

Meetinghouse Meraki Firewall and Switch Installation Guide

2025-2026
Meetinghouse
Technology Refresh

Meraki Managed Firewall

- The Meraki MX67 is the recommended firewall for meetinghouses at this time.
- If your meetinghouse has a MX64, MX65, or MX68 firewall replace it with an MX67.
- We also support the following firewalls. If your location already has one of these, it does not need to be replaced: MX75, MX85, MX95, MX250, and MX450
- Port 2 on the MX67 should be connected to an SFP port on the Meraki Switch using an SFP Module. * Ports 3, 4, 5 will be disabled.

*If you don't have an SFP module then connect to one of the Switch Access Ports and configure that switch port to be "LINK" in Church Network Manager. (CNM) (See page 13)

Meraki MX67 Firewall



Meraki Managed Switches

- ✓ For a successful install, please read the instructions before beginning the switch install or contacting the GSD for assistance. Reading and understanding this guide before you begin is imperative for success.
- ✓ Label cables before disconnecting them from any current switches.
- ✓ At least one Meraki managed switch must be installed in every meetinghouse worldwide
- ✓ All MS120 model Meraki switches will be removed as part of this install process. If a meetinghouse already has MS130 model switches, those can continue to be used
- ✓ Many meetinghouses use a combination of a Meraki switch and non-Meraki, unmanaged switches. **After this network refresh, unmanaged switches will no longer be allowed.** Any and all unmanaged switches must be removed and their connected devices connected to appropriately configured ports on Meraki managed switches (see page 13)
- ✓ The installer will need access to a mobile computer or an iPad with independent internet access in order to activate and configure the new switch(es) in CNM
- ✓ All wireless access points (APs) in the meetinghouse must connect directly to a Meraki managed switch. Do not connect old legacy Cisco APs into a Meraki Switch. Upgrade Cisco APs to Meraki APs.
- ✓ Order an SFP module when ordering a Meraki Switch.
- ✓ If a second Meraki switch is needed in the same meetinghouse then two additional SFP modules will be needed. Same goes for a third Meraki switch if needed
- ✓ You will need a screwdriver and wood screws if you are mounting a switch to a wall, cabinet, or rack
- ✓ You will need a pen or pencil, tape and paper to create a cable mapping sheet of the meetinghouse data drops
- ✓ The Switch installation will be much easier if you have 2 people to identify where each data cable connects. Especially for the Wireless Access Points.
- ✓ The Meraki switch(es) installed in a meetinghouse will be logically tied to the Meraki Firewall in the Meraki Cloud Management application.
- ✓ Use of the 48-port switch is an exception and should only be used when the number of in-use Ethernet network lines running to a single location exceeds 22. Any 48 port switches will have to be purchased by the FM group as none have been included in this 2025-2026 refresh project

MS130-8P (PoE) 8 Port Meraki Managed Switch



MS130-24P (PoE) 24 Port Meraki Managed Switch



MS130-48P (PoE) 48 Port Meraki Managed Switch

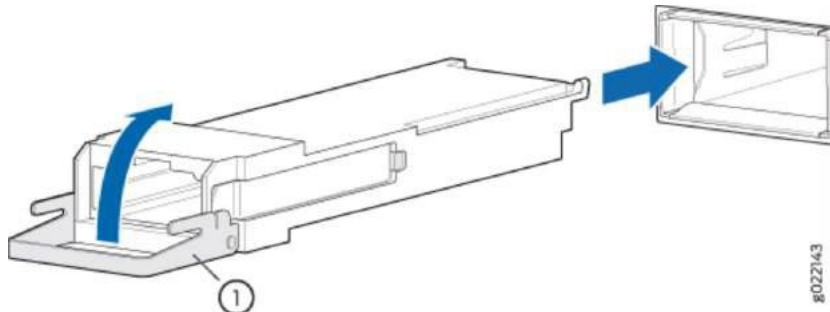


SFP Module – Approved Optics
1000BASE-T SFP transceiver
module for Category 5e/6
copper wire



SFP Modules

- Every switch will need a SFP module installed in port SFP 25 on the "24 Port switch" (port SFP 9 on the "8 Port switch" and port SFP 49 on the "48 port switch")
- If a second Meraki switch is needed in the same meetinghouse then two additional SFP modules will be needed. Install the extra SFP module in Port 26 of the first Meraki 24 Port switch (or port SFP 10/SFP 50 on the first 8 or 48 port switch respectively) to connect the two Meraki Switches.
- To install the SFP module- open the lock, insert the module and close the lock. This will lock the SFP module into the switch.
- Connect the data cable to the SFP modules with the lock closed in the locked position.
- To remove an SFP module- open the lock and remove the module from the switch.



