering, easier to get access to for maintenance purposes and installation costs are lower. Consider physical security of access points by placing them higher or in harder to reach areas. If you're providing wireless access to outdoor areas such as restaurant patio areas, swimming pools or courtyards, please use IP rated outdoor ruggedized access points, such as MR74 or MR84.

Public areas and high-density areas such as reception, conference rooms, fitness rooms etc. we recommend installing more than one access point specifically in those areas with a much lower power setting. For HD deployment please click here or visit https://documentation.meraki.com/MR/Deployment_Guides/High_Density_Wi-Fi_Deployment_Guide_(CVD)

Placement is very important to reduce negative effect of co-channel interference. When placing an access point you must consider 3D, not just along the horizontal plane, but above and below as well. The power of client devices is generally very low, and the power of access point must be similar to the devices connected, so coverage is symmetrical.

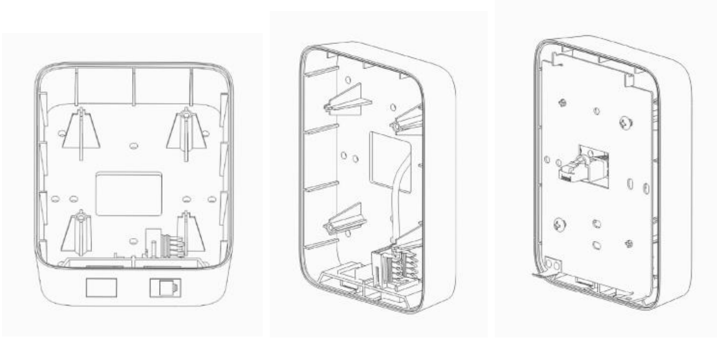
Access point placement:

1. Access point should be securely mounted, ensuring it cannot move or fall.
2. Please place access point in line of sight.
3. Install access point below suspend ceiling, if possible. Should you require to place access point above the ceiling please make sure you place access point face down.
4. Where possible, try to avoid mounting an AP against a wall, as most of the RF output will not be serving its intended purpose. APs with internal antennas are designed to be mounted on ceilings to provide 360-degree coverage.
5. Never place access points on desks.
6. Avoid installing access points in closets.
7. Please be aware of sources of interference such as cordless phones, microwave ovens, Bluetooth devices etc.
8. Metal objects reflect wireless signal. Do not place access points behind metal shelfs, metal doors and alike.

MR30H/MR36H mount kit:

The MR30H/MR36H surface mount kit is designed to be used in installations where additional cabling outlets are needed via the same wall plate used by an MR30H/MR36H access point. The surface kit houses a keystone jack port, enabling additional non-Ethernet cables (for example, telephone lines) to run from the wall plate — far more aesthetically pleasing than drilling an additional hole in a wall to string cabling through.

The MR30H/MR36H Surface Mount Kit MA-MNT-MR-H2
https://documentation.meraki.com/MR/Installation_Guides/MA-MNT-MR-H2_Installation_Guide



7.6 Configure access point details

Management information for each device can be configured by drilling down on that particular device in the dashboard. To configure AP details:

1. Navigate to **Wireless -> Monitor -> Access points**
2. Select an access point
3. Click **Edit configuration**
4. Configure AP name using naming convention as per example below:

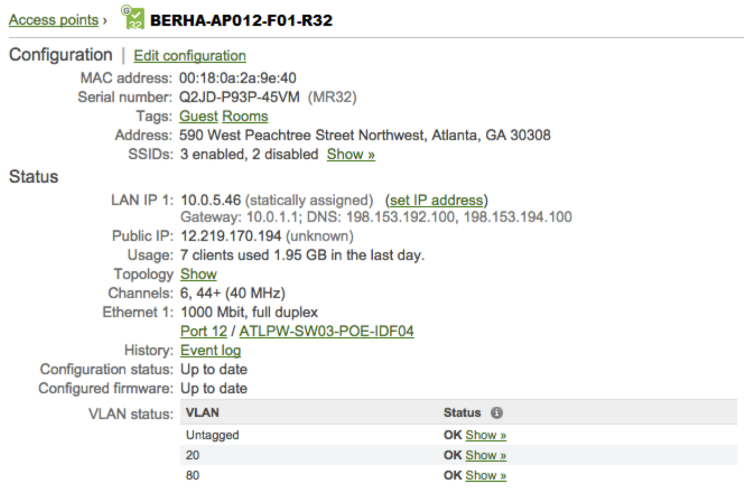
<u>Hotel Code – AP Access Points Number – F Floor Number – R Room Number or Area in the Building</u>

First Floor:	`BERHA-AP012-F01-R032`
Reception Ground Floor:	`BERHA-AP001-F00-RECEPTION`
Basement:	`BERHA-AP012-F-1-R002`

NB: naming conventions must be limited to 40 characters and contain only:

Alphabet: A-Z (no special alphabet characters like á é í ó ú ü ä ö ñ etc. are allowed)
Numeric: 0-9
Special characters: / - _ ( ) [ ]

Configure the physical address of the device for proper placement on Google maps



Access points › BERHA-AP012-F01-R32

Configuration | Edit configuration

MAC address: 00:18:0a:2a:9e:40
Serial number: Q2JD-P93P-45VM (MR32)
Tags: Guest Rooms
Address: 590 West Peachtree Street Northwest, Atlanta, GA 30308
SSIDs: 3 enabled, 2 disabled Show »

Status

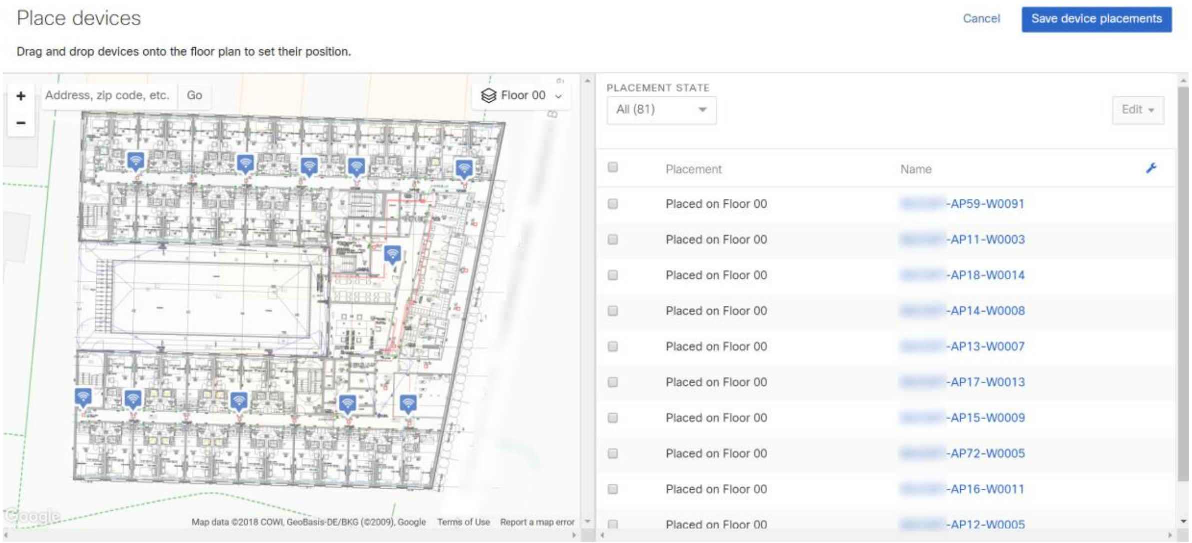
LAN IP 1: 10.0.5.46 (statically assigned) (set IP address)
Gateway: 10.0.1.1; DNS: 198.153.192.100, 198.153.194.100
Public IP: 12.219.170.194 (unknown)
Usage: 7 clients used 1.95 GB in the last day.
Topology Show
Channels: 6, 44+ (40 MHz)
Ethernet 1: 1000 Mbit, full duplex
Port 12 / ATLPW-SW03-POE-IDF04
History: Event log
Configuration status: Up to date
Configured firmware: Up to date
VLAN status:

VLAN	Status
Untagged	OK Show »
20	OK Show »
80	OK Show »

7.7 Maps & floor plans

All floorplans will need to be uploaded to the Meraki Dashboard and APs placed at the appropriate location.

1. Navigate to Wireless -> Monitor -> Map & floor plans
2. Select Add a new floor plan and upload the floor plan images
3. Select Place devices on floor and drag and drop each AP to its correct location on the floor plan
4. When you have finished select Save device placements



Drag and drop devices onto the floor plan to set their position.

□	Placement	Name
□	Placed on Floor 00	[redacted]-AP59-W0091
□	Placed on Floor 00	[redacted]-AP11-W0003
□	Placed on Floor 00	[redacted]-AP18-W0014
□	Placed on Floor 00	[redacted]-AP14-W0008
□	Placed on Floor 00	[redacted]-AP13-W0007
□	Placed on Floor 00	[redacted]-AP17-W0013
□	Placed on Floor 00	[redacted]-AP15-W0009
□	Placed on Floor 00	[redacted]-AP72-W0005
□	Placed on Floor 00	[redacted]-AP16-W0011
□	Placed on Floor 00	[redacted]-AP12-W0005

7.8 SSID configuration

To configure the SSID for the hotel, simply navigate to the **Wireless -> Configure -> SSIDs**.

1. Navigate to Wireless -> Configure -> SSIDs
2. Click rename to configure the SSID1 as IHG ONE REWARDS Free WI-FI
3. This should *always* be configured on SSID1
4. Ensure it is enabled

"IHG ONE REWARDS Free WI-FI" is the only authorised SSID for the guest Wi-Fi network. Any variations or changes to this must be first approved by IHG Connect Team.

