Power is knowledge.™

LifeSafety Power®

MSM200
Multi-Site Manager Installation Manual

FLEXPOWER®

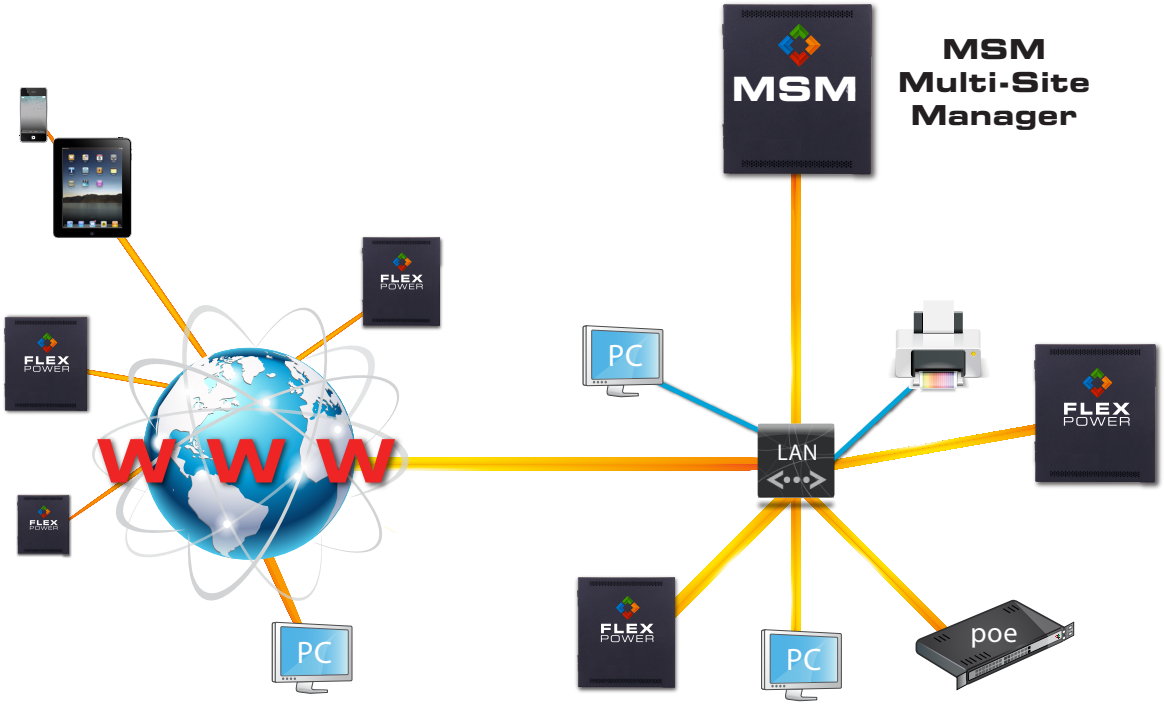
LifeSafety Power, Inc. | PH 888.577.2898 | TechSupport@LifeSafetyPower.com

P03-047 Rev A04

Table of Contents

Section 1 – Introduction

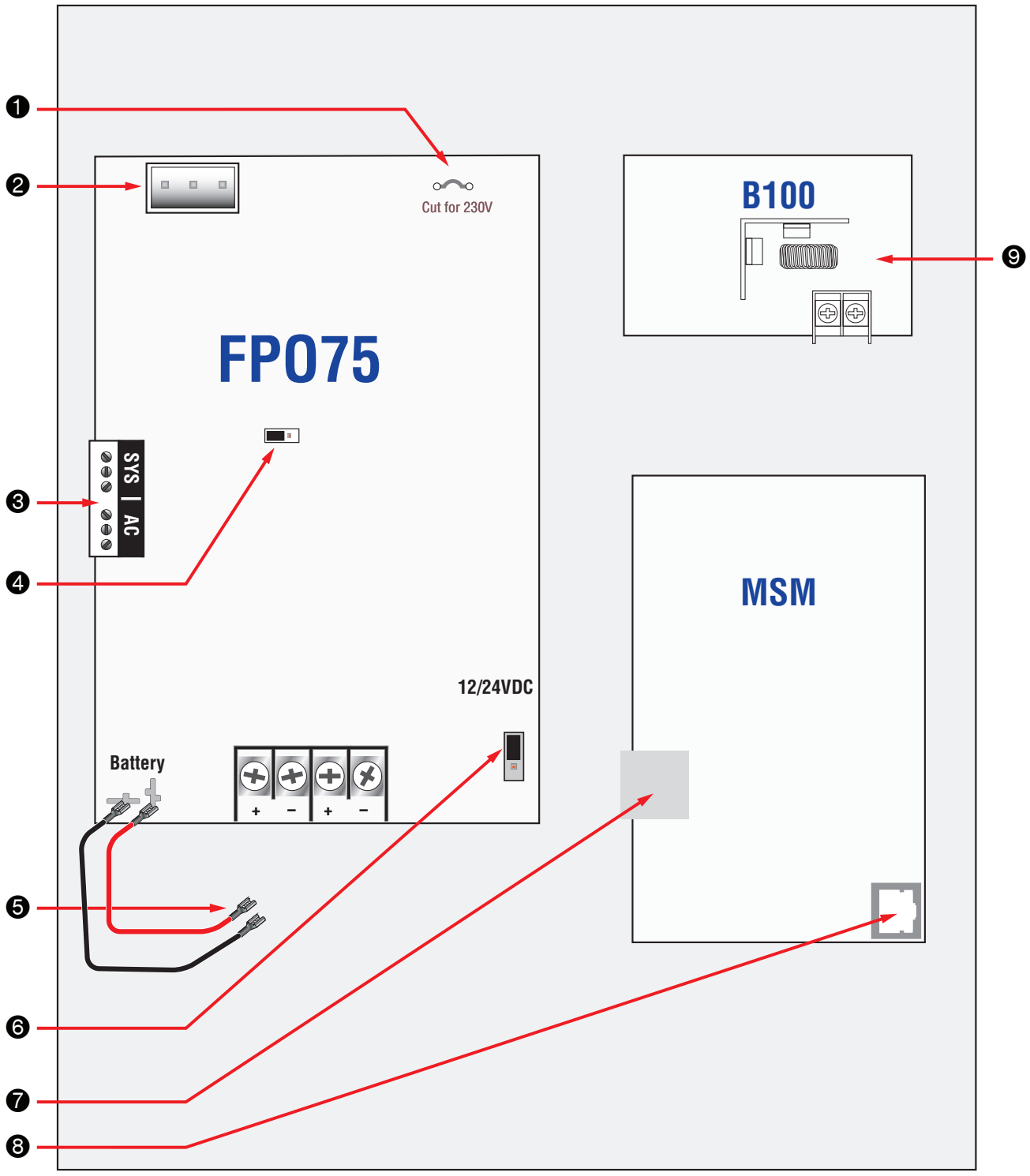
LifeSafety Power's Multi-Site Manager (MSM) is a VPN server which allows management of multiple LifeSafety Power network power management systems. Through the MSM's web browser interface, a user can monitor and access any LSP network device connected to the Virtual Private Network from within a local network or via the internet from anywhere in the world.



Section 2 – Connecting the Hardware

2.1 MSM Hardware Description

The internal FPO75 board charges the 12V backup battery and supplies power to the internal B100 board. The FPO75 should be left as configured by the factory (12V output, EG Fault Disabled) and should not be used to power any other external devices. The B100 should also be left as configured by the factory (5V output) and should not be used to power any other external devices.



Section 2 – Connecting the Hardware

❶ *AC Input Voltage Selection (JP1)*

This jumper configures the MSM for the AC input voltage to be used.

- Leave jumper INTACT for 120V input
- CUT and remove jumper for 230V input

⚠ Failure to cut this jumper when using the MSM with a 230VAC input will result in damage to the system and void the warranty.

❷ *AC Input (J9)*

J9 accepts the provided three-wire connector harness for connection to the AC Line. Cut jumper JP1 if powering the FPO with a 230VAC input. Connections are by wire nut as follows:

120VAC	**230VAC**
Green – Earth Ground	Green – Earth Ground
Black – Hot	Black – Phase 1
White – Neutral	White – Phase 2

⚠ Always connect earth ground first and disconnect last

❸ *Fault Output Connections (TB3)*

These terminals provide the System Fault and AC Fault contact outputs. The terminals are removable and are labeled on the PC board in the non-powered (fault) state.

Fault conditions reported include:

AC FLT

- Low AC
- Missing AC
- Internal Fault

SYS FLT

- Missing Battery (If BAT DET jumper is ON)
- Earth Ground Fault (If EARTH GND DET jumper is ON)
- Battery voltage out of range
- DC output voltage out of range
- Ruptured fuse
- Accessory Board Fault
- Internal Fault

❹ *Battery Presence Detection (JP3)*

The BAT DET jumper enables or disables Battery Presence (BP) fault detection as follows:

- ***Position 1 (jumper ON)*** Enable BP Fault Detection
- ***Position 2 (jumper OFF)*** Disable BP Fault Detection

Note: Postion 1 (enabled) is the factory default position
Battery Presence fault detection indicates a fault when the backup battery is disconnected from the FPO power supply. If no backup battery is being used, this jumper should be removed.

❺ *Battery Connection (BAT+ & BAT–)*

Faston connectors for connection of the backup battery set. Pre-terminated battery leads are provided. A 12V lead-acid or gel-cell backup battery between 7 and 40AH should be used with the MSM to provide backup in the event of a power outage. If a battery is not used with the MSM, disable Battery Presence detection.

⚠ Observe polarity or damage to the system will occur.

❻ *Output Voltage Selection (SW1)*

This jumper selects the output voltage of the FPO power supply. The FPO power supply is factory set for 12VDC in the MSM and should remain at the 12V setting. Voltage settings are labeled on the PC board.

