



M86 Web Filter
INSTALLATION GUIDE
Models: 300, 500, 700

M86 WEB FILTER INSTALLATION GUIDE FOR 300, 500, 700 MODELS

© 2011 M86 Security

All rights reserved. Printed in the United States of America

Local: 714.282.6111 • Domestic U.S.: 1.888.786.7999 • International: +1.714.282.6111

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form without prior written consent from M86 Security.

Every effort has been made to ensure the accuracy of this document. However, M86 Security makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. M86 Security shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. Due to future enhancements and modifications of this product, the information described in this documentation is subject to change without notice.

Trademarks

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Part# WF-IG-110121

CONTENTS

M86 WF APPLIANCE INTRODUCTION	1
About this Document.....	2
Conventions Used in this Document.	2
SERVICE INFORMATION	3
M86 Technical Support Call Procedures.	3
PRELIMINARY SETUP PROCEDURES	4
Unpack the Unit from the Carton.....	4
Select a Site for the Server.....	5
300 Series Server Setup Procedures	5
Set Top Applications	5
Optional 1U 2-Unit Tray Kit Applications	5
Rack Mount the Server.	6
Rack Setup Precautions	6
Rack Mount Instructions for 500 Series Servers	7
Rack Setup Suggestions	7
Install the Inner Slides	7
Install the Outer Slides	7
Install the Slide Assemblies to the Rack	8
Install the Chassis into the Rack	9
Rack Mount Instructions for 700 Series Servers	10
Rack Setup Suggestions	10
Identify the Sections of the Rack Rails	10
Install the Inner Rails	11
Install the Outer Rails	11
Install the Server into the Rack	13
Install the Server into a Telco Rack	14
Install the Bezel on the 500 and 700 Series Chassis	15
Check the Power Supply.	16
Power Supply Precautions	16
General Safety Information.	16
Server Operation and Maintenance Precautions	16
AC Power Cord and Cable Precautions	17
Electrical Safety Precautions	17
Motherboard Battery Precautions	18
INSTALL THE SERVER	19
Step 1: Setup Procedures.	19
Quick Start Setup Requirements	19
LCD Panel Setup Requirements	19
Step 1A: Quick Start Setup Procedures.....	20
Link the Workstation to the Web Filter	20

Monitor and Keyboard Setup	20
Serial Console Setup	20
Power on the Web Filter	21
Power up a 300 Series Model	21
Power up a 500 or 700 Series Model	21
HyperTerminal Setup Procedures	22
Login screen	25
Quick Start menu screen	25
Quick Start menu: administration menu	26
Change filtering mode	27
Configure network interface LAN1	27
Configure network interface LAN2	27
Configure default gateway	27
Configure DNS servers	27
Configure host name	28
Time Zone regional setting	28
Non-Quick Start procedures or settings	29
Reset system to factory defaults	29
Reboot system	29
Change Quick Start password	29
Reset admin console account	29
System Status screen	30
Log Off, Disconnect the Peripherals	30
Step 1B: LCD Panel Setup Procedures.....	31
LCD Panel	31
LCD panel keypad	31
LCD Menu	31
M86 menu	32
WF Filter Mode	33
IP / LAN1 and 2	33
Gateway	33
DNS 1 and 2	34
Host Name	34
Regional Setting (Time Zone, date, time)	34
Non-Quick Start procedures or settings	35
WF Patch Level	35
Reset WF Admin Console Password	35
Reboot	35
Shutdown	35
LCD Options menu	36
Heartbeat	36
Backlight	36
LCD Controls	36
Step 2: Physically Connect the Unit to the Network.....	37
Step 3: Access the Web Filter Online.....	38
Access the Web Filter via its LAN 1 IP Address	38
Accept the Security Certificate in Firefox	39
Temporarily Accept the Security Certificate in IE	41
Accept the Security Certificate in Safari	42
Step 4: Log in, Generate SSL Certificate.	43
Log in to the Web Filter	43
Generate SSL Certificate	44
IE Security Certificate Installation Procedures	45

Accept the Security Certificate in IE	45
Windows XP or Vista with IE 7 or 8.....	45
Windows 7 with IE 8.....	49
Map the Web Filter's IP Address to the Server's Host Name	50
Step 5: Test Filtering or the Mobile Client Connection.	52
Test Filtering on the Web Filter	52
Test the Mobile Client Connection	52
Step 6: Set Library Updates.	53
Activate and Register the Web Filter	53
Perform a Complete Library Update	54
Monitor the Library Update Process	55
CONCLUSION	56
BEST FILTERING PRACTICES	57
Threat Class Groups.....	58
I. Threats/Liabilities	59
1. Category block	59
2. Rule block	59
3. X-Strike on blocked categories	59
4. Custom Lock, Block, Warn, X Strikes, Quota pages	60
5. URL Keywords	60
6. Search Engine Keywords	60
7. Custom Category (blocked)	61
8. Minimum Filtering Level	61
9. Override Account bypass	61
10. Exception URL bypass	62
11. Proxy Patterns	62
12. File type blocking	62
II. Bandwidth/Productivity	63
1. Time Quota/Hit Quota	63
2. Overall Quota	63
3. Time Based Profiles	63
4. Warn option with low filter settings	64
5. Warn-strike	64
6. P2P patterns	64
7. IM patterns	65
8. Game patterns	65
9. Streaming Media patterns	65
10. Remote Access patterns	66
11. HTTPS settings	66
12. Category block	66
13. Rule block	67
14. SE Keywords	67
15. URL Keywords	67
16. Custom Block/Warn/X Strikes/Quota pages	68
17. Real Time Probe information	68
III. General/Productivity	68
1. Warn Feature with higher thresholds	68
2. Warn-strike with higher thresholds	69
3. Time Quota/Hit Quota	69
4. Time Based Profiles	69
5. Overall Quota	70

6. Customize an M86 Supplied Category	70
7. Local category adds/deletes	70
8. Custom Block/Warn/X Strikes/Quota pages	71
IV. Pass/Allow	71
1. Always Allow Custom Category	71
2. URL exceptions	71
3. IP exceptions	72
4. Override Accounts	72
5. Pattern detection bypass	72
LED INDICATORS AND BUTTONS	73
Front Control Panels on 500 and 700 Series Units	73
Rear Panel on the 700 Series Unit	74
Front Control Panel on a 300 Series Unit	74
REGULATORY SPECIFICATIONS AND DISCLAIMERS	75
Declaration of the Manufacturer or Importer	75
Safety Compliance	75
Electromagnetic Compatibility (EMC)	75
Federal Communications Commission (FCC) Class A Notice (USA)	75
FCC Declaration of Conformity	75
Electromagnetic Compatibility Class A Notice	75
Industry Canada Equipment Standard for Digital Equipment (ICES-003)	75
EC Declaration of Conformity	76
European Community Directives Requirement (CE)	76
INDEX	77

M86 WF APPLIANCE INTRODUCTION

Thank you for choosing to install and evaluate the M86 Web Filter appliance. M86 Security's Web Filter tracks each user's online activity, and can be configured to block specific Web sites, service ports, and pattern and file types, and lock out an end user from Internet access, thereby protecting your organization against lost productivity, network bandwidth issues, and possible legal problems that can result from the misuse of Internet resources.

The Web Filter provides an extensive library filtering category database, user authentication, implementation of time and quota filtering profiles, and tools for tailoring a user's filtering profile to comply with your organization's Internet usage policy, based on the end user's Internet usage habits.

Quick setup procedures—to implement the best filtering practices—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 the Web Filter 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 Web Filter appliance in your network environment
- **Install the Server** - This section explains how to configure the Web Filter for filtering
- **Conclusion** - This section indicates that the installation steps have been completed
- **Best Filtering Practices** - This section is comprised of suggested best practices for implementing and using the Web Filter
- **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 Web Filter appliance models referenced therein
- **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.



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 Web Filter 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 Web Filter appliance (WF)
- 1 serial port cable
- 1 CD-ROM containing supplemental product applications and EULA



NOTES:

For 500 and 700 series models, the following items are also included in the carton:

- 1 AC power cord for 500 series models, 2 AC power cords for 700 series models
- 1 bezel to be installed on the front of the chassis
- 1 set of rack mounting rails

For 300 series models, the following items are also included in the carton:

- 1 power adapter with power cord
- 1 set of 4 pressure sensitive feet to be affixed to the bottom corners of a non-rack mounted unit

For 300 series models, if you have purchased the optional 1U two-unit tray for mounting the half-U server(s) in a rack, this item will be shipped in a separate carton.

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

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



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.



TIP: Please consult the Web Filter User Guide for information about RAID and hardware maintenance. User Guides for the Web Filter product can be obtained from <http://www.m86security.com/support/wf/documentation.asp>.

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.

300 Series Server Setup Procedures

Set Top Applications

If you have a 300 series server you do not wish to rack mount, apply the pressure sensitive feet (that came with the server) to the bottom corners of the unit, and then place the unit in a location that meets server site selection criteria.

Optional 1U 2-Unit Tray Kit Applications

If you have purchased the optional 1U 2-unit tray kit for rack mounting one or two 300 series servers, proceed to the instructional “300 Series Appliance Tray Installation” document packaged within the 1U 2-unit tray kit’s shipping carton.

When you have finished installing the 300 series server(s) in your server rack, continue to the Install the Server section of this Installation Guide.

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 (T_{ma}) 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.*

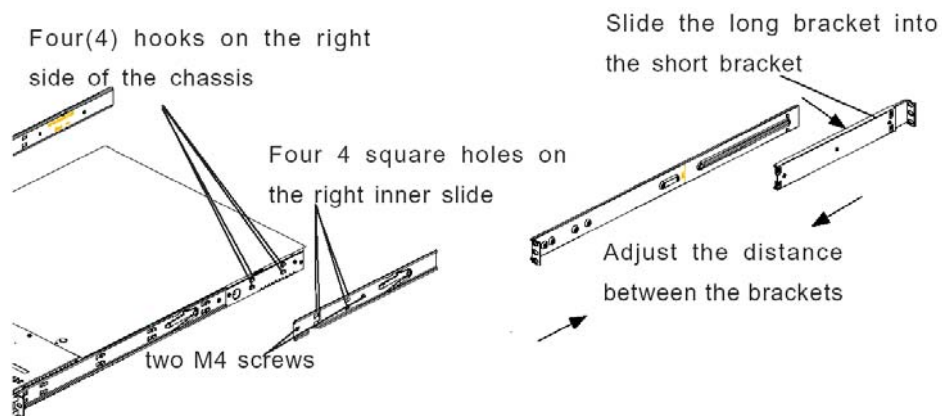
Rack Mount Instructions for 500 Series Servers

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.

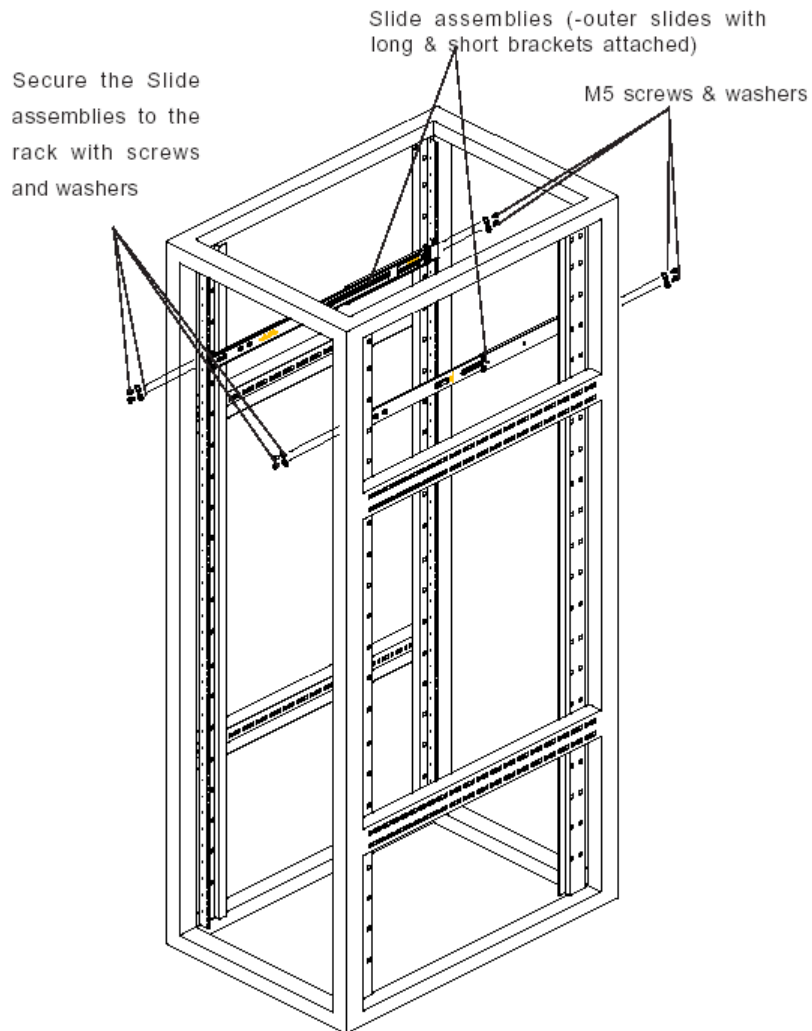


Install the Outer Slides

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.