If the hotel has a conference group requesting their own SSID, the hotel should utilise Access Code Manager. Additional SSIDs, other than "IHG ONE REWARDS Free WI-FI" will not be allowed unless approved by the IHG Connect Team.

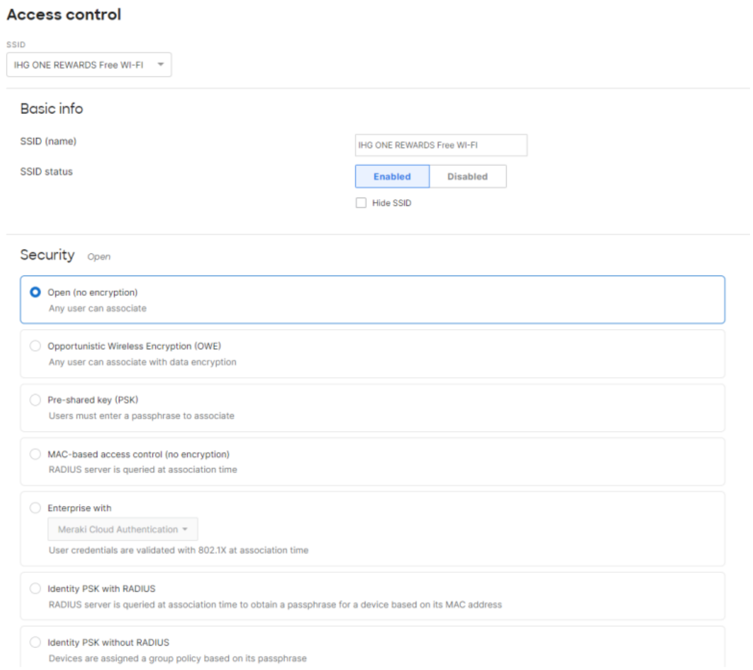
NB: The Global Standard for SSIDs in all IHG hotels is IHG ONE REWARDS Free WI-FI, this is only available to hotels participating in the IHG Connect programme with IHG EDGE.

For any questions, please contact IHGConnectEMEAA@ihg.com

7.9 Wireless access configuration

By navigating to the **Wireless -> Configure -> Access Control** tab, a variety of different configurations can be implemented that determine how devices access the wireless network. Here, you can configure any wireless security settings, splash page configurations, VLAN tagging, minimum bitrate configurations and band selection. The splash page related configurations will be covered in the next section (Captive Portal Configuration). To configure the wireless access control settings:

1. Navigate to Wireless -> Configure -> Access Control
2. Under Security, ensure that Open (no encryption) is selected.



Access control

SSID: IHG ONE REWARDS Free WI-FI

Basic info

SSID (name): IHG ONE REWARDS Free WI-FI

SSID status: Enabled | Disabled

□ Hide SSID

Security Open

● Open (no encryption)
Any user can associate

○ Opportunistic Wireless Encryption (OWE)
Any user can associate with data encryption

○ Pre-shared key (PSK)
Users must enter a passphrase to associate

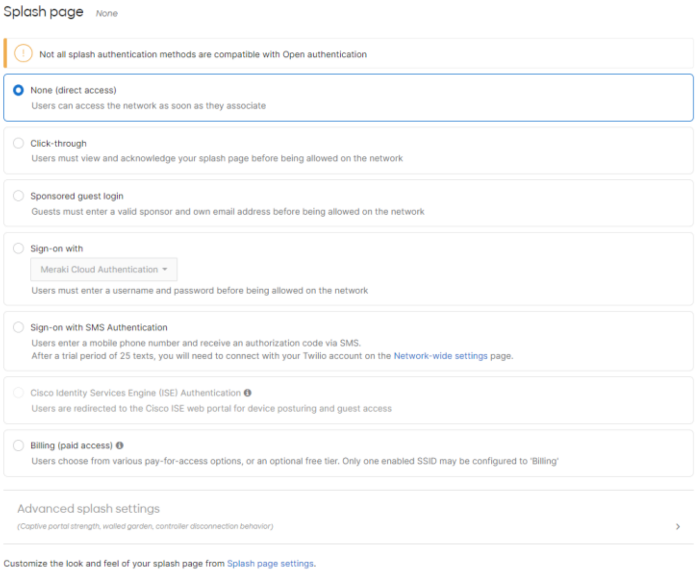
○ MAC-based access control (no encryption)
RADIUS server is queried at association time

○ 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

○ Identity PSK without RADIUS
Devices are assigned a group policy based on its passphrase

3. Scroll down to Splash page and ensure that None (direct access) is selected. The splash page will be configured as part of the EDGE interface activation.



Splash page None

Not all splash authentication methods are compatible with Open authentication

● 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

○ Sponsored guest login
Guests must enter a valid sponsor and own email address before being allowed on the network

○ Sign-on with Meraki Cloud Authentication
Users must enter a username and password before being allowed on the network

○ Sign-on with SMS Authentication
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.

○ Cisco Identity Services Engine (ISE) Authentication
Users are redirected to the Cisco ISE web portal for device posturing and guest access

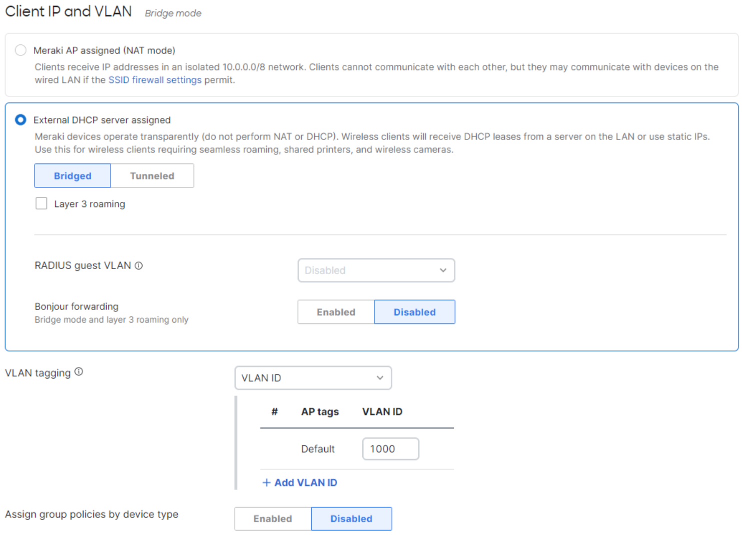
○ Billing (paid access)
Users choose from various pay-for-access options, or an optional free tier. Only one enabled SSID may be configured to 'Billing'

Advanced splash settings
(Captive portal strength, walled garden, controller disconnection behavior)

Customize the look and feel of your splash page from Splash page settings.

4. Scroll down further to Client IP and VLAN (previously Addressing and traffic). Select the option for External DHCP server assigned and set to Bridged

5. Underneath you have an option for VLAN Tagging, set VLAN ID to 1000



Client IP and VLAN *Bridge mode*

○ Meraki AP assigned (NAT mode)
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.

● External DHCP server assigned
Meraki devices operate transparently (do not perform NAT or DHCP). Wireless clients will receive DHCP leases from a server on the LAN or use static IPs. Use this for wireless clients requiring seamless roaming, shared printers, and wireless cameras.
[✓ Bridged] Tunneled
□ Layer 3 roaming

RADIUS guest VLAN: Disabled

Bonjour forwarding (Bridge mode and layer 3 roaming only): Enabled [✓ Disabled]

VLAN tagging: VLAN ID

#	AP tags	VLAN ID
	Default	1000

+ Add VLAN ID

Assign group policies by device type: Enabled [✓ Disabled]

6. Click save

NB: Wireless options for Per-SSID band and bitrate settings have moved to the Radio Settings page and are now part of the RF Profiles configuration.

7.10 Firewall & traffic shaping

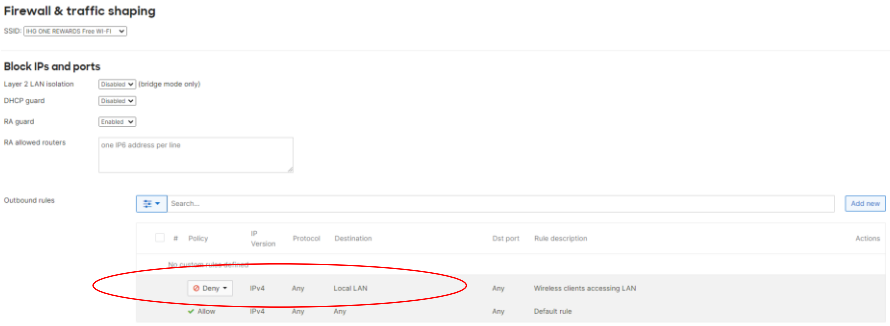
The Meraki MR Access Point have built in Layer 3 and Layer 7 Firewall and Layer 7 traffic shaping capabilities. It is possible to configure firewall and traffic shaping rules on the MR as opposed to the MX for the wireless clients connecting to the network. For locations with wireless access only, this would be recommended to block traffic at the edge of the network.

