



M86 Threat Analysis Reporter

INSTALLATION GUIDE

Models: HL, SL, MSA

M86 THREAT ANALYSIS REPORTER INSTALLATION GUIDE FOR HL, SL, MSA

© 2010 M86 Security

All rights reserved. Printed in the United States of America

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

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

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

Trademarks

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

Part# TAR-IG-HSM-100601

CONTENTS

| | |
|--|-----------|
| THREAT ANALYSIS REPORTER INTRODUCTION | 1 |
| About this Document..... | 2 |
| Conventions Used in this Document. | 2 |
| SERVICE INFORMATION | 3 |
| M86 Security Corporate Headquarters (USA)..... | 3 |
| M86 Security Taiwan..... | 3 |
| 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 for HL Servers | 7 |
| Rack Setup Suggestions | 7 |
| Identify the Sections of the Rack Rails | 7 |
| Install the Inner Rails | 7 |
| Install the Outer Rails | 8 |
| Install the Server into the Rack | 9 |
| Install the Server into a Telco Rack | 10 |
| Rack Mount Instructions for SL Servers | 11 |
| Rack Setup Suggestions | 11 |
| Install the Inner Slides | 11 |
| Install the Outer Slides | 11 |
| Install the Slide Assemblies to the Rack | 12 |
| Install the Chassis into the Rack | 13 |
| Rack Mount Instructions for MSA Servers | 14 |
| Optional: Install the Chassis Rails | 14 |
| Optional: Install the Traditional UP Racks | 16 |
| Optional: Install the Open Racks | 18 |
| Install the Chassis into the Rack | 21 |
| Install the SL or HL Server Bezel | 22 |
| Check the Power Supply. | 23 |
| Power Supply Precautions | 23 |
| General Safety Information. | 24 |
| Server Operation and Maintenance Precautions | 24 |
| AC Power Cord and Cable Precautions | 25 |
| Electrical Safety Precautions | 25 |
| Motherboard Battery Precautions | 26 |
| INSTALL THE SERVER | 27 |

| | |
|--|-----------|
| Step 1: Initial Setup Procedures..... | 27 |
| Quick Start Setup Requirements | 27 |
| LCD Panel Setup Requirements (for SL and HL Units) | 27 |
| Step 1A: Quick Start Setup Procedures..... | 28 |
| Link the Workstation to the Threat Analysis Reporter | 28 |
| Monitor and Keyboard Setup | 28 |
| Serial Console Setup | 28 |
| HyperTerminal Setup Procedures | 30 |
| Quick Start menu instructions | 33 |
| Login screen, password prompts | 33 |
| Configure Network Interface screen | 34 |
| Configure default gateway screen | 34 |
| Configure Domain Name Servers screen | 35 |
| Configure Host Name screen | 35 |
| Time zone regional configuration screen | 36 |
| Configure Wizard user screen | 36 |
| Quick Start Setup confirmation screen | 37 |
| Administration menu | 37 |
| System Status screen | 38 |
| Log Off, Disconnect the Peripherals | 38 |
| Step 1B: LCD Panel Setup Procedures..... | 39 |
| LCD Menu | 39 |
| Main Menu | 39 |
| IP / LAN1 and LAN2 | 40 |
| Gateway | 40 |
| DNS 1 and 2 | 40 |
| Host Name | 41 |
| Regional Setting (Time Zone, date, time) | 41 |
| Admin Console Wizard User | 41 |
| Non-Quick Start procedures or settings | 42 |
| Current Patch Level | 42 |
| Reboot..... | 42 |
| Shutdown | 42 |
| LCD Options menu | 42 |
| Heartbeat | 42 |
| Backlight | 43 |
| LCD Controls | 43 |
| Step 2: Physically Connect the Unit to the Network..... | 44 |
| Bandwidth Management | 44 |
| Step 3: Register TAR and its Applications. | 45 |
| Access TAR via its LAN 1 IP Address | 45 |
| Accept the Security Certificate in Firefox | 46 |
| Temporarily Accept the Security Certificate in IE | 47 |
| Accept the Security Certificate in Safari | 48 |
| Accept the End User License Agreement | 49 |
| Log in to the Threat Analysis Reporter Wizard | 49 |
| Use the TAR Wizard to Specify Application Settings | 50 |
| Enter Main Administrator Criteria | 50 |
| Enter Bandwidth Range | 50 |
| Enter Web Filter Setup Criteria | 51 |
| Enterprise Reporter registration | 51 |
| Save settings | 51 |

| | |
|---|-----------|
| Step 4: Generate SSL Certificate..... | 52 |
| Generate a Self-Signed Certificate for TAR | 52 |
| IE Security Certificate Installation Procedures | 54 |
| Accept the Security Certificate in IE | 54 |
| Windows XP or Vista with IE 7 or 8..... | 54 |
| Windows 7 with IE 8..... | 57 |
| Map TAR's IP Address to the Server's Host Name | 58 |
| CONCLUSION | 60 |
| BEST USAGE PRACTICES | 61 |
| Threat Analysis Reporter Usage Scenarios. | 61 |
| I. Screen navigation exercise | 61 |
| Step A: Navigate panels in the Gauges section | 61 |
| Step B: Navigate panels in the Policy section | 62 |
| Step C: Navigate panels in the Report/Analysis section | 63 |
| Step D: Navigate panels in the Administration section | 63 |
| II. Drill down into a gauge exercise | 64 |
| Step A: Select the gauge with the highest score | 64 |
| Step B: Investigate a user's activity in a specified gauge | 66 |
| Step C: Investigate the user's Internet activity in other gauges | 67 |
| III. Create a gauge exercise | 68 |
| Step A: Access the Add/Edit Gauges panel | 68 |
| Step B: Add a URL Gauge | 69 |
| IV. Create an email alert exercise | 71 |
| Step A: Add a new alert | 71 |
| Step C: Select Email Alert Action | 73 |
| Step D: Receiving an email alert | 74 |
| LED INDICATORS AND BUTTONS | 75 |
| SL and MSA Units. | 75 |
| Front LED Indicators and Buttons for Hardware Status Monitoring | 75 |
| HL Unit. | 76 |
| Front LED Indicators and Buttons for Hardware Status Monitoring | 76 |
| Rear LED Indicators for Hardware Status Monitoring | 77 |
| HL and SL Units. | 78 |
| Front LED Indicators for Software and Hardware Status Monitoring | 78 |
| REGULATORY SPECIFICATIONS AND DISCLAIMERS | 79 |
| Declaration of the Manufacturer or Importer..... | 79 |
| Safety Compliance | 79 |
| Electromagnetic Compatibility (EMC) | 79 |
| Federal Communications Commission (FCC) Class A Notice (USA) | 80 |
| FCC Declaration of Conformity | 80 |
| Electromagnetic Compatibility Class A Notice | 81 |
| Industry Canada Equipment Standard for Digital Equipment (ICES-003) | 81 |
| Bureau of Standards Metrology and Inspection (BSMI) - Taiwan | 81 |
| EC Declaration of Conformity | 82 |
| European Community Directives Requirement (CE) | 82 |

APPENDIX: OPTIONAL ETHERNET TAP INSTALLATION83

Preliminary Setup Procedures..... 83

 Unpack the Ethernet Tap Unit from the Box83

 Other Required Installation Items83

Install the Ethernet Tap Unit. 84

INDEX87

THREAT ANALYSIS REPORTER INTRODUCTION

Thank you for choosing to install the M86 Security Threat Analysis Reporter. This product addresses user-generated Web threats such as excessive use of bandwidth and inappropriate Internet usage, and provides network administrators tools to monitor such threats so management can enforce corporate Internet usage policies.

Working in conjunction with M86 Security's Web Filter, the Threat Analysis Reporter translates end user Internet activity from the Web Filter's logs into dynamic graphical snapshots of network Internet traffic. Using remediation tools in the console, administrators and management can then manage and control user-generated Web threats in real time.

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

Quick setup procedures—to implement the best usage practices for the Threat Analysis Reporter—are included in the Best Usage Practices section that follows the Conclusion of this guide.