⚠ If the output voltage must be changed, remove power first or damage to the power supply could occur.

❼ *SD Memory Card*

This memory card holds the software for the MSM and should remain installed in the MSM board at all times.

❽ *Network Connection*

This connector accepts the CAT5 cable which connects to the local network. A standard CAT5 or better cable may be used.

❾ *B100 Board*

The B100 board converts the 12V output of the FPO to 5VDC to power the MSM board. It is pre-set from the factory and must remain in the adjustable output range setting, set for a 5VDC output. The B100 should not be used to power any other external devices.

Section 2 – Connecting the Hardware

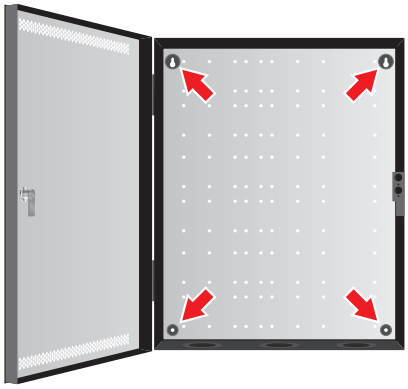
2.2 Mounting the Enclosure

Mounting an Enclosure

Use the following procedure to mount the MSM enclosure.

1. (Optional) Remove the enclosure's cover.
2. Locate the top keyhole mounting holes in the back of the enclosure.
3. Mark and pre-drill the locations for the keyholes in the mounting surface.
4. Partially install two fasteners appropriate for the surface on which the enclosure is being installed. Leave the heads of the fasteners approximately ¼" out from the surface. Recommended fastener size is #10.
5. Hang the enclosure on the two fasteners and mark the locations of the remaining mounting holes.
6. Remove the enclosure and pre-drill the locations for the remaining mounting holes.
7. Re-hang the enclosure on the top mounting fasteners, start the remaining fasteners and tighten all fasteners.
8. Reinstall the enclosure's cover, if removed in step 1.

⚠ It is the installer's responsibility to determine the appropriate fastening system for use with the surface the enclosure is being mounted to.

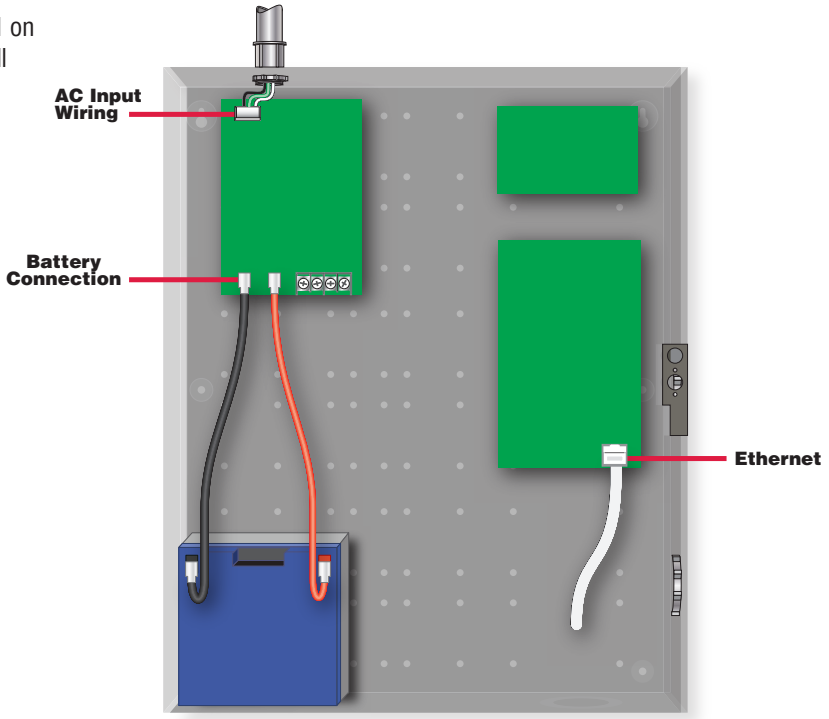


2.3 Wiring the MSM

1. Ensure the MSM is securely mounted as shown in Section 2.2
2. Connect the AC wires of the MSM's internal FPO power supply to a suitable AC source. Ensure the connector at the other end of the AC harness is plugged securely into the connector on the power supply board.

   ⚠ If powering the MSM from a 230VAC source, jumper JP1 on the FPO board MUST be cut or damage to the system will occur. See section 2.1
3. Connect the Ethernet port on the MSM to the local area network (LAN) using a standard CAT5 cable.
4. If using battery backup in the MSM, connect a 12V sealed lead acid battery to the red and black battery leads.

   ⚠ Observe polarity or damage to the system will occur.



Section 3 – Setting Up the MSM

The MSM creates a Virtual Private Network (VPN) within the local network. It allows local and remote connections between LifeSafety Power network devices and PC's, smartphones and tablets. In order to set up the MSM to work properly, the device used to access the MSM must be connected to the VPN server within the MSM. Once connected, the MSM's interface can be accessed via any web browser. For remote access to the MSM, port 1723 must be accessible. This section provides instructions for setting up the MSM.

3.1 Determine the Local IP address of the MSM

The local IP address of the MSM is assigned by the local DHCP server on initial installation. Once assigned, it is necessary to know the local IP address that is assigned in order to setup the VPN client for MSM access. There are two methods which can be used to determine the local IP address of the VPN.

3.1.1 Method 1 - via Network Scan software

This method MUST be used for the initial setup of an MSM. The local IP address can be obtained by using network scanning software, such as LifeSafety Power's scan tool or SoftPerfect's free "NetScan" software. In the scanning software's options, enable the SNMP HostName. Figure 2 shows a screenshot from SoftPerfect's network scanner.

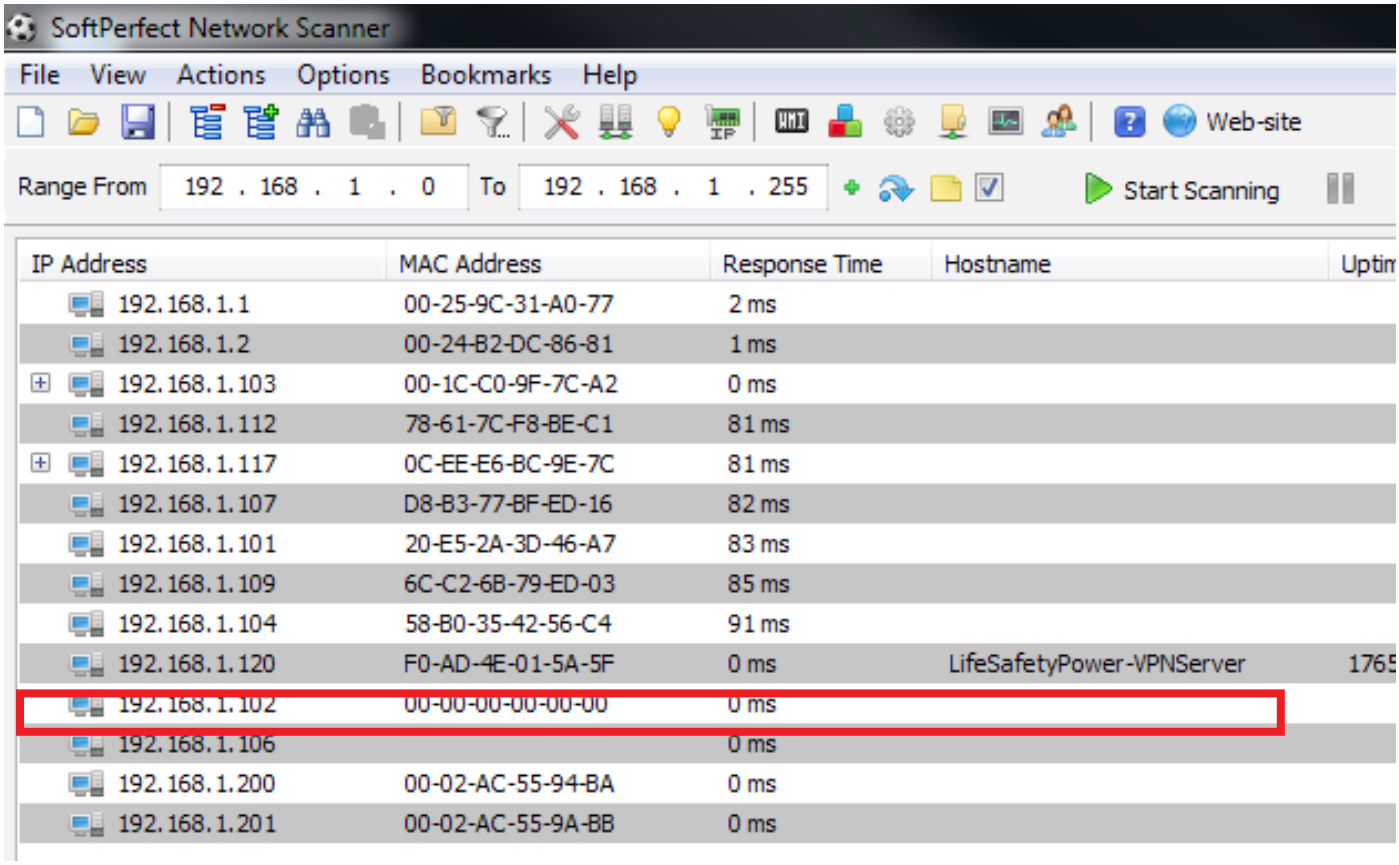


Figure 2: Network scanner screenshot

We can see the IP address for "LifeSafetyPower-VPNServer" is 192.168.1.120

3.1.2 Method 2 - via Automatic Email

This method will not work for the initial configuration of the MSM. After the email settings have been configured, the MSM will send an email any time it receives a new IP address from the DHCP server, assuming that the local area network is connected to the Internet. If the LAN is not connected to the Internet, then Method 1 must always be used.

