



M86 IR
INSTALLATION GUIDE
Model: MSA

M86 IR INSTALLATION GUIDE FOR MSA

© 2011 M86 Security

All rights reserved. Printed in the United States of America

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# IR-IG-MSA-111010

CONTENTS

M86 IR INTRODUCTION	1
About this Document.....	1
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
Rack Mount the Server.	6
Rack Setup Precautions	6
Rack Mount Instructions	7
Optional: Install the Chassis Rails	7
Optional: Install the Traditional UP Racks	9
Optional: Install the Open Racks	11
Install the Chassis into the Rack	14
Check the Power Supply.	15
Power Supply Precautions	15
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
Administrator Console Setup Requirements	19
Step 1A: Quick Start Setup Procedures.....	20
Link the Workstation to the IR	20
Monitor and Keyboard Setup	20
Serial Console Setup	20
HyperTerminal Setup Procedures	21
Login screen	24
Quick Start menu screen	24
Quick Start menu: administration menu	25
Change filtering mode	26
Configure network interface LAN1	26
Configure network interface LAN2	26
Configure default gateway	26
Configure DNS servers	26
Configure host name	27

Time Zone regional setting	27
Non-Quick Start procedures or settings	28
Reboot system	28
Change Quick Start password	28
Reset admin console account	28
System Status screen	29
Log Off, Disconnect the Peripherals	29
Physically Connect the IR to the Network	30
Access the IR Online	31
Accept the Security Certificate in Firefox	32
Temporarily Accept the Security Certificate in IE	34
Accept the Security Certificate in Safari	35
Accept the Security Certificate in Chrome	36
Step 2: Log in Web Filter, Generate SSL Certificate.....	37
Log in to the Web Filter	37
Generate SSL Certificate	38
IE Security Certificate Installation Procedures	40
Access the IR splash page	40
Accept the Security Certificate in IE	40
Windows XP or Vista with IE 8.....	40
Windows 7 with IE 8.....	44
Map the IR's IP Address to the Server's Host Name	45
Step 3: Test Filtering or the Mobile Client Connection.	47
Test Filtering	47
Test the Mobile Client Connection	47
Step 4: Set Library Updates.	48
Activate and Register the Web Filter	48
Perform a Complete Library Update	48
Monitor the Library Update Process	50
Step 5: Change the ER Admin User Name and Password, Set Self-Monitoring.	51
Log in to the ER Administrator Console	51
Change User Name and Password	52
Set Self-Monitoring	53
Step 6: Launch the ER Client.....	54
CONCLUSION	56
BEST FILTERING PRACTICES	57
Threat Class Groups.....	58
I. Threats/Liabilities	59
A. Category block	59
B. Rule block	59
C. X-Strike on blocked categories	59
D. Custom Lock, Block, Warn, X Strikes, Quota pages	60
E. URL Keywords	60
F. Search Engine Keywords	60
G. Custom Category (blocked)	61
H. Minimum Filtering Level	61
I. Override Account bypass	61
J. Exception URL bypass	62

K. Proxy Patterns	62
L. File type blocking	62
II. Bandwidth/Productivity	63
A. Time Quota/Hit Quota	63
B. Overall Quota	63
C. Time Based Profiles	63
D. Warn option with low filter settings	64
E. Warn-strike	64
F. P2P patterns	64
G. IM patterns	65
H. Game patterns	65
I. Streaming Media patterns	65
J. Remote Access patterns	66
K. HTTPS settings	66
L. Category block	66
M. Rule block	67
N. SE Keywords	67
O. URL Keywords	67
P. Custom Block/Warn/X Strikes/Quota pages	68
Q. Real Time Probe information	68
III. General/Productivity	68
A. Warn Feature with higher thresholds	68
B. Warn-strike with higher thresholds	69
C. Time Quota/Hit Quota	69
D. Time Based Profiles	69
E. Overall Quota	70
F. Customize an M86 Supplied Category	70
G. Local category adds/deletes	70
H. Custom Block/Warn/X Strikes/Quota pages	71
IV. Pass/Allow	71
A. Always Allow Custom Category	71
B. URL exceptions	71
C. IP exceptions	72
D. Override Accounts	72
E. Pattern detection bypass	72
BEST REPORTING PRACTICES	73
Reporting Scenarios	74
I. Executive Report and Drill Down Report exercise	74
Step A: Start with the dashboard for a high level activity overview	74
Step B: Further investigate using a Summary Drill Down Report	75
Step C: Create a New Report using yesterday's date scope	75
Step D: Create a double-break report with two sets of criteria	76
Step E: Create a Detail Drill Down Report to obtain a list of URLs	77
II. Double-break Report and Export Report exercise	78
Step A: Drill down to view the most visited sites in a category	78
Step B: Modify the report view to only display top 10 site records	79
Step C: Export the report view in the .PDF output format	80
III. Save and schedule a report exercise	82
Step A. Save a report	82
Step B. Schedule a recurring time for the report to run	83
IV. Create a custom category group and generate reports	84
Step A: Create a custom category group	84
Step B: Run a report for a specified category group	85
V. Create a custom user group and generate reports	85

Step A: Create a custom user group	85
Step B: Generate a report for a custom user group	86
Summary Report	86
Detail Report	86
IMPORTANT INFORMATION ABOUT USING THE ER IN THE EVALUATION MODE ..	87
Evaluation Mode Pop-Ups.....	87
Administrator Console, Expiration Screen.....	87
ER Web Client, ER Server Information Window.....	88
LED INDICATORS AND BUTTONS	89
Diagrams and Descriptions	89
REGULATORY SPECIFICATIONS AND DISCLAIMERS	90
Declaration of the Manufacturer or Importer.....	90
Safety Compliance	90
Electromagnetic Compatibility (EMC)	90
Federal Communications Commission (FCC) Class A Notice (USA)	90
FCC Declaration of Conformity	90
Electromagnetic Compatibility Class A Notice	91
Industry Canada Equipment Standard for Digital Equipment (ICES-003)	91
Bureau of Standards Metrology and Inspection (BSMI) - Taiwan	91
EC Declaration of Conformity	92
European Community Directives Requirement (CE)	92
APPENDIX: CONSOLE SETUP PROCEDURES	93
Preliminary Setup.....	93
Workstation Configuration.....	93
Link the Workstation to the IR.	94
The Boot Up Process	94
Security Certificate Acceptance Procedures.	95
Accept the Security Certificate in Firefox	95
Temporarily Accept the Security Certificate in IE	97
Accept the Security Certificate in Safari	98
Network Setup.	99
Access the Web Filter Administrator Console	99
Network	100
Network: Operation Mode	101
Network: LAN Settings	102
Network: NTP Servers	103
Network: Regional Setting	104
Physically Connect the IR to the Network.	105
Test the IR Console Connection.....	106
INDEX	107

M86 IR INTRODUCTION

Thank you for choosing to install the M86 Security IR (Web Filter with Integrated Reporter). This product combines the Web Filter with the Enterprise Reporter (ER) to track end user Internet activity and generate reports that assist administrators in developing policies and targeting sites to be filtered, in order to maximize bandwidth utilization and productivity.

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

The ER is comprised of the server and client application. Once the ER server is configured and Web Filter log files have populated the database, an administrator can use the ER client reporting application to virtually generate an unlimited number of queries and reports from data in the database. This data shows which end user is accessing which site, the duration of each site visit, and the frequency of these visits. The client gives the administrator the ability to interrogate massive datasets through flexible drill-down technology, until the desired view is obtained, and then memorize and save the view to a user-defined report menu for repetitive, scheduled execution and distribution.

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

Additionally, quick setup procedures to implement the best reporting practices using the ER client are included in the Best Reporting Practices section that follows the Best Filtering Practices section of this guide.

About this Document

This document is divided into the following sections:

- **Introduction** - This section is comprised of an overview of the IR 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 IR in your network environment
- **Install the Server** - This section explains how to configure the IR for filtering and reporting
- **Conclusion** - This section indicates that the installation steps have been completed
- **Best Filtering Practices** - This section includes a chart of library categories organized into Threat Class Groups, accompanied by filtering scenarios and directions for implementing the best filtering practices to secure your network, prevent excessive bandwidth usage, and increase productivity

- **Best Reporting Practices** - This section includes reporting scenarios and instructions for implementing the best reporting practices to capture a snapshot of end user activity on your network that tells you whether or not policies are being enforced
- **Evaluation Mode** - This section gives information on using the ER in the evaluation mode
- **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 IR model referenced in this document
- **Appendix** - The appendix provides an alternate way of installing the Web Filter by using a crossover cable
- **Index** - An alphabetized list of some topics included in this document

Conventions Used in this Document

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



NOTE: The “note” icon is followed by additional information to be considered.



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



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



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 M86 IR Web Filter User Guide or ER Web Client User Guide. This icon is found in the Best Filtering / Reporting 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 IR unit
- 1 AC Power Cord
- 1 Serial Port Cable

User guides can be obtained at <http://www.m86security.com/support/R3000/documentation.asp> and <http://www.m86security.com/support/Enterprise-Reporter/documentation.asp>.

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



NOTE: Rack mount brackets (2) also may be included for installing the unit in a rack.

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



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

Select a Site for the Server

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

- Clean and relatively free of excess dust.
- Well-ventilated and away from sources of heat, with the ventilating openings on the server kept free of obstructions.
- Away from sources of vibration or physical shock.
- Isolated from strong electromagnetic fields and noise caused by electrical devices such as elevators, copy machines, air conditioners, large fans, large electric motors, radio and TV transmitters, and high-frequency security devices.
- Access space provided so the server power cord can be unplugged from the power supply or the wall outlet—this is the only way to remove the AC power cord from the server.
- Clearance provided for cooling and airflow: Approximately 30 inches (76.2 cm) in the back and 25 inches (63.5 cm) in the front.
- Located near a properly earthed, grounded, power outlet.

Rack Mount the Server

Rack Setup Precautions



WARNING:

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


- The weight of all units in the rack is evenly distributed. Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- The rack will not tip over when the server is mounted, even when the unit is fully extended from the rack.
- For a single rack installation, stabilizers are attached to the rack.
- For multiple rack installations, racks are coupled together.
- Reliable earthing of rack-mounted equipment is maintained at all times. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).
- A power cord will be long enough to fit into the server when properly mounted in the rack and will be able to supply power to the unit.
- The connection of the server to the power supply will not overload any circuits. Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment name-plate 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

Optional: Install the Chassis Rails


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

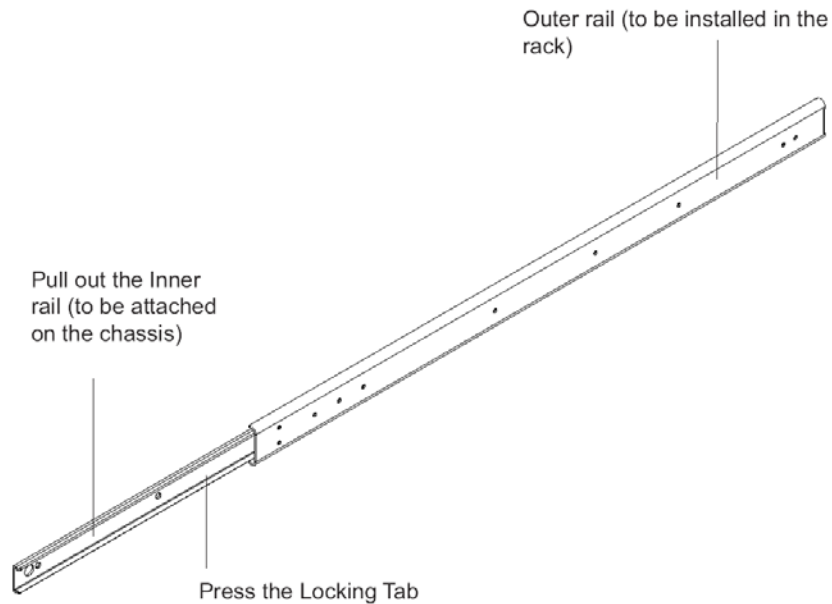
 **CAUTION:** Please make sure that the chassis covers and chassis rails are installed on the chassis before you install the chassis into the rack. To avoid personal injury and property damage, please carefully follow all the safety steps listed below:

Before installing the chassis rails:

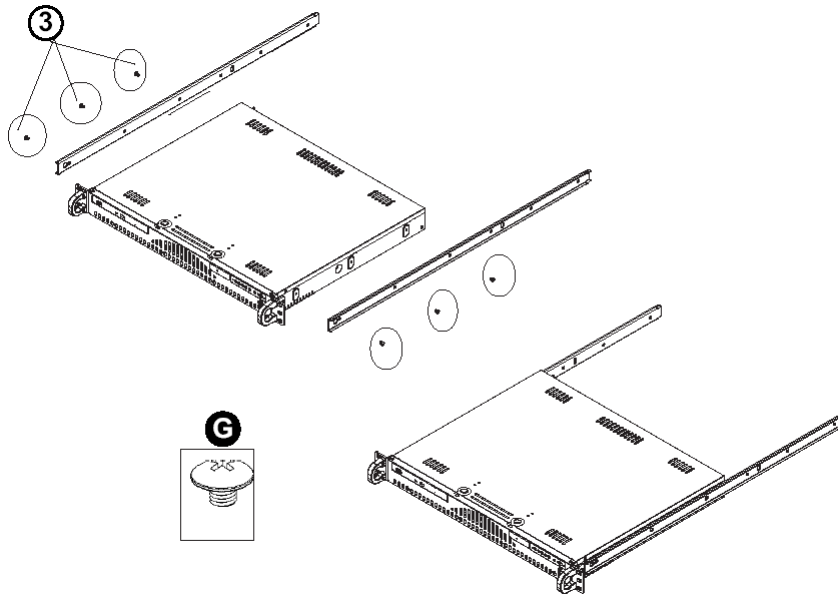
- Close the chassis using the chassis cover.
- Unplug the AC power cord(s).
- Remove all external devices and connectors.

1. Included in the shipping package are a pair of rail assemblies. In each rail assembly, locate the inner rail and the outer rail.
2. Press the locking tab to release the inner rail from its locking position and pull out the inner rail from the rail assembly.

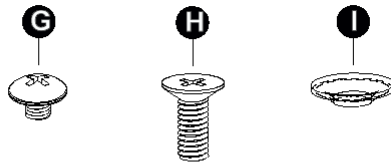
 **NOTE:** The inner rails are to be attached to the chassis and the outer rails are to be installed in the rack.



3. Locate the three holes on each side of the chassis and locate the three corresponding holes on each of the inner rail.



4. Attach an inner rail to each side of the chassis and secure the inner rail to the chassis by inserting three Type G screws through the holes on each side of the chassis and the inner rail. (See the diagram below for a description of the Type G screw.)



- G. Round head M4 x 4 mm [0.157]
- H. Flat head M5 x 12 mm [0.472]
- I. Washer for M5

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

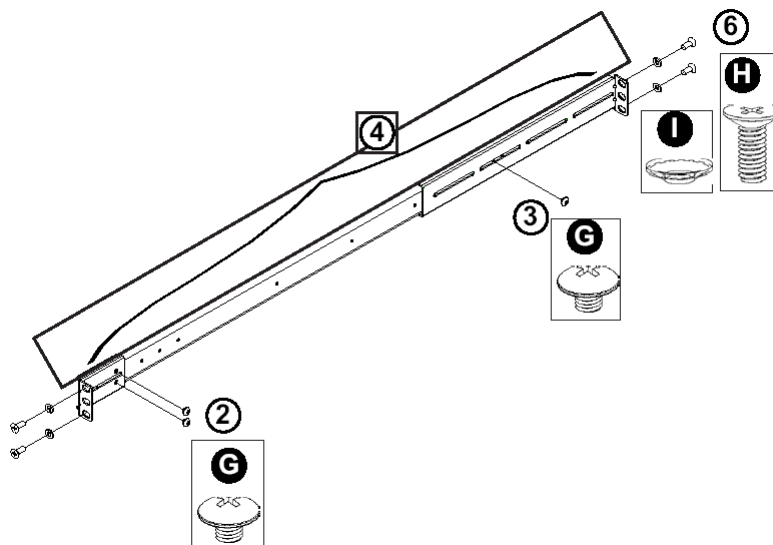
Optional: Install the Traditional UP Racks

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



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

- Determine the placement of each component in the rack before you install the rails.
 - Install the heaviest server components on the bottom of the rack first, and then work up.
1. In the package, locate a pair of front (short) and rear (long) brackets. Please note that the brackets are marked with Up/Front Arrows (front) and Up/Rear arrows (rear).
 2. Secure the front (short) bracket (marked with the Up/Front arrows) to the outer rail with two Type G screws. (See the previous page for a description of the Type G screw.)
 3. Attach the rear (long) bracket to the other end of the outer rail and secure the rear (long) bracket to the outer rail with a Type G screw as shown below.
 4. Measure the depth of your rack and adjust the length of the rails accordingly.
 5. Repeat the same steps to install the other outer rail on the chassis.
 6. Secure both outer rail assemblies to the rack with Type H screws and Type I washers. (See the previous page for descriptions of Type H and Type I hardware components.)

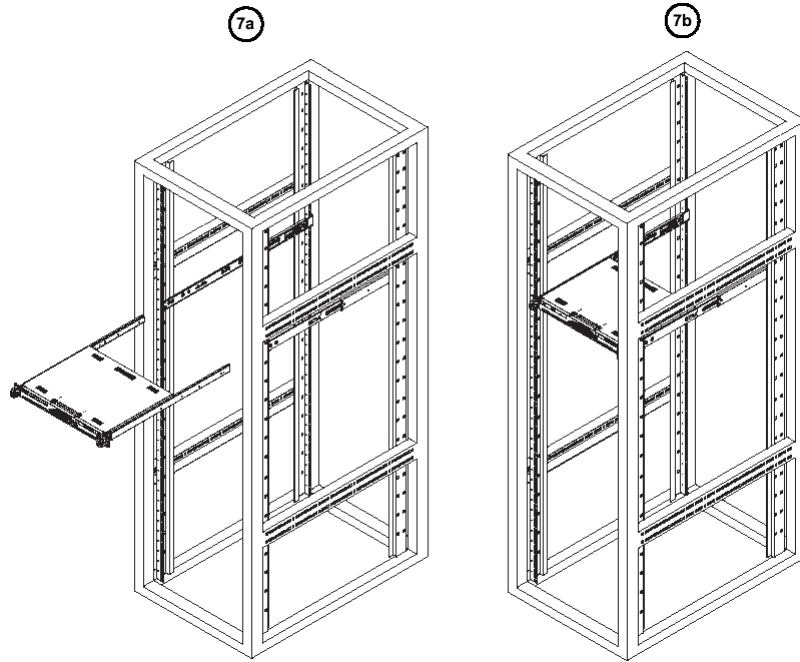


7. Slide the chassis into the rack as shown below.



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

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



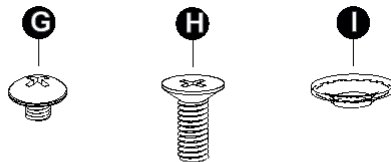
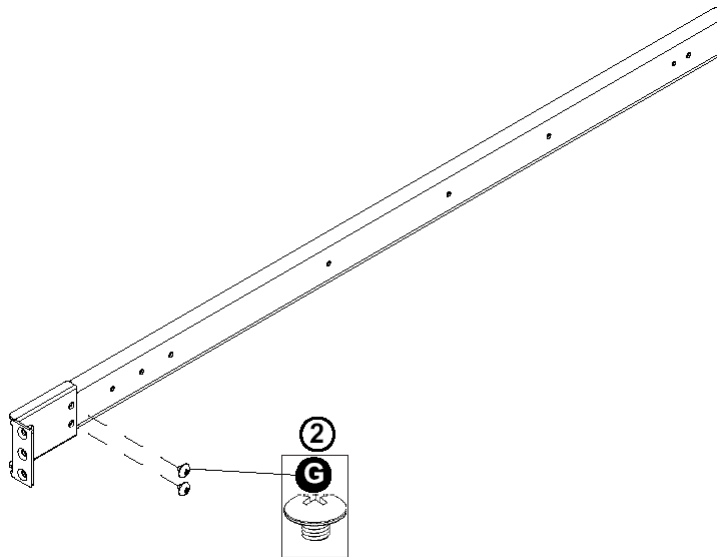
Optional: Install the Open Racks

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



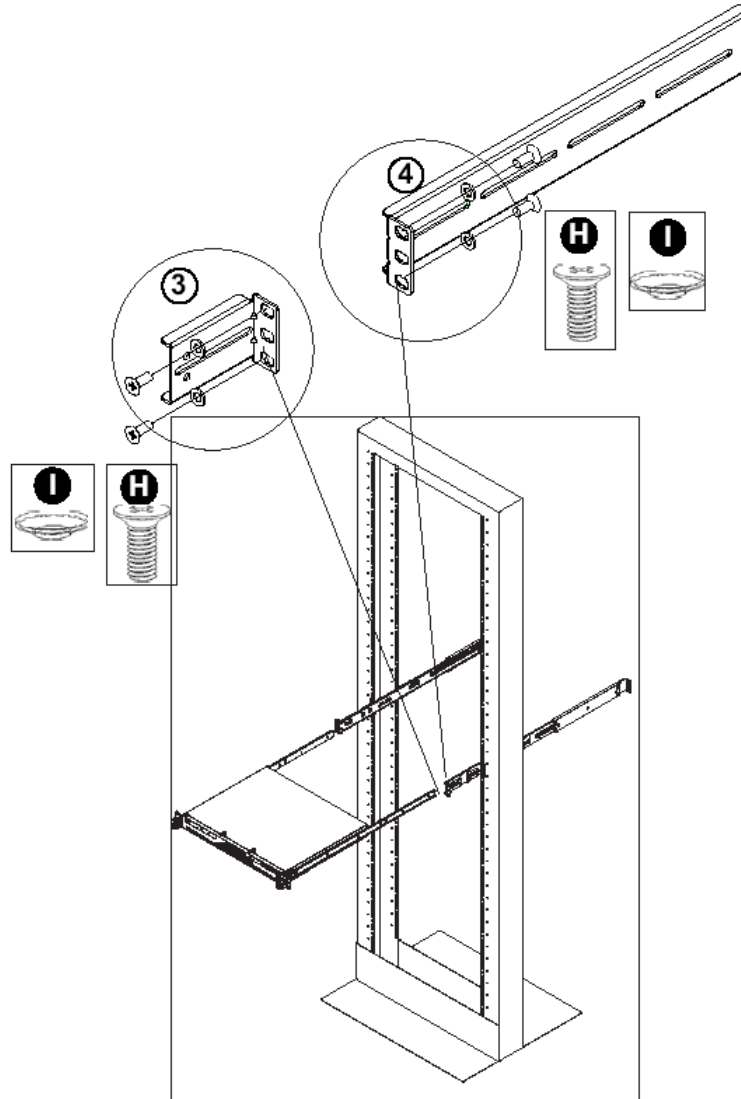
NOTE: The rails are designed to fit in the racks with the depth of 28" to 33".