About this Document

This document is divided into the following sections:

- **Introduction** - This section is comprised of an overview of the Threat Analysis Reporter 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 Threat Analysis Reporter in your network environment
- **Install the Server** - This section explains how to configure the Threat Analysis Reporter
- **Conclusion** - This section indicates that the installation steps have been completed
- **Best Usage Practices** - This section includes scenarios and instructions for implementing the best practices when using the Threat Analysis Reporter
- **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 TAR models referenced in this document
- **Appendix: Optional Ethernet Tap Installation** - This appendix explains how to install the optional Ethernet Tap device on your network for bandwidth monitoring
- **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 Threat Analysis Reporter User Guide. This icon is found in the Best 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.

M86 Security Corporate Headquarters (USA)

Local : 714.282.6111
Domestic US : 1.888.786.7999
International : +1.714.282.6111

M86 Security Taiwan

Taipei Local : 2397-0300
Domestic Taiwan : 02-2397-0300
International : 886-2-2397-0300

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 Threat Analysis Reporter unit
- 1 AC Power Cord, 2 AC Power Cords for HL servers
- 1 Serial Port Cable
- 1 CAT-5E Crossover Cable
- Rack Mount Brackets (2)
- 1 End User License Agreement (EULA)
- 1 CD-ROM containing supplemental product applications and EULA

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



NOTES: Threat Analysis Reporter servers come with a NetOptics 10/100 BaseT Ethernet Tap kit to be installed at your option. For HL and SL servers, 1 bezel to be installed on the front of the chassis also is included, as well as 1 spare parts kit. For HL servers, this kit contains a hard drive and power supply. For SL servers, this kit contains a hard drive. Please refer to the appendix of the user guide for information on replacing a hard drive or power supply.

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



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

Select a Site for the Server

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

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

Rack Mount the Server

Rack Setup Precautions

**WARNING:**

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

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

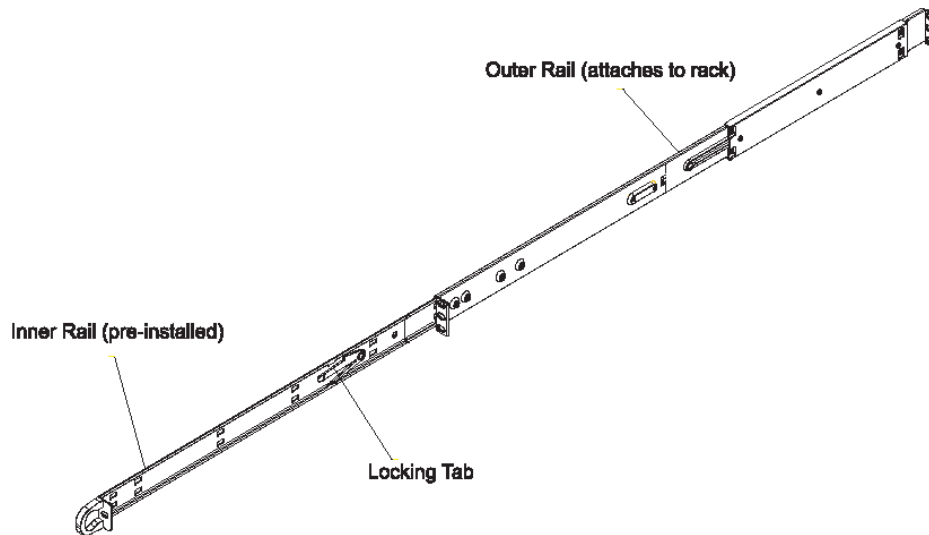
Rack Mount Instructions for HL Servers

Rack Setup Suggestions

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

Identify the Sections of the Rack Rails

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



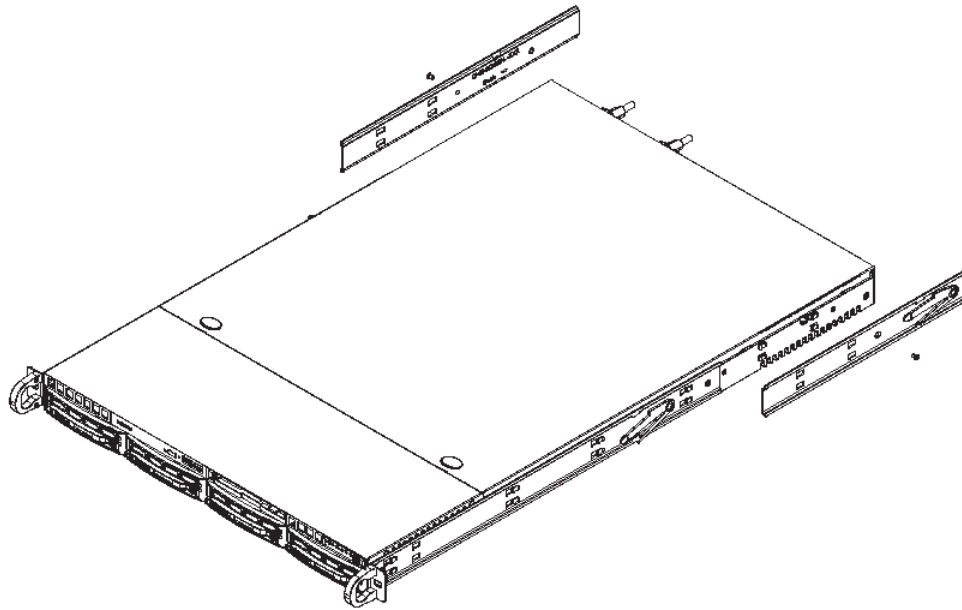
Install the Inner Rails

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

Install the Outer Rails

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

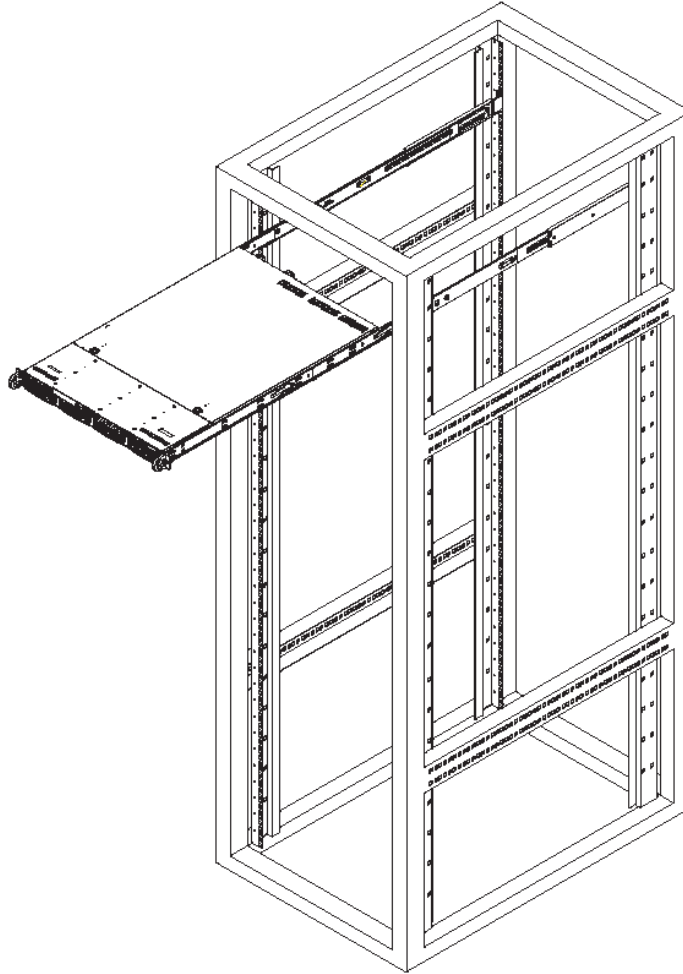
Locking Tabs: Both chassis rails have a locking tab, which serves two functions. The first is to lock the server into place when installed and pushed fully into the rack, which is its normal position. Secondly, these tabs also lock the server in place when fully extended from the rack. This prevents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