Section 3 – Setting Up the MSM

3.2 Open a Port for the VPN Server on the Local Router

If access to the MSM is required from outside the local network (i.e. access from the internet), port 1723 must be made accessible in the local modem, router, or firewall settings. Use the MSM's local IP address as determined in Section 3.1. Figure 3 shows an example of port forwarding on a router.

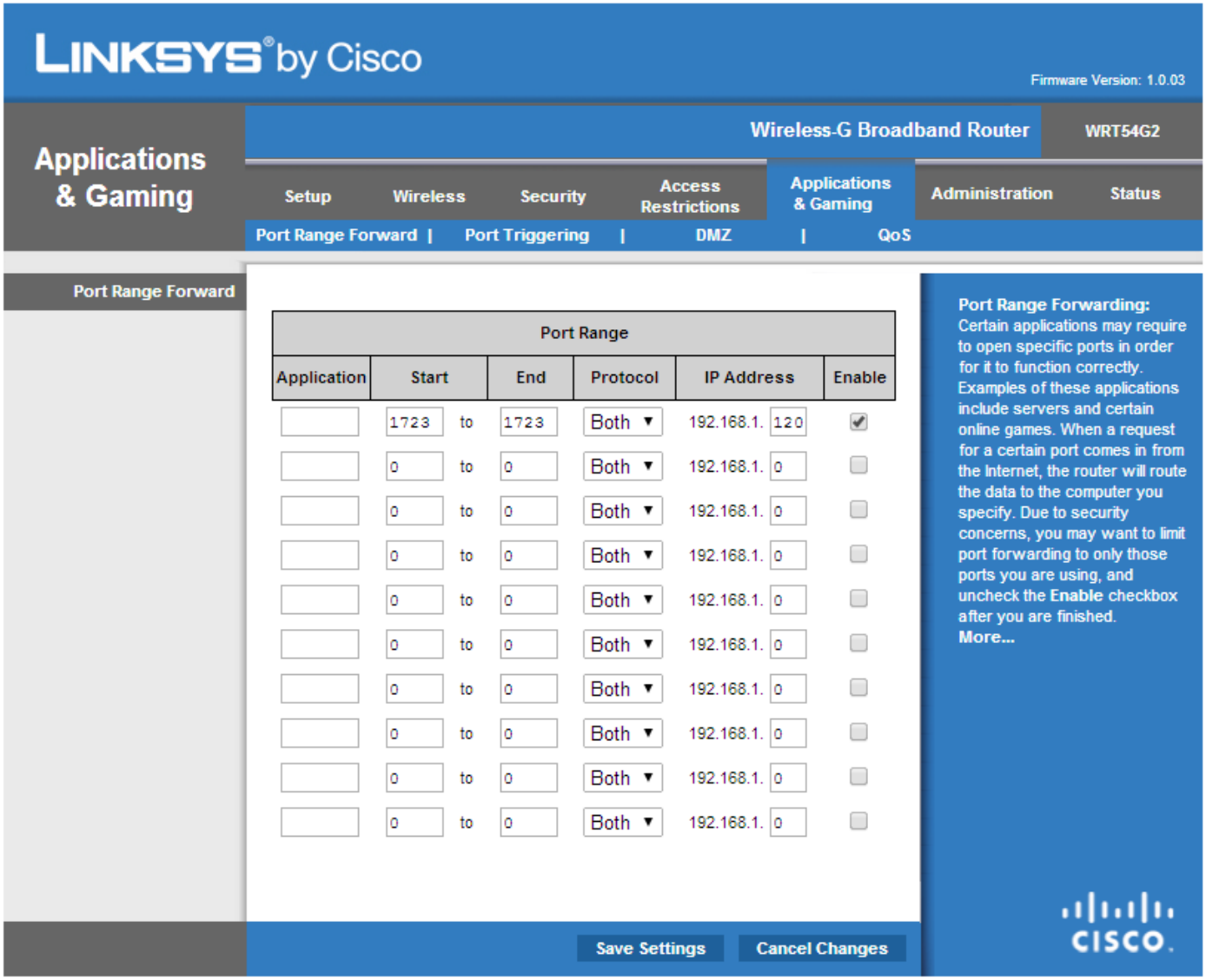


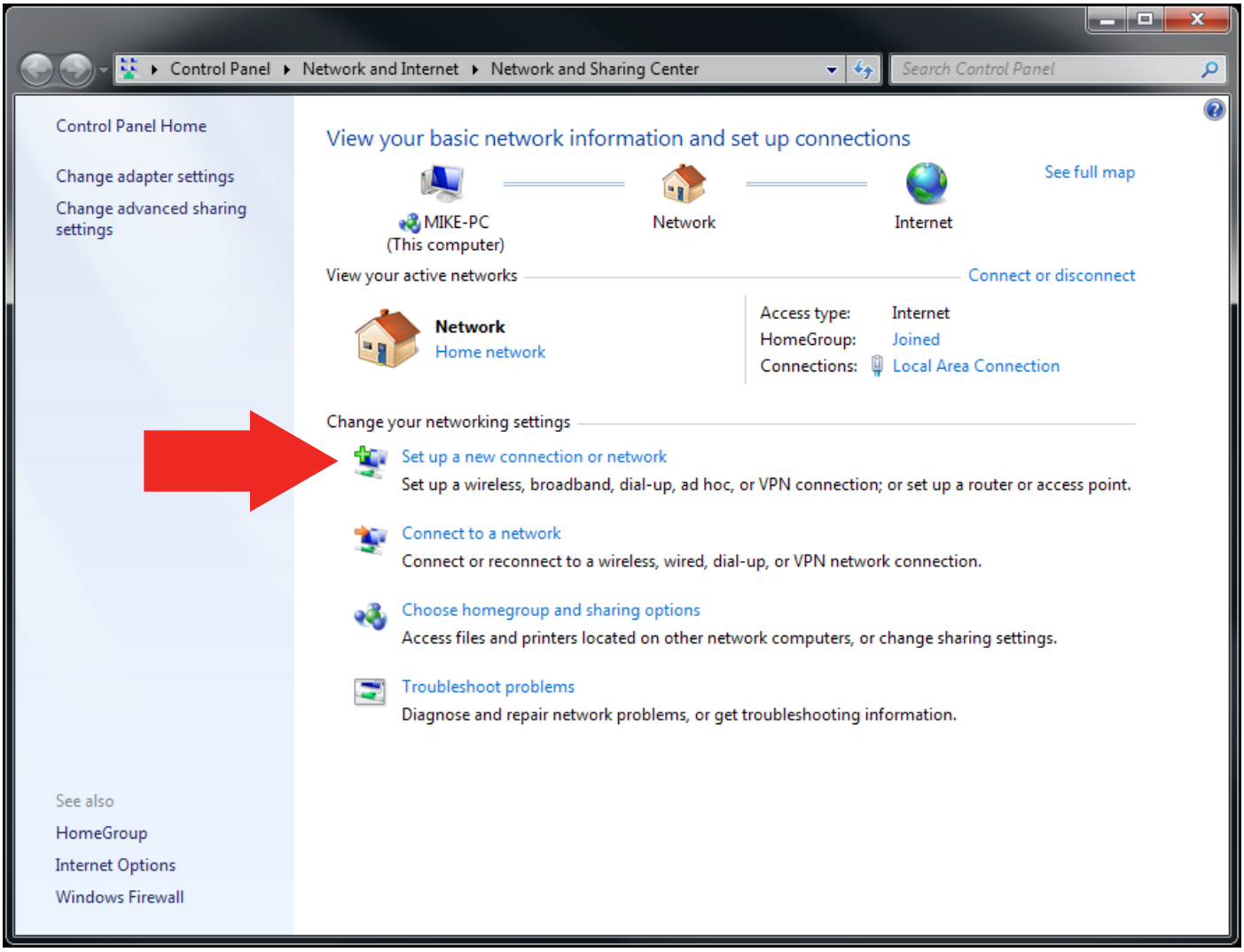
Figure 3: Example of local router port forwarding for MSM

Section 3 – Setting Up the MSM

3.3 Configure the MSM (VPN) Client Settings

To access the MSM (VPN server), the user must setup a VPN connection to the MSM on the device to be used to access it. For Windows 7 Professional, the major steps for client setup are given below:

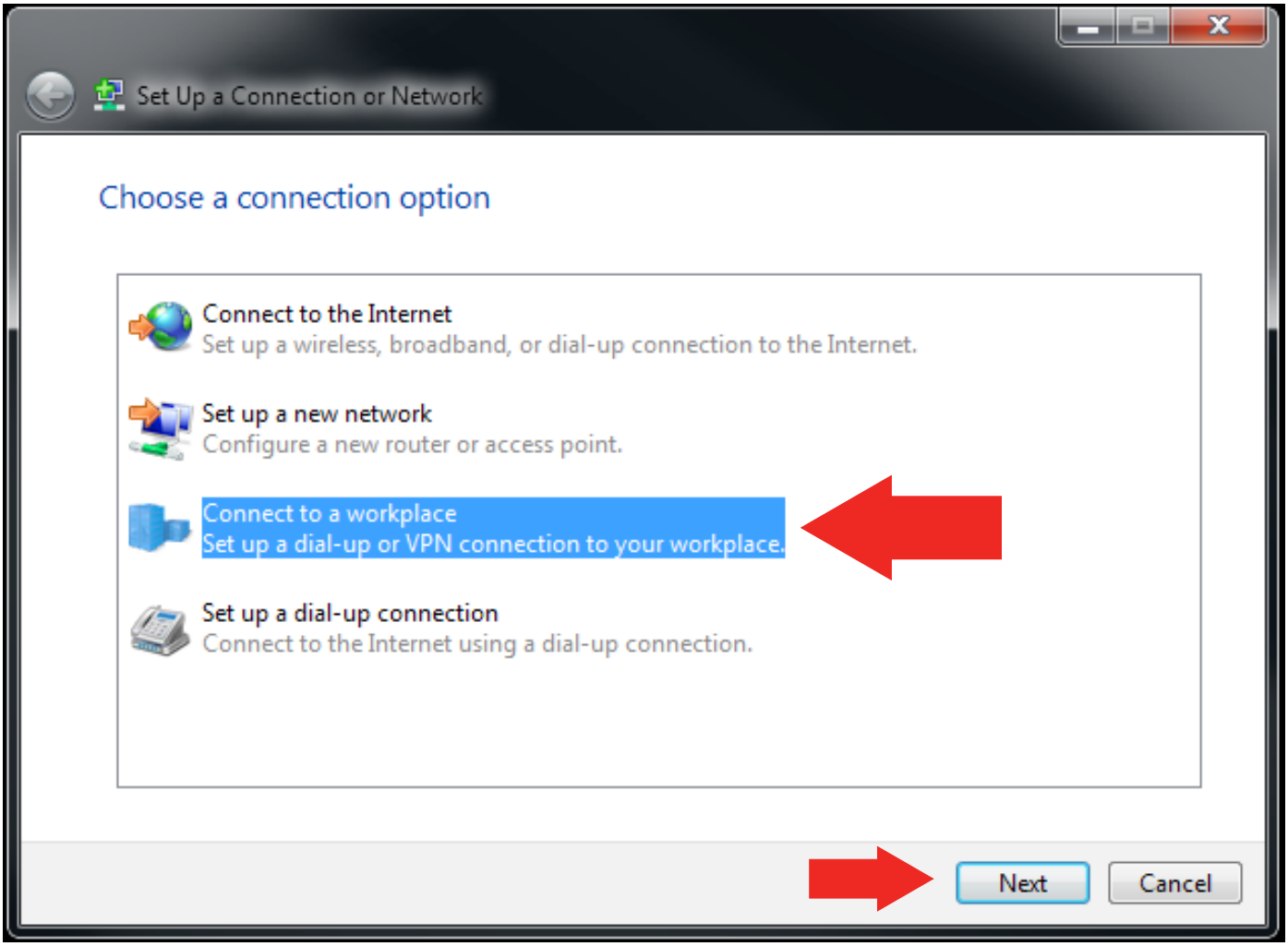
1. Open the “Network and Sharing Center”
2. Click “Setup a new connection or network” (as shown by the red arrow in the figure below):



Section 3 – Setting Up the MSM

3.3 Configure the MSM (VPN) Client Settings - continued

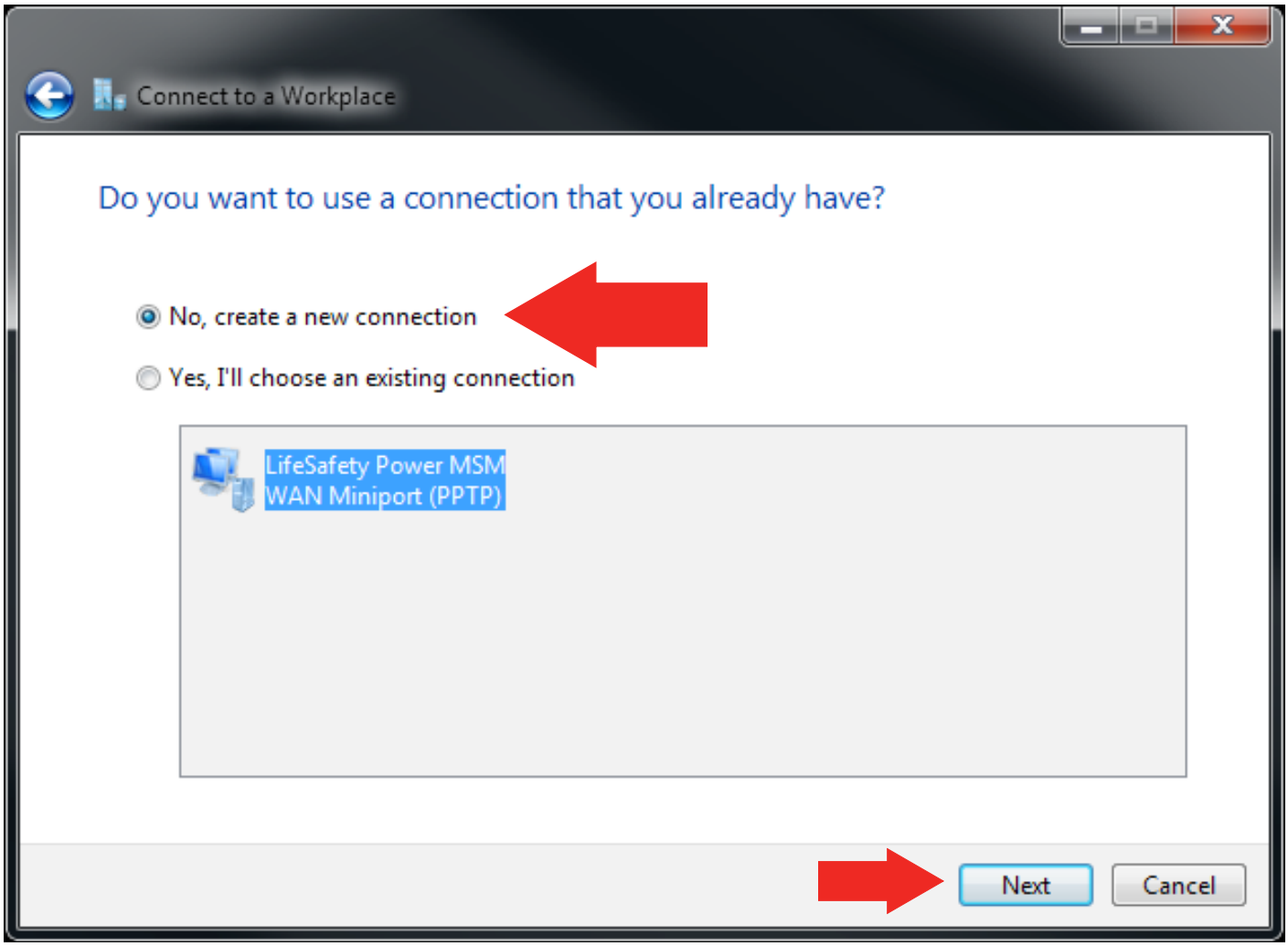
3. Select “Connect to a workplace”, then click the “Next” button (see figure below):



Section 3 – Setting Up the MSM

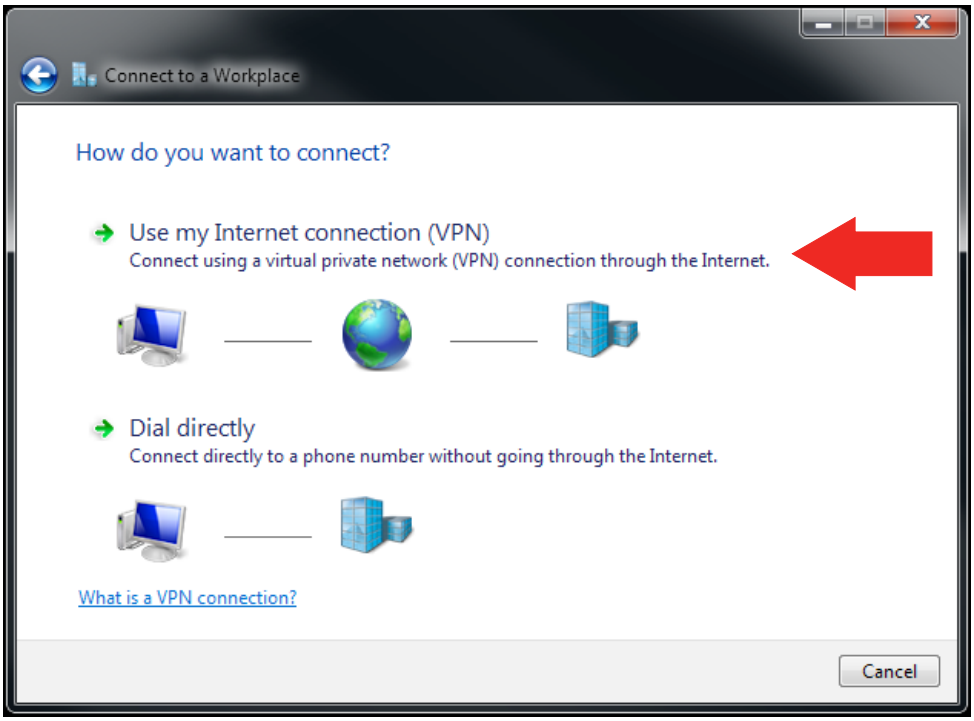
3.3 Configure the MSM (VPN) Client Settings - continued

4. If a dialog box appears asking if you want to use a connection that you already have, select "No, create a new connection" and click the "Next" button (see figure below):