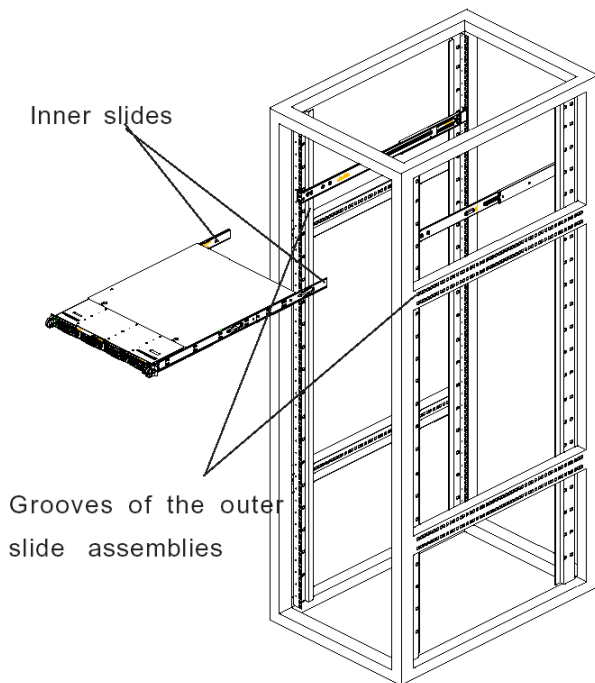
Install the Slide Assemblies to the Rack

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:

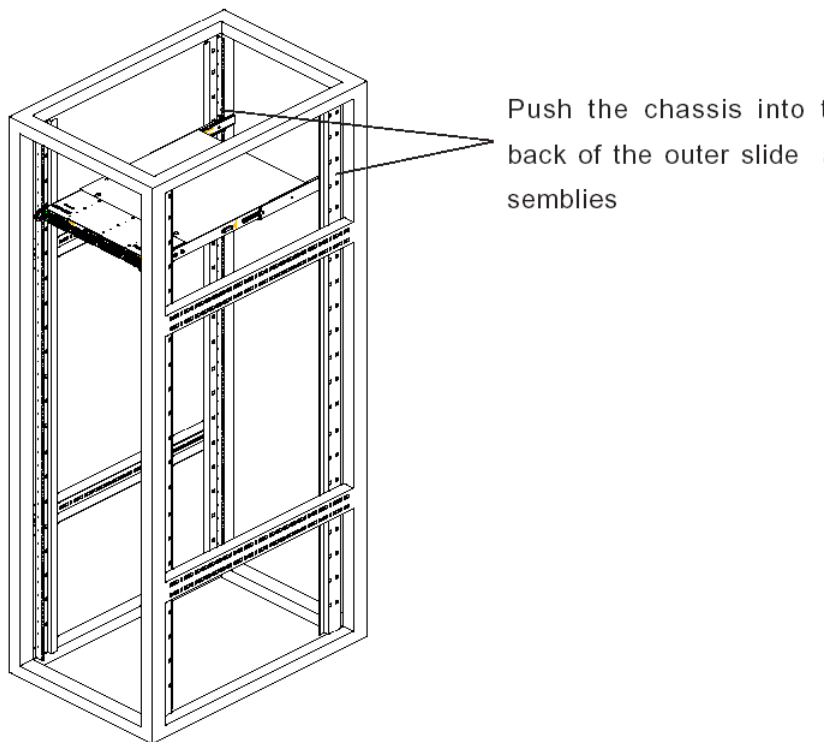


Install the Chassis into the Rack

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:



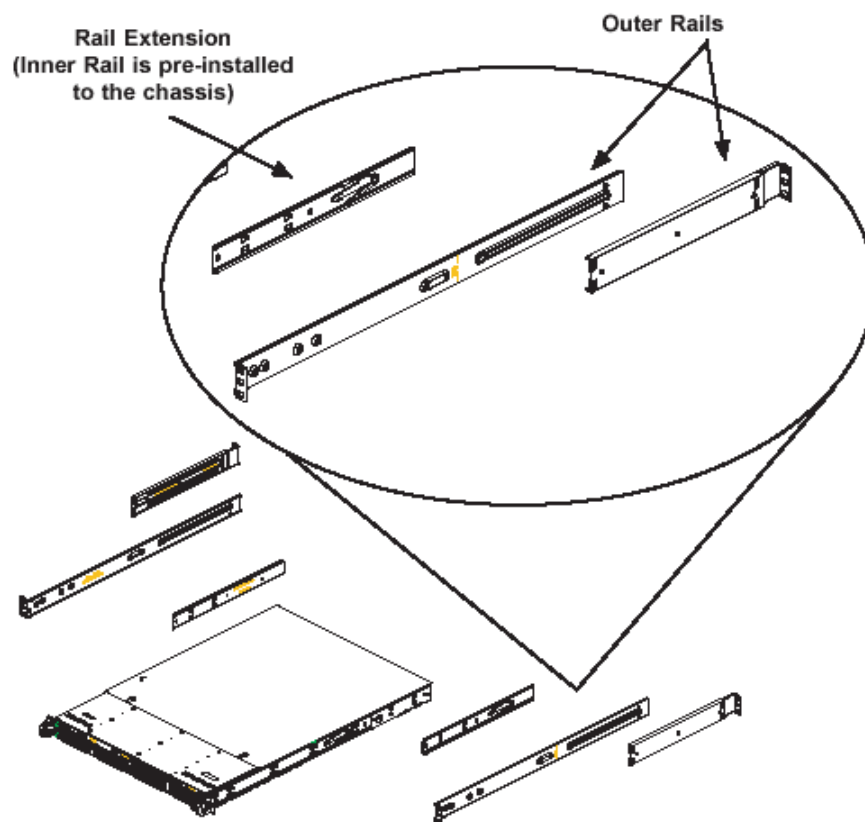
Rack Mount Instructions for 700 Series Servers

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

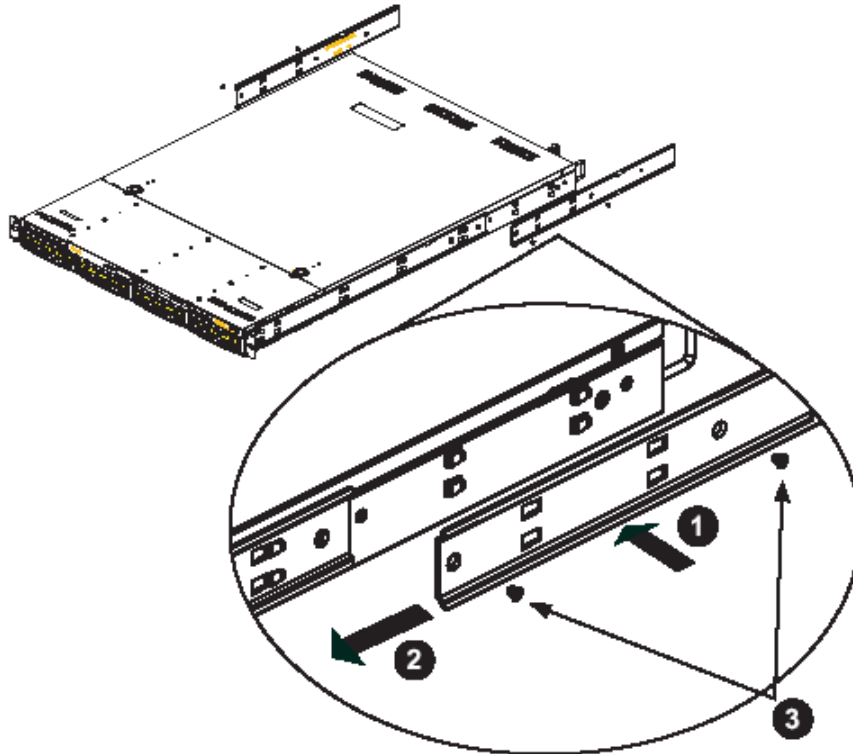
The chassis package includes two rack rail assemblies in the rack mounting kit. Each assembly consists of two sections: an inner fixed chassis rail that secures directly to the server chassis and an outer fixed rack rail that secures directly to the rack itself.



The 700 series chassis includes a set of inner rails in two sections: inner rails and inner rail extensions. The inner rails are pre-attached and do not interfere with normal use of the chassis if you decide not to use a server rack. Attach the inner rail extension to stabilize the chassis within the rack.

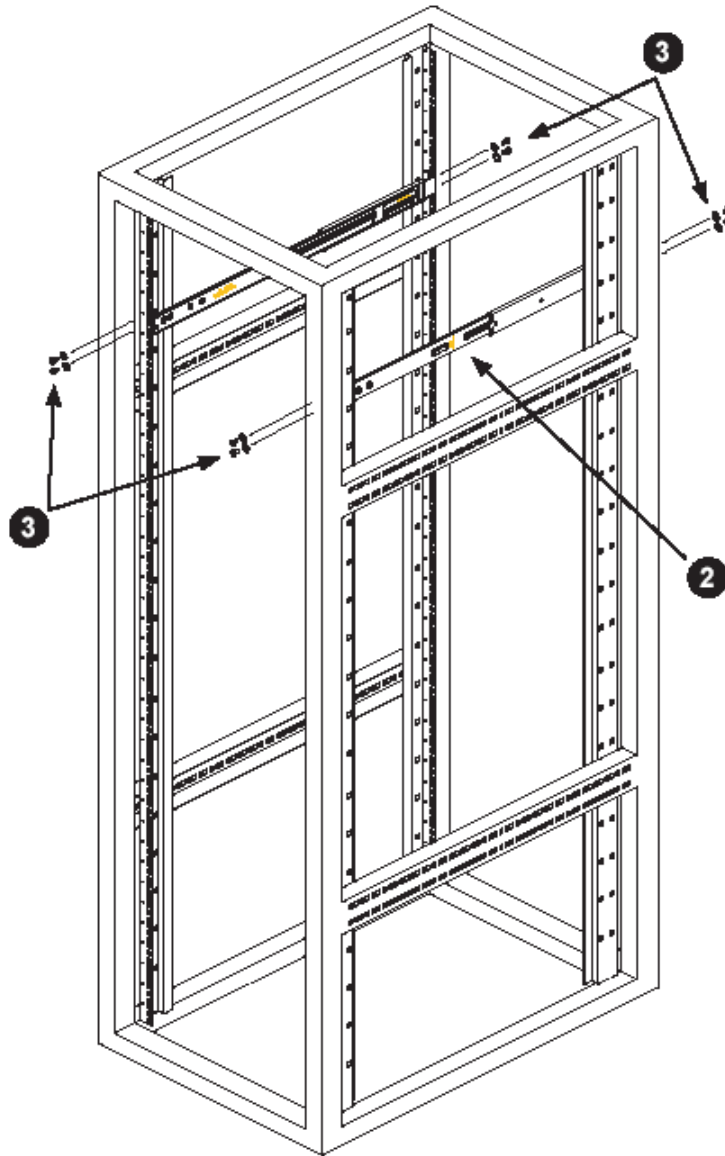
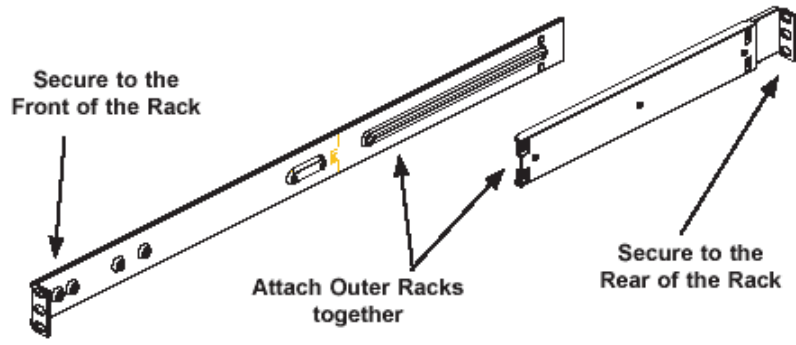
Install the Inner Rails

1. Place the inner rack extensions on the side of the chassis aligning the hooks of the chassis with the rail extension holes. Make sure the extension faces "outward" just like the pre-attached inner rail.
2. Slide the extension toward the front of the chassis.
3. Secure the chassis with 2 screws as illustrated.
4. Repeat steps 1-3 for the other inner rail extension.