Install the Server into the Rack

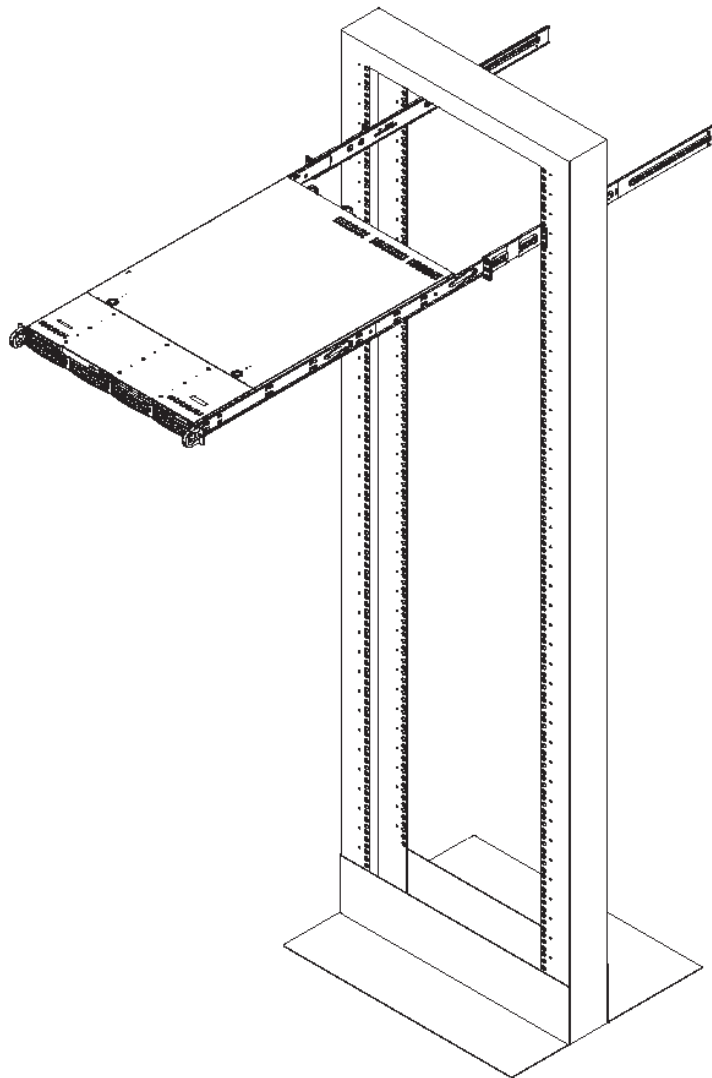
You should now have rails attached to both the chassis and the rack unit. The next step is to install the server chassis into the rack. Do this by lining up the rear of the chassis rails with the front of the rack rails. Slide the chassis rails into the rack rails, keeping the pressure even on both sides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

When the server has been pushed completely into the rack, you should hear the locking tabs “click.”



Install the Server into a Telco Rack

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



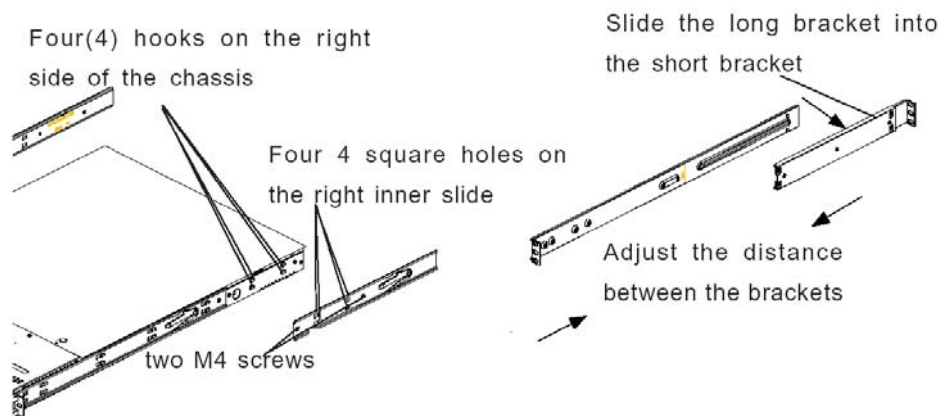
Rack Mount Instructions for SL Servers

Rack Setup Suggestions

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

Install the Inner Slides

1. Locate the right inner slide, (the slide that will be used on the right side of chassis when facing the front panel of the chassis).
2. Align the four (4) square holes on the right inner slide against the hooks on the right side of the chassis as show below on the left.
3. Securely attach the slide to the chassis with two M4 flat head screws and repeat the steps 1-3 to install the left inner slide to the left side of the chassis.

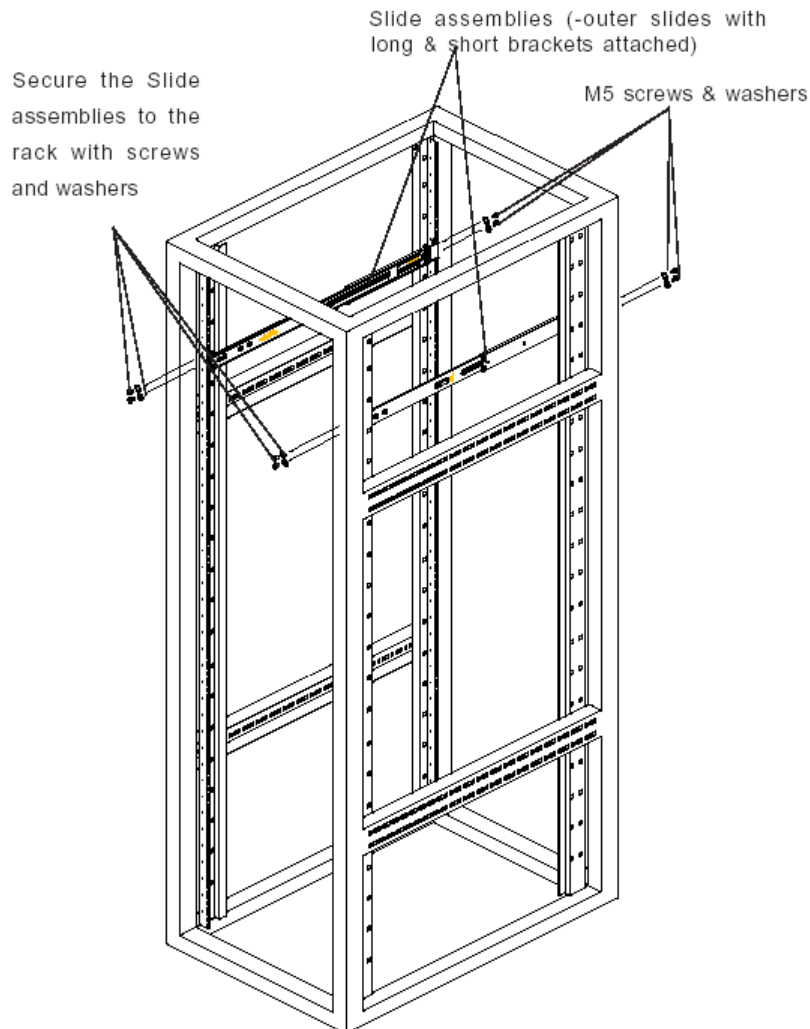


Install the Outer Slides

1. Measure the distance from the front rail of the rack to the rear rail of the rack.
2. Attach a short bracket to the rear side of the right outer slide, and a long bracket to the front side of the right outer slide as shown above on the right.
3. Adjust the short and long brackets to the proper distance so that the chassis can snugly fit into the rack.
4. Secure the slides to the cabinet with screws.
5. Repeat steps 1-4 for the left outer slide.