- Determine the placement of each component in the rack before you install the rails.
 - Install the heaviest server components on the bottom of the rack first, and then work up.
1. In the package, locate a pair of front (short) and rear (long) brackets. Please note that the brackets are marked with Up/Front Arrows (front) and Up/Rear arrows (rear).
 2. Secure the front (short) bracket (marked with the Up/Front arrows) to the outer rail with two Type G screws as shown below.



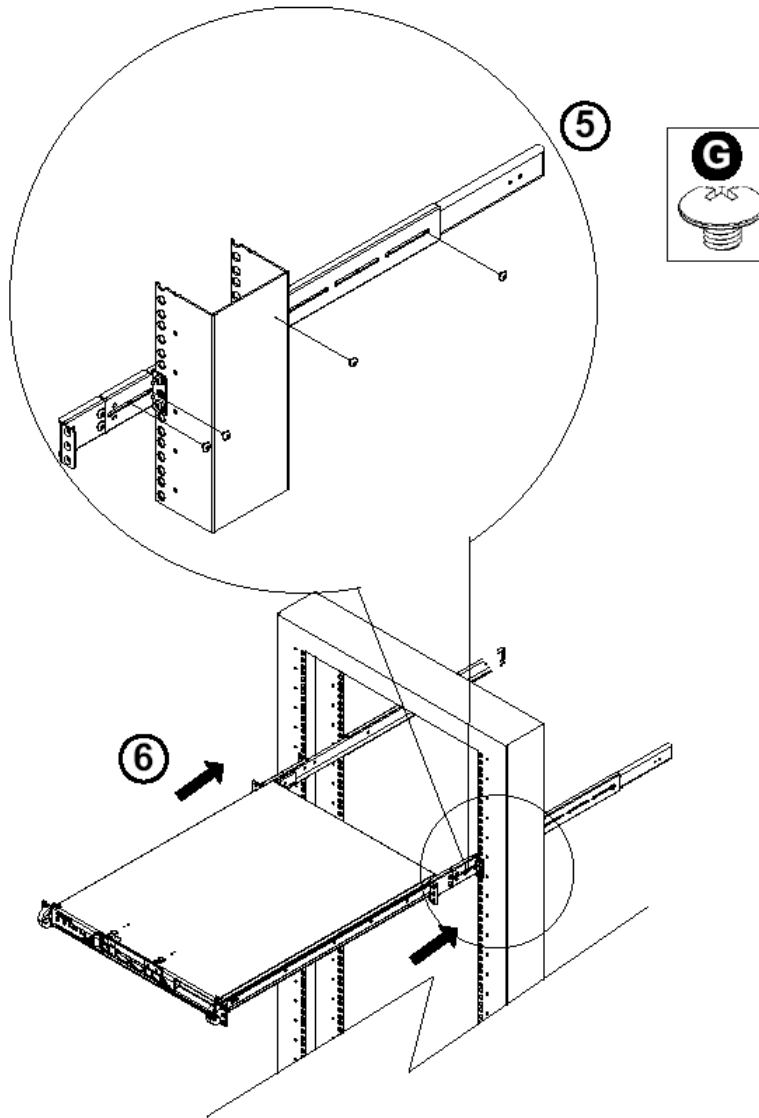
- G. Round head M4 x 4 mm [0.157]
- H. Flat head M5 x 12 mm [0.472]
- I. Washer for M5

3. Attach the front (short) bracket to the front end of the rack, and secure it to the rack with two Type H screws and Type I washers as shown below. (See the previous page for descriptions of Type H and Type I hardware components.)
4. Attach the rear (long) bracket to the rear end of the rack, and secure it to the rack with two Type H screws and Type I washers as shown below. Repeat the same steps to install the other outer rail to the other side of rack.



5. Measure the depth of your rack and adjust the length of the rails accordingly. Then, secure the rails to the chassis with Type G screws.

- Slide the inner rails which are attached to the chassis into the outer rails on the rack.



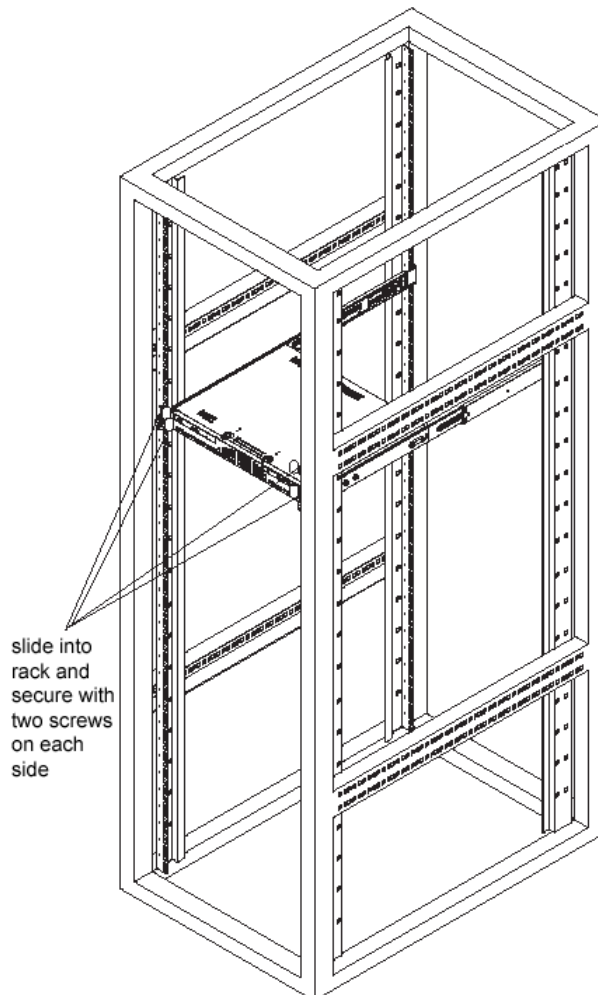
Install the Chassis into the Rack



CAUTION: Before installing the chassis into the rack:

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

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



Check the Power Supply

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

Power Supply Precautions



WARNING:

- Use a regulating uninterruptible power supply (UPS) to protect the server from power surges, voltage spikes and to keep the server operating in case of a power failure.
- In geographic regions that are susceptible to electrical storms, M86 Security highly recommends plugging the AC power cord for the server into a surge suppressor.
- Use appropriately rated extension cords or power strips only.
- Allow power supply units to cool before touching them.

General Safety Information

Server Operation and Maintenance Precautions

**WARNING:**

Observe the following safety precautions during server operation and maintenance:



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



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



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



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



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

- Do not insert objects through openings in the chassis. Doing so could result in a short circuit that might cause a fire or an electrical shock.
- Do not operate the server in an explosive atmosphere, in the presence of flammable gases.
- To ensure proper cooling, always operate the server with its covers in place. Do not block any openings on the chassis. Do not place the server near a heater.
- Always exit the software application properly before turning off the server to ensure data integrity.
- Do not expose the server to rain or use near water. If liquids of any kind should leak into the chassis, power down the server, unplug it, and contact M86 Security technical support.
- Disconnect power from the server before cleaning the unit. Do not use liquid or aerosol cleaners.

AC Power Cord and Cable Precautions



WARNING:

- The AC power cord for the server must be plugged into a grounded, power outlet.
- Do not modify or use a supplied AC power cord if it is not the exact type required in the region where the server will be installed and used. Replace the cord with the correct type.
- Route the AC power cord and cables away from moving parts and foot traffic.
- Do not allow anything to rest on the AC power cord and cables.
- Never use the server if the AC power cord has been damaged.
- Always unplug the AC power cord before removing the unit for servicing.

Electrical Safety Precautions



WARNING:

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



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

- To prevent damage to the server, read the information in this document for selection of the proper input voltage.
- Do not wear rings or wristwatches when troubleshooting electrical circuits.
- To avoid fire hazard, use only the specified fuse(s) with the correct type number, voltage, and current ratings. Only qualified service personnel should replace fuses.
- Qualified service personnel should be properly grounded when servicing the unit.
- Qualified service personnel should perform a safety check after any service is performed.

Motherboard Battery Precautions



CAUTION:

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

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

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

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

ATTENTION: IL Y A DANGER D'EXPLOSION S'IL Y A 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 link the workstation to the IR. You have the option of using the text-based Quick Start setup procedures described in Step 1A, or the Administrator console setup procedures described in the Appendix.

Quick Start Setup Requirements

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

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

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

Administrator Console Setup Requirements

The following hardware is required for the Administrator console setup procedures:

- IR with AC power cord
- CAT-5E crossover cable
- PC laptop computer, or PC monitor with AC power cord and keyboard

Go to the Appendix to execute Console Setup Procedures.

Step 1A: Quick Start Setup Procedures

Link the Workstation to the IR

Monitor and Keyboard Setup

- A. Connect the PC monitor and keyboard cables to the rear of the chassis (see Fig. 1).
- B. Turn on the PC monitor.
- C. Connect the AC power cord to the back of the chassis and plug the cord into a UPS power supply unit.
- D. Power on the IR by dropping down the face plate and pressing the large button at the right of the front panel (see Fig. 2).

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

Serial Console Setup

- A. Using the serial port cable (and USB DB9 serial adapter, if necessary), connect the laptop to the rear of the chassis (see Fig. 1).
- B. Power on the laptop.
- C. Connect the AC power cord to the back of the chassis and plug the cord into a UPS power supply unit.
- D. Power on the IR by dropping down the face plate and pressing the large button at the right of the front panel (see Fig. 2).



Fig. 1 - Portion of MSA chassis rear

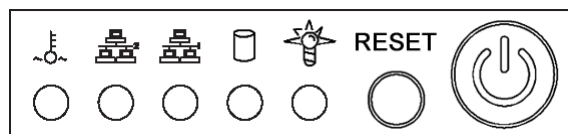


Fig. 2 - Diagram of MSA chassis front panel, power button at far right

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

HyperTerminal Setup Procedures

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



NOTE: *HyperTerminal is no longer included with Windows as of Microsoft's Vista system. Please note on Microsoft's Web page "What happened to HyperTerminal?" at <http://windows.microsoft.com/en-us/windows-vista/What-happened-to-HyperTerminal> (accessed August 16, 2011), 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."*

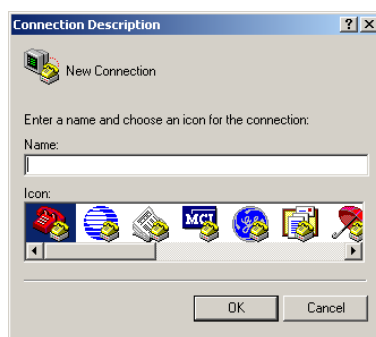
If you are using a Windows Vista or Windows 7 machine to conduct these quick start setup procedures and do not have an equivalent type of terminal emulator program installed on your workstation, Hilgraeve, Inc., the maker of HyperTerminal, offers HyperTerminal Private Edition for Windows Vista and Windows 7. The following information is included on Hilgraeve's Web page at <http://www.hilgraeve.com/hyperterminal.html> (accessed August 16, 2011): "HyperTerminal Private Edition is an award winning terminal emulation program capable of connecting to systems through TCP/IP Networks, Dial-Up Modems, and COM ports.... Download HyperTerminal free 30 day trial."

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

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

On the Windows XP machine:

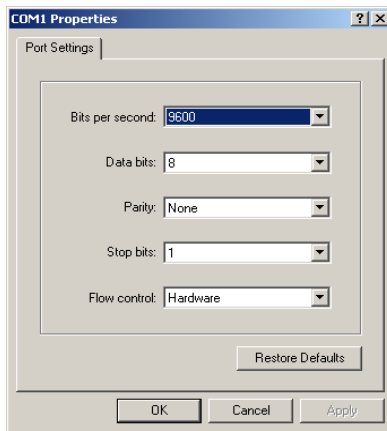
- A. Launch HyperTerminal by going to Start > Programs > Accessories > Communications > HyperTerminal:



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



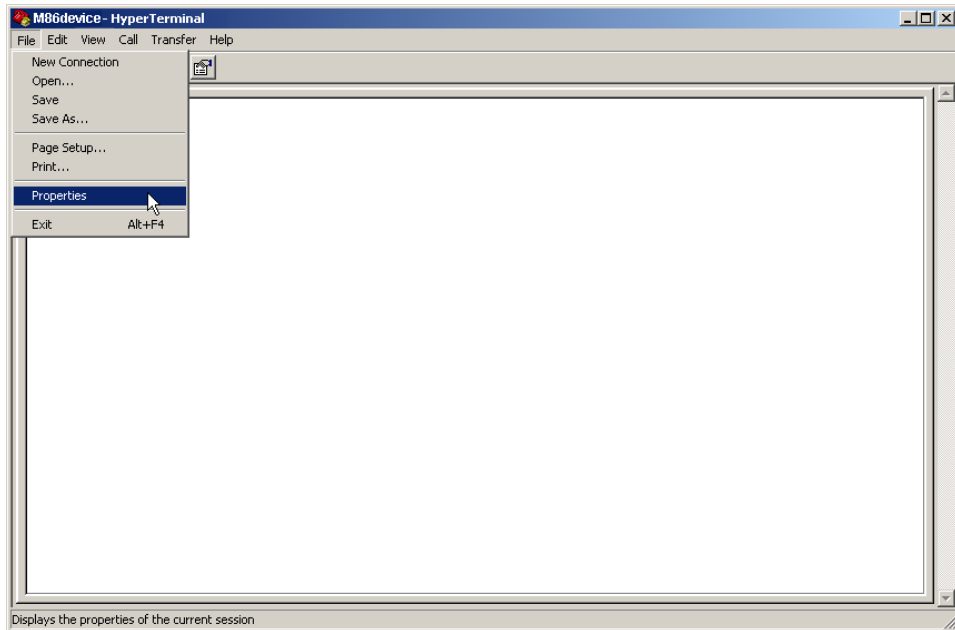
- C. At the **Connect using** field, select the COM port assigned to the serial port on the laptop (probably “COM1”), and then click **OK** to open the Properties dialog box, displaying the Port Settings tab:



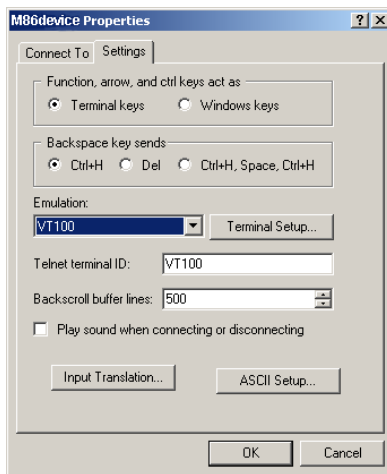
- D. Specify the following session settings:

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

- E. Click **OK** to connect to the HyperTerminal session:



- F. In the HyperTerminal session window, go to File > Properties to open the Properties dialog box, displaying the Connect To and Settings tabs:



- G. Click the Settings tab, and at the **Emulation** menu select “VT100”.
- H. Click **OK** to close the dialog box, and to go to the login screen.

Login screen

The login screen displays after powering on the IR unit using a monitor and keyboard, or creating a HyperTerminal session.



NOTES: If using a HyperTerminal session, the login screen will display with black text on a white background.

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

- A. At the **login** prompt, type in **menu**.
- B. Press the **Enter** key to display the Password prompt.
- C. At the **Password** prompt, type in the following: **#s3tup#r3k**
- D. Press **Enter** to display the Quick Start menu screen.

Quick Start menu screen

```
Wed Jun 9 10:23:54 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

```

Wed Jun  9 10:25:21 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
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 for configuring the IR:

- 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 IR and review the entries you made using the Quick Start setup, press **1** to view the System Status screen.



NOTES: Changing your password using option C, “Change Quick Start password”, will change the password for the console menu but not the Web Filter console login screen. Option D, “Reset admin console account”, should be used for resetting the administrator console username and password to the factory default ‘admin’/‘user3’ and for unlocking all IP addresses currently locked.

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.

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

```

Wed Jun  9 10:25:38 PDT 2010
M86 Security
System Status - updates every 10 seconds

Serial Number  5K0259112014
Web Filter is configured in Invisible mode
lan1 is the Capturing Interface
lan1 IP = 192.168.20.56 Mask = 255.255.0.0           Active
lan2 is the Management and Blocking Interface
lan2 IP = 1.2.3.4 Mask = 255.0.0.0                 Inactive
Default gateway IP: 192.168.20.1
Web Filter host name: r3000-20-56.qc.8e6.net

DNS server IP address(es): 192.168.168.200 192.168.20.1
Regional timezone setting: US/Pacific

Web Filter processing is normal
Current Version: Web Filter 4.0.10.7
Library was last updated on 2010/06/09
ER processing is normal

Press any key to return to menu...

```

The System Status screen contains the following information:

- **Serial Number** assigned to the chassis
- **Operation Mode** specified in screen 3 (Change filter 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
- Current status of the ER



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 IR.

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

Physically Connect the IR to the Network

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


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

- A. Restart the server using the steps defined below (i-iii). These steps must always be performed when restarting the IR. **Never** reset the server by using the power or reset buttons.
 - i. From the navigation panel of the System section of the Web Filter console, click Control and select Reboot from the pop-up menu to display the Reboot window.
 - ii. Click the **Reboot** button.
 - iii. From the time you click Reboot, you have approximately 2 minutes to perform sub-steps B through E while the IR goes through the reboot process.
- B. If you used a crossover cable for the quick start setup procedures, disconnect that crossover cable from the IR.
- C. Plug one end of a standard CAT-5E cable into the IR's LAN 1 port.
- D. Plug the other end of the CAT-5E cable into an open port on the network hub that handles the Internet traffic you wish to filter.
- E. Repeat sub-steps B and C for the IR's LAN 2 port.



Portion of MSA chassis rear

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

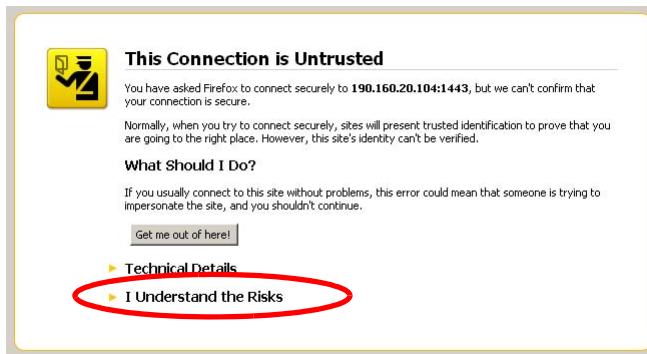
 **NOTE:** If you receive a connection failure message during the reboot process, please disregard it, as this often occurs when there is a change in the IP address.

Access the IR Online

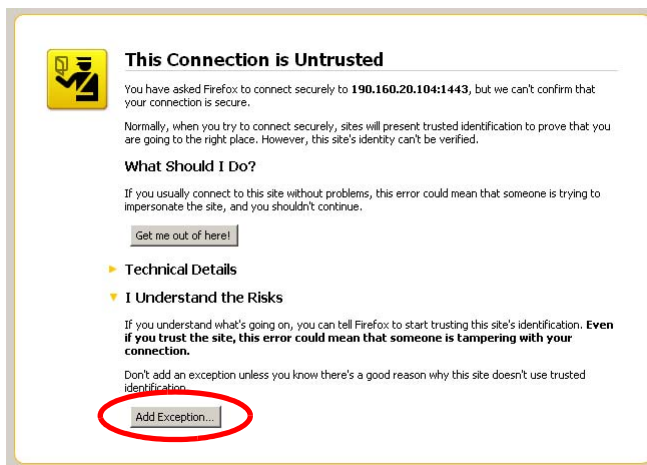
- A. From the workstation you are using, launch an Internet supported browser such as Firefox 6.0, Internet Explorer 8.0, Safari 5.1, or Google Chrome 13.0.
- B. Type in **https://x.x.x.x:1443** in the address field (in which 'x.x.x.x' represents the LAN 1 IP address assigned to the IR).
- C. Click **Go** to display the security issue page:
 - If using Firefox, proceed to Accept the Security Certificate in Firefox.
 - If using IE, proceed to Temporarily Accept the Security Certificate in IE.
 - If using Safari, proceed to Accept the Security Certificate in Safari.
 - If using Google Chrome, proceed to Accept the Security Certificate in Chrome.
 - If the security issue page does not display in your browser, verify the following:
 - The IR is powered on.
 - The IR is connected to the same hub as your router/firewall.
 - Can the administrator workstation normally connect to the Internet?
 - Is the IR 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 IR's LAN 1 IP address?
 - If pinging the IP address of the IR is unsuccessful, try restarting the network service or rebooting the IR.
 - If still unsuccessful, contact an M86 Security solutions engineer or technical support representative.