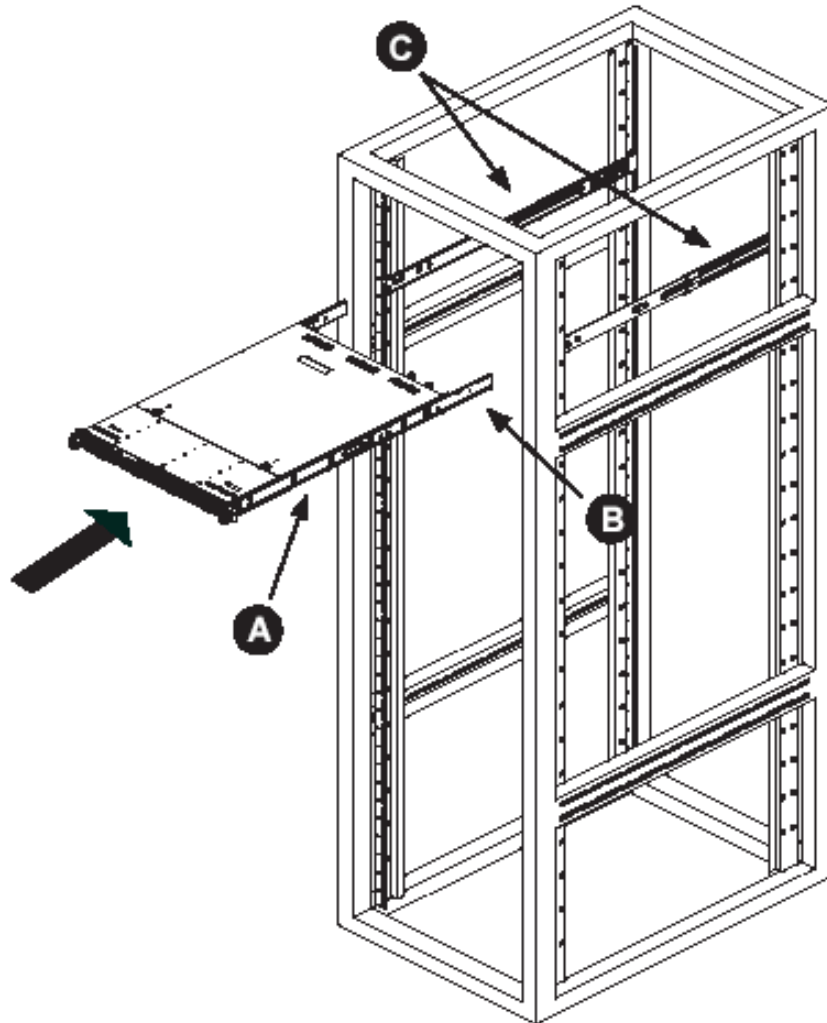
Install the Outer Rails

1. Attach the short bracket to the outside of the long bracket. You must align the pins with the slides. Also, both bracket ends must face the same direction.
2. Adjust both the short and long brackets to the proper distance so that the rail fits snugly into the rack.
3. Secure the long bracket to the front side of the outer rail with two M5 screws and the short bracket to the rear side of the outer rail with three M5 screws.
4. Repeat steps 1-4 for the left outer rail.



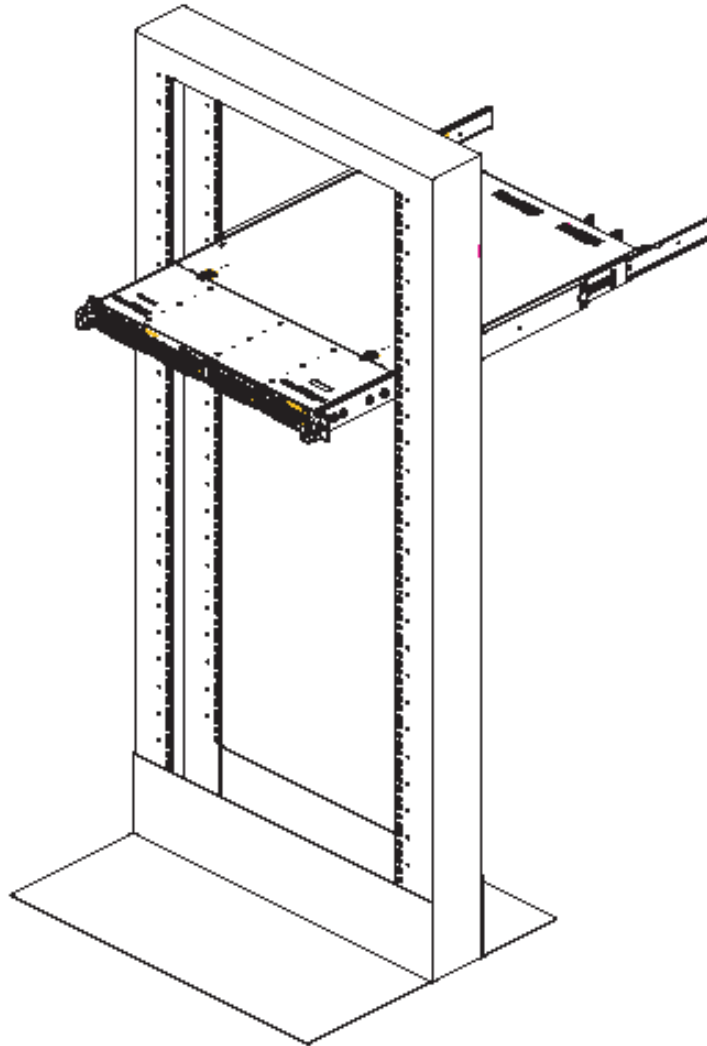
Install the Server into the Rack

1. Confirm that chassis includes the inner rails (A) and rail extensions (B). Also, confirm that the outer rails (C) are installed on the rack.
2. Line chassis rails (A and B) with the front of the rack rails (C).
3. 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".
4. (Optional) Insert and tightening the thumbscrews that hold the front of the server to the rack.




Install the Server into a Telco Rack

If you are installing the server into a Telco type rack, follow the directions given on the previous pages for rack installation. The only difference in the installation procedure will be the positioning of the rack brackets to the rack. They should be spaced apart just enough to accommodate the width of the Telco rack.



Install the Bezel on the 500 and 700 Series Chassis

After rack mounting a 500 or 700 series 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 the short pair of end pins on the left side (Fig. 2), and the longer pair of fixed pins on the inside top towards the middle (Fig. 3).



Fig. 2 - Pins on the left end

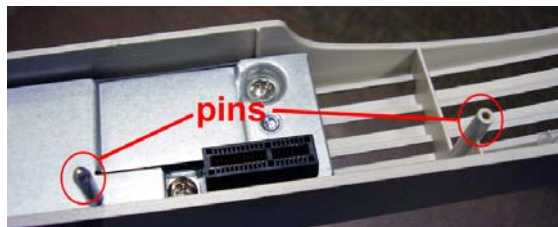


Fig. 3 - Pins on the inside at the top of the bezel

C. Note the end pin holes (Fig. 5) on the inside of the U-shaped, aluminum rail handles on both ends of the chassis rails (Fig. 4: U-shaped handles). Note also that the holes for the longer pair of pins are located on the front of the chassis above the third hard drive bay (Fig. 4: holes).



Fig. 4 - Front of chassis with U-shaped handles and holes above third hard drive identified

D. Insert the end pins into the holes of the left U-shaped handle (Fig. 5).

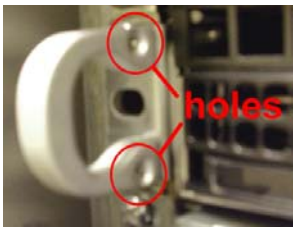


Fig. 5 - Holes in handle



Fig. 6 - Release knob

E. Align the bezel with the front of the chassis, and then gently push the bezel towards the front of the chassis, inserting the pins on the inside of the bezel (Fig. 3) into the holes on the front of the chassis (Fig. 4: holes).

F. Press in the release knob on the right side of the bezel to retract the end pins on that side (Fig. 6), and then release the knob to let the end pins extend into the holes of the right U-shaped handle (Fig. 4: U-shaped handles).

Check the Power Supply

The 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 700 series 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 REMPLACEMENT 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 CONFORMÉMENT 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 set up parameters for the Web Filter to function on the network. You have the option of using the text-based Quick Start setup procedures described in Step 1A, or the LCD panel setup procedures described in Step 1B.

Quick Start Setup Requirements

A. The following hardware is required for the Quick Start setup procedures:

- Web Filter 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)

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



NOTE:

* For 300 series models, the power adapter supplied with the power cord must also be used

** 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

A. The following hardware is required for LCD panel setup procedures:

- Web Filter with AC power cord(s) *

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



NOTE:

* For 300 series models, the power adapter supplied with the power cord must also be used

Step 1A: Quick Start Setup Procedures

Link the Workstation to the Web Filter

Monitor and Keyboard Setup

- A. Connect the PC monitor and keyboard cables to the rear of the Web Filter chassis.
- B. Turn on the PC monitor.
- C. Proceed to the next set of instructions: Power on the Web Filter.

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 “serial port” in Fig. 1 for a 300 series unit, Fig. 2 for a 500 series unit, and Fig. 3 for a 700 series unit).

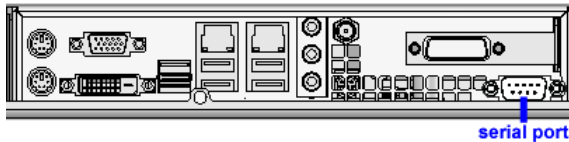


Fig. 1 - Rear of 300 series chassis with serial port identified

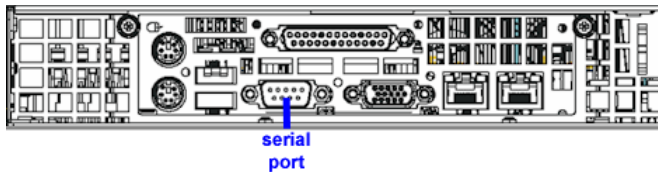


Fig. 2 - Portion of 500 series chassis rear with serial port identified

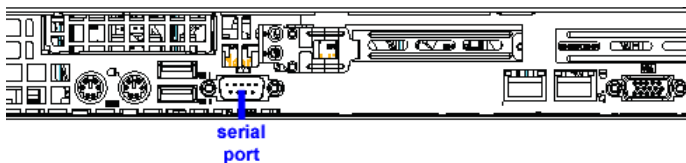


Fig. 3 - Portion of 700 series chassis rear with serial port identified

- B. Power on the laptop.
Proceed to the next set of instructions: Power on the Web Filter.

Power on the Web Filter

Power up a 300 Series Model

- A. Make sure the power adapter is plugged into the back of the chassis and connected to the power cord.
- B. Plug the power cord into a power source with an appropriate rating.



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

- C. Go to the LCD panel on the front of the chassis, and press down the green checkmark key for three seconds (Fig. 4).



Fig. 4 - 300 series LCD panel and keypad

- D. When the LCD panel displays a message that indicates the Web Filter is running, proceed to the following set of instructions:

- For Monitor and Keyboard Setup, go to Login screen.
- For Serial Console Setup, go to HyperTerminal Setup Procedures.

Power up a 500 or 700 Series Model

- A. Make sure the power cord(s) is/are plugged into the back of the chassis.
- B. Plug the power cord(s) into a power source with an appropriate rating.