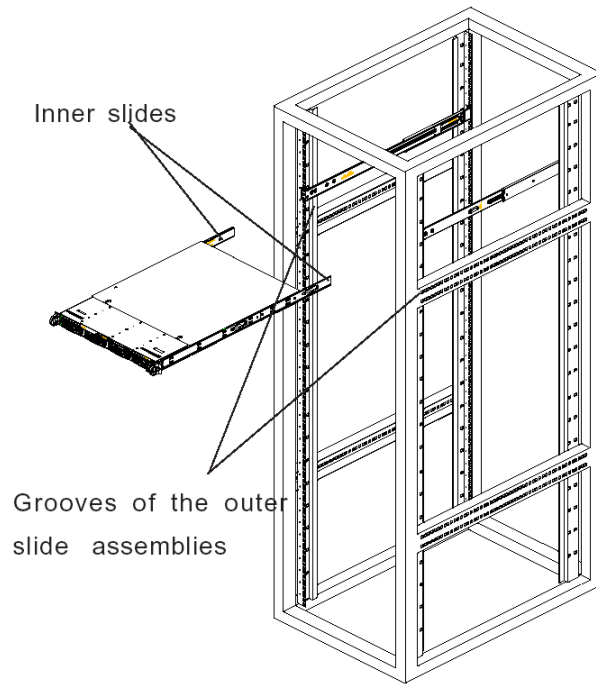
Install the Slide Assemblies to the Rack

1. After you have installed the short and long brackets to the outer slides, you are ready to install the whole slide assemblies (outer slides with short and long brackets attached) to the rack. (See the previous page.)
2. Use M5 screws and washers to secure the slide assemblies into the rack as shown below:

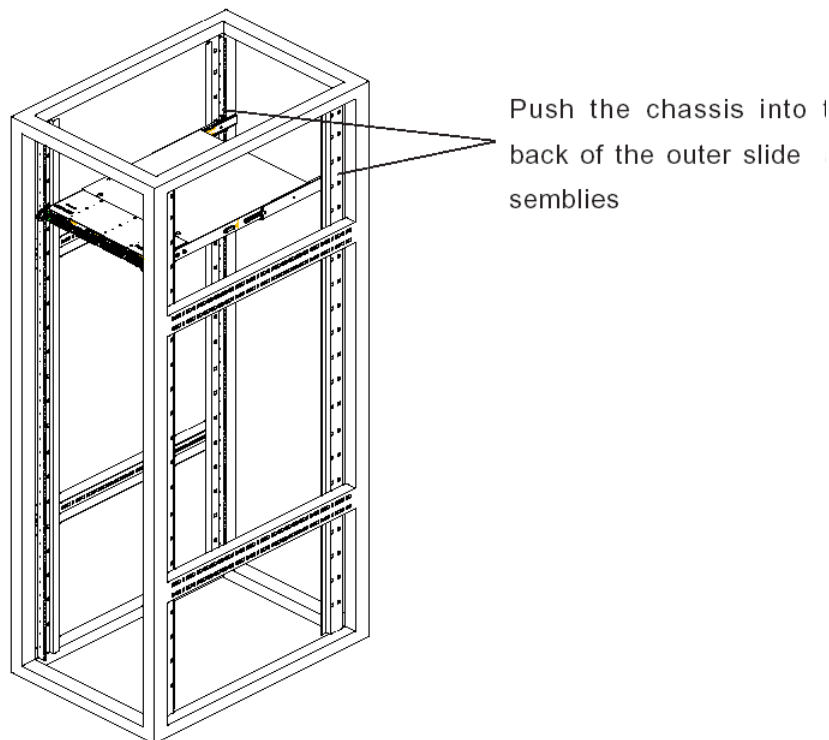


Install the Chassis into the Rack

1. Push the inner slides, which are attached to the chassis, into the grooves of the outer slide assemblies that are installed in the rack as shown below:





2. Push the chassis all the way to the back of the outer slide assemblies as shown below:



Rack Mount Instructions for MSA Servers

Optional: Install the Chassis Rails


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

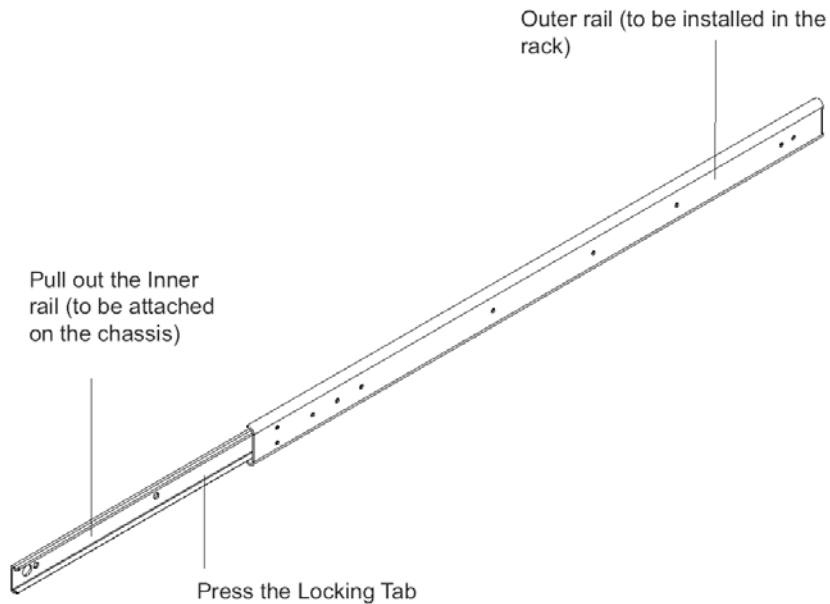
 **CAUTION:** Please make sure that the chassis covers and chassis rails are installed on the chassis before you install the chassis into the rack. To avoid personal injury and property damage, please carefully follow all the safety steps listed below:

Before installing the chassis rails:

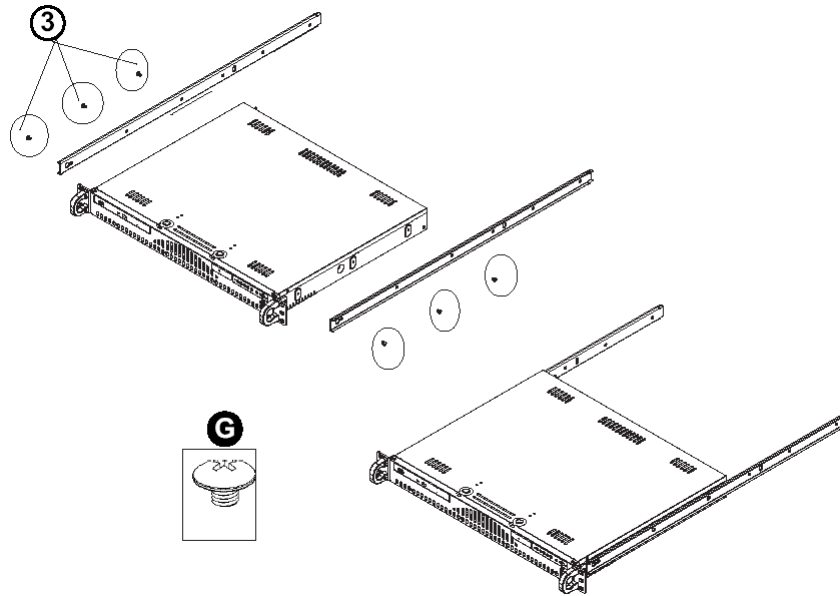
- Close the chassis using the chassis cover.
- Unplug the AC power cord(s).
- Remove all external devices and connectors.

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

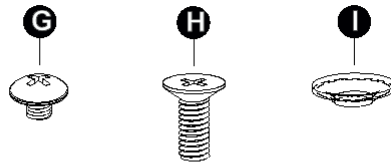
 **NOTE:** The inner rails are to be attached to the chassis and the outer rails are to be installed in the rack.



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.

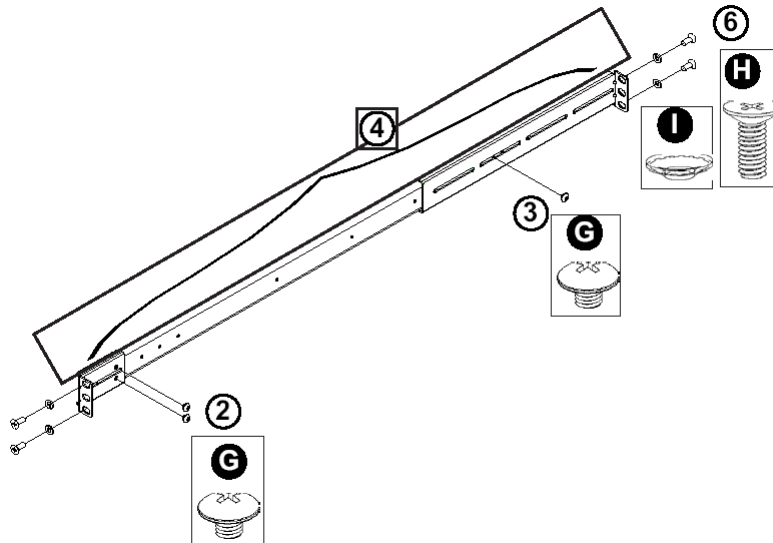
Optional: Install the Traditional UP Racks

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.)

