M86 Web Filter Installation Guide

Models: HL, SL, MSA

Version 5.0.10

Publication Date: 08.06.12

Legal Notice

The most current version of this document may be obtained by contacting:

Trustwave Technical Support:
Phone: +1.800.363.1621
Email: support@trustwave.com

Trademarks

Part# WF-IG-HSM-120806

CONTENTS

M86 WEB FILTER INTRODUCTION

Thank you for choosing to install the M86 Security Web Filter. The Web Filter tracks end users' online activity, and can be configured to block specific Web sites or service ports, thereby protecting your organization against lost productivity, network bandwidth issues, and possible legal problems that can result from the misuse of Internet resources. This product also features expansive library categories, instant message and peer-to-peer blocking, user authentication, and intuitive screens and fields for ease of use when configuring and maintaining the server, as well as managing user and group filtering profiles.

The HL and SL server models include RAID technology for fault tolerance and high performance.

Quick setup procedures—to implement the best filtering practices for the scenarios described in the first paragraph—are included in the Best Filtering Practices section that follows the Conclusion of this guide.

About this Document

This document is divided into the following sections:

- **Introduction** - This section is comprised of an overview of this product and how to use this document

- **Service Information** - This section provides M86 Security contact information

- **Preliminary Setup Procedures** - This section includes instructions on how to physically set up the appliance in your network environment

- **Install the Server** - This section explains how to configure the appliance for filtering

- **Conclusion** - This section indicates that the installation steps have been completed

- **Best Filtering Practices** - This section includes a chart of library categories organized into Threat Class Groups, accompanied by filtering scenarios and directions for implementing the best filtering practices to secure your network, prevent excessive bandwidth usage, and increase productivity

- **LED Indicators and Buttons** - This section explains how to read LED indicators and use LED buttons for troubleshooting the unit

- **Regulatory Specifications and Disclaimers** - This section cites safety and emissions compliance information for the models referenced in this document

- **Appendix** - The appendix provides an alternate way of installing the Web Filter by using a crossover cable

- **Index** - An alphabetized list of some topics included in this document

Conventions Used in this Document

The following icons are used throughout this document to call attention to important information pertaining to handling, operation, and maintenance of the server; safety and preservation of the equipment, and personal safety:

NOTE: *The "note" icon is followed by additional information to be considered.*

WARNING: *The "warning" icon is followed by information alerting you to a potential situation that may cause damage to property or equipment.*

CAUTION: *The "caution" icon is followed by information warning you that a situation has the potential to cause bodily harm or death.*

TIP: *The "tip" icon is followed by italicized text giving you hints on how to execute a task more efficiently.*

IMPORTANT: *The "important" icon is followed by information M86 Security recommends that you review before proceeding with the next action.*

The "book" icon references the R3000 User Guide. This icon is found in the Best Filtering Practices section of this document.

SERVICE INFORMATION

The user should not attempt any maintenance or service on the unit beyond the procedures outlined in this document.

Any initial hardware setup problem that cannot be resolved at your internal organization should be referred to an M86 Security solutions engineer or technical support representative.

For technical assistance or warranty repair, please visit **http://www.m86security.com/support/** .

M86 Technical Support Call Procedures

When calling M86 Security regarding a problem, please provide the representative the following information:

- Your contact information.

- Serial number or original order number.

- Description of the problem.

- Network environment in which the unit is used.

- State of the unit before the problem occurred.

- Frequency and repeatability of the problem.

- Can the product continue to operate with this problem?

- Can you identify anything that may have caused the problem?

PRELIMINARY SETUP PROCEDURES

Unpack the Unit from the Carton

Inspect the packaging container for evidence of mishandling during transit. If the packaging container is damaged, photograph it for reference.

Carefully unpack the unit from the carton and verify that all accessories are included. Save all packing materials in the event that the unit needs to be returned to M86 Security.

The carton should contain the following items:

• 1 HL, SL, or MSA unit
• 1 AC Power Cord, 2 AC Power Cords for HL servers
• 1 Serial Port Cable
• Rack Mount Brackets (2)

User guides can be obtained at **http://www.m86security.com/support/R3000/documentation.asp**

For troubleshooting tips to assist you during the installation process, visit **http://www.m86security.com/software/8e6/ts/r3000.html**

For hardware specifications of this model, see: **http://www.m86security.com/software/8e6/hd/8e6_r3000_hd_specs.pdf**

NOTES: For HL and SL servers, 1 bezel to be installed on the front of the chassis also is included, as well as 1 spare parts kit. For HL servers, this kit contains a hard drive and power supply. For SL servers, this kit contains a hard drive. Please refer to the appendix of the user guide for information on replacing a hard drive or power supply.

Inspect the server and accessories for damage. If the contents appear damaged, file a damage claim with the carrier immediately.

WARNING: To avoid danger of suffocation, do not leave plastic bags used for packaging the server or any of its components in places where children or infants may play with them.

Select a Site for the Server

The server operates reliably within normal office environmental limits. Select a site that meets the following criteria:

- Clean and relatively free of excess dust.

- Well-ventilated and away from sources of heat, with the ventilating openings on the server kept free of obstructions.

- Away from sources of vibration or physical shock.

- Isolated from strong electromagnetic fields and noise caused by electrical devices such as elevators, copy machines, air conditioners, large fans, large electric motors, radio and TV transmitters, and high-frequency security devices.

- Access space provided so the server power cord can be unplugged from the power supply or the wall outlet—this is the only way to remove the AC power cord from the server.

- Clearance provided for cooling and airflow: Approximately 30 inches (76.2 cm) in the back and 25 inches (63.5 cm) in the front.

- Located near a properly earthed, grounded, power outlet.

Rack Mount the Server

Rack Setup Precautions

⚠ **WARNING:**

Before rack mounting the server, the physical environment should be set up to safely accommodate the server. Be sure that:

- The weight of all units in the rack is evenly distributed. Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

- The rack will not tip over when the server is mounted, even when the unit is fully extended from the rack.

- For a single rack installation, stabilizers are attached to the rack.

- For multiple rack installations, racks are coupled together.

- Reliable earthing of rack-mounted equipment is maintained at all times. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).

- A power cord will be long enough to fit into the server when properly mounted in the rack and will be able to supply power to the unit.

- The connection of the server to the power supply will not overload any circuits. Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

- The server is only connected to a properly rated supply circuit. Reliable earthing (grounding) of rack-mounted equipment should be maintained.

- The air flow through the server's fan or vents is not restricted. Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

- The maximum operating ambient temperature does not exceed 104°F (40°C). If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.

⚠ *WARNING: Extend only one component at a time. Extending two or more components simultaneously may cause the rack to become unstable.*

Rack Mount Instructions for HL Servers

Rack Setup Suggestions

- Determine the placement of each component in the rack before you install the rails.
- Install the heaviest server components on the bottom of the rack first, and then work up.

Identify the Sections of the Rack Rails

You should have received two rack rail assemblies with the M86 Security server unit. Each of these assemblies consists of two sections: An inner fixed chassis rail that secures to the unit (A), and an outer fixed rack rail that secures directly to the rack itself (B). Two pairs of short brackets to be used on the front side of the outer rails are also included.

Outer Rail (attaches to rack)

Inner Rail (pre-installed)

Locking Tab
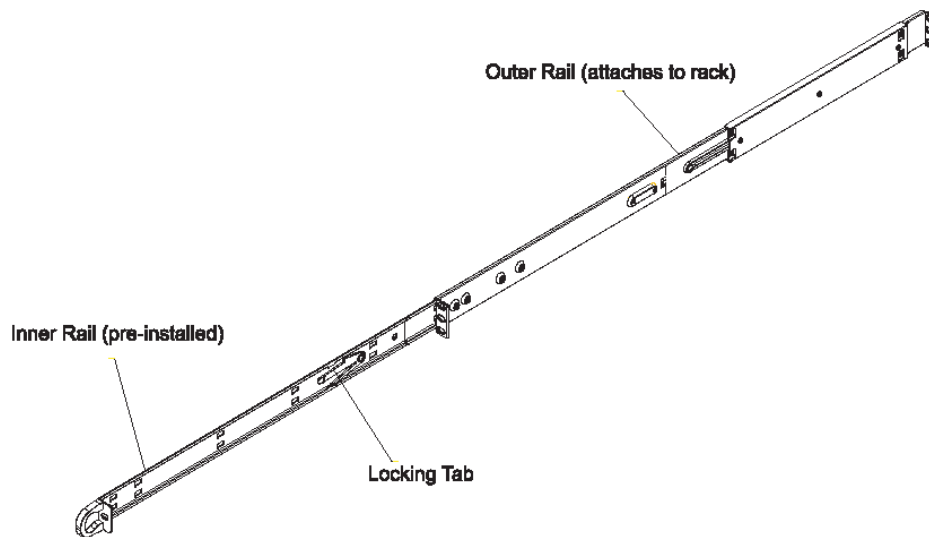
Install the Inner Rails

Both the left and right side inner rails have been pre-attached to the chassis. Proceed to the next step.

Install the Outer Rails

Begin by measuring the distance from the front rail to the rear rail of the rack. Attach a short bracket to the front side of the right outer rail and a long bracket to the rear side of the right outer rail. Adjust both the short and long brackets to the proper distance so that the rail can't snugly into the rack. Secure the short bracket to the front side of the outer rail with two M4 screws and the long bracket to the rear side of the outer rail with three M4 screws. Repeat these steps for the left outer rail.

Locking Tabs: Both chassis rails have a locking tab, which serves two functions. The first is to lock the server into place when installed and pushed fully into the rack, which is its normal position. Secondly, these tabs also lock the server in place when fully extended from the rack. This prevents the server from coming completely out of the rack when you pull it out for servicing.
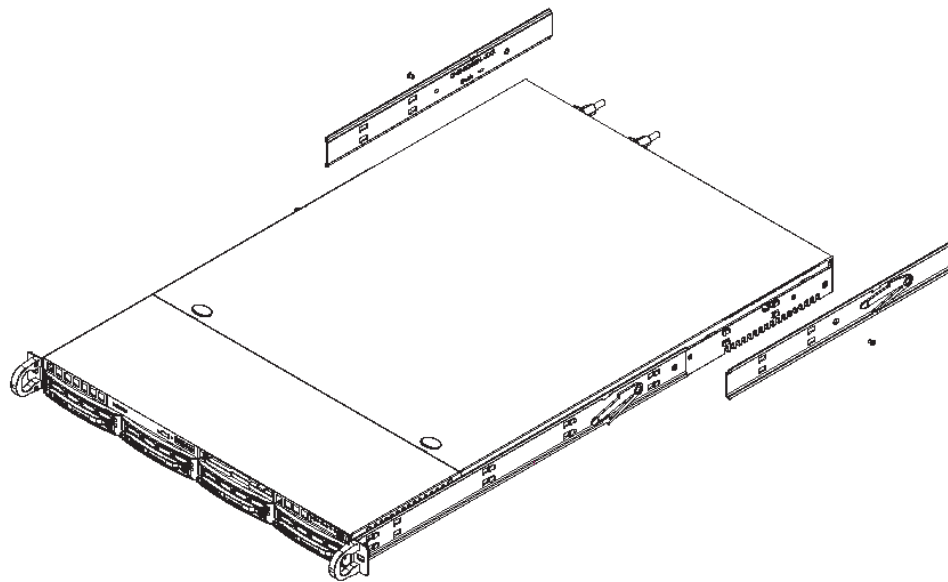
Install the Server into the Rack

You should now have rails attached to both the chassis and the rack unit. The next step is to install the server chassis into the rack. Do this by lining up the rear of the chassis rails with the front of the rack rails. Slide the chassis rails into the rack rails, keeping the pressure even on both sides (you may have to depress the locking tabs when inserting).

When the server has been pushed completely into the rack, you should hear the locking tabs "click."
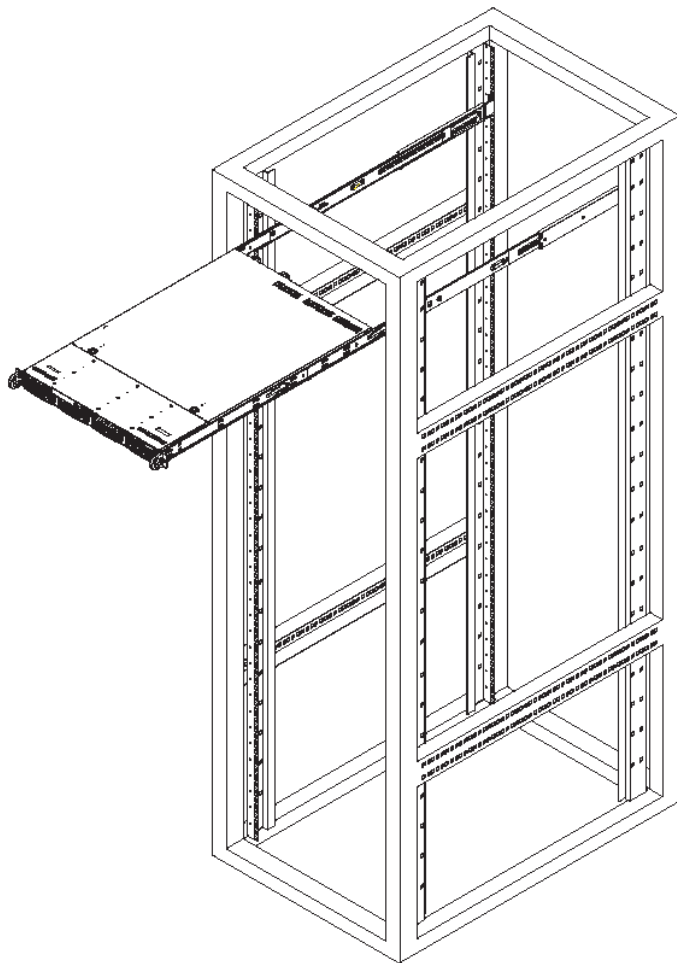
Install the Server into a Telco Rack

If you are installing the M86 Security server unit into a Telco type rack, use two L-shaped brackets on either side of the chassis (four total). First, determine how far follow the server will extend out the front of the rack. A larger chassis should be positioned to balance the weight between front and back. If a bezel is included on your server, remove it. Then attach the two front brackets to each side of the chassis, then the two rear brackets positioned with just enough space to accommodate the width of the Telco rack. Finish by sliding the chassis into the rack and tightening the brackets to the rack.
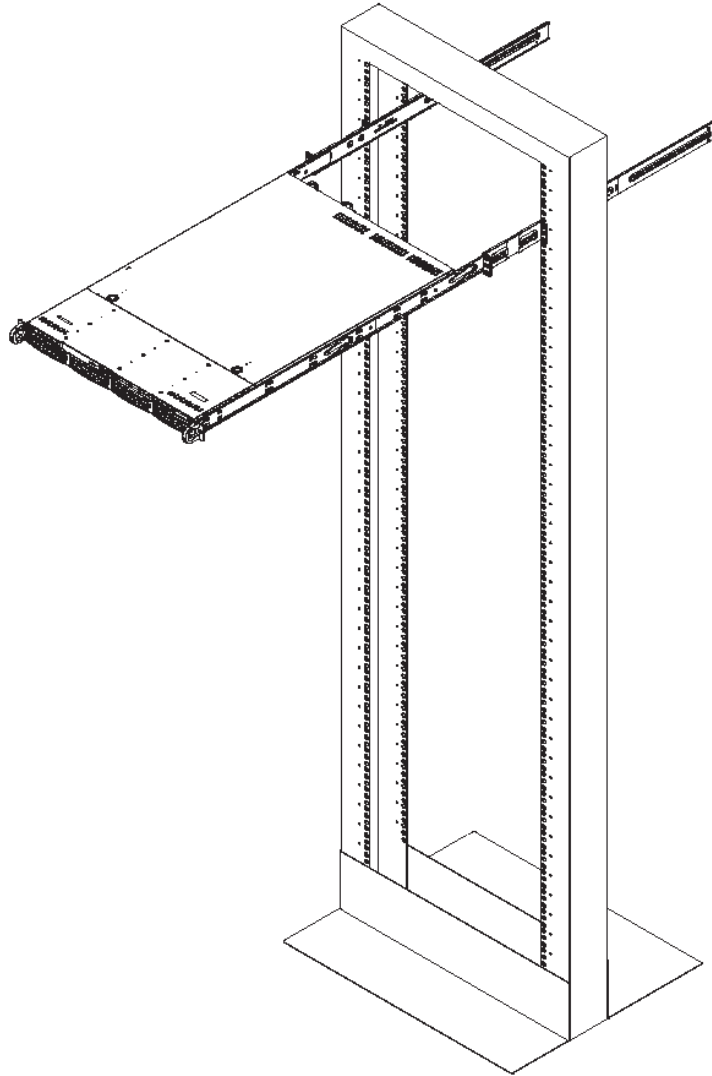
Rack Mount Instructions for SL Servers

Rack Setup Suggestions

- Determine the placement of each component in the rack before you install the rails.
- Install the heaviest server components on the bottom of the rack first, and then work up.

Install the Inner Slides

1. Locate the right inner slide, (the slide that will be used on the right side of chassis when facing the front panel of the chassis).

2. Align the four (4) square holes on the right inner slide against the hooks on the right side of the chassis as show below on the left.

3. Securely attach the slide to the chassis with two M4 flat head screws and repeat the steps 1-3 to install the left inner slide to the left side of the chassis.
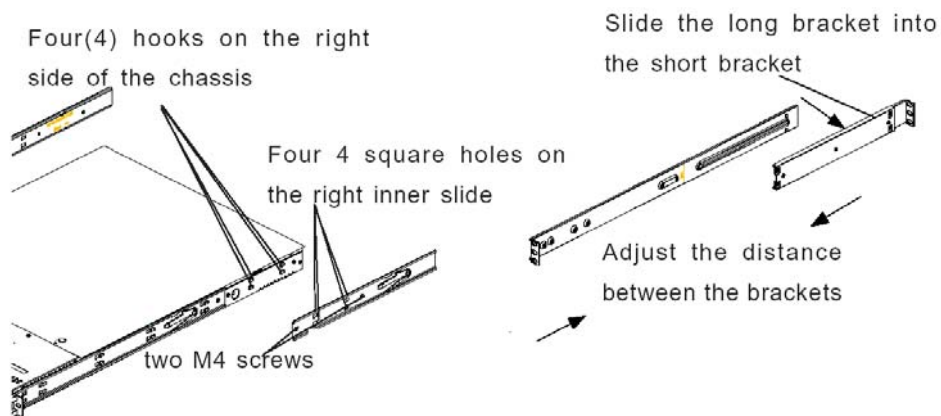
Install the Outer Slides

1. Measure the distance from the front rail of the rack to the rear rail of the rack.

2. Attach a short bracket to the rear side of the right outer slide, and a long bracket to the front side of the right outer slide as shown above on the right.

3. Adjust the short and long brackets to the proper distance so that the chassis can snugly fit into the rack.

4. Secure the slides to the cabinet with screws.

5. Repeat steps 1-4 for the left outer slide.

Install the Slide Assemblies to the Rack

1. After you have installed the short and long brackets to the outer slides, you are ready to install the whole slide assemblies (outer slides with short and long brackets attached) to the rack. (See the previous page.)

2. Use M5 screws and washers to secure the slide assemblies into the rack as shown below:
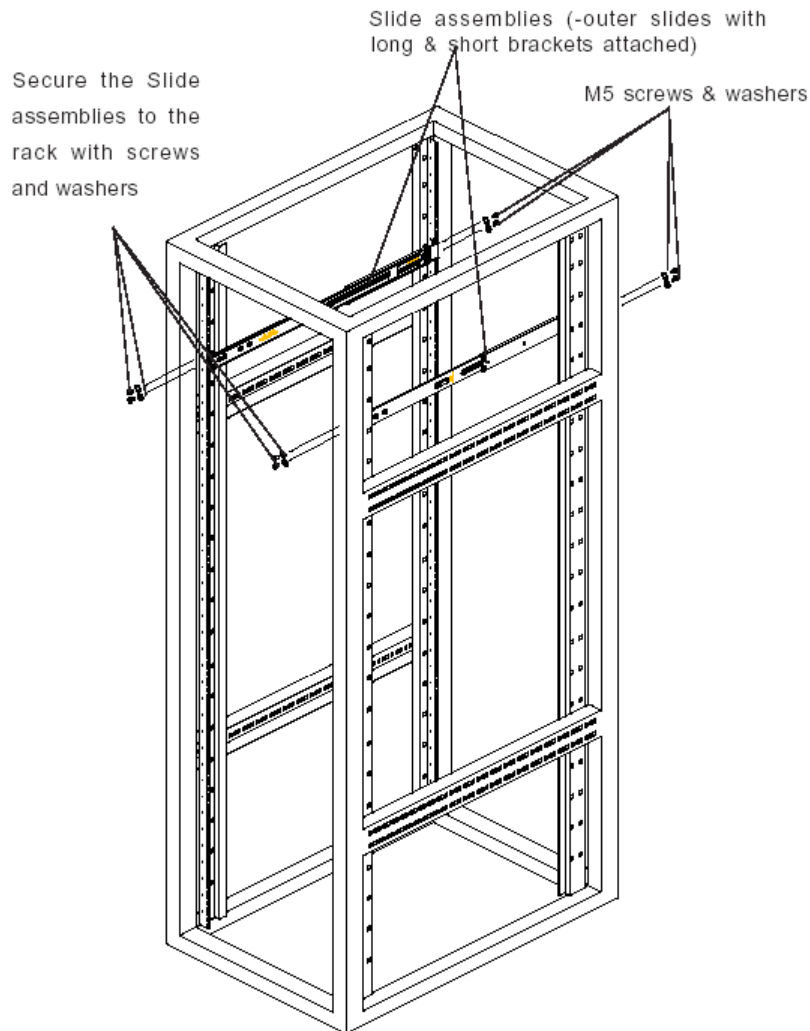
Install the Chassis into the Rack

1. Push the inner slides, which are attached to the chassis, into the grooves of the outer slide assemblies that are installed in the rack as shown below:
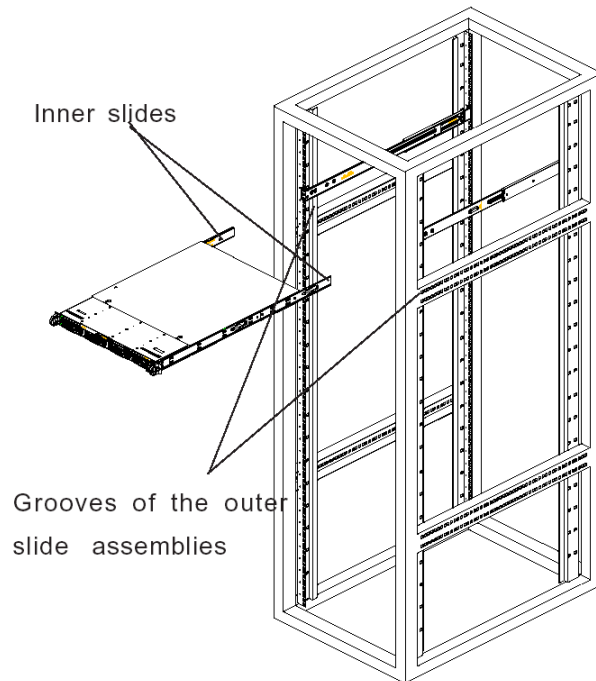
2. Push the chassis all the way to the back of the outer slide assemblies as shown below:
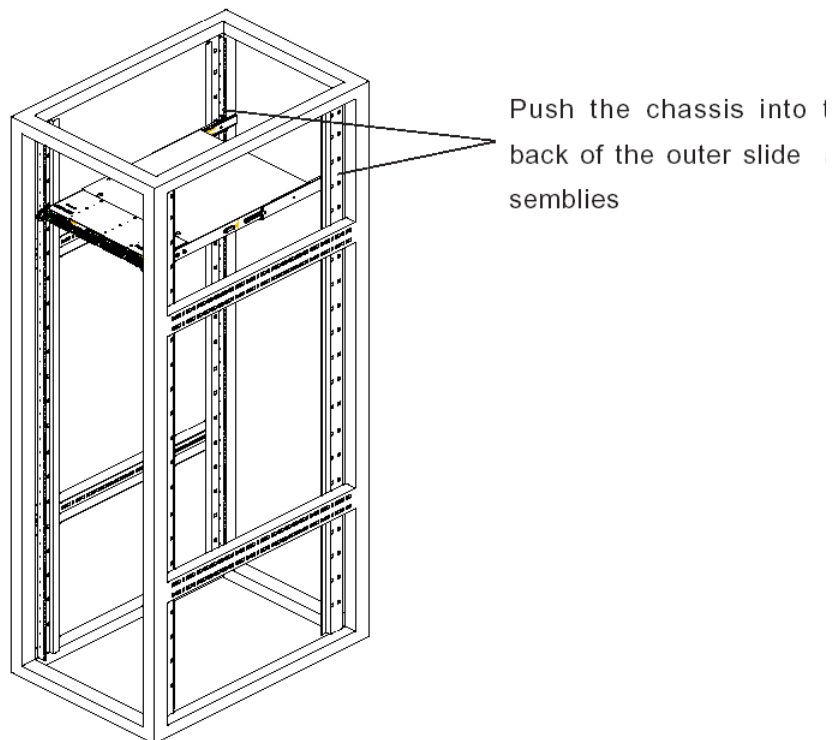
Rack Mount Instructions for MSA Servers

Optional: Install the Chassis Rails

NOTE: If your chassis does not come with chassis rails, please follow the procedure listed on the last page of this sub-section to install the unit directly into the rack.

