Meetinghouse Meraki Switch Overview

The Cisco company purchased the Meraki company years ago and that is why the Cisco brand is on the Meraki Switch.

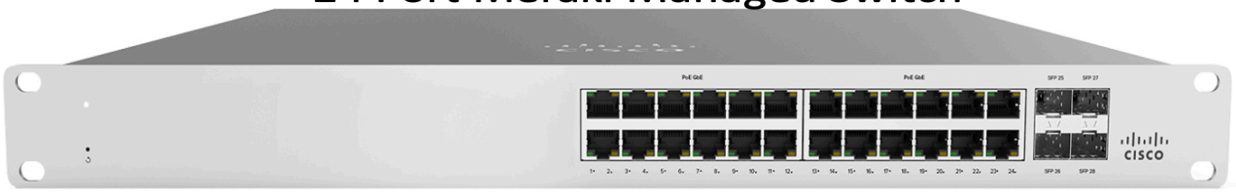
Meetinghouse firewalls have a limited number of local area network (LAN) ports that devices can be connected to. A network switch can be used to increase the number of available network ports. In most cases, facility management groups are responsible for purchasing and installing network switches.

A Meraki managed switch, pictured below, will provide remote management capabilities via TM and the Meraki dashboard. This remote management capability was not possible with the unmanaged switches. There are two Meraki managed switches models available for meetinghouses: MS120-8FP(PoE) and the MS120-24P(PoE).

MS120-8FP (PoE)
8 Port Meraki Managed Switch



MS120-24P (PoE)
24 Port Meraki Managed Switch



SFP Module -Optics 1000BASET
SFP transceiver module for
Category 5 copper wire



Meraki managed switches and SFP modules (shown above) are available for facility management groups to purchase on LDS eMarket.

Speeds – 10/100/1000
Power-over-Ethernet (PoE) Ports – required because the Meraki MR33 wireless access points and other PoE enabled devices must connect to the Meraki managed switch.
Port Density – varies depending on local needs.
Type - Managed via internet in TM and the Meraki dashboard

A Meraki managed switch is installed by connecting port SFP9 on an 8 Port switch or SFP25 on a 24 port Meraki Switch to port 1 on the Meraki firewall using a network cable. An SPF module is required in the SFP ports prior to connecting a data cable.

For complete installation details refer to the Meraki Switch Installation Guide.pdf.

Installing and Activating the Meraki Switch in Technology Manager

1. Remove the Meraki Switch from the box and enter the Serial Number(SN) into Technology Manager on the Switches page.
2. To locate the Switches page in TM:
    1. Locate the meetinghouse name where you are installing the new Meraki Switch
    2. Click on the Firewall serial number of the correct meetinghouse
        - IMPORTANT NOTE - Verify you are adding the switch to the correct Firewall by matching the SN on the Firewall to the Serial Number on this TM page
        - If the Serial Numbers do not match then call the GSD. The Firewall must have been activated at the incorrect meetinghouse
    3. Click on the "DEVICES" drop down menu and click on "Switches"
    4. Enter the new Switch's Serial Number into the "Add a Switch" field
    5. Click Submit

Configuring each Meraki Switch Port

In Technology Manager you can configure each Meraki Switch port to one of the following values. To do so click on the “Manage” button next to the switch that you are configuring.

AP – use this for Meraki Wireless Access Points(APs) only. Meraki APs must be connected to the Meraki Switch. The Meraki Switches are POE and do not require a power injector.

Link - only use if the SFP ports are unavailable on the first Meraki Switch and an additional Meraki Switch is needed in the same meetinghouse. “LINK” can also be used to connect a Meraki switch to Port 1 on the Meraki Firewall if an SFP port is not available.

Public Zone – Clerk’s and Unit Leader’s offices, Material Center, Podium, Chapel, and all classrooms in the Meetinghouse. Most data cables will be on the Public Zone.

Facility Zone - Devices that are managed remotely by facility managers, or need the ability to communicate between buildings (Generally HVAC, Door Looks, etc.) Prior to installing the Meraki switch these devices were connected to Port 4 on the Meraki Firewall. Do not leave these devices connected to the Firewall ports.