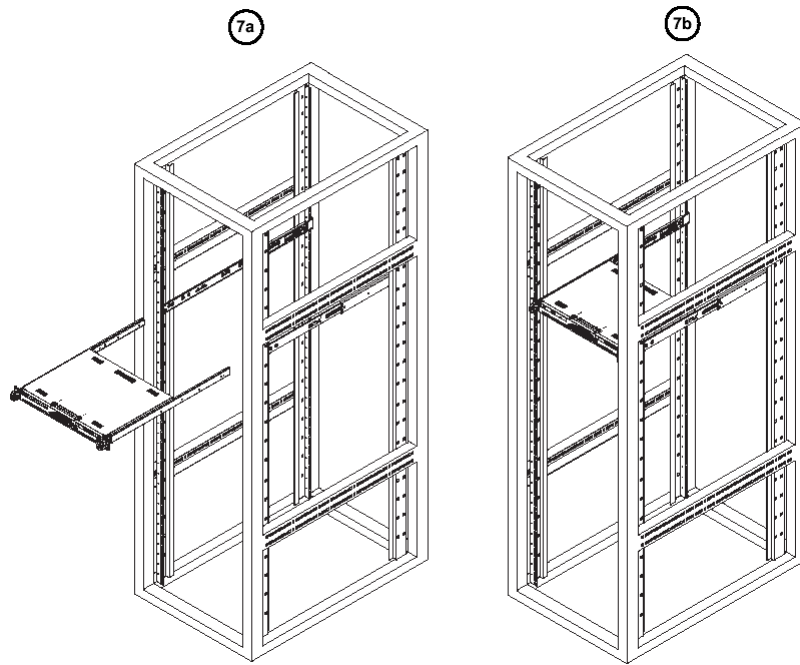


7. Slide the chassis into the rack as shown below.



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.



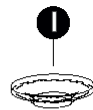
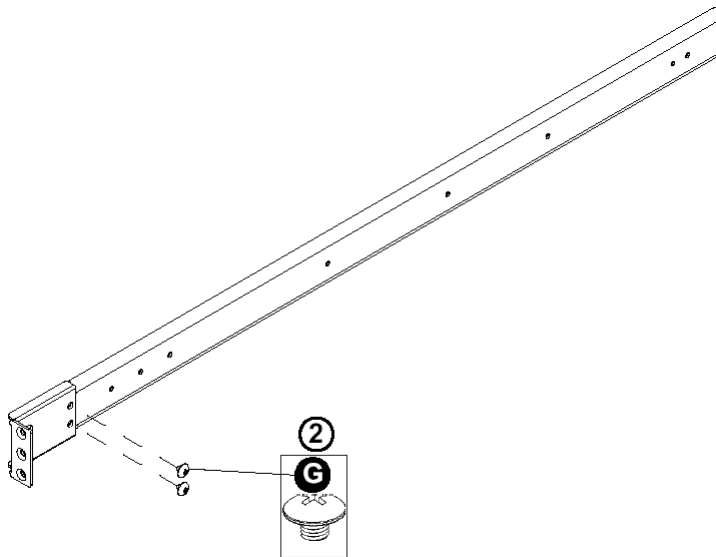
Optional: Install the Open Racks

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



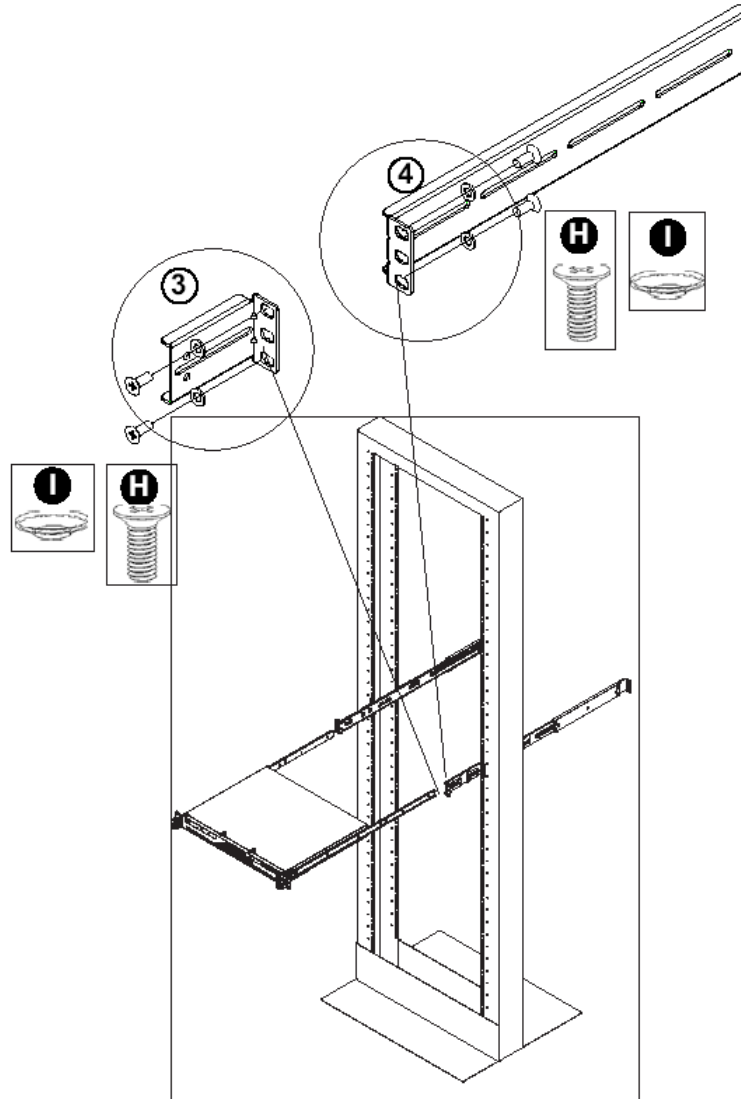
NOTE: The rails are designed to fit in the racks with the depth of 28" to 33".

- 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.



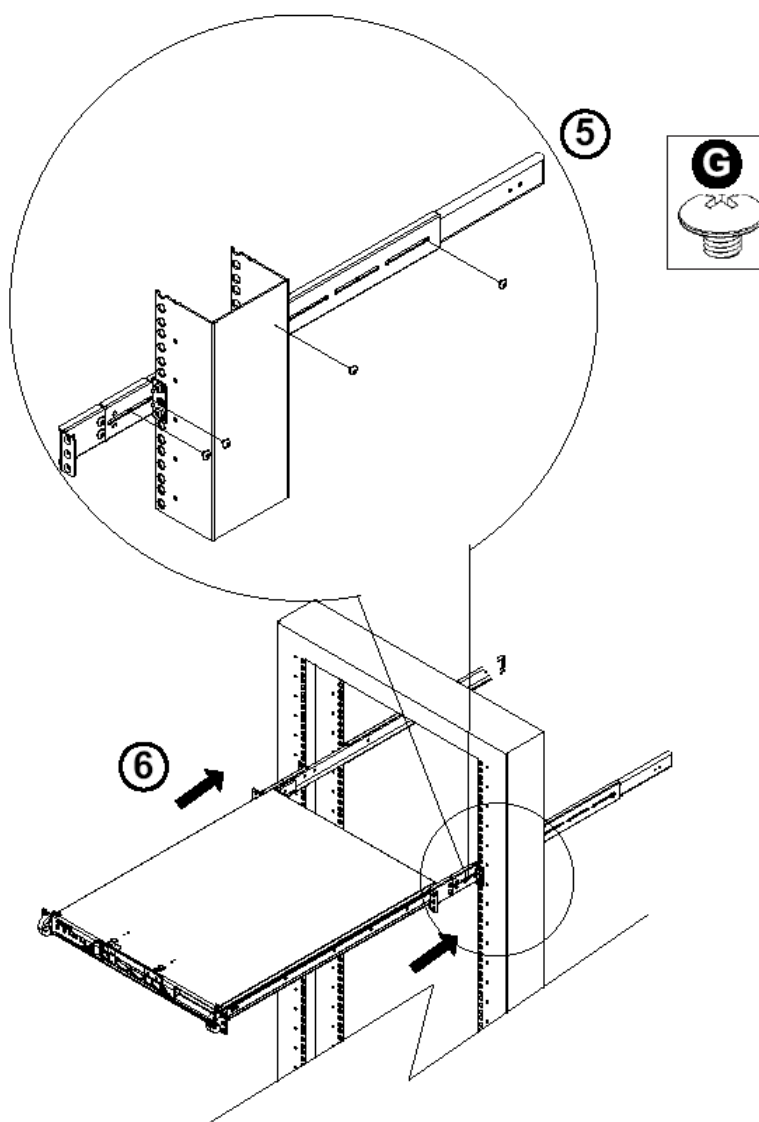
- G. Round head M4 x 4 mm [0.157]
H. Flat head M5 x 12 mm [0.472]
I. Washer for M5