CAUTION: Please make sure that the chassis covers and chassis rails are installed on the chassis before you install the chassis into the rack. To avoid personal injury and property damage, please carefully follow all the safety steps listed below:

Before installing the chassis rails:
- *Close the chassis using the chassis cover.*
- *Unplug the AC power cord(s).*
- *Remove all external devices and connectors.*

1. Included in the shipping package are a pair of rail assemblies. In each rail assembly, locate the inner rail and the outer rail.

2. Press the locking tab to release the inner rail from its locking position and pull out the inner rail from the rail assembly.

NOTE: The inner rails are to be attached to the chassis and the outer rails are to be installed in the rack.

Outer rail (to be installed in the rack)

Pull out the Inner rail (to be attached on the chassis)

Press the Locking Tab
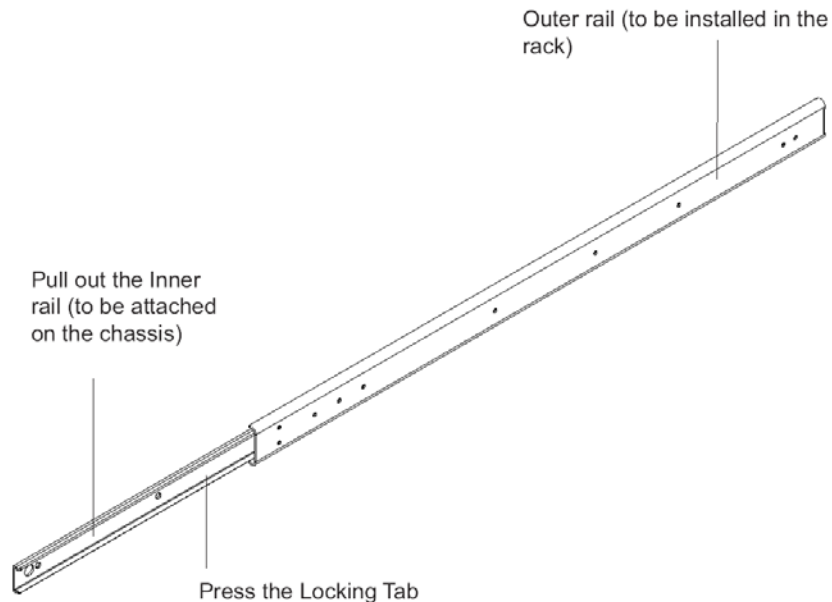
3. Locate the three holes on each side of the chassis and locate the three corre-
sponding holes on each of the inner rail.
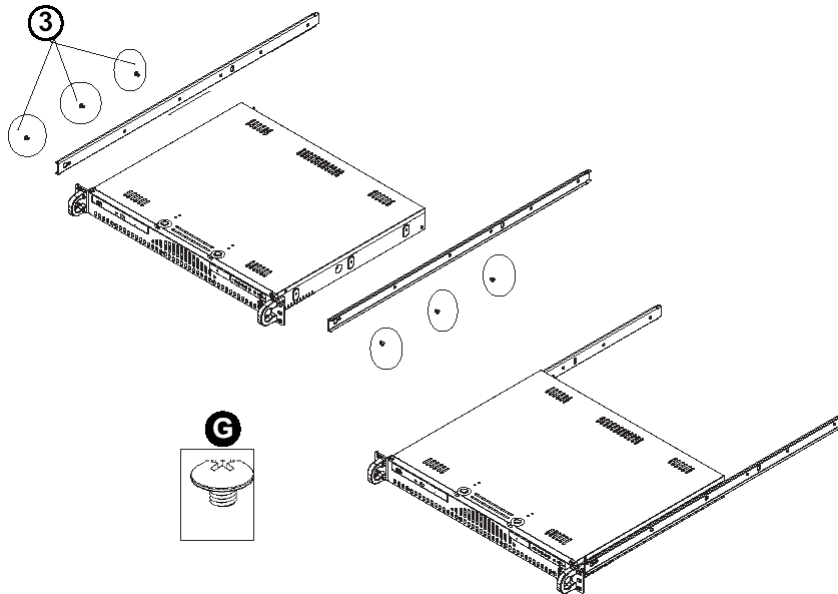
4. Attach an inner rail to each side of the chassis and secure the inner rail to the
chassis by inserting three Type G screws through the holes on each side of the
chassis and the inner rail. (See the diagram below for a description of the Type
G screw.)
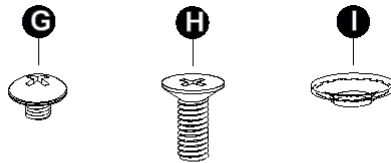
G. Round head M4 x 4 mm [0.157]

H. Flat head M5 x 12 mm [0.472]

I. Washer for M5

5. Repeat the above steps to install the other rail on the chassis.

Optional: Install the Traditional UP Racks

After you have installed the inner rails on the chassis, you are ready to install the outer rails of rail assemblies to the rack.

*NOTE: The rails are designed to fit in the racks with the depth of 28" to 33".*

- *Determine the placement of each component in the rack before you install the rails.*
- *Install the heaviest server components on the bottom of the rack first, and then work up.*

1. In the package, locate a pair of front (short) and rear (long) brackets. Please note that the brackets are marked with Up/Front Arrows (front) and Up/Rear arrows (rear).

2. Secure the front (short) bracket (marked with the Up/Front arrows) to the outer rail with two Type G screws. (See the previous page for a description of the Type G screw.)

3. Attach the rear (long) bracket to the other end of the outer rail and secure the rear (long) bracket to the outer rail with a Type G screw as shown below.

4. Measure the depth of your rack and adjust the length of the rails accordingly.

5. Repeat the same steps to install the other outer rail on the chassis.

6. Secure both outer rail assemblies to the rack with Type H screws and Type I washers. (See the previous page for descriptions of Type H and Type I hardware components.)
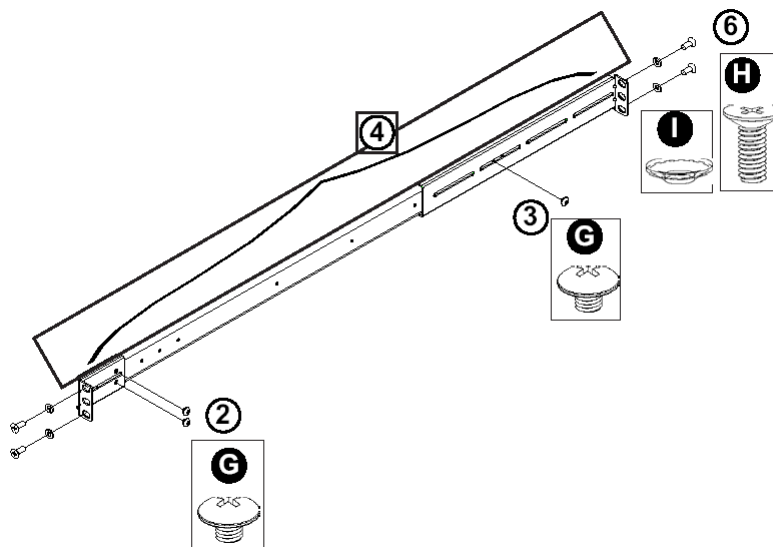
7. Slide the chassis into the rack as shown below.

NOTE: The chassis may not slide into the rack smoothly or easily when installed the first time. Some adjustment to the slide assemblies might be needed for easy installation.

8. You will need to release the safety taps on both sides of the chassis in order to completely remove the chassis out of the rack.
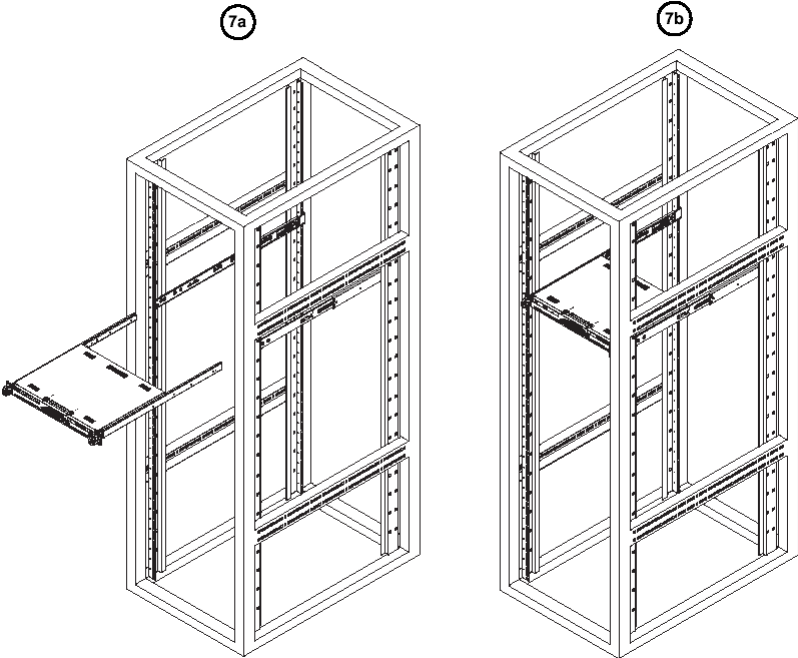
Optional: Install the Open Racks

After you have installed the inner rails on the chassis, you are ready to install the outer rails of rail assemblies to the rack.

NOTE: The rails are designed to fit in the racks with the depth of 28" to 33".

- *Determine the placement of each component in the rack before you install the rails.*
- *Install the heaviest server components on the bottom of the rack first, and then work up.*

1. In the package, locate a pair of front (short) and rear (long) brackets. Please note that the brackets are marked with Up/Front Arrows (front) and Up/Rear arrows (rear).

2. Secure the front (short) bracket (marked with the Up/Front arrows) to the outer rail with two Type G screws as shown below.
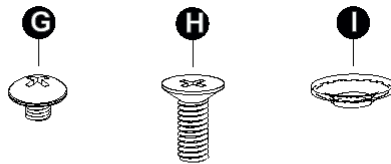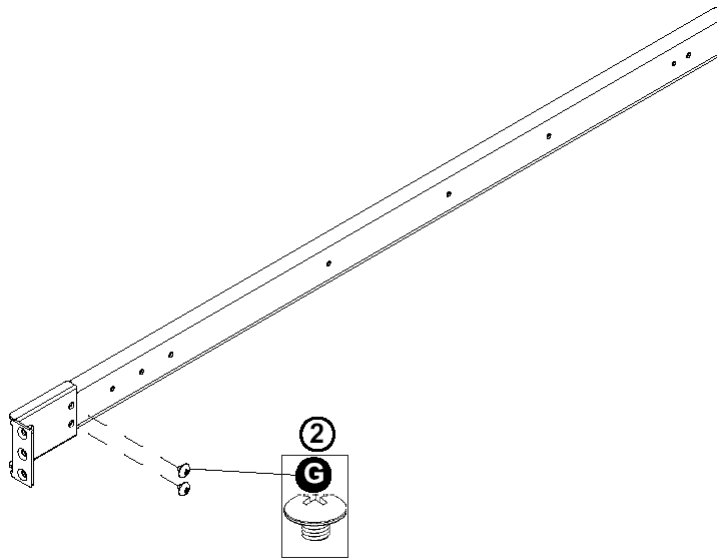
G.   Round head M4 x 4 mm [0.157]

H.   Flat head M5 x 12 mm [0.472]

I.   Washer for M5

3. Attach the front (short) bracket to the front end of the rack, and secure it to the rack with two Type H screws and Type I washers as shown below. (See the previous page for descriptions of Type H and Type I hardware components.)

4. Attach the rear (long) bracket to the rear end of the rack, and secure it to the rack with two Type H screws and Type I washers as shown below. Repeat the same steps to install the other outer rail to the other side of rack.
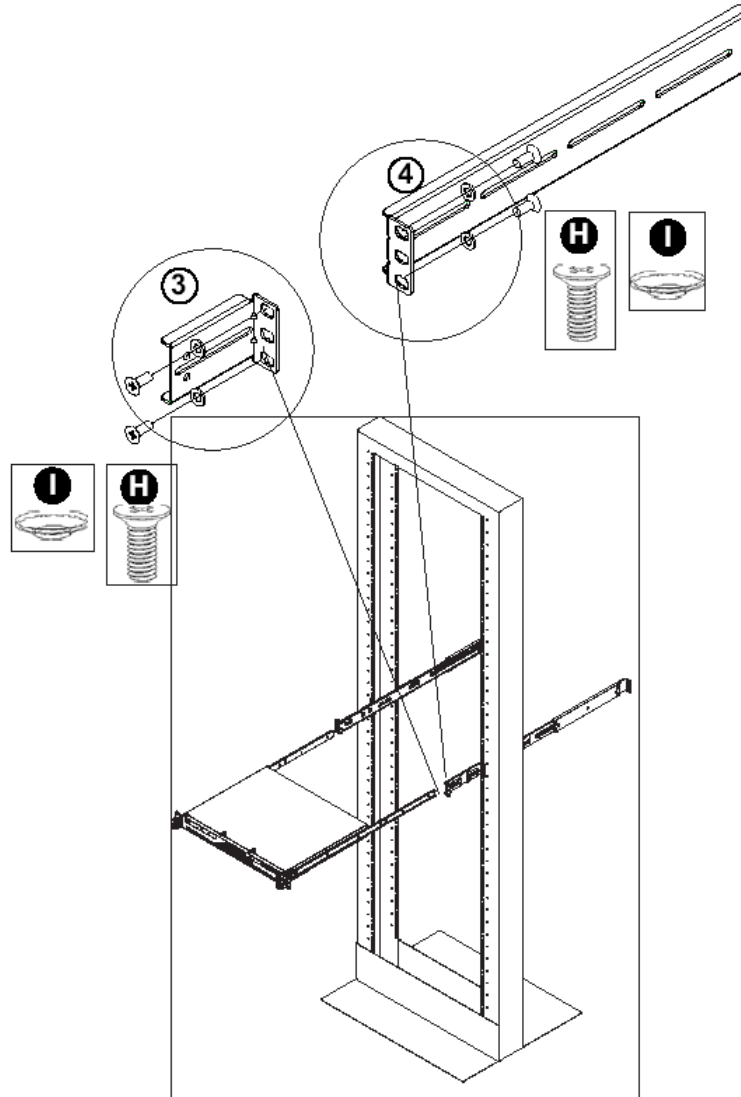
5. Measure the depth of your rack and adjust the length of the rails accordingly. Then, secure the rails to the chassis with Type G screws.

6. Slide the inner rails which are attached to the chassis into the outer rails on the rack.
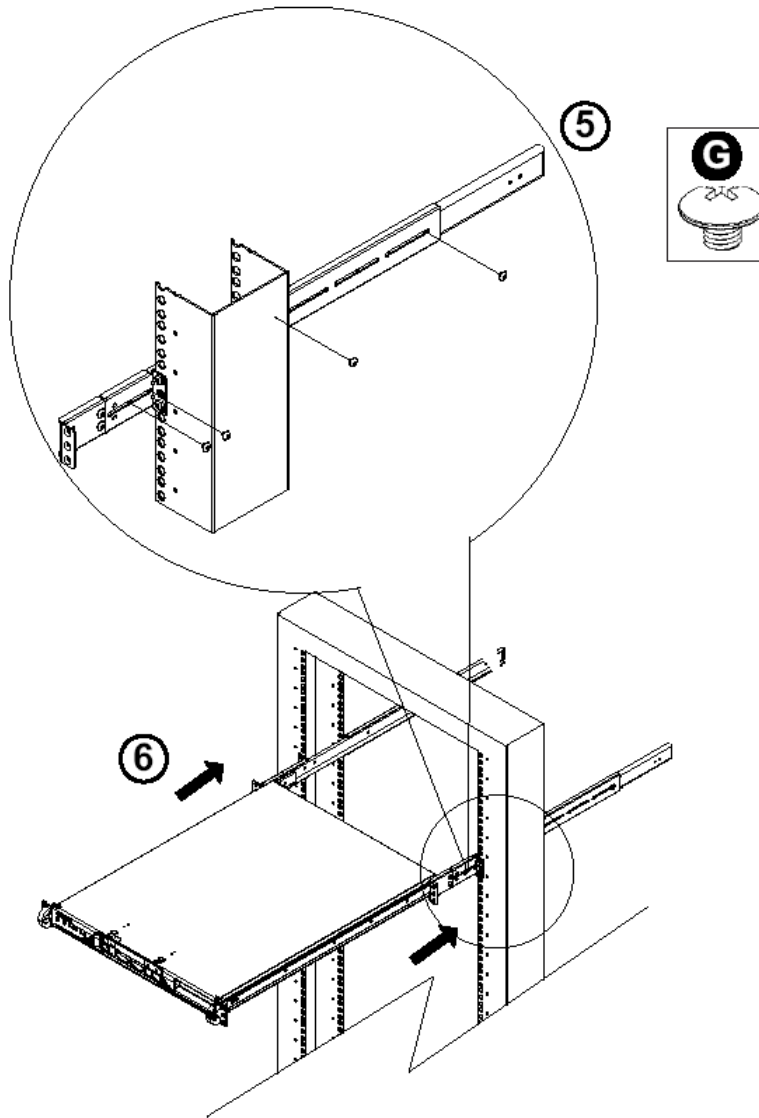
Install the Chassis into the Rack

CAUTION: Before installing the chassis into the rack:

- *Make sure that the rack is securely anchored onto an unmovable surface or structure before installing the chassis into the rack.*
- *Unplug power cord(s) of the rack before installing the chassis into the rack.*
- *Make sure that the system is adequately supported. Make sure that all the components are securely fastened to the chassis to prevent components falling off from the chassis.*
- *The rack assembly should be properly grounded to avoid electric shock.*
- *The rack assembly must provide sufficient airflow to the chassis for proper cooling.*
- *Please make sure that all components and all chassis covers are properly installed in the chassis before you install the chassis into the racks; otherwise, out-of-warranty damage may occur.*

Slide the chassis into the rack and secure it with two screws on each side of the rack as shown in the picture.

slide into
rack and
secure with
two screws
on each
side
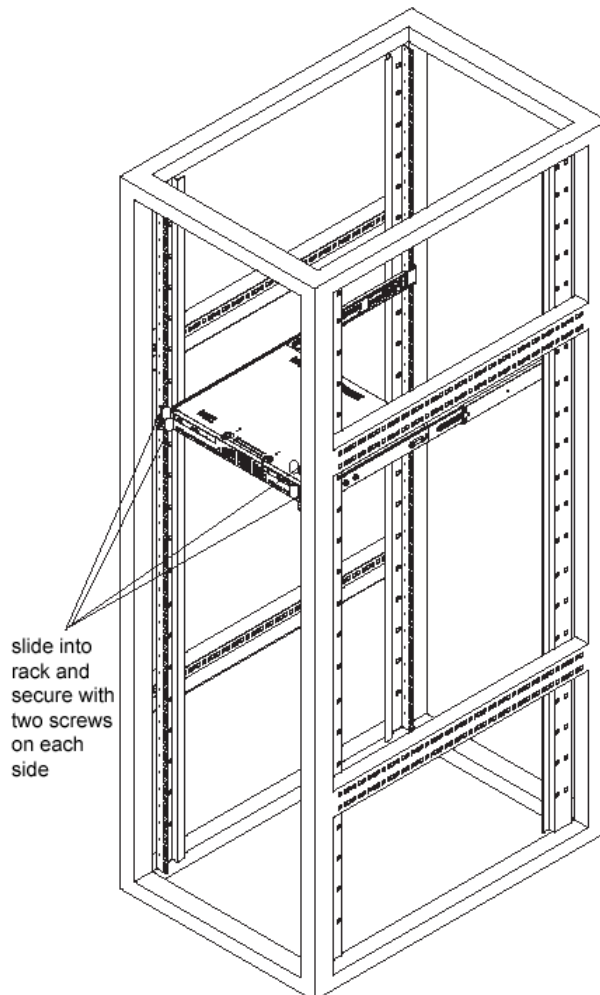
Install the SL or HL Server Bezel

After rack mounting an SL or HL server, the bezel should be installed on the front end of the chassis.

NOTE: *This portion of the installation process requires you to unpack the bezel. The bezel has been packaged separately from the unit to prevent damage during shipping.*

A. Hold the bezel upright and facing towards you (Fig. 1).

Fig. 1 - Front of bezel

B. Note that each end of the bezel contains two raised bumps (Fig. 2).

Fig. 2 - Bumps on right end of bezel

Fig. 3 - Grooves in right U-shaped handle

C. Align these bumps along the two parallel grooves inside each U-shaped aluminum chassis handle affixed to the front end of the chassis rail (Fig. 3).

D. Push the bezel towards the front of the chassis, inserting the USB B-type plug on the back of the bezel (Fig. 4) into the USB port on the chassis.

Fig. 4 - Section of back of bezel with USB B-type plug

Check the Power Supply

This server is equipped with a universal power supply that handles 100-240 V, 50/60 Hz. A standard power cord interface (IEC 950) facilitates power plugs that are suitable for most European, North American, and Pacific Rim countries.

Power Supply Precautions

⚠ *WARNING*:

• Use a regulating uninterruptible power supply (UPS) to protect the server from power surges, voltage spikes and to keep the server operating in case of a power failure.

• In geographic regions that are susceptible to electrical storms, M86 Security highly recommends plugging the AC power cord for the server into a surge suppressor.

• Use appropriately rated extension cords or power strips only.

• Allow power supply units to cool before touching them.

General Safety Information

Server Operation and Maintenance Precautions

⚠ **WARNING:**

Observe the following safety precautions during server operation and maintenance:

⚠ *WARNING: If the server is used in a manner not specified by the manufacturer, the protection provided by the server may be impaired.*

⚠ *WARNING: M86 Security is not responsible for regulatory compliance of any server that has been modified. Altering the server's enclosure in any way other than the installation operations specified in this document may invalidate the server's safety certifications.*

☠ *CAUTION: Never pile books, papers, or other objects on the chassis, drop it, or subject it to pressure in any other way. The internal circuits can be damaged, and the battery may be crushed or punctured. Besides irreparable damage to the unit, the result could be dangerous heat and even fire.*

☠ *CAUTION: There are no user-serviceable components inside the chassis. The chassis should only be opened by qualified service personnel. Never disassemble, tamper with, or attempt to repair the server. Doing so may cause smoke, fire, electrical shock, serious physical injury, or death.*

⚠ *WARNING: In HL servers, multiple sources of supply exist. Be sure to disconnect all sources before servicing.*

- Do not insert objects through openings in the chassis. Doing so could result in a short circuit that might cause a fire or an electrical shock.

- Do not operate the server in an explosive atmosphere, in the presence of flammable gases.

- To ensure proper cooling, always operate the server with its covers in place. Do not block any openings on the chassis. Do not place the server near a heater.

- Always exit the software application properly before turning off the server to ensure data integrity.

- Do not expose the server to rain or use near water. If liquids of any kind should leak into the chassis, power down the server, unplug it, and contact M86 Security technical support.

- Disconnect power from the server before cleaning the unit. Do not use liquid or aerosol cleaners.

AC Power Cord and Cable Precautions

⚠ **WARNING**:

- The AC power cord for the server must be plugged into a grounded, power outlet.

- Do not modify or use a supplied AC power cord if it is not the exact type required in the region where the server will be installed and used. Replace the cord with the correct type.

- Route the AC power cord and cables away from moving parts and foot traffic.

- Do not allow anything to rest on the AC power cord and cables.

- Never use the server if the AC power cord has been damaged.

- Always unplug the AC power cord before removing the unit for servicing.

Electrical Safety Precautions

⚠ **WARNING:**

Heed the following safety precautions to protect yourself from harm and the server from damage:

☢ **CAUTION**: *Dangerous voltages associated with the 100-240 V AC power supply are present inside the unit. To avoid injury or electrical shock, do not touch exposed connections or components while the power is on.*

- To prevent damage to the server, read the information in this document for selection of the proper input voltage.

- Do not wear rings or wristwatches when troubleshooting electrical circuits.

- To avoid fire hazard, use only the specified fuse(s) with the correct type number, voltage, and current ratings. Only qualified service personnel should replace fuses.

- Qualified service personnel should be properly grounded when servicing the unit.

- Qualified service personnel should perform a safety check after any service is performed.

Motherboard Battery Precautions

CAUTION:

The battery on the motherboard should not be replaced without following instructions provided by the manufacturer. Only qualified service personnel should replace batteries.

The battery contains energy and, as with all batteries, a malfunction can cause heat, smoke, or fire, release toxic materials, or cause burns. Do not disassemble, puncture, drop, crush, bend, deform, submerge or modify the battery. Do not incinerate or expose to heat above 140°F (60°C).

There is a danger of explosion if the battery on the motherboard is installed upside down, which will reverse its polarities.

CAUTION: DANGER OF EXPLOSION IF BATTERY IS INCORRECTLY REPLACED. REPLACE ONLY WITH THE SAME OR EQUIVALENT TYPE RECOMMENDED BY THE MANUFACTURER. DISPOSE OF THE USED BATTERIES ACCORDING TO THE MANUFACTURER'S INSTRUCTIONS.

