Upgrading an Existing Meetinghouse Firewall

Beginning the summer of 2014 (U.S.) a new Meetinghouse Firewall configuration was introduced. This new configuration increases the firewall data throughput to better utilize the speed of the Internet Service Provider (ISP). The configuration also creates two network zones: the Public Network (with 990 dynamic and 31 static network addresses) and the Facilities Zone (with 13 static network address for meetinghouse systems).

DEDICATED MEETINGHOUSE FIREWALL PORTS

The new Meetinghouse Firewall configuration requires dedicated firewall ports for network connectivity. After the upgrade you must ensure that network cables are connected to the correct firewall ports (see table below).

Dedicated Firewall Port Assignments	
Firewall Port(s)	**Connection Description**
FE LAN Ports 0 and 1	Public Network
FE LAN Port 2	Reserved
FE LAN Port 3	Facilities Zone
FE WAN Port 4	Internet Service Provider

NOTE: The “Reserved” firewall port is saved for special purposes. For example if an official Family History Center exists in the meetinghouse, the Global Service Center may create a Special Purpose Zone on the firewall and assign the Family History Center to the “Reserved” port. If a Special Purpose Zone is not created on the firewall, then the “Reserved” port may be used for connecting Public Network devices.

FACILITIES ZONE

The firewall upgrade automatically creates a Facilities Zone that is assigned to a dedicated firewall port. Even if a facilities device does not currently exist in the meetinghouse, a Facilities Zone port will be assigned for meetinghouse facilities systems (e.g., heating/cooling system, sprinkler system, alarm system). The Facilities Zone includes only static IP addresses.

When the firewall upgrade is complete any non-facilities devices connected to the dedicated Facilities Zone port will no longer work. This includes existing PCs, wireless access points, or other devices connected to the dedicated facilities port. The facilities port is not designed for USER traffic, so you will need to move any USER-based devices to firewall ports assigned to the Public Network.

NOTE: If a Facilities Zone existed on the firewall before the configuration upgrade, after the firewall upgrade the existing IP network addresses will remain the same. This means that the static IP addresses of existing facilities devices will not need to be changed after the firewall upgrade.

PUBLIC NETWORK

To create the Public Network the firewall upgrade changes the existing meetinghouse IP address range from 10.x.x.x addresses to 192.168.x.x addresses. After the upgrade any statically assigned USER devices

(clerk PCs, printers, etc.) will need to be changed to the new static IP address range of the Public Network to resume network connectivity (see table below).

IP Address Range after Firewall Upgrade

ZONE	IP Addresses
Public Network	**Dynamic IP Address:** (DHCP, Auto Assigned) IP Range: 192.168.108.32 to 192.168.111.254 **Static IP Address:** IP Range: 192.168.108.2 to 192.168.108.31 Gateway: 192.168.108.1 DNS: 8.34.34.92 and 8.35.35.92
Facilities Zone	**Static IP Address:** IP Range: 10.x.x.x

ISSUES TO ADDRESS BEFORE THE MEETINGHOUSE FIREWALL UPGRADE

1. **Family History Center.** If the meetinghouse contains an official Family History Center, then DO NOT PROCEED with firewall upgrade. Please contact the Global Service Center (GSC) at +1 855-537-4357 for additional information.
   a. If needed the GSC will perform the firewall upgrade and create a Special Purpose Zone for the Family History Center.
   b. If a Special Purpose Zone is created for a Family History Center, then only Family History Center devices should be connected to the "Reserved" firewall port (see "Dedicated Meetinghouse Firewall Ports" section above). After the firewall upgrade, if a static IP addressed device exists in the Family History Center, that device will need to be assigned to a different IP network address in the Special Purpose Zone.
   c. You should consult with the director of local Family History Center before performing the firewall upgrade. The director should help you identify any devices that have an assigned static IP address.
2. **Identify Static IP address devices.** Identify any static IP addressed devices in the meetinghouse. This may include clerk PCs, network printers, or other devices. This may also include devices in a Family History Center if it exists. After the firewall upgrade, those devices will need to be assigned a new address in the new IP address space.
3. **Connect network devices to correct firewall ports.** Ensure that network devices (PCs, wireless access points, etc.) are connected to the correct firewall ports. Refer to information in the "Dedicated Meetinghouse Firewall Ports" and "Facilities Zone" sections above.