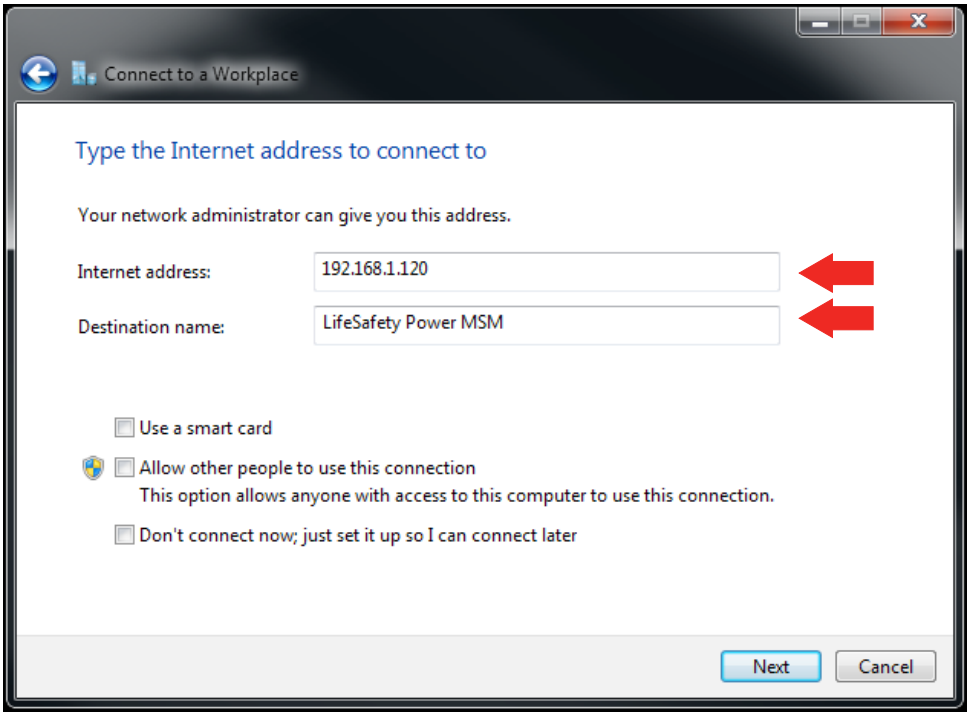


3.3 Configure the MSM (VPN) Client Settings - continued

5. Click “Use my Internet connection (VPN)" as shown by the red arrow (see figure below):



6. Enter the Internet address to connect to. This is the IP address of the MSM as determined earlier (Section 3.1). You may also enter the “Destination name”. Default value is “VPN Connection” (see figure below):

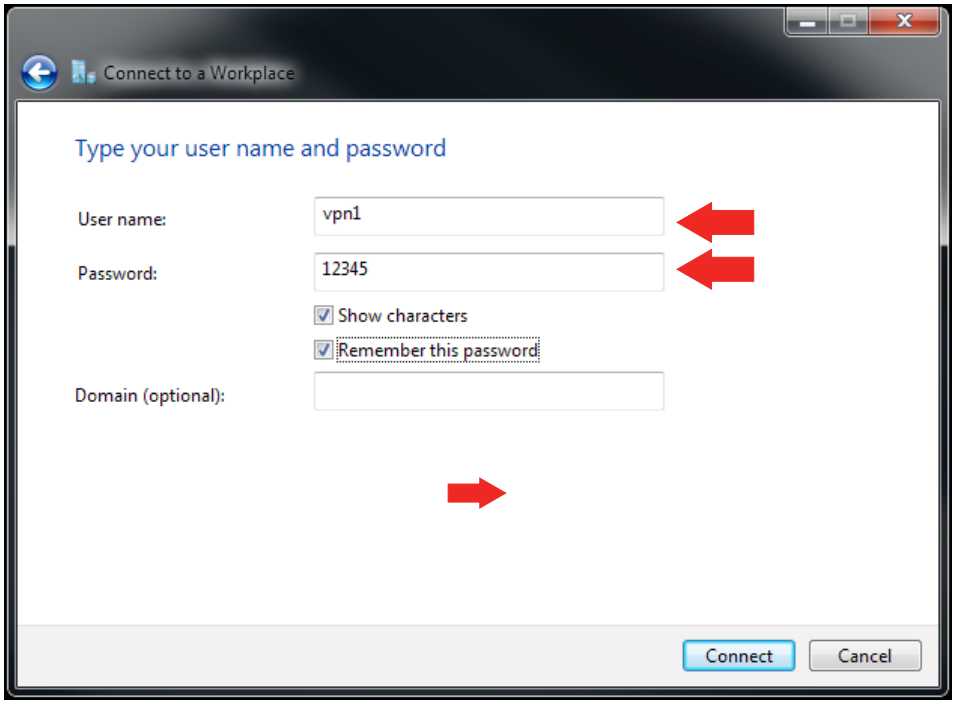


3.3 Configure the MSM (VPN) Client Settings - continued

7. Enter a User Name and Password.

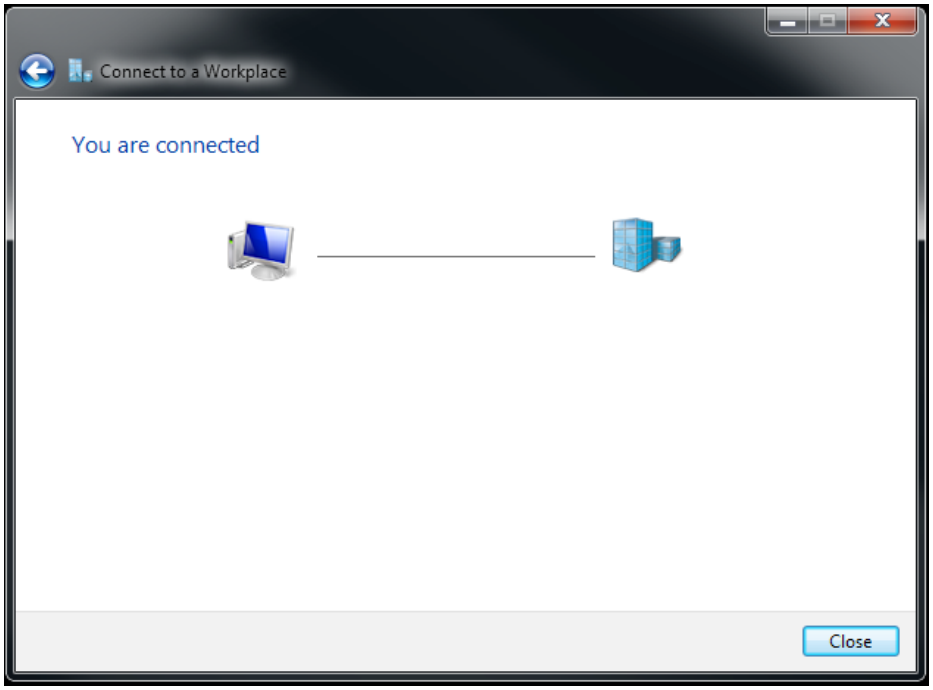
By default the MSM has one valid user name preconfigured: vpn1. The default password for this account is “12345”. MSM Administrators can setup extra user account names and passwords. Each user should have his own user name and password.

Once assigned, enter the user name and password and click “Connect”



8. After the “Connect” button is clicked, the VPN client will attempt to connect to the VPN server.

The screen will display the handshaking message between the VPN client and the server. If everything is entered correctly, the connection will be established within a minute (see figure below).



3.4 Open the MSM Browser Interface

Once the VPN connection is established, the user can open the MSM browser interface by typing the default IP address into a browser: 192.168.3.1. The browser interface requires a user name and password. The default user name is “admin”; and the password is “admin”. The password can be changed in the “Configure” page of the MSM's interface.

Figure 4 shows the HOME page of the VPN Interface.

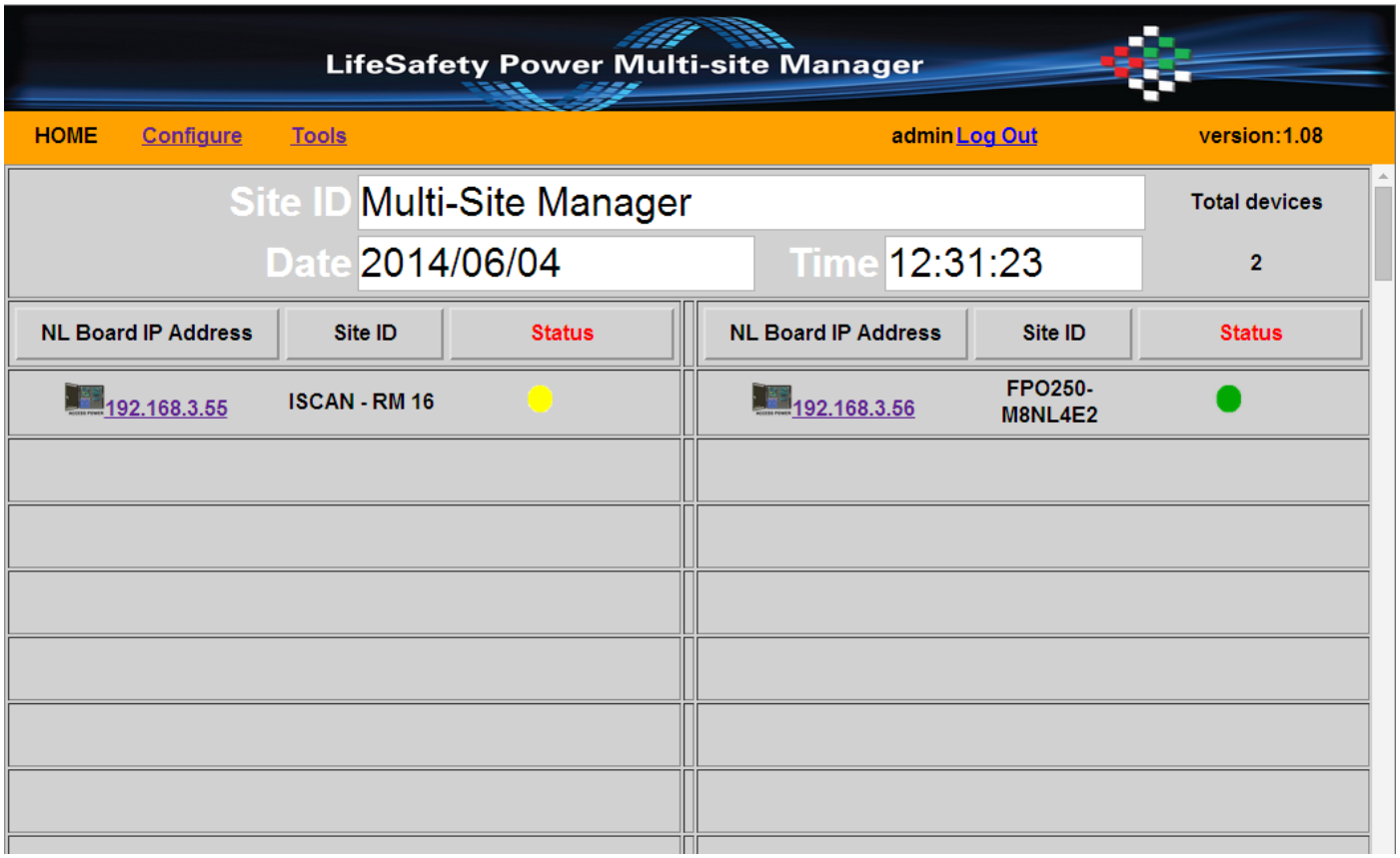


Figure 4: MSM Interface: HOME page

The orange bar at the top contains the navigation menu to the Home, Configuration, and Tools pages. The firmware version number is also present at the right of the orange bar.