Disabled - unused port or a port that you don't want to be used without authorization

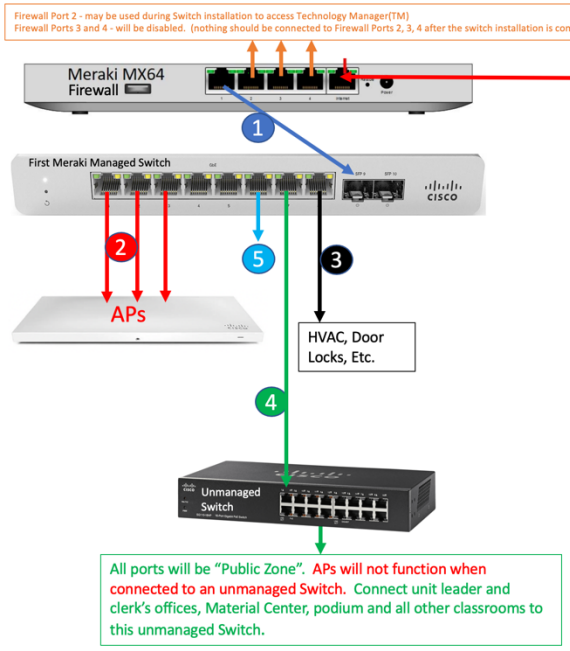
The following 2 options will only be available on the port configuration menu if they have been added to the Firewall as a possible zone.

Special Purpose Zone - Family History Center (FHC), if the FHC is already using the PUBLIC zone then continue to use the PUBLIC Zone. If APs are in the FHC then they must be connected directly to a Meraki Switch. You may need to purchase an additional Meraki Switch for the FHC or run a data cable from the AP back to the main Meraki Switch that is connected to the Firewall.

Workforce Zone - Seminary and Institute Teacher Offices, FM offices, Family Services offices, or any port that is being used by a Church employee.

Meetinghouse Firewall and Switch network configurations

Figure 1 - One Meraki MS120-8FP (8 port switch) Configuration

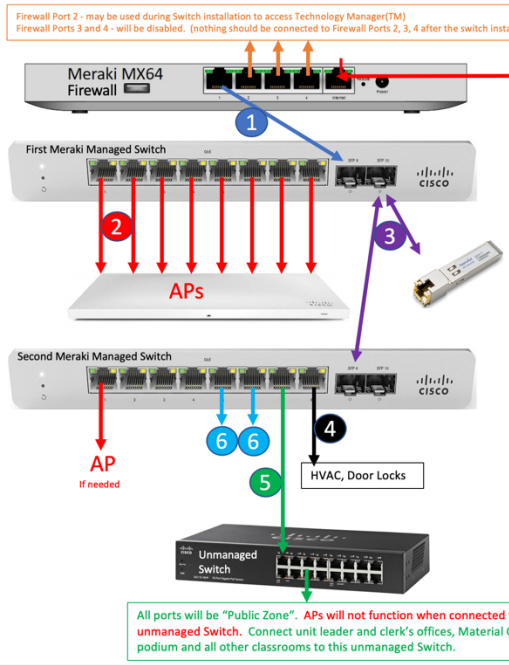


Steps to configure a single 8 port Meraki Switch with an unmanaged Switch:

1. Connect Port 1 of the MX64 Meraki Firewall to the SFP 9 port on the new Meraki Switch (The SFP module is already installed in SFP 9)
2. Connect all Meraki Wireless Access Points (APs) to the first Meraki Switch starting with Port 1. Use as many ports as needed. If the meetinghouse has more than 4 APs then see Figure 2 – Configuration for two Meraki Switches.
3. Disconnect the Facility Zone device from the Firewall and connect to Port 8 on the Meraki Switch. Facility Zone devices are normally managed remotely by facility managers, or need the ability to communicate between buildings (Generally HVAC, Door Looks, etc.) If the meetinghouse has more than 1 Facility Zone device then use another available port on the Meraki Switch or use an unmanaged switch on port 8.
4. Connect Port7 on the Meraki Switch to Port 1 on the unmanaged switch. Connect unit leader and clerk's offices, material center, podium, chapel and all other classrooms in the meetinghouse to the unmanaged Switch. An SFP module is not needed to connect the unmanaged switch to the Meraki Switch. All of these will be "Public Zone" connections.
5. If a Special Purpose Zone(Family History Center) and/or a Workforce Zone(Seminary, Institute) is present in the meetinghouse then configure these ports to be the correct zone.