Accept the Security Certificate in Firefox

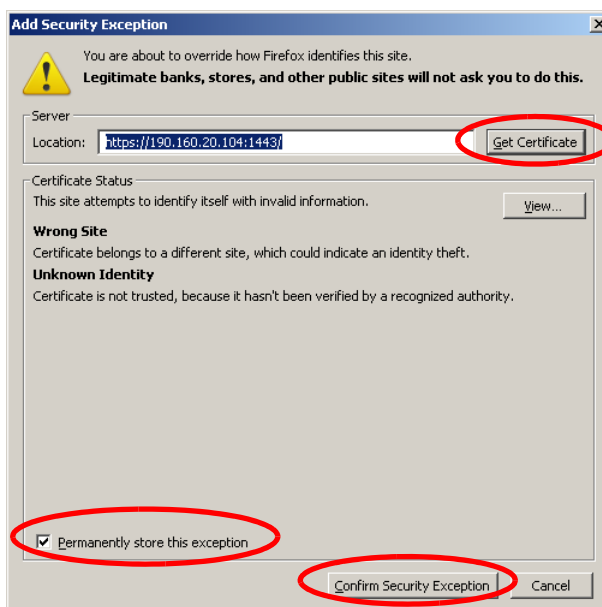
- A. If using a Firefox browser, in the page “This Connection is Untrusted,” click the option **I Understand the Risks**:



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




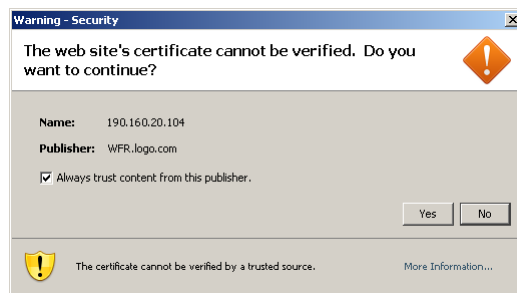
Clicking Add Exception opens the Add Security Exception window:



- C. In the Add Security Exception window, click **Get Certificate** and wait a few seconds until the security certificate is obtained by the server.
- D. With the checkbox **Permanently store this exception** selected (or grayed-out), click **Confirm Security Exception** to open the Welcome window of the IR user interface:



 **NOTE:** You will need to add a security exception for the Web Filter, Enterprise Reporter (Web Client), and Enterprise Reporter Administration Module when you attempt to access each of these applications for the first time. On a newly installed unit, the ER Web Client will remain inaccessible until logs are transferred to the ER Administration Module and the ER's database is built.

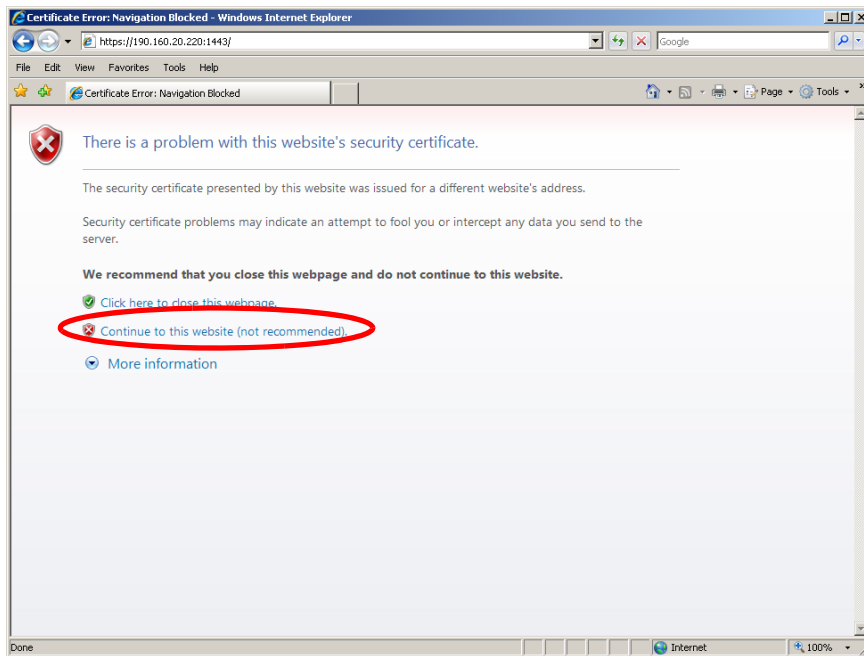


When attempting to access the Web Filter user interface for the first time, the Security warning dialog box (shown in the sample image at left) will open instead of the Security Exception page. With the checkbox "Always trust content from this publisher." populated, click **Yes** to close the Security warning dialog box and to access the login window of the Web Filter user interface.

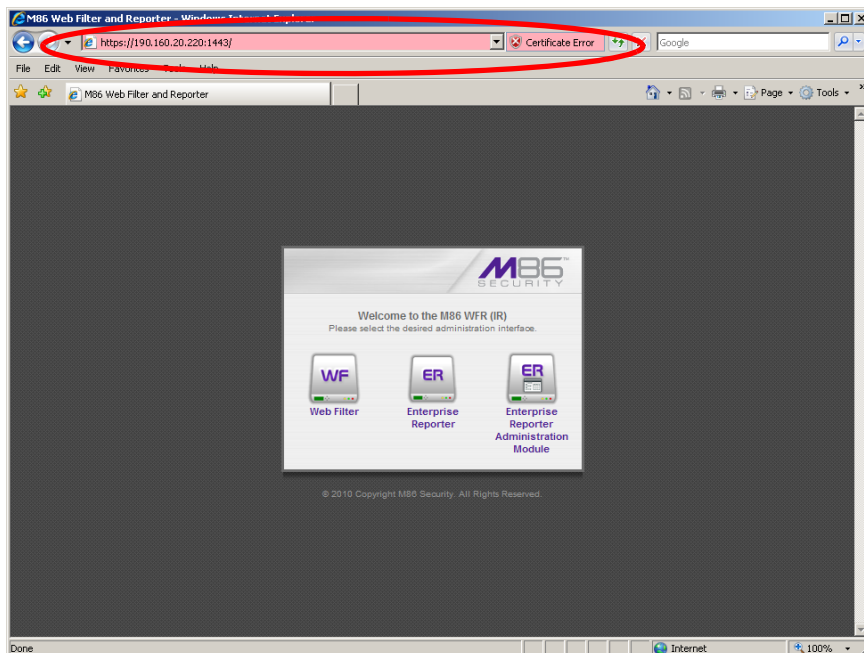
- E. Proceed to Step 2: Log in Web Filter, Generate SSL Certificate.

Temporarily Accept the Security Certificate in IE

- A. 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 IR splash page with the address field and the Certificate Error button to the right of the field shaded a reddish color:



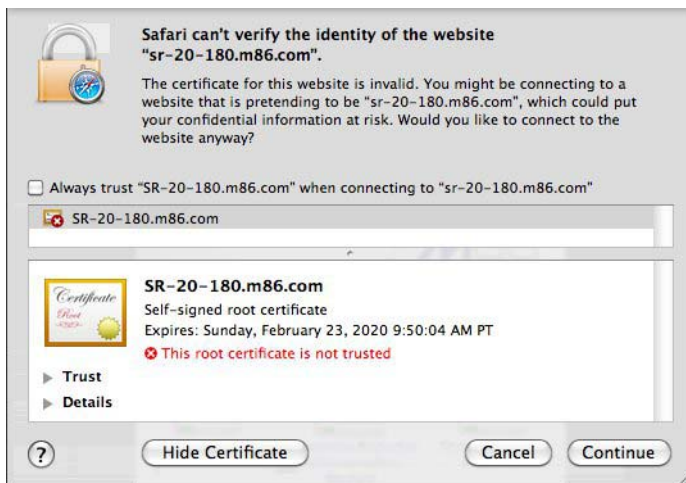
- B. Proceed to Step 2: Log in Web Filter, Generate SSL Certificate.

Accept the Security Certificate in Safari

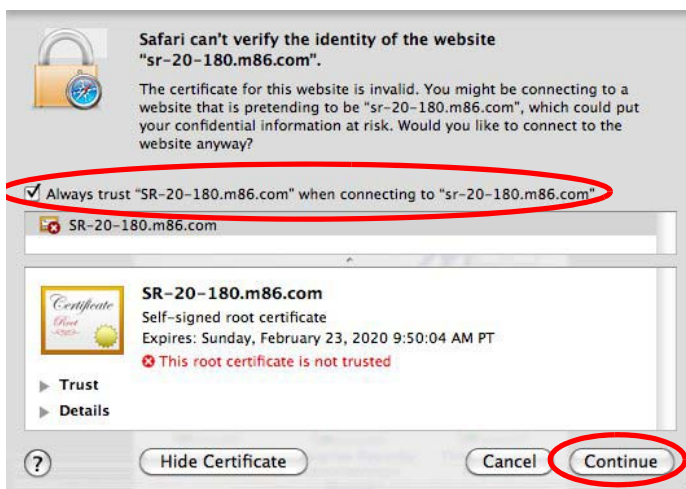
- A. If using a Safari browser, the pop-up window "Safari can't verify the identity of the website..." opens:



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



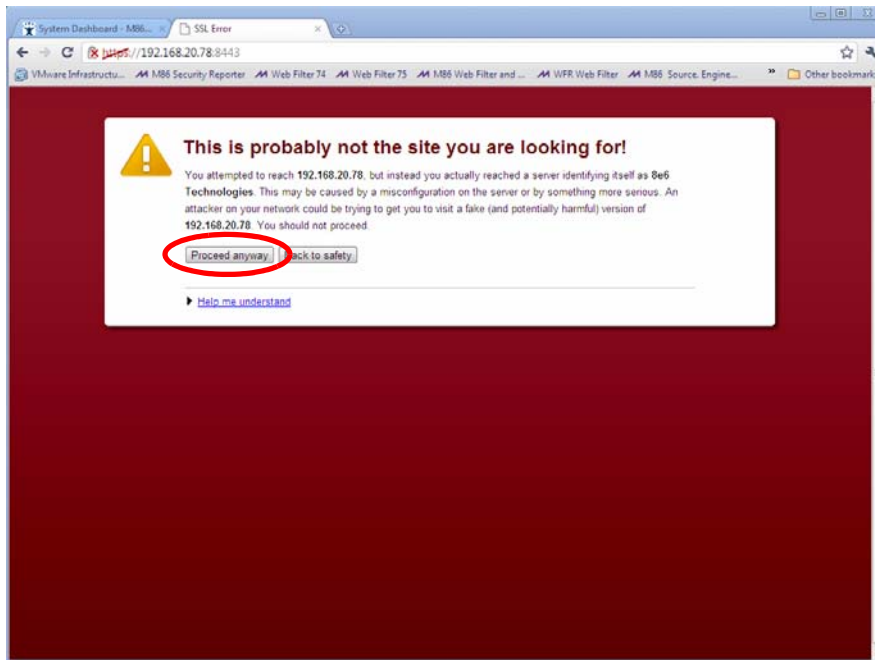
- B. Click the "Always trust..." checkbox and then click **Continue**:



- C. You will be prompted to enter your password in order to install the certificate. After the security certificate is installed, proceed to Step 2: Log in Web Filter, Generate SSL Certificate.


Accept the Security Certificate in Chrome

- A. If using a Chrome browser, in the page “This is probably not the site you are looking for!” click the button **Proceed anyway**:



Clicking this button launches the IR splash page:



 **NOTE:** The Security Certificate must be accepted each time a new browser is launched.

- B. Proceed to Step 2: Log in Web Filter, Generate SSL Certificate.

Step 2: Log in Web Filter, Generate SSL Certificate

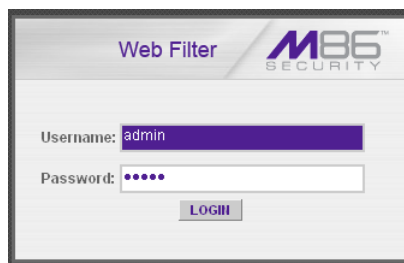
This step requires you to log in to the Web Filter and generate a self-signed certificate for the IR to ensure secure exchanges between the appliance and your browser. If using an IE browser, you will need to complete the security certificate acceptance procedures.


Log in to the Web Filter

A. From the IR splash page, click WF:



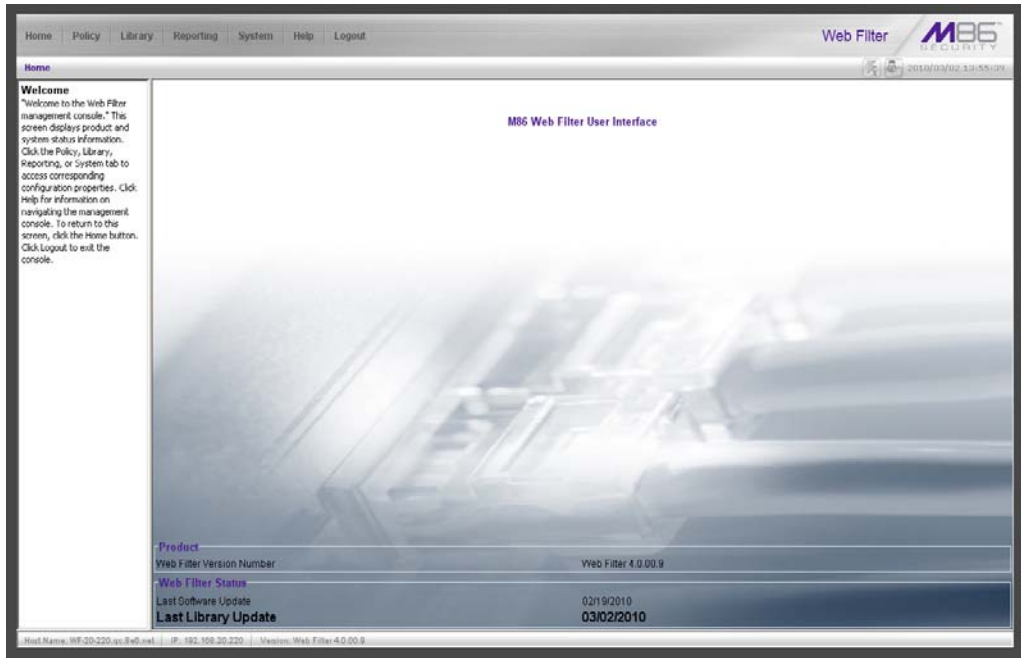
This action opens the Web Filter Administrator console login window:



 **NOTE:** You will need to follow the procedures for accepting the security certificate and/or acknowledging the security warning for the Web Filter.

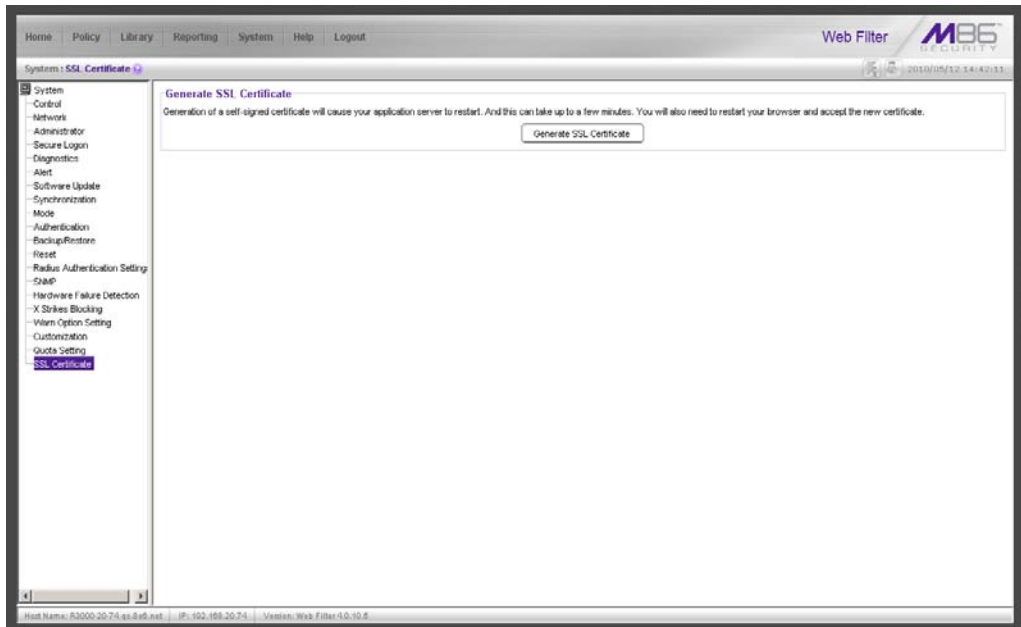
B. Type in the **Username** (*admin*) and **Password** (*user3*):

C. 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 IR.

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

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

If using a Firefox, Safari, or Chrome browser, proceed to Step 3: Test Filtering or the Mobile Client Connection.

IE Security Certificate Installation Procedures

Access the IR splash page

- A. Launch an Internet Explorer 8 browser window.
- B. Type in **https://x.x.x.x:1443** in the address field (in which 'x.x.x.x' represents the LAN 1 IP address assigned to the IR).
- C. Click Go to display the security issue page.

Accept the Security Certificate in IE

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

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

Windows XP or Vista with IE 8

- A. If using an IE 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)**:

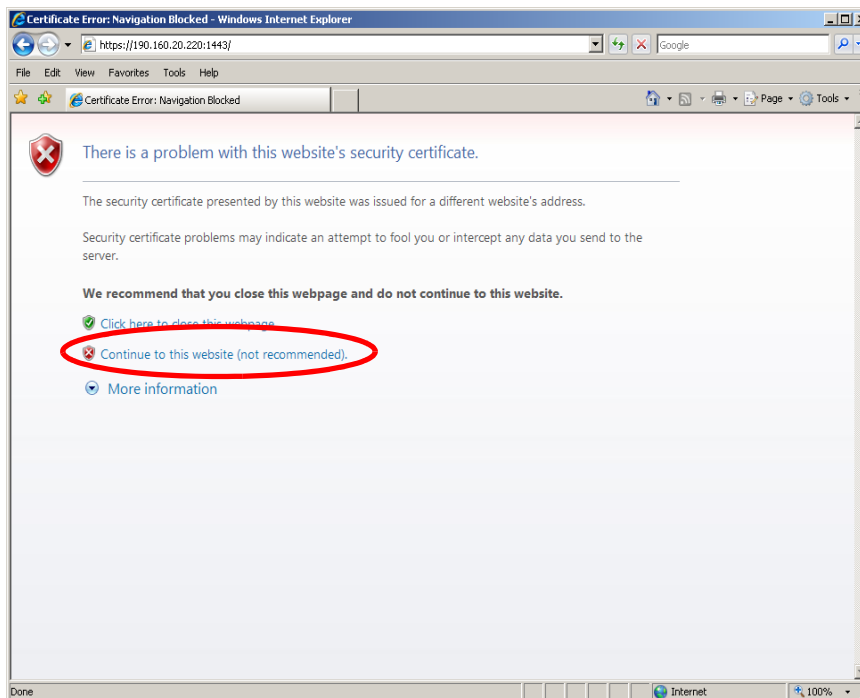


Figure A1: Windows XP, IE 8

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

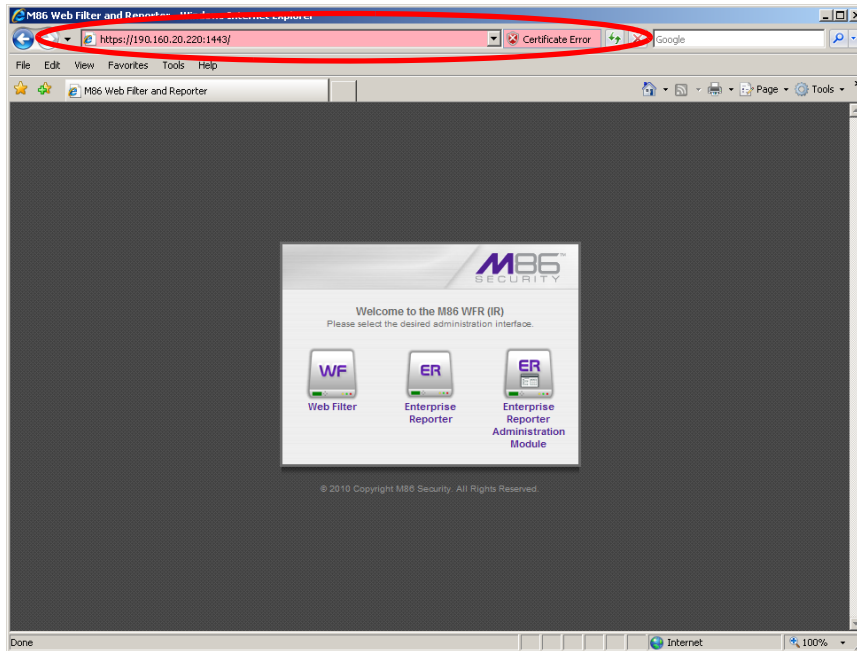


Figure A2: Windows XP, IE 8

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

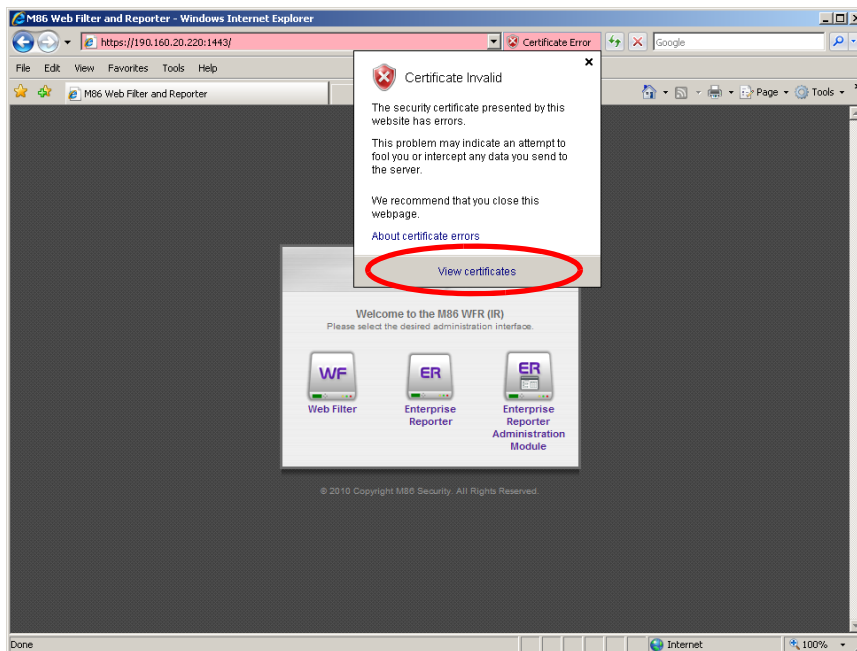


Figure B: Windows XP, IE 8

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

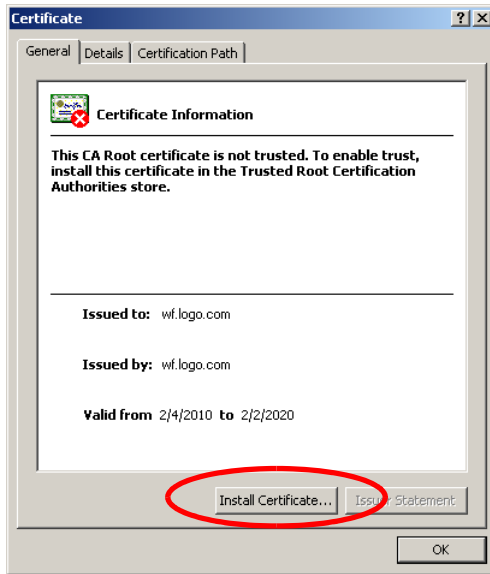


Figure C: Windows XP, IE 8

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

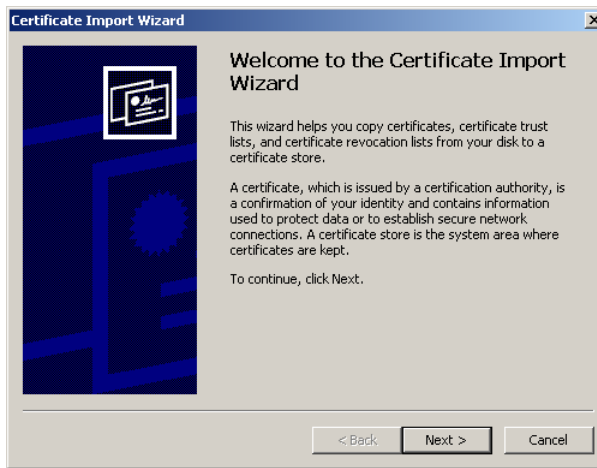


Figure D: Windows XP, IE 8

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

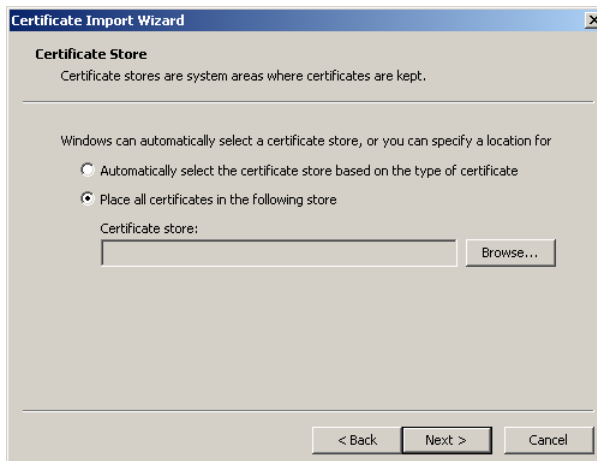


Figure E: Windows XP, IE 8

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

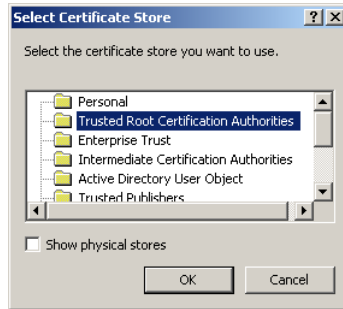


Figure F: Windows XP, IE 8

- 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:

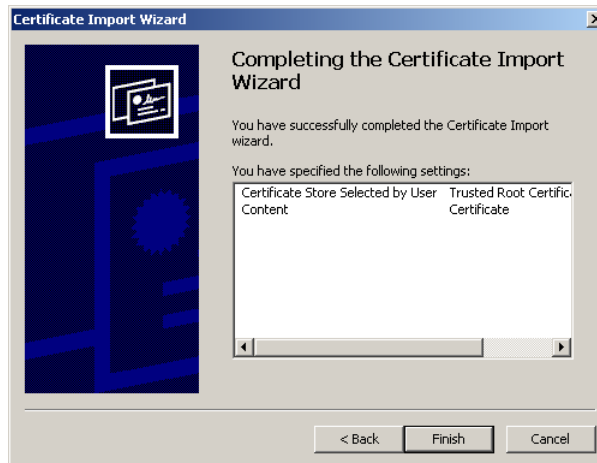


Figure H: Windows XP, IE 8

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

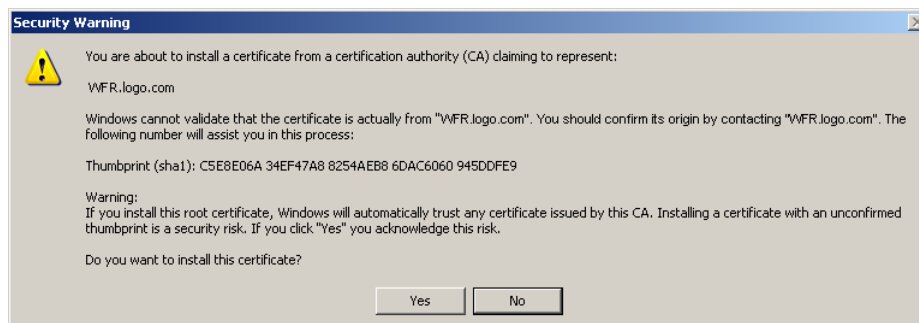


Figure I: Windows XP, IE 8

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

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

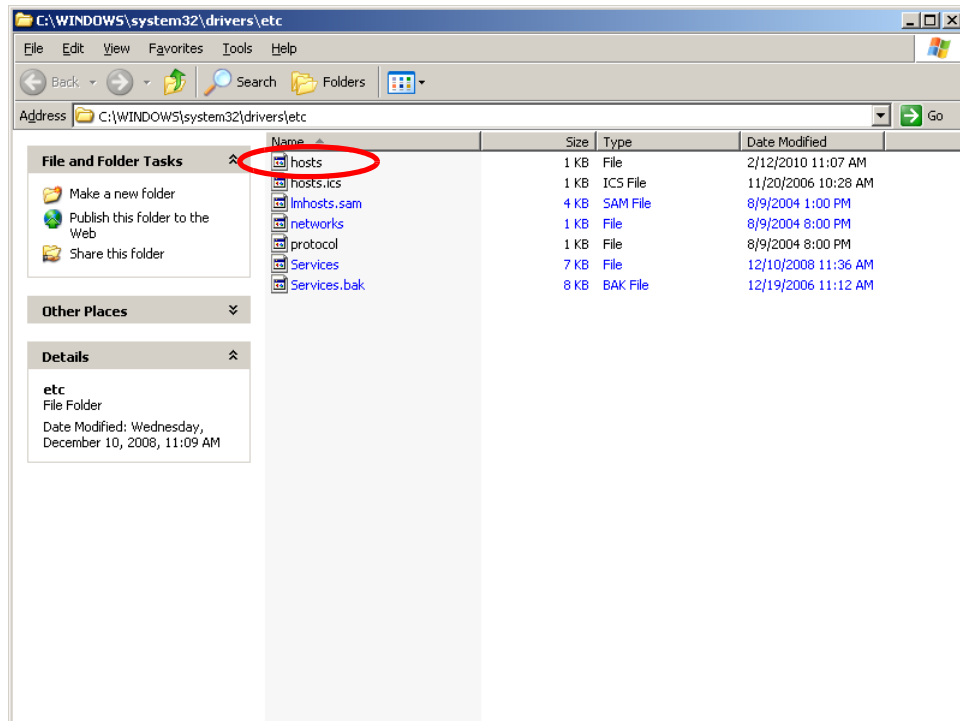
Windows 7 with IE 8

- 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 IR, 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 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 IR splash page 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 IR (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 IR's IP address to its host name. Proceed to Map the IR's IP Address to the Server's Host Name.

Map the IR'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:

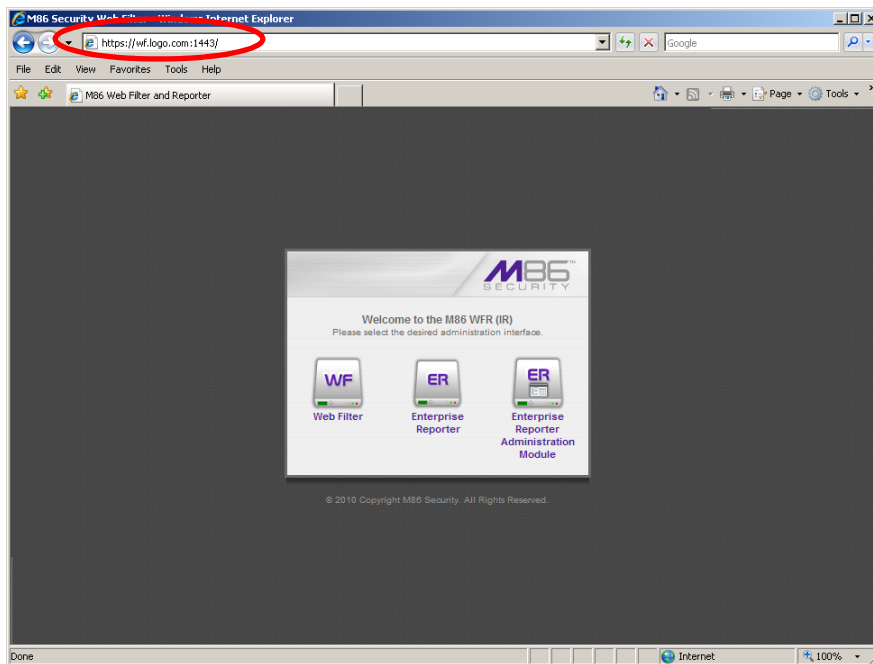


- B. Double-click "hosts" to open a window asking which program you wish to use to open the file. Double-click "Notepad" or "TextPad" to launch the hosts file using that selected program:

```

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 IR'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 Network: LAN Settings steps from the Console Setup Procedures (in the Appendix)—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 IR's host name instead of its IP address—that is **https://host-name:1443** would be used instead of **https://x.x.x.x:1443**. Click **Go** to open the IR splash page:



Proceed to Step 3: Test Filtering or the Mobile Client Connection.

Step 3: Test Filtering or the Mobile Client Connection

Test Filtering

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

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

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

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

Test the Mobile Client Connection

If this IR has been set up in the Mobile mode, you do not need to test filtering. Instead, once you have accessed the Web Filter Administrator console, you should verify that the Mobile 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 4: Set Library Updates

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



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

Activate and Register the Web Filter

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

- A. Open an Internet browser window and go to **<http://www.m86security.com/support/activate-appliance.asp>**.
- B. After reading through the online End User License Agreement, click **Accept** to go to Step 2 of the activation process.
- C. Enter your activation code.
- D. Click **Submit** to go to the Web Filter 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.

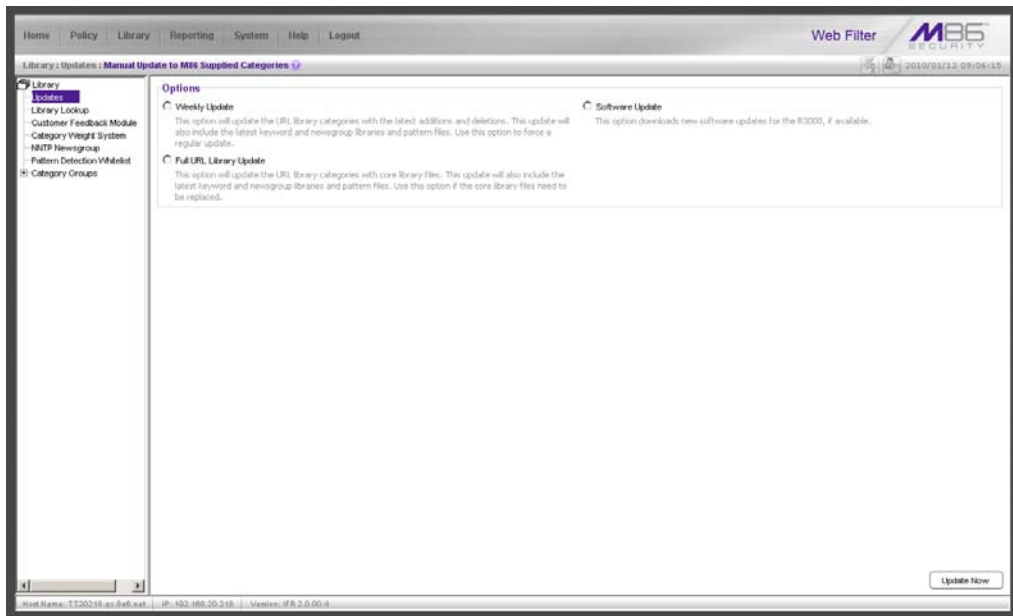
You may wish to print the confirmation page for future reference in dealing with technical issues.

Perform a Complete Library Update

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

To download the latest library updates, go to the Web Filter Administrator console.

- A. Click the **Library** link at the top of the screen.
- B. From the navigation panel, click Updates and select Manual Update from the menu:

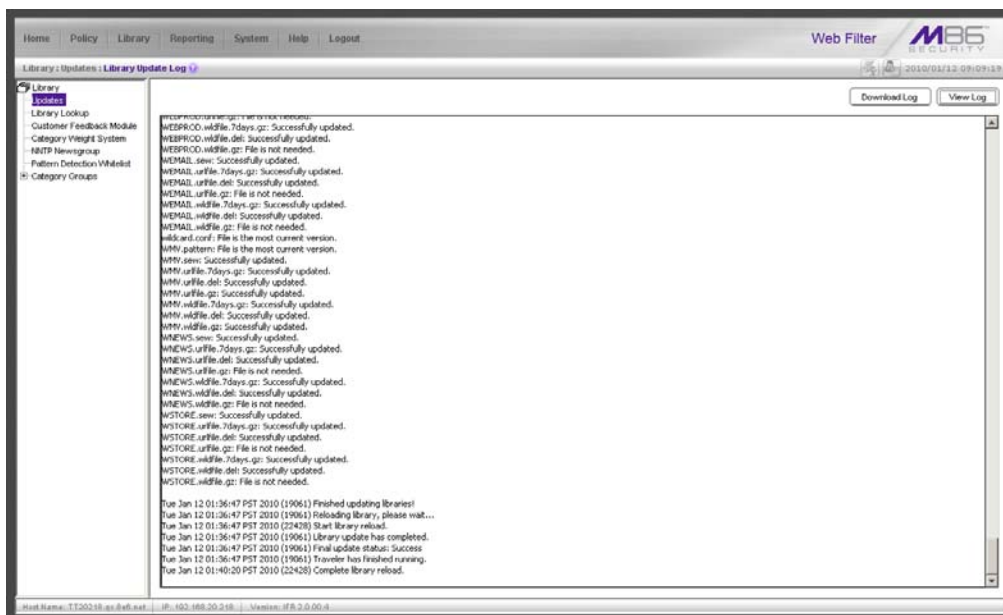



- C. In the Manual Update to M86 Supplied Categories window, click the radio button corresponding to **Full URL Library Update**.
- D. Click **Update Now** to begin the update process.


Monitor the Library Update Process

To verify that the library is being updated:

- A. From the navigation panel, click Updates and select Library Update Log from the menu.
- B. In the Library Update Log window, click **View Log** to display the update activity:



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


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

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 M86 IR 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 M86 IR Web Filter User Guide at <http://www.m86security.com/support/R3000/documentation.asp>

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

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

Step 5: Change the ER Admin User Name and Password, Set Self-Monitoring

After configuring the Web Filter, click the **Quit** button at the top of the screen to exit the Web Filter Administrator console. You will now need to log in to the ER Administrator console and make some changes to settings in screens.


Log in to the ER Administrator Console

- A. From the IR splash page, click the button corresponding to Enterprise Reporter Administration Module:



This action opens the ER Administrator console login window:



 **NOTE:** You will need to follow the procedures for accepting the security certificate for the ER Administrator Console.

- B. In the **Username** field, type in **admin**.
- C. In the **Password** field, type in **reporter**.
- D. Click **Login** to go to the Server Status screen of the Administrator console:

Enterprise Reporter M86 SECURITY

Network Server Database Help Logout

Product Version:
Enterprise Reporter
Version 6.0.10.1
March 11, 2010
Copyright 2010 M86 Security

Server Status

CPU Utilization

CPU Load Averages: 1.38, 1.59, 1.32
 CPU states: 0.9%us, 0.5%sy, 0.0%ni, 96.8%id, 1.8%wa, 0.0%hi, 0.0%si, 0.0%st
 Memory: 4151508k total, 3911804k used, 239704k free, 38204k buffers
 Swap: 2097144k total, 84k used, 2097060k free, 2335500k cached


PID	USER	PR	NI	VRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
3607	dbus	20	0	2712	860	700	S	0	0.0	0:00.00	dbus-daemon
30011	root	20	0	7024	1964	1404	S	0	0.0	0:43.48	dbcontrol

Disk drives status

Filesystem	1k-blocks	Used	Available	Use%	Mounted on
/dev/mapper/VG00-rootlv					
20931580	1730224	26680924	7%	/	
none	2075752	0	2075752	0%	/dev/shm
/dev/mapper/VG00-8e6lv					
79473544	2477232	72959296	4%	/usr/local/8e6	
/dev/mapper/VG00-backuplv					
126951204	7862204	112640280	7%	/backup	
/dev/mapper/VG00-dblv1					
219112724	186212228	32800496	85%	/database/d1	

NETSTAT

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program Name
tcp	0	0	eriii-md.qq.8e6.net:mysql	192.168.30.92:ums	ESTABLISHED	3667/mysql
tcp	0	0	ERSL-121.8e6.com:mysql	ERSL-121.8e6.com:40985	ESTABLISHED	3667/mysql
tcp	0	0	eriii-md.qq.8e6.net:mysql	192.168.30.92:nstsp	ESTABLISHED	3667/mysql

 **NOTE:** If using the ER in the Evaluation Mode, the ER Status pop-up window opens when accessing the Server Status screen. See the M86 IR Enterprise Reporter Administrator User Guide for information about the Evaluation Mode.

Change User Name and Password

- A. Set up a new administrator user name and password by clicking on the Network pull-down menu and choosing **Administrators** to display the Add/Edit/Delete Administrators screen:

Add/Edit/Delete Administrators

New Administrator

User Name: admin

Password: [masked]

Confirm Password: [empty]

Save Delete

- B. Select **New Administrators** from the pull-down menu.
- C. Enter a **User Name** and **Password**.

- D. In the **Confirm Password** field, re-enter the password.
- E. Click **Save**.

Set Self-Monitoring

- A. From the Server pull-down menu, choose **Self-Monitoring** to display the Self Monitoring screen:

The screenshot shows the 'Security Reporter' interface with the 'Self Monitoring' dialog box open. The dialog box contains the following elements:

- Header: **Self Monitoring**
- Question: **Would you like to activate self-monitoring?** with radio buttons for **YES** (selected) and **NO**.
- Text: **If yes, indicate who will receive the emergency e-mail notification. You may assign up to four individuals. One of them has to match with the Master Administrator email. The Master Administrator receives all messages.**
- Field: **Master Administrator's E-Mail Address:**
- Options:
 - Choice one** Send e-mail to e-mail address:
 - Choice two** Send e-mail to e-mail address:
 - Choice three** Send e-mail to e-mail address:
 - Choice four** Send e-mail to e-mail address:
- Button: **Save**

- B. Choose **YES** to activate monitoring.
- C. Enter the **Master Administrator's E-Mail Address**.
- D. Click **Choice one** and enter an e-mail address of an individual in your organization that you would like notified if the ER detects any problems when processing data. This can be the same e-mail address entered in the previous field. Enter up to four e-mail addresses.
- E. Click **Save**.

Now that the ER server settings have been made, you need to configure a client workstation for reporting.


Step 6: Launch the ER Client

A. From the IR splash page, click the button corresponding to Enterprise Reporter:




This action opens the ER Web Client login window:

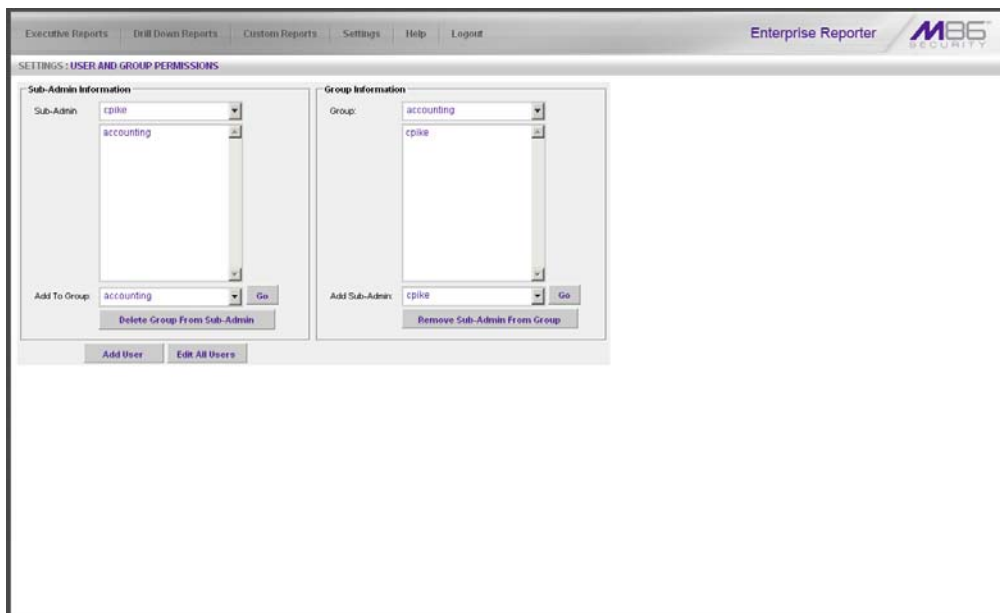


 **NOTE:** You will need to follow the procedures for accepting the security certificate for the ER Web Client.

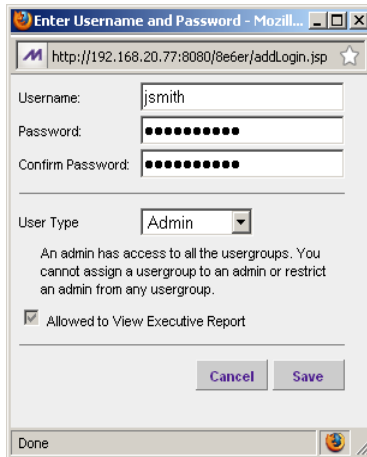
B. Enter your **Username** and **Password**, and then click **Login** to access the main screen of the client.

 **NOTE:** If you do not have your own Username and Password set up in the ER client, the default Username is **manager** and the default Password is **8e6Report**.

C. In the navigation panel, select **Settings**, and then choose **User Permissions** from the menu:



D. Click **Add User** to open the Enter User Permissions dialog box:



Enter Username and Password - Mozill...
http://192.168.20.77:8080/8e6er/addlogin.jsp

Username: jsmith
Password: ●●●●●●●●
Confirm Password: ●●●●●●●●

User Type: Admin

An admin has access to all the usergroups. You cannot assign a usergroup to an admin or restrict an admin from any usergroup.

Allowed to View Executive Report

Cancel Save

Done


E. Enter the **Username**.

F. Enter the **Password**, and **Confirm Password**.

G. Select the **User Type** (“Admin” or “Sub-Admin”).

H. Click **Save** to close the dialog box, and to add the username to the user list.

I. Exit the client. You can now launch the client and enter the password you just set up.

 **NOTE:** For instructions on logging into the client after initial set up, refer to the *ER Web Client User Guide*.

CONCLUSION

Congratulations; you have completed the IR installation procedures. Now that the Web Filter and ER server are set up on your network, once the ER database is populated with logs from the Web Filter, the client can be used for generating reports.

Initially, you will only be able to report on IP addresses. To implement user names in ER reporting, please consult the M86 IR Enterprise Reporter Administrator User Guide.

Refer to the ER Web Client User Guide for information on generating reports.



NOTE: *If you cannot view reports, or if your specific environment is not covered in the ER Administrator User Guide, contact an M86 Security solutions engineer or technical support representative. Port 22 (SSH) and Port 3306 (SQL) must be open on your network to allow access by remote technical support.*



IMPORTANT: *M86 Security recommends proceeding to the Best 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 IR 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	
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 Patterns	Recreation	
	My Space IM		Government/Law/Politics	Self Defense	
	PaPo		Government	Social Opinion	
	QQ		Legal	Tobacco	
	ToToMoMo		Military Appreciation	Travel/Events	
	WangWang		Military Official	Tickets	
	Windows Live Messenger		Political Opinion	Travel	
	Yahoo IM		Health/Fitness	Vehicles	
			Fitness		
			Health/Medical		
			Holistic		
			Self Help		

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.

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

I. Threats/Liabilities

A. Category block

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

To block categories in a profile, go to:

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



In the IR Web Filter User Guide index, see:

- *How to: use library categories in a profile*

B. Rule block

Use a rule to block categories that threaten your network/organization.

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

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

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



In the IR Web Filter User Guide index, see:

- *How to: use rules*
- *How to: use library categories in a profile*

C. X-Strike on blocked categories

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

To block categories in a profile using the X Strikes Blocking feature, go to:

- SYSTEM: System > X Strikes Blocking > Configuration tab, and Categories tab
- POLICY: Policy > IP > member > member Profile > Filter Options tab, X Strikes Blocking enabled
or POLICY: Policy > Global Group > Global Group Profile > Filter Options tab (X Strikes Blocking enabled)



In the IR Web Filter User Guide index, see:

- *How to: set up X Strikes Blocking*
- *How to: set up profile options*

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

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

To customize pages, go to:

- SYSTEM: System > Customization > Common Customization window, and other applicable customization windows



In the IR Web Filter User Guide index, see:

- *How to: customize pages*

E. URL Keywords

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

To set up URL keywords to be blocked, go to:

- LIBRARY: Library > Category Groups > category > URL Keywords
- POLICY: Policy > IP > member > member Profile > Filter Options tab (URL Keyword Filter Control enabled)
or POLICY: Policy > Global Group > Global Group Profile > Filter Options tab (URL Keyword Filter Control enabled)



In the IR Web Filter User Guide index, see:

- *How to: set up URL Keywords*
- *How to: set up profile options*

F. Search Engine Keywords

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

To set up Search Engine Keywords to be blocked, go to:

- LIBRARY: Library > Category Groups > category > Search Engine Keywords
- POLICY: Policy > IP > member > member Profile > Filter Options tab (Search Engine Keyword Filter Control enabled)
or POLICY: Policy > Global Group > Global Group Profile > Filter Options tab (Search Engine Keyword Filter Control enabled)



In the IR Web Filter User Guide index, see:

- *How to: set up Search Engine Keywords*
- *How to: set up profile options*

G. Custom Category (blocked)

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

To set up a custom category and block it, go to:

- LIBRARY: Library > Category Groups > Custom Categories > Add Category
- POLICY: Policy > IP > member > member Profile > Category tab
or POLICY: Policy > Global Group > Global Group Profile > Category tab



In the IR Web Filter User Guide index, see:

- *How to: set up a custom category*
- *How to: use library categories in a profile*

H. Minimum Filtering Level

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

To configure the minimum filtering level, go to:

- POLICY: Policy > Global Group > Minimum Filtering Level
- Policy > Global Group > Global Group Profile > Category tab



In the IR Web Filter User Guide index, see:

- *How to: configure the Minimum Filtering Level*
- *How to: use library categories in a profile: Global Group Profile*

I. Override Account bypass

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

To set up an override account at the Global Group level, go to:

- POLICY: Policy > Global Group > Override Account window

To configure the bypass feature and set up a group level override account, go to:

- POLICY: Policy > Global Group > Minimum Filtering Level > Min. Filter Bypass
- Policy > IP > group > Override Account window



In the IR Web Filter User Guide index, see:

- *How to: set up an Override Account: Global Group*
- or:
- *How to: configure the Minimum Filtering Level: Bypass Options*
- *How to: set up an Override Account: Group profile*

J. Exception URL bypass

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

To set up the Exception URL bypass for users to bypass blocked URLs, go to:

- POLICY: Policy > Global Group > Minimum Filtering Level > Min. Filter Bypass
- Policy > IP > member > Exception URL window



In the IR Web Filter User Guide index, see:

- *How to: configure the Minimum Filtering Level: Bypass Options*
- *How to: set up Exception URLs*

K. Proxy Patterns

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

To set up the proxy pattern blocking feature and apply it to profiles, go to:

- SYSTEM: System > Control > Filter window
- POLICY: Policy > IP > member > member Profile > Category tab
or POLICY: Policy > Global Group > Global Group Profile > Category tab



In the IR Web Filter User Guide index, see:

- *How to: configure filtering*
- *How to: use library categories in a profile*

L. File type blocking

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

To set up file type blocking and apply this feature to profiles, go to:

- LIBRARY: Library > Category Groups > Custom Categories > Add Category
- Library > Custom Categories > category > URL Keywords
- POLICY: Policy > IP > member > member Profile > Category tab, and Filter Options tab (URL Keyword Filter Control and extension options enabled)
or POLICY: Policy > Global Group > Global Group Profile > Category tab, and Filter Options tab (URL Keyword Filter Control and extension options enabled)



In the IR Web Filter User Guide index, see:

- *How to: set up a custom category*
- *How to: set up URL Keywords: Custom Categories*
- *How to: use library categories in a profile*
- *How to: set up profile options*

II. Bandwidth/Productivity

A. Time Quota/Hit Quota

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

To set up the quota feature and configure profiles to use this feature, go to:

- SYSTEM: System > Quota Setting window
- POLICY: Policy > IP > member profile > Category tab (Quota column)
or Policy > Global Group > Global Group Profile > Category tab (Quota column)



In the IR Web Filter User Guide index, see:

- *How to: set up Quotas*
- *How to: use library categories in a profile*

B. Overall Quota

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

To set up the quota option and configure profiles to use the Overall Quota, go to:

- SYSTEM: System > Quota Setting window
- POLICY: Policy > IP > member profile > Category tab (Overall Quota)
or Policy > Global Group > Global Group Profile > Category tab (Overall Quota)



In the IR Web Filter User Guide index, see:

- *How to: set up Quotas*
- *How to: use library categories in a profile*

C. Time Based Profiles

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

To set up Time Profiles, go to:

- POLICY: Policy > IP > member > Time Profile window



In the IR Web Filter User Guide index, see:

- *How to: set up a Time Profile*

D. Warn option with low filter settings

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

To set up and use the warn option, go to:

- SYSTEM: System > Control > Filter window
- System > Warn Option Setting window
- POLICY: Policy > IP > member > member profile > Category tab (Warn column) or POLICY: Policy > Global Group > Global Group Profile > Category tab (Warn column)



In the IR Web Filter User Guide index, see:

- *How to: configure filtering*
- *How to: configure the Warn Option Setting*
- *How to: use library categories in a profile*

E. Warn-strike

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

To set up and use the warn option with X Strikes Blocking, go to:

- SYSTEM: System > X Strikes Blocking window
- System > Warn Option Setting window
- POLICY: Policy > IP > member > member profile > Category Profile tab (Warn column), and Filter Options tab (X Strikes Blocking enabled) or POLICY: Policy > Global Group > Global Group Profile > Category tab (Warn column), and Filter Options tab (X Strikes Blocking enabled)



In the IR Web Filter User Guide index, see:

- *How to: set up X Strikes Blocking*
- *How to: configure the Warn Option Setting*
- *How to: use library categories in a profile*
- *How to: set up profile options*

F. P2P patterns

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

To block P2P services, go to:

- SYSTEM: System > Control > Filter window
- POLICY: Policy > IP > member > member profile > Category tab or POLICY: Policy > Global Group > Global Group Profile > Category tab



In the IR Web Filter User Guide index, see:

- *How to: configure filtering*
- *How to: use library categories in a profile*

G. IM patterns

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

To block IM services, go to:

- SYSTEM: System > Control > Filter window
- POLICY: Policy > IP > member > member profile > Category tab
or POLICY: Policy > Global Group > Global Group Profile > Category tab



In the IR Web Filter User Guide index, see:

- *How to: configure filtering*
- *How to: use library categories in a profile*

H. Game patterns

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

To block game patterns, go to:

- SYSTEM: System > Control > Filter window
- POLICY: Policy > IP > member > member profile > Category tab
or POLICY: Policy > Global Group > Global Group Profile > Category tab



In the IR Web Filter User Guide index, see:

- *How to: configure filtering*
- *How to: use library categories in a profile*

I. Streaming Media patterns

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

To block streaming media patterns, go to:

- SYSTEM: System > Control > Filter window
- POLICY: Policy > IP > member > member profile > Category tab
or POLICY: Policy > Global Group > Global Group Profile > Category tab



In the IR Web Filter User Guide index, see:

- *How to: configure filtering*
- *How to: use library categories in a profile*

J. Remote Access patterns

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

To block remote access patterns, go to:

- SYSTEM: System > Control > Filter window
- POLICY: Policy > IP > member > member profile > Category tab
or POLICY: Policy > Global Group > Global Group Profile > Category tab



In the IR Web Filter User Guide index, see:

- *How to: configure filtering*
- *How to: use library categories in a profile*

K. HTTPS settings

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

To configure HTTPS settings, go to:

- SYSTEM: System > Control > Filter window



In the IR Web Filter User Guide index, see:

- *How to: configure filtering*

L. Category block

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

To block the Bandwidth category, go to:

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



In the IR Web Filter User Guide index, see:

- *How to: use library categories in a profile*

M. Rule block

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

To create and block a rule for the Bandwidth category, go to:

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



In the IR Web Filter User Guide index, see:

- *How to: use rules*
- *How to: use library categories in a profile*

N. SE Keywords

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

To set up search engine keywords and block them in a profile, go to:

- LIBRARY: Library > Category Groups > category group > category > Search Engine Keywords
- POLICY: Policy > IP > member > member Profile > Filter Options tab (Search Engine Keyword Filter Control enabled)
or POLICY: Policy > Global Group > Global Group Profile > Filter Options tab (Search Engine Keyword Filter Control enabled)



In the IR Web Filter User Guide index, see:

- *How to: set up Search Engine Keywords*
- *How to: set up profile options*

O. URL Keywords

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

To set up and block URL keywords in a profile, go to:

- LIBRARY: Library > Category Groups > category group > category > URL Keywords
- POLICY: Policy > IP > member > member Profile > Filter Options tab (URL Keyword Filter Control enabled)
or POLICY: Policy > Global Group > Global Group Profile > Filter Options tab (URL Keyword Filter Control enabled)



In the IR Web Filter User Guide index, see:

- *How to: set up URL Keywords*
- *How to: set up profile options*

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

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

To customize pages, go to:

- SYSTEM: System > Customization > Common Customization window, and other applicable customization windows



In the IR Web Filter User Guide index, see:

- *How to: customize pages*

Q. Real Time Probe information

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

To enable and use Real Time Probe reporting, go to:

- REPORTING: Report > Real Time Probe > Configuration tab
- Real Time Probe > Go to Real Time Probe Reports GUI link > Real Time Probe Reports > Create tab



In the IR Web Filter User Guide index, see:

- *How to: set up Real Time Probes*

III. General/Productivity

A. Warn Feature with higher thresholds

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

To set up and use the warn option with high filter settings, go to:

- SYSTEM: System > Control > Filter window
- System > Warn Option Setting window
- POLICY: Policy > IP > member profile > Category tab (Warn column) or POLICY: Policy > Global Group > Global Group Profile > Category tab (Warn column)



In the IR Web Filter User Guide index, see:

- *How to: configure filtering*
- *How to: configure the Warn Option Setting*
- *How to: use library categories in a profile*

B. Warn-strike with higher thresholds

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

To set up and use the warn option, go to:

- SYSTEM: System > Control > Filter window
- System > X Strikes Blocking window
- System > Warn Option Setting window
- POLICY: Policy > IP > member > member profile > Category tab (Warn column), and Filter Options tab (X Strikes Blocking enabled)
or POLICY: Policy > Global Group > Global Group Profile > Category tab (Warn column), and Filter Options tab (X Strikes Blocking enabled)



In the IR Web Filter User Guide index, see:

- *How to: configure filtering*
- *How to: set up X Strikes Blocking*
- *How to: configure the Warn Option Setting*
- *How to: use library categories in a profile*
- *How to: set up profile options*

C. Time Quota/Hit Quota

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

To set up the Quota feature and use quotas in profiles, go to:

- SYSTEM: System > Quota Setting window
- POLICY: Policy > IP > member > profile > Category tab (Quota column)
or POLICY: Policy > Global Group > Global Group Profile > Category tab (Quota column)



In the IR Web Filter User Guide index, see:

- *How to: set up Quotas*
- *How to: use library categories in a profile*

D. Time Based Profiles

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

To set up and use time profiles, go to:

- POLICY: Policy > IP > member > Time Profile window



In the IR Web Filter User Guide index, see:

- *How to: set up a Time Profile*

E. Overall Quota

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

To set up the quota option and configure profiles to use the Overall Quota, go to:

- SYSTEM: System > Quota Setting window
- POLICY: Policy > IP > member profile > Category tab (Overall Quota)
or Policy > Global Group > Global Group Profile > Category tab (Overall Quota)



In the IR Web Filter User Guide index, see:

- *How to: set up Quotas*
- *How to: use library categories in a profile*

F. Customize an M86 Supplied Category

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

To customize and use an M86 Supplied Category in a profile, go to:

- LIBRARY: Library > Category Groups > category group > category (add/delete URLs, URL Keywords, Search Engine Keywords)
- POLICY: Policy > IP > member > member profile > Category tab
or POLICY: Policy > Global Group > Global Group Profile > Category tab



In the IR Web Filter User Guide index, see:

- *How to: set up URLs in categories: M86 Supplied Categories*
- *How to: use library categories in a profile*

G. Local category adds/deletes

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

To create a Custom Category and use it in a profile, go to:

- LIBRARY: Library > Category Groups > Custom Categories > Add Category (add URLs, URL Keywords, Search Engine Keywords)
- POLICY: Policy > IP > member > member profile > Category tab
or POLICY: Policy > Global Group > Global Group Profile > Category tab



In the IR Web Filter User Guide index, see:

- *How to: set up a custom category*
- *How to: use library categories in a profile*

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

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

To customize pages, go to:

- SYSTEM: System > Customization > Common Customization window, and other applicable customization windows



In the IR Web Filter User Guide index, see:

- *How to: customize pages*

IV. Pass/Allow

A. Always Allow Custom Category

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

To create a white list custom category and use it in a profile, go to:

- LIBRARY: Library > Category Groups > Custom Categories > Add Category (add URLs, URL Keywords, Search Engine Keywords)
- POLICY: Policy > IP > member > member profile > Category tab or POLICY: Policy > Global Group > Global Group Profile > Category tab



In the IR Web Filter User Guide index, see:

- *How to: set up a custom category*
- *How to: use library categories in a profile*

B. URL exceptions

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

To set up the Exception URL bypass for users to bypass blocked URLs, go to:

- POLICY: Policy > Global Group > Minimum Filtering Level > Min. Filter Bypass
- Policy > IP > member > Exception URL window



In the IR Web Filter User Guide index, see:

- *How to: configure the Minimum Filtering Level: Bypass Options*
- *How to: set up Exception URLs*

C. IP exceptions

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

To set up the Exception URL bypass for bypassing blocked IP addresses, go to:

- POLICY: Policy > Global Group > Minimum Filtering Level > Min. Filter Bypass
- Policy > IP > member > Exception URL window



In the IR Web Filter User Guide index, see:

- *How to: configure the Minimum Filtering Level: Bypass Options*
- *How to: set up Exception URLs*

D. Override Accounts

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

To set up an override account at the Global Group level, go to:

- POLICY: Policy > Global Group > Override Account window

To configure the bypass feature and set up a group level override account, go to:

- POLICY: Policy > Global Group > Minimum Filtering Level > Min. Filter Bypass
- Policy > IP > group > Override Account window



In the IR Web Filter User Guide index, see:

- *How to: set up an Override Account: Global Group*
- or:*
- *How to: configure the Minimum Filtering Level: Bypass Options*
- *How to: set up an Override Account: Group profile*

E. Pattern detection bypass

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

To set up pattern detection whitelisting, go to:

- SYSTEM: System > Control > Filter window
- LIBRARY: Library > Pattern Detection Whitelist



In the IR Web Filter User Guide index, see:

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

BEST REPORTING PRACTICES

Now that the ER is installed on the network and you have successfully logged into the client, you are ready to generate reports. This section provides an overview on using tools to produce reports that identify potential violators of your acceptable Internet usage policy, so you can take effective action.

You will learn how to:

- access Executive Reports to obtain a high level snapshot of end user Internet activity
- use Drill Down Reports to conduct an investigation of specific Internet activity
- modify a report view
- create a double-break report to combine two sets of criteria into one report
- generate a summary report view and a detail report view
- create a new report view
- export a report view to an output format
- save a report
- schedule a report to run on a regular basis to capture Internet activity at set intervals of time
- create a custom category group
- generate a summary report and a detail report for a custom category group
- create a custom user group
- generate a summary report and a detail report for a single user group

Please review the Reporting Scenarios sub-section for instructions and tips on using the client to fulfill the scenarios described above.



NOTE: *The ER must collect data for a full day in order to generate Executive Reports. To use Drill Down Reports, the ER must collect data for a couple of hours. Therefore, it would be best to wait a day after the ER has been installed and fully operational before beginning any of the exercises described in the Enterprise Reporter Usage Scenarios sub-section.*

Reporting Scenarios

This collection of reporting scenarios is designed to help you use the client to create typical snapshots of end user Internet activity. Each scenario is followed by client setup information. Please consult the “How to” section in the index of the ER Web Client User Guide for pages containing detailed, step-by-step instructions on configuring and/or using the tools and features described in that scenario.

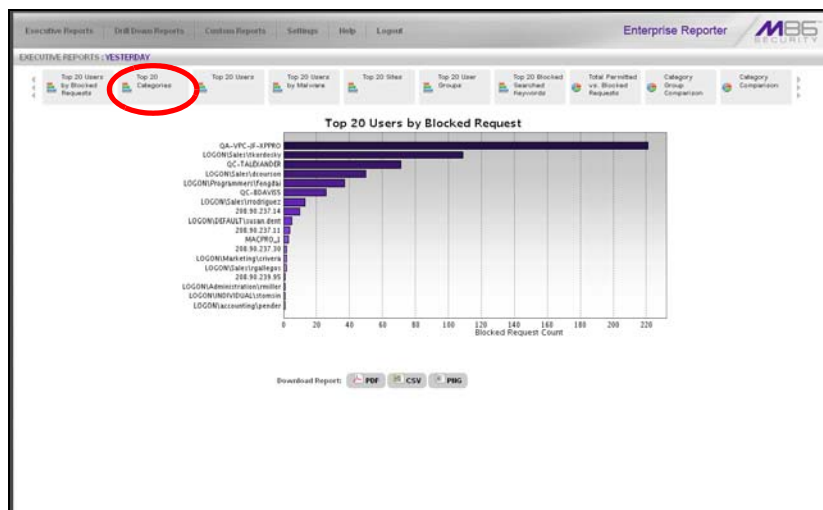
I. Executive Report and Drill Down Report exercise

In this exercise you will learn how to use Executive Reports to obtain a high level overview of end user activity, and then use Drill Down Reports to obtain more detailed information on specific user activity. You will also learn that there are two basic types of Drill Down Reports (summary and detail reports), and various types of reports you can generate for each of these two basic drill down report types.

Step A: Start with the dashboard for a high level activity overview

By default, the panel in the middle of the screen displays yesterday’s Executive Report containing pre-generated data. Since the data has already been captured from the previous day, the report loads quickly in your browser.

In the dashboard that displays near the top of the panel, click the thumbnail that corresponds to the type of Executive Report you wish to view. For this example, click “Top 20 Categories”:



This report shows the top 20 categories that were most frequently visited by users yesterday.

Review the list of categories in this canned report. In a later step you will need to select the category to be further investigated.



NOTE: Click the left or right arrow in the dashboard to view additional thumbnails.



In the ER Web Client User Guide index, see:

- How to: generate an Executive Report

Step B: Further investigate using a Summary Drill Down Report

Now you will use a Drill Down Report to find out which user(s) are visiting sites in the category you've targeted for investigation.

From the top panel, go to **Drill Down Reports > Categories** to display the generated Summary Drill Down Report view, ranking categories in order by the most visited:

Categories	Category Obj	Category Items	Category Sites	Category Count	IP Count	User Count	Site Count	Page Count	Object Count	Time
JMS/TMS				04	591	200	4,707	950		0:20:50
Search Engine					200	1,784	18	3,200	2,387	4:40
Banner/Web Ads					88	658	04	707	2,062	1:26:30
Information Technology					72	562	26	797	1,700	1:7:30
Web Based Email					48	404	12	874	656	1:24:00
Chat					33	206	7	832	24	1:18:10
Shipping					17	150	15	207	353	0:32:40
General Business					57	547	25	280	4,429	0:30:30
Internet Radio					11	107	8	160	281	0:13:00
Entertainment					17	153	14	153	626	0:15:30
Travel					11	110	11	137	1,200	0:11:30
News					20	283	24	139	1,641	8:14:0
R Rated					3	36	2	114	0	0:12:00
Pornography/Adult Content					7	81	10	102	654	0:13:40
Video					3	31	3	82	300	0:4:30
Online Gaming Cards					3	22	2	81	1,656	0:6:30
Gambling					1	13	1	36	12	0:9:00
Online Auction					8	88	8	70	870	0:11:40
Games					7	57	5	70	80	0:7:20
Financial Institution					10	121	9	64	424	0:8:50
Dating/Personals					12	118	5	80	736	0:8:20
Message Boards					3	29	2	51	97	0:3:10
Recreation					6	37	6	46	311	0:5:00
Web Log/Personal Pages					5	47	3	42	89	0:4:50
Spells					4	41	4	20	36	0:4:00
Government					6	35	6	27	610	0:2:0

Note that this drill down report view has been generated for today's activity by default. To continue this investigation using data from yesterday's Executive Report, you must create a "New Report" from this current report view and change the date scope.



In the ER Web Client User Guide index, see:

- How to: generate a Drill Down Report

Step C: Create a New Report using yesterday's date scope

1. At the top of the Summary Drill Down Report view, click the **New Report** button to open the Drill Down Report pop-up window:

2. By default, "Today" displays in the **Date Scope** field. Choose "Yesterday" from this menu.

- Click **Apply** to accept your selection and to close the pop-up window. The regenerated report now displays yesterday's data in the Summary Drill Down Report view.



In the ER Web Client User Guide index, see:
 • How to: create a New Report from the current report view

Step D: Create a double-break report with two sets of criteria

- To continue this exercise, select the record for the category you wish to further investigate.



NOTE: If necessary, scroll down to view the entire list of categories in the report view.

- Now, to find out who is visiting sites in this category, you will need to identify the user(s).

Since there are two sets of criteria you need for this exercise, you must drill down into the selected category and also specify that you wish to view user IP addresses. By specifying two sets of criteria, you create a double-break report view.

Note the columns of filter buttons to the right of the Categories column. Click the **Category/IPs** button corresponding to the targeted category:

IP	Category	Site	Category Users	Category Sites	Category Count	IP Count	User Count	Site Count	Page Count	Object Count	Time
10.10.0.5							11	140	3,407	0	5:47:28
10.10.0.0							11	103	1,706	0	3:40:20
10.10.0.7							11	1	200	0	0:8:30
10.10.2.21							9	2	81	9	0:1:30
10.10.0.53							11	0	36	0	0:0:0
10.10.1.56							11	1	25	0	0:1:50
10.10.1.15							5	1	10	0	0:0:50
10.10.1.205							0	1	0	0	0:1:30
10.10.1.217							9	1	9	0	0:1:30
10.10.3.16							4	1	0	0	0:0:40
10.10.0.12							11	1	0	0	0:0:0
10.10.0.126							11	1	0	0	11:0:0
10.10.0.136							11	1	0	0	11:0:0
10.10.0.142							11	1	0	0	25:0:0
10.10.0.160							11	1	0	0	25:0:0
10.10.0.162							11	1	0	0	24:0:0
10.10.0.164							11	1	0	0	24:0:0
10.10.0.202							11	1	0	0	11:0:0
10.10.0.22							11	1	0	0	21:0:0
10.10.0.229							11	1	0	0	24:0:0
10.10.0.23							5	1	0	0	6:0:0
10.10.0.238							9	1	0	0	11:0:0
10.10.0.29							9	1	0	0	30:0:0
10.10.0.38							0	1	0	0	11:0:0
10.10.0.47							11	1	0	0	26:0:0

After executing the last command, note that user IP addresses now display in the first column of the report view instead of categories.



In the ER Web Client User Guide index, see:
 • How to: use filter columns and buttons

For the last step of this exercise, you will select a user from the current Summary Drill Down Report view and then drill down further to see which URLs that user visited, thereby creating a Detail Drill Down Report view.

Step E: Create a Detail Drill Down Report to obtain a list of URLs

1. To investigate the activity of a specific user listed in the current Summary Drill Down Report view, select that user's record and then click the down arrow in the Page Count column at the far right to show results in the Detail Drill Down Report view that now displays:

Date	Category	User IP	User	Site	Filter Action	Content Type	Content	Search String
6/7/2010 9:09:28 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	142.180.3.173	Allowed	Pattern	in:0142:180.3.173	in:0142:180.3.173
6/7/2010 9:09:28 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	142.180.51.242	Allowed	Pattern	in:0142:180.51.242	in:0142:180.51.242
6/7/2010 9:09:28 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	142.117.8.46	Allowed	Pattern	in:0142:117.8.46	in:0142:117.8.46
6/7/2010 9:09:27 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	142.180.3.173	Allowed	Pattern	in:0142:180.3.173	in:0142:180.3.173
6/7/2010 9:09:27 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	142.127.169.706	Allowed	Pattern	in:0142:127.169.706	in:0142:127.169.706
6/7/2010 9:09:27 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	142.113.79.130	Allowed	Pattern	in:0142:113.79.130	in:0142:113.79.130
6/7/2010 9:09:27 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	142.183.222.66	Allowed	Pattern	in:0142:183.222.66	in:0142:183.222.66