ATTENTION: IL Y A DANGER D'EXPLOSION S'IL Y A REPLACEMENT INCORRECT DE LA BATTERIE, REMPLACER UNIQUEMENT AVEC UNE BATTERIE DU MÊME TYPE OU D'UN TYPE ÉQUIVALENT RECOMMANDÉ PAR LE CONSTRUCTEUR. METTRE AU REBUT LES BATTERIES USAGÉES CONFORMÊMENT AUX INSTRUCTIONS DU FABRICANT.

WARNING: Users in Member States should consult Article 20 of Directive 2006/66/EC of the European Parliament and of the Council before disposing the motherboard battery.

INSTALL THE SERVER

Step 1: Setup Procedures

This step requires you to link the workstation to the HL, SL, or MSA server. You have the option of using the text-based Quick Start setup procedures described in Step 1A, the Administrator console setup procedures described in the Appendix, or, if you have an SL or HL unit, the LCD panel setup procedures described in Step 1B.

NOTE: See the Appendix for instructions on using a crossover cable to install the Web Filter on the network.

Quick Start Setup Requirements

The following hardware can be used for the Quick Start setup procedures:

- HL, SL, or MSA with AC power cord(s)
- either one of two options:
  - PC monitor with AC power cord and keyboard, or
  - PC laptop computer with HyperTerminal and serial port cable (and USB DB9 serial adapter, if there is no serial port on your laptop)

Go to Step 1A to execute Quick Start Setup Procedures.

NOTE: If using a Windows Vista or Windows 7 laptop, please be sure HyperTerminal or an equivalent terminal emulator program is installed on your machine. See the note under HyperTerminal Setup Procedures if selecting this option.

LCD Panel Setup Requirements (for SL and HL Units)

The following hardware is required for LCD panel setup procedures, if using an HL or SL unit:

- HL or SL with AC power cord(s)
- Bezel with LCD panel mounted on chassis front

Go to Step 1B to execute LCD Panel Setup Procedures.

Step 1A: Quick Start Setup Procedures

Link the Workstation to the HL, SL, or MSA

Monitor and Keyboard Setup

A. Connect the PC monitor and keyboard cables to the rear of the chassis (see Fig. 1 for an SL or MSA unit, and Fig. 2 for an HL unit).

B. Turn on the PC monitor.

C. Connect the AC power cord(s) to the back of the chassis and plug the cord(s) into a UPS power supply unit.

D. Power on the server by dropping down the face plate and pressing the large button at the right of the front panel (see Fig. 3 for an SL unit, Fig. 4 for an MSA unit, and Fig. 5 for an HL unit).

Once the server is powered up, proceed to the Login screen instructions.

Serial Console Setup

A. Using the serial port cable (and USB DB9 serial adapter, if necessary), connect the laptop to the rear of the chassis (see Fig. 1 for an SL or MSA unit, and Fig. 2 for an HL unit).

B. Power on the laptop.

C. Connect the AC power cord(s) to the back of the chassis and plug the cord(s) into a UPS power supply unit.

D. Power on the server by dropping down the face plate and pressing the large button at the right of the front panel (see Fig. 3 for an SL unit, Fig. 4 for an MSA unit, and Fig. 5 for an HL unit).

Fig. 1 - Portion of SL and MSA chassis rear
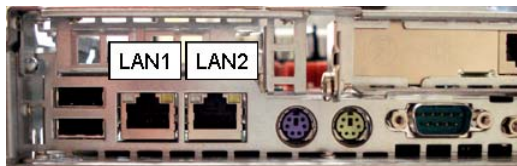
Fig. 2 - Portion of HL chassis rear
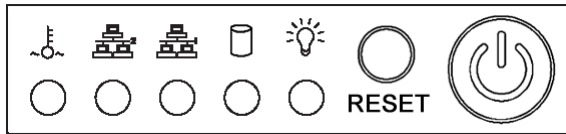
Fig. 3 - Diagram of SL chassis front panel, power button at far right
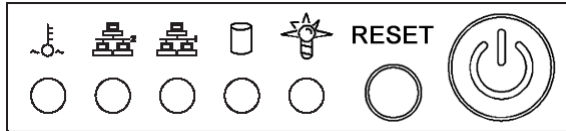
Fig. 4 - Diagram of MSA chassis front panel, power button at far right

Button   LED
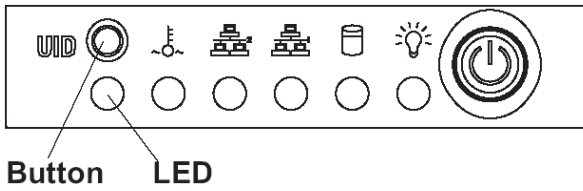
Fig. 5 - Diagram of HL chassis front panel, power button at far right

Once the server is powered up, proceed to the instructions for HyperTerminal Setup Procedures.

HyperTerminal Setup Procedures

If using a serial console, follow these procedures on a Windows XP machine to create a HyperTerminal session.

NOTE: HyperTerminal is no longer included with Windows as of Microsoft's Vista system. Please note on Microsoft's Web page "What happened to HyperTerminal?" at http://windows.microsoft.com/en-us/windows-vista/What-happened-to-HyperTerminal (accessed May 22, 2012), Microsoft states: "HyperTerminal is no longer part of Windows.... If you previously used HyperTerminal to control serial devices, you can usually find a downloadable version of HyperTerminal on the Internet that is free for personal use."

If you are using a Windows Vista or Windows 7 machine to conduct these quick start setup procedures and do not have an equivalent type of terminal emulator program installed on your workstation, Hilgraeve, Inc., the maker of HyperTerminal, offers HyperTerminal Private Edition for Windows Vista and Windows 7. The following information is included on Hilgraeve's Web page at http://www.hilgraeve.com/hyperterminal.html (accessed May 22, 2012): "HyperTerminal Private Edition is an award winning terminal emulation program capable of connecting to systems through TCP/IP Networks, Dial-Up Modems, and COM ports.... Download HyperTerminal free 30 day trial."

If you have a terminal emulator program other than HyperTerminal or a derivative of HyperTerminal installed on your workstation, please specify these session settings:

- *9600 bits per second*
- *8 data bits*
- *no parity*
- *1 stop bit*
- *hardware flow control*
- *VT100 emulation settings*

On the Windows XP machine:

A. Launch HyperTerminal by going to Start > Programs > Accessories > Communications > HyperTerminal:
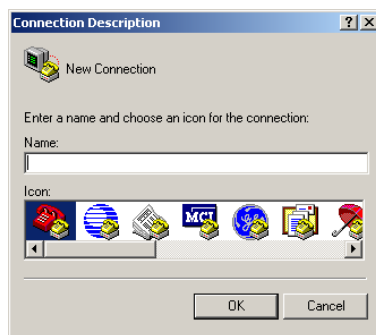
B. In the Connection Description dialog box, enter any session **Name**, and then click **OK** to open the Connect To dialog box:
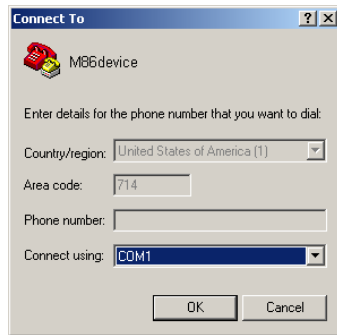
C. At the **Connect using** field, select the COM port assigned to the serial port on the laptop (probably "COM1"), and then click **OK** to open the Properties dialog box, displaying the Port Settings tab:
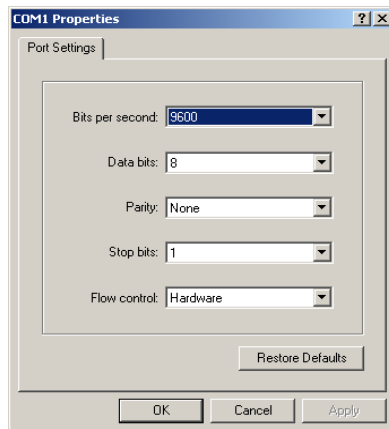
D. Specify the following session settings:

- Bits per second: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: Hardware
- VT100 emulation settings

E. Click **OK** to connect to the HyperTerminal session:
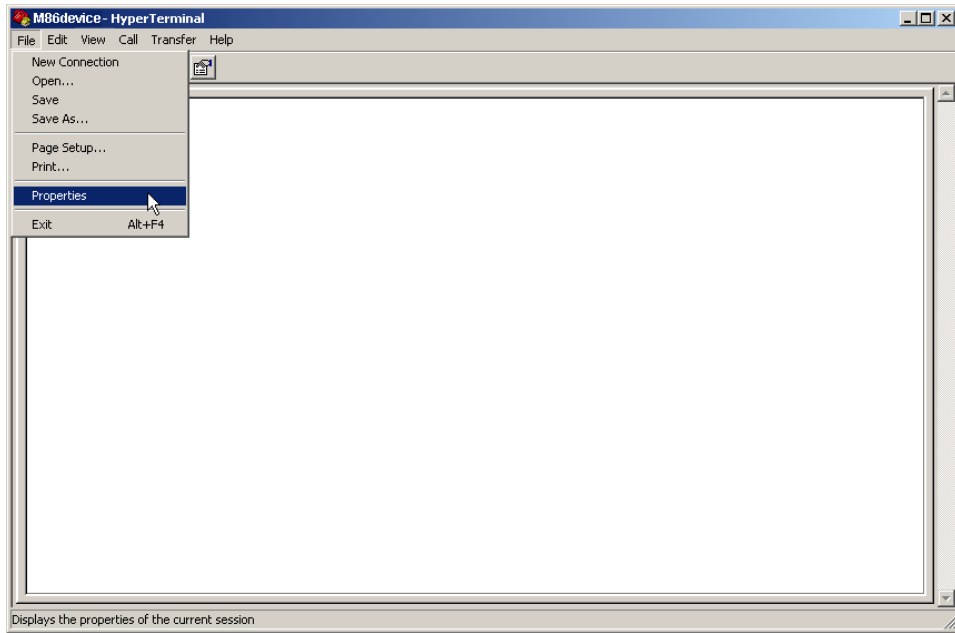
F. In the HyperTerminal session window, go to File > Properties to open the Properties dialog box, displaying the Connect To and Settings tabs:
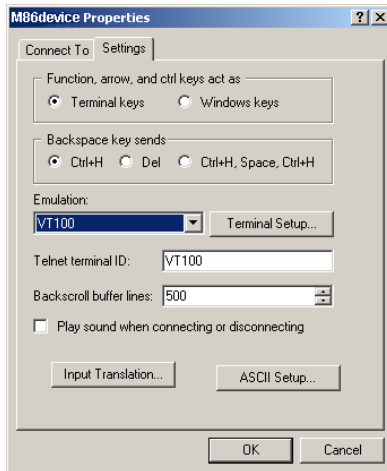
G. Click the Settings tab, and at the **Emulation** menu select "VT100".

H. Click **OK** to close the dialog box, and to go to the login screen.

Login screen

The login screen displays after powering on the server, or creating a HyperTerminal session.
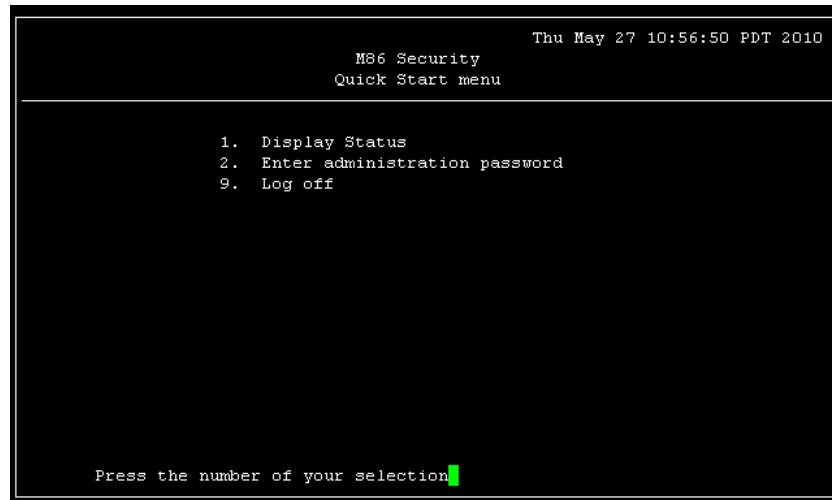
NOTES: *If using a HyperTerminal session, the login screen will display with black text on a white background.*

*If the screensaver currently displays on your screen, press the **Enter** key to display the login screen.*

A. At the **login** prompt, type in **menu**.

B. Press the **Enter** key to display the Password prompt.

C. At the **Password** prompt, type in the following: **#s3tup#r3k**

D. Press **Enter** to display the Quick Start menu screen.

Quick Start menu screen

```
                                      Thu May 27 10:56:50 PDT 2010
                            M86 Security
                            Quick Start menu
    ─────────────────────────────────────────────────────────────────

            1.   Display Status
            2.   Enter administration password
            9.   Log off

        Press the number of your selection
```

A. At the **Press the number of your selection** prompt, press **2** to select the Quick Start setup process.

B. At the login prompt, re-enter your password: **#s3tup#r3k**

C. Press **Enter** to display the administration menu where you can begin using the Quick Start setup procedures.

Quick Start menu: administration menu

```
                                    Thu May 27 11:00:26 PDT 2010
                        M86 Security
                        Quick Start menu

            1.  Display Status
            2.  Quick Start setup
            3.  Change filtering mode
            4.  Configure network interface LAN1
            5.  Configure network interface LAN2
            6.  Configure default gateway
            7.  Configure DNS servers
            8.  Configure host name
            9.  Time Zone regional setting
            A.  Reset system to factory defaults
            B.  Reboot system
            C.  Change Quick Start password
            D.  Reset admin console account
            X.  Exit administration menu


    Press the number of your selection
```

A. At the **Press the number of your selection** prompt, press **2** to select the "Quick Start Setup" process.

The Quick Start menu takes you to the following configuration screens to make entries:

- Change filtering mode
- Configure network interface LAN1
- Configure network interface LAN2
- Configure default gateway
- Configure DNS servers
- Configure host name
- Time Zone regional setting

B. After making all entries using the Quick Start setup procedures, press **X** to return to the Quick Start menu screen. Or, to verify the status of the Web Filter and review the entries you made using the Quick Start setup, press **1** to view the System Status screen.

NOTES: *To configure an individual screen from the Quick Start menu, press the number or alphabet corresponding to that menu option, as described in the following sub-sections. Option A, "Reset system to factory defaults", should only be used by an M86 Security technical representative.*

Change filtering mode

A. From the Quick Start menu, press **3** to go to the Filter mode configuration screen.

B. Select a filter mode (Invisible, Router, or Firewall) using up-arrow and down-arrow keys. Press **Y** when you have selected the appropriate mode, or press **Esc** to cancel this change.

Configure network interface LAN1

A. From the Quick Start menu, press **4** to go to the Configure Network Interface screen for LAN1.

B. At the **Enter interface LAN1 IP address** prompt, type in the LAN1 IP address and press **Enter**.

C. At the **Enter interface LAN1 netmask** prompt, type in the netmask for the LAN1 IP address and press **Enter**.

D. Press **Y** to confirm, or press any other key to cancel this change.

Configure network interface LAN2

A. From the Quick Start menu, press **5** to go to the Configure Network Interface screen for LAN2.

B. At the **Enter interface LAN2 IP address** prompt, type in the LAN2 IP address and press **Enter**.

C. At the **Enter interface LAN2 netmask** prompt, type in the netmask for the LAN2 IP address and press **Enter**.

D. Press **Y** to confirm, or press any other key to cancel this change.

Configure default gateway

A. From the Quick Start menu, press **6** to go to the Configure default gateway screen.

B. At the **Enter default gateway IP** prompt, type in the gateway IP address and press **Enter**.

C. Press **Y** to confirm, or press any other key to cancel this change.

Configure DNS servers

A. From the Quick Start menu, press **7** to go to the Configure Domain Name Servers screen.

B. At the **Enter first DNS server IP** prompt, type in the IP address of the DNS server to use and press **Enter**.

C. At the **Enter (optional) second DNS server IP** prompt, either type in the IP address of an alternate DNS server to use and press **Enter**, or just press **Enter** to bypass making a second DNS server entry.

Configure host name

A. From the Quick Start menu, press **8** to go to the Configure host name screen.

B. At the **Enter host name** prompt, type in the host name and press **Enter**.

C. Press **Y** to confirm, or press any other key to cancel this change.

Time Zone regional setting

A. From the Quick Start menu, press **9** to go to the Time Zone regional configuration screen.

B. Select a region using up-arrow and down-arrow. Press **Y** when you have selected the appropriate region, or Press **Esc** to cancel this change.

NOTE: If this server is located in the USA, please select "US" and not "America".

C. After you select the region, you may be prompted to select the locality within the selected region. Select the locality and press **Y** to confirm, or press **Esc** to cancel the change.

Non-Quick Start procedures or settings

The options described below do not pertain to the quick start setup process.

Reset system to factory defaults

A. From the Quick Start menu, press **A** to go to the Reset confirmation screen.

B. At the **Press Y to continue** prompt, press **Y** to continue, or press any other key to cancel the reset process.

⚠️ *WARNING: This option will delete all configuration settings and profiles stored on the server, and revert the server back to the original software version on the hard drive. Any software updates applied since the original version on the hard drive will need to be downloaded and re-applied.*

Reboot system

A. From the Quick Start menu, press **B** to go to the Reboot confirmation screen.

B. At the **Really reboot the system?** prompt, press **Y** to continue, or press any other key to cancel reboot.

Change Quick Start password

A. From the Quick Start menu, press **C** to go to the Change Administrator Password screen.

📝 *NOTE: This option will change the password used for accessing the Quick Start menu (the default password being **#s3tup#r3k**) but will not change the password used for accessing the Web Filter login screen. Option D, "Reset Admin account", should be used for resetting the Web Filter Administrator console username and password to the factory default 'admin'/'user3' and for unlocking all IP addresses currently locked.*

B. At the **Enter the new administrator password** prompt, type in the new password to be used for accessing the Quick Start menu and press **Enter**.

C. At the **Re-enter the new administrator password** prompt, re-type the password you just entered and press **Enter**, or press **Esc** to cancel the change.

Reset admin console account

A. From the Quick Start menu, press **D** to go to the Reset admin GUI account confirmation screen that displays the following message:

Reset admin account password? Are you sure?
NOTE: This process will also unlock the admin account and unlock all currently locked IPs.

📝 *NOTE: This option resets the Web Filter Administrator console username and password to the factory default 'admin'/'user3' and will unlock all IP addresses currently locked.*

B. Press **Y** to continue, or press any other key to cancel admin account reset.

System Status screen

```
                                     Thu May 27 11:13:06 PDT 2010
                               M86 Security
                      System Status - updates every 10 seconds


          Serial Number   13WFB1102312
          Web Filter is configured in Invisible mode
          lan1 is the Management and Blocking Interface
          lan1 IP = 192.168.10.120 Mask = 255.255.0.0          Active
          lan2 is the Capturing Interface
          lan2 IP = 192.168.10.111 Mask = 255.255.0.0          Active
          Default gateway IP: 192.168.10.1
          Web Filter host name: WF20201.qc.logo.com

          DNS server IP address(es):  192.168.10.1 192.168.168.200
          Regional timezone setting: US/Pacific

          Web Filter processing is normal
          Current Version: Web Filter 4.2.00.3
          Library was last updated on 2011/05/27


         -Press any key to return to menu...
```

The System Status screen contains the following information:

- **Serial Number** assigned to the chassis
- **Operation Mode** for the Web FIlter specified in screen 3 (Change filtering mode)
- **Capturing Interface** specified in screen 4 or 5 (Configure network interface LAN1 or LAN2)
- **Management and Blocking Interface** specified in screen 4 or 5 (Configure network interface LAN1 or LAN2)
- **lan1 IP** address and netmask specified in screen 4, and current status ("Active" or "Inactive")
- **lan2 IP** address and netmask specified in screen 5, and current status ("Active" or "Inactive")
- **Default gateway** IP address specified in screen 6 (Configure default gateway)
- **Web Filter host name** specified in screen 8 (Configure host name)
- **DNS server IP address(es)** specified in screen 7 (Configure DNS servers)
- **Regional timezone setting** specified in screen 9 (Time Zone regional setting)
- Current status of the Web Filte
- Current Web Filter software **Version** installed
- Library update status

NOTE: *Modifications can be made at any time by returning to the specific screen of the Quick Start procedures.*

Log Off, Disconnect the Peripherals

A. After completing the Quick Start setup procedures, return to the Quick Start menu screen and press **9** to log out.

B. Disconnect the peripherals from the server.

Proceed to Step 2: Physically Connect the Unit to the Network.

Step 1B: LCD Panel Setup Procedures

A. Connect the AC power cord(s) to the back of the chassis and plug the cord(s) into a UPS power supply unit.

B. Power on the server by dropping down the face plate and pressing the large button at the right of the front panel.

On an SL or HL unit, the Web Filter can be configured using the LCD panel on front of the chassis bezel. When the bezel is placed on the front of the chassis, with the USB plug inserted into the USB port, the default LCD screen displays.

To the right of the LCD screen, the keypad displays, consisting of the following keys: up arrow, down arrow, left arrow, right arrow, checkmark, and "X".

M86 Menu

Press the "X" key to display the M86 Menu. In the LCD panel, an arrow displays to the left of the currently selected menu item. Use the up or down arrow keys to navigate the menu. After making your menu selection, press the checkmark key to accept your selection.

NOTE: On the M86 Menu, press "X" to toggle the display between the main menu and the following information: "Web Filter (software version number)", "Filtering Status (Active, Inactive)", and "Last Library Update: MMDD/YYYY".

Main Menu

When the main menu entry is selected, the following menu items display:

- WF Patch Level >
- Serial Number >
- WF Filter Mode > *
- IP / LAN1 > *
- IP / LAN2 > *
- Gateway > *
- DNS 1 > *
- DNS 2 > *
- Host Name > *
- Regional Setting (Time Zone, date, time) *
- Reset WF Admin Console Password
- Reboot >
- Shutdown >

*NOTES: When using the M86 menu to execute quick start setup procedures, be sure to configure all menu items marked in the list above with an asterisk (*).*

TIPS: Navigation tips in the M86 menu:
- *Use the up / down arrow key to scroll up / down the menu*
- *Press the checkmark key to choose the current selection*
- *Press the "X" to go back to the previous screen*

Make a selection from the menu, and press the checkmark key to go to that screen.

After making all settings in the required menu items, proceed to Step 2: Physically Connect the Unit to the Network.

WF Filter Mode

When the WF Filter Mode option is selected, the WF Filter Mode screen displays.

A. At the **Mode** field, use the left / right arrow keys to view and choose from the available options: Invisible, Router, Firewall.

B. Press the checkmark key to go to the Save Changes screen.

C. On the Save Changes screen:

- Choose **Yes** to accept your changes and to return to the main menu.
- Choose **No** to return to the Mode field.

IP / LAN1 and LAN2

When the IP / LAN 1 (LAN 2) option is selected, the IP / LAN 1 (LAN 2) screen displays with the following menu items:

- Configure LAN 1 (2) IP
- Change LAN1 (2) Netmask

A. Choose **Configure LAN 1 (2) IP** and press the checkmark key to go to the Configure LAN 1 (2) IP screen.

B. Use the up / down keys to increase / decrease the current value, and the left / right arrow keys to navigate across the line.

C. Press the checkmark key to accept your entry and to return to the previous screen.

D. Choose **Change LAN1 (2) Netmask** and press the checkmark key to go to the Change LAN1 (2) Netmask screen.

E. Use the up / down keys to increase / decrease the current value, and the left / right arrow keys to navigate across the line.

F. Press the checkmark key to accept your entry and to return to the previous screen.

G. Press the "X" key to return to the main menu.

Gateway

When the Gateway option is selected, the Gateway screen displays with the Configure Gateway IP menu item.

A. Choose **Configure Gateway IP** and press the checkmark key to go to the Configure Gateway IP screen.

B. Use the up / down keys to increase / decrease the current value, and the left / right arrow keys to navigate across the line.

C. Press the checkmark key to accept your entry and to return to the previous screen.

D. Press the "X" key to return to the main menu.

DNS 1 and 2

When the DNS 1 (2) option is selected, the DNS 1 (2) screen displays with the Configure DNS IP 1 (2) menu item.

A. Choose **Configure DNS IP 1 (2)** and press the checkmark key to go to the Configure DNS IP 1 (2) screen.

B. Use the up / down keys to increase / decrease the current value, and the left / right arrow keys to navigate across the line.

C. Press the checkmark key to accept your entry and to return to the previous screen.

D. Press the "X" key to return to the main menu.

Host Name

When the Host Name option is selected, the Host Name screen displays with the Configure Hostname menu item.

A. Choose **Configure Hostname** and press the checkmark key to go to the Configure Hostname screen.

B. Use the arrow keys to navigate the menu. Press the right arrow key to view the alphabets in first uppercase and then lowercase, numbers from 0-9, and lastly the symbol characters.

