

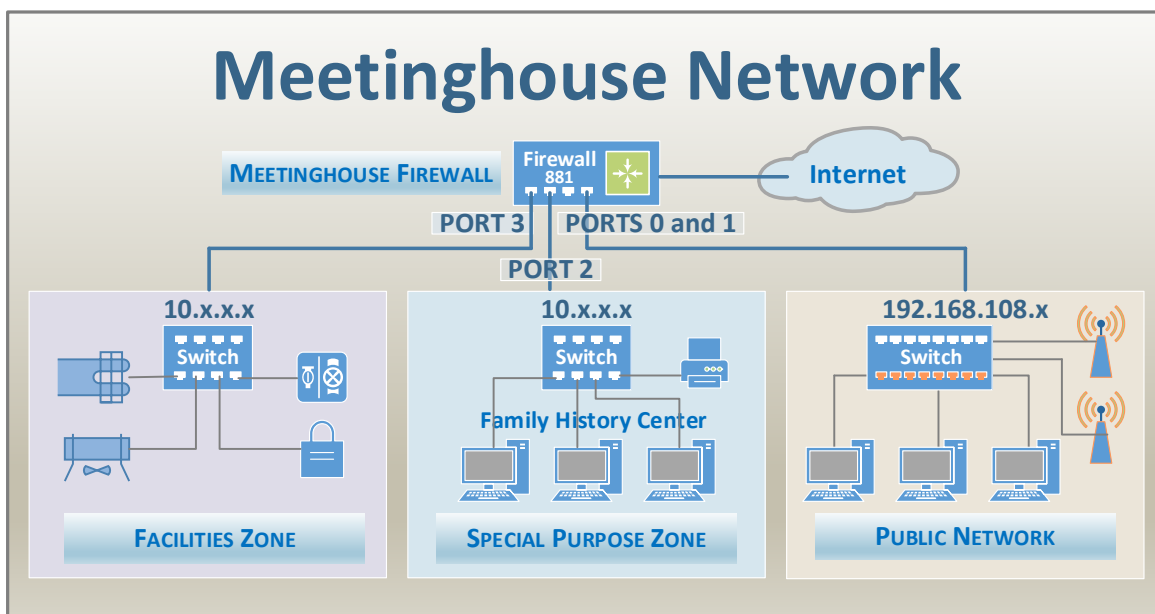
Upgrading an Existing Meetinghouse Firewall

Meetinghouse Firewalls must be updated to the latest configuration to improve network performance and allow more network connections. This document describes steps for upgrading the firewall.

DEDICATED MEETINGHOUSE FIREWALL PORTS

The firewall upgrade creates separate network zones connected to dedicated firewall ports.

Dedicated Firewall Port Assignments	
Firewall Port(s)	Connection Description
FE LAN Ports 0 and 1	Public Network
FE LAN Port 2	Family History Center
FE LAN Port 3	Facilities Zone



PUBLIC NETWORK

The upgrade creates a Public Network zone, and changes the existing network IP address space from 10.x.x.x to 192.168.x.x.

FACILITIES ZONE

The upgrade creates a Facilities Zone for meetinghouse systems (e.g., webstat, card access, heating/cooling/sprinkler/alarm systems) on firewall Port 3. After the upgrade only meetinghouse systems should be connected to this port.

WHAT TO DO BEFORE UPGRADING THE FIREWALL

1. **CONNECT NETWORK DEVICES TO CORRECT FIREWALL PORTS.** Connect Public Network devices (PCs, wireless access points, etc.) to firewall Ports 0 and 1, connect Family History Center devices to firewall Port 2, and connect meetinghouse facility systems to firewall Port 3.
2. **STATIC IP ADDRESS DEVICES.** Identify any devices (clerk PC, network printers, etc.) that use static IP addresses—which are network addresses that do not change. These devices must be assigned a new static IP address after the firewall upgrade.

3. **FAMILY HISTORY CENTER.** If an “official” Family History Center exists then you must contact the Global Service Center (GSC) at +1 855-537-4357 for additional information.
 - a. Talk with the Family History Center director before performing the firewall upgrade.
 - b. Connect all Family History Center devices to firewall Port 2.
 - c. The GSC will create a “Special Purpose Zone” on the firewall for the Family History Center.
 - i. Afterwards the GSC should tell you the IP Address range of the new zone (be sure to record this information).
 - ii. Family History Center devices that are assigned a static IP address (e.g., some printers) must be assigned a new address from the Special Purpose Zone static IP address range.