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.

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



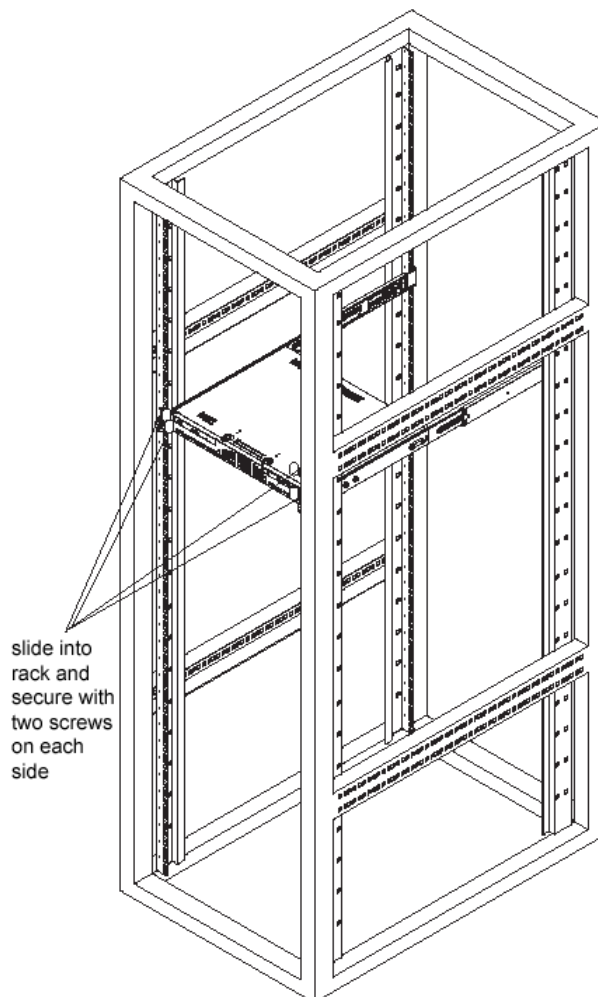
Install the Chassis into the Rack



CAUTION: Before installing the chassis into the rack:


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

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



Install the SL or HL Server Bezel

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

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

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



Fig. 1 - Front of bezel

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



Fig. 2 - Bumps on right end of bezel



Fig. 3 - Grooves in right U-shaped handle

- C. Align these bumps along the two parallel grooves inside each U-shaped aluminum chassis handle affixed to the front end of the chassis rail (Fig. 3).
- D. Push the bezel towards the front of the chassis, inserting the USB B-type plug on the back of the bezel (Fig. 4) into the USB port on the chassis.



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

Check the Power Supply

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

Power Supply Precautions



WARNING:

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

General Safety Information

Server Operation and Maintenance Precautions

**WARNING:**

Observe the following safety precautions during server operation and maintenance:



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



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



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



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



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

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

AC Power Cord and Cable Precautions

**WARNING:**

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

Electrical Safety Precautions

**WARNING:**

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



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

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

Motherboard Battery Precautions

**CAUTION:**

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

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

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

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

ATTENTION: IL Y A DANGER D'EXPLOSION S'IL Y A 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: Initial Setup Procedures

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



NOTE: Before installing the Threat Analysis Reporter server, the Web Filter server to be used with this server must already be installed and running software version 4.0.00 or higher.

Quick Start Setup Requirements

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



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

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

LCD Panel Setup Requirements (for SL and HL Units)

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

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

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

Step 1A: Quick Start Setup Procedures

Link the Workstation to the Threat Analysis Reporter

Monitor and Keyboard Setup

- A. Connect the PC monitor and keyboard cables to the rear of the chassis (see Fig. 1 for an SL or MSA unit, and Fig. 2 for an HL unit).
- B. Turn on the PC monitor.
- C. Connect the AC power cord(s) to the back of the chassis and plug the cord(s) into a UPS power supply unit.
- D. Power on the Threat Analysis Reporter by dropping down the face plate and pressing the large button at the right of the front panel (see Fig. 3 for an SL unit, Fig. 4 for an MSA unit, and Fig. 5 for an HL unit).

Once the Threat Analysis Reporter is powered up, proceed to the Quick Start menu instructions.

Serial Console Setup

- A. Using the serial port cable (and USB DB9 serial adapter, if necessary), connect the laptop to the rear of the chassis (see Fig. 1 for an SL or MSA unit, and Fig. 2 for an HL unit).
- B. Power on the laptop.
- C. Connect the AC power cord(s) to the back of the chassis and plug the cord(s) into a UPS power supply unit.
- D. Power on the Threat Analysis Reporter by pressing the large button at the right of the front panel (see Fig. 3 for an SL unit, Fig. 4 for an MSA unit, and Fig. 5 for an HL unit).



Fig. 1 - Portion of SL and MSA chassis rear



Fig. 2 - Portion of HL chassis rear

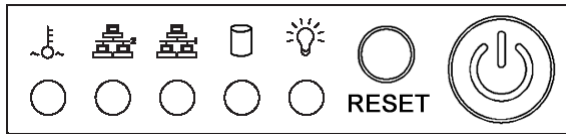


Fig. 3 - Diagram of SL chassis front panel, power button at far right

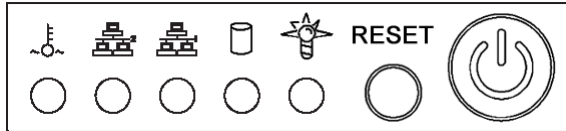


Fig. 4 - Diagram of MSA chassis front panel, power button at far right

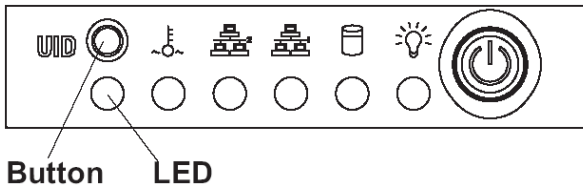


Fig. 5 - Diagram of HL chassis front panel, power button at far right

Once the Threat Analysis Reporter 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 February 10, 2010), Microsoft states: "HyperTerminal is no longer part of Windows.... If you previously used HyperTerminal to control serial devices, you can usually find a downloadable version of HyperTerminal on the Internet that is free for personal use."*

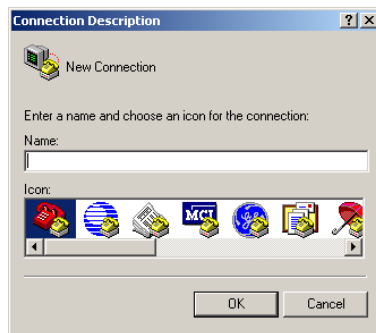
If you are using a Windows Vista or Windows 7 machine to conduct these quick start setup procedures and do not have an equivalent type of terminal emulator program installed on your workstation, Hilgraeve, Inc., the maker of HyperTerminal, offers HyperTerminal Private Edition for Windows Vista and Windows 7. The following information is included on Hilgraeve's Web page at <http://www.hilgraeve.com/hyperterminal.html> (accessed February 10, 2010): "HyperTerminal Private Edition is a terminal emulation program that supports communications over TCP/IP networks, Dial-Up Modems, and serial COM ports.... Please enter your email address below to download the free 30 day trial." Instructions are provided for installing this application on your workstation.