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

- C. Remove the bezel and press the large button at the right of the front panel (see Fig. 5 for a 500 series unit, and Fig. 6 for a 700 series unit).



Fig. 5 - 500 series chassis front panel, power button at far right

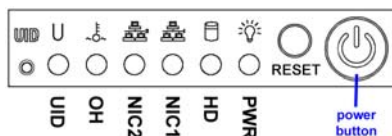


Fig. 6 - 700 series chassis front panel, power button at far right

- D. Replace the bezel on the front of the chassis. When the LCD panel displays a message that indicates the Web Filter is running, proceed to the following set of instructions:

- For Monitor and Keyboard Setup, go to Login screen.
- For Serial Console Setup, go to 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 September 16, 2010), 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."*

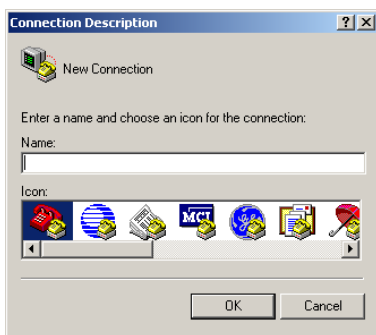
If you are using a Windows Vista or Windows 7 machine to conduct these quick start setup procedures and do not have an equivalent type of terminal emulator program installed on your workstation, Hilgraeve, Inc., the maker of HyperTerminal, offers HyperTerminal Private Edition for Windows Vista and Windows 7. The following information is included on Hilgraeve's Web page at <http://www.hilgraeve.com/hyperterminal.html> (accessed September 16, 2010): "HyperTerminal Private Edition is a terminal emulation program that supports communications over TCP/IP networks, Dial-Up Modems, and serial COM ports.... Click here to download the 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:

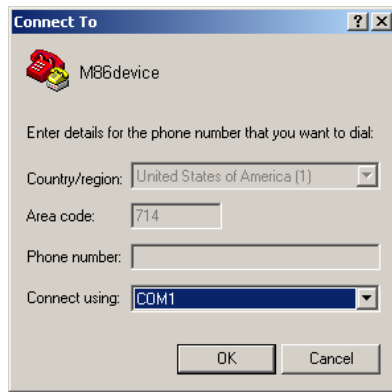
- 9600 bits per second
- 8 data bits
- no parity
- 1 stop bit
- hardware flow control
- VT100 emulation settings

On the Windows XP machine:

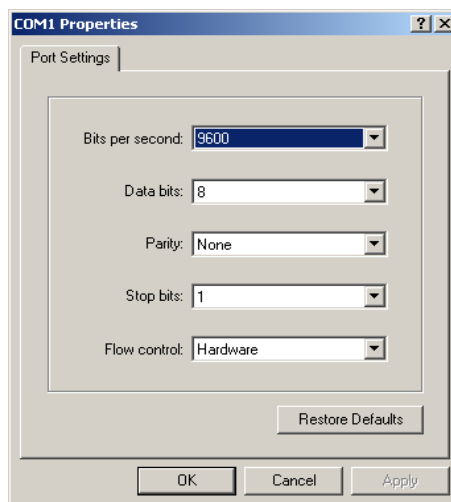
- A. Launch HyperTerminal by going to Start > Programs > Accessories > Communications > HyperTerminal:



- B. In the Connection Description dialog box, enter any session **Name**, and then click **OK** to open the Connect To dialog box:



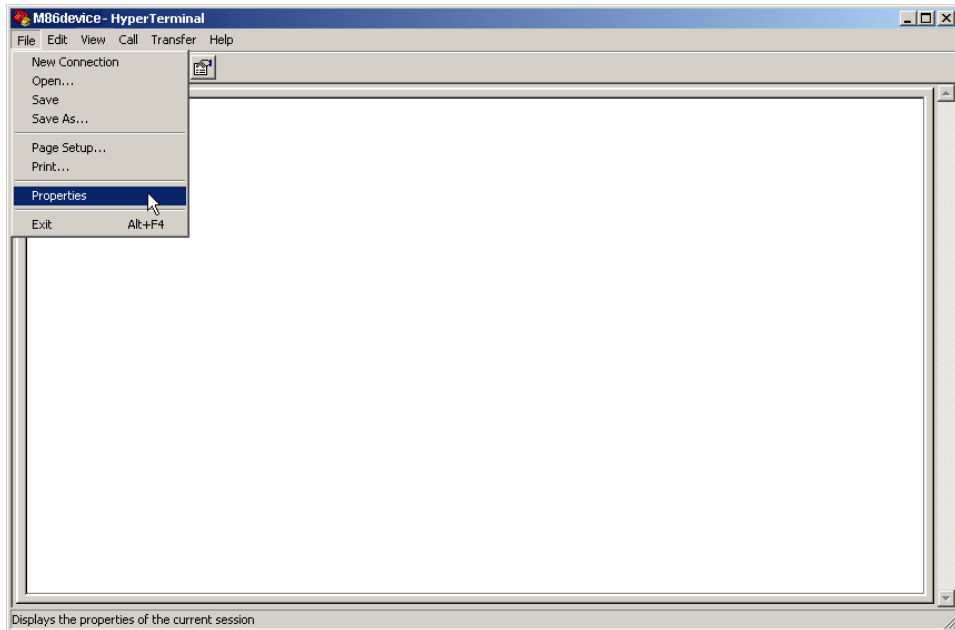
- C. At the **Connect using** field, select the COM port assigned to the serial port on the laptop (probably “COM1”), and then click **OK** to open the Properties dialog box, displaying the Port Settings tab:



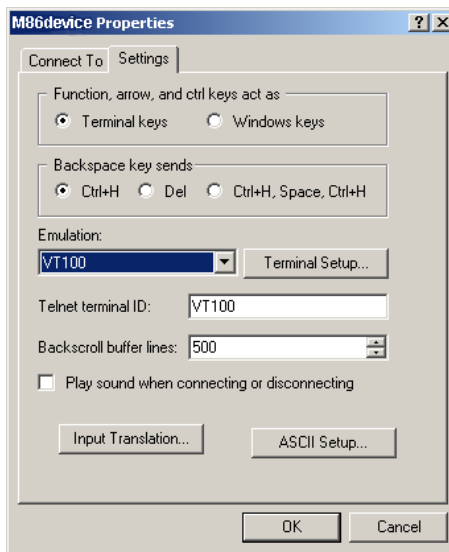
- D. Specify the following session settings:

- 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 Web Filter using a monitor and keyboard, or after 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.



NOTE: 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.

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

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: R3000-10-120.qc.8e6.net

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 4.0.10.5
Library was last updated on 2010/05/27