<u>Mandatory</u>: To configure client isolation between wireless clients while the AP is configured in bridge mode:

1. Navigate to Wireless -> Configure -> Firewall and traffic shaping

2. Select the SSID from drop down menu – IHG ONE REWARDS Free WI-FI

3. Under Block IPs and ports and Outbound rules, ensure that Deny Local LAN is active to prevent clients from being able to communicate with one another



Firewall & traffic shaping

SSID: IHG ONE REWARDS Free WI-FI

Block IPs and ports

Layer 2 LAN isolation: Disabled (bridge mode only)

DHCP guard: Disabled

RA guard: Enabled

RA allowed routers: one IP6 address per line

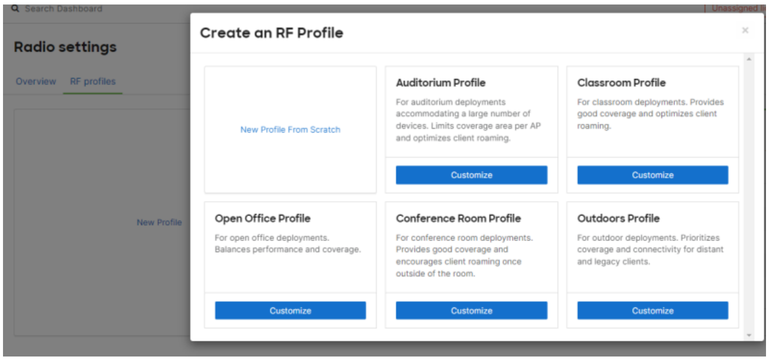
Outbound rules: Search... Add new

#	Policy	IP Version	Protocol	Destination	Dst port	Rule description	Actions
No custom rules defined							
	Deny	IPv4	Any	Local LAN	Any	Wireless clients accessing LAN	
	Allow	IPv4	Any	Any	Any	Default rule	

7.11 Radio settings

1. Navigate to Wireless -> Configure -> Radio Settings and select RF Profiles

2. Create a new profile from scratch called *IHGConnect RF Profile* (for indoor APs) and assign the following settings



Search Dashboard

Radio settings

Overview RF profiles

New Profile

Create an RF Profile

New Profile From Scratch

Auditorium Profile

For auditorium deployments accommodating a large number of devices. Limits coverage area per AP and optimizes client roaming.

Customize

Classroom Profile

For classroom deployments. Provides good coverage and optimizes client roaming.

Customize

Open Office Profile

For open office deployments. Balances performance and coverage.

Customize

Conference Room Profile

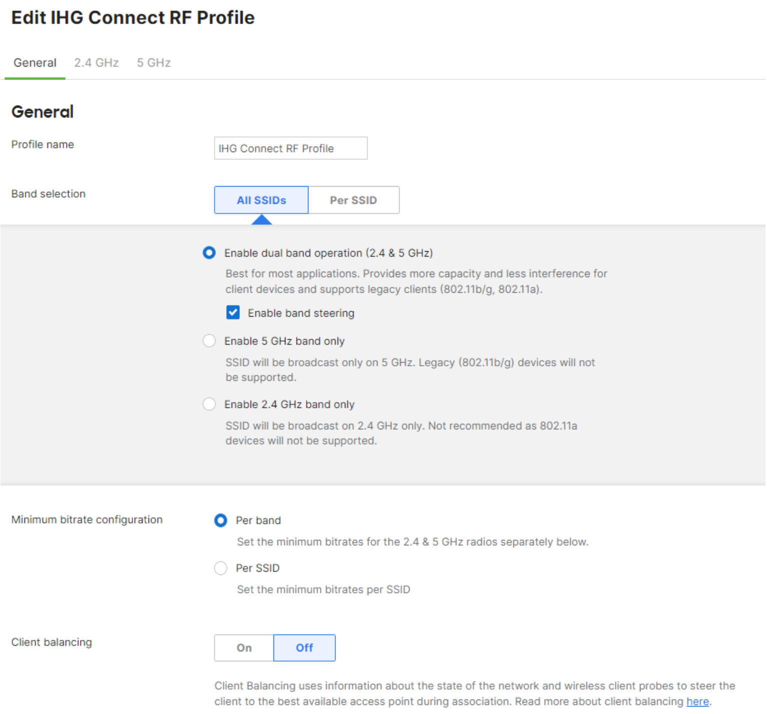
For conference room deployments. Provides good coverage and encourages client roaming once outside of the room.

Customize

Outdoors Profile

For outdoor deployments. Prioritizes coverage and connectivity for distant and legacy clients.

Customize



Edit IHG Connect RF Profile

General 2.4 GHz 5 GHz

General

Profile name: IHG Connect RF Profile

Band selection: All SSIDs | Per SSID

● Enable dual band operation (2.4 & 5 GHz)
Best for most applications. Provides more capacity and less interference for client devices and supports legacy clients (802.11b/g, 802.11a).
☑ Enable band steering

○ Enable 5 GHz band only
SSID will be broadcast only on 5 GHz. Legacy (802.11b/g) devices will not be supported.

○ Enable 2.4 GHz band only
SSID will be broadcast on 2.4 GHz only. Not recommended as 802.11a devices will not be supported.

Minimum bitrate configuration:
● Per band
Set the minimum bitrates for the 2.4 & 5 GHz radios separately below.
○ Per SSID
Set the minimum bitrates per SSID

Client balancing: On [✓ Off]

Client Balancing uses information about the state of the network and wireless client probes to steer the client to the best available access point during association. Read more about client balancing here.

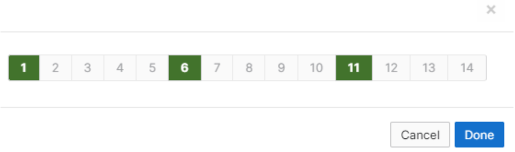
3. Band selection -> enable dual band operation and band steering

4. Minimum bitrate configuration -> Per band

5. Client balancing -> Off

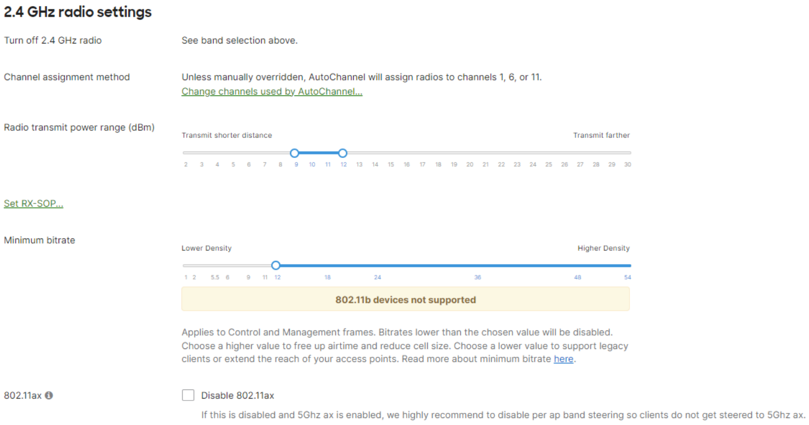
6. 2.4 GHz radio settings

   a. Channel assignment method -> leave as default 1, 6 and 11



   b. Radio transmit power range (dBm) -> set at 9 to 12

   c. Minimum bitrate -> set to 12



2.4 GHz radio settings

Turn off 2.4 GHz radio — See band selection above.

Channel assignment method — Unless manually overridden, AutoChannel will assign radios to channels 1, 6, or 11.
Change channels used by AutoChannel...

Radio transmit power range (dBm) — 9 – 12

Set RX-SOP...

Minimum bitrate — 12

802.11b devices not supported

Applies to Control and Management frames. Bitrates lower than the chosen value will be disabled. Choose a higher value to free up airtime and reduce cell size. Choose a lower value to support legacy clients or extend the reach of your access points. Read more about minimum bitrate here.

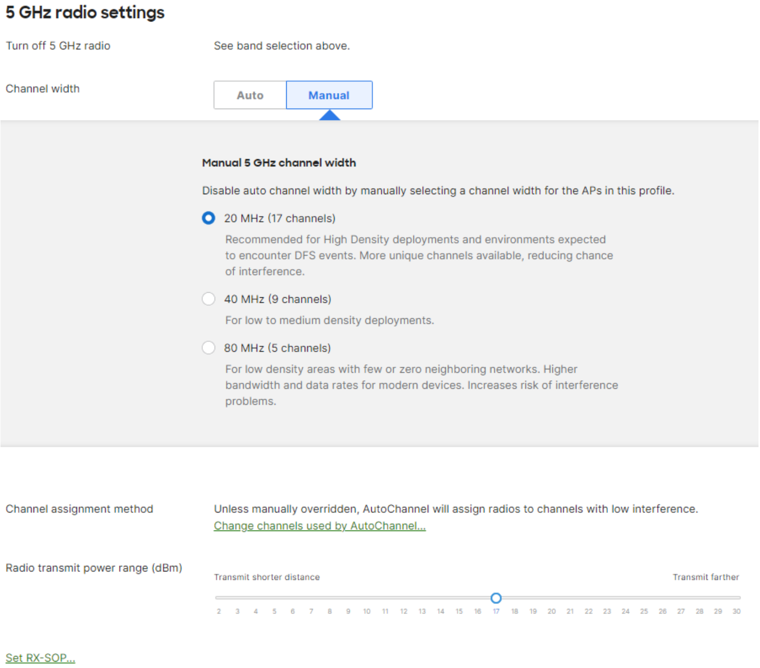
802.11ax — □ Disable 802.11ax

If this is disabled and 5Ghz ax is enabled, we highly recommend to disable per ap band steering so clients do not get steered to 5Ghz ax.

7. **5 GHz radio settings**

   a. Channel width -> Manual

   b. Manual 5 GHz channel width -> 20 MHz (17 channels)



5 GHz radio settings

Turn off 5 GHz radio — See band selection above.

Channel width — Auto | **Manual**

Manual 5 GHz channel width

Disable auto channel width by manually selecting a channel width for the APs in this profile.