Under the orange bar, the Site ID, Date, and Time are shown. These can all be set on the Configure page. See section 3.5

The bottom of the page shows each connected device and its related status in two columns. The devices can be sorted by IP, Site ID, or Status by clicking the "NL Board IP Address", "Site ID", or "Status" buttons, respectively. Multiple clicking the buttons will toggle between ascending and descending order. The status of each device is represented by a colored dot. A normal status is indicated by a green dot. Any fault condition will change this dot to yellow. If the device contains a fire alarm interface (FAI), the dot will change to flashing red when FAI is activated.

⚠ Note that after first powering the MSM, it may take several minutes for the MSM to locate all of the LSP network devices on the local network.

The example in Figure 4 shows a total of 2 devices connected to the MSM. Clicking any of the device icons or IP addresses will bring up the GUI of that particular device.

3.5 Configuration page of the MSM GUI

Clicking the “Configure” tab opens the Configure page of the MSM as shown in Figures 5a and 5b:

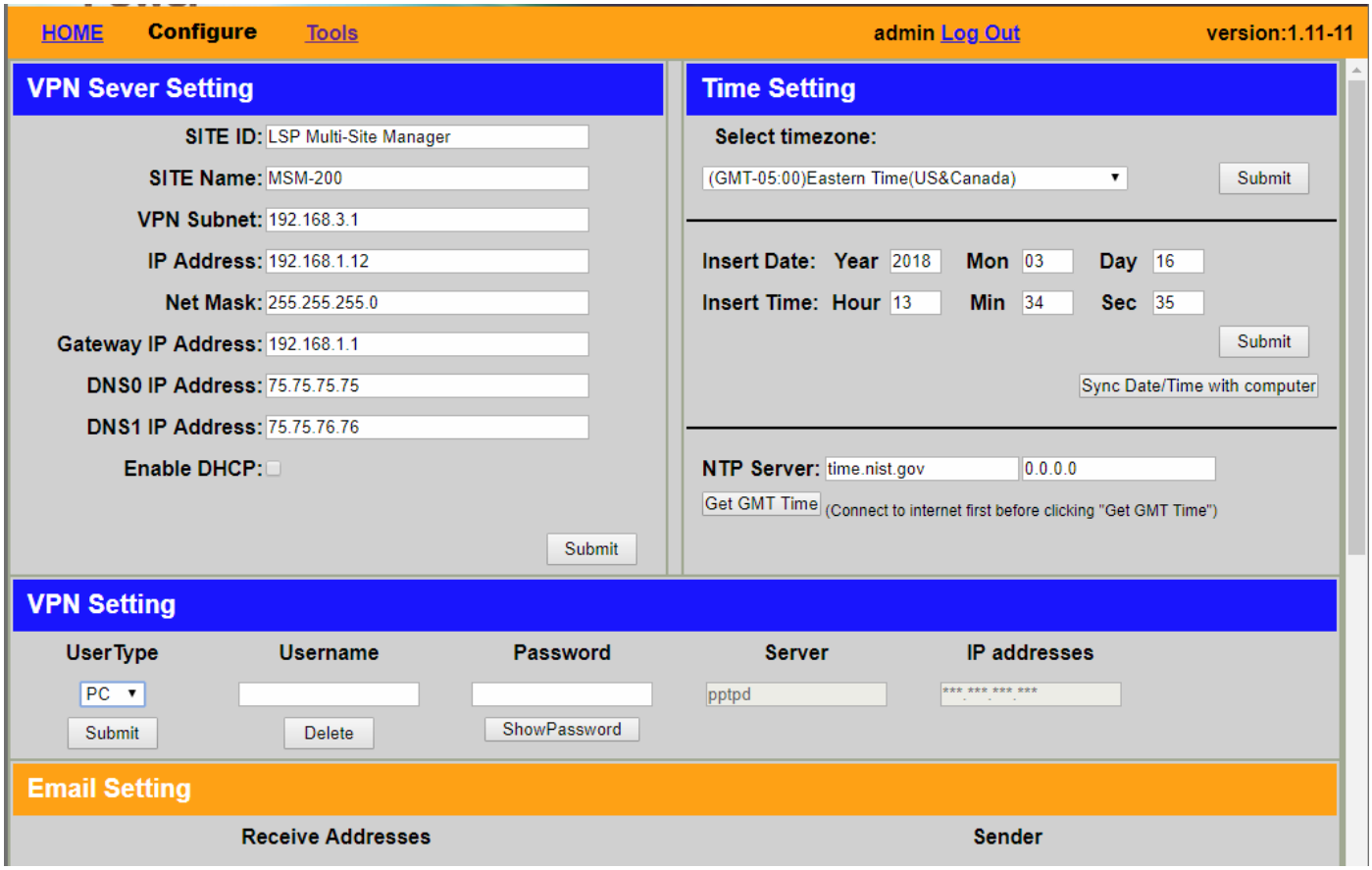


Figure 5a: Configure page (upper half)

Under VPN Server Settings, enter the Site ID, Site Name and VPN Subnet IP address, along with the local IP settings. If DHCP rather than a static IP is desired, check the Enable DHCP box. Click the “Submit” button to save the settings for this section. The factory default VPN IP address is 192.168.3.1. The MSM must be rebooted after changing the VPN Subnet IP Address for the changes to take effect. See section 3.6.2

In the Time Settings section, select the desired time zone in the Time Zone drop down menu. Click the “Submit” button to save the time zone. Enter the current date and time in the Insert Date and Insert Time fields. Click the “Submit” button to save the date and time. To synchronize the MSM date and time with an NTP server, enter the URL of an NTP server of your choice, then click the “Get GMT Time” button. Ensure the time zone has been set (including clicking the Submit button) before synchronizing with an NTP server.

Under the VPN Settings section, Administrator-level users can create new VPN user accounts. When creating a new user account, select "PC" for the “User Type” in the drop down menu. Enter the new user name and password, and click “submit” to save the new user. The new account will not be accessible until the MSM is rebooted from the "Tools" page. New MSM user accounts may only be added one at a time (each one requiring a reboot of the MSM). Up to ten new user accounts can be created. To delete a user account, select the checkbox on the right of the account you wish to delete, then click the “Delete” button. The "LSP" user type is currently unused - always select "PC".

There is one preset user account available by default. The user name is vpn1 and the password is 12345.

⚠ ***WARNING*** - Passwords may not contain any special characters. Only numbers and letters may be used. Creating a password with a special character will result in the user being locked out of the device and will require a device reset.

⚠ If the wrong password is entered three consecutive times, the user will be locked out of the device for 24 hours. Enter the password carefully to avoid lockout.

3.5 Configuration page of the MSM GUI - continued

Below the VPN Settings section of the Configure page is the Email Settings section (Figure 5b).

In the Email Settings section, the sender and recipient email information can be entered. The sender email account must be a valid SMTP type email account. The recipient email accounts should be accessible by the installer of the VPN if the user needs to obtain the VPN local IP address via email. The Email Test section will test the email settings set above.

In the User Settings section, Administrator-level users can setup MSM interface access accounts. There are three levels of user accounts: admin, manager and guest. Guest users can only view the interface and cannot change anything in the system. Manager users can access all interface pages except the Configure pages. Admin users can perform all operations on all pages of the interface.

⚠ ***WARNING*** - Passwords may not contain any special characters. Only numbers and letters may be used. Creating a password with a special character will result in the user being locked out of the device and will require a device reset.

Note: This section configures the MSM interface access accounts. This is different from the VPN User Accounts described in Figure 5a on the previous page.