Press any key to return to menu...

```

The System Status screen contains the following information:

- **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 Filter
- 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

- After completing the Quick Start setup procedures, return to the Quick Start menu screen and press **9** to log out.
- Disconnect the peripherals from the Web Filter.

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

Step 1B: LCD Panel Setup Procedures

LCD Panel

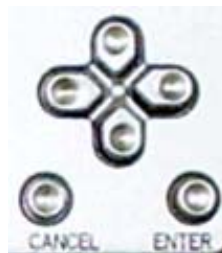
- A. Connect the AC power cord(s) to the back of the chassis and plug the cord(s) into a UPS power supply unit.
- B. Power on the server following the instructions at Step 1A: Quick Start Setup Procedures, Power on the Web Filter.

LCD panel keypad

To configure the Web Filter via the LCD panel on front of the chassis bezel, use the keypad located to the right of the LCD screen.

The keypad consists of the following keys:

- On a 300 series model: Up arrow, down arrow, left arrow, right arrow, checkmark, and "X" keys.
- On a 500 or 700 series model: Up, down, left, right, CANCEL, and ENTER keys.



300 series keypad at left, 500 and 700 series keypad at right

To display software status information about the Web Filter, press the right (arrow) key. To go to the LCD Menu, press "X" / CANCEL. Pressing "X" / CANCEL again returns you to the software status display.

LCD Menu

The LCD Menu tree includes the following two main menu selections:

- LCD Options - This choice includes options for viewing the LCD display and monitoring the Web Filter once it is configured and running on the network. Information about using LCD Options is included in this document after the M86 menu sub-section.
- M86 menu - Many of the menu items in this sub-section are used for configuring the Web Filter unit.

The menu tree displays an arrow 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 / ENTER key to accept your selection.

M86 menu

When the M86 menu option is selected from the LCD Menu tree, the following menu items display in the panel, the entire list which is viewable by using the navigation keys:

- WF Patch Level >
- 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 (*).

Please make a note of the LAN 1 and LAN 2 IP address and host name you assign to the Web Filter server, as you will need to use this information in later steps of the installation procedure.



TIPS: Navigation tips in the M86 menu:

- Use the up / down (arrow) key to scroll up / down the menu
- Press the checkmark / ENTER key to choose the current selection
- Press the "X" / CANCEL key to go back to the previous screen

Make a selection from the menu, and press the checkmark / ENTER 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 / ENTER 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 2

When the IP / LAN 1 (2) option is selected, the IP / LAN 1 (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 / ENTER 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 / ENTER key to accept your entry and to return to the previous screen.
 - D. Choose **Change LAN1 (2) Netmask** and press the checkmark / ENTER 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 / ENTER key to accept your entry and to return to the previous screen.
 - G. Press the "X" / CANCEL key to return to the M86 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 / ENTER 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 / ENTER key to accept your entry and to return to the previous screen.
- D. Press the "X" / CANCEL key to return to the M86 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 / ENTER 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 / ENTER key to accept your entry and to return to the previous screen.
- D. Press the "X" / CANCEL key to return to the M86 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 up, down, left, right (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.



NOTE: *Navigation tips:*

- *If the down (arrow) key is pressed first—instead of the right (arrow) key—the symbol characters display first.*
- *Press the "X" / CANCEL key to remove a character and move the cursor to the first position in the line.*

- C. Press the checkmark / ENTER key to return to the previous screen.
- D. Press the "X" / CANCEL key to return to the M86 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 / ENTER 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 / ENTER key to display the Save Changes? screen:
 - Choose **Yes** to save your changes and to return to the M86 menu.
 - Choose **No** to return to the previous screen.

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.

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” / CANCEL key to return to the M86 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” / CANCEL 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 / ENTER key to go to that screen.

Heartbeat

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

- A. Press the checkmark / ENTER or right (arrow) key three times to view each of the three available options:
 - heartbeat feature enabled (populated field)
 - heartbeat feature disabled (empty field)
 - check for a heartbeat now (blinking heartbeat symbol displayed in the line above)
- B. After making your selection, press the “X” / CANCEL key to return to the previous screen.

Backlight

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

- A. Press the checkmark / ENTER or right (arrow) key three times to view each of the three available options:
 - backlight feature enabled (populated field, backlight turns on)
 - backlight feature disabled (empty field, backlight turns off)
 - display the backlight now (populated field, backlight turns on)
- B. After making your selection, press the “X” / CANCEL key to return to the previous screen.

LCD Controls

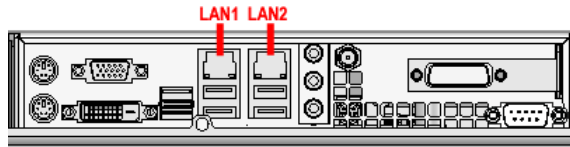
When the LCD Controls option is selected, the LCD Controls screen displays with the following menu items: Contrast, On Brightness, Off Brightness.

- A. Choose one of the menu selections and press the checkmark / ENTER or right (arrow) 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” / CANCEL key to return to the previous screen.

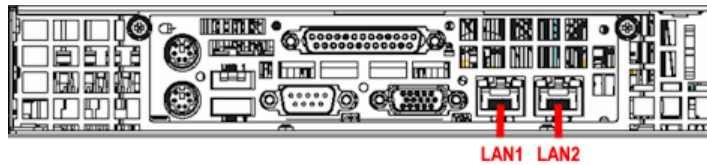
Step 2: Physically Connect the Unit to the Network

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.

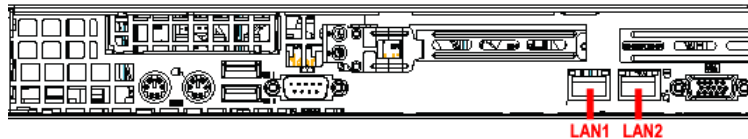
- A. Plug one end of a standard CAT-5E cable into the Web Filter's LAN 1 port, the port on the left.



Rear of 300 series chassis with LAN ports identified



Portion of 500 series chassis rear with LAN ports identified



Portion of 700 series chassis rear with LAN ports identified

- B. 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.
- C. Repeat the sub-steps above for the Web Filter's LAN 2 port.
- D. 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 (as described in Step 1B: LCD Panel Setup Procedures).

Step 3: Access the Web Filter Online

Access the Web Filter via its LAN 1 IP Address

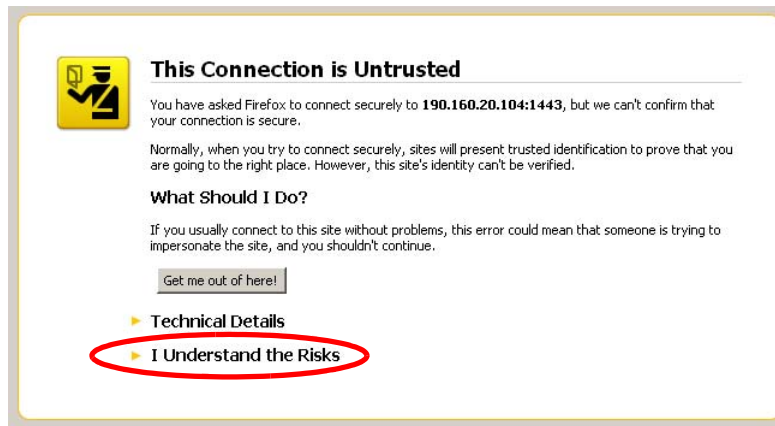
- A. Launch an Internet supported browser:
 - Firefox 3.6
 - Internet Explorer 7 or 8
 - Safari 4.0

- 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.

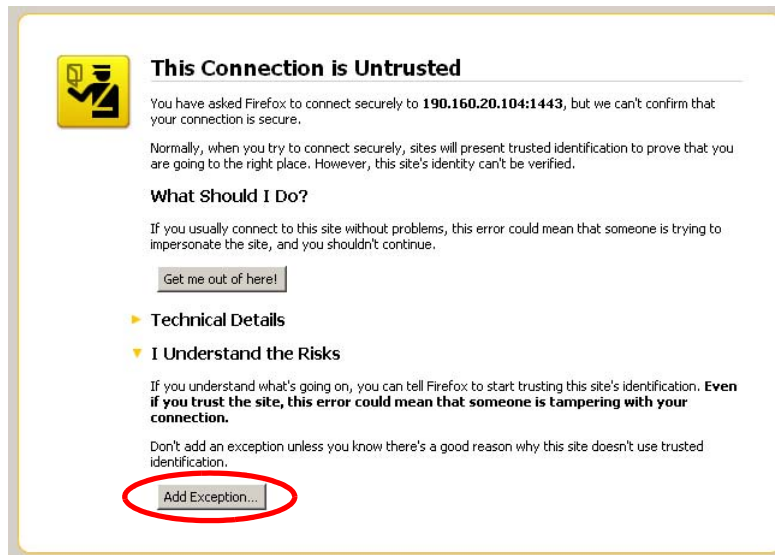
- C. Click **Go** to display the security issue page:
 - If using Firefox, proceed to Accept the Security Certificate in Firefox.
 - If using IE, proceed to Temporarily Accept the Security Certificate in IE.
 - If using Safari, proceed to Accept the Security Certificate in Safari.
 - If the security 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? (To ping the Web Filter using the Command Prompt in Windows XP, Vista, and 7, go to **Start > All Programs > Accessories > Command Prompt**, type in **Ping** and the IP address using the x.x.x.x format—in which each ‘x’ represents an octet—and then press **Enter**.)
 - 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

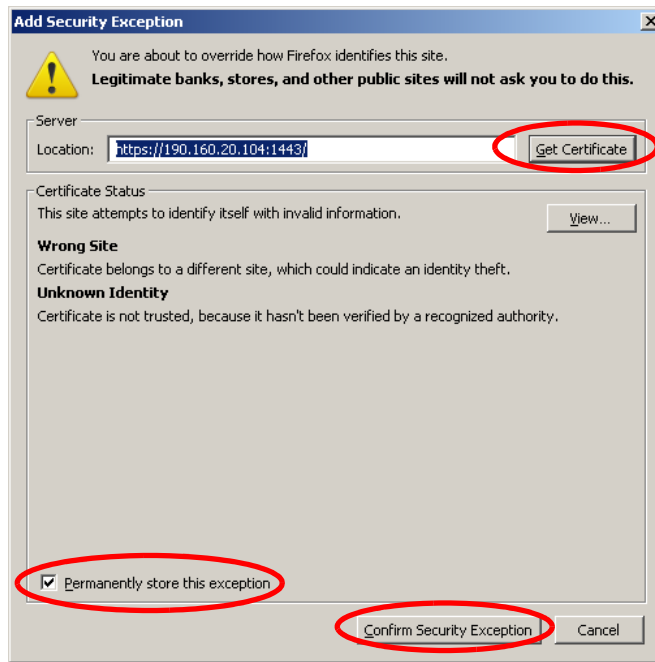
- A. If using a Firefox browser, in the page “This Connection is Untrusted,” click the option **I Understand the Risks**:



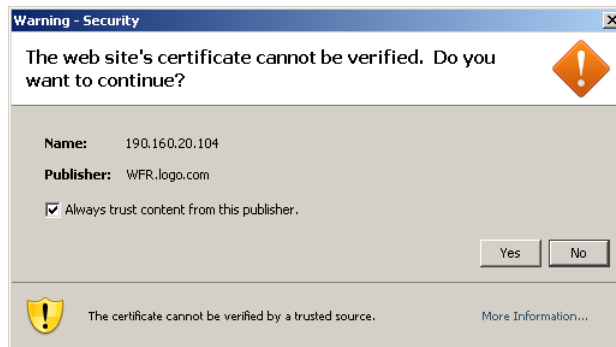
- B. In the next set of instructions that display, click **Add Exception...**:



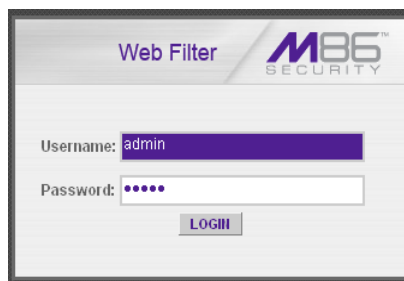
Clicking Add Exception opens the Add Security Exception window:



- 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, click **Confirm Security Exception** to open the Security warning dialog box:



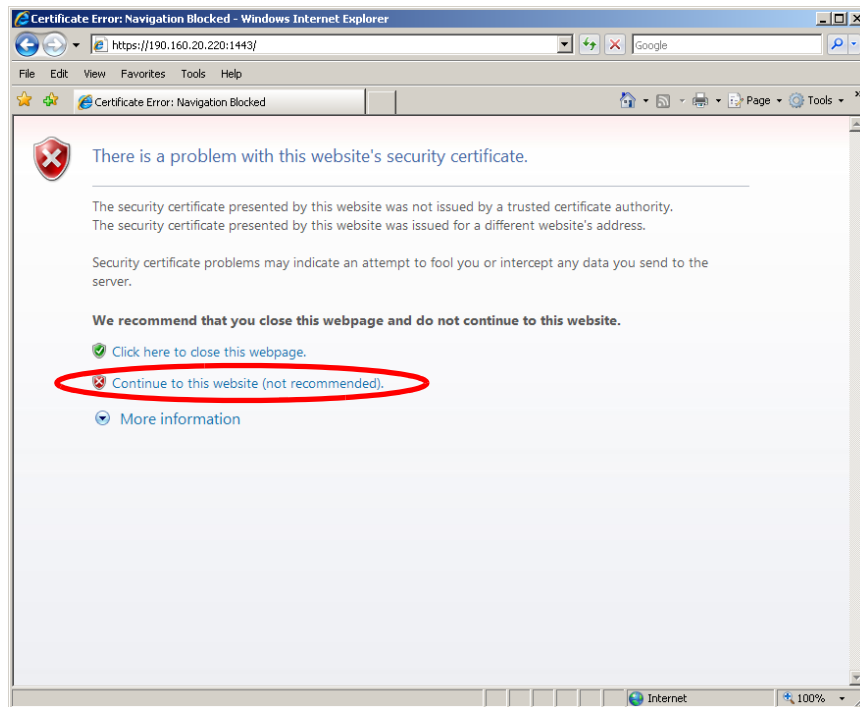
- E. With the checkbox “Always trust content from this publisher.” populated, click **Yes** to close the Security warning dialog box and to access the login window of the Web Filter user interface:



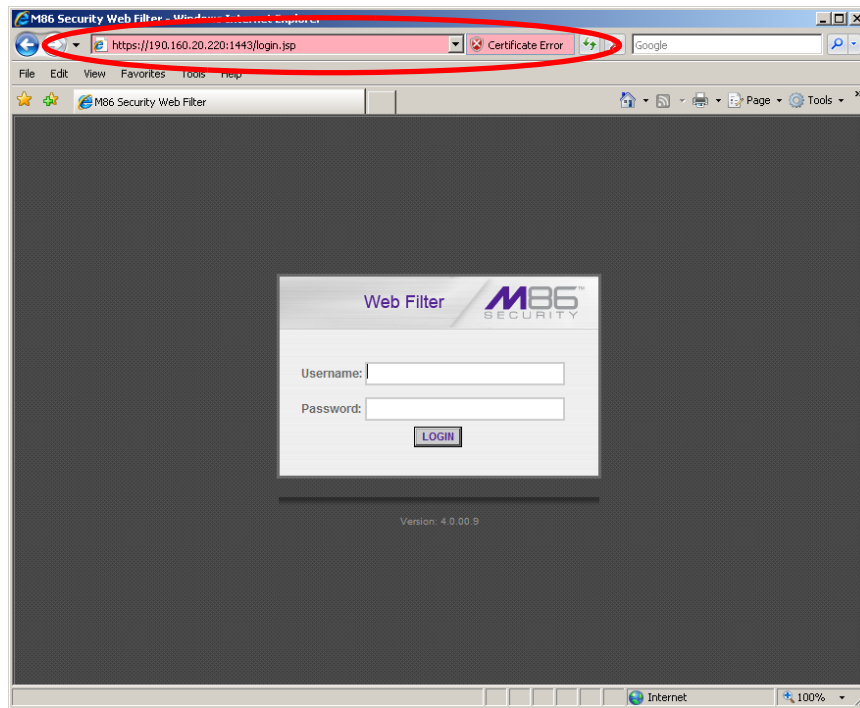
Proceed to Step 4: Log in, Generate SSL Certificate.