● 20 MHz (17 channels)
Recommended for High Density deployments and environments expected to encounter DFS events. More unique channels available, reducing chance of interference.

○ 40 MHz (9 channels)
For low to medium density deployments.

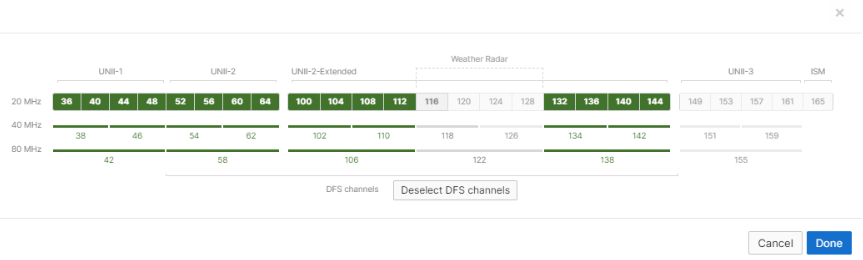
○ 80 MHz (5 channels)
For low density areas with few or zero neighboring networks. Higher bandwidth and data rates for modern devices. Increases risk of interference problems.

Channel assignment method — Unless manually overridden, AutoChannel will assign radios to channels with low interference.
Change channels used by AutoChannel...

Radio transmit power range (dBm) — 17

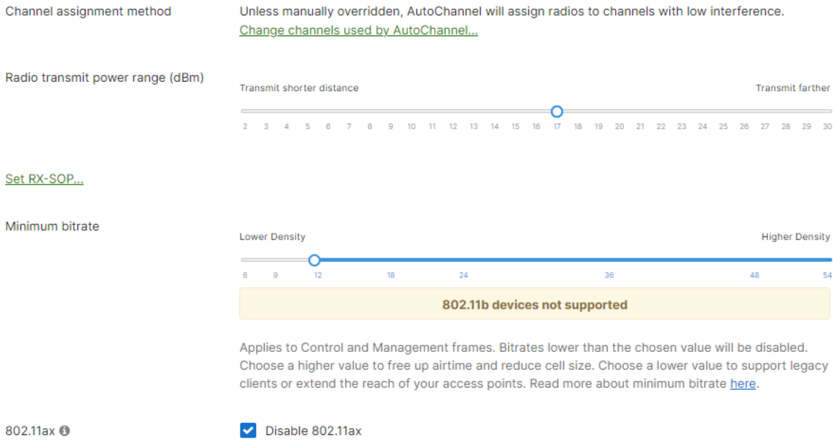
Set RX-SOP...

c. Channel assignment method -> Change the 5 GHz channels used by AutoChannel and include 12-16 channels (channel availability will vary by country) but avoid those listed as weather radar.



d. Radio transmit power range (dBm) -> set to 17

e. Minimum bitrate -> set to 12



Channel assignment method

Unless manually overridden, AutoChannel will assign radios to channels with low interference.
Change channels used by AutoChannel...

Radio transmit power range (dBm)

Set RX-SOP...

Minimum bitrate

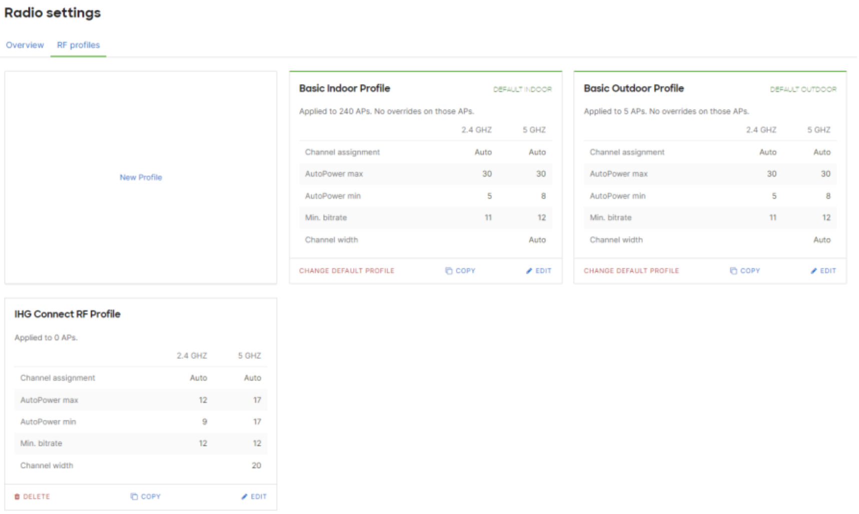
802.11b devices not supported

Applies to Control and Management frames. Bitrates lower than the chosen value will be disabled. Choose a higher value to free up airtime and reduce cell size. Choose a lower value to support legacy clients or extend the reach of your access points. Read more about minimum bitrate here.

802.11ax ℹ

☑ Disable 802.11ax

f. Save the profile to return to the RF Profile screen.



Radio settings

Basic Indoor Profile DEFAULT INDOOR

Applied to 240 APs. No overrides on those APs.

	2.4 GHZ	5 GHZ
Channel assignment	Auto	Auto
AutoPower max	30	30
AutoPower min	5	8
Min. bitrate	11	12
Channel width		Auto

Basic Outdoor Profile DEFAULT OUTDOOR

Applied to 5 APs. No overrides on those APs.

	2.4 GHZ	5 GHZ
Channel assignment	Auto	Auto
AutoPower max	30	30
AutoPower min	5	8
Min. bitrate	11	12
Channel width		Auto

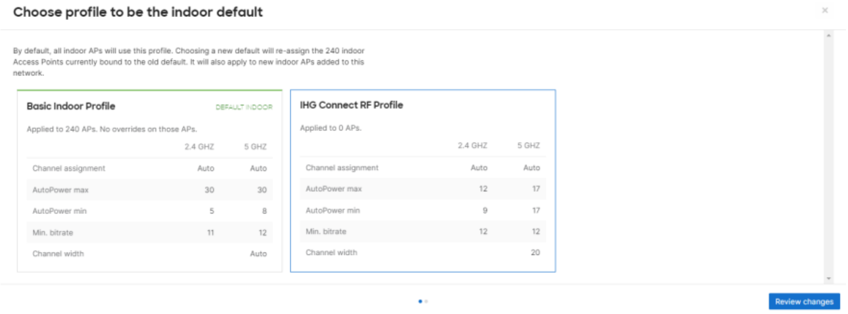
IHG Connect RF Profile

Applied to 0 APs.

	2.4 GHZ	5 GHZ
Channel assignment	Auto	Auto
AutoPower max	12	17
AutoPower min	9	17
Min. bitrate	12	12
Channel width		20

g. Under Basic Indoor profile, click Change Default Profile

h. Choose the new *IHGConnect RF Profile* and click Review changes



Choose profile to be the indoor default

By default, all indoor APs will use this profile. Choosing a new default will re-assign the 240 indoor Access Points currently bound to the old default. It will also apply to new indoor APs added to this network.

Basic Indoor Profile DEFAULT INDOOR

Applied to 240 APs. No overrides on those APs.

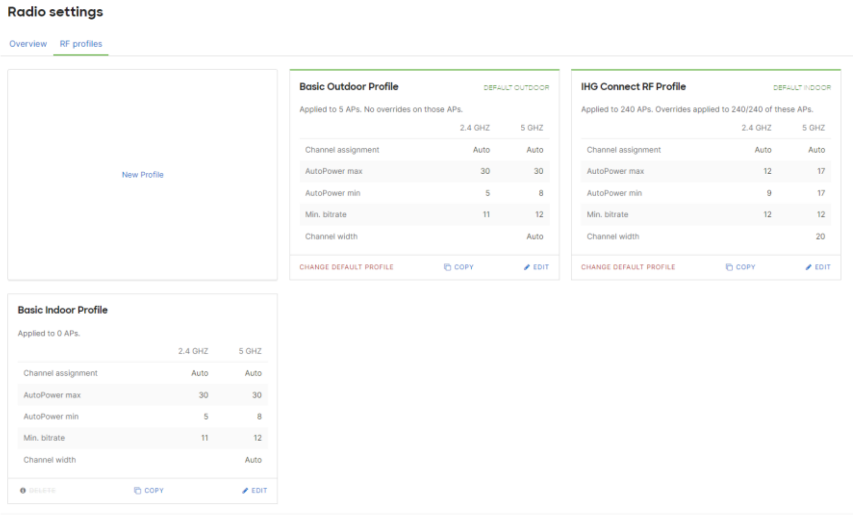
	2.4 GHZ	5 GHZ
Channel assignment	Auto	Auto
AutoPower max	30	30
AutoPower min	5	8
Min. bitrate	11	12
Channel width		Auto

IHG Connect RF Profile

Applied to 0 APs.

	2.4 GHZ	5 GHZ
Channel assignment	Auto	Auto
AutoPower max	12	17
AutoPower min	9	17
Min. bitrate	12	12
Channel width		20

i. Next click Apply changes, which will assign the profile to all access points and set the IHGConnect profile as the new default indoor profile.



Radio settings

Basic Outdoor Profile DEFAULT OUTDOOR

Applied to 5 APs. No overrides on those APs.

	2.4 GHZ	5 GHZ
Channel assignment	Auto	Auto
AutoPower max	30	30
AutoPower min	5	8
Min. bitrate	11	12
Channel width		Auto

IHG Connect RF Profile DEFAULT INDOOR

Applied to 240 APs. Overrides applied to 240/240 of these APs.

	2.4 GHZ	5 GHZ
Channel assignment	Auto	Auto
AutoPower max	12	17
AutoPower min	9	17
Min. bitrate	12	12
Channel width		20

Basic Indoor Profile

Applied to 0 APs.