1. Insert the SFP modules into the switch with the lock open and then close the lock

SFP Module –Approved Optics
1000BASE-T SFP transceiver
module for Category 5e/6
copper wire



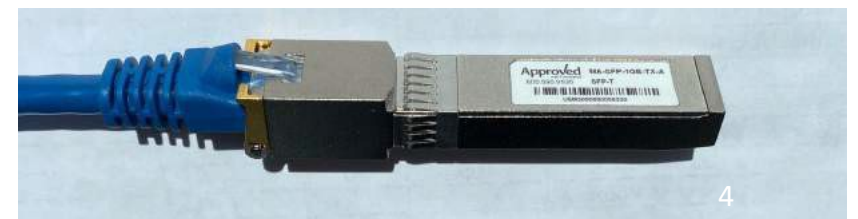
Lock is open



Lock is closed



Lock is closed with data cable connected

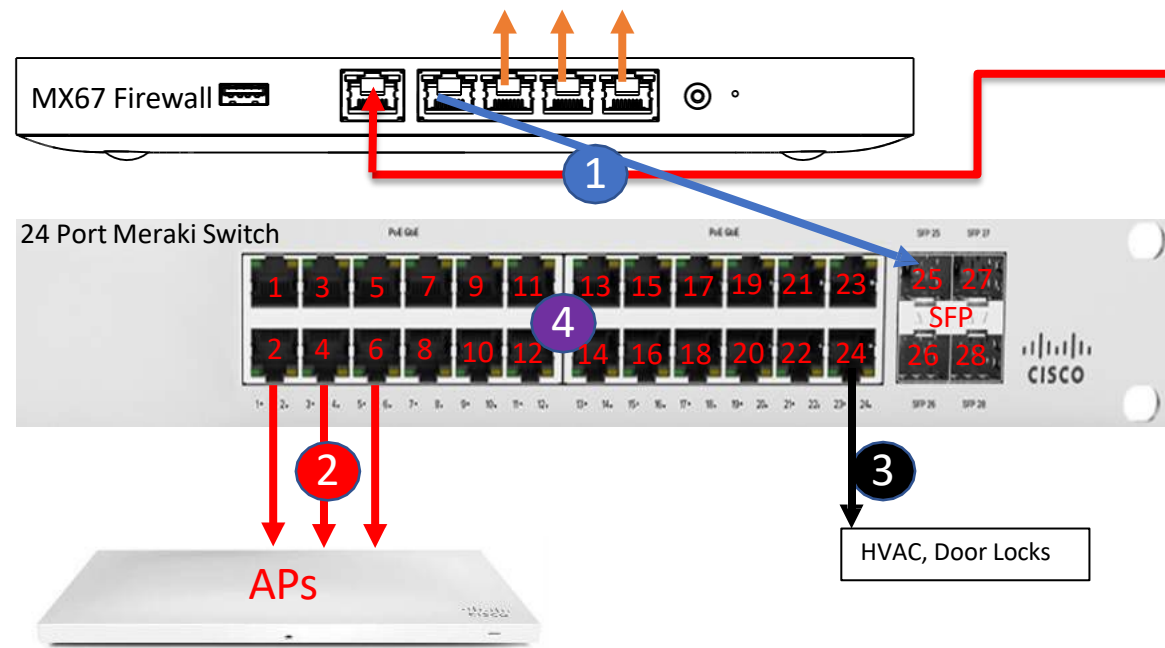


Steps before installing Meraki Managed Switches (MS130-8P,-24P,-48P)

1. Using tags or tape, identify and label the following possible cables connecting to:
 1. Wireless Access Points (tag as AP)
 2. Clerk's and unit Leader's offices (tag as Clerk or BP or SP)
 3. The HVAC, Door locks, and other Facility devices (tag as HVAC or Locks or FAC)
 4. Webcast equipment, Audio/Video distribution systems (tag as AV)
 5. The Family History Center (if present) (tag as FHC)
 6. The Seminary and Institute Teacher Offices and student classrooms (if present) (tag as S&I)
 7. FM office, Mission office, etc... (if present) (tag as FM or Mission)
 8. All other rooms in the meetinghouse (all of these will be public zone)
2. This is a great opportunity to determine if all classroom connections are used or needed. If they are no longer used, then leave the cables disconnected to reduce the number of needed switch ports. If you leave a room disconnected, then add a sticker to the data jack faceplate in that room stating that it is disconnected.
3. After labeling, take photos of the current configuration to inform the troubleshooting process if problems occur during the new switch installation.
 - a. It is recommended that you leave a sheet of paper with the cable and port mappings next to the switch. This will facilitate future changes to the network. (example: Port 7 on the switch goes to the Clerk's office, etc.)