6/7/2010 9:09:27 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	142.180.188.33	Allowed	Pattern	in:0142:180.188.33	in:0142:180.188.33
6/7/2010 9:09:27 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	181.219.191.198	Allowed	Pattern	in:0181:219.191.198	in:0181:219.191.198
6/7/2010 9:09:27 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	142.182.30.42	Allowed	Pattern	in:0142:182.30.42	in:0142:182.30.42
6/7/2010 9:09:27 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	172.26.224.26	Allowed	Pattern	in:0172:26.224.26	in:0172:26.224.26
6/7/2010 9:09:27 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	142.127.133.54	Allowed	Pattern	in:0142:127.133.54	in:0142:127.133.54
6/7/2010 9:09:28 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	172.16.1.63	Allowed	Pattern	in:0172:16.1.63	in:0172:16.1.63
6/7/2010 9:09:28 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	142.182.118.79	Allowed	Pattern	in:0142:182.118.79	in:0142:182.118.79
6/7/2010 9:09:33 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	142.184.79.90	Allowed	Pattern	in:0142:184.79.90	in:0142:184.79.90
6/7/2010 9:09:33 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	142.113.72.62	Allowed	Pattern	in:0142:113.72.62	in:0142:113.72.62
6/7/2010 9:09:33 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	142.117.26.16	Allowed	Pattern	in:0142:117.26.16	in:0142:117.26.16
6/7/2010 9:09:33 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	181.219.142.32	Allowed	Pattern	in:0181:219.142.32	in:0181:219.142.32
6/7/2010 9:09:33 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	142.122.104.78	Allowed	Pattern	in:0142:122.104.78	in:0142:122.104.78
6/7/2010 9:09:33 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	142.117.8.46	Allowed	Pattern	in:0142:117.8.46	in:0142:117.8.46
6/7/2010 9:09:33 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	142.127.137.52	Allowed	Pattern	in:0142:127.137.52	in:0142:127.137.52
6/7/2010 9:09:33 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	142.127.133.54	Allowed	Pattern	in:0142:127.133.54	in:0142:127.133.54
6/7/2010 9:09:33 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	172.26.224.140	Allowed	Pattern	in:0172:26.224.140	in:0172:26.224.140
6/7/2010 9:09:33 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	172.24.64.33	Allowed	Pattern	in:0172:24.64.33	in:0172:24.64.33
6/7/2010 9:09:33 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	142.122.79.22	Allowed	Pattern	in:0142:122.79.22	in:0142:122.79.22
6/7/2010 9:09:33 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	142.184.242.18	Allowed	Pattern	in:0142:184.242.18	in:0142:184.242.18
6/7/2010 9:09:33 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	142.117.155.103	Allowed	Pattern	in:0142:117.155.103	in:0142:117.155.103
6/7/2010 9:09:33 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	142.182.30.34	Allowed	Pattern	in:0142:182.30.34	in:0142:182.30.34
6/7/2010 9:09:33 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	142.188.242.18	Allowed	Pattern	in:0142:188.242.18	in:0142:188.242.18
6/7/2010 9:09:33 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	142.180.180.251	Allowed	Pattern	in:0142:180.180.251	in:0142:180.180.251
6/7/2010 9:09:33 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	142.181.105.75	Allowed	Pattern	in:0142:181.105.75	in:0142:181.105.75
6/7/2010 9:09:33 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	142.128.103.31	Allowed	Pattern	in:0142:128.103.31	in:0142:128.103.31
6/7/2010 9:09:33 AM	INSTMS	10.1.0.5	ledfcmantel@psg.com	172.25.244.196	Allowed	Pattern	in:0172:25.244.196	in:0172:25.244.196

Note that the Detail Drill Down Report view contains columns of information pertaining to the user's machine and setup on the network, sites visited, categorized URLs, and clickable links to access pages the user viewed.

2. In this report view, click any URL link to open the page for that URL.



In the ER Web Client User Guide index, see:

- How to: create a detail Page Count report from a summary report

See also:

- How to: create a detail Object Count report from a summary report

You have now learned how to access Executive Reports and to use Drill Down Reports to conduct an investigation. You have also learned how to change the date scope of a Drill Down Report to create a new report, generate a double-break report view to include two sets of criteria, and drill down into the current summary report view to create a detail report view.

These tools and other tools can be used separately or combined to create many different types of reports to fulfill different purposes.

II. Double-break Report and Export Report exercise

In this exercise you will learn how to display only the top 10 records of a summary drill down double-break report view, export that report view in the .PDF output format, and then view the results of the generated .PDF file.

Step A: Drill down to view the most visited sites in a category

1. From the top panel, go to **Drill Down Reports > Categories** to generate a Summary Drill Down Report view, ranking categories in order by the most visited to the least visited:

Executive Reports | Drill Down Reports | Custom Reports | Settings | Help | Logout

Enterprise Reporter **M86 SECURITY**

DRILL DOWN REPORTS : CATEGORY/IPS

Summary Drill Down Report
 → Category/IPS → Display: Top 50 by Page Count → Date: 6/7/2010 → Search: None → Sort By: Page Count, Descending
 Records: 1 of 50

IP#	IP/ Categories	IP/ Sites	Category/ IP Users	Category/ IP Sites	Category Count	IP Count	User Count	Site Count	Page Count	Object Count	Time (HH:MM:SS)
10.1.0.5							11	140	2,401	0	5:47:20
10.1.0.0							11	103	1,706	0	9:40:20
10.1.0.7							11	1	200	0	0:9:30
10.1.2.21							9	2	81	0	0:1:30
10.1.0.131							11	2	36	0	0:8:8
10.1.1.99							11	1	22	0	0:1:50
10.1.1.12							5	1	10	0	0:0:50
10.1.1.205							9	1	9	0	0:1:30
10.1.1.217							9	1	9	0	0:1:30
10.1.3.18							4	1	9	0	0:0:40
10.1.0.12							11	1	0	80	0:0:0
10.1.0.126							11	1	0	11	0:0:0
10.1.0.139							11	1	0	11	0:0:0
10.1.0.142							11	1	0	26	0:0:0
10.1.0.180							11	1	0	32	0:0:0
10.1.0.192							11	1	0	24	0:0:0
10.1.0.194							11	1	0	29	0:0:0
10.1.0.202							11	1	0	11	0:0:0
10.1.0.22							11	1	0	21	0:0:0
10.1.0.229							11	1	0	24	0:0:0
10.1.0.237							5	1	0	6	0:0:0
10.1.0.239							9	1	0	11	0:0:0
10.1.0.20							9	1	0	30	0:0:0
10.1.0.38							9	1	0	11	0:0:0
10.1.0.47							11	1	0	36	0:0:0

2. To find out which sites were visited in a popular category, target the category and then click the **Category/Sites** filter button corresponding to that category to create a double-break report view:

Executive Reports | Drill Down Reports | Custom Reports | Settings | Help | Logout

Enterprise Reporter **M86 SECURITY**

DRILL DOWN REPORTS : CATEGORY/SITES

Summary Drill Down Report
 → Category/Sites → Display: Top 50 by Page Count → Date: 6/6/2010 → Search: None → Sort By: Page Count, Descending
 Records: 1 of 50

Site#	Site/ Categories	Site/ Users	Category/ Site/ IP#	Category/ Site/ Users	Category Count	IP Count	User Count	Site Count	Page Count	Object Count	Time (HH:MM:SS)
142.102.19.27						5	40		251	0	0:14:0
142.117.1.48						1	15		171	0	0:3:30
181.216.142.32						1	15		160	0	0:5:48
142.113.112.169						1	13		129	0	0:5:50
142.113.72.82						1	13		122	0	0:4:48
142.117.26.16						1	13		120	0	0:5:30
142.113.79.130						1	13		100	0	0:7:50
172.25.244.180						1	12		86	0	0:5:40
142.126.8.42						1	9		69	0	0:7:30
142.180.108.33						1	13		85	0	0:7:50
142.127.133.54						1	13		78	0	0:8:8
142.182.81.242						1	13		73	0	0:6:50
142.117.42.20						1	12		70	0	0:8:50
142.117.100.94						1	13		60	0	0:7:30
142.104.70.12						1	6		56	0	0:1:0
142.122.75.75						1	12		65	0	0:5:20
142.104.242.19						1	13		69	0	0:2:18
172.22.26.28						1	13		62	0	0:4:10
142.104.70.90						1	13		60	0	0:5:10
142.127.180.106						1	13		57	0	0:4:30
142.117.20.231						1	13		55	0	0:6:0
142.160.0.191						1	12		49	0	0:5:10
142.190.3.172						1	12		42	0	0:3:30
142.127.107.62						1	13		41	0	0:7:40
142.182.10.28						3	26		41	0	0:4:10

Note that URLs/IP addresses of sites users visited in the category now display in the first column of the modified report view, instead of category names.

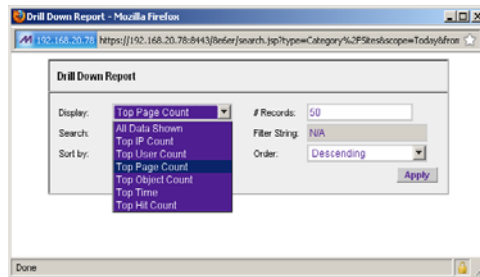


In the ER Web Client User Guide index, see:

- How to: generate a Drill Down Report
- How to: use filter columns and buttons

Step B: Modify the report view to only display top 10 site records

1. Now, to only display the top 10 sites users visited in that category, click **Modify Report** to open the Drill Down Report pop-up window where you make customizations to the current report view:



NOTE: Notice that by default the report will be set to Sort by "Page Count."

2. Select "Top IP Count" from the Display drop-down menu, and type in **10** in the **# Records** field.
3. Click **Apply** to close the pop-up window and to display the report view showing only the top 10 site records for the selected category:

Site	Site Categories	Site Users	Category Site IP	Category Site Users	Category Count	IP Count	User Count	Site Count	Page Count	Object Count	Time (HH:MM:SS)
142.192.19.27						5	40		291	0	0:14:0
142.192.19.28						3	25		41	0	0:4:10
142.113.112.100						1	13		30	0	0:3:10
142.113.112.119						1	2		4	0	0:0:20
207.46.110.14						16	103		0	226	0:0:0
207.46.110.15						6	67		0	121	0:0:0
207.46.110.35						15	147		0	212	0:0:0
207.46.110.36						8	86		0	159	0:0:0
hulkmail.com						6	27		0	29	0:0:0
imgag.com						2	14		0	106	0:0:0

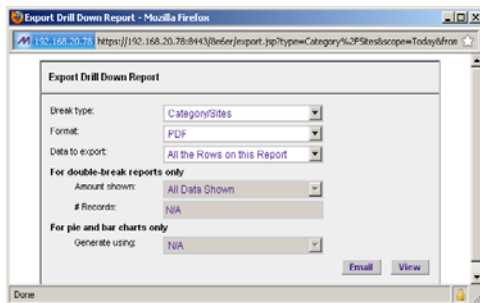


In the ER Web Client User Guide index, see:

- How to: modify a Drill Down Report
- How to: display only a specified number of records

Step C: Export the report view in the .PDF output format

1. To export the current report view in the .PDF format, at the top of the report view click **Export Report** to open the Export Drill Down Report pop-up window:




By default, “PDF” displays in the **Format** field, so the format selection does not need to be changed.

2. Click **View** to begin the exportation process. When this process has been completed, the .PDF file opens in a separate browser window:

Enterprise Reporter		Jun 08, 2010 - Jun 08, 2010		M86 SECURITY			
Sort Order: Page Count, descending		Category/Sites					
INSTMS							
Sites	IP Count	User Count	Page Count	Object Count	Time (HH:MM:SS)	Hit Count	Blocked Hits
142.182.19.27	5	43	281	0	0:14:0	281	0
142.182.19.28	3	25	41	0	0:4:10	41	0
142.113.112.109	1	13	32	0	0:3:10	32	0
142.113.112.118	1	2	4	0	0:0:20	4	0
207.46.110.14	18	153	0	228	0:0:0	228	0
207.46.110.15	8	67	0	121	0:0:0	121	0
207.46.110.35	15	147	0	212	0:0:0	212	0
207.46.110.36	9	98	0	159	0:0:0	159	0
hotmail.com	6	27	0	29	0:0:0	29	0
imgag.com	2	14	0	125	0:0:0	125	0
Grand Total	68	577	338	872	0:21:40	1,210	0
Count: 10							

6/8/2010 1:58:46 PM Generated by: manager Filter: None Page 1 of 1

The generated .PDF file for the report includes a list of the top 10 Sites records for the selected category, as well as the following counts for each record in the report: IP, User, Page, Object, Time (HH:MM:SS), Hit, and Blocked Hits. The Grand Total and total Count display at the end of the report.

 **NOTE:** Notice that the report is sorted by Page Count, the default selection in the Modify Report pop-up window.

3. Print or save the .PDF file using available tools or icons in the .PDF file window, or close the .PDF file.



In the ER Web Client User Guide index, see:

- *How to: export a summary Drill Down Report*
- *How to: view and print a Web Client report*

See also:

- *How to: export a detail Custom Report*
 - *How to: email a report*
-

You have now learned how to modify a double-break Summary Drill Down Report view to include only the top 10 records, and then export that content for viewing in the .PDF format.

Variations of this exercise can be performed to generate and export countless reports using criteria of your specifications.

III. Save and schedule a report exercise

In this exercise you will learn how to save a report view and then create a schedule for running a report on a regular basis using criteria specified for that report. While a Summary Drill Down Report is used in this exercise, these steps also apply to a Detail Drill Down Report.

Step A. Save a report

1. After generating a Summary Drill Down Report, to save the criteria used in that report view, click **Save Report** at the top of the report view to open the Save Custom Report pop-up window:

The screenshot shows a web browser window titled "Save Custom Report - Mozilla Firefox". The address bar shows a URL starting with "https://192.168.20.78". The main content area is a form with the following fields and options:

- Save Name: [Text input]
- Description: [Text input]
- Date Scope: [Dropdown menu, selected: Today]
- From Date: [Date picker]
- To Date: [Date picker]
- From Time: [Time picker]
- To Time: [Time picker]
- Break type: [Dropdown menu, selected: Categories]
- Output type: [Dropdown menu, selected: E-Mail As Attachment]
- Format: [Dropdown menu, selected: PDF]
- Hide Un-identified IPs
- For double-break reports only**
 - Amount shown: [Dropdown menu, selected: All Data Shown]
 - # Records: [Text input, value: N/A]
- For pie and bar charts only**
 - Generate using: [Dropdown menu, selected: N/A]
- For E-Mail output only**
 - To: [Text input]
 - Cc: [Text input]
 - Bcc: [Text input]
 - Subject: [Text input]
 - Body: [Text area]

At the bottom of the form are three buttons: "Save and Schedule", "Save and Run", and "Save Only".

Note that this window is populated with specifications used in the current report view.

2. For this exercise, make entries in the following fields: **Save Name**, **Description**, and **For E-Mail output only (To and Subject fields)**.
3. Choose the **Save and Schedule** option from the "Save" options at the bottom of the window. The three "Save" options are as follows:
 - **Save and Schedule** - this option lets you save criteria from the current report view and then set up a schedule to run the report using that criteria.
 - **Save and Run** - this option lets you save criteria from the current report view and then automatically generate a report in the specified output format.
 - **Save Only** - this option lets you save criteria from the current report view.



NOTE: Saved reports can be edited at any time. These reports are accessed by going to Custom Reports, selecting Saved Custom Reports, and then choosing the report from the **Report Name** drop-down menu.



In the ER Web Client User Guide index, see:

- How to: save a custom report

See also:

- How to: access Saved Custom Reports
- How to: edit a saved report

Step B. Schedule a recurring time for the report to run

Now that you've saved the report, you must schedule a time for the report to run.

1. When clicking **Save and Schedule**, an alert box opens to let you know the "Custom Report has been saved."
2. Click **OK** to close this alert box and to display the Event Schedules panel, and also open the Add to Event Schedule pop-up window:

3. In the Add Event to Schedule pop-up window, enter a **Name** for this event, select the run frequency (Daily, Weekly, Monthly), and specify Day and Time options.
4. Click **Save** to save your settings and close the pop-up window, and to open the alert box that informs you of the next scheduled run for the report.
5. Click **OK** to close the alert box and to add the event to the schedule:

Name	Interval	Last Run	Next Run	Report Name	Start Time	Creator		
RCTMS	Daily		06/05/2010 08:00:00 AM	RCTMS	08:00 AM	manager	Select	Edit

NOTE: If you would like your scheduled event to run today, be sure to specify a future Start Time in the Add Event to Schedule menu.



In the ER Web Client User Guide index, see:

- *How to: schedule a report to run*

You have now learned how to save a report and schedule a recurring event for running this report.

Reports created for a variety of purposes can be scheduled to run on different dates and times to capture records of specified user activity as necessary.

IV. Create a custom category group and generate reports

After you've run a few summary and detail reports for the top visited categories, you might want to generate reports targeting specified categories only. To do so, you must first create a custom category group.

Step A: Create a custom category group

1. To create a category group, choose Settings from the top panel.
2. Select Category Groupings.
3. In the Group Information frame, type in the name for the category group and then click **Add**.



In the ER Web Client User Guide index, see:

- *How to: add a category group in the Web Client*

Step B: Run a report for a specified category group

1. To create a report for category group, choose Custom Reports from the top panel.
2. Select Custom Report Wizard.
3. Specify the type of report to be generated:
 - **Summary Report** - If making this selection, click the **Next** button, choose the sort **Type** for the results (Categories, IPs, Users, or Sites), select the **Category Group** name, and then click the **View Drill Down Results** button to generate the report.
 - **Specific User Detail by Page/Object** - If making this selection, click the **Next** button, choose the **Category Group** name, and then click the **View Drill Down Results** button to generate the report.



In the ER Web Client User Guide index, see:

- *How to: generate a custom Web Client report*

V. Create a custom user group and generate reports

In addition to running reports for various custom category groups, you might want to create one or more custom user groups and run reports for these user groups.



NOTE: *In order to generate reports for a custom user group, the user group must be created a day in advance, since the list of users is updated each day automatically based on group definitions and latest usage data.*

Step A: Create a custom user group

1. To create a user group, choose Settings from the top panel.
2. Select User Groupings.
3. In the Group Information frame, type in the name of the user group and then click **Add**.
4. In the Group Definitions frame, select the **Group Name** from the list.
5. Click **Add To Group** to open the pop-up window.
6. For this example, in the **Please enter a filter** field of the Individual Adds/ Removes frame, make a wildcard entry by typing in the % (percent) symbol followed by the username, and then clicking **Apply Filter** for results.
7. Select the user(s) from the results list box, and then click **Add to Individuals** to include the user(s) in the Group Definitions list box for the user group.



In the ER Web Client User Guide index, see:

- *How to: add a user group in the Web Client*

Step B: Generate a report for a custom user group

Once the custom user group is recognized by the ER (on the following day), reports can be generated.

Summary Report

There are two ways to generate a summary report for a custom user group. You can use the Custom Report Wizard option (from Custom Reports), or you can use the Single User Group Drill Down Report option (from Drill Down Reports).

- **Custom Report Wizard** - To use this option, choose Custom Reports from the top panel, select Custom Report Wizard, and then specify **Summary Report**. Click the **Next** button, choose the sort **Type** for the results (Categories, IPs, Users, or Sites), select the User Group name, and then click the **View Drill Down Results** button to generate the report.
- **Single User Group Drill Down Report** - To use this option, choose Drill Down Reports from the top panel, select Single User Group, and then specify Single User Group Report criteria for the **User Group** you select from the menu. Click **Apply** to generate the report.

Detail Report