	2.4 GHZ	5 GHZ
Channel assignment	Auto	Auto
AutoPower max	30	30
AutoPower min	5	8
Min. bitrate	11	12
Channel width		Auto

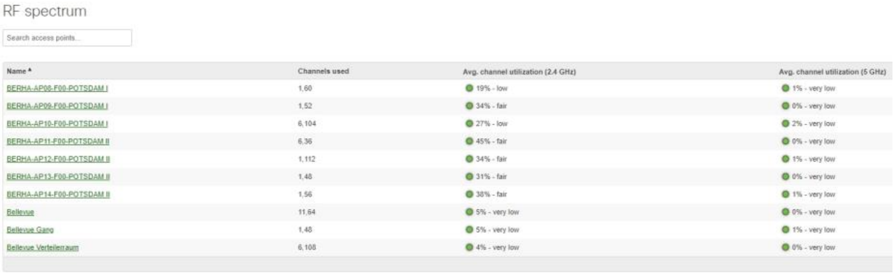
j. If required repeat this to create an IHGConnect Outdoor profile.

NB: in some instances, it will be necessary to manually set 2.4 GHz radios channels and power depending on RF environment.

IMPORTANT: for very high-density areas, it may be necessary to turn off some 2.4 GHz radios to reduce RF interference. This might be common in meeting areas where there are a dense number of APs to support high client density and also with in-room AP deployments where much more fine-tuning is required.

To validate the 2.4 GHz coverage and minimal RF interference. RF Interference can be validated by browsing the Wireless -> Monitor -> RF spectrum

Please make sure that adjustments are made to the 2.4 GHz broadcasts before leaving site; some APs will need to be powered down, manually channel set or switched off to ensure the band is still usable for guests and other hotel devices.



RF spectrum

Name ▴	Channels used	Avg. channel utilization (2.4 GHz)	Avg. channel utilization (5 GHz)
BERHA-AP08-F00-POTSDAM I	1,60	● 19% - low	● 1% - very low
BERHA-AP09-F00-POTSDAM I	1,52	● 34% - fair	● 0% - very low
BERHA-AP10-F00-POTSDAM I	6,104	● 27% - low	● 2% - very low
BERHA-AP11-F00-POTSDAM II	6,36	● 45% - fair	● 0% - very low
BERHA-AP12-F00-POTSDAM II	1,112	● 34% - fair	● 1% - very low
BERHA-AP13-F00-POTSDAM II	1,48	● 31% - fair	● 0% - very low
BERHA-AP14-F00-POTSDAM II	1,56	● 38% - fair	● 1% - very low
Bellevue	11,64	● 5% - very low	● 0% - very low
Bellevue Gang	1,48	● 5% - very low	● 1% - very low
Bellevue Verteilerraum	6,108	● 4% - very low	● 0% - very low

Please make sure you verify appropriate 5GHz coverage while onsite during the post install survey by verifying -65dBm coverage with a smartphone and/or tablet. Please refer to the IHG Connect: Cisco Meraki Testing Installation Guide on the partner SharePoint site.

8. Splash page configuration

The splash page was previously provided by Cisco (EMSP, CMX, or DNA Spaces) has now been replaced by IHG EDGE.

The EDGE splash page requires an interface into the PMS which is now mandatory for all hotels and included in the brand standards. To get started, introduce the hotel IT contact by emailing EDGE.EMEAA@ihg.com

Further details on the EDGE interface along with process documentation can be found by visiting the IHG Connect Approved Wi-Fi Service Partners SharePoint site here or https://ihg.sharepoint.com/sites/euwsps

9. Meraki port profiles

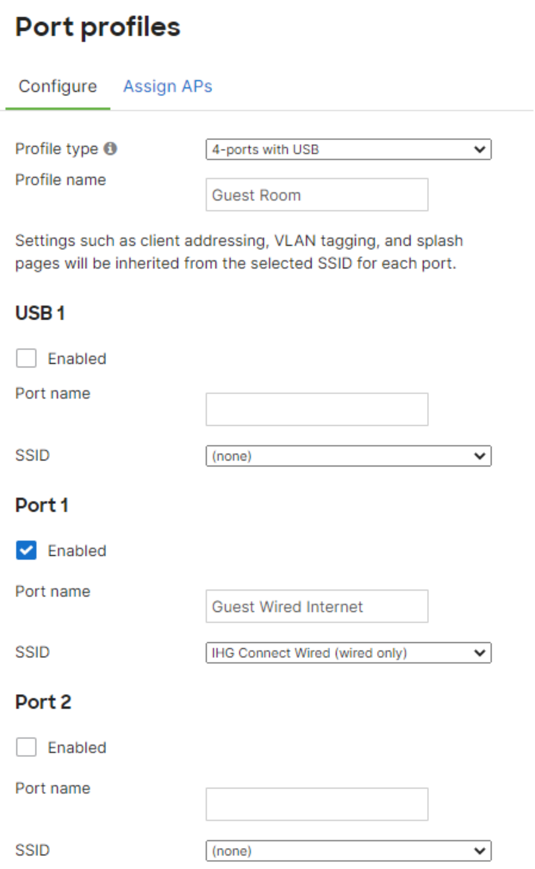
MR port profiles is a feature delivered via the dashboard to set configuration of the LAN ports on Meraki MR30H/MR36H access points. The AP port profiles map an SSID to a wired port on an access point. An AP Port profile can be found on the Summary tab of an AP that contains multiple ports.

The configuration page can also be accessed either on the AP's Ports tab or navigating to:
Wireless -> Configure -> Port Profiles

Configuring an AP Port Profile

To configure and manage port profiles, navigate to: **Wireless -> Configure -> Port profiles**.

Create a new Profile by clicking the Create new profile button or select an existing profile to adjust the configuration. Enable the ports via the toggle switches, name the port for future reference, and select the SSID intended to be extended to wired devices on each



Port profiles

Profile type: 4-ports with USB
Profile name: Guest Room

Settings such as client addressing, VLAN tagging, and splash pages will be inherited from the selected SSID for each port.

USB 1
□ Enabled
Port name:
SSID: (none)

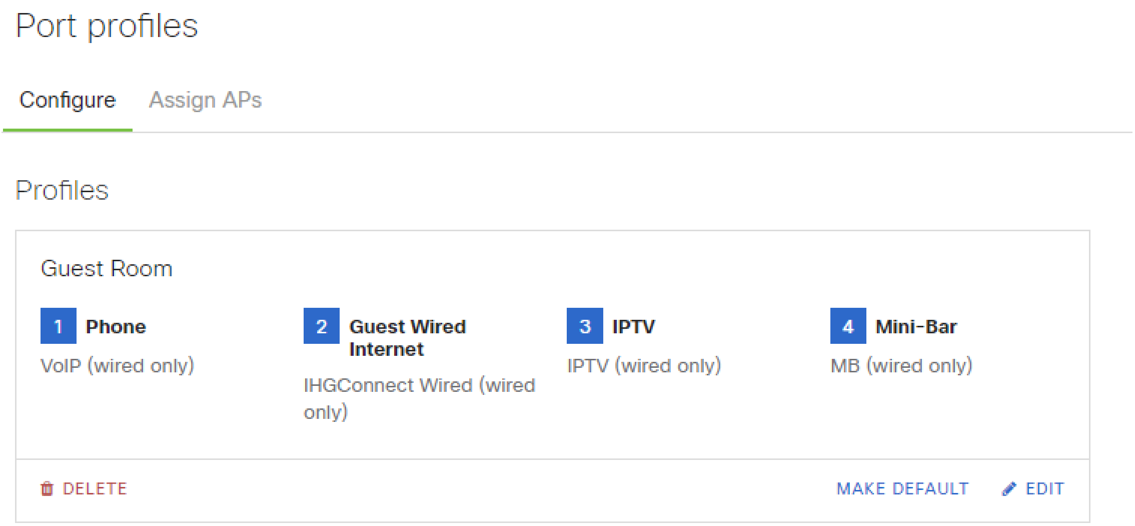
Port 1
☑ Enabled
Port name: Guest Wired Internet
SSID: IHG Connect Wired (wired only)

Port 2
□ Enabled
Port name:
SSID: (none)

9.1 Applying an AP port profile

The AP port profile that is currently configured on a given AP (with multiple ports) can be viewed and changed on the details page under the Summary tab. When an AP is initially added to the Dashboard, the default AP port profile will be applied to the Access Point. Only one default profile is needed, no additional configuration is necessary.

In most cases, it is common for a main AP port profile to be configured across all APs. **Setting an AP port profile as the "Default" will configure all APs that don't have an existing override to inherit the default profile.**



Port profiles

Configure | Assign APs

Profiles

Guest Room

1 **Phone**
VoIP (wired only)

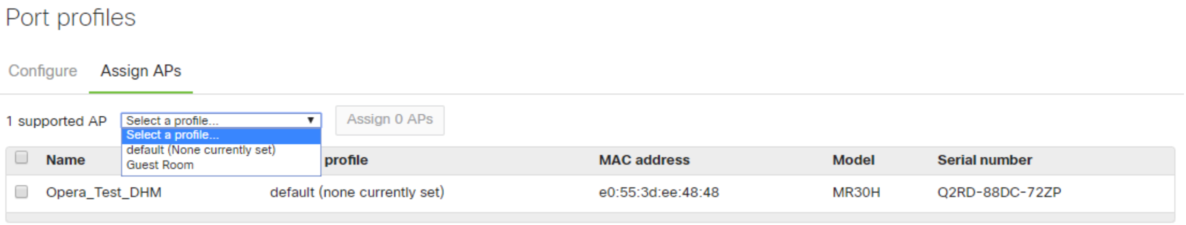
2 **Guest Wired Internet**
IHGConnect Wired (wired only)

3 **IPTV**
IPTV (wired only)

4 **Mini-Bar**
MB (wired only)

Bulk Override and Configure Profiles

Please navigate to **Wireless -> Configure -> Port profile -> Assign APs** page in order to bulk update the override configuration for the port profiles. Check the box next to each AP to assign a new profile or restore back to the default.