Figure 1 - One Meraki MS130-24P (24 port switch) Configuration

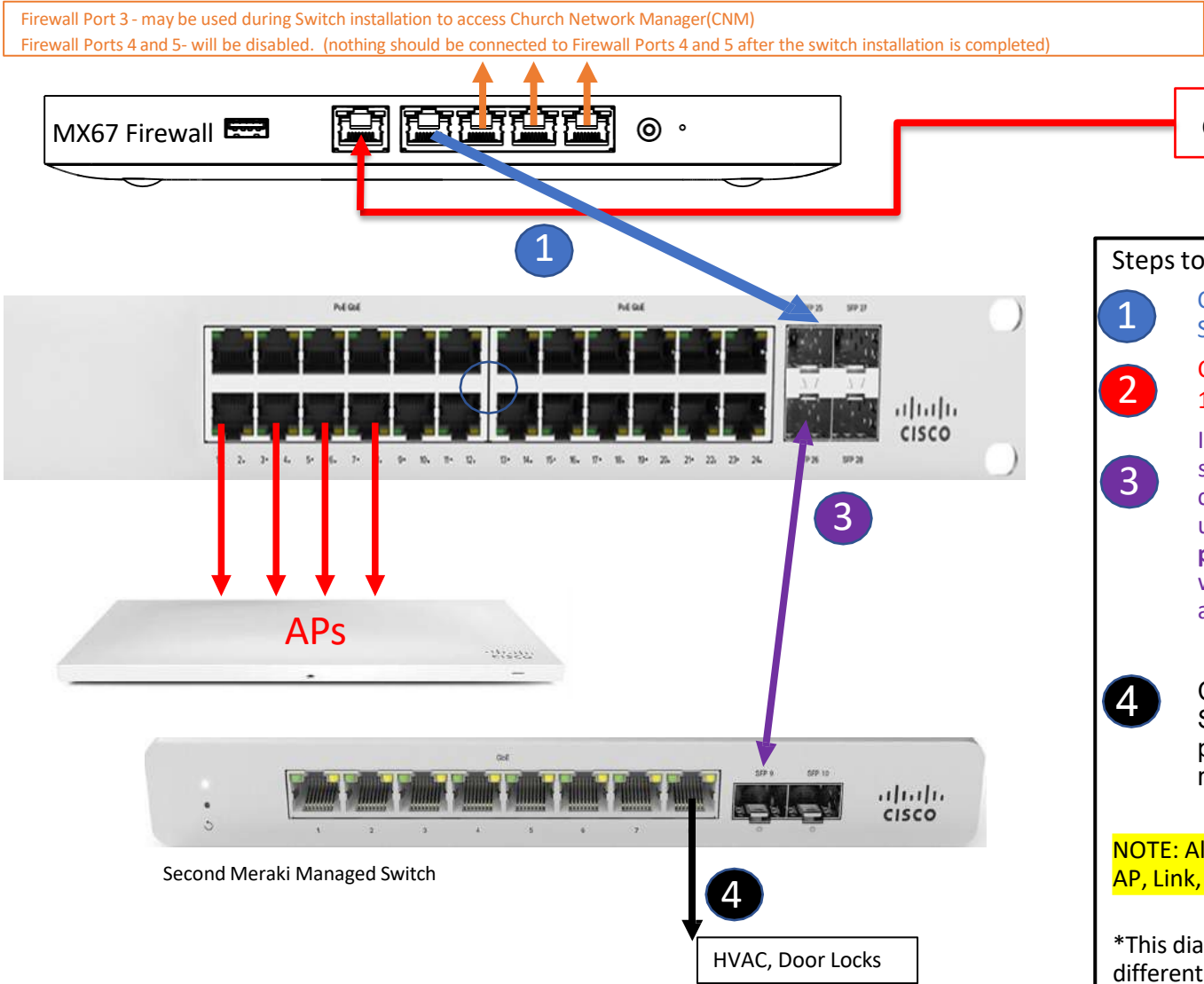
Firewall Port 3 - may be used during Switch installation to access CNM
Firewall Ports 4 and 5 - will be disabled. (nothing connected to Ports 4 and 5 after the switch installation is completed)



Cable Modem/ISP provided Internet Connection

- Steps to configure a 24 port Meraki Switch with an (if needed) unmanaged Switch:
- 1 Connect Port 2 of the MX67 Meraki Firewall to port SFP 25 on the new Meraki Switch (The SFP module should already be 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 any Facility Zone devices currently connected to the firewall or to any unmanaged switches and connect them to the highest numbered ports on the Meraki Switch, starting at 24 and moving down. Facility Zone Devices are normally managed remotely by facility managers, or need the ability to communicate between buildings (Generally HVAC, Door Locks, etc.)
 - 4 All remaining available ports on the Meraki 24 Port Switch can be configured to AP, Link, Public, Facility, IoT, Workforce or disabled. Move all cables from any unmanaged switches to the new Meraki 24 Port Switch. 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.
- NOTE: All remaining ports on the Meraki switch can be configured as needed to be AP, Link, Public, Facility, IOT, Workforce or disabled if not used.