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:



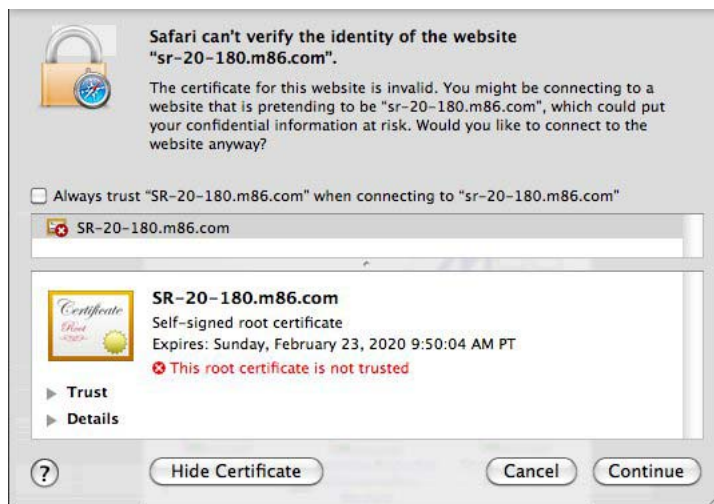
Proceed to Step 4: Log in, Generate SSL Certificate.

Accept the Security Certificate in Safari

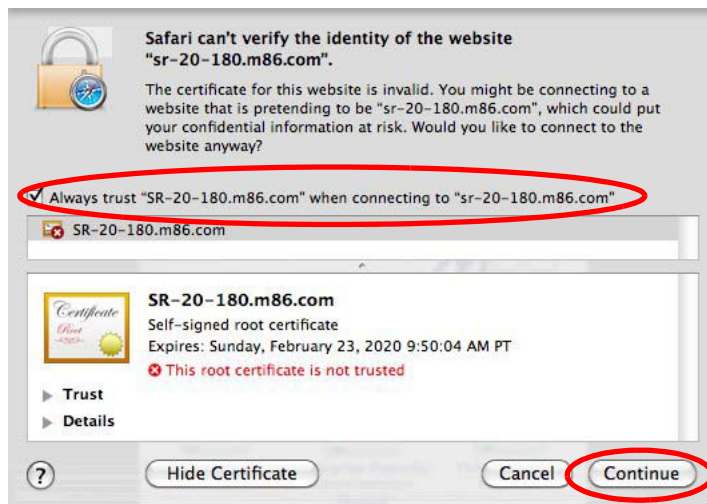
- A. If using a Safari browser, the pop-up window "Safari can't verify the identity of the website..." opens:



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**:



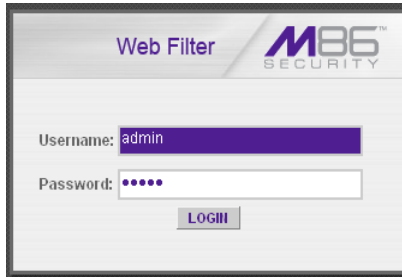
- C. You will be prompted to enter your password in order to install the certificate. After the security certificate is installed, proceed to Step 4: Log in, Generate SSL Certificate.

Step 4: Log in, Generate SSL Certificate

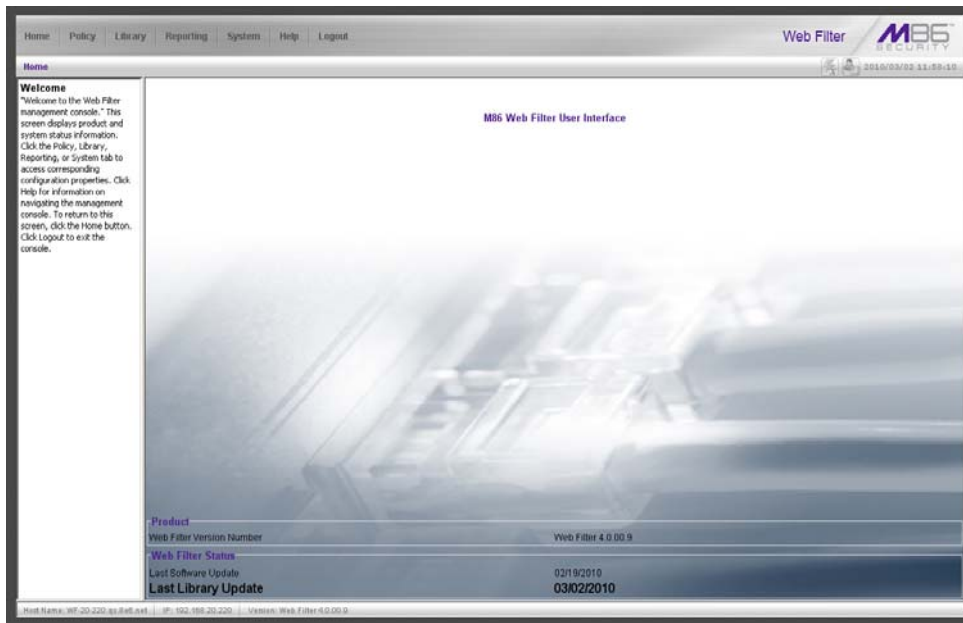
This step requires you to log in and generate a self-signed certificate for the Web Filter to ensure secure exchanges between the appliance and your browser. If using an IE browser, you will need to complete the security certificate acceptance procedures.

Log in to the Web Filter

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

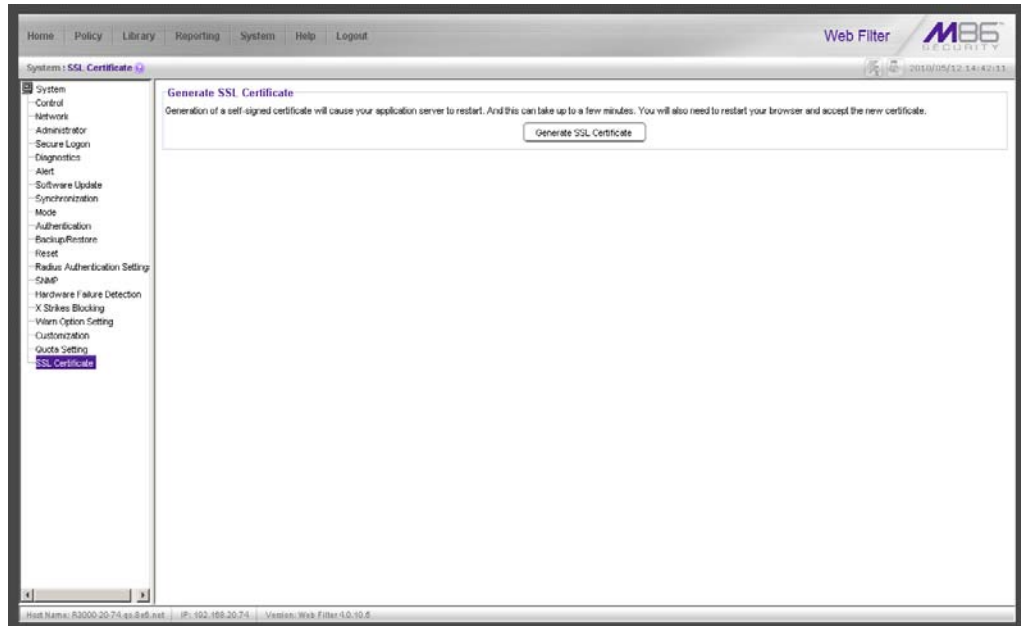


- B. Click **LOGIN** to display the Web Filter Admin console Welcome window:



Generate SSL Certificate

- A. Navigate to **System > SSL Certificate** to open the SSL Certificate window:



- B. Click **Generate SSL Certificate** to open the pop-up 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 or Safari browser, proceed to Step 5: Test Filtering or the Mobile 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 7 or 8
- Windows 7 with IE 8

Windows XP or Vista with IE 7 or 8

- A. If using an IE 7 or 8 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)**:

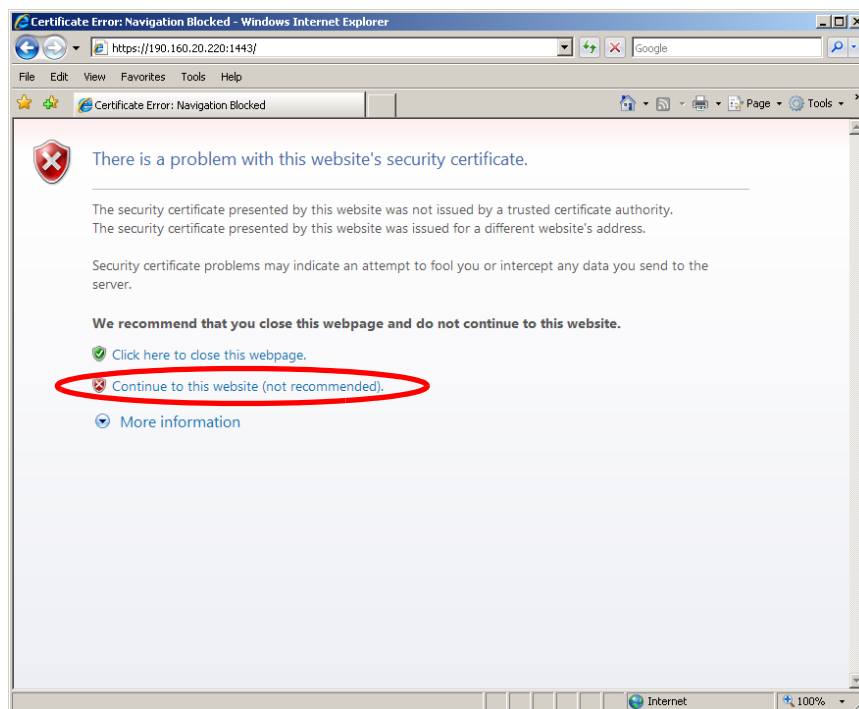


Figure A1: Windows XP, IE 7

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:

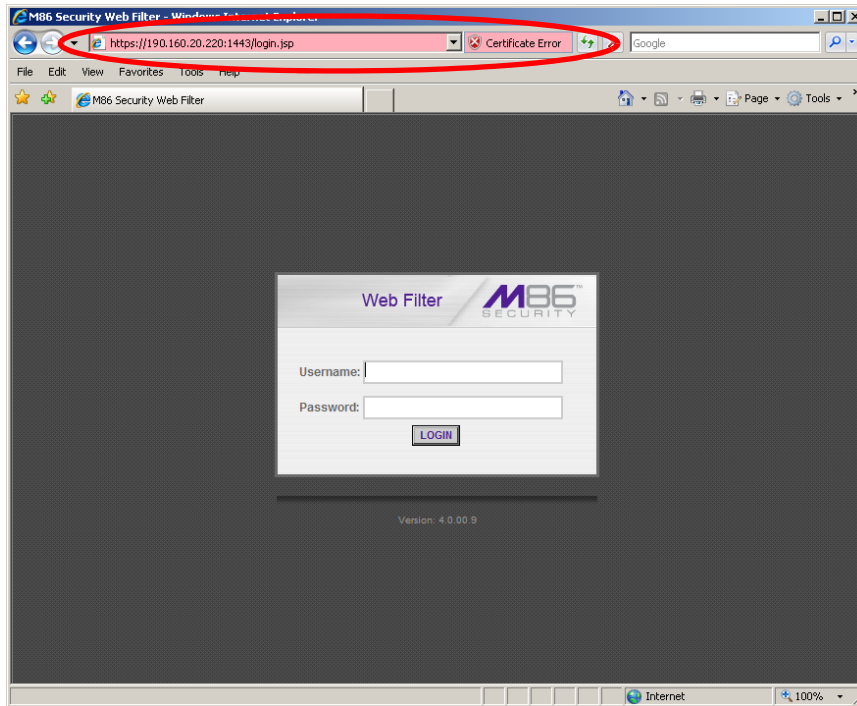


Figure A2: Windows XP, IE 7

B. Click **Certificate Error** to open the Certificate Invalid pop-up box:

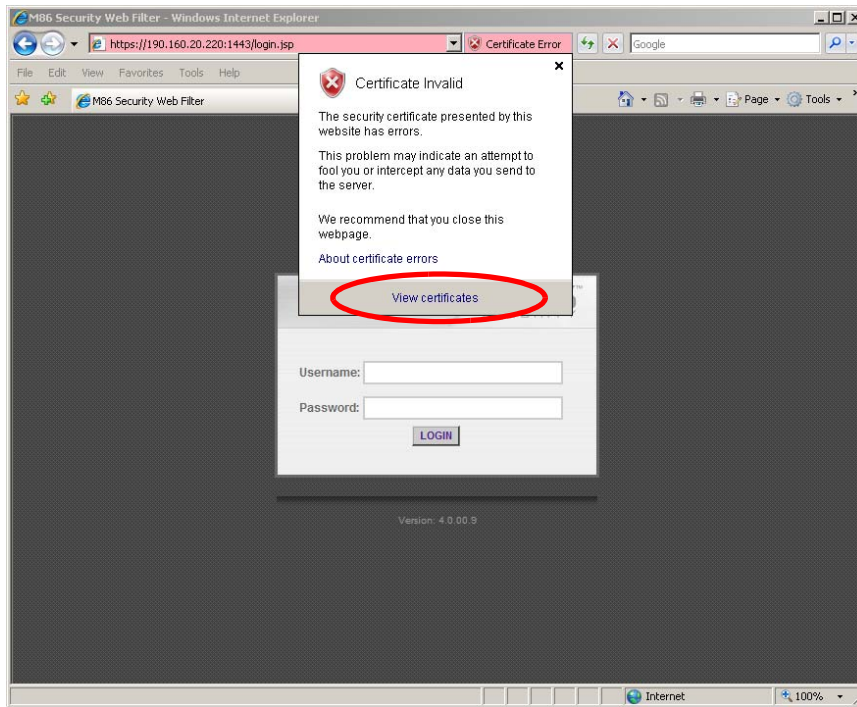


Figure B: Windows XP, IE 7

C. Click **View certificates** to open the Certificate window that includes the host name you assigned to the Web Filter:

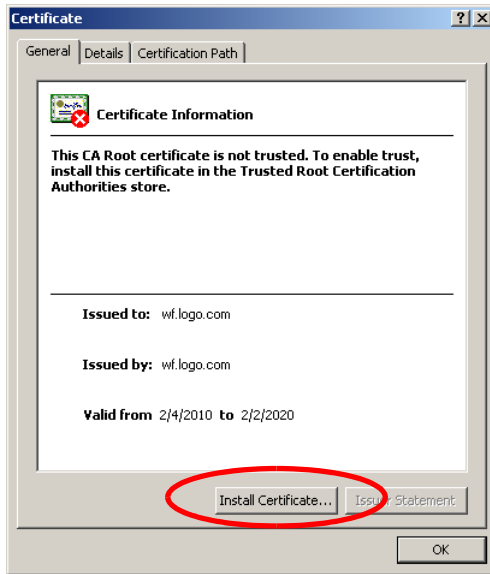


Figure C: Windows XP, IE 7

D. Click **Install Certificate...** to launch the Certificate Import Wizard:

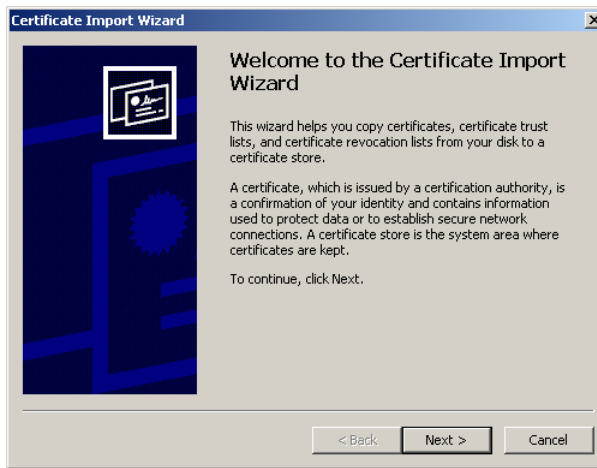


Figure D: Windows XP, IE 7

E. Click **Next >** to display the Certificate Store page:

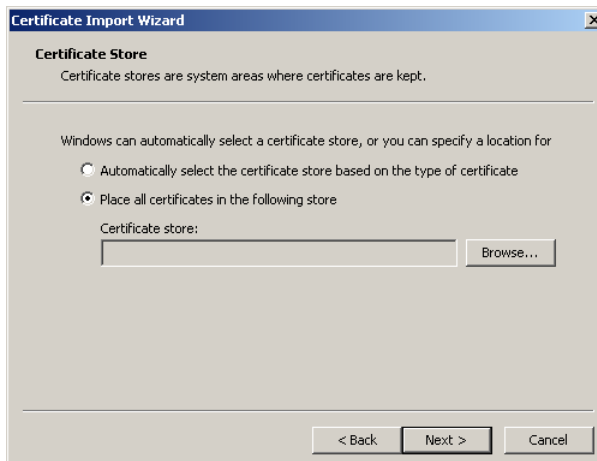


Figure E: Windows XP, IE 7

- F. Choose the option “Place all certificates in the following store” and then click **Browse...** to open the Select Certificate Store pop-up box:



Figure F: Windows XP, IE 7

- G. Choose “Trusted Root Certification Authorities” and then click **OK** to close the pop-up box.
- H. Click **Next >** to display the last page of the wizard:



Figure H: Windows XP, IE 7

- I. Click **Finish** to close the wizard and to open the Security Warning dialog box asking if you wish to install the certificate:

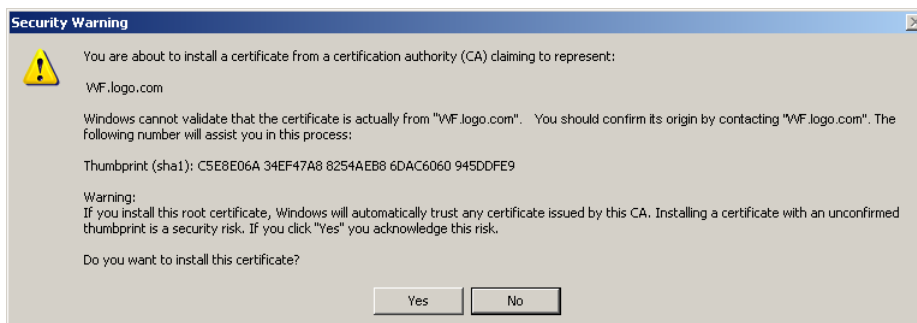


Figure I: Windows XP, IE 7

- 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.

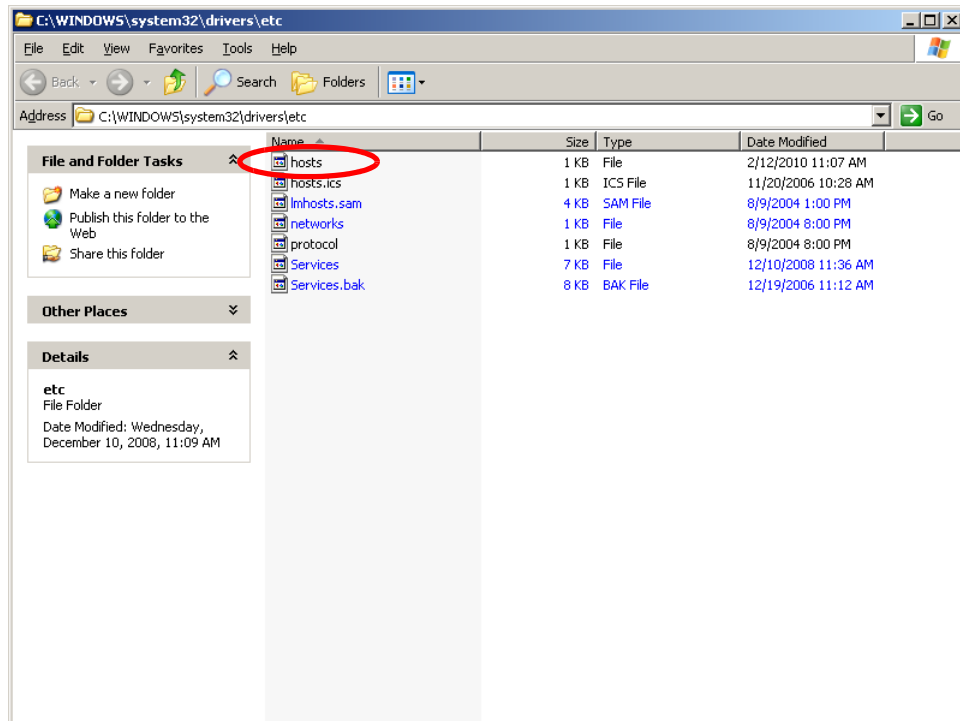
Windows 7 with IE 8

- A. If using an IE 8 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 pop-up box.
- C. Select the Security tab, click **Trusted sites**, and then click **Sites** to open the Trusted sites pop-up box.
- D. In the Trusted sites pop-up 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 pop-up 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 7 or 8:
 - 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 pop-up 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 pop-up box (see Figure F).
 - Choose "Trusted Root Certification Authorities" and then click **OK** to close the pop-up 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 pop-up box.
- I. Select the Security tab, click **Trusted sites**, and then click **Sites** to open the Trusted sites pop-up box.
- J. Select the URL you just added, click **Remove**, and then click **Close**.

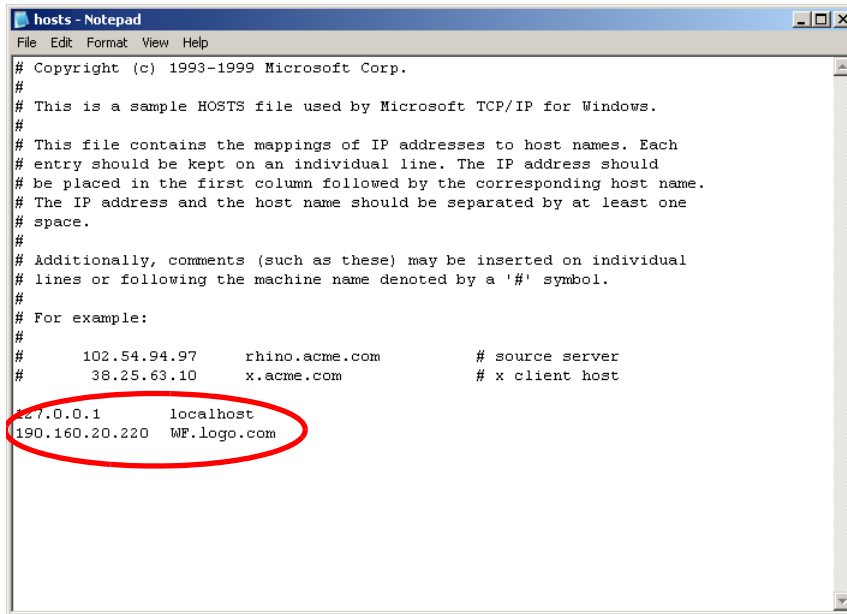
Now that the security certificate is installed, you will need to map the Web Filter's IP address to its host name. Proceed to Map the Web Filter's IP Address to the Server's Host Name.

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:

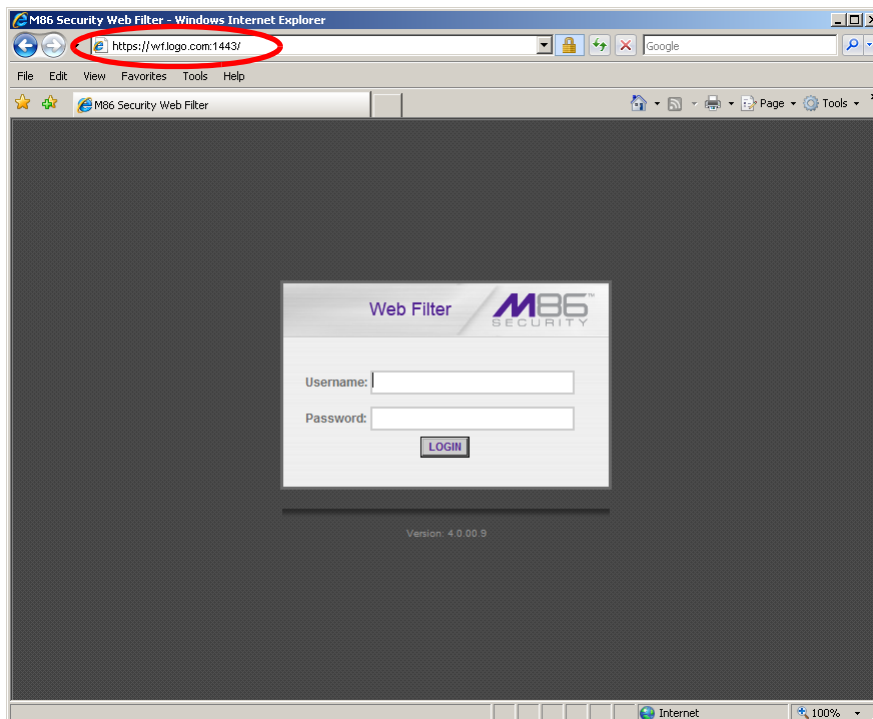