Port profiles

Configure | Assign APs

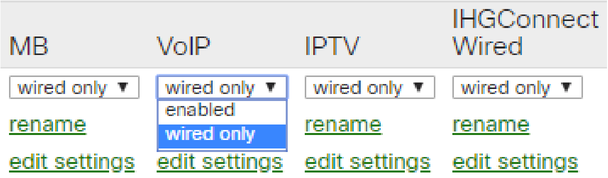
1 supported AP — Select a profile...

	Name	profile	MAC address	Model	Serial number
□	Opera_Test_DHM	default (none currently set)	e0:55:3d:ee:48:48	MR30H	Q2RD-88DC-72ZP

NB: We recommend that when assigning switch ports to wired services, you do so in sequential order starting with port 1.

9.2 Wired only SSID

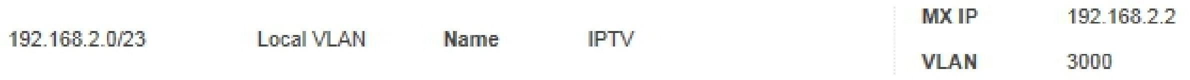
Any SSID can be mapped to a wired port even if it is not intended to serve wireless clients. SSIDs that are disabled become "wired only" when selected by a port profile. "Wired only" is an SSID mode that disables wireless connectivity, only allowing for wired connectivity. To remove wired access from a "wired only" SSID, the SSID must be removed from the AP port profiles.



MB	VoIP	IPTV	IHGConnect Wired
wired only ▼	wired only ▼ enabled wired only	wired only ▼	wired only ▼
rename		rename	rename
edit settings	edit settings	edit settings	edit settings

Prerequisites as an example:

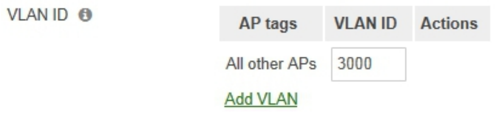
1. Create new SSID called IPTV
2. You can leave the network disabled for now.
3. Association requirements - Open (no encryption)
4. Client IP assignment - Bridge mode: Make clients part of the LAN
5. VLAN tagging – use VLAN tagging
6. Create VLAN 3000 with IP address 192.168.2.2/23



192.168.2.0/23 Local VLAN Name IPTV

MX IP	192.168.2.2
VLAN	3000

Assign VLAN 3000 to the IPTV network in the SSID settings page.



VLAN ID

AP tags	VLAN ID	Actions
All other APs	3000	

Add VLAN

7. Assign the IPTV SSID to AP Port Profile and name the ports.
8. The SSID will be activated on the port profile as wired only.

Test the configuration.

10. Network wide configuration

10.1 Local administrators

In some instances, it may be necessary to add local administrators for a particular hotel. Available privileges include full access, read only access, or monitor mode access where local administrators or hotel management have visibility into some of the analytics.

To request a user, please email IHGConnectEMEAA@ihg.com

Due to data privacy legislation and liability issues this needs to be agreed before any external party has access to any IHG Connect Meraki ORG. Partners should not under any circumstances add users to hotel networks.

10.2 Alerts

There are a variety of alerts that can be triggered from the Dashboard and sent via email or SMS. Alerts for the MX Security Appliance, MS Switches, and MR Access Points can all be configured on the Alerts & administration page.

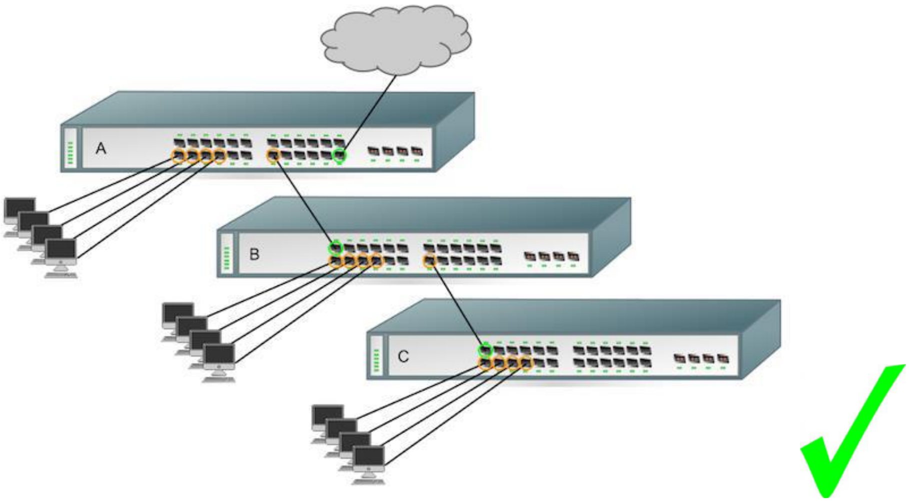
All alerts must be set to a 5-minute minimum to meet IHG Service Level Agreements. Please configure as required and include integrator support email addresses in each field.

11. Implementation best practices

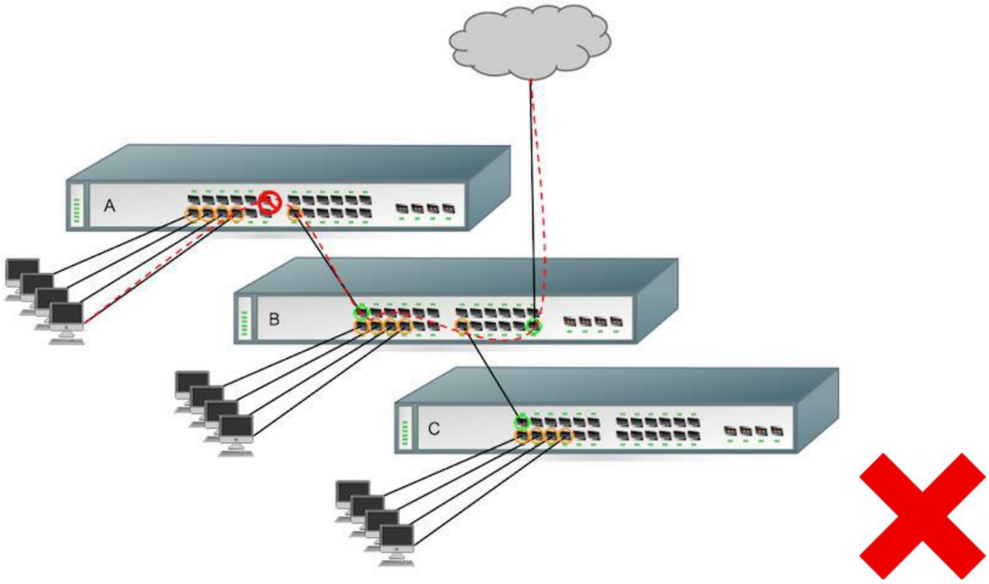
11.1 Port isolation

When ports on a switch have been isolated, the MS will not send any layer-2 network traffic from one isolated port to another. This can be useful in a multi-tenant environment, for example, where clients should be unable to send traffic to each other.

In the following two example diagrams, the orange ports indicate isolated ports, and the green ports have isolation disabled. The topology below is an example of port isolation being used to block inter-client communication, while still allowing Internet access:



When implementing port isolation, it is important to ensure that the appropriate ports have been isolated, so that traffic can reach the appropriate destination. In the example below, switch A’s uplink port has been isolated, so clients connected to any other isolated port on A are unable to communicate with the gateway:



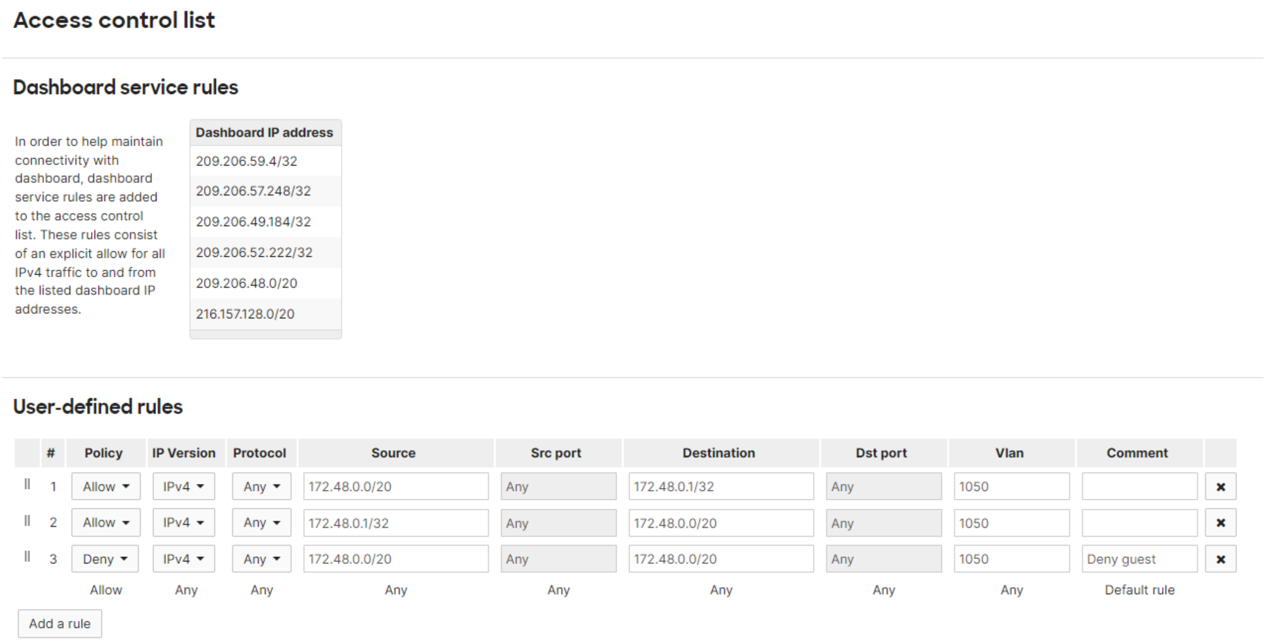
In instances when port isolation cannot be applied because of switch hardware limitation or switch configured as a cross stack member, please apply Access Control List (ACL) as per below screenshot to restrict traffic between users on (wired) guest VLAN 1050.