Figure 2 - Two Meraki Switches Configuration



Steps to configure two Meraki Switches:

- 1 Connect Port 2 of the MX67 Meraki Firewall to the SFP 25 port on the new Meraki Switch (the SFP module should already be 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 Install an SFP Module into Port 26 on the first Meraki Switch and connect it to Port 9 on the second Meraki Switch. All remaining available ports on the Meraki 24 Port Switch can be configured to AP, Link, Public, Facility, IoT, Workforce or disabled. Move all cables from any unmanaged switches to the new Meraki 24 Port Switch. **No unmanaged switches are permitted to remain in meetinghouse network after this upgrade.** Most of the switch ports will be "Public Zone" ports for local unit leader and clerk's offices, material center, podium, and all other classrooms in the meetinghouse.
- 4 Connect facility devices (HVAC, door locks, etc.) to any available port on any Meraki Switch. Configure these ports as 'Facility' in CNM (see page 13). Remember: any port on a managed Meraki switch can be configured for any role as needed. The roles include AP, Link, Public, Facility, IOT, and Workforce.

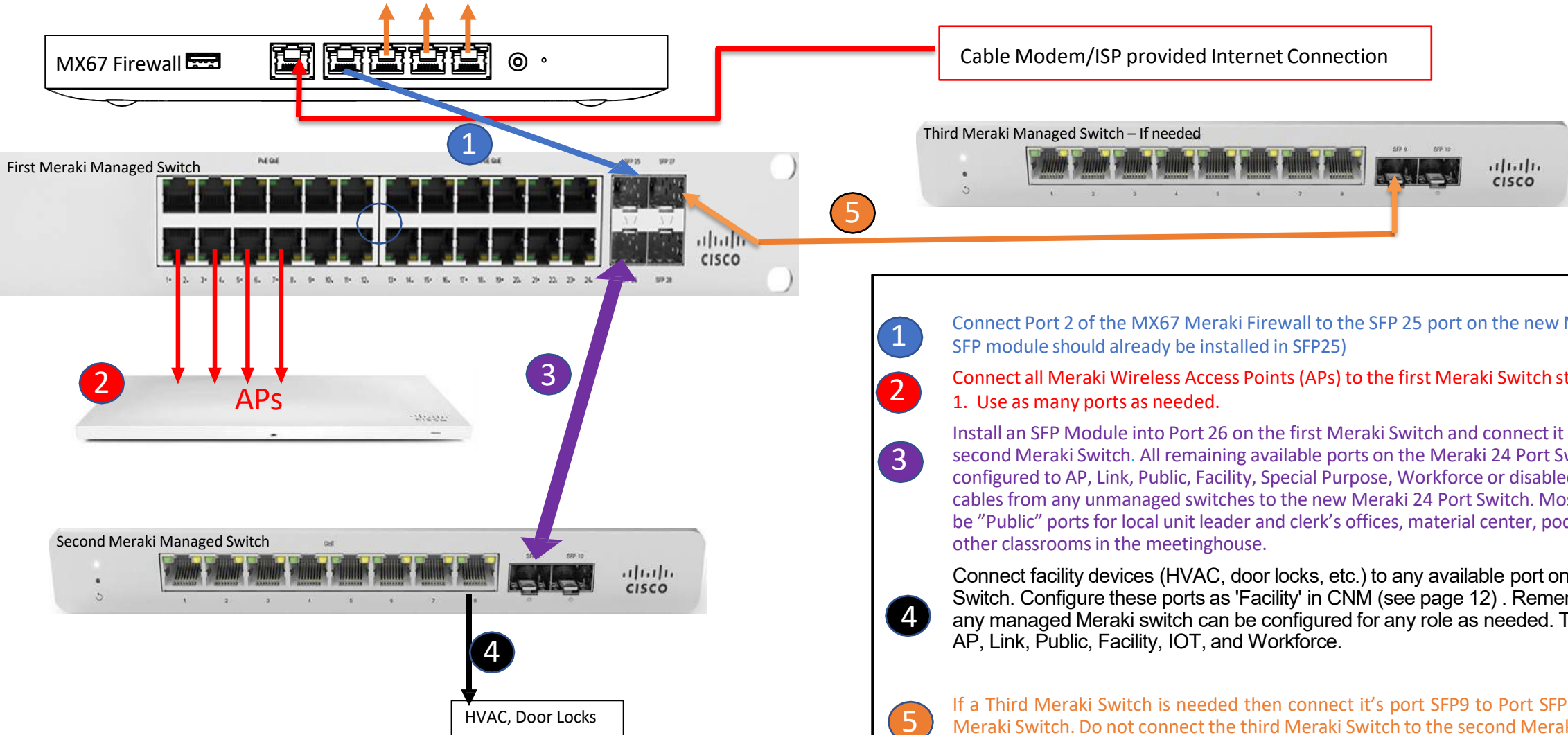
NOTE: All remaining ports on the First and Second Meraki switches can be configured as needed to be AP, Link, Public, Facility, IOT, Workforce or disabled if not used.