NOTE: All remaining ports on the First Meraki Switch can be configured as needed to be AP, Link, Public, Facility, Special Purpose, Workforce or disabled if not used.

Figure 2 - Two Meraki MS120-8FP (8 port switches) Configuration

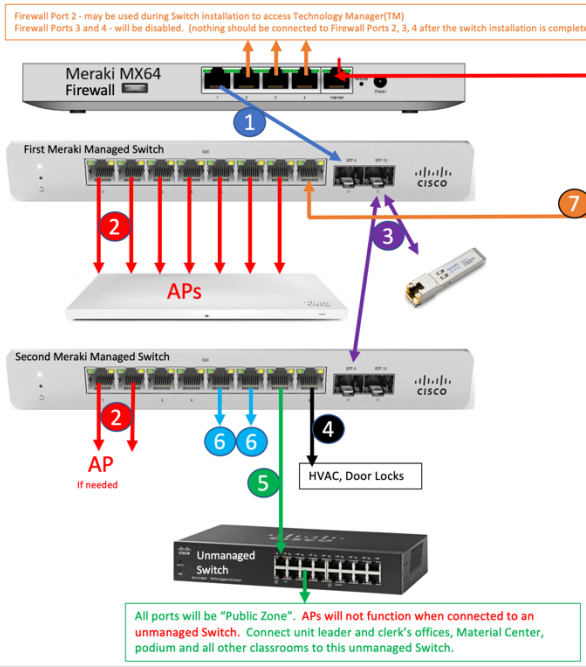


Steps to configure two 8 port Meraki Switches with an unmanaged Switch:

1. Connect Port 1 of the MX64 Meraki Firewall to the SFP 9 port on the new Meraki Switch (the SFP module is already installed in SFP9)
2. Connect all Meraki Wireless Access Points (APs) to the first Meraki Switch starting with Port 1. Use as many ports as needed. If you have more than 8 APs then connect the additional APs to the second Meraki Switch.
3. Install an SFP Module into Port 10 on the first Meraki Switch and connect it to Port 9 on the second Meraki Switch.
4. Disconnect Facility Zone devices from the Firewall and connect these to Port 8 on the Meraki Switch. Facility Zone Devices are normally managed remotely by facility managers, or need the ability to communicate between buildings (Generally HVAC, Door Looks, etc.) If the meetinghouse has more than 1 Facility Zone device then use another available port on the Meraki Switch or an unmanaged Switch on port 8.
5. Connect Port7 on the second Meraki Switch to Port 1 on the unmanaged Switch. Connect unit leader and clerk's offices, material center, podium, chapel and all other classrooms in the meetinghouse to this unmanaged Switch. An SFP module is not needed to connect the unmanaged switch to the Meraki Switch. All of these will be "Public Zone" connections.
6. If a Special Purpose Zone(Family History Center) and/or a Workforce Zone(Seminary, Institute) is present in the meetinghouse then configure these ports to be the correct zone.

NOTE: All remaining ports on the First and Second Meraki switches can be configured as needed to be AP, Link, Public, Facility, Special Purpose, Workforce or disabled if not used.