Navigate to Switching -> Configure -> ACL

Default rule allow Any will be added automatically.

Rule 1: Allow traffic to reach default gateway
Rule 2: Allow return traffic
Rule 3: Deny guest to guest traffic
Default rule allow any will be added automatically

Save.



Access control list

Dashboard service rules

In order to help maintain connectivity with dashboard, dashboard service rules are added to the access control list. These rules consist of an explicit allow for all IPv4 traffic to and from the listed dashboard IP addresses.

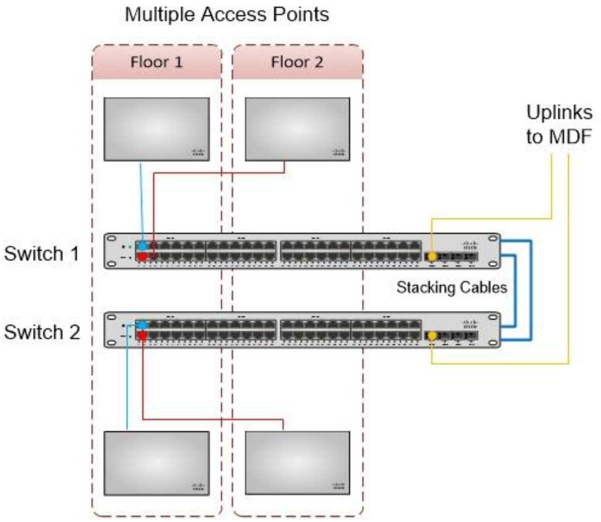
Dashboard IP address
209.206.59.4/32
209.206.57.248/32
209.206.49.184/32
209.206.52.222/32
209.206.48.0/20
216.157.128.0/20

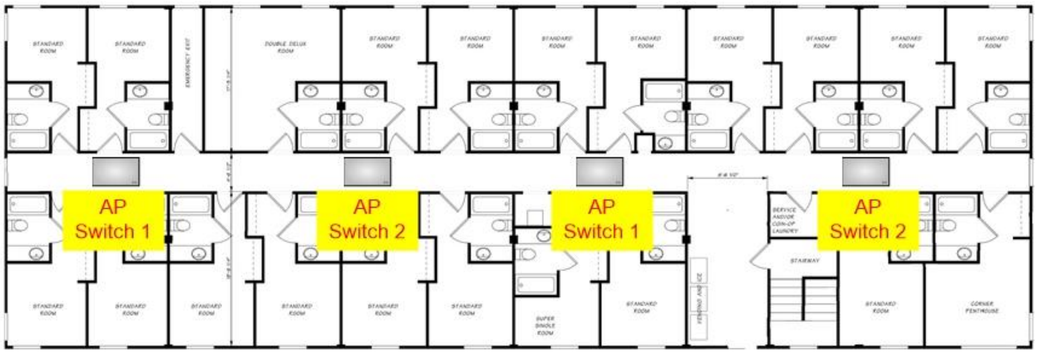
User-defined rules

#	Policy	IP Version	Protocol	Source	Src port	Destination	Dst port	Vlan	Comment	
1	Allow	IPv4	Any	172.48.0.0/20	Any	172.48.0.1/32	Any	1050		✖
2	Allow	IPv4	Any	172.48.0.1/32	Any	172.48.0.0/20	Any	1050		✖
3	Deny	IPv4	Any	172.48.0.0/20	Any	172.48.0.0/20	Any	1050	Deny guest	✖
	Allow	Any	Any	Any	Any	Any	Any	Any	Default rule	

11.2 Access point to switch connectivity

Should you have multi-floor connectivity to the same IDF switch stack of two or more switches, please use the approach as per the diagram below to build in redundancy in the event of a single switch failure.





11.3 Guest authentication page setup (wired & wireless)

This is configured by the IHG EDGE team.

The wired authentication page is not configured as standard, therefore please email IHGConnectEMEAA@ihg.com to make this request.

11.4 Schedule firmware upgrades

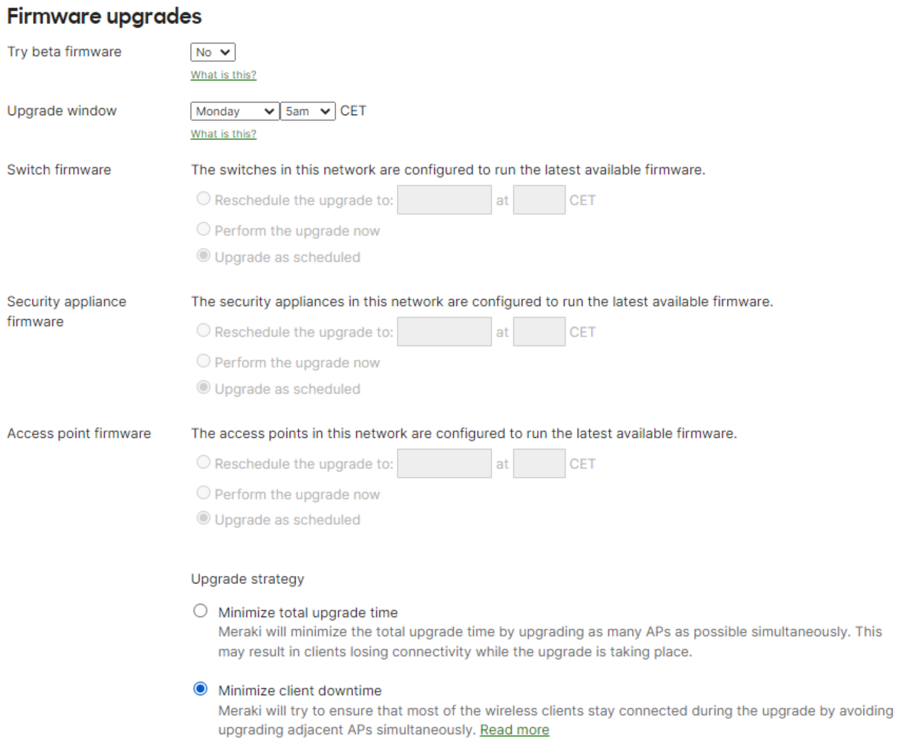
Please be aware that Meraki hardware may not be delivered with latest firmware pre-installed, so ensure that the firmware is upgraded to the latest version.

Check firmware version for the security appliance, switches, and access points by clicking on device via the Dashboard. Under the Status section, refer to the line for Configured firmware. This should read "Up to date".

Firmware upgrades must be done at the beginning of the hardware installation

You may connect a few devices first to initiate upgrade, then every other device of the same type will upgrade automatically when it comes online.

Network Wide - Configure - General



Firmware upgrades

Try beta firmware: No
What is this?

Upgrade window: Monday 5am CET
What is this?

Switch firmware: The switches in this network are configured to run the latest available firmware.
○ Reschedule the upgrade to: ___ at ___ CET
○ Perform the upgrade now
● Upgrade as scheduled

Security appliance firmware: The security appliances in this network are configured to run the latest available firmware.
○ Reschedule the upgrade to: ___ at ___ CET
○ Perform the upgrade now
● Upgrade as scheduled

Access point firmware: The access points in this network are configured to run the latest available firmware.
○ Reschedule the upgrade to: ___ at ___ CET
○ Perform the upgrade now
● Upgrade as scheduled

Upgrade strategy

○ Minimize total upgrade time
Meraki will minimize the total upgrade time by upgrading as many APs as possible simultaneously. This may result in clients losing connectivity while the upgrade is taking place.

● Minimize client downtime
Meraki will try to ensure that most of the wireless clients stay connected during the upgrade by avoiding upgrading adjacent APs simultaneously. Read more

Firmware upgrades are released periodically in a manner that is minimally disruptive to administrators and users. For a Meraki device to upgrade to the latest firmware, Meraki devices must be connected to the Internet to reach the Meraki Cloud. Set the upgrade strategy to Minimize client downtime.

The best way to see if a device is up to date is by navigating to the details page on Dashboard. Please check Status section check line Configure firmware.