*This diagram applies to any dual switch meetinghouse setup, including when the switches are in different rooms

Figure 3 - Three Meraki Switches Configuration

Firewall Port 3 - may be used during Switch installation to access Church Network Manager(CNM)

Firewall Ports 4 and 5 - will be disabled. (nothing should be connected to Firewall Ports 4, and 5 after the switch installation is completed)



- 1 Connect Port 2 of the MX67 Meraki Firewall to the SFP 25 port on the new Meraki Switch (the SFP module should already be installed in SFP25)
- 2 Connect all Meraki Wireless Access Points (APs) to the first Meraki Switch starting with Port 1. Use as many ports as needed.
- 3 Install an SFP Module into Port 26 on the first Meraki Switch and connect it to Port 9 on the second Meraki Switch. All remaining available ports on the Meraki 24 Port Switch can be configured to AP, Link, Public, Facility, Special Purpose, Workforce or disabled. Move all cables from any unmanaged switches to the new Meraki 24 Port Switch. Most of these will be "Public" ports for local unit leader and clerk's offices, material center, podium, and all other classrooms in the meetinghouse.
- 4 Connect facility devices (HVAC, door locks, etc.) to any available port on any Meraki Switch. Configure these ports as 'Facility' in CNM (see page 12) . Remember: any port on any managed Meraki switch can be configured for any role as needed. The roles include AP, Link, Public, Facility, IOT, and Workforce.
- 5 If a Third Meraki Switch is needed then connect it's port SFP9 to Port SFP 27 on the first Meraki Switch. Do not connect the third Meraki Switch to the second Meraki Switch.

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

Replacing the current Meraki Firewall with a Meraki MX67 firewall in CNM

****This procedure should only be performed if a meetinghouse is NOT currently operating with an MX67 firewall. If there is already an MX67 firewall present, or if the site has been previously upgraded to an MX75, MX85, or MX95 firewall, skip forward to the switch activation procedure**

1. Remove the new Meraki MX67 Firewall from the box and locate its Serial Number(SN) (Cloud ID). Then, log into Church Network Manager (CNM)
 1. To access CNM enter <http://cnm.churchofjesuschrist.org> into the browser's address bar
 2. Login to CNM using your Church Account Username and Password
2. Locate the Meetinghouse’s page in CNM using the Search function and replace the current firewall with the new MX67 firewall:
 1. Choose from the search dropdown which information item you want to use to find the meetinghouse you are working on (see screenshot 1 to the right)
 2. Once you have entered the search data, press the Search button
 3. From the results list, select the meetinghouse you are working on (if you search by firewall/device serial number, skip to step 7)
 4. In the Properties screen that appears, select the appropriate property
 5. In the next screen, which shows the property you selected, look in the Networks box and select the network which contains the serial number of the currently installed firewall (See Screenshot 2 to the right)
 6. Use CNM to replace the current firewall with the new MX67 firewall
 7. On the Network Details screen, press the Menu button at the top right of the screen and select the “Replace (RMA)” item (see screenshot 3 to the right)
 8. This will bring up a box asking for the serial number of the firewall you want to replace the current firewall with. Insert the serial number of the new MX67 firewall here and press the Save Changes button:

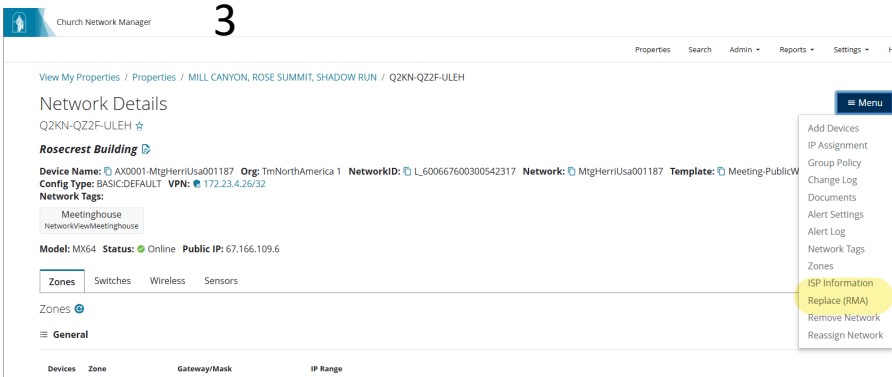
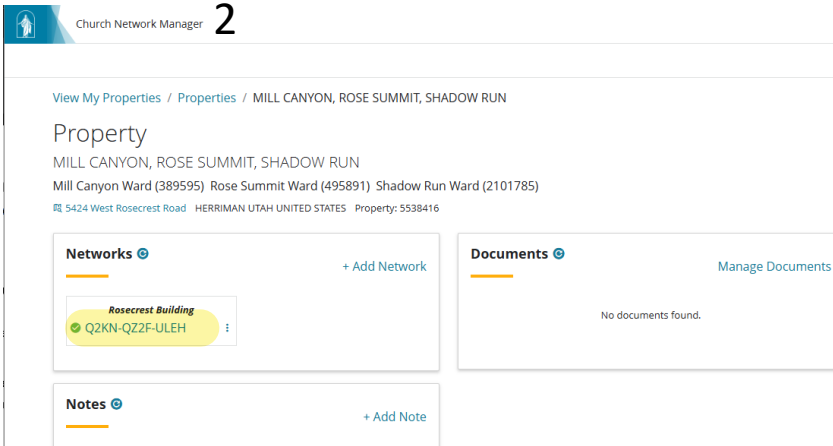
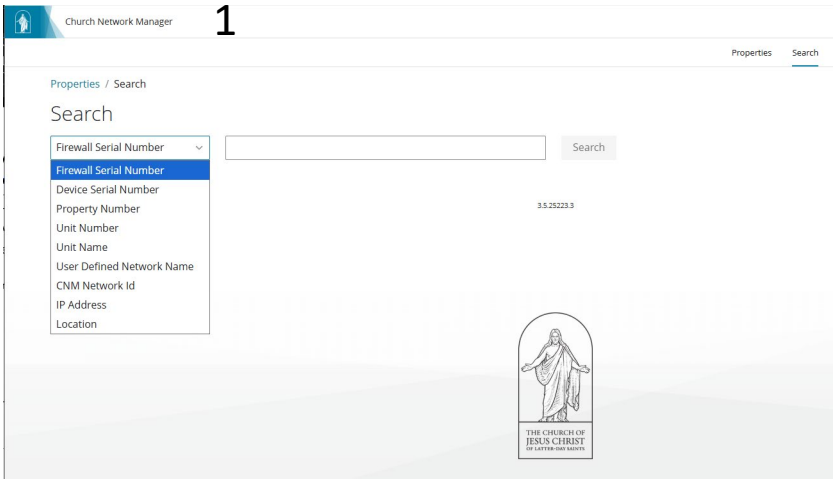
Replace (RMA)