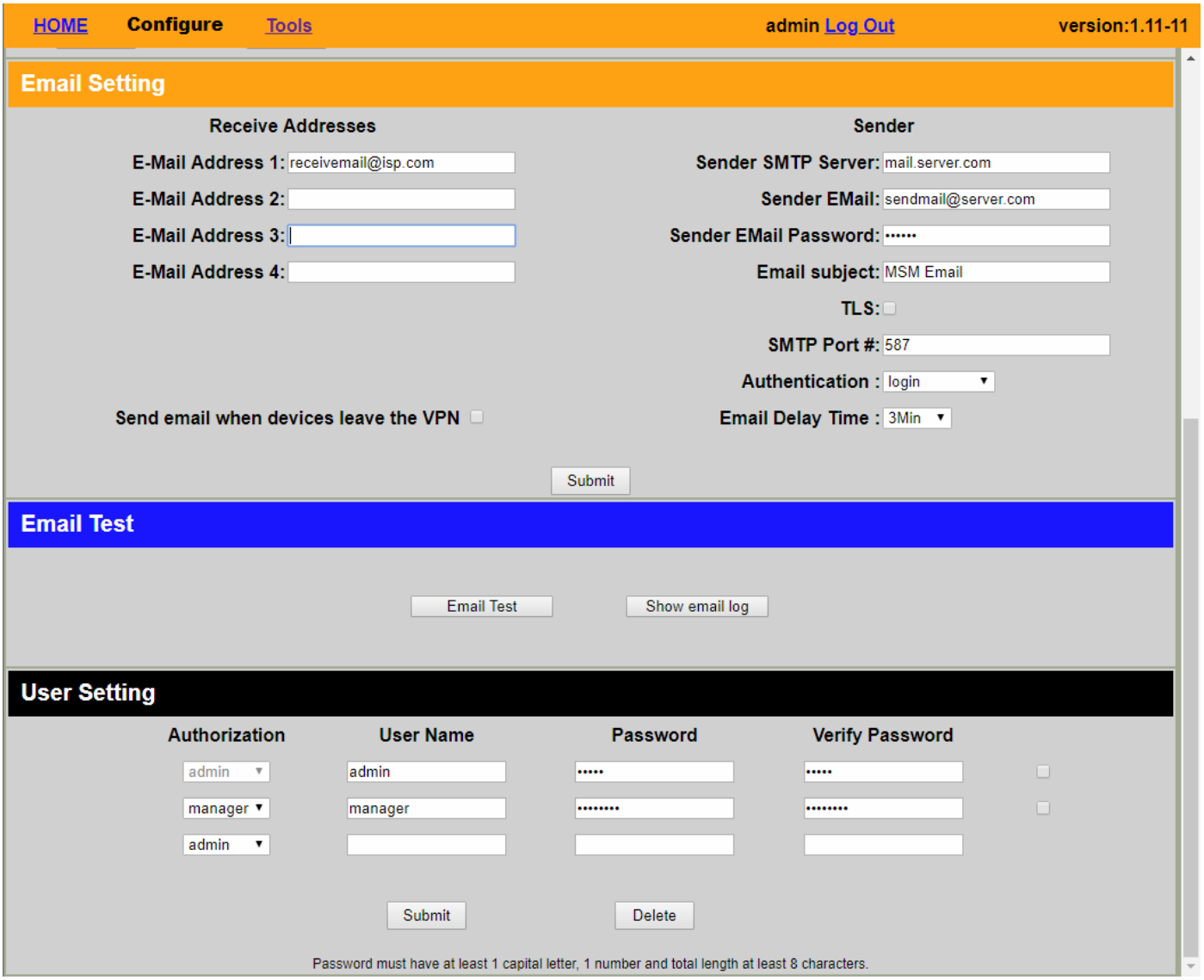


Figure 5b: Configure page (bottom half)

3.6 Tools Page of the GUI

Clicking the Tools tab in the orange bar opens the Tools page, as shown in Figure 6.

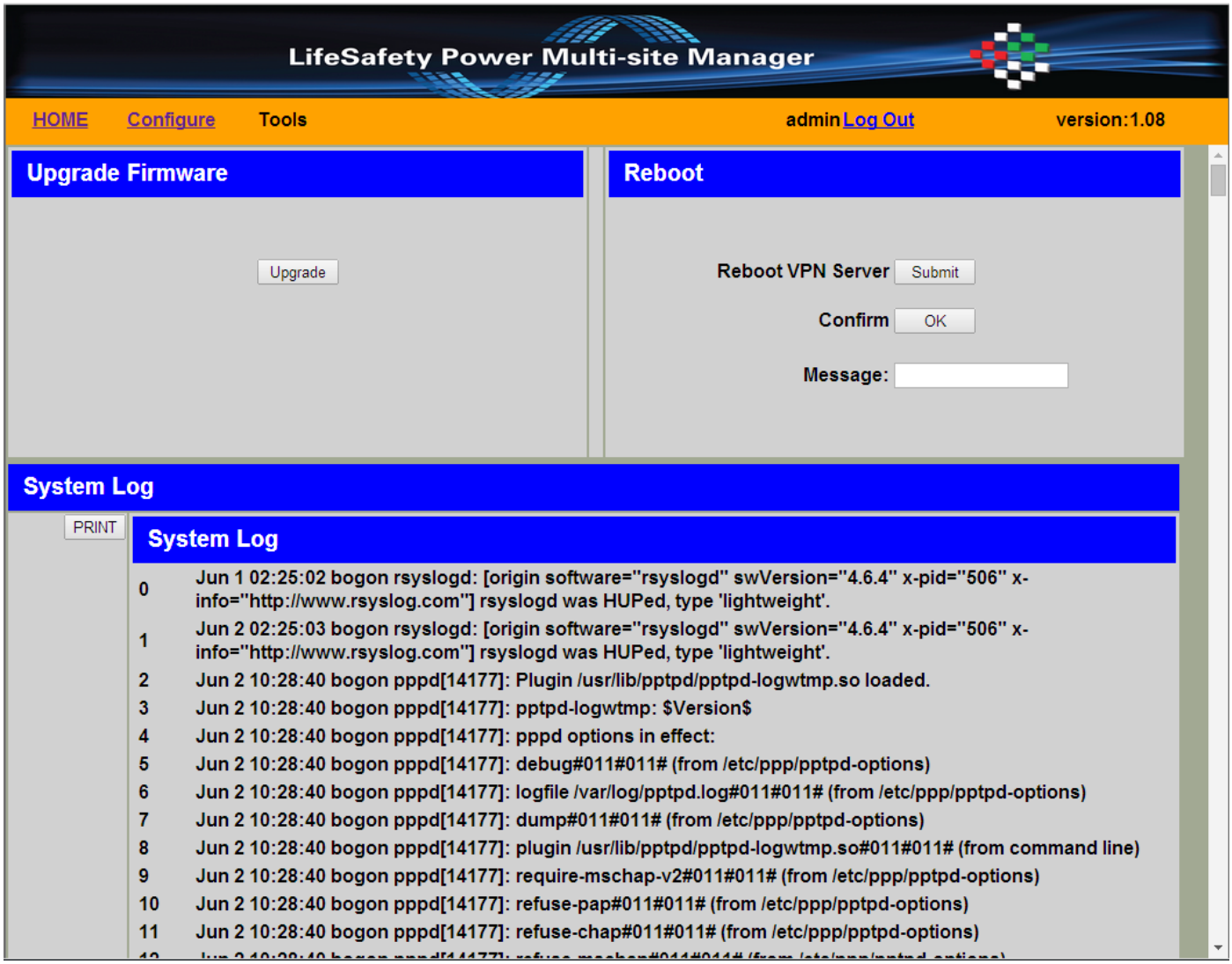


Figure 6: TOOLS page

3.6.1 Upgrading the Firmware

The “Upgrade Firmware” section is located at the upper left corner of the “Tools” page as shown in Figure 6. To upgrade the MSM firmware, click the “Upgrade” button. The upgrade window will appear as shown in Figure 7.

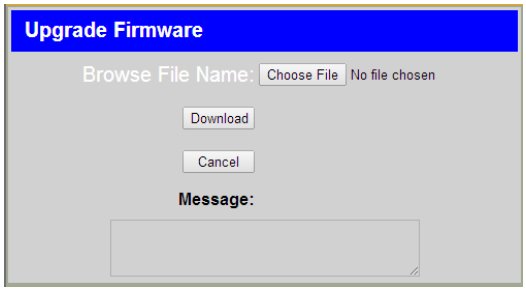


Figure 7: “Upgrade Firmware” screen after clicking “Upgrade” button

Click the “Browse…” button (Figure 7) and locate the new firmware file *.tar.gz on your PC, as shown in the screenshot on the left side of Figure 8 (next page).

3.6.1 Upgrading the Firmware - continued

Note that the firmware file has the extension of .tar.gz. Do not unzip the firmware file.

After selecting the new firmware file, click the "Download" button - See Figure 8. The new firmware will be downloaded to the RAM of the VPN server. During the downloading process, the message box will indicate "Download …". Once the firmware download is completed, the screen in Figure 9 will appear.

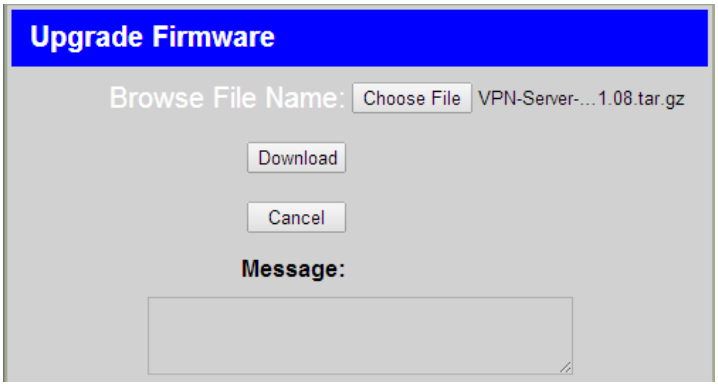


Figure 8: "Upgrade Firmware" screen after the download is complete page

Click the "Confirm" button (Figure 9) to confirm the upgrade of the firmware to the downloaded file ("VPN-Server-SW-1.08.tar.gz" in this example). After clicking the "Confirm" button, the screen in Figure 10 will appear.