NOTES:

Entry tips:
* *The entry made in this field should not include any spaces, and can only include alphanumeric characters and the following symbols: underscore (_), dash (-), and period (.).*

Navigation tips:
* *If the down arrow key is pressed first—instead of the right arrow key—the symbol characters display first.*
* *Press the "X" key to remove a character and move the cursor to the first position in the line.*

C. Press the checkmark key to return to the previous screen.

D. Press the "X" key to return to the main menu.

Regional Setting (Time Zone, date, time)

When the Regional Setting (Time Zone, date, time) option is selected, the Regional Setting (Time Zone, date, time) screen displays with the Region menu item.

A. Choose **Region**, and use the left / right arrow keys to view the available region selections.

B. After making a selection, press the checkmark key to display the Choose a Location screen.

C. Choose **Location**, and use the left / right arrow keys to view the available location selections.

D. After making a selection, press the checkmark key to display the Save Changes? screen:

- Choose **Yes** to save your changes and to return to the main menu.
- Choose **No** to return to the previous screen.

Go to Step 1B: Console Setup Procedures, Access the Web Filter via its LAN 1 IP Address.

Non-Quick Start procedures or settings

The options described below do not pertain to the quick start setup process.

WF Patch Level

When the WF Patch Level option is selected, "Web Filter" and the version number of the currently installed software build displays.

Serial Number

When the Serial Number option is selected, the serial number of the chassis displays.

Reset WF Admin Console Password

When the Reset WF Admin Console Password option is selected, the Reset Admin Console screen displays with a WARNING menu item.

A. Choose ***** WARNING ***** to display the message screen:

*** WARNING *** The Admin console username/password will be reset to 'admin'/'user3' and all locked IPs will be unlocked.

B. After reading the warning message, select one of two options on the screen:

- Choose **Yes, reset it now!** to reset the password and to return to the main menu.
- Choose **No, cancel reset** to return to the previous screen.

Reboot

When the Reboot option is selected, the Reboot screen displays with two menu items.

A. Choose one of two options:

- **Yes, reboot now!!!** - This selection reboots the Web Filter.
- **No, cancel reboot** - This selection returns you to the previous screen.

B. Press the "X" key to return to the main menu.

Shutdown

When the Shutdown option is selected, the Shutdown screen displays with two menu items.

A. Choose one of two options:

- **Yes, shutdown now!!** - This selection shuts down the Web Filter.
- **No, cancel shutdown** - This selection returns you to the previous screen.

B. Press the "X" key to return to the main menu.

LCD Options menu

When "**LCD Options >**" is selected, the following menu items display on the screen:

- Heartbeat
- Backlight
- LCD Controls >

Make a selection from the menu, and press the checkmark key to go to that screen.

Heartbeat

When the Heartbeat option is selected, the Heartbeat screen displays.

A. Press the checkmark or right arrow key three times to view each of the three available options:

- heartbeat feature enabled (checkbox populated with "x")
- heartbeat feature disabled (checkbox empty)
- check for a heartbeat now (checkbox populated with checkmark, and blinking heartbeat symbol displayed in the line above)

B. After making your selection, press the "X" key to return to the previous screen.

Backlight

When the Backlight option is selected, the Backlight screen displays.

A. Press the checkmark or right arrow key three times to view each of the three available options:

- backlight feature enabled (checkbox populated with "x" and backlight turns on)
- backlight feature disabled (checkbox empty and backlight turns off)
- display the backlight now (checkbox populated with checkmark, and backlight turns on)

B. After making your selection, press the "X" key to return to the previous screen.

LCD Controls

When the LCD Controls option is selected, the LCD Controls screen displays with the following menu items: Contrast, On Brightness, Off Brightness.

A. Choose one of the menu selections and press the checkmark key to go to that screen:

- **Contrast** - In the Contrast screen, use the left / right arrow keys to decrease / increase the text and screen contrast.
- **On Brightness** - In the On Brightness screen, use the left / right arrow keys to decrease / increase the brightness of a screen with a feature that is enabled.
- **Off Brightness** - In the Off Brightness screen, use the left / right arrow keys to decrease / increase the brightness of a screen with a feature that is disabled.

B. After making your selection, press the "X" key to return to the previous screen.

Step 2: Physically Connect the Unit to the Network

Now that your Web Filter network parameters are set, you can physically connect the unit to your network. This step requires two standard CAT-5E cables.

A. Reboot the server by using the Reboot system option (as described in Step 1A: Quick Start Setup Procedures), or by using the Reboot option on the LCD panel of the SL or HL unit (as described in Step 1B: LCD Panel Setup Procedures).

B. Plug one end of a standard CAT-5E cable into the Web Filter's LAN 1 port, the port on the left.

Portion of SL and MSA chassis rear
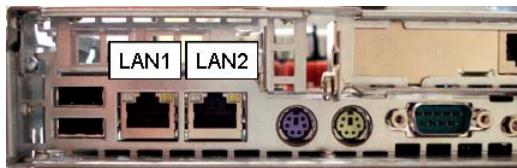
Portion of HL chassis rear

C. Plug the other end of the CAT-5E cable into an open port on the network hub that handles the Internet traffic you wish to filter.

D. Repeat sub-steps B and C for the Web Filter's LAN 2 port.

E. Wait until the reboot process has completed, indicated by the drive light staying off for 30 seconds. This process may take 5 to 10 minutes.

NOTE: *If you receive a connection failure message during the reboot process, please disregard it, as this often occurs when there is a change in the IP address.*

Step 3: Access the Web Filter Online

Access the Web Filter via its LAN 1 IP Address

A. Launch an Internet supported browser:

- Firefox 9 or 10
- Internet Explorer 8 or 9
- Safari 5.0 or 5.1
- Google Chrome 16 or 17

B. In the address field, type in the LAN 1 IP address you assigned to the Web Filter in Step 1A (Quick Start setup) or Step 1B (IP / LAN1 and 2). Be sure to use "https" and port **:1443** for a secure connection, appended by "/login.jsp". For example, if the Web Filter were assigned an IP address of 10.10.10.10, you would enter **https://10.10.10.10:1443/login.jsp** in the browser's address field.

C. Click **Go** to display the security issue page:

- If using Firefox, proceed to Accept the Security Certificate in Firefox.
- If using IE, proceed to Temporarily Accept the Security Certificate in IE.
- If using Safari, proceed to Accept the Security Certificate in Safari.
- If using Google Chrome, proceed to Accept the Security Certificate in Chrome.
- If the security issue page does not display in your browser, verify the following:
  - The Web Filter is powered on.
  - The Web Filter is connected to the same hub as your router/firewall.
  - Can the administrator workstation normally connect to the Internet?
  - Is the Web Filter plugged into a switch instead of a hub?
  - Do you have both LAN ports connected to your network hub?
  - Is there a caching server?
  - Is the administrator workstation able to ping the Web Filter's LAN 1 IP address?
  - If pinging the IP address of the Web Filter is unsuccessful, try restarting the network service or rebooting the Web Filter.
  - If still unsuccessful, contact an M86 Security solutions engineer or technical support representative.

Accept the Security Certificate in Firefox

A. If using a Firefox browser, in the page "This Connection is Untrusted," click the option **I Understand the Risks**:
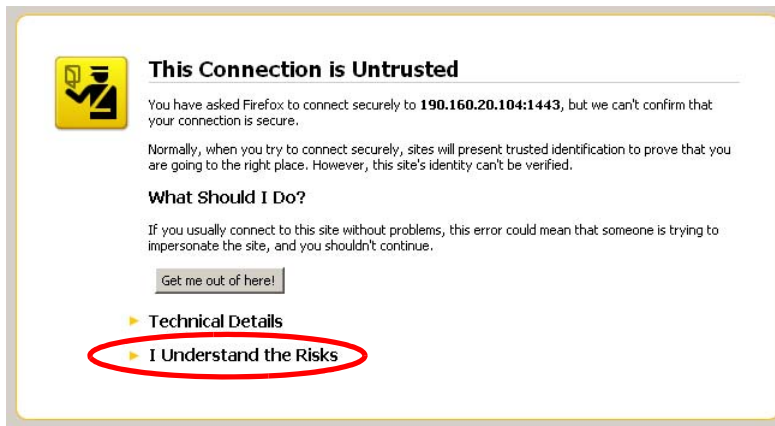
B. In the next set of instructions that display, click **Add Exception...**:
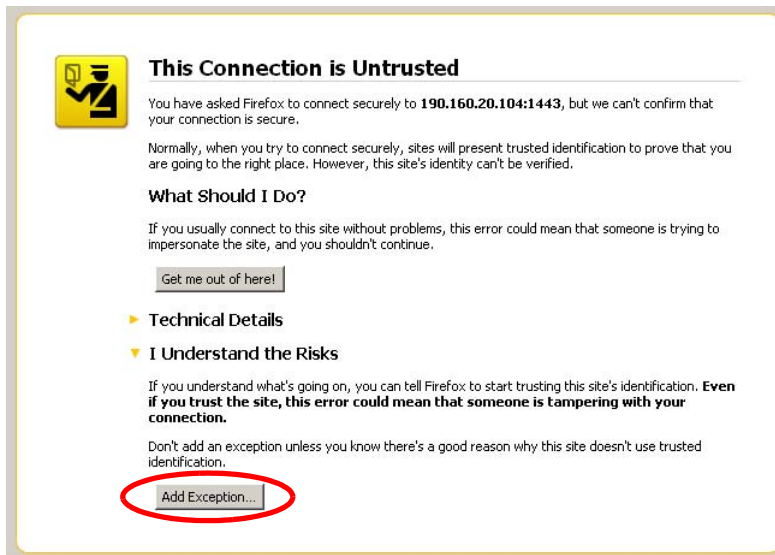
Clicking Add Exception opens the Add Security Exception window:
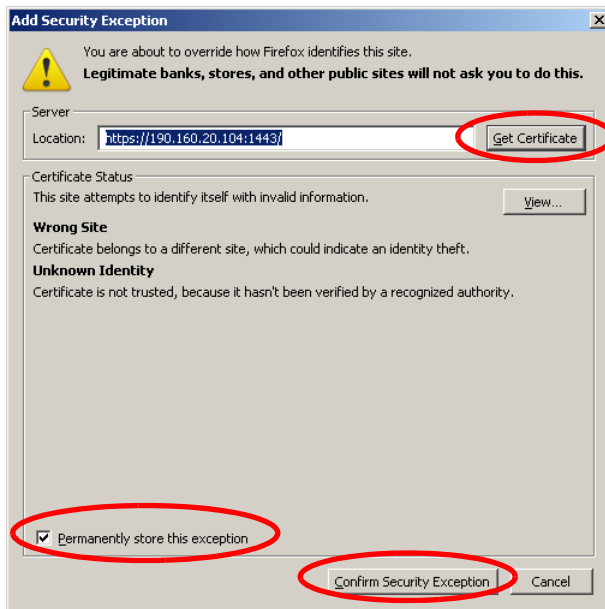
C. In the Add Security Exception window, click **Get Certificate** and wait a few seconds until the security certificate is obtained by the server.

D. With the checkbox **Permanently store this exception** selected (or grayed-out), click **Confirm Security Exception** to open the Security warning dialog box:
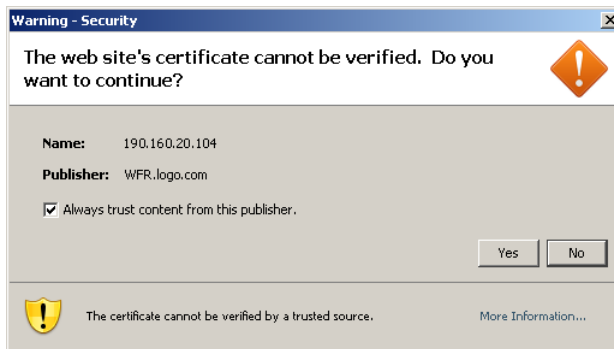
E. With the checkbox "Always trust content from this publisher." populated, click **Yes** to close the Security warning dialog box and to access the login window of the Web Filter user interface:
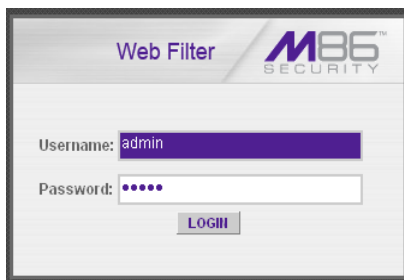
Proceed to Step 4: Log in, Generate SSL Certificate.

Temporarily Accept the Security Certificate in IE

If using an IE browser, in the page "There is a problem with this website's security certificate.", click **Continue to this website (not recommended)**:
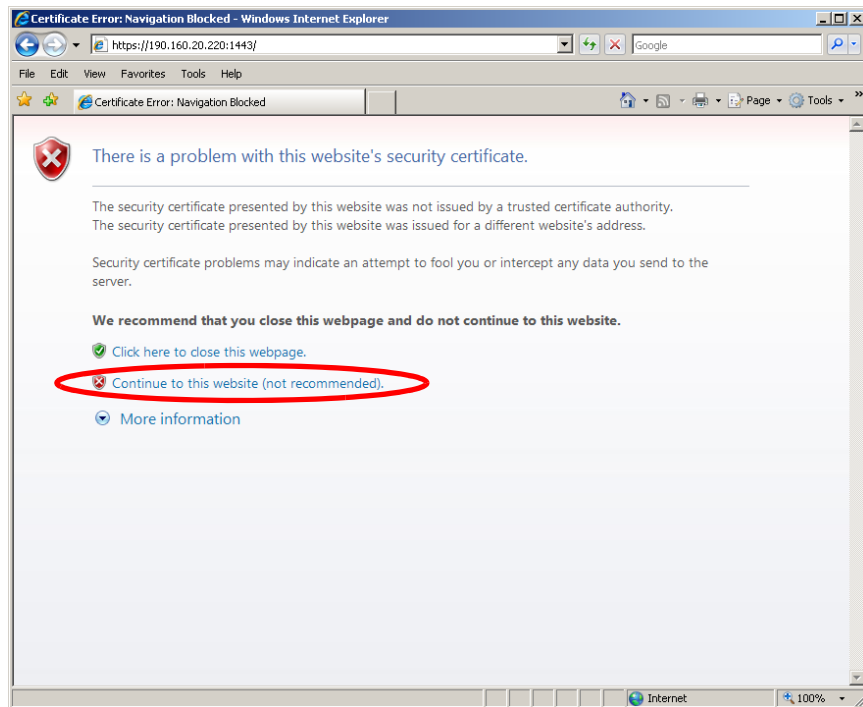
Selecting this option displays the Web Filter login page with the address field and the Certificate Error button to the right of the field shaded a reddish color:

Proceed to Step 4: Log in, Generate SSL Certificate.

Accept the Security Certificate in Safari

A. If using a Safari browser, the window explaining "Safari can't verify the identity of the website..." opens:

Click **Show Certificate** to open the certificate information box at the bottom of this window:
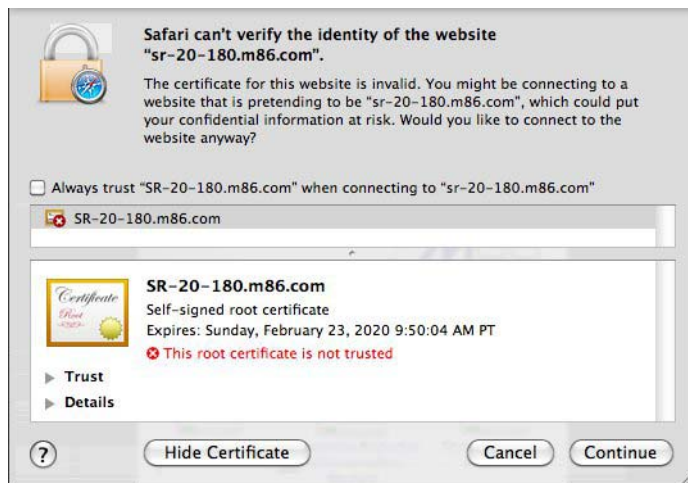
B. Click the "Always trust..." checkbox and then click **Continue**:
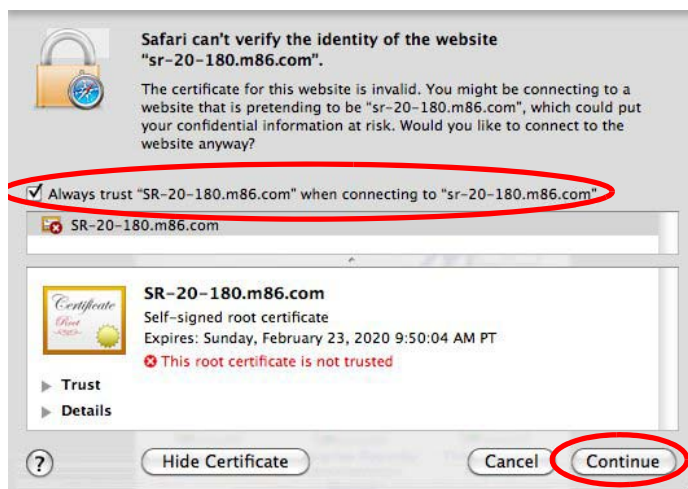
C. You will be prompted to enter your password in order to install the certificate.

Once you are able to access the Web Filter login window, proceed to Step 4: Log in, Generate SSL Certificate.

Accept the Security Certificate in Chrome

A. If using a Chrome browser, in the page "This is probably not the site you are looking for!" click the button **Proceed anyway**:
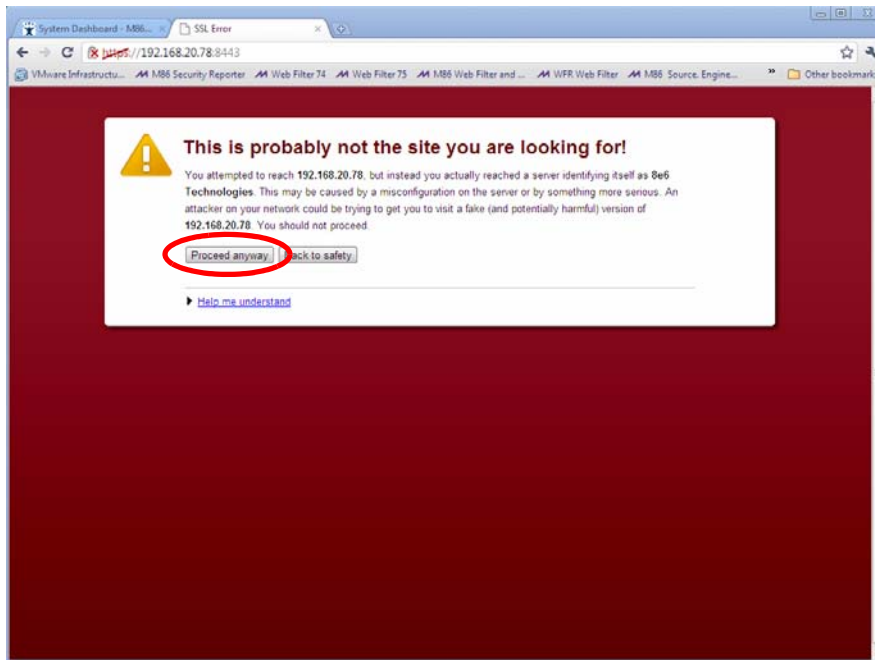
Clicking this button launches the Web Filter login window:

NOTE: The Security Certificate must be accepted each time a new browser is launched.
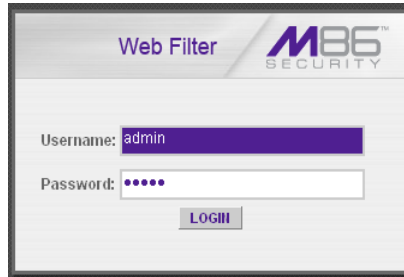
B. Proceed to Step 4: Log in, Generate SSL Certificate.

Step 4: Log in, Generate SSL Certificate
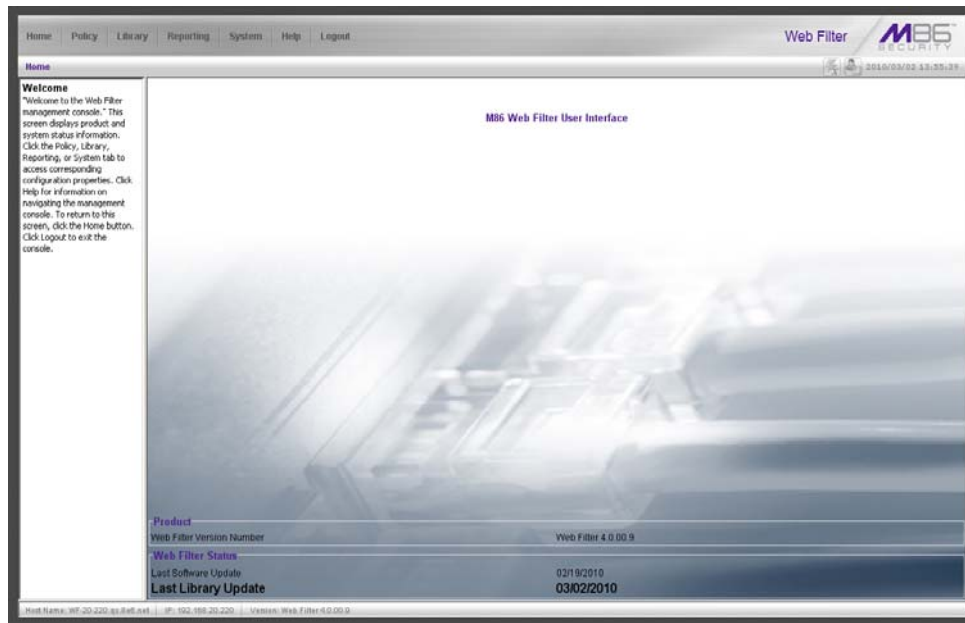
This step requires you to log in and generate a self-signed certificate for the Web Filter to ensure secure exchanges between the appliance and your browser. If using an IE browser, you will need to complete the security certificate acceptance procedures.

Log in to the Web Filter

A. In the Web Filter Administrator console login window, type in the **Username** (*admin*) and **Password** (*user3*):

B. Click **LOGIN** to display the Web Filter Admin console Welcome window:

Generate SSL Certificate

A. Navigate to **System > UI SSL Certificate** to open the SSL Certificate window:
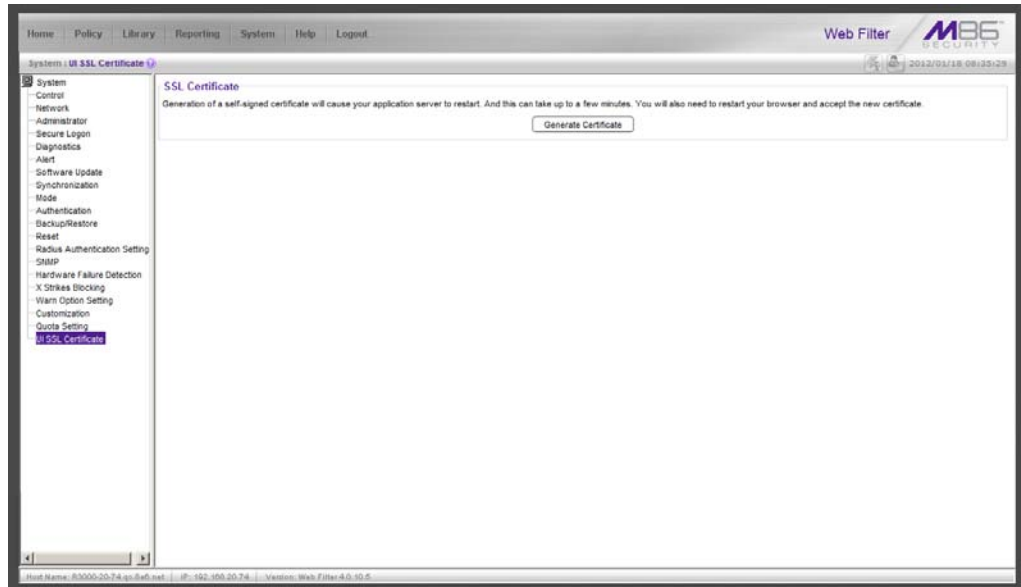
B. Click **Generate Certificate** to open the box that asks if you wish to continue, which would restart your server.

C. Click **Yes** to generate the SSL certificate and restart the Web Filter.

D. After the certificate is generated, you will be prompted to click **OK** and close your browser. Wait a few minutes before attempting to access the user interface.

If using an IE browser, proceed to IE Security Certificate Installation Procedures.

If using a Firefox, Safari, or Chrome browser, proceed to Step 5: Test Filtering or the Mobile Security Client Connection.