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:

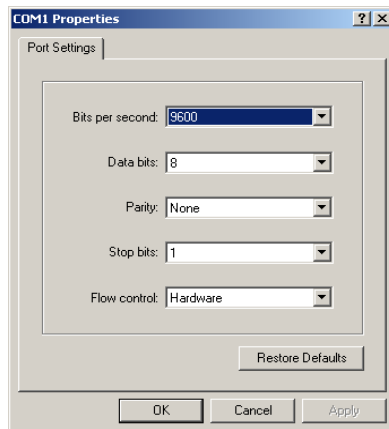
- A. Launch HyperTerminal by going to Start > Programs > Accessories > Communications > HyperTerminal:



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



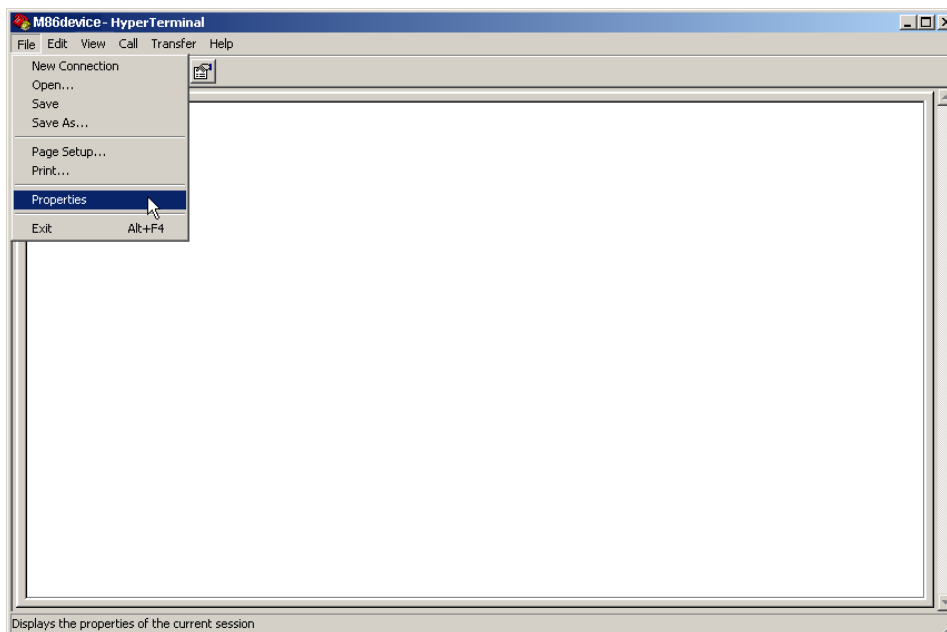
- C. At the **Connect using** field, select the COM port assigned to the serial port on the laptop (probably “COM1”), and then click **OK** to open the Properties dialog box, displaying the Port Settings tab:



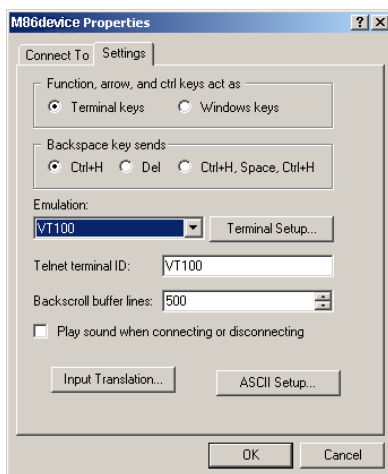
- D. Specify the following session settings:

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

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.



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

Quick Start menu instructions

For these Quick Start setup procedures, you will need your network administrator to provide you the LAN 1 and LAN 2 IP address and subnet mask, gateway IP address, DNS server IP address(es), host name of the server, and IP address for the Web interface (if using a NAT device).

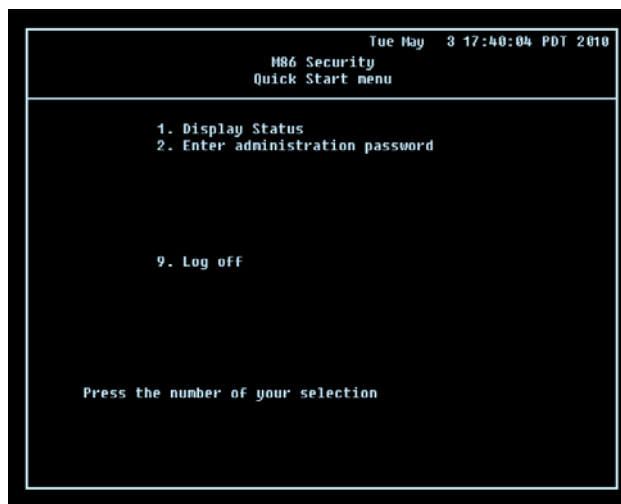
Login screen, password prompts

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



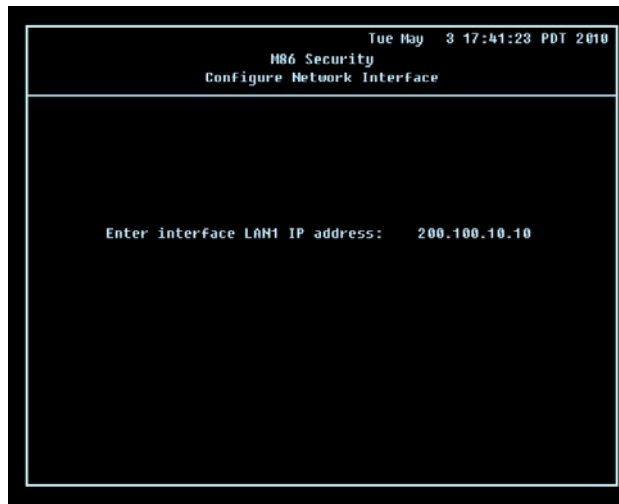
NOTE: If the screensaver currently displays on your screen, press the **Enter** key to display the login screen.

- 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:



- E. At the **Press the number of your selection** prompt, press **2** to display the Administrator Password Entry screen.
- F. At the **Enter the administrator password** prompt, re-enter your password: **#s3tup#r3k**
- G. Press **Enter** to display the Administration menu where you can begin the Quick Start setup process using the configuration screens.
- H. At the **Press the number of your selection** prompt, press **2** to select the "Quick Start setup" process. This process takes you to the Configure Network Interface screen.

Configure Network Interface screen



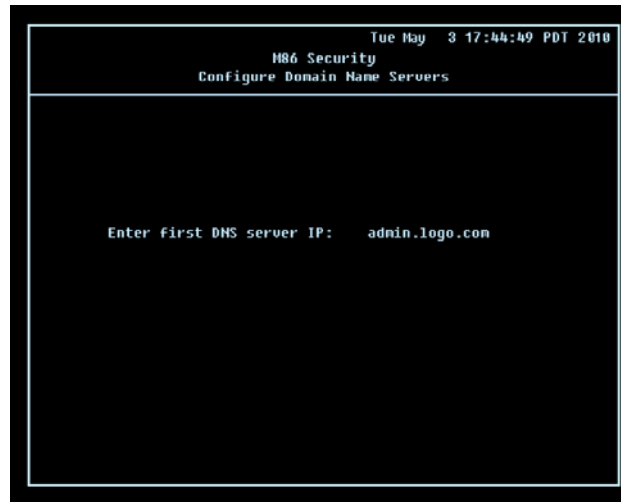
- A. At the **Enter interface lan1 IP address** field, enter the IP address for the LAN 1 interface, and then press **Enter** to go to the next screen.
- B. At the **Enter interface lan1 netmask** field, enter the subnet mask for the LAN 1 interface using the dotted decimals notation format. Press **Enter** to display the confirmation prompt.
- C. Press **Y** for “Yes” to confirm and save your entries for the LAN1 interface, and to go to the next screen.
- D. At the **Enter interface lan2 IP address** field, enter the IP address for the LAN 2 interface, and then press **Enter** to go to the next screen.
- E. At the **Enter interface lan2 netmask** field, using the dotted decimals notation format, enter the subnet mask for the LAN 2 interface. Press **Enter** to display the confirmation prompt.
- F. Press **Y** for “Yes” to confirm and save your entries for the LAN 2 interface, and to go to the Configure default gateway screen.