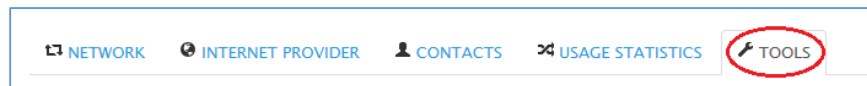
NOTE: An “official” Family History Center has a *Church Directory of Leaders* unit number (<https://cdol.lds.org>) that is different from the stake/ward unit number.

PERFORMING THE MEETINGHOUSE FIREWALL UPGRADE

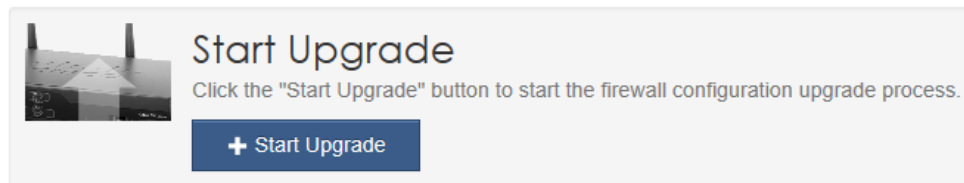
The firewall upgrade is performed by Facilities Managers and Stake Technology Specialists using the Technology Manager tool.

FIREWALL UPGRADE STEPS:

1. Sign-in to the Technology Manager tool (<https://tm.lds.org/>).
2. Locate existing Meetinghouse Firewall (Firewalls > locate Church unit in Firewall Management window > then select firewall to upgrade by clicking its serial number).
3. Select the Tools menu (to the right of the Usage Statistics menu).



4. Select the “Start Upgrade” button, read the message, then press “confirm.”



5. Technology Manager will install the new firewall configuration, and then restart the firewall. After about eight minutes the firewall upgrade will be complete.

WHAT TO DO AFTER THE FIREWALL UPGRADE

1. **TEST NETWORK CONNECTION.** Connect a PC to the meetinghouse network and connect to <http://www.lds.org>. If the Internet page can be accessed then the upgrade was successful.
2. **ASSIGN STATIC IP ADDRESSES.** Assign a static IP address to devices that need one.

IP Address Range after Firewall Upgrade

ZONE	IP Addresses
Public Network	Dynamic IP Address: (DHCP, Auto Assigned) IP Range: 192.168.108.33 to 192.168.111.254 Static IP Address: IP Range: 192.168.108.2 to 192.168.108.32 Gateway: 192.168.108.1 Mask: 255.255.252.0 DNS: 8.34.34.92 and 8.35.35.92
Facilities Zone	Static IP Address: IP Range: 10.x.x.x

Static Addresses in a Special Purpose Zone. If the Global Service Center (GSC) creates a Special Purpose Zone for a Family History Center (FHC) in the meetinghouse, then any FHC device that uses a static IP address must be assigned a new network address.

After it is created the GSC may tell you the static IP address range of the Special Purpose Zone; otherwise this information can be found in Technology Manager (Firewalls > locate Church unit in Firewall Management window > select firewall to upgrade and select its serial number> select the “Network” tab page > then locate the Special Purpose Zone [“VPN”] section).

Special Purpose Zone IP Address Range

ZONE	IP Addresses
Special Purpose Zone	Dynamic IP Address: (DHCP, Auto Assigned) IP Range: 10.x.x.17 to 10.x.x.254 Static IP Address: IP Range: 10.x.x.2 to 10.x.x.16

The Director of the FHC should keep a record of the Special Purpose Zone static IP address range, and a list of FHC devices assigned a static IP address.

3. **Facilities Zone Devices.** If a facilities device does not function the same way it did before the upgrade, then try connecting the device to the Public Network instead of being connected to the Facilities Zone firewall port.
4. **NOTIFY FACILITIES MANAGER.** When the firewall upgrade is completed please notify the meetinghouse Facilities Manager. In the message please include the property address and the firewall serial number.

If you experience any problems performing the Meetinghouse Firewall upgrade, please contact the Global Service Center (GSC) at +1 855-537-4357 or dial the [toll-free number for your area](#).