IE Security Certificate Installation Procedures

Accept the Security Certificate in IE

Go to the appropriate sub-section if using the following Windows operating system and IE browser:

- Windows XP or Vista with IE 8 or 9
- Windows 7 with IE 8 or 9

Windows XP or Vista with IE 8 or 9

A. If using an IE 8 or 9 browser on a Windows XP or Vista machine, in the page "There is a problem with this website's security certificate.", click **Continue to this website (not recommended)**:
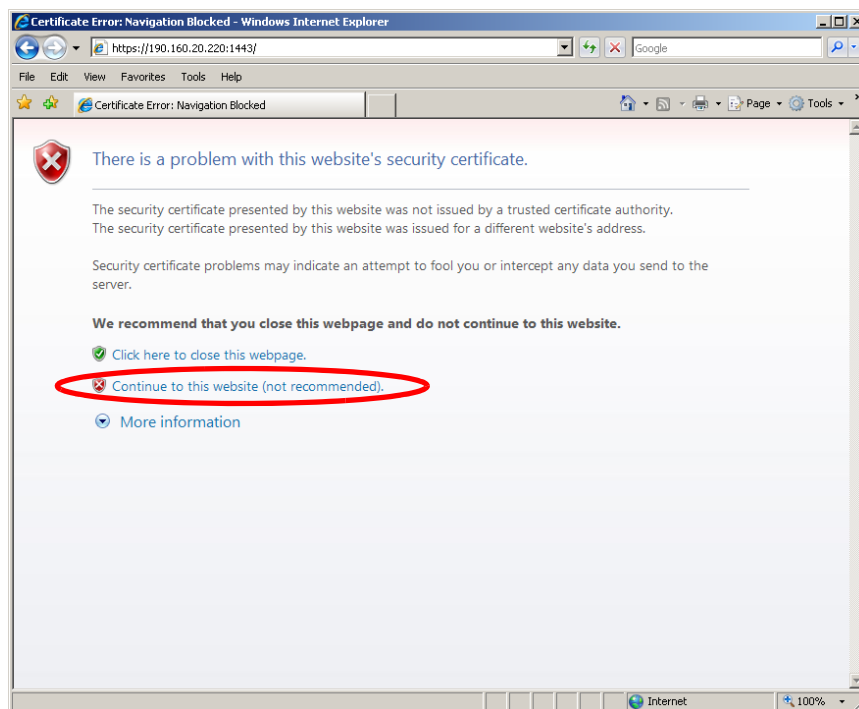
Figure A1: Windows XP, IE 8

Selecting this option displays the Web Filter login page with the address field and the Certificate Error button to the right of the field shaded a reddish color:

*Figure A2: Windows XP, IE 8*

B. Click **Certificate Error** to open the Certificate Invalid box:
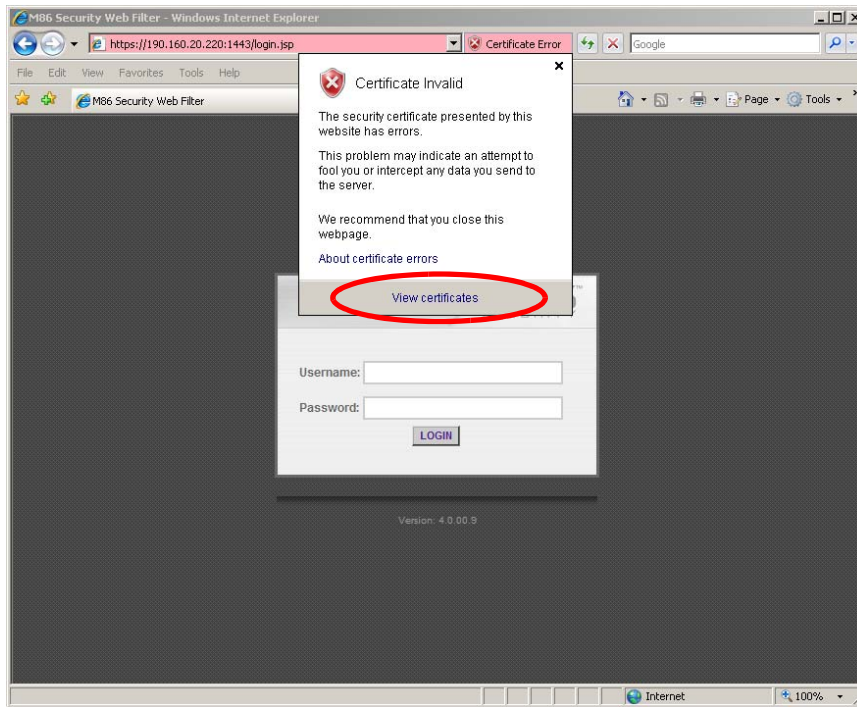
Figure B: Windows XP, IE 8

C. Click **View certificates** to open the Certificate window that includes the host name you assigned to the Web Filter:
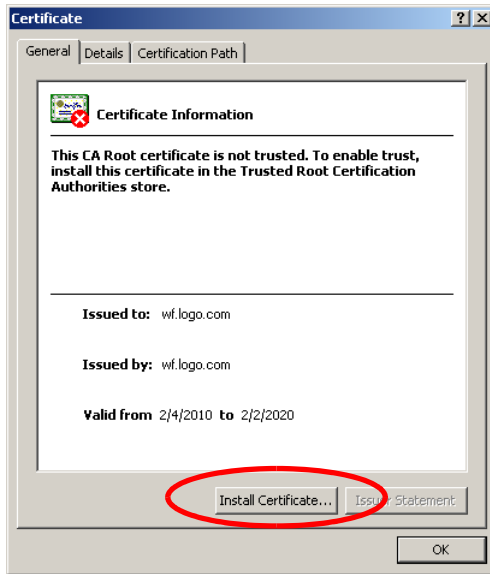
Figure C: Windows XP, IE 8

D. Click **Install Certificate...** to launch the Certificate Import Wizard:
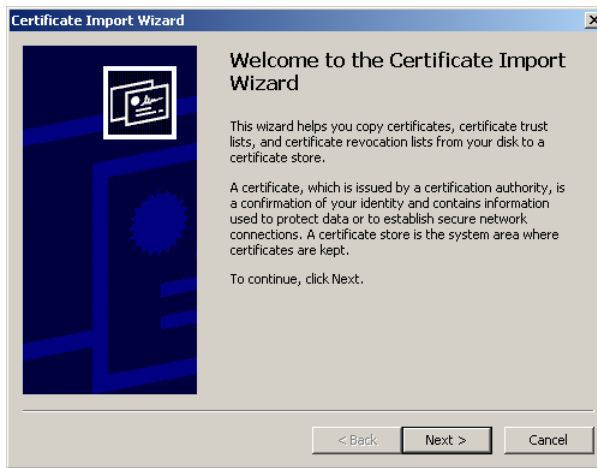
Figure D: Windows XP, IE 8

E. Click **Next >** to display the Certificate Store page:
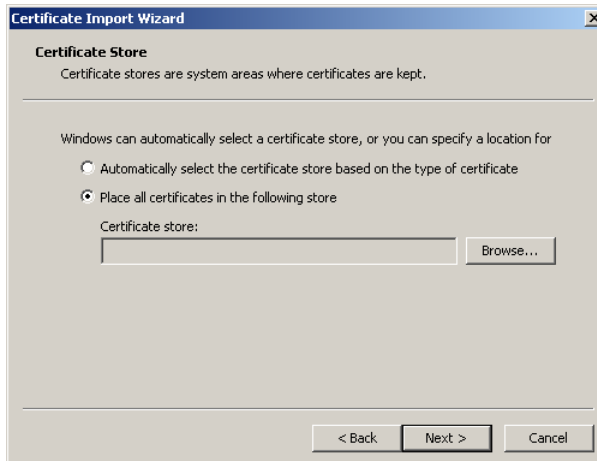
Figure E: Windows XP, IE 8

F. Choose the option "Place all certificates in the following store" and then click **Browse...** to open the Select Certificate Store box:

Figure F: Windows XP, IE 8

G. Choose "Trusted Root Certification Authorities" and then click **OK** to close the box.

H. Click **Next >** to display the last page of the wizard:

Figure H: Windows XP, IE 8

I. Click **Finish** to close the wizard and to open the Security Warning dialog box asking if you wish to install the certificate:
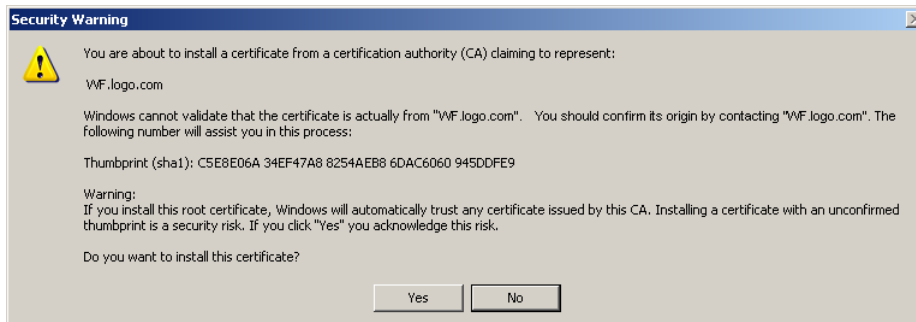
Figure I: Windows XP, IE 8

J. Click **Yes** to install the certificate and to close the dialog box. When the certificate is installed, the alert window opens to inform you the certificate installation process has been completed.

K. Click **OK** to close the alert box, and then close the Certificate window.

Now that the security certificate is installed, you will need to map the Web Filter's IP address to its host name. Proceed to Map the Web Filter's IP Address to the Server's Host Name.

Windows 7 with IE 8 or 9

A. If using an IE 8 or 9 browser on a Windows 7 machine, in the page "There is a problem with this website's security certificate.", click **Continue to this website (not recommended)**.

B. From the toolbar, select **Tools > Internet Options** to open the Internet Options box.

C. Select the Security tab, click **Trusted sites**, and then click **Sites** to open the Trusted sites box.

D. In the Trusted sites box, confirm the URL displayed in the field matches the IP address of the Web Filter, and then click **Add** and **Close**.

E. Click **OK** to close the Internet Options box.

F. Refresh the current Web page by pressing the **F5** key on your keyboard.

G. Follow steps A to K documented in Windows XP or Vista with IE 8 or 9:

- When the security issue page re-displays with the message: "There is a problem with this website's security certificate.", click **Continue to this website (not recommended)** (see Figure A1). Choosing this option displays the Web Filter login window with the address field and the Certificate Error button to the right of the field shaded a reddish color (see Figure A2).
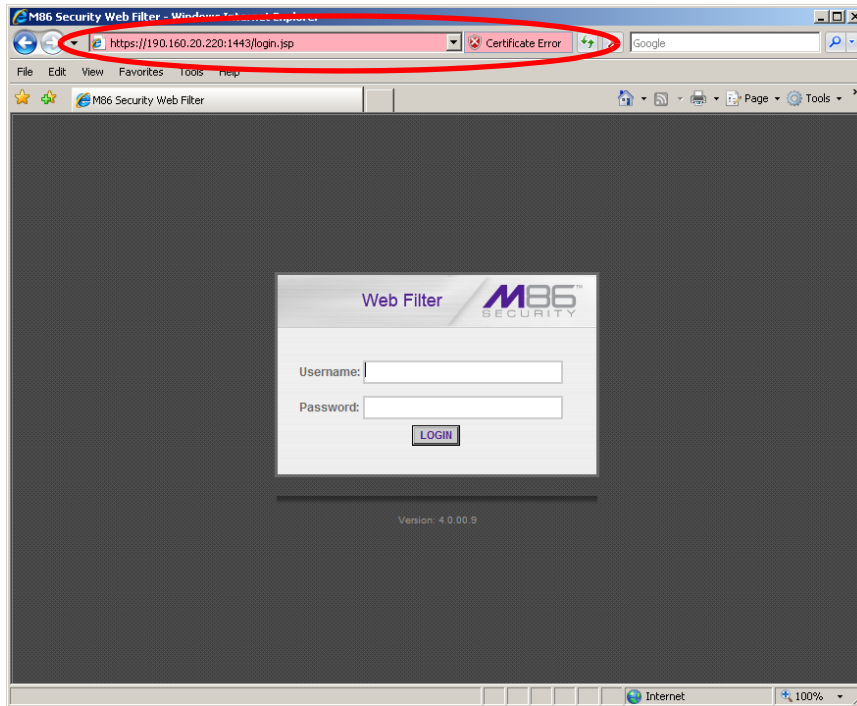- Click **Certificate Error** to open the Certificate Invalid box (see Figure B).
- Click **View certificates** to open the Certificate window that includes the host name you assigned to the Web Filter (see Figure C).
- Click **Install Certificate...** to launch the Certificate Import Wizard (see Figure D).
- Click **Next >** to display the Certificate Store page (see Figure E).
- Choose the option "Place all certificates in the following store" and then click **Browse...** to open the Select Certificate Store box (see Figure F).
- Choose "Trusted Root Certification Authorities" and then click **OK** to close the box.
- Click **Next >** to display the last page of the wizard (see Figure G).
- Click **Finish** to close the wizard and to open the Security Warning dialog box asking if you wish to install the certificate (see Figure H).
- Click **Yes** to install the certificate and to close the dialog box. When the certificate is installed, the alert window opens to inform you the certificate installation process has been completed (see Figure I).
- Click **OK** to close the alert box, and then close the Certificate window.

H. From the toolbar of your browser, select **Tools > Internet Options** to open the Internet Options box.

I. Select the Security tab, click **Trusted sites**, and then click **Sites** to open the Trusted sites box.

J. Select the URL you just added, click **Remove**, and then click **Close**.
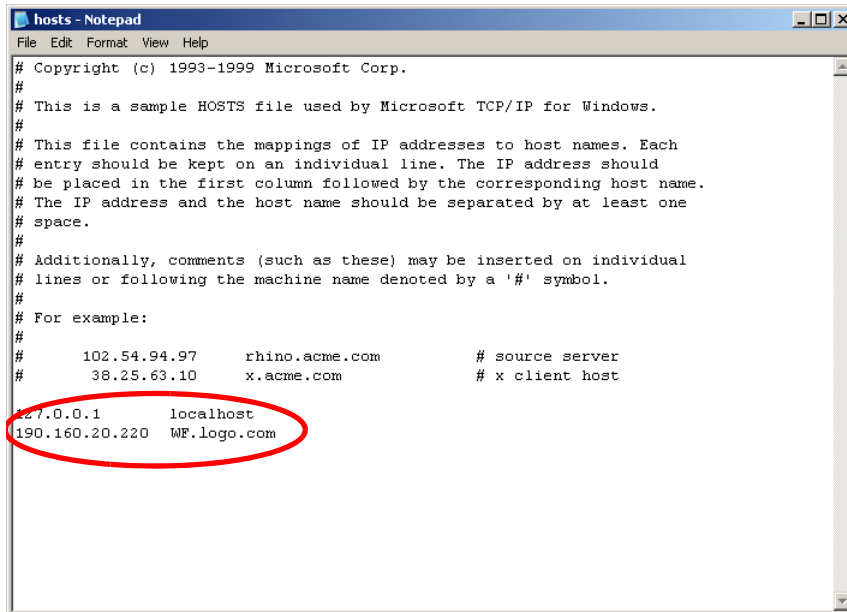
Now that the security certificate is installed, you will need to map the Web Filter's IP address to its host name. Proceed to Map the Web Filter's IP Address to the Server's Host Name.

Map the Web Filter's IP Address to the Server's Host Name

A. From your workstation, launch Windows Explorer and enter **C:\WINDOWS\system32\drivers\etc** in the address field to open the folder where the hosts file is located:
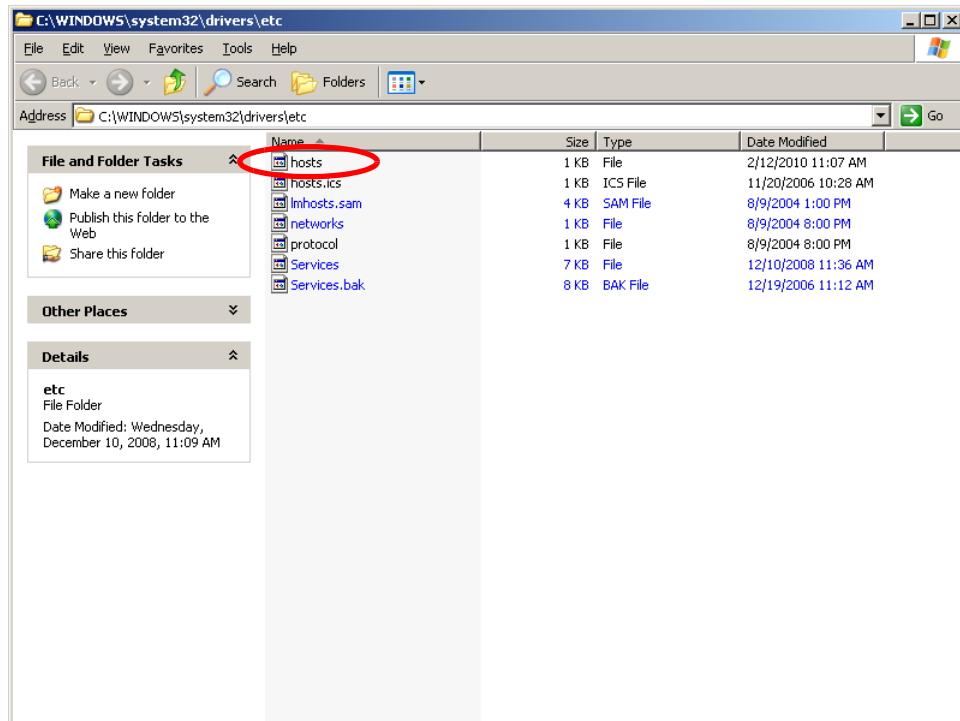
B. Double-click "hosts" to open a window asking which program you wish to use to open the file. Double-click "Notepad" or "TextPad" to launch the hosts file using that selected program:

C. Enter a line in the hosts file with the Web Filter's IP address and its host name—the latter entered during the Configure host name screen of the Quick Start Setup Procedures (Step 1A), or the Host Name screen in LCD Panel Setup Procedures (Step 1B)—and then save and close the file.

D. In the address field of your newly opened IE browser, from now on you will need to use the Web Filter's host name instead of its IP address—that is **https://hostname:1443/login.jsp** would be used instead of **https://x.x.x.x:1443/login.jsp**. Click **Go** to open the Web Filter login window:
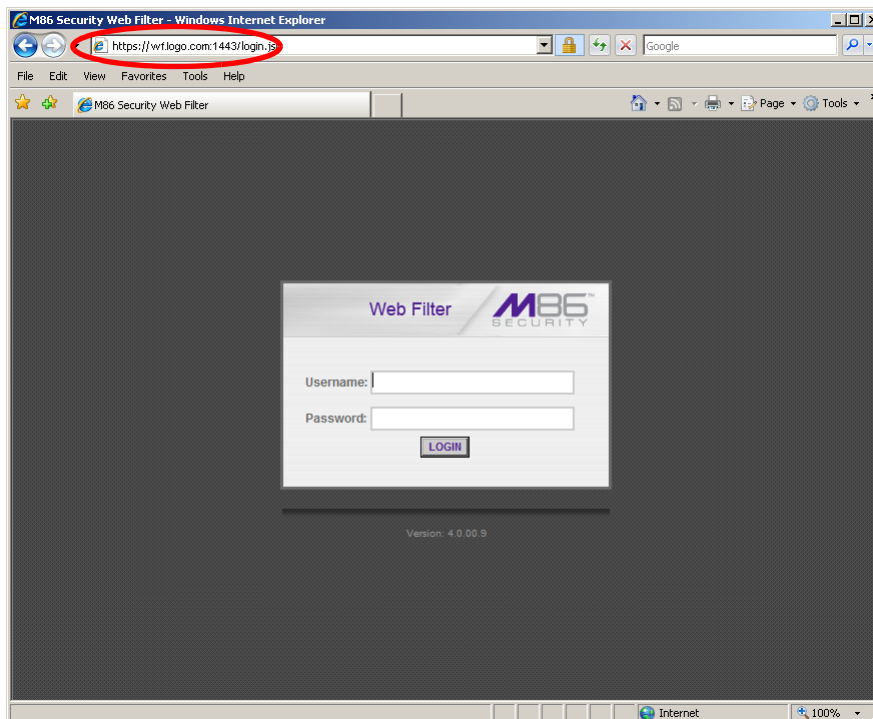
Proceed to Step 5: Test Filtering or the Mobile Security Client Connection.

Step 5: Test Filtering or the Mobile Security Client Connection

Test Filtering

If this Web Filter has been set up in the Invisible, Router, or Firewall mode, once you have accessed the Web Filter Administrator console, you should test filtering.

A. Test the Web Filter's filtering by opening a browser window on a network workstation, and then going to the following empty sites to test pornography filtering:

- **http://test.8e6.net**
- **http://testsite.marshal.com**

B. You should receive a block page for each URL tested. If you do not, contact an M86 Security solutions engineer or technical support representative.

Test the Mobile Security Client Connection

If this Web Filter has been set up in the Mobile mode, you do not need to test filtering. Instead, once you have accessed the Web Filter Administrator console, you should verify that the Mobile Security Client can reach the Web Filter.

A. Use a workstation on which the Mobile Security Client is installed that is not on a filtered portion of the LAN. Open a browser window on a network workstation, and then go to a few test sites you set up to be blocked by the Mobile Security Client.

B. The connections should be blocked, and the block pages served by the Web Filter should display in the browser's address field. If you do not receive a block page for each tested URL, contact an M86 Security solutions engineer or technical support representative.

Step 6: Set Library Updates

After verifying that the Web Filter is correctly installed on your network, you need to activate Web Filter library updates. Library updates are critical for filtering as new sites are added to the M86 Security library each day. To activate updates, visit the M86 Security Web site and enter the activation code that was issued to you by e-mail (also included on the product invoice).

NOTE: *Port 443 (HTTPS) must be open for outgoing requests so that the Web Filter can receive library updates.*

Activate and Register the Web Filter

Be sure you have a valid host name chosen before activating your account.

A. Open an Internet browser window and go to **http://www.m86security.com/ support/activate-appliance.asp**.

B. After reading through the online End User License Agreement, click **Accept** to go to Step 2 of the activation process.

C. Enter your activation code.

D. Click **Submit** to go to the Activation and Registration page.

E. Verify that your serial number and activation code are the same as shown on this registration page.

F. Fill out the information on this page, including the host name for the public DNS server. ***The entry of the unique host name you've chosen is mandatory in order to receive library updates.***

G. After all information is entered, click **Activate** to activate your service. You should receive confirmation that the Web Filter at your host name has been activated.

You may wish to print the confirmation page for future reference in dealing with technical issues.

Perform a Complete Library Update

Your Web Filter was shipped with the latest library update for the current software release. However, as new updates continually become available, before you begin using the Web Filter you must perform a complete library update to ensure you have the latest library updates.

To download the latest library updates:

A. Click the **Library** link at the top of the screen.

B. From the navigation panel, click Updates and select Manual Update from the menu:
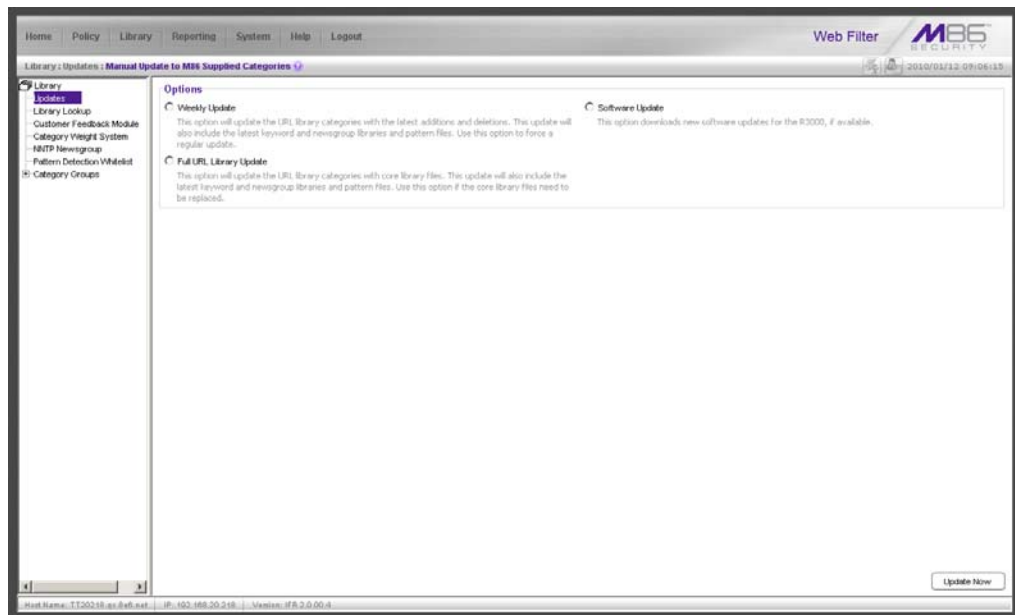
C. In the Manual Update to M86 Supplied Categories window, click the radio button corresponding to **Full URL Library Update**.