Specific User Detail by Page/Object - To use this option, choose Custom Reports from the left panel, select Custom Report Wizard, and then specify **Specific User Detail by Page/Object**. Click the **Next** button, choose the **User Group** name, and then click the **View Drill Down Results** button to generate the report.



In the ER Web Client User Guide index, see:

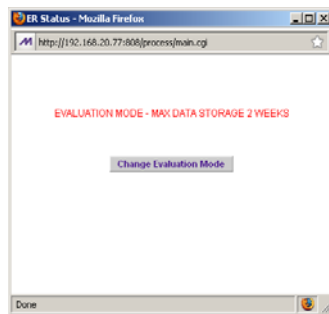
- *How to: generate a custom Web Client report*
 - *How to: generate a Single User Group Report*
-

IMPORTANT INFORMATION ABOUT USING THE ER IN THE EVALUATION MODE

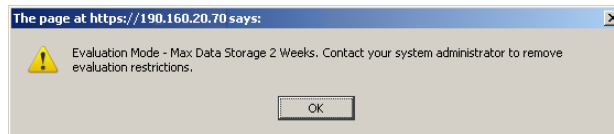
When evaluating the ER and using this product in the evaluation mode, the Expiration screen in the Administrator console and the ER Server Statistics window in the client will display and function differently than they do in the activated (standard) mode of the ER (described in the M86 Enterprise Reporter Administrator User Guide and ER Web Client User Guide).

Evaluation Mode Pop-Ups

When evaluating the ER in the evaluation mode, the ER Status pop-up box opens after logging in to the ER Administrator console:




In the ER Web Client user interface, the following alert pop-up box opens when navigating to **Settings > Server Statistics** and accessing the ER Server Information window:



Click **OK** to close this alert pop-up box.

These two pop-up boxes will continue to open in the user interfaces until the ER is in the activated mode.

 **NOTE:** See Appendix A in the ER Administrator User Guide for information about changing the ER's mode from evaluation to activated.

Administrator Console, Expiration Screen

In the Expiration screen, the following message displays at the top of the screen: "Evaluation Mode – Max Data Storage 'X' Weeks" (in which 'X' represents the maximum number of weeks in the ER's data storage scope). In the evaluation mode, you will not be able to make adjustments to the data storage scope. Thus, the Save button is not included at the bottom of the screen. Evaluation Mode information is for viewing purposes only.

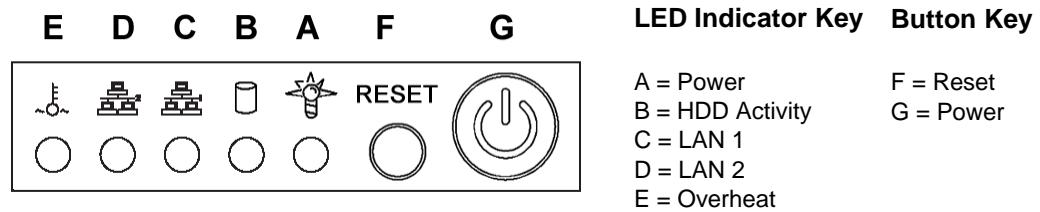
ER Web Client, ER Server Information Window

In the ER Server Information window, the note “*Evaluation Mode Enabled” displays above the ER Activity frame. To the right of this note, the Server Info button displays. When this button is clicked, an alert box opens with the message: “Evaluation Mode – Max Data Storage ‘X’ Weeks” (in which ‘X’ represents the maximum number of weeks in the data storage scope). Click **OK** to close the box.

LED INDICATORS AND BUTTONS

Diagrams and Descriptions

LED indicators and buttons for hardware status monitoring display on the front panel, located on the right side of the chassis (see diagram below).



Chassis control panel

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

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

REGULATORY SPECIFICATIONS AND DISCLAIMERS

Declaration of the Manufacturer or Importer

Safety Compliance

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

Electromagnetic Compatibility (EMC)

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

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

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

FCC Declaration of Conformity

Model: MSA-002-003

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.

Bureau of Standards Metrology and Inspection (BSMI) - Taiwan

BSMI EMC STATEMENT -- TAIWAN

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

警告使用者：

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

EC Declaration of Conformity

European Community Directives Requirement (CE)

Declaration of Conformity

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

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

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

Product Name(s): Internet Appliance

Product Model Number(s): MSA-002-003

Year in which conformity is declared: 2008

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

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

Location: Orange, CA, USA

Signature:



Date: January 21, 2008

Full Name: Gregory P. Smith

Position: Director of Engineering Operations

APPENDIX: CONSOLE SETUP PROCEDURES

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


Preliminary Setup

Create a “setup workstation” using a Windows-based laptop or desktop machine with a network card and Internet Explorer 7.0 (or later). The setup workstation will be used for accessing the IR server on the network and configuring the unit.



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

Workstation Configuration

- A. From the desktop of the setup workstation, while logged in with Administrator privileges, follow the procedures for your machine type:
 - **Windows XP:** Go to Start > Control Panel. Open Network Connections. Right-click the link for LAN or High-Speed Internet and choose Properties.
 - **Windows Vista:** Go to the start icon > Control Panel > Network and Internet > Network and Sharing Center > Manage network connections. Right-click the Local Area Connection you want to change, then choose Properties.
 - **Windows 7:** Go to the start icon > Control Panel. In the search box, type **adapter**. Under Network and Sharing Center, choose View network connections. Right-click the Local Area Connection you want to change, then choose Properties.
 - B. On a Windows XP machine, click on **Internet Protocol (TCP/IP)** to highlight it. On a Windows Vista or Windows 7 machine, go to the Networking tab. Under This connection uses the following items, choose **Internet Protocol Version 4 (TCP/IPv4)** to highlight it.
 - C. Click the **Properties** button.
-  **WARNING:** *Be sure to make note of the current network settings on the setup workstation as you will need to return them for further setup procedures.*
- D. Choose the option **Use the following IP address**.
 - E. Type in the **IP address** of 1.2.3.1.
 - F. Type in the **Subnet mask** (netmask) of 255.0.0.0 and click **OK**.
 - G. Close the LAN connection properties box.

Link the Workstation to the IR

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

- A. Plug one end of the CAT-5E crossover cable into the IR's **LAN 2** port.



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



Portion of MSA chassis rear

- B. Plug the other end of the CAT-5E crossover cable into the setup workstation's network card.
- C. Connect the AC power cord to the back of the chassis and plug the cord into a UPS power supply unit.
- D. Power on the server by lowering the bezel and pressing the large button at the right of the front panel:

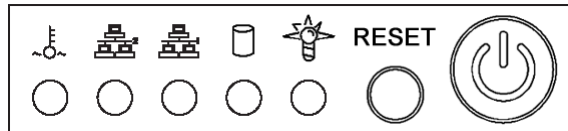


Diagram of MSA chassis front panel, power button at far right

The Boot Up Process

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

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

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

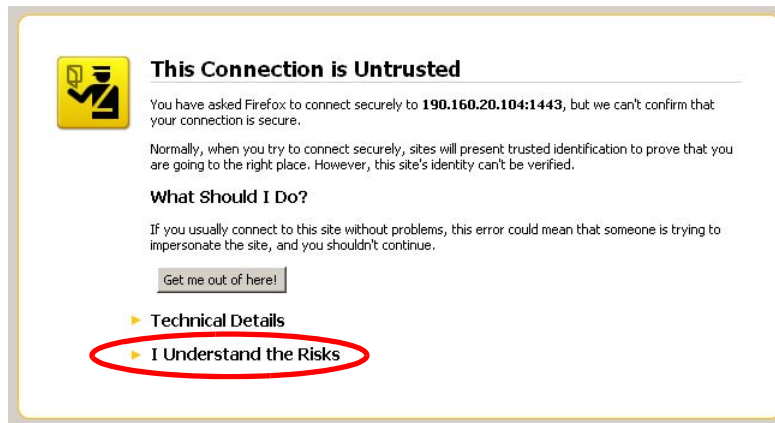
If you receive a reply, the unit is up.

Security Certificate Acceptance Procedures

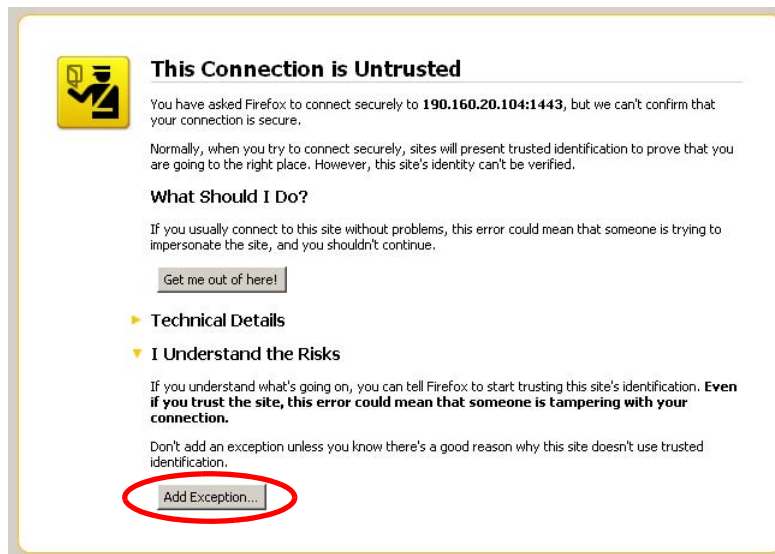
- A. From the setup workstation, launch an Internet supported browser such as Firefox 3.6, Internet Explorer 7 or 8, or Safari 4.0.
- B. Type in **https://1.2.3.4:1443** in the address field.
- C. Click **Go** to display the security issue page:
 - If using Firefox, proceed to Accept the Security Certificate in Firefox.
 - If using IE, proceed to Temporarily Accept the Security Certificate in IE.
 - If using Safari, proceed to Accept the Security Certificate in Safari.

Accept the Security Certificate in Firefox

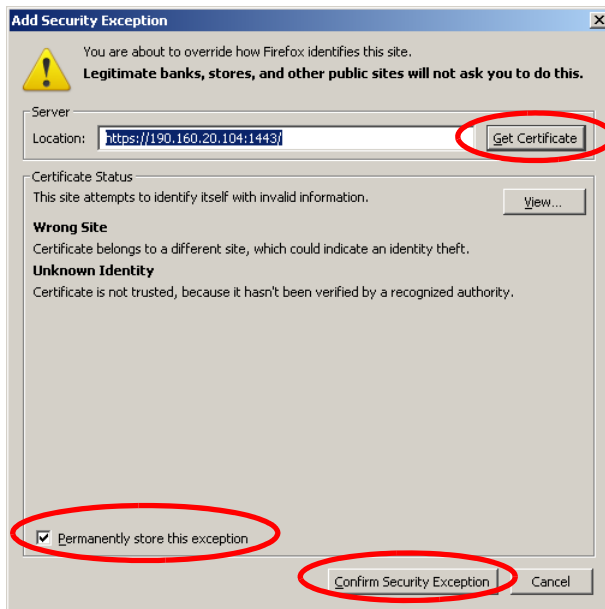
- A. If using a Firefox browser, in the page “This Connection is Untrusted,” click the option **I Understand the Risks**:



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




Clicking Add Exception opens the Add Security Exception window:

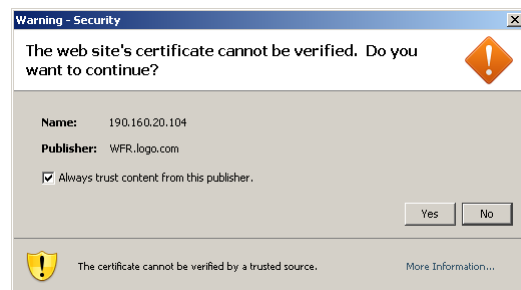


- C. In the Add Security Exception window, click **Get Certificate** and wait a few seconds until the security certificate is obtained by the server.
- D. With the checkbox **Permanently store this exception** selected, click **Confirm Security Exception** to open the Welcome window of the IR user interface:



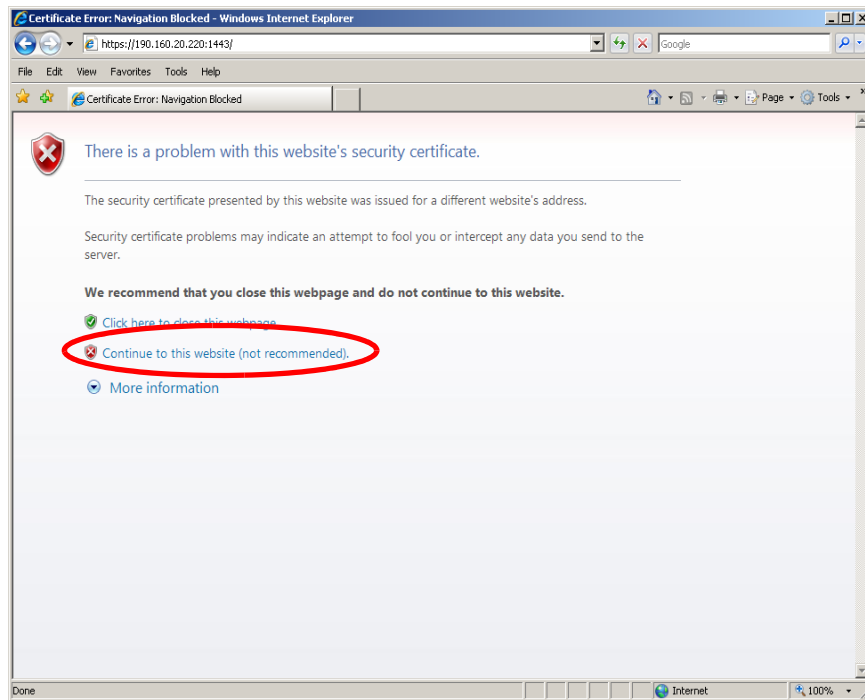
 **NOTE:** You will need to add a security exception for the Web Filter, Enterprise Reporter (Web Client), and Enterprise Reporter Administration Module when you attempt to access each of these applications for the first time. On a newly installed unit, the ER Web Client will remain inaccessible until logs are transferred to the ER Administration Module and the ER's database is built.

When attempting to access the Web Filter user interface for the first time, the Security warning dialog box (shown in the sample image at left) will open instead of the Security Exception page. With the checkbox "Always trust content from this publisher." populated, click **Yes** to close the Security warning dialog box and to access the login window of the Web Filter user interface.

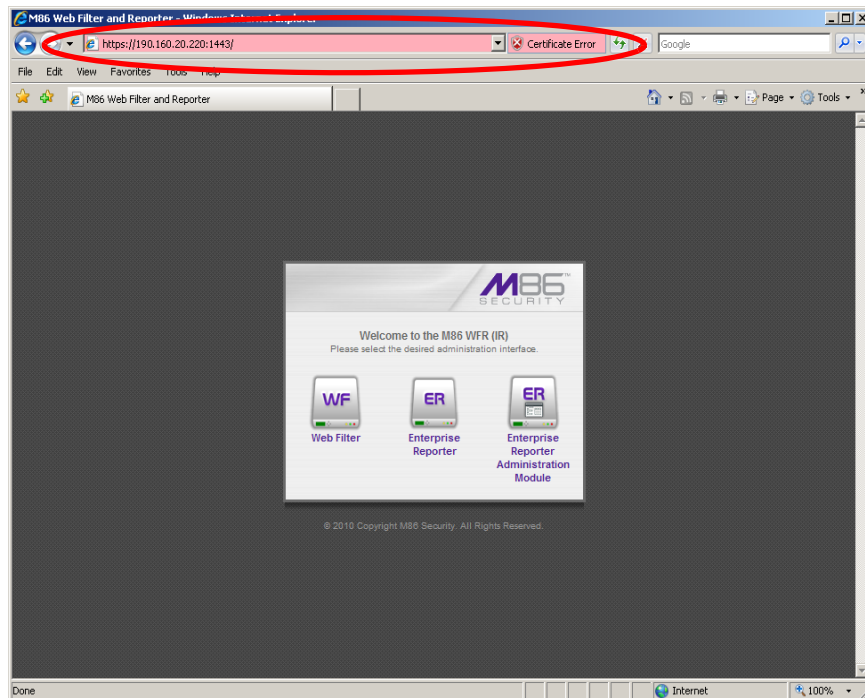


Temporarily Accept the Security Certificate in IE

If using an IE browser, in the page “There is a problem with this website's security certificate.”, click **Continue to this website (not recommended)**:



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



Accept the Security Certificate in Safari

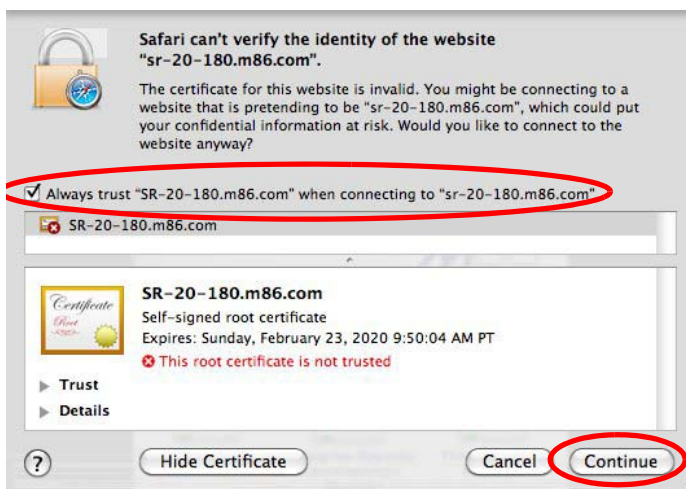
- A. If using a Safari browser, the pop-up window "Safari can't verify the identity of the website..." opens:



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.

Network Setup

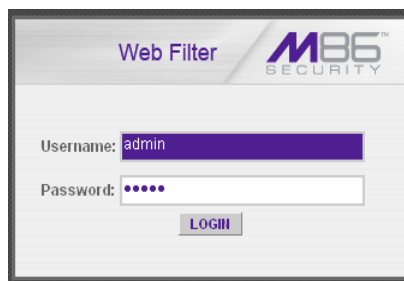
For this step, you will need your network administrator to provide you the host name, gateway address, and two unused IP addresses. You will first configure the Web Filter server. Later you will configure the ER server.

Access the Web Filter Administrator Console

- A. From the IR Welcome window, click the WF button to open the Web Filter login window.

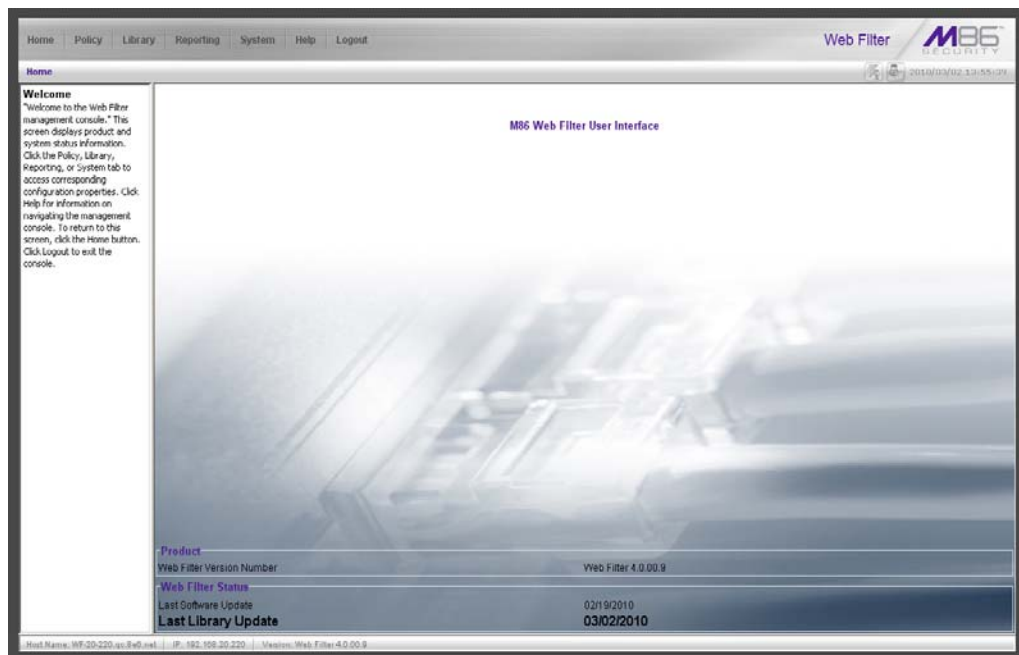
 **NOTE:** You will need to follow the procedures for accepting the security certificate and/or acknowledging the security warning for the Web Filter.

- B. In the **Username** field, type in **admin**.



- C. In the **Password** field, type in **user3**.

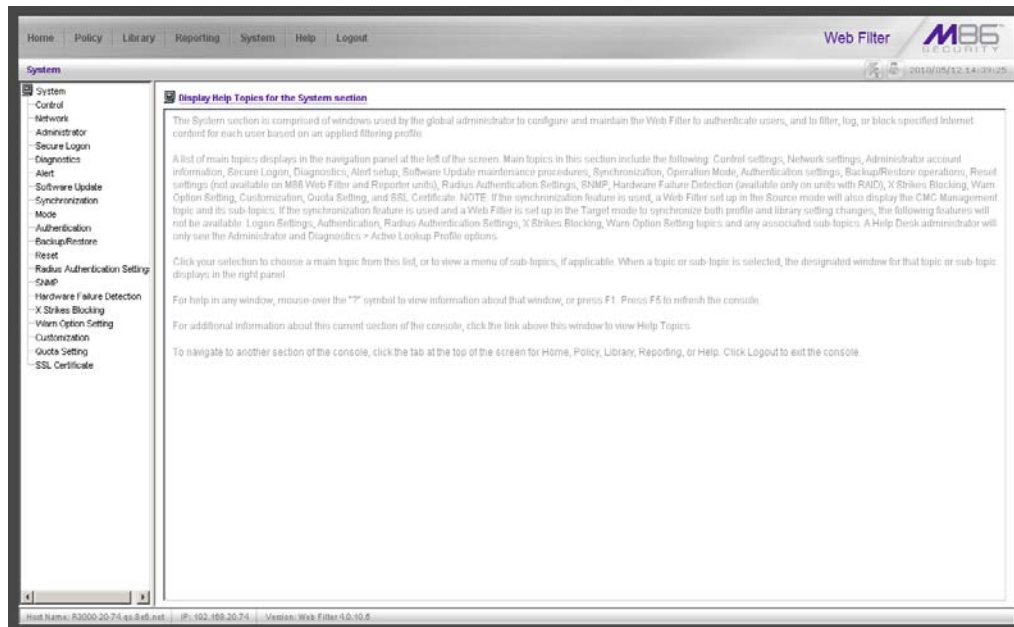
- D. Click **LOGIN** to go to the main screen of the Web Filter Administrator console:



Product	
Web Filter Version Number	Web Filter 4.0.00.9
Web Filter Status	
Last Software Update	02/19/2010
Last Library Update	03/02/2010

Network

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



In this section of the console you will:

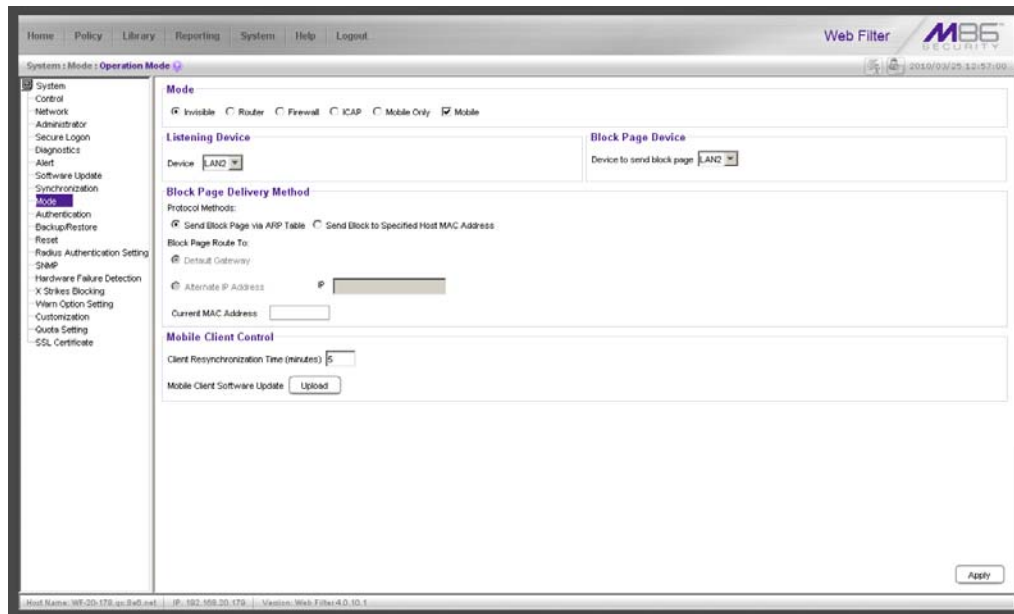
- Specify the operation mode the Web Filter will use for filtering the network, listening to traffic, and sending traffic
- Configure LAN settings the Web Filter will use on your network
- Select NTP servers the Web Filter will use for time synchronization with Internet clocks
- Indicate the region in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



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


Network: Operation Mode

From the navigation panel at the left of the screen, click Mode and choose Operation Mode from the pop-up menu:



Make the following entries in the Operation Mode window:

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

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


- B. In the Listening Device frame, select the device for listening to traffic:
- **For the invisible mode:** “LAN1” is generally used as the default listening device
 - **For the router or firewall mode:** Select the network card that will be used to “listen to”—as opposed to “send”—traffic on the network
- C. In the Block Page Device frame, select the device for sending block pages to client PCs:
- **For the invisible mode:** The block page device should be a different device than the one selected in the Listening Device frame—“LAN2” is generally used as the default device for sending block pages
 - **For the router or firewall mode:** The device should be the same as the one selected in the Listening Device frame
- D. Click **Apply**.

Network: LAN Settings

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

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

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


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

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

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

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

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

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

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

- E. Enter the **Secondary IP** address of the second DNS name server. The Web Filter will use this name server to resolve the domain name requested by users from the LAN if the first DNS isn't working.
- F. Enter the **Gateway IP** address for the default router or firewall that is the main gateway for the entire network. The Web Filter will use this IP address to communicate outside the network.

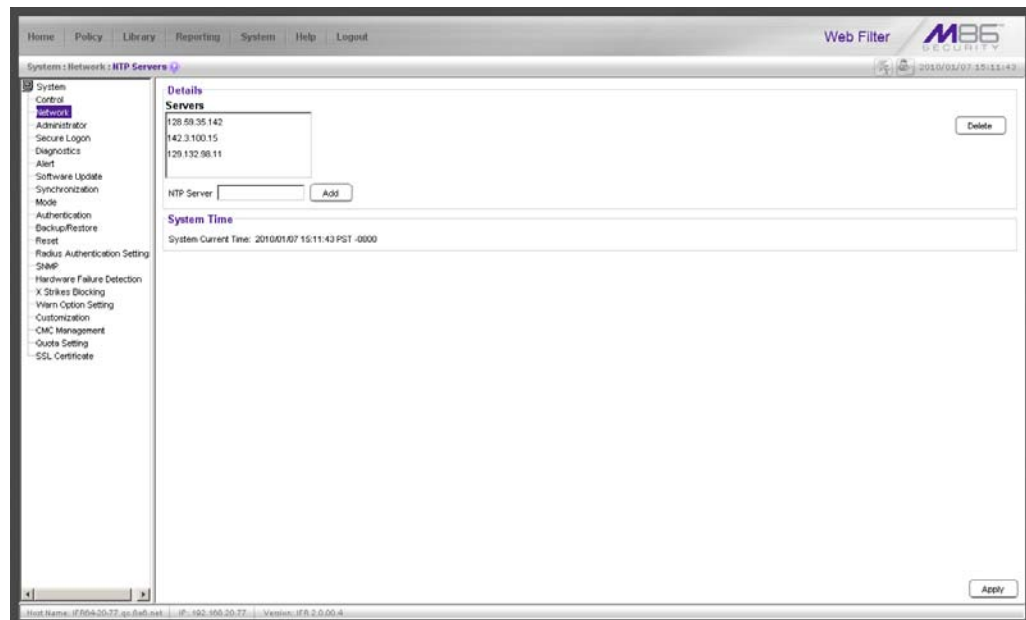


WARNING: Be sure to take note of the LAN 1 and LAN 2 IP addresses and host name you assigned to the Web Filter. It is strongly suggested you document and store this information as it is now the only way of communicating with the Web Filter.

- G. Click **Apply**.

Network: NTP Servers

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



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

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



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

- A. In the **NTP Server** field, enter the IP address of the primary NTP server you wish to use for clock settings on your server.
- B. Click **Add** to include this IP address in the Servers list box.

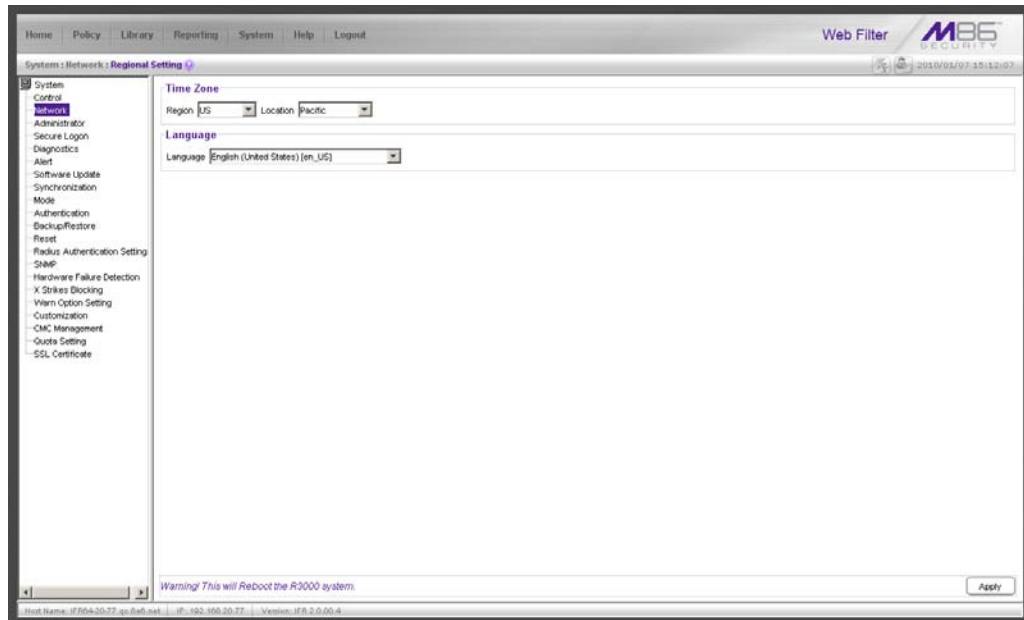
- C. Enter two more NTP servers, following the procedures in sub-steps A and B. These will be the secondary and tertiary NTP servers, in order as they appear in the list box.
- D. Click **Apply**.



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

Network: Regional Setting

From the navigation panel, click Network and choose Regional Setting from the pop-up menu:




Make the following selections in the Regional Setting window:

- A. At the **Region** pull-down menu, select your country from the available choices.
- B. At the **Location** pull-down menu, select the time zone for the specified region.
If necessary, select a language set from the **Language** pull-down menu to display that text in the console.
- C. Click **Apply** to apply your settings, and to reboot the Web Filter.

Physically Connect the IR to the Network

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


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

- A. Restart the server using the steps defined below (i-iii). These steps must always be performed when restarting the IR. **Never** reset the server by using the power or reset buttons.
 - i. From the navigation panel of the System section of the Web Filter console, click Control and select Reboot from the pop-up menu to display the Reboot window.
 - ii. Click the **Reboot** button.
 - iii. From the time you click Reboot, you have approximately 2 minutes to perform sub-steps B through E while the IR goes through the reboot process.
- B. Disconnect the crossover cable from the IR.
- C. Plug one end of a standard CAT-5E cable into the IR's LAN 1 port.
- D. Plug the other end of the CAT-5E cable into an open port on the network hub that handles the Internet traffic you wish to filter.
- E. Repeat sub-steps B and C for the IR's LAN 2 port.



Portion of MSA chassis rear

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

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

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

Test the IR Console Connection

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

- A. Restore the setup workstation you used for the Network Setup to its original settings, and connect it to the network hub to create a “network workstation.” (You could also use another workstation already on the network that has Internet access.)
- B. Launch a supported Internet browser on the network workstation, and enter the IP address you assigned to LAN 1 (Network: LAN Settings, sub-step B). Be sure to include the port information **:1443** for a secure connection in the address field. For example, if the IR was assigned an IP address of 10.10.10.10, you would enter **https://10.10.10.10:1443** in the browser window's address field.
- C. Click **Go**. You should be prompted to log into the Administrator console, giving the Username and Password.

If you can access the IR splash page, the IR is functioning on your network and you should proceed to Step 3: Log in, Generate SSL Certificate, from the Install the Server portion of this Installation Guide.

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

- The IR is turned on.
 - The IR is connected to the same hub as your router/firewall.
 - Can the PC normally connect to the Internet?
 - Is the PC able to ping LAN 1 of the IR?
 - Is the IR plugged into a switch instead of a hub?
 - Is there a caching server?
 - Can the IR ping the filtered PC? (Refer to the System Command window in the Diagnostics section of the IR Web Filter User Guide)
 - Did you restart the IR after changing the network settings?
 - Do you have both LAN ports connected to your network hub?
 - If still unsuccessful, contact an M86 Security solutions engineer or technical support representative.
- D. Once you are able to access the IR splash page, proceed to Step 2: Log in Web Filter, Generate SSL Certificate from the Install the Server portion of this Installation Guide.

INDEX

A

Add to Event Schedule 83
Always Allow Custom Category 71

B

Bandwidth/Productivity 63
Boot Up 94
BSMI 90, 91

C

Category block 59, 66
Change Quick Start password 25, 28
Change User Name and Password 52
crossover cable 4, 19, 94
Custom Block/Warn/X Strikes/Quota pages 68, 71
Custom Category (blocked) 61
custom category group 73, 84
Custom Lock, Block, Warn, X Strikes, Quota pages 60
custom user group 73, 85
Customize an M86 Supplied Category 70

D

Detail Drill Down Report 77, 82
Double-break Report 78
double-break report 73, 76

E

EMC 90
ER Client 54
ER Server Information 88
Evaluation Mode 87, 88
Exception URL bypass 62
Executive Reports 73, 74
Expiration 87
Export Report 78, 80

F

FCC 90
File type blocking 62

G

Game patterns 65
General/Productivity 68

H

HL 16
HTTPS settings 66

HyperTerminal Setup 21

I

ICES-003 90, 91
IM patterns 65
IP exceptions 72

L

Local category adds/deletes 70
Login screen 24
LVD 90

M

Minimum Filtering Level 61
Mobile Client 47, 101
Modify Report 79
MSA 20, 30, 94, 105

N

New Report 75

O

Overall Quota 63, 70
Overheat 89
Override Account bypass 61
Override Accounts 72

P

P2P patterns 64
Pass/Allow 71
Pattern detection bypass 72
Physically Connect the Web Filter to the Network 30, 105
Power Supply Precautions 15
Proxy Patterns 62

Q

Quick Start menu 24

R

Rack Setup Precautions 6
Real Time Probe information 68
reboot 28, 30, 105
Remote Access patterns 66
report for a custom user group 86
Reset Admin account 28
Reset admin console account 25
RoHS compliant 92
Rule block 59, 67

S

Save Report 82
SE Keywords 67
Search Engine Keywords 60
serial port cable 19, 20
shut down 30, 105
Streaming Media patterns 65
Summary Drill Down Report 75, 77, 78, 81, 82

T

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

U

UL 90
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):
8845 Irvine Center Drive, CA 92618 • Tel: 949.932.1000 or 888.786.7999
Fax: 949.932.1086