Configure default gateway screen



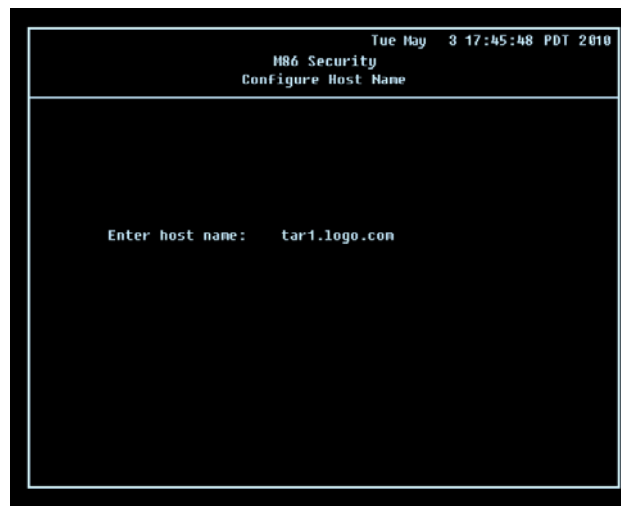
- A. At the **Enter default gateway IP** field, enter the IP address for the default gateway. Press **Enter** to display the confirmation prompt.
- B. Press **Y** for “Yes” to confirm and save your entry for the gateway IP address, and to go to the Configure Domain Name Servers screen.

Configure Domain Name Servers screen



- A. At the **Enter first DNS server IP** field, enter the IP address for the primary Domain Name Server. Press **Enter** to go to the next screen.
- B. At the **Enter (optional) second DNS server IP** field, if you have a secondary Domain Name Server you wish to use, enter the IP address for that server. Press **Enter** to display the confirmation prompt.
- C. Press **Y** for “Yes” to confirm and save your entries for the domain name servers, and to go to the Configure Host Name screen.

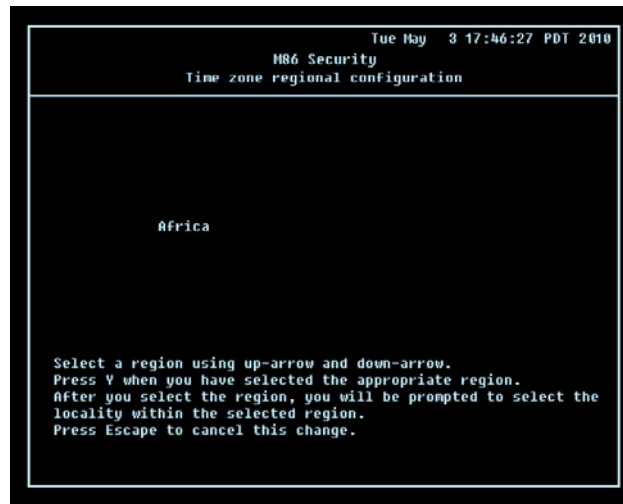
Configure Host Name screen



- A. At the **Enter host name** field, enter the host name of the server. Press **Enter** to display the confirmation prompt.

- B. Press **Y** for “Yes” to confirm and save your entry for the host name, and to go to the Time zone regional configuration screen.

Time zone regional configuration screen



- A. Use the up and down arrows in your keyboard to select your region. After selecting your locality, press **Y** for “Yes” to confirm and save your regional selection, and to go to the next screen:
- B. Use the up and down arrows in your keyboard to select your region. After selecting your locality, press **Y** for “Yes” to confirm and save your regional selection, and to go to the Configure Wizard user screen.

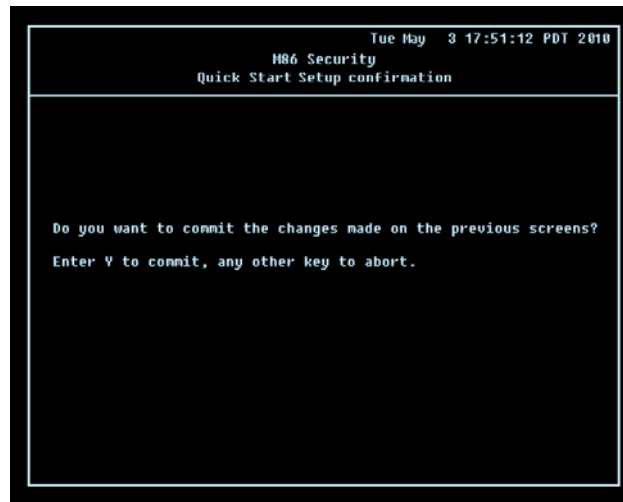
Configure Wizard user screen



- A. At the **Enter wizard user name** field, enter the username that will be used to access the setup wizard in the Threat Analysis Reporter interface. Press **Enter** to display the confirmation prompt.
- B. Press **Y** for “Yes” to confirm and save your entry and to go to the next screen.

- C. At the **Enter wizard password** field, enter the password that will be used to access the setup wizard in the Threat Analysis Reporter interface. Press **Y** for “Yes” to confirm and save your entry and to go to the Quick Start Setup confirmation screen.

Quick Start Setup confirmation screen



Press **Y** for “Yes” to save all your Quick Start setup entries and to return to the Administration menu.



NOTE: When saving your entries, there may be a 4-10 second delay before the Administration menu displays.

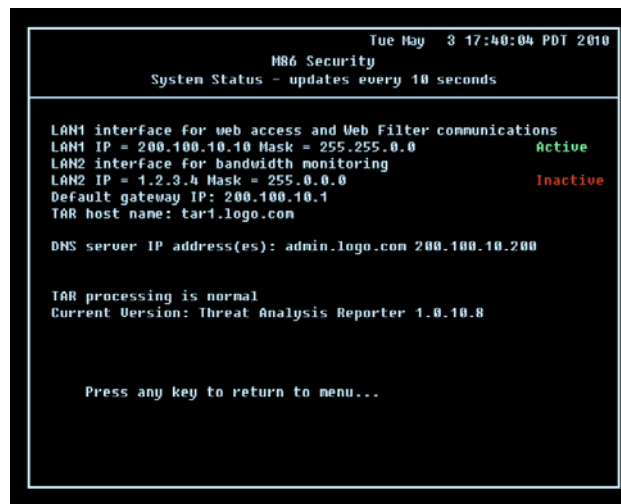
Administration menu

After making all entries using the Quick Start setup process, you will return to the Administration menu. Press **X** to return to the Quick Start menu screen. Or, to verify the status of the Threat Analysis Reporter and review the entries you made using the Quick Start setup process, press **1** to view the System Status screen.



NOTE: Changing your password using option C, “Change Quick Start password”, will change the password for the console menu but not the Threat Analysis Reporter console login screen.

System Status screen



```

Tue May  3 17:40:04 PDT 2010
M86 Security
System Status - updates every 10 seconds

LAN1 interface for web access and Web Filter communications
LAN1 IP = 200.100.10.10 Mask = 255.255.0.0      Active
LAN2 interface for bandwidth monitoring
LAN2 IP = 1.2.3.4 Mask = 255.0.0.0           Inactive
Default gateway IP: 200.100.10.1
TAR host name: tar1.logo.com

DNS server IP address(es): admin.logo.com 200.100.10.200

TAR processing is normal
Current Version: Threat Analysis Reporter 1.0.10.8

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

The System Status screen contains the following information:

- **lan1 interface for web access and Web Filter communications:** LAN1 IP address and **netmask** specified in screen 3 (Configure Network Interface), and current status (“Active” or “Inactive”)
- **lan2 interface for bandwidth monitoring:** LAN2 IP address and **netmask** specified in screen 4 (Configure Network Interface), and current status (“Active” or “Inactive”)
- **Default gateway IP** address specified in screen 5 (Configure