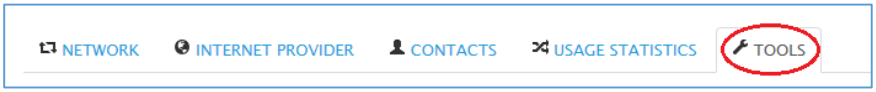
PERFORMING THE MEETINGHOUSE FIREWALL UPGRADE

The Meetinghouse Firewall upgrade is performed by the Technology Manager (TM) tool. Initially only the Global Service Center may upgrade existing Meetinghouse Firewalls, but later Facilities Managers and Stake Technology Specialists will be granted permissions in the TM Tool to perform the upgrade.

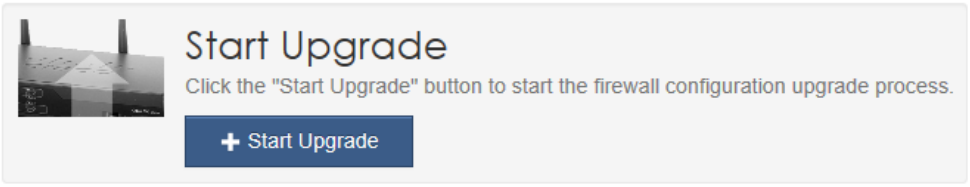
When doing the firewall upgrade the TM Tool creates and installs a new firewall configuration, and then restarts the firewall. Soon afterwards the firewall upgrade will complete, and connected devices will be able to access the network.

FIREWALL UPGRADE STEPS:

1. Launch and sign-in to the Technology Manager tool (https://tm.lds.org/).
2. Locate existing Meetinghouse Firewall (Firewalls > Locate Church unit in Firewall Management window > 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 from the Upgrade Firewall Configuration section, and confirm that you wish to proceed.



5. At this point the TM Tool creates and installs a new firewall configuration, and then automatically restarts the firewall. After two to eight minutes the firewall upgrade will be complete, and connected devices can access the network.

STEPS TO TAKE AFTER THE MEETINGHOUSE FIREWALL UPGRADE

1. **TEST NETWORK CONNECTION.** Connect a PC to the meetinghouse network, open a web browser, and connect to an Internet site like http://www.lds.org/ or http://www.mormon.org/. If you are able to link to these pages then the firewall upgrade was successful. Test both wired and wireless connectivity (if the meetinghouse has installed wireless access points) in the meetinghouse.

2. **ASSIGN STATIC IP ADDRESSED DEVICES.** Assign identified static IP addressed devices to the correct static IP address range. See the "IP Address Range after Firewall Upgrade" table in the "Public Network" section above. This may include clerk PCs, network printers, or other devices.

   Static Addresses in a Special Purpose Zone. If the Global Service Center created a Special Purpose Zone for a Family History Center (FHC), any FHC devices having static IP address will need to be assigned a new static IP address in the new Special Purpose Zone IP address space (the address space is unique for each firewall). After the firewall upgrade the Special Purpose Zone IP address range can be identified using the TM Tool (Firewalls > Locate Church unit in Firewall Management window > Select firewall to upgrade by clicking its serial number > Select the "Network" tab page and down to locate the "Special Purpose Zone" 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

   Devices with static IP addresses should be assigned to the static IP range. A record of assigned static IP addresses should be kept by the organization (e.g., Family History Director).

3. **NOTIFY FACILITIES MANAGER.** Notify the Facilities Manager that the Meetinghouse Firewall was upgraded. In the communication be sure to include the property address and the firewall serial number. This information is found in the TM Tool (Firewalls > Locate Church unit in Firewall Management window > Locate property and 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.

THE CHURCH OF
JESUS CHRIST
OF LATTER-DAY SAINTS