D. Click **Update Now** to begin the update process.
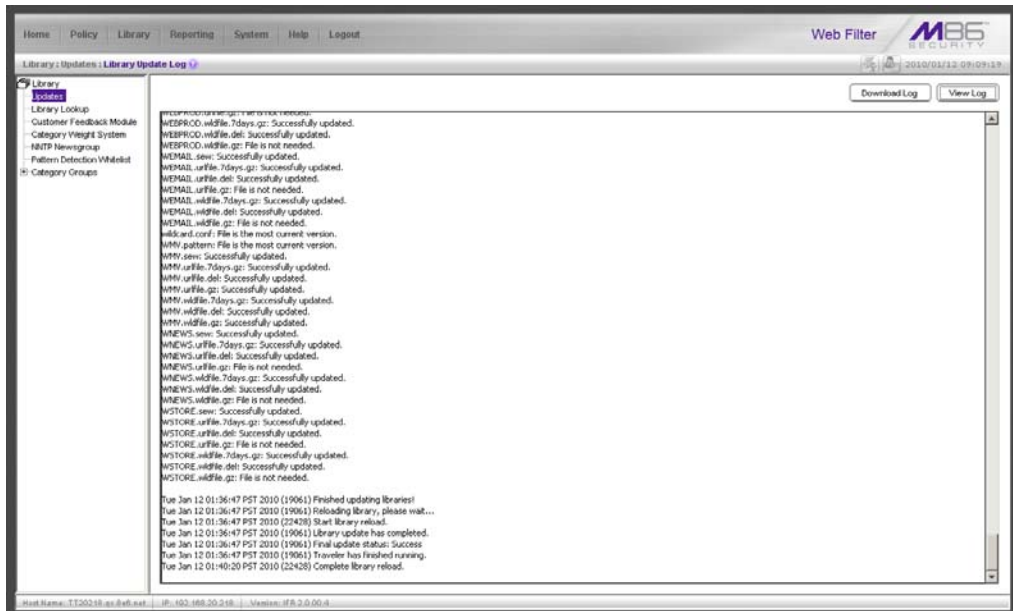
Monitor the Library Update Process

To verify that the library is being updated:

A. From the navigation panel, click Updates and select Library Update Log from the menu.

B. In the Library Update Log window, click **View Log** to display the update activity:

NOTE: *You will be notified in the log when the library has been completely updated by the message: "Full URL Library Update has completed." If this message does not yet display, click **View Log** again to view the latest information.*

WARNING: *At the conclusion of this step, your Web Filter will be actively filtering your network. The Web Filter is initially set to filter pornography sites on all of your network traffic associated with the hub to which it is connected.*

CONCLUSION

Congratulations; you have completed the Web Filter installation procedures. Now that the Web Filter is filtering your network, the next step is to set up groups and create filtering profiles for group members.

To activate a default filter profile more appropriate for your operations, or to specify a more limited IP range to filter, consult Chapter 2: Group screen in the Global Administrator Section of the Web Filter User Guide. Refer to Chapter 1: System screen for information on how to give end users access to acceptable HTTPS sites if strict HTTPS filtering settings are used.

Obtain the latest Web Filter User Guide at **http://www.m86security.com/ support/R3000/documentation.asp**

For troubleshooting tips, visit **http://www.m86security.com/software/8e6/ts/ r3000.html**

IMPORTANT: M86 Security recommends proceeding to the Best Filtering Practices section to implement setup procedures for the filtering scenarios described within that section.

BEST FILTERING PRACTICES

This collection of setup and usage scenarios is designed to help you understand and use basic tools in the Web Filter console for configuring the user interface and creating filtering profiles for users in your network. Each scenario is followed by console setup information. Please consult the "How to" section in the index of the Web Filter User Guide for pages containing detailed, step-by-step instructions on configuring and/or using the tools and features described in that scenario.

In this section you will learn how to:

- block user access to filtering categories, URL and search engine keywords, and various pattern types and file types
- set up user profiles or accounts to bypass blocked filtering categories
- create a custom category for URLs and keywords you wish to block
- establish time quotas and time profiles for user access to specified library categories
- lock out end users from Internet access after a designated number of hits to specified sites

Threat Class Groups

M86 Security's filtering library currently consists of 104 library filtering categories, each placed in one of the 20 filtering category groups defined in the interface: Adult Content, Bandwidth, Business/Investments, Community/Organizations, Education, Entertainment, Government/Law/Politics, Health/Fitness, Illegal/Questionable, Information Technology, Internet Communication, Internet Productivity, Internet/Intranet Misc., News/Reports, Religion/Beliefs, Security, Shopping, Society/Lifestyles, Travel/Events, and Custom Categories.

Outside of the interface, we have also grouped these library categories into four Threat Class Groups, based on the type of security level that best defines them:

- Threats/Liabilities
- Bandwidth/Productivity
- General/Productivity
- Pass/Allow

Threats/Liabilities	Bandwidth/Productivity		General/Productivity		Pass/Allow
Adult Content	**Bandwidth**	**Internet Productivity**	**Business/Investments**	**Information Technology**	**Custom Categories**
Child Pornography	Image Servers/Search Engines	Adware	Employment	Dynamic DNS	Intranet/Internal Servers
Explicit Art	Internet Radio	Banner/Web Ads	Financial Institution	Freeware/Shareware	Company Internal
Obscene/Tasteless	Peer-to-Peer (P2P) File Sharing	Fantasy Sports	General Business	Information Technology	School District Internal
Pornography/Adult Content	Video Sharing	Free Hosts	Online Trading/Brokerage	Internet Service Providers	**Always Allow Categories**
R-rated	VoIP	Web Hosts	Real Estate	Portals	Partner or business-related
Security	Web-based storage	Remote Access	**Community/Organizations**	Web-based News groups	
Bad Reputation Domains	Streaming Media	Generic Remote Access	Community Organizations	Search Engines	NOTE: The only M86 filtering category
BotNet	Flash Video	GoToMyPC	Local Community	**Internet/Intranet Misc.**	in the Pass/Allow group is
Hacking	Generic Streaming Media	Remote Desktop	**Education**	Domain Landing	Intranet/Internal Servers in the
Malicious Code/Virus	Quick Time Video	Secure Shell	Education	Edge Content Servers	Custom Categories category group.
Phishing	Real Time Streaming Protocol	Virtual Network Computing	Educational Games	Invalid Web pages	This category must be maintained by
Spyware	Windows Media Video	pcAnywhere	Online Classes	Reviewed/Miscellaneous	your administrator. The other listings
Web-based Proxies/Anonymizers	**Internet Communication**	**Shopping**	Reference	**News/Reports**	under Pass/Allow are suggested
Illegal/Questionable	Chat	Online Auction	**Entertainment**	News	topics you might wish to set up.
Criminal Skills	Message Boards	Shopping	Art	Sports	
Dubious/Unsavory	Online Communities		Comics	Weather/Traffic	
Hate & Discrimination	Translation Services		Entertainment	**Religion/Beliefs**	
Illegal Drugs	Web-based E-mail		Gambling	Paranormal	
School Cheating	Web logs/Personal Pages		Humor	Religion	
Terrorist/Militant/Extremist	Web-based Productivity Apps		Kids	**Society/Lifestyles**	
	Instant Messaging (IM)		Movies & Television	Alcohol	
	Generic IM		Music Appreciation	Animals/Pets	
	Google Chat		Online Greeting Cards	Books & Literature/Writings	
	Google Talk		Restaurants/Dining	Dating/Personals	
	ICQ & AIM		Theater	Fashion	
	IRC		Games	Lifestyle	
	Meebo		Games	Recreation	
	My Space IM		Games Patterns	Self Defense	
	PoPo		**Government/Law/Politics**	Social Opinion	
	QQ		Government	Tobacco	
	ToToMoMo		Legal	Weapons	
	WangWang		Military Appreciation	**Travel/Events**	
	Windows Live Messenger		Military Official	Tickets	
	Yahoo IM		Political Opinion	Travel	
			Health/Fitness	Vehicles	
			Fitness		
			Health/Medical		
			Holistic		
			Self Help		

Please review the scenarios for each of the four Threat Class Groups to fulfill the functions specified therein.

I. Threats/Liabilities

A. Category block

Block categories that threaten your network/organization. In pertinent profiles, block access to the Security category group and other categories containing content that threaten your organization.

To block categories in a profile, go to:
- POLICY: Policy > IP > member > member profile > Category tab
  or POLICY: Policy > Global Group > Global Group Profile > Category tab

In the Web Filter User Guide index, see:
• How to: use library categories in a profile

B. Rule block

Use a rule to block categories that threaten your network/organization. Create a rule that blocks access to the Security category group and other categories containing content that threaten your organization, and then apply this rule to pertinent profiles. Or use a defined rule—such as the CIPA Compliance rule, if in the educational sector—to block related categories.

To create a rule and block categories in a profile, go to:

- POLICY: Policy > Global Group > Rules
- Policy > IP > member > member profile > Category tab
  or Policy > Global Group > Global Group Profile > Category tab

In the Web Filter User Guide index, see:
• How to: use rules
• How to: use library categories in a profile

C. X-Strike on blocked categories

Lock out users from workstations after "X" number of attempts are made to access content that could endanger your network/organization. Enable and configure the X Strikes Blocking feature, specifying categories that threaten your organization. Enable the X Strikes Blocking filter option in applicable profiles. The user receives a block page and is locked out of Internet/Intranet access after the specified number of "strikes" are made to any of these categories.

To block categories in a profile using the X Strikes Blocking feature, go to:
- SYSTEM: System > X Strikes Blocking > Configuration tab, and Categories tab
- POLICY: Policy > IP > member > member Profile > Filter Options tab, X Strikes Blocking enabled
  or POLICY: Policy > Global Group > Global Group Profile > Filter Options tab (X Strikes Blocking enabled)

In the Web Filter User Guide index, see:
• How to: set up X Strikes Blocking
• How to: set up profile options

D. Custom Lock, Block, Warn, X Strikes, Quota pages

Customize a lock, block, warning, X Strikes, or quota page. Modify page contents to point to a URL within your organization, send a request to your administrator's email address, or include verbiage of your choice that informs users of their Internet usage activities that triggered the page.

To customize pages, go to:
•   SYSTEM: System > Customization > Common Customization window, and other applicable customization windows

In the Web Filter User Guide index, see:
• How to: customize pages

E. URL Keywords

Block access to network-endangering content via URL keywords. In pertinent library categories, enter URL keywords to be blocked. Block these categories in applicable profiles.

To set up URL keywords to be blocked, go to:
•   LIBRARY: Library > Category Groups > category > URL Keywords
•   POLICY: Policy > IP > member > member Profile > Filter Options tab (URL Keyword Filter Control enabled)
    or POLICY: Policy > Global Group > Global Group Profile > Filter Options tab (URL Keyword Filter Control enabled)

In the Web Filter User Guide index, see:
• How to: set up URL Keywords
• How to: set up profile options

F. Search Engine Keywords

Block access to network-endangering content via search engine keywords. In pertinent library categories, enter SE keywords to be blocked. Block these categories in applicable profiles.

To set up Search Engine Keywords to be blocked, go to:
•   LIBRARY: Library > Category Groups > category > Search Engine Keywords
•   POLICY: Policy > IP > member > member Profile > Filter Options tab (Search Engine Keyword Filter Control enabled)
    or POLICY: Policy > Global Group > Global Group Profile > Filter Options tab (Search Engine Keyword Filter Control enabled)

In the Web Filter User Guide index, see:
• How to: set up Search Engine Keywords
• How to: set up profile options

G. Custom Category (blocked)

Add a category to block content that could endanger your network/organization. Create a custom category with contents tailored to safeguard your organization. Block this category in appropriate profiles.

To set up a custom category and block it, go to:
* LIBRARY: Library > Category Groups > Custom Categories > Add Category
* POLICY: Policy > IP > member > member Profile > Category tab
  or POLICY: Policy > Global Group > Global Group Profile > Category tab

In the Web Filter User Guide index, see:
• How to: set up a custom category
• How to: use library categories in a profile

H. Minimum Filtering Level

At the root level, block categories that could endanger your network/organization. Configure the Minimum Filtering Level to block specified categories, and do the same in the Global Group Profile.

To configure the minimum filtering level, go to:
* POLICY: Policy > Global Group > Minimum Filtering Level
* Policy > Global Group > Global Group Profile > Category tab

In the Web Filter User Guide index, see:
• How to: configure the Minimum Filtering Level
• How to: use library categories in a profile: Global Group Profile

I. Override Account bypass

Use an Override Account to grant a user access to categories blocked at the root level. To grant designated users access to globally-blocked categories, set up an Override Account at the Global Group level, or enable the option to allow the Minimum Filtering Level to be bypassed with an Override Account, and then set up the Override Account at the group level.

To set up an override account at the Global Group level, go to:
* POLICY: Policy > Global Group > Override Account window

To configure the bypass feature and set up a group level override account, go to:
* POLICY: Policy > Global Group > Minimum Filtering Level > Min. Filter Bypass
* Policy > IP > group > Override Account window

In the Web Filter User Guide index, see:
• How to: set up an Override Account: Global Group
or:
• How to: configure the Minimum Filtering Level: Bypass Options
• How to: set up an Override Account: Group profile

J. Exception URL bypass

Use exception URLs to grant users access to URLs blocked at the root. To grant users access to globally-blocked URLs, enable the exception URL bypass option in the Minimum Filtering Level. For these users, add the exception URLs in their profiles.

To set up the Exception URL bypass for users to bypass blocked URLs, go to:
*   POLICY: Policy > Global Group > Minimum Filtering Level > Min. Filter Bypass
*   Policy > IP > member > Exception URL window

In the Web Filter User Guide index, see:
• How to: configure the Minimum Filtering Level: Bypass Options
• How to: set up Exception URLs

K. Proxy Patterns

Prevent users from using proxy patterns to bypass the Internet filter. Enable Pattern Blocking for all users. In the profile, block Security > Web-based Proxies/Anonymizers.

To set up the proxy pattern blocking feature and apply it to profiles, go to:
*   SYSTEM: System > Control > Filter window
*   POLICY: Policy > IP > member > member Profile > Category tab
    or POLICY: Policy > Global Group > Global Group Profile > Category tab

In the Web Filter User Guide index, see:
• How to: configure filtering
• How to: use library categories in a profile

L. File type blocking

Prevent users from downloading and using executable files that may threaten your network security. Create a custom category for file extensions and add ".exe" to the URL Keyword list. Other files you might include in the list are: .dll, .ocx, .scr, .bat, .pif, .cpl, .cmd, .hta, .lnk, .inf, .sys, .vbs, .vb, .wsc, .wsh, .wsf. Do NOT include ".com" in the list, or the files will not be found and blocked. In the applicable profiles, block this custom category and enable both URL Keyword Filter Control and extension options.

To set up file type blocking and apply this feature to profiles, go to:
*   LIBRARY: Library > Category Groups > Custom Categories > Add Category
*   Library > Custom Categories > category > URL Keywords
*   POLICY: Policy > IP > member > member Profile > Category tab, and Filter Options tab (URL Keyword Filter Control and extension options enabled)
    or POLICY: Policy > Global Group > Global Group Profile > Category tab, and Filter Options tab (URL Keyword Filter Control and extension options enabled)

In the Web Filter User Guide index, see:
• How to: set up a custom category
• How to: set up URL Keywords: Custom Categories
• How to: use library categories in a profile
• How to: set up profile options

II. *Bandwidth/Productivity*

A. Time Quota/Hit Quota

Limit time spent in PASSED categories to prevent excessive bandwidth usage and increase productivity. Enable the Quota Settings feature, and configure the Seconds Per Hit. Set up pertinent categories in the user's profile with quotas so the user is notified and then locked out of those categories after all minutes in the quota have been used.

To set up the quota feature and configure profiles to use this feature, go to:
• SYSTEM: System > Quota Setting window
• POLICY: Policy > IP > member profile > Category tab (Quota column)
   or Policy > Global Group > Global Group Profile > Category tab (Quota column)

In the Web Filter User Guide index, see:
• How to: set up Quotas
• How to: use library categories in a profile

B. Overall Quota

Restrict all quota time in a profile to improve bandwidth usage and productivity. Cap the amount of time a user spends in all quota-marked categories by enabling the Overall Quota option and specifying the number of minutes the end user can visit quota-marked categories before being notified and then locked out of these categories.

To set up the quota option and configure profiles to use the Overall Quota, go to:
• SYSTEM: System > Quota Setting window
• POLICY: Policy > IP > member profile > Category tab (Overall Quota)
   or Policy > Global Group > Global Group Profile > Category tab (Overall Quota)

In the Web Filter User Guide index, see:
• How to: set up Quotas
• How to: use library categories in a profile

C. Time Based Profiles

Schedule a profile to be used at a specific time. Set up one or more profiles for each user or group to be active at a scheduled time.

To set up Time Profiles, go to:
• POLICY: Policy > IP > member > Time Profile window

In the Web Filter User Guide index, see:
• How to: set up a Time Profile

D. Warn option with low filter settings

Warn users before they access unacceptable content that their Internet activities are logged. Set HTTPS filtering at the "low" level, and then configure the number of minutes for the interval the warning page will re-display for any user who attempts to access content deemed unacceptable. In the end user's profile, set the Warn categories.

To set up and use the warn option, go to:
- SYSTEM: System > Control > Filter window
- System > Warn Option Setting window
- POLICY: Policy > IP > member > member profile > Category tab (Warn column) or POLICY: Policy > Global Group > Global Group Profile > Category tab (Warn column)

In the Web Filter User Guide index, see:
• How to: configure filtering
• How to: configure the Warn Option Setting
• How to: use library categories in a profile

E. Warn-strike

Warn users before they access unacceptable content and may be locked out of the Internet. Enable the Warn feature along with X Strikes Blocking. After the end user is warned for the designated number of times defined in X Strikes Blocking, that user is locked out of all Internet/intranet access.

To set up and use the warn option with X Strikes Blocking, go to:
- SYSTEM: System > X Strikes Blocking window
- System > Warn Option Setting window
- POLICY: Policy > IP > member > member profile > Category Profile tab (Warn column), and Filter Options tab (X Strikes Blocking enabled) or POLICY: Policy > Global Group > Global Group Profile > Category tab (Warn column), and Filter Options tab (X Strikes Blocking enabled)

In the Web Filter User Guide index, see:
• How to: set up X Strikes Blocking
• How to: configure the Warn Option Setting
• How to: use library categories in a profile
• How to: set up profile options

F. P2P patterns

Block P2P services. Enable Pattern Blocking for all users. In the profile, block Bandwidth > Peer-to-peer/File Sharing category.

To block P2P services, go to:
- SYSTEM: System > Control > Filter window
- POLICY: Policy > IP > member > member profile > Category tab or POLICY: Policy > Global Group > Global Group Profile > Category tab

In the Web Filter User Guide index, see:
• How to: configure filtering
• How to: use library categories in a profile

G. IM patterns

Block IM services. Enable Pattern Blocking for all users. In the profile, block Internet Communication > Chat and Instant Messaging (IM) categories.

To block IM services, go to:
*   SYSTEM: System > Control > Filter window
*   POLICY: Policy > IP > member > member profile > Category tab
    or POLICY: Policy > Global Group > Global Group Profile > Category tab

In the Web Filter User Guide index, see:
• How to: configure filtering
• How to: use library categories in a profile

H. Game patterns

Block game patterns. Enable Pattern Blocking for all users. In the profile, block Entertainment > Games category.

To block game patterns, go to:
*   SYSTEM: System > Control > Filter window
*   POLICY: Policy > IP > member > member profile > Category tab
    or POLICY: Policy > Global Group > Global Group Profile > Category tab

In the Web Filter User Guide index, see:
• How to: configure filtering
• How to: use library categories in a profile

I. Streaming Media patterns

Block streaming media patterns. Enable Pattern Blocking for all users. In the profile, block Bandwidth > Streaming Media category.

To block streaming media patterns, go to:
*   SYSTEM: System > Control > Filter window
*   POLICY: Policy > IP > member > member profile > Category tab
    or POLICY: Policy > Global Group > Global Group Profile > Category tab

In the Web Filter User Guide index, see:
• How to: configure filtering
• How to: use library categories in a profile

J. Remote Access patterns

Block remote access patterns. Enable Pattern Blocking for all users. In the profile, block Internet Productivity > Remote Access category.

To block remote access patterns, go to:
- SYSTEM: System > Control > Filter window
- POLICY: Policy > IP > member > member profile > Category tab
  or POLICY: Policy > Global Group > Global Group Profile > Category tab

In the Web Filter User Guide index, see:
• How to: configure filtering
• How to: use library categories in a profile

K. HTTPS settings

Establish the security level for HTTPS site access. Configure HTTPS filter settings in the Filter window. Choose "None" if you do not want the Web Filter to filter HTTPS sites, "Low" if you want the Web Filter to filter HTTPS sites without having the Web Filter communicate with IP addresses or hostnames of HTTPS servers, "Medium" if you want the Web Filter to communicate with HTTPS servers in order to get the URL from the certificate for URL validation only (this is the default setting), or "High" if you want the Web Filter to communicate with HTTPS servers to obtain the certificate with a very strict validation of the return URL.

To configure HTTPS settings, go to:
- SYSTEM: System > Control > Filter window

In the Web Filter User Guide index, see:
• How to: configure filtering

L. Category block

Block the Bandwidth category. Set the Bandwidth category to be blocked in pertinent profiles.

To block the Bandwidth category, go to:
- POLICY: Policy > IP > member > member profile > Category tab
  or POLICY: Policy > Global Group > Global Group Profile > Category tab

In the Web Filter User Guide index, see:
• How to: use library categories in a profile

M. Rule block

Use a rule to block the Bandwidth category. Create a rule that blocks the Bandwidth category and apply this rule to pertinent profiles.

To create and block a rule for the Bandwidth category, go to:
*   POLICY: Policy > Global Group > Rules
*   Policy > IP > member > member profile > Category tab
    or Policy > Global Group > Global Group Profile > Category tab

In the Web Filter User Guide index, see:
• How to: use rules
• How to: use library categories in a profile

N. SE Keywords

Block specific search engine keywords to restrict access to bandwidth-consumptive categories. In pertinent library categories, enter URL keywords to be blocked. Block these categories in the profile.

To set up search engine keywords and block them in a profile, go to:
*   LIBRARY: Library > Category Groups > category group > category > Search Engine Keywords
*   POLICY: Policy > IP > member > member Profile > Filter Options tab (Search Engine Keyword Filter Control enabled)
    or POLICY: Policy > Global Group > Global Group Profile > Filter Options tab (Search Engine Keyword Filter Control enabled)

In the Web Filter User Guide index, see:
• How to: set up Search Engine Keywords
• How to: set up profile options

O. URL Keywords

Block specific URL keywords to restrict access to bandwidth-consumptive categories. In pertinent library categories, enter SE keywords to be blocked. Block these categories in the profile.

To set up and block URL keywords in a profile, go to:
*   LIBRARY: Library > Category Groups > category group > category > URL Keywords
*   POLICY: Policy > IP > member > member Profile > Filter Options tab (URL Keyword Filter Control enabled)
    or POLICY: Policy > Global Group > Global Group Profile > Filter Options tab (URL Keyword Filter Control enabled)

In the Web Filter User Guide index, see:
• How to: set up URL Keywords
• How to: set up profile options

P. Custom Block/Warn/X Strikes/Quota pages

Customize a block, warning, X Strikes, or quota pages. Modify page contents to point to a URL within your organization, send a request to your administrator's email address, or include verbiage of your choice that informs users of their Internet usage activities that triggered the page.

To customize pages, go to:
• SYSTEM: System > Customization > Common Customization window, and other applicable customization windows

In the Web Filter User Guide index, see:
• How to: customize pages

Q. Real Time Probe information

Monitor Internet usage activity in real time. Enable Real Time Probe reporting. Create a probe to monitor Internet traffic by category, user IP address, username, or URL. Set up a schedule for the probe to run during a specific time period.

To enable and use Real Time Probe reporting, go to:
• REPORTING: Report > Real Time Probe > Configuration tab
• Real Time Probe > Go to Real Time Probe Reports GUI link > Real Time Probe Reports > Create tab

In the Web Filter User Guide index, see:
• How to: set up Real Time Probes

III. General/Productivity

A. Warn Feature with higher thresholds

Warn users before they access unacceptable content. Set HTTPS filtering at the "high" level to block certificates that may be questionable. Configure Warning settings. In the end user's profile, apply the warn option to pertinent categories. The end user may not be able to access all requested sites due to high settings, and will receive the warning message for excessive Internet usage.

To set up and use the warn option with high filter settings, go to:
• SYSTEM: System > Control > Filter window
• System > Warn Option Setting window
• POLICY: Policy > IP > member profile > Category tab (Warn column)
  or POLICY: Policy > Global Group > Global Group Profile > Category tab (Warn column)

In the Web Filter User Guide index, see:
• How to: configure filtering
• How to: configure the Warn Option Setting
• How to: use library categories in a profile

B. Warn-strike with higher thresholds

Warn users before they access unacceptable content and may be locked out of the Internet. Set HTTPS filtering at the "high" level, configure Warning settings, and enable X Strikes Blocking. In the end user's profile, set the Warn categories, and enable X Strikes Blocking. The end user may not be able to access all requested sites due to high settings, and will receive the warning message for excessive Internet usage. After being warned for the designated number of times defined in X Strikes Blocking, that user is locked out of all Internet/Intranet access.

To set up and use the warn option, go to:
- SYSTEM: System > Control > Filter window
- System > X Strikes Blocking window
- System > Warn Option Setting window
- POLICY: Policy > IP > member > member profile > Category tab (Warn column), and Filter Options tab (X Strikes Blocking enabled)
  or POLICY: Policy > Global Group > Global Group Profile > Category tab (Warn column), and Filter Options tab (X Strikes Blocking enabled)

In the Web Filter User Guide index, see:
• How to: configure filtering
• How to: set up X Strikes Blocking
• How to: configure the Warn Option Setting
• How to: use library categories in a profile
• How to: set up profile options

C. Time Quota/Hit Quota

Limit time spent in PASSED categories to increase productivity. Enable the Quota Settings feature, and configure the Seconds Per Hit. Set up pertinent categories in the user's profile with quotas so the user is notified and then locked out of those categories after all minutes in the quota have been used.