Figure 3 - Three Meraki MS120-8FP (8 port switches) Configuration

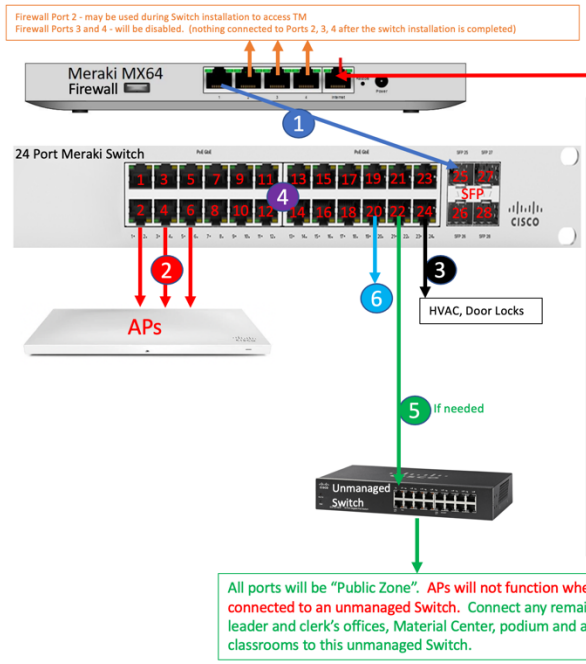


NOTE: All remaining ports on the Meraki switches can be configured as needed to be AP, Link, Public, Facility, Special Purpose, Workforce or disabled if not used.

Steps to configure two 8 port Meraki Switches with an unmanaged Switch:

1. Connect Port 1 of the MX64 Meraki Firewall to the SFP 9 port on the new Meraki Switch (the SFP module is already installed in SFP9)
2. Connect all Meraki Wireless Access Points (APs) to the first Meraki Switch starting with Port 1. Use as many ports as needed. If you have more than 8 APs then connect the additional APs to a second Meraki Switch.
3. Install an SFP Module into Port 10 on the first Meraki Switch and connect it to Port 9 on the second Meraki Switch.
4. Disconnect Facility Zone devices from the Firewall and connect these to Port 8 on the Meraki Switch. Facility Zone Devices are normally managed remotely by facility managers, or need the ability to communicate between buildings (Generally HVAC, Door Looks, etc.) If the meetinghouse has more than 1 Facility Zone device then use another available port on the Meraki Switch or an unmanaged Switch on port 8.
5. Connect Port7 on the second Meraki Switch to Port 1 on the unmanaged Switch. Connect unit leader and clerk's offices, material center, podium, chapel and all other classrooms in the meetinghouse to this unmanaged Switch. An SFP module is not needed to connect the unmanaged switch to the Meraki Switch. These connections will be "Public Zone".
6. If a Special Purpose Zone(Family History Center) and/or a Workforce Zone(Seminary, Institute) is present in the meetinghouse then configure these ports to be the correct zone.
7. If a Third Meraki Switch is needed then connect it to Port 8 on the first Meraki Switch and configure Port 8 on the first Meraki Switch to be "Link". Do not connect the third Meraki Switch to the second Meraki Switch.

Figure 4 - One Meraki MS120-24P (24 port switch) Configuration



Steps to configure a 24 port Meraki Switch with an (if needed) unmanaged Switch:

1. Connect Port 1 of the MX64 Meraki Firewall to port SFP 25 on the new Meraki Switch (The SFP module is already installed in SFP 25)
2. Connect all Meraki Wireless Access Points (APs) to the first Meraki Switch starting with Port 1. Use as many ports as needed.
3. Disconnect Facility ZTMone devices from the Firewall and connect these to Ports 23 and 24 on the Meraki Switch. Facility Zone Devices are normally managed remotely by facility managers, or need the ability to communicate between buildings (Generally HVAC, Door Looks, etc.) If the meetinghouse has more than 1 Facility Zone device then use another available port on the Meraki Switch or an unmanaged Switch on port 24.
4. All remaining available ports on the Meraki 24 Port Switch can be configured to AP, Link, Public, Facility, Special Purpose, Workforce or disabled. Move as many cables from the unmanaged Switch to the new Meraki 24 Port Switch as possible. Most of these will be "Public Zone" ports for local unit leader and clerk's offices, material center, podium, and all other classrooms in the meetinghouse.
5. If needed – Connect Port 22 on the Meraki Switch to Port 1 on the unmanaged Switch. Connect any remaining unit leader and clerk's offices, material center, podium, chapel and all other classrooms in the meetinghouse to this unmanaged Switch. An SFP module is not needed to connect the unmanaged switch to the Meraki Switch. These connections will be "Public Zone"
6. If a Special Purpose Zone(Family History Center) and/or a Workforce Zone(Seminary, Institute) is present in the meetinghouse then configure these ports to be the correct zone.

NOTE: All remaining ports on the Meraki switch can be configured as needed to be AP, Link, Public, Facility, Special Purpose, Workforce or disabled if not used.