```

hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10      x.acme.com               # x client host
#
127.0.0.1        localhost
190.160.20.220  WF.logo.com

```

- 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 Client Connection.

Step 5: Test Filtering or the Mobile Client Connection

Test Filtering on the Web Filter

If the Web Filter has been set up in the Invisible, Router, or Firewall mode, you should test filtering the Web Filter.

A. Open a browser window on a network workstation, and then go to the following empty sites to test pornography filtering:

- <http://test.8e6.com>
- <http://testsite.marshal.com>
- <http://test.marshal8e6.com.tw>

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 Client Connection

If the Web Filter has been set up to use the Mobile mode, you should verify that the Mobile Client can reach the Web Filter.

A. Use a workstation on which the Mobile 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 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 functioning 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.

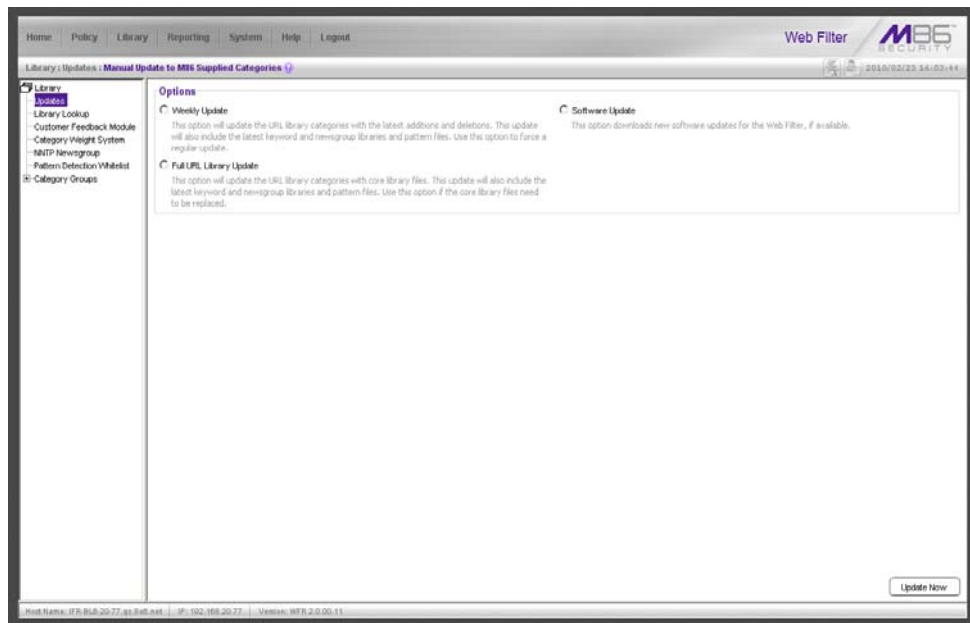
You may wish to print the confirmation page for future reference in dealing with technical issues.

Perform a Complete Library Update

Your Web Filter was shipped with the latest filtering 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** button at the top of the screen.
- B. From the navigation panel to the left, click Updates and select Manual Update from the menu:

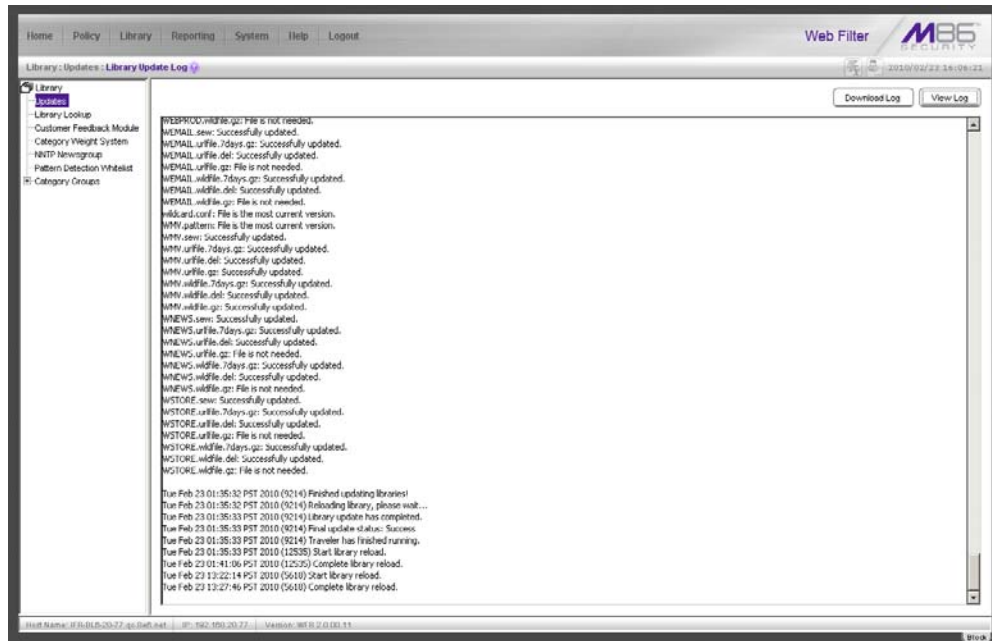



- C. In the Manual Update to M86 Supplied Categories window, click the radio button corresponding to **Full URL Library Update**.
- D. Click **Update Now** to begin the update process.


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/wf/documentation.asp> .

For troubleshooting tips, visit <http://www.m86security.com/software/8e6/ts/wf.html> .

 **IMPORTANT:** M86 Security recommends proceeding to the *Best Filtering and Reporting Practices* section to implement setup procedures for the reporting 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	Search Engines	
Bad Reputation Domains	Streaming Media	Generic Remote Access	Community Organizations	Web-based News groups	NOTE: The only M86 filtering category in the Pass/Allow group is Intranet/Internal Servers in the Custom Categories category group. This category must be maintained by your administrator. The other listings under Pass/Allow are suggested topics you might wish to set up.
BotNet	Flash Video	GoToMyPC	Local Community	Internet/Intranet Misc.	
Hacking	Generic Streaming Media	Remote Desktop	Education	Domain Landing	
Malicious Code/Virus	Quick Time Video	Secure Shell	Education	Edge Content Servers	
Phishing	Real Time Streaming Protocol	Virtual Network Computing	Educational Games	Invalid Web pages	
Spyware	Windows Media Video	pcAnywhere	Online Classes	Reviewed/Miscellaneous	
Web-based Proxies/Anonymizers	Internet Communication	Shopping	Reference	News/Reports	
Illegal/Questionable	Chat	Online Auction	Entertainment	News	
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 Email		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	
	FOFO		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

1. 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*

2. 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*

3. 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*

4. 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*

5. 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*

6. 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*

7. 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*

8. 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*

9. 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*

10. 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*

11. 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*

12. 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

1. 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*

2. 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*

3. 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*

4. 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*

5. 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*

6. 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*

7. 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*

8. 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*

9. 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*

10. 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*

11. 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*

12. 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*

13. 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*

14. 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*

15. 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*

16. 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*

17. 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

1. 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*

2. 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*

3. 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*

4. 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*

5. 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*

6. 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*

7. 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*

8. 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

1. 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*

2. 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*

3. 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*

4. 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*

5. 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



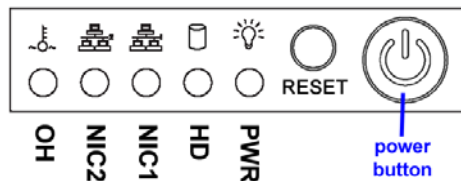
In the Web Filter User Guide index, see:

- *How to: configure filtering*
- *How to: set up pattern detection whitelisting*

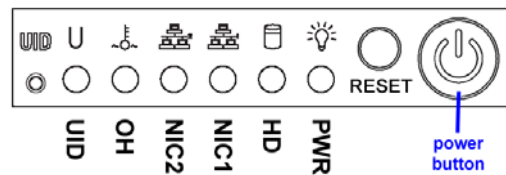
LED INDICATORS AND BUTTONS

Front Control Panels on 500 and 700 Series Units

Control panel buttons, icons, and LED indicators display on the right side of the 500 and 700 series model front panel. The buttons let you perform a function on the unit, while an LED indicator corresponding to an icon alerts you to the status of that feature on the unit.



500 series chassis front panel



700 series chassis front panel

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



UID (button) and U icon – On a 700 series unit, when the UID button is pressed, a steady blue LED displays on both the front and rear of the 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. On a 500 series unit, the LED is a steady green with link connectivity, and unlit if there with no link connectivity.



NIC1 (icon) – A flashing green LED indicates network activity on LAN1. On a 500 series unit, the LED is a steady green with link connectivity, and unlit if there with no link connectivity.



HDD (icon) – In addition to displaying in the control panel, this icon also displays on the front panel on each hard drive carrier. Hard drive activity is indicated by a flashing amber LED in the control panel, and a flashing green LED on a drive carrier. An unlit LED on a drive carrier may indicate a hard drive failure.



RESET

RESET (button) – The RESET button is used for rebooting the server.



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.



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 Panel on the 700 Series Unit

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.

UID (LED indicator) – On the rear of the 700 series chassis, to the right of the LAN ports, 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.



Front Control Panel on a 300 Series Unit

In addition to executing functions listed in the LCD panel menu, the keypad on the front of the server is also used for performing basic server functions.



- **Boot up** - Depress and hold the checkmark key for 3 seconds.
- **Reboot** - Depress and hold the checkmark key for 10 seconds.
- **Shut down** - Depress and hold the 'X' key for 10 seconds.

REGULATORY SPECIFICATIONS AND DISCLAIMERS

Declaration of the Manufacturer or Importer

Safety Compliance

USA:	UL 60950-1 1st ed. 2007
Europe:	Low Voltage Directive (LVD) 2006/95/EC to CB Scheme IEC 60950-1: 2001
Canada	CSA C22.2 No. 60950-1 1st ed. 2006
International:	IEC 60950-1 1st ed. 2001

Electromagnetic Compatibility (EMC)

USA:	FCC CFR47 Part 15 Subpart B
Canada:	IC ICES-003 Class A Limit
Europe:	EMC Directive, 2004/108/EC

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



NOTE: 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: 300-001-001, 500-003-001, 700-004-001

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 sur 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.

EC Declaration of Conformity

European Community Directives Requirement (CE)

Declaration of Conformity

Manufacturer's Name: M86 Security
 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 • EN60950-1:2001+A11:2004
 EMC • EN55022:2006+A1:2007
 • EN55024:1998+A2:2003
 • IEC CISPR 22:2008
 • IEC CISPR 24:1997+A1:2001+A2:2002
 • EN61000-3-2:2006
 • EN61000-3-3:2008
 • CFR47 Part 15 Subpart B: 2009

Product Name(s): Security Appliance
 Product Model Number(s): 300-001-001, 500-003-001, 700-004-001

Year in which conformity is declared: 2010

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: April 5, 2010

Full Name: Gregory P. Smith

Position: Director, Engineering Operations

INDEX

A

Activate and Register the R3000 53
Always Allow Custom Category 71

B

Bandwidth/Productivity 63
boot up
 300 series server 74
 500, 700 series server 73

C

Category block 59, 66
Change Quick Start password 29
CSA 75
Custom Block/Warn/X Strikes/Quota pages 68, 71
Custom Category (blocked) 61
Custom Lock, Block, Warn, X Strikes, Quota pages 60
Customize an M86 Supplied Category 70

E

EMC 75
Exception URL bypass 62

F

FCC 75
File type blocking 62

G

Game patterns 65
General/Productivity 68

H

HTTPS settings 66
HyperTerminal Setup 22

I

ICES-003 75
IEC 75
IM patterns 65
IP exceptions 72

L

LCD Panel 19, 31
Local category adds/deletes 70
Login screen 25
LVD 75

M

Minimum Filtering Level 61
Mobile Client 52

O

Overall Quota 63, 70
Override Account bypass 61
Override Accounts 72

P

P2P patterns 64
Pass/Allow 71
Pattern detection bypass 72
ping the SR 38
Power Supply Precautions 16
Proxy Patterns 62

Q

Quick Start menu 25

R

Rack Setup Precautions 6
Real Time Probe information 68
reboot 29, 35
 300 series server 74
 500, 700 series server 73
Remote Access patterns 66
Reset Admin account 29
Reset system to factory defaults 29
Reset WF Admin Console Password 35
RoHS compliant 76
Rule block 59, 67

S

SE Keywords 67
Search Engine Keywords 60
serial port cable 19, 20
shut down 35
 300 series server 74
 500, 700 series server 73
Streaming Media patterns 65

T

Threats/Liabilities 59
Time Based Profiles 63, 69
Time Quota/Hit Quota 63, 69

U

UID 73
UL 75

URL exceptions 71
URL Keywords 60, 67

W

Warn Feature with higher thresholds 68
Warn option with low filter settings 64
Warn-strike 64
Warn-strike with higher thresholds 69

X

X-Strike on blocked categories 59

M86 Security Corporate Headquarters (USA):
828 West Taft Avenue Orange, CA 92865-4232 • Tel: 714.282.6111 or 888.786.7999
Fax: 714.282.6116 (Sales/Technical Support) • 714.282.6117 (General Office)