To set up the Quota feature and use quotas in profiles, go to:
- SYSTEM: System > Quota Setting window
- POLICY: Policy > IP > member > profile > Category tab (Quota column)
  or POLICY: Policy > Global Group > Global Group Profile > Category tab (Quota column)

In the Web Filter User Guide index, see:
• How to: set up Quotas
• How to: use library categories in a profile

D. Time Based Profiles

Schedule a profile to be used at a specific time. Set up one or more profiles for each user or group to be active at a scheduled time.

To set up and use time profiles, go to:
- POLICY: Policy > IP > member > Time Profile window

In the Web Filter User Guide index, see:
• How to: set up a Time Profile

E. Overall Quota

Restrict all quota time in a profile to improve productivity. Cap the amount of time a user spends in all quota-marked categories by enabling the Overall Quota option and specifying the number of minutes the end user can visit quota-marked categories before being notified and then locked out of these categories.

To set up the quota option and configure profiles to use the Overall Quota, go to:
- SYSTEM: System > Quota Setting window
- POLICY: Policy > IP > member profile > Category tab (Overall Quota)
  or Policy > Global Group > Global Group Profile > Category tab (Overall Quota)

In the Web Filter User Guide index, see:
• How to: set up Quotas
• How to: use library categories in a profile

F. Customize an M86 Supplied Category

Include region-specific content in an M86 Supplied category. Add/delete content to/from an existing M86 Supplied Category that only includes content pertinent to your organization or region that should be blocked. Apply this category to a profile.

To customize and use an M86 Supplied Category in a profile, go to:
- LIBRARY: Library > Category Groups > category group > category (add/delete URLs, URL Keywords, Search Engine Keywords)
- POLICY: Policy > IP > member > member profile > Category tab
  or POLICY: Policy > Global Group > Global Group Profile > Category tab

In the Web Filter User Guide index, see:
• How to: set up URLs in categories: M86 Supplied Categories
• How to: use library categories in a profile

G. Local category adds/deletes

Include region-specific content in a Custom category. Set up a custom category that only includes content pertinent to your organization or region that should be blocked. Apply this category to a profile.

To create a Custom Category and use it in a profile, go to:
- LIBRARY: Library > Category Groups > Custom Categories > Add Category (add URLs, URL Keywords, Search Engine Keywords)
- POLICY: Policy > IP > member > member profile > Category tab
  or POLICY: Policy > Global Group > Global Group Profile > Category tab

In the Web Filter User Guide index, see:
• How to: set up a custom category
• How to: use library categories in a profile

H. Custom Block/Warn/X Strikes/Quota pages

Customize a block, warning, X Strikes, or quota pages. Modify page contents to point to a URL within your organization, send a request to your administrator's email address, or include verbiage of your choice that informs users of their Internet usage activities that triggered the page.

To customize pages, go to:
*   SYSTEM: System > Customization > Common Customization window, and other applicable customization windows

In the Web Filter User Guide index, see:
• How to: customize pages

IV. Pass/Allow

A. Always Allow Custom Category

Create a white list custom category. Set up an Always Allow category and add all URLs deemed acceptable. Apply this category to all pertinent profiles. Please keep in mind that if any library category in this list is set up to be blocked in the Minimum Filtering Level, the Minimum Filtering Level setting will override the entry in the Always Allow custom category.

To create a white list custom category and use it in a profile, go to:
*   LIBRARY: Library > Category Groups > Custom Categories > Add Category (add URLs, URL Keywords, Search Engine Keywords)
*   POLICY: Policy > IP > member > member profile > Category tab
    or POLICY: Policy > Global Group > Global Group Profile > Category tab

In the Web Filter User Guide index, see:
• How to: set up a custom category
• How to: use library categories in a profile

B. URL exceptions

Use Exception URLs to let specified individuals bypass the Minimum Filtering Level. Enable the option to bypass the Minimum Filtering Level using exception URLs. Enter the exception URLs in the applicable profile.

To set up the Exception URL bypass for users to bypass blocked URLs, go to:
*   POLICY: Policy > Global Group > Minimum Filtering Level > Min. Filter Bypass
*   Policy > IP > member > Exception URL window

In the Web Filter User Guide index, see:
• How to: configure the Minimum Filtering Level: Bypass Options
• How to: set up Exception URLs

C. IP exceptions

Use Exception URLs to grant individuals access to IPs blocked by the Minimum Filtering Level. Enable the option to bypass the Minimum Filtering Level using exception URLs. Enter the exception Internet/intranet IP addresses in the applicable profile.

To set up the Exception URL bypass for bypassing blocked IP addresses, go to:
• POLICY: Policy > Global Group > Minimum Filtering Level > Min. Filter Bypass
• Policy > IP > member > Exception URL window

In the Web Filter User Guide index, see:
• How to: configure the Minimum Filtering Level: Bypass Options
• How to: set up Exception URLs

D. Override Accounts

Set up override accounts to grant specified users access to URLs blocked for general users. Enable the option to bypass the Minimum Filtering Level using an override account. Create the override account profile, including the accessible categories. To grant designated users access to globally-blocked categories, set up an Override Account at the Global Group level, or enable the option to allow the Minimum Filtering Level to be bypassed with an Override Account, and then set up the Override Account at the member level.

To set up an override account at the Global Group level, go to:
• POLICY: Policy > Global Group > Override Account window

To configure the bypass feature and set up a group level override account, go to:
• POLICY: Policy > Global Group > Minimum Filtering Level > Min. Filter Bypass
• Policy > IP > group > Override Account window

In the Web Filter User Guide index, see:
• How to: set up an Override Account: Global Group
or:
• How to: configure the Minimum Filtering Level: Bypass Options
• How to: set up an Override Account: Group profile

E. Pattern detection bypass

Allow specific IP addresses to always bypass filtering. Block all patterns with the exception of a list of specific IP addresses that should always bypass the filter.

To set up pattern detection whitelisting, go to:
• SYSTEM: System > Control > Filter window
• LIBRARY: Library > Pattern Detection Whitelist

*In the Web Filter User Guide index, see:*
• How to: configure filtering
• How to: set up pattern detection whitelisting

LED INDICATORS AND BUTTONS

SL and MSA Units

Front LED Indicators and Buttons for Hardware Status Monitoring
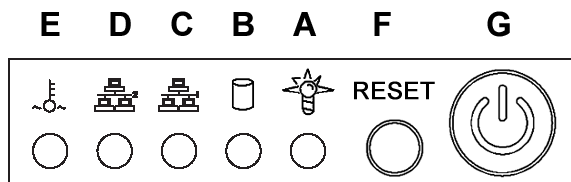
LED indicators and buttons for hardware status monitoring display on the front panel, located on the right side of the SL and MSA chassis (see diagrams below).

LED Indicator Key

PWR = Power
HD = HDD Activity
NIC1 = LAN 1
NIC2 = LAN 2
OH = Overheat
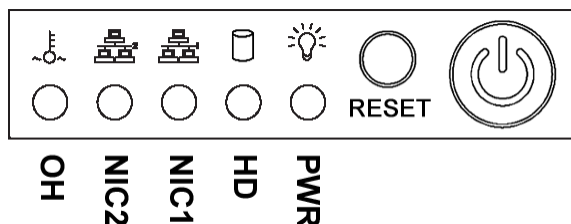
SL chassis control panel

LED Indicator Key   **Button Key**

A = Power   F = Reset
B = HDD Activity   G = Power
C = LAN 1
D = LAN 2
E = Overheat

MSA chassis control panel

LED indicators alert you to the status of a feature on the unit while buttons let you perform a function on the unit.

LED Indicator	Color	Condition	Description
Power	Green	On	System On
	--	Off	System Off
HDD	Amber	Blinking	HDD Activity
	--	Off	No HDD Activity
LAN 1 & LAN 2	Green	On	Link Connected
	--	Blinking	LAN Activity
	--	Off	Disconnected
Overheat	Red	On	System Overheated
	--	Off	System Normal

HL Unit

Front LED Indicators and Buttons for Hardware Status Monitoring

On an HL unit, the following control panel buttons, icons, and LED indicators for hardware status monitoring display on the right side of the front panel:
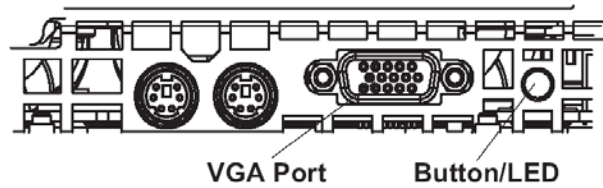
LED Indicator Key

PWR = Power
HD = HDD Activity
NIC1 = LAN 1
NIC2 = LAN 2
OH = Overheat
UID = Unique IDentifier
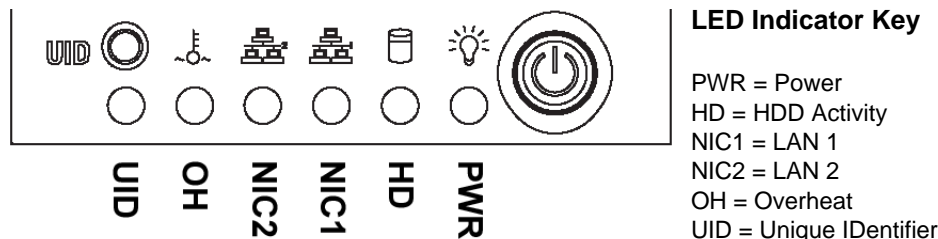
HL chassis control panel

The buttons and LED indicators for the depicted icons function as follows:

UID (button) – On an HL unit, when the UID button is pressed, a steady blue LED displays on both the front and rear of the chassis (see also Rear of chassis). These indicators are used for easy location of the chassis in a large stack configuration. The LED remains on until the button is pressed a second time.

Overheat/Fan Fail (icon) – This LED is unlit unless the chassis is overheated. A flashing red LED indicates a fan failure. A steady red LED (on and not flashing) indicates an overheating condition, which may be caused by cables obstructing the airflow in the system or the ambient room temperature being too warm.

NIC2 (icon) – A flashing green LED indicates network activity on LAN2.

NIC1 (icon) – A flashing green LED indicates network activity on LAN1.

HDD (icon) – In addition to displaying in the control panel, this icon also displays on the front panel on each hard drive carrier. A green LED indicates hard drive activity. An unlit LED on a drive carrier may indicate a hard drive failure.

Power (icon) – The LED is unlit when the server is turned off. A steady green LED indicates power is being supplied to the unit's power supplies. (See also Rear of chassis.) A steady amber LED—or an unlit LED—may indicate a disconnected or loose power supply cord.

Power (button) – When the power button is pressed, the main power to the server is turned on. When the power button is pressed again, the main power to the server is removed but standby power is still supplied to the server.

Rear LED Indicators for Hardware Status Monitoring

UID (LED indicator) – On the rear of the HL chassis, to the left of the power supplies, a steady blue UID LED indicator displays when the UID button on the control panel is pressed. This LED remains lit until the UID button is pressed again.

Power Supplies (LED indicators) – The power supplies are located at the right on the rear of the chassis. An LED indicator is located above each of the power plugs.
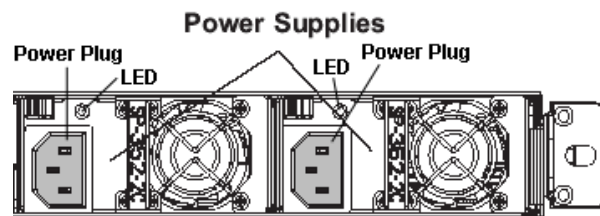
HL and SL Units

Front LED Indicators for Software and Hardware Status Monitoring

On an HL or SL unit, the following LED indicators for software and hardware status monitoring display on the left side of the front panel:

○ **FLTR**
○ **LIBR**
○ **RAID**
○ **UPDT**

LED Indicator Key

FLTR = Filtering Status
LIBR = Library Update Status
RAID = Hard Drive Status
UPDT = Software Update Status

left side of the front panel

Below is a chart of LED indicators in the "SL" and "HL" unit:

LED Indicator	Color	Condition	Description
FLTR	Green	On	Filtering traffic
	Amber	On	Library being uploaded or one or more processes being started
	Red	On	Not filtering traffic
LIBR	Green	On	Library updated within the past two days or less
	Amber	On	Library updated more than two days ago, but within the past three days
	Red	On	Library updated more than three days ago
RAID	Green	On	RAID mode enabled and running
	--	Off	RAID mode is inactive
	Red	On	Hard drive fault or failure
UPDT	Amber	On	Software update detected
	--	Off	No software update detected

REGULATORY SPECIFICATIONS AND DISCLAIMERS

Declaration of the Manufacturer or Importer

Safety Compliance

USA:	UL 60950-1 2nd ed. 2007
Europe:	Low Voltage Directive (LVD) 2006/95/EC to CB Scheme EN 60950: 2006
International:	UL/CB to IEC 60950-1:2006

Electromagnetic Compatibility (EMC)

USA:	FCC CFR 47 Part 15, Verified Class A Limit
Canada:	IC ICES-003 Class A Limit
Europe:	EMC Directive, 2004/108/EC & Low Voltage Directive (LVD) 2006/95/EC
Taiwan:	Bureau of Standards and Metrology Inspection (BSMI), CNS 13438: 2006

Federal Communications Commission (FCC) Class A Notice (USA)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Declaration of Conformity

Models: HL-005-001, HL-015-001, SL-004-001, SL-014-001, MSA-004-001

Electromagnetic Compatibility Class A Notice

Industry Canada Equipment Standard for Digital Equipment (ICES-003)

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sure le matériel brouilleur du Canada.

English translation of the notice above:

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Bureau of Standards Metrology and Inspection (BSMI) - Taiwan

BSMI EMC STATEMENT -- TAIWAN

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成設頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

EC Declaration of Conformity

European Community Directives Requirement (CE)

Declaration of Conformity

Manufacturer's Name:	8e6 Technologies
Manufacturer's Address:	828 W. Taft Avenue
	Orange, CA 92865

Application of Council Directive(s):	Low Voltage	• 2006/95/EC
	EMC	• 2004/108/EC

Standard(s):	Safety	• EN60950: 2006
	EMC	• EN55022: 2006
		• EN55024: 1998 +A2:2003
		• EN61000-3-2: 2000
		• EN61000-3-3: 2001

Product Name(s):	Internet Appliance
Product Model Number(s):	HL-005-001, HL-015-001, SL-004-001, SL-014-001, MSA-004-001
Year in which conformity is declared:	2008

All hardware components supplied in this unit's shipping carton are certified by our vendors to be RoHS compliant.

I, the undersigned, hereby declare that the equipment specified above conforms to the above Directive(s) and Standard(s).

Location:	Orange, CA, USA	Signature:	
Date:	January 21, 2008	Full Name:	Gregory P. Smith
		Position:	Director of Engineering Operations

APPENDIX: CONSOLE SETUP PROCEDURES

The steps in this appendix provide an alternative way to install the Web Filter on your network, by using a crossover cable and configuring the application via the user interface.

Preliminary Setup

Create a "setup workstation" using a Windows-based laptop or desktop machine with a network card and Internet Explorer 8 (or later). The setup workstation will be used for accessing the HL, SL, or MSA server on the network and configuring the unit.

NOTE: The Java Plug-in version specified for the Web Filter software version must be installed on your workstation. If your workstation does not have Java Runtime Environment, you will be prompted to install it.

Workstation Configuration

A. From the desktop of the setup workstation, while logged in with Administrator privileges, follow the procedures for your machine type:

- **Windows XP**: Go to Start > Control Panel. Open Network Connections. Right-click the link for LAN or High-Speed Internet and choose Properties.

- **Windows Vista**: Go to the start icon > Control Panel > Network and Internet > Network and Sharing Center > Manage network connections. Right-click the Local Area Connection you want to change, then choose Properties.

- **Windows 7**: Go to the start icon > Control Panel. In the search box, type *adapter*. Under Network and Sharing Center, choose View network connections. Right-click the Local Area Connection you want to change, then choose Properties.

B. On a Windows XP machine, click on **Internet Protocol (TCP/IP)** to highlight it. On a Windows Vista or Windows 7 machine, go to the Networking tab. Under This connection uses the following items, choose **Internet Protocol Version 4 (TCP/IPv4)** to highlight it.

C. Click the **Properties** button.

WARNING: Be sure to make note of the current network settings on the setup workstation as you will need to return them for further setup procedures.

D. Choose the option **Use the following IP address**.

E. Type in the **IP address** of 1.2.3.1.

F. Type in the **Subnet mask** (netmask) of 255.0.0.0 and click **OK**.

G. Close the LAN connection properties box.

Link the Workstation to the HL, SL, MSA

The procedures outlined in this sub-section require the use of a CAT-5E crossover cable.

A. Plug one end of the CAT-5E crossover cable into the HL, SL, or MSA's **LAN 2** port.

NOTE: *When facing the rear of the chassis, the LAN 2 port is the port on the right.*

Portion of SL and MSA chassis rear

Portion of HL chassis rear

B. Plug the other end of the CAT-5E crossover cable into the setup workstation's network card.

C. Connect the AC power cord(s) to the back of the chassis.

D. Plug the HL, SL, or MSA into a power source with an appropriate rating.

WARNING: *It is strongly suggested you use an uninterruptible power supply.*

E. Power on the server by lowering the bezel and pressing the large button at the right of the front panel (see diagrams below):
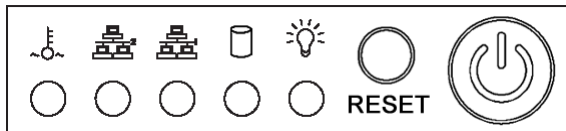
Diagram of SL chassis front panel, power button at far right
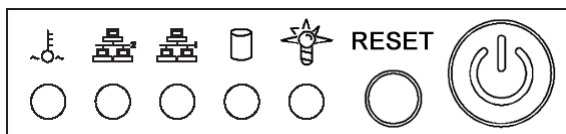
Diagram of MSA chassis front panel, power button at far right
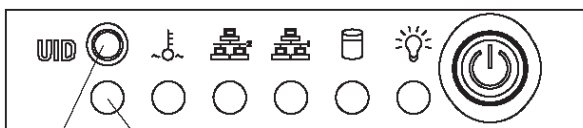
Button   LED

Diagram of HL chassis front panel, power button at far right

The Boot Up Process

The boot-up process may take 5 - 10 minutes. When the drive light remains off for 30 seconds, the system is booted up. (See the LED Indicators and Buttons section for a description of front panel LED indicators and buttons.)

If you wish to verify that the unit has been booted up, you can perform the following test on your workstation:

1. On a Windows XP, Vista, and 7 machine, go to your taskbar and click **Start > All Programs > Accessories > Command Prompt**.
2. Type in *ping 1.2.3.4*
3. Press **Enter** on your keyboard.

If you receive a reply, the unit is up.

Security Certificate Acceptance Procedures

A. From the workstation you are using, launch an Internet supported browser such as:

- Firefox 9 or 10
- Internet Explorer 8 or 9
- Safari 5.0 or 5.1
- Google Chrome 16 or 17

B. Type in **https://1.2.3.4:1443** in the address field.

C. Click **Go** to display the security issue page:

- If using Firefox, proceed to Accept the Security Certificate in Firefox.
- If using IE, proceed to Temporarily Accept the Security Certificate in IE.
- If using Safari, proceed to Accept the Security Certificate in Safari.

Accept the Security Certificate in Firefox

A. If using a Firefox browser, in the page "This Connection is Untrusted," click the option **I Understand the Risks**:
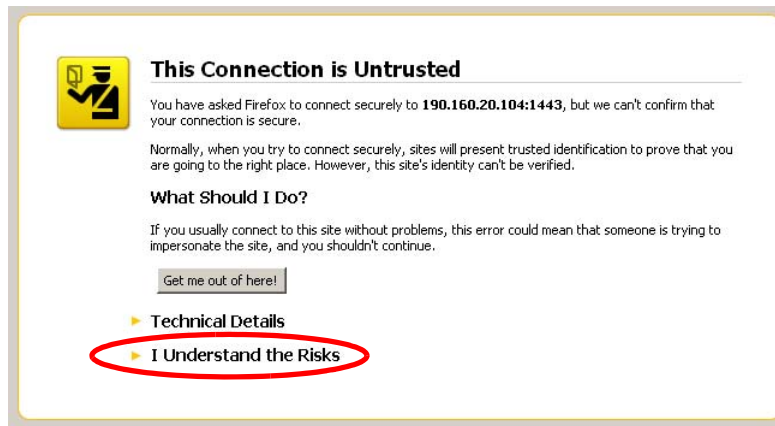
B. In the next set of instructions that display, click **Add Exception...**:
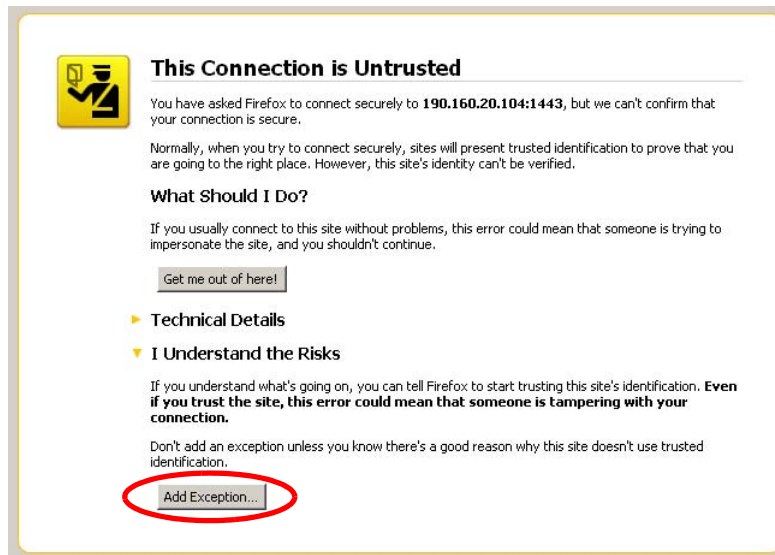
Clicking Add Exception opens the Add Security Exception window:
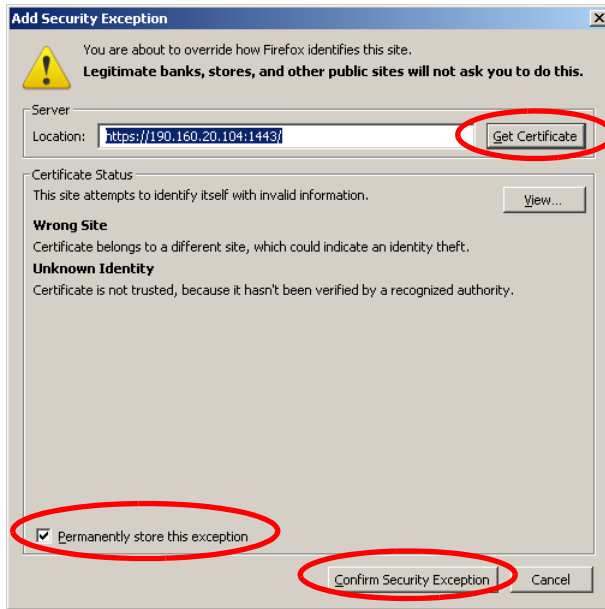
C. In the Add Security Exception window, click **Get Certificate** and wait a few seconds until the security certificate is obtained by the server.

D. With the checkbox **Permanently store this exception** selected, click **Confirm Security Exception** to open the Security warning dialog box:
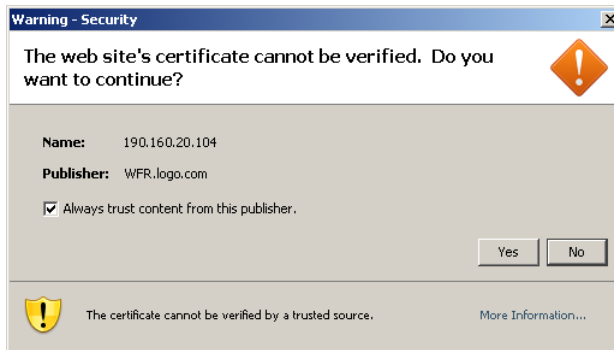
E. With the checkbox "Always trust content from this publisher." populated, click **Yes** to close the Security warning dialog box and to access the login window of the Web Filter user interface:
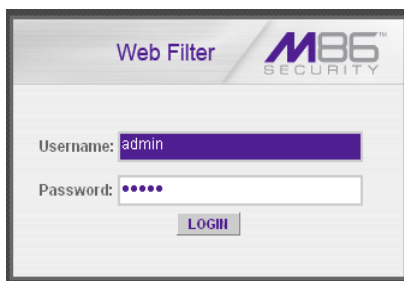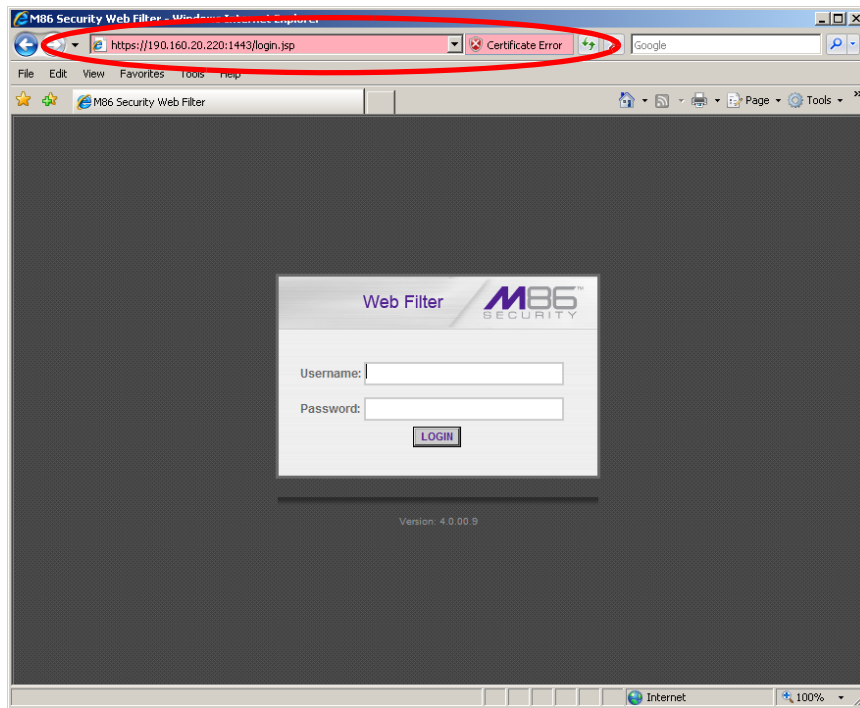
Temporarily Accept the Security Certificate in IE

If using an IE browser, in the page "There is a problem with this website's security certificate.", click **Continue to this website (not recommended)**:
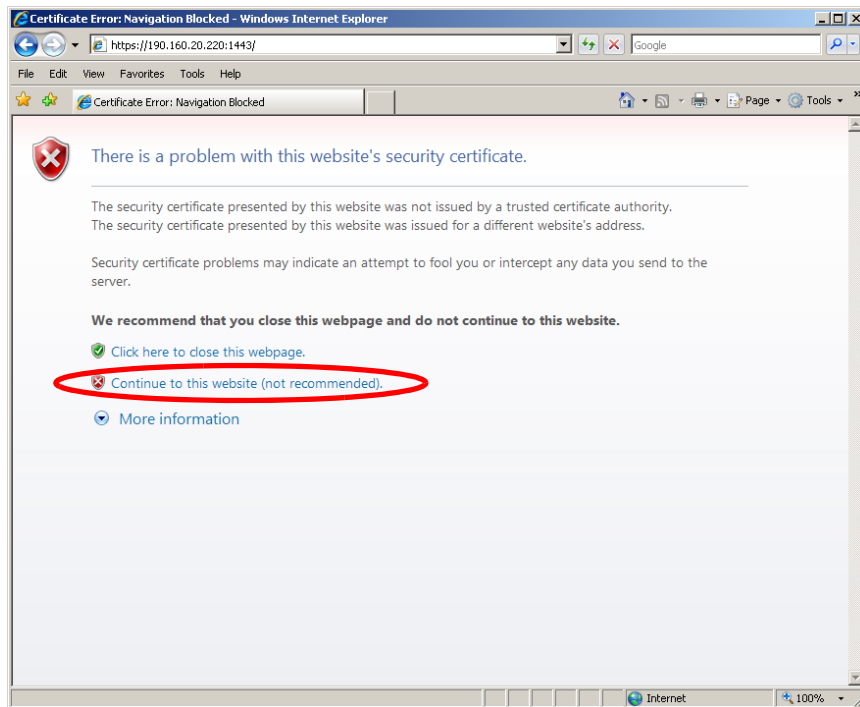
Selecting this option displays the Web Filter login page with the address field and the Certificate Error button to the right of the field shaded a reddish color:
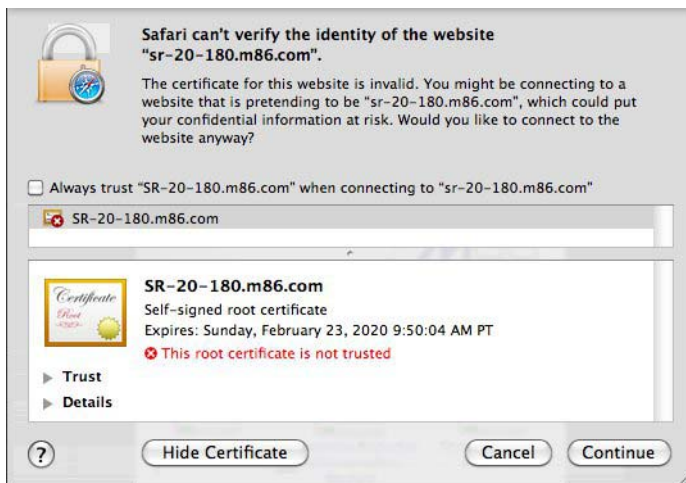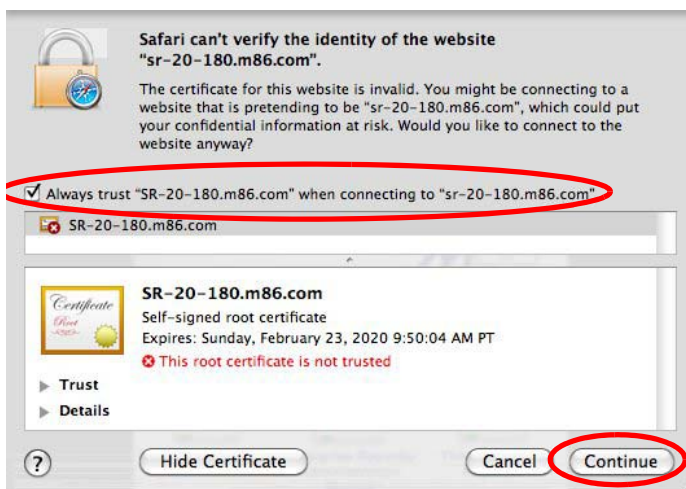
Accept the Security Certificate in Safari

A. If using a Safari browser, the window explaining "Safari can't verify the identity of the website..." opens:

Click **Show Certificate** to open the certificate information box at the bottom of this window:

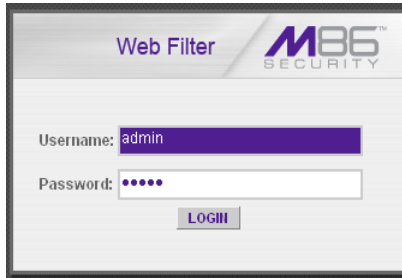B. Click the "Always trust..." checkbox and then click **Continue**:

C. You will be prompted to enter your password in order to install the certificate.

Network Setup

For this step, you will need your network administrator to provide you the host name, gateway address, and two unused IP addresses.
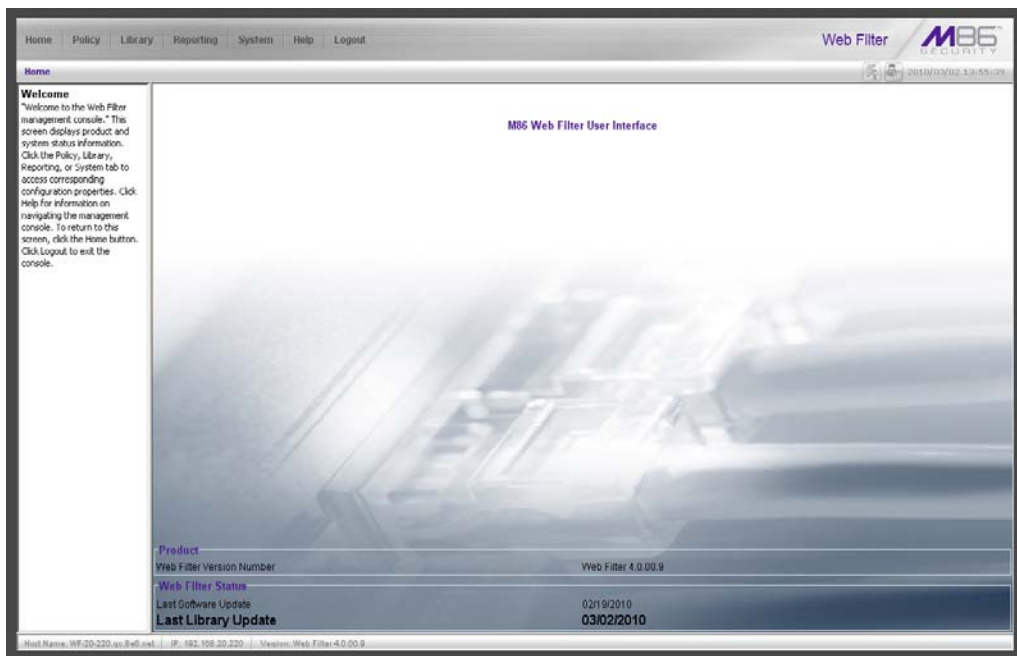
Access the Web Filter Administrator Console

A. In the **Username** field, type in *admin*.

B. In the **Password** field, type in *user3*.

C. Click **LOGIN** to go to the main screen of the Web Filter Administrator console:

Network

Click the **System** link at the top of the screen to go to the System section of the console:


In this section of the console you will:

- Specify the operation mode the Web Filter will use for filtering the network, listening to traffic, and sending traffic
- Configure LAN settings the Web Filter will use on your network
- Select NTP servers the Web Filter will use for time synchronization with Internet clocks
- Indicate the region in which the Web Filter is geographically located

*NOTE: After saving your entries in each of these windows (Operation Mode, LAN Settings, NTP Servers, Regional Setting), you may be prompted to restart or reboot the server. Click **OK** to acknowledge the contents of the alert box, and then proceed to the next sub-step **without** restarting or rebooting the server.*

Network: Operation Mode

From the navigation panel at the left of the screen, click Mode and choose Operation Mode from the menu:
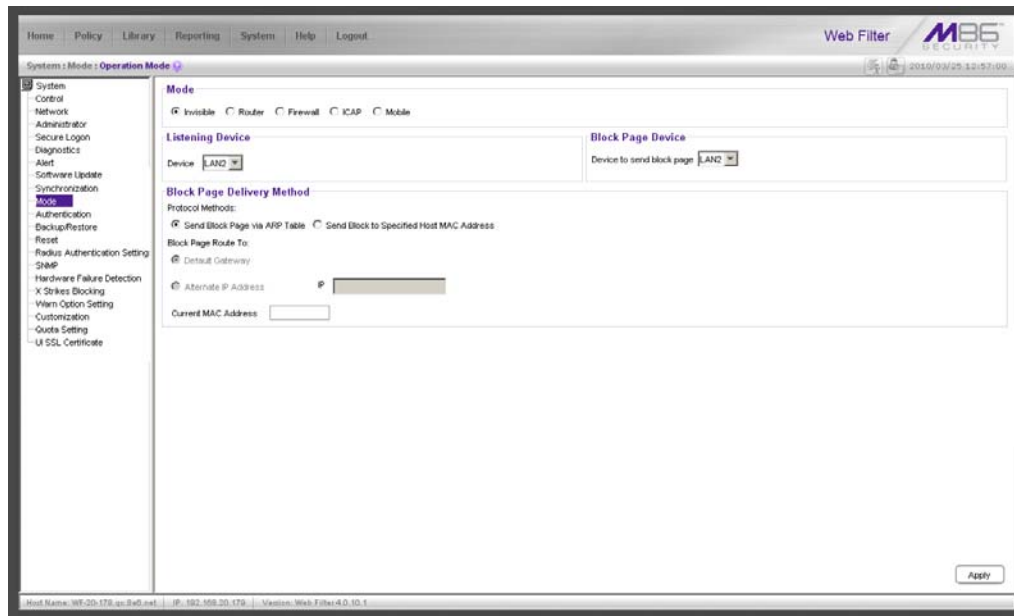
Make the following entries in the Operation Mode window:

A. In the Mode frame, select the operational mode the Web Filter will use for filtering: Invisible, Router, Firewall, Mobile, or ICAP.

NOTE: Refer to the appendix in the Web Filter User Guide for information on configuring the Web Filter to use the Mobile mode option with the Mobile Client.

B. In the Listening Device frame, select the device for listening to traffic:

- **For the invisible mode**: "LAN1" is generally used as the default listening device
- **For the router or firewall mode**: Select the network card that will be used to "listen to"—as opposed to "send"—traffic on the network

C. In the Block Page Device frame, select the device for sending block pages to client PCs:

- **For the invisible mode**: The block page device should be a different device than the one selected in the Listening Device frame—"LAN2" is generally used as the default device for sending block pages
- **For the router or firewall mode**: The device should be the same as the one selected in the Listening Device frame

D. Click **Apply**.

Network: LAN Settings

From the navigation panel, click Network and choose LAN Settings from the menu:

Make the following entries for the Web Filter in the LAN Settings window:

A. Enter the **Host Name** that includes your domain name, for example FILTER.myserver.com (the NetBIOS name must be capitalized). It is important to enter something identifiable, because once the product is registered, this host name is used by M86 Security to recognize your account for library updates. This name needs to be a valid DNS entry.

NOTE: *The entry made in this field should not include any spaces, and can only include alphanumeric characters and the following symbols: underscore (_), dash (-), and period (.).*

B. Enter the **LAN1 IP** address and specify the subnet for LAN 1, the Web Filter's first Ethernet Network Interface Card (NIC).

For the invisible mode, you may use a non-routeable IP address for the listening interface and a subnet mask of 255.255.255.255 (32 bites).

C. Enter the **LAN2 IP** address and subnet for LAN 2, the Web Filter's second Ethernet NIC. The subnet selection is usually 255.255.0.0 (16 bites) or 255.255.255.0 (24 bites), but cannot be ***255.255.255.255 (32 bites)***.

For the router or firewall mode, the LAN 1 IP address should be in a different subnet than the LAN 2 IP address.

WARNING: *For the router and firewall mode, do not use the same subnet for LAN 1 and LAN 2 or the console will become inaccessible.*

D. Enter the **Primary IP** address of the first DNS name server. The Web Filter uses this name server to resolve the domain name requested by users from the LAN.

E. Enter the **Secondary IP** address of the second DNS name server. The Web Filter will use this name server to resolve the domain name requested by users from the LAN if the first DNS isn't working.

F. Enter the **Gateway IP** address for the default router or firewall that is the main gateway for the entire network. The Web Filter will use this IP address to communicate outside the network.
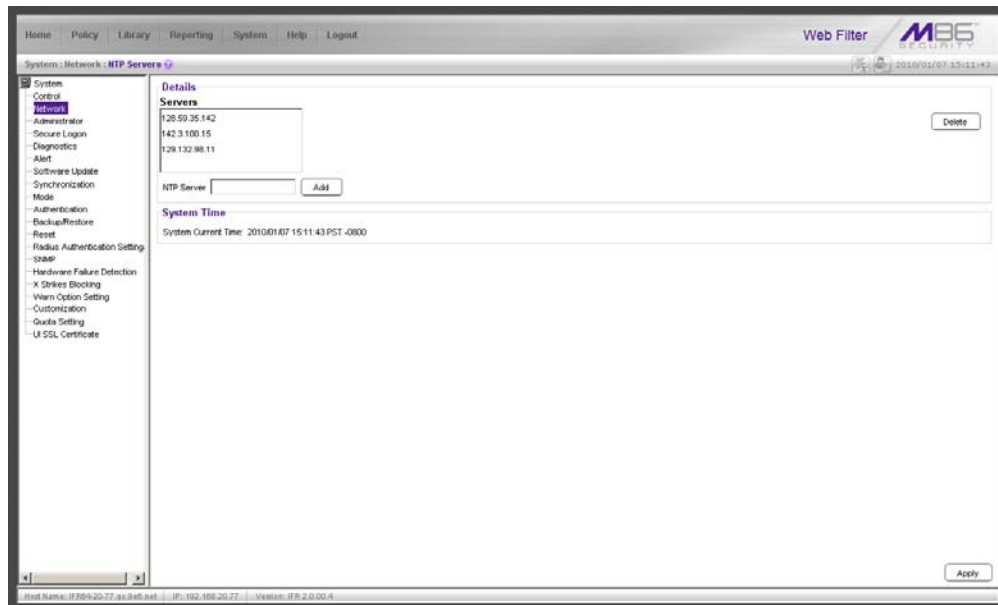
⚠️ *WARNING: Be sure to take note of the LAN 1 and LAN 2 IP addresses and host name you assigned to the Web Filter. It is strongly suggested you document and store this information as it is now the only way of communicating with the Web Filter.*

G. Click **Apply**.

Network: NTP Servers

From the navigation panel, click Network and choose NTP Servers from the menu:

The NTP Servers window is used for specifying the Network Time Protocol (NTP) servers to be used by the Web Filter, so that the Web Filter is synchronized with computer clocks on the Internet.

Note that the following server IP addresses display in the Servers list box: 128.59.35.142, 142.3.100.15, 129.132.98.11. If necessary, any of these servers can be deleted by selecting the IP address and clicking **Delete**.

📝 *NOTE: If you need to find another NTP server to use, most university Web sites provide these servers for public usage.*

A. In the **NTP Server** field, enter the IP address of the primary NTP server you wish to use for clock settings on your server.

B. Click **Add** to include this IP address in the Servers list box.

C. Enter two more NTP servers, following the procedures in sub-steps A and B. These will be the secondary and tertiary NTP servers, in order as they appear in the list box.

D. Click **Apply**.

📝 *NOTE: If the primary server fails, the secondary will be used. If the secondary server fails, the tertiary server will be used.*

Network: Regional Setting

From the navigation panel, click Network and choose Regional Setting from the menu:
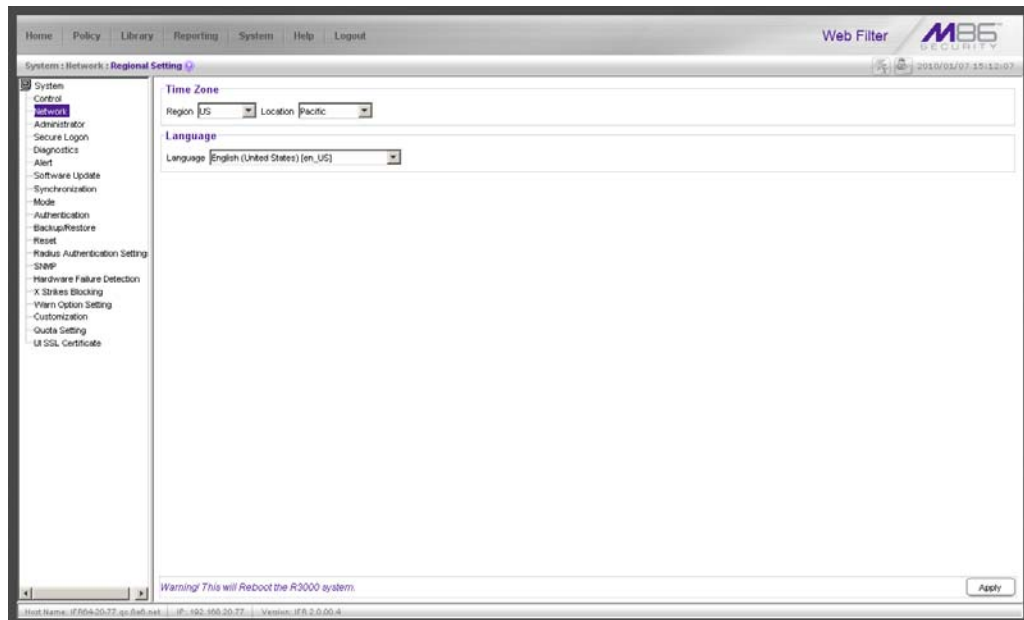
Make the following selections in the Regional Setting window:

A. At the **Region** pull-down menu, select your country from the available choices.

B. At the **Location** pull-down menu, select the time zone for the specified region.

If necessary, select a language set from the **Language** pull-down menu to display that text in the console.

C. Click **Apply** to apply your settings, and to reboot the Web Filter.

# Physically Connect the Web Filter to the Network

Now that your Web Filter network parameters are set, you can physically connect the unit to your network. This step requires two standard CAT-5E cables.

NOTE: This section requires you to restart the Web Filter. If you wish to relocate the Web Filter before connecting it to the network, you must first shut down the server instead of restarting it. To shut down the Web Filter, go to the navigation panel, click Control, and then select ShutDown. Once the server is shut down, you must power on the Web Filter and then log back into the Administrator console.

A. Restart the server using the steps defined below (i-iii). These steps must always be performed when restarting the Web Filter. *Never* reset the server by using the power or reset buttons.

   i. From the navigation panel of the System section of the console, click Control and select Reboot from the menu to display the Reboot window.

   ii. Click the **Reboot** button.

   iii. From the time you click Reboot, you have approximately 2 minutes to perform sub-steps B through E while the Web Filter goes through the reboot process.

B. Disconnect the crossover cable from the Web Filter.

C. Plug one end of a standard CAT-5E cable into the Web Filter's LAN 1 port.

D. Plug the other end of the CAT-5E cable into an open port on the network hub that handles the Internet traffic you wish to filter.

E. Repeat sub-steps B and C for the Web Filter's LAN 2 port.

Portion of SL and MSA chassis rear
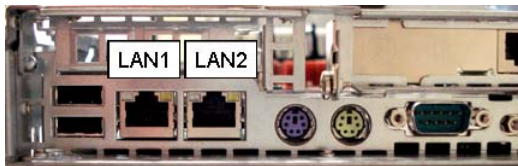
Portion of HL chassis rear

F. Wait until the reboot process has completed, indicated by the drive light staying off for 30 seconds. This process may take 5 to 10 minutes.

NOTES: If you receive a connection failure message during the reboot process, please disregard it, as this often occurs when there is a change in the IP address.

To restart the browser window, close the Web Filter Administrator console. Begin a new session by opening a new browser window and then logging back into the Administrator console.

Test the Web Filter Console Connection

Now that the Web Filter is physically installed on your network and you have configured its network settings, you need to test the unit to see if it is set up properly.

A. Restore the setup workstation you used for the Network Setup to its original settings, and connect it to the network hub to create a "network workstation." (You could also use another workstation already on the network that has Internet access.)

B. Launch a supported Internet browser on the network workstation, and enter the IP address you assigned to LAN 1 (Network: LAN Settings, sub-step B). Be sure to include the port information **:1443** for a secure connection, appended by "/login.jsp" in the address field. For example, if the Web Filter was assigned an IP address of 10.10.10.10, you would enter **https://10.10.10.10:1443/login.jsp** in the browser window's address field.

C. Click **Go**. You should be prompted to log into the Administrator console, giving the Username and Password.

If you can access the Web Filter Administrator console, the Web Filter is functioning on your network and you should proceed to Step 4: Log in, Generate SSL Certificate, from the Install the Server portion of this Installation Guide.

If you cannot access the Web Filter Administrator console, please verify the status of the LAN connection in Windows on the network workstation, and then try enabling/disabling the LAN connection. If that fails to work, check the following:

- The Web Filter is turned on.
- The Web Filter is connected to the same hub as your router/firewall.
- Can the PC normally connect to the Internet?
- Is the PC able to ping LAN 1 of the Web Filter?
- Is the Web Filter plugged into a switch instead of a hub?
- Is there a caching server?
- Can the Web Filter ping the filtered PC? (Refer to the System Command window in the Diagnostics section of the Web Filter User Guide)
- Did you restart the Web Filter after changing the network settings?
- Do you have both LAN ports connected to your network hub?
- If still unsuccessful, contact an M86 Security solutions engineer or technical support representative.

D. Once you are able to access the Web Filter Administrator console, proceed to Step 4: Log in, Generate SSL Certificate.

INDEX

A

Activate and Register the Web Filter *63*
activation code *63*
Always Allow Custom Category *81*

B

Bandwidth/Productivity *73*
Boot Up *93*
BSMI *87*, *89*

C

Category block *69*, *76*
Change Quick Start password *37*
crossover cable *4*, *92*
Custom Block/Warn/X Strikes/Quota pages *78*, *81*
Custom Category (blocked) *71*
Custom Lock, Block, Warn, X Strikes, Quota pages *70*
Customize an M86 Supplied Category *80*

E

EMC *87*
Exception URL bypass *72*

F

FCC *87*
File type blocking *72*

G

Game patterns *75*
General/Productivity *78*

H

hardware specifications *4*
HL *4*, *7*, *22*, *24*, *27*, *28*, *29*, *46*, *84*, *85*, *86*, *92*, *105*
HTTPS settings *76*
HyperTerminal Setup *30*

I

ICES-003 *87*, *89*
IM patterns *75*
Install Bezel *22*
IP exceptions *82*

L

LCD Panel *27*, *39*
Local category adds/deletes *80*

About Trustwave®

Trustwave is a leading provider of information security and compliance management solutions to large and small businesses throughout the world. Trustwave analyzes, protects and validates an organization's data management infrastructure from the network to the application layer—to ensure the protection of information and compliance with industry standards and regulations such as the PCI DSS and ISO 27002, among others. Financial institutions, large and small retailers, global electric exchanges, educational institutions, business service firms and government agencies rely on Trustwave. The company's solutions include on-demand compliance management, managed security services, digital certificates and 24x7 multilingual support. Trustwave is headquartered in Chicago with offices throughout North America, Central and South America, Europe, the Middle East, Africa, and Asia-Pacific.