Enter the firewall serial number you are replacing Q2KN-QZ2F-ULEH with.

New Serial Number:

Close Save changes

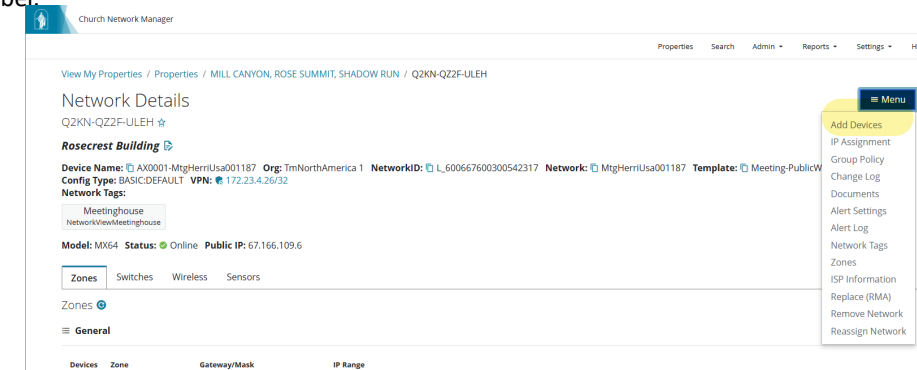
9. Wait for the process to complete. Once completed, remove the ISP connection and the connection to the first switch from the old firewall. Connect the ISP connection to the new MX67 firewall’s Internet port per the applicable diagram shown previously. Power up the new firewall. Wait for the firewall status light to turn solid white (See steps 1-2 in the “Steps after installing the Meraki Firewall and/or Meraki Switch” on page 12 of these instructions)



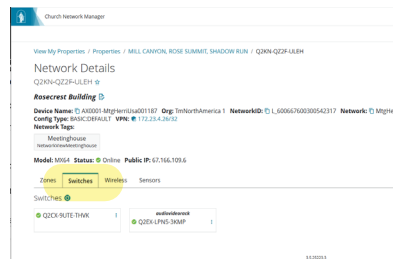
Adding the new Meraki Managed Switch(es) in CNM

1. Remove the new Meraki Switch from the box and find the Serial Number (or Cloud ID)
2. Add the new switch(es) to the meetinghouse's network in CNM:
 1. Locate the meetinghouse name where you are installing the new Meraki Switch. Step 2 substeps 1-4 on the previous page can be used to do this
 2. Click on the "MENU" in the upper righthand corner and then click on "Add Devices" from the drop-down menu (see screenshot to the right)
 3. Enter the new switch's Serial Number into the Serial Number field, click into the Label field provide an appropriate switch label:

Switch Serial Numbers (SN) are located on the switch back panel



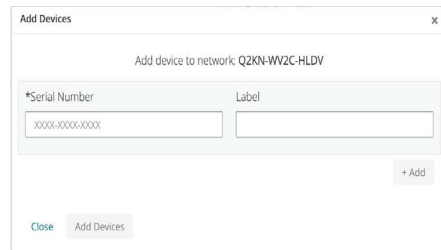
4. Click the "Add Devices" button
5. Wait for the process to complete and for the new switch to appear in the Switches list for the property:



6. Using a network cable, connect the new switch to the firewall or to another switch per the applicable diagram shown earlier in these instructions
7. Wait for the switch's status light to turn solid white (See steps 3-5 in the "Steps after installing the Meraki Firewall and/or Meraki Switch" on page 12 of these instructions)
8. Repeat these steps for any additional switches that need to be installed in the meetinghouse