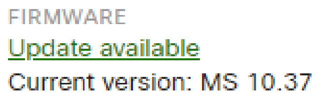
For MX Series Security Appliances go to:
Security & SD-WAN -> Monitor -> Appliance status

For MS Series Switches go to:
Switching -> Monitor -> Switches

For MR Series Access Points go to:
Wireless -> Monitor -> Access points

If a newer firmware version is available, the **configured firmware** field will indicate that an update is available and provide a link to where it can be scheduled:

For example



FIRMWARE

Update available

Current version: MS 10.37

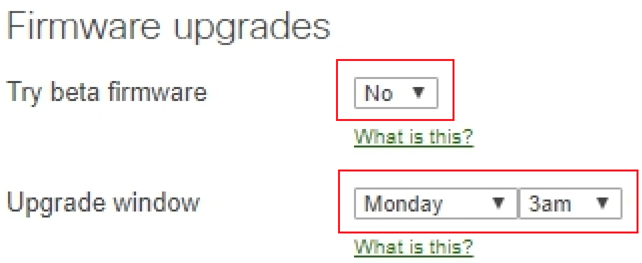
Periodic upgrades will be scheduled to occur beginning at the **Upgrade window** time specified in:

Network-wide -> Configure -> General -> Firmware upgrades

Please do not enable beta firmware upgrade.

Set upgrade window to Monday 3 AM local time (please check with hotels if they require a different time window)

Sections for Switch, Security appliance, Access Point firmware should be set to Upgrade as scheduled.



Firmware upgrades

Try beta firmware: No ▼

What is this?

Upgrade window: Monday ▼ 3am ▼

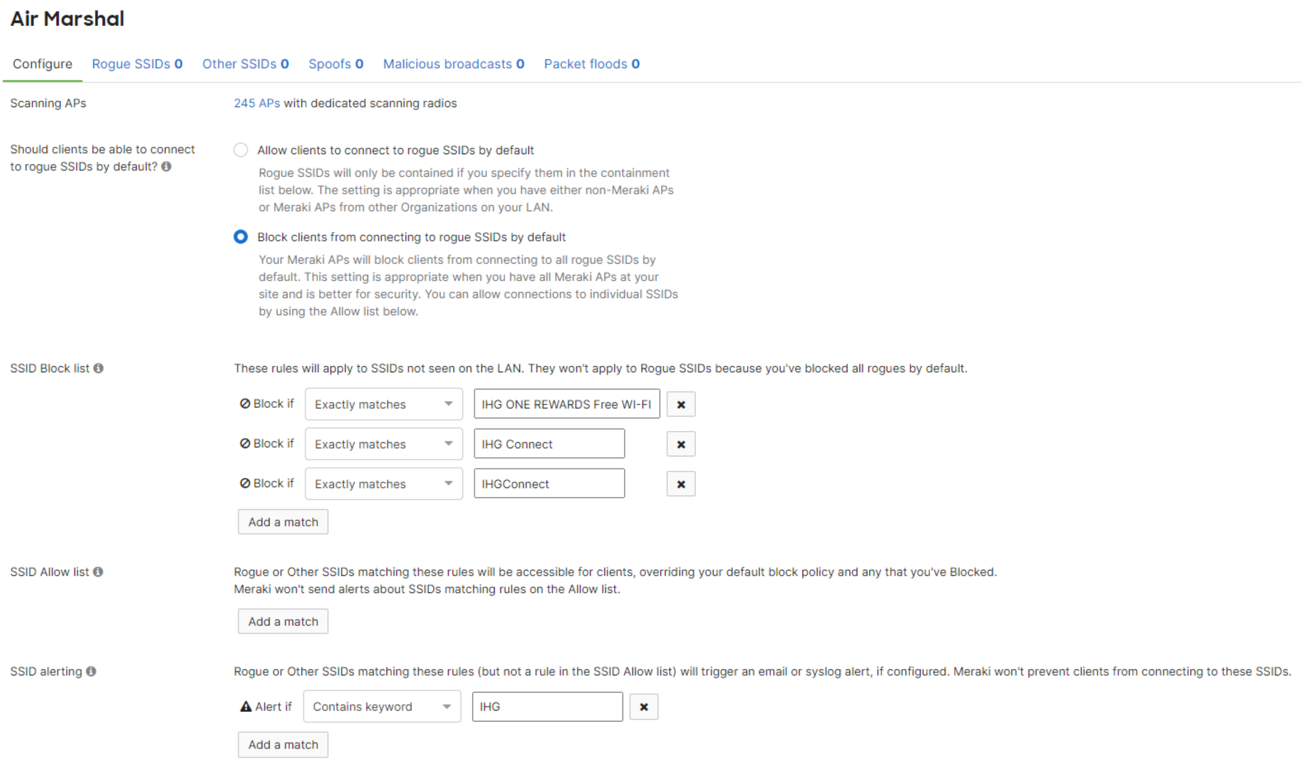
What is this?

11.5 Air Marshal

Meraki’s cloud managed wireless access points come equipped with Air Marshal, a built-in wireless intrusion detection and prevention system (WIDS/WIPS) for threat detection and attack remediation. APs configured in Air Marshal mode will scan their environment in real-time and take pre-emptive action based on intuitive user-defined preferences. Air Marshal triggers alarms and automatically contains malicious rogue APs.

Wireless > Monitor > Air Marshal > Configure

Please configure Air Marshall as per the settings below.



Air Marshal

Scanning APs: 245 APs with dedicated scanning radios

Should clients be able to connect to rogue SSIDs by default?

○ Allow clients to connect to rogue SSIDs by default

Rogue SSIDs will only be contained if you specify them in the containment list below. The setting is appropriate when you have either non-Meraki APs or Meraki APs from other Organizations on your LAN.

● Block clients from connecting to rogue SSIDs by default

Your Meraki APs will block clients from connecting to all rogue SSIDs by default. This setting is appropriate when you have all Meraki APs at your site and is better for security. You can allow connections to individual SSIDs by using the Allow list below.

SSID Block list

These rules will apply to SSIDs not seen on the LAN. They won't apply to Rogue SSIDs because you've blocked all rogues by default.

- Block if Exactly matches IHG ONE REWARDS Free WI-FI
- Block if Exactly matches IHG Connect
- Block if Exactly matches IHGConnect

SSID Allow list

Rogue or Other SSIDs matching these rules will be accessible for clients, overriding your default block policy and any that you've Blocked.
Meraki won't send alerts about SSIDs matching rules on the Allow list.

SSID alerting

Rogue or Other SSIDs matching these rules (but not a rule in the SSID Allow list) will trigger an email or syslog alert, if configured. Meraki won't prevent clients from connecting to these SSIDs.

- Alert if Contains keyword IHG

12. IHG Connect team help & support

Should you require further assistance, please contact the IHG Connect EMEAA team IHGConnectEMEAA@ihg.com or for the splash page the IHG EDGE team EDGE.EMEAA@ihg.com

13. Meraki dashboard configuration checklist

Network-wide settings

1. Configure -> General
   a. Set the local time zone under Local time zone □
   b. Set the Traffic analysis to Detailed □
   c. Set the Local credentials under Device configuration □
   d. Set the Firmware upgrade schedule and upgrade all hardware to the latest version □
   e. If required, turn off LED lights (for MR30H/MR36H installations) □

2. Configure -> Administration
   a. Do not add any additional users here. If required email the IHG Connect team. □

3. Configure -> Alerts
   a. Configure the Meraki alerts as required. □

4. Configure -> Group policies
   a. Setup the required group policy: Deny Local WLAN □
   b. Setup the required group policy: Deny Local LAN □
   c. Setup the required group policy: ByPass Splash □

5. Monitor -> Map & floor plans
   a. Upload all the hotel floor plans and place the access points in the correct locations □

Security & SD-WAN settings

1. Monitor -> Appliance status
   a. Set the MX(s) name as per the naming convention □
   b. Uplink -> Configuration and set the public IP details □
   c. Configure warm spare (if required) □
   d. Add the hotel address location □

2. Configure -> Addressing & VLANs
   a. Configure the mandatory VLAN 100 □
   b. Configure the mandatory VLAN 999 □
   c. Configure the mandatory VLAN 1000 □
   d. Configure the mandatory VLAN 1050 □
   e. Assign the Per-port VLAN Settings □
   f. Disable the unused ports □
   g. Set the Static route for VLAN 999 □

3. Configure -> DHCP
   a. Set the reserved ranges □
   b. Disable DHCP for VLAN 999 □

4. Configure -> Firewall
   a. Add the deny rules □

5. Configure -> SD-WAN & traffic shaping
   a. Set the uplink configuration □
   b. Set the Uplink selection □
   c. Set the Traffic shaping rules □

Switching settings

1. Monitor -> Switches
   a. Set the switch names as per the naming convention □
   b. Add the address details □
   c. Set static IPs for all switches on VLAN 100 □
   d. Set port configuration and apply naming convention on all switches □
   e. Disable all unused ports on all switches □

2. Configure -> ACL
   a. Set the ACL configuration □

Wireless settings

1. Monitor -> Access points
   a. Set the access point names as per the naming convention □

2. Configure -> SSIDs
   a. Ensure IHG ONE REWARDS Free WI-FI is configured on SSID1 □

3. Configure -> Access control
   a. Network access leave as Open (no encryption) □
   b. Splash page leave as default None (direct access). Splash page configuration is done as part of the EDGE activation □
   c. Set Client IP and VLAN to External DHCP server assigned Bridge mode □
   d. Enable VLAN tagging set the VLAN ID to 1000 □

4. Configure -> Radio settings
   a. Setup RF profiles and assign to all APs □
   b. Manually configure APs power/channels if required □

5. Configure -> Firewall & traffic shaping
   a. Ensure that Wireless clients accessing LAN is set to Deny □
   b. Set the Per-client bandwidth limit □
   c. Disable traffic shaping on the SSID IHG ONE REWARDS Free WI-FI □

6. Configure -> Port profiles (switching APs only)
   a. Create the required SSIDs (for wired only) □
   b. Create new Port profile □
   c. Assign profile to APs □

7. Monitor -> Air Marshall
   a. Set the configuration □