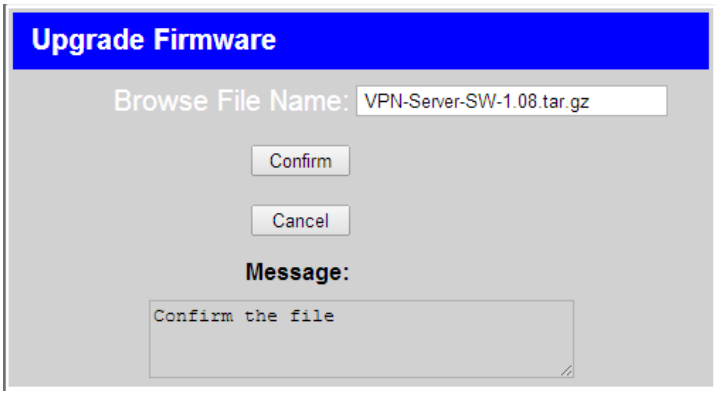


Figure 9: "Upgrade Firmware" screen when the download is complete

Click the "Burn" button (Figure 10) to begin the firmware programming. After clicking the "Burn" button, the screen will appear as shown in Figure 11 while the new firmware is being programmed to the flash memory of the MSM. This process may take up to 30 seconds. **Warning: DO NOT TURN OFF THE POWER TO THE MSM DURING THE UPGRADE PROCESS.** Power interruption during the program upgrade will damage the firmware of the VPN server and render it nonfunctional. Once the new firmware programming is complete, a message will appear in the message box as shown in Figure 12. The MSM must now be rebooted.

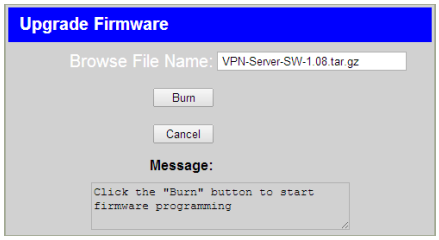


Figure 10:
"Upgrade Firmware" screen after clicking the "Confirm" button

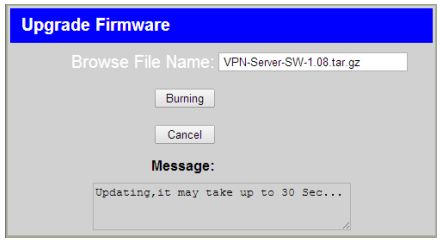


Figure 11:
"Upgrade Firmware" screen after clicking the "Burn" button

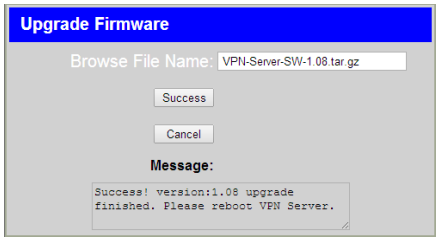


Figure 12:
"Upgrade Firmware" screen after the firmware upgrade is completed

3.6.2 Rebooting the MSM

The “Reboot” section is at the upper right hand corner of the “Tools” page, as shown in Figure 6. Click the “Submit” button next to “Reboot VPN Server”. The screen in Figure 13 will appear.

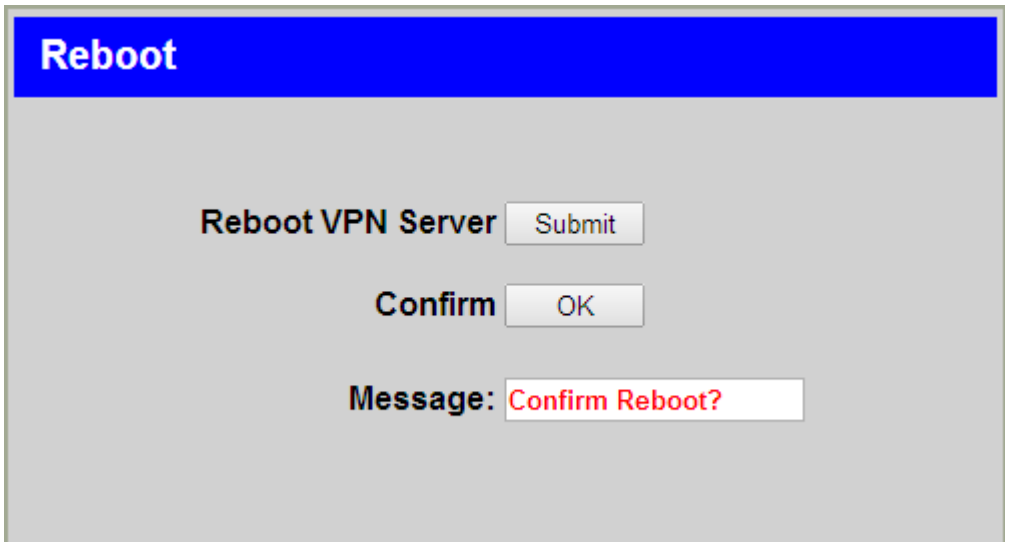


Figure 13: “Reboot” screen after clicking the “Submit” button

Click the “OK” button next to “Confirm”, the VPN server will start the reboot process. While rebooting, the screen will briefly appear as in Figure 14. As the reboot continues, the connection to the network will be momentarily lost. Once the VPN is fully restarted with the new firmware, it will send an email to the preprogrammed email addresses indicating the VPN IP address assigned by the local router.

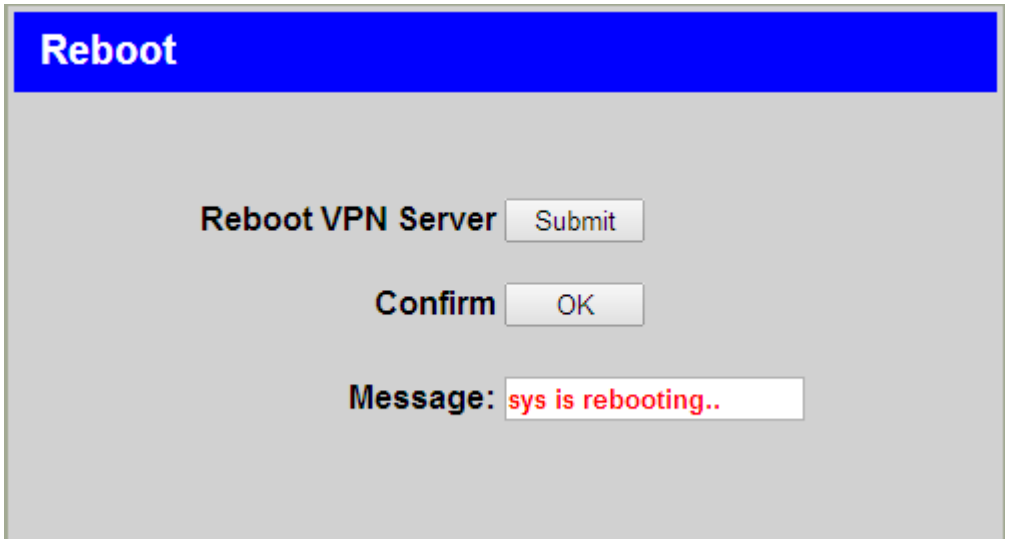


Figure 14: VPN server is rebooting

Technical Support

For technical support please contact the factory at 1 888.577.2898

Section 4 – Setting Up NetLink Devices for use with the MSM-200

The MSM-200 will auto discover NetLink and NPR devices when these devices are properly configured. The configuration method is determined by the MSM's IP subnet in relation to the device being configured.

4.1 NetLink Devices in the same subnet as the MSM-200

If the NetLink devices are within the same local network as the MSM-200 and are set to be within the same subnet, the MSM will auto-detect the devices.

For example, if the MSM is properly configured on a LAN and has the local IP address of 192.168.1.100, the NetLink should also have an IP address of 192.168.1.xxx to be auto-discovered. The MSM may take several minutes to find the NetLink device(s). Once discovered, the MSM will auto assign the VPN IP address for the NetLink devices (for example, 192.168.3.xxx.

4.2 - NetLink Devices not within the same subnet or LAN as the MSM-200

If the NetLink devices are not within the same subnet as the MSM-200, additional configuration must be performed in order to connect the device to the MSM-200. NOTE: To configure a NetLink device which is NOT on the same LAN as the MSM-200, both the MSM-200 and the NetLink device must be on networks with internet access.

Within the NetLink device's "Configuration" screen is a VPN Settings section (see Figure 15). To configure the device to be auto detected by them MSM-200, configure this section as follows:

EnableRemoteVPNServer - Check this box to enable the remote VPN Server

IP Address - Enter the IP address of the remote MSM-200.

The **User Name** and **Password** fields are preset and grayed out. Only the IP address is required.

Click the "Submit" button to apply the settings and reboot the NetLink device for the settings to take effect. The MSM may take several minutes to discover the NetLink device, depending on network speed and traffic.

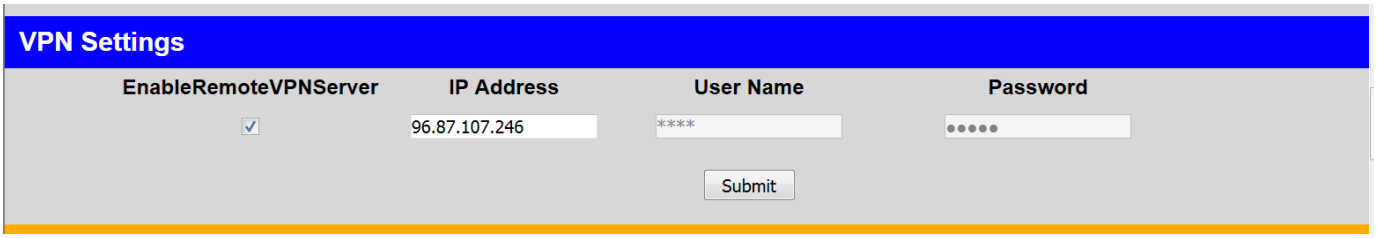


Figure 15: VPN Setting Configuration Screen

P03-047 Rev A04 07/19

LifeSafety Power Inc.
899 E. Park Avenue
Libertyville, IL 60048 USA
www.lifesafetypower.com
Phone (888) 577-2898
info1@lifesafetypower.com