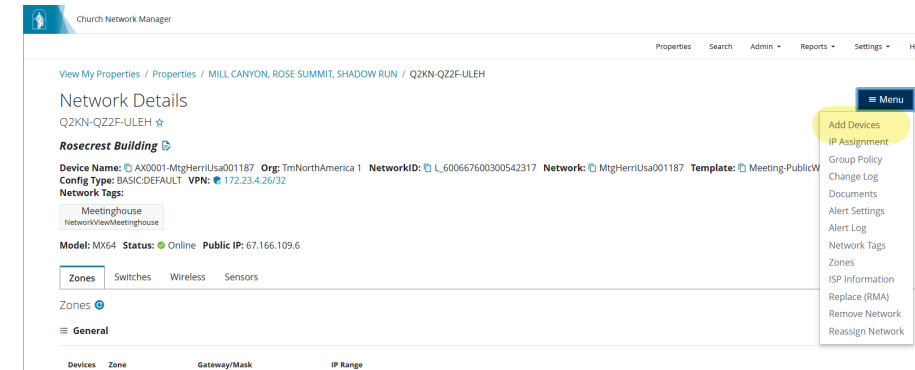
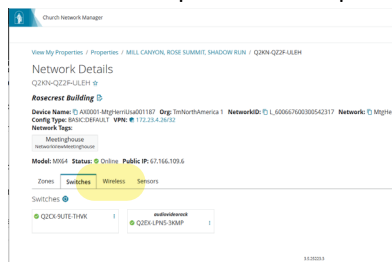
Adding the new Meraki Access Points (AP) in CNM

1. Remove the new Meraki AP (Model CW9172I) from the box and find the Serial Number (aka Cloud ID)
2. Add the new AP to the meetinghouse's network in CNM:
 1. Locate the meetinghouse name where you are installing the new Meraki Switch. Step 2 substeps 1-4 on the previous page can be used to do this
 2. Click on the "MENU" in the upper righthand corner and then click on "Add Devices" from the drop-down menu (see screenshot to the right)
 3. Enter the new AP's Serial Number into the Serial Number field, click into the Label field provide an appropriate switch label:



If needed, press the "+Add" button to expose additional lines so you can add additional APs all at once

4. Click the "Add Devices" button
5. Wait for the process to complete and for the new AP to appear in the Wireless list for the property:



6. Using a network cable, connect the new AP to a Meraki switch per the applicable diagram shown earlier in these instructions
7. Wait for the AP's status light to turn solid green or blue (See page 14)
8. Repeat these steps for any additional APs that need to be installed in the meetinghouse

Steps after installing the Meraki Firewall and/or Meraki Switch

Note: we have learned that in some cases, the firewall/switch indicator light will return to a solid orange state for several minutes. The firewall/switch should eventually return to a solid white light.

1. Verify that the Meraki Firewall has a white light
 1. Orange = Firewall is booting up or may not find access to the internet if light stays orange
 2. Rainbow cycle = Firewall is communicating with the Meraki cloud
 3. Blinking White = Firewall is functional but is updating firmware from the Meraki cloud
 4. Solid White = Firewall is online and ready to proceed
2. If the Firewall light is not Blinking or Solid White then review the [Meetinghouse Network Troubleshooting guide](#)
3. Verify that the Meraki Switch has a flashing or solid white light
 1. Orange = switch is booting up or may not find access to the internet if light stays orange
 2. Rainbow cycle = communicating with the Meraki cloud
 3. Blinking white = switch is functional and updating firmware from the Meraki cloud
 1. The switch will reboot once the firmware is installed(light will go back to orange)
 4. Solid White = Complete and ready
4. If the Switch Light is not Blinking or Solid White then then review the [Meetinghouse Network Troubleshooting guide](#)
5. Once the light on the new Meraki Switch is solid white then configure each port in CNM (see the next page)

Church Network Manager

View My Properties / Properties / MILL CANYON, ROSE SUMMIT, Network Details

Q2KN-Q2ZF-ULEH ☆

Rosecrest Building ☆

Meetinghouse
NetworkViewMeetinghouse

Device Name: Q AX0001-MtgherrnUsa001187 Org: TrnNorthAm
Config Type: BASIC.DEFAULT VPN: 172.23.4.36/32

Network Tags:

Meetinghouse
NetworkViewMeetinghouse

Model: MX64 Status: Online Public IP: 67.166.109.6

Zones

Switches

Wireless

Sensors

Switches

Q2CX-9UTE-THVK

andfieldnetwork

Tools

Q2CX0001-MtgherrnUsa001187
Q2CX-9UTE-THVK
M5120-B9P
192.168.12.5
961188802.usg94

Label

Barcode

Ports










































Documents

Link

Reboot

Replace

Remove

Manage Switch Ports 									
Q2CX-9UTE-THVK Edit									
<input type="checkbox"/>	Port	Assignment	Label	LLDP	Enabled	PoE 	Connected		
<input type="checkbox"/>	1	AP	Label	Meraki MR33 Cloud Managed AP				⋮	
<input type="checkbox"/>	2	AP	Label	No LLDP data				⋮	
<input type="checkbox"/>	3	AP	Label	Meraki MR33 Cloud Managed AP				⋮	
<input type="checkbox"/>	4	Public	Label					⋮	
<input type="checkbox"/>	5	AP	Label	Meraki MR33 Cloud Managed AP				⋮	
<input type="checkbox"/>	6	AP	Label	No LLDP data				⋮	
<input type="checkbox"/>	7	Disabled	Label					⋮	
<input type="checkbox"/>	8	Facility	Label	No LLDP data				⋮	
<input type="checkbox"/>	9	IoT	Label	No LLDP data				⋮	
<input type="checkbox"/>	10	Link	Label					⋮	
		Public	Label	Meraki MX64 Cloud Managed Router				⋮	
		Workforce	Label					⋮	
		SFP	Label	Meraki M5120-24P Cloud Managed PoE Switch				⋮	

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

Once all switch ports are configured appropriately, make sure that the switch's status light is solid white. Then, connect all wired network connections to the switch, including all connections to the access points

Now that the firewall and switch are activated in CNM and each Switch port is properly configured in CNM:

Note: we have learned that in some cases, the switch indicator light will return to a solid orange state for several minutes. The switch should eventually return to a solid white light.

1. Verify that the Meraki Wireless Access Points (AP) lights are Green or Blue:
 1. Orange - AP is booting (permanent Orange suggests hardware issue)
 2. Rainbow - AP is initializing/scanning
 3. Blinking Blue - AP is upgrading
 4. Green - AP is ready with nothing connected
 5. Blue - AP is ready with clients connected
 6. Blinking Orange - AP can't find uplink to switch
2. If the AP lights are not Green or Blue, then then review the [Meetinghouse Network Troubleshooting guide](#).
3. Both the wireless Liahona network and wired clerk computers should be able to access ComeUntoChrist.org (Liahona wireless clients need to accept the Terms of Service splash page in order to gain internet access).
4. If the Network is not working, then review the [Meetinghouse Network Troubleshooting guide](#)

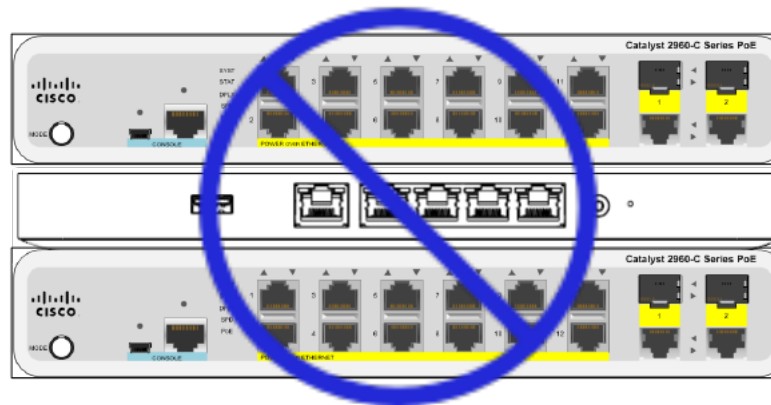
When is a second or third Meraki Switch needed?

A second or third Meraki Switch will be needed if:

- Installing a 24 Port switch and the meetinghouse has more than 22 switch ports in use, including the Wireless Access Points(APs). (All wired network devices must be connected to a Meraki switch)
- If a third Meraki Switch is needed then it should ideally be connected to port SFP 27 on the first Meraki Switch. If SFPs are not available, the third switch can be connected to any available port of the First Meraki Switch (port must be configured as a “Link” port). **Do not connect the third Meraki Switch to the second Meraki Switch (no daisy chaining of switches).**
- If the meetinghouse has multiple network closets then each closet will need a Meraki Switch but the second and third Meraki Switches must be connected to the First Meraki Switch which is connected to the Meraki Firewall.

• Heat Concern- Do Not Stack

- Do not stack electronic devices on top of or under the MX 67 Firewall
- Do not stack an 8 Port Meraki Switches on or under another electronic device if possible
- The 8 port switch and MX 67 Firewall need open space around them to stay cool
- Stacking directly on other devices creates a lack of heat dissipation which can lead to failures
- The 24 Port switch has a fan inside to keep it cool. You can stack switches on top of it.



Post-Installation Cleanup Tasks

- Once the installation is complete, any old Meraki switches (MS120 models) should be removed from the network and from CNM. This can be done by pressing the 3 dots next to the old switch in CNM and selecting the red “Remove” button (see screenshot to the right).
- Go to the Wireless tab in the Network Details screen. Remove any old Meraki APs (MR32, MR33 and MR36 models) from CNM using the red “Remove” button in the 3 dots menu of any APs that are being removed.
- Take photos of the finished racks and equipment and upload them to the Documents section of the Property screen in CNM by pressing “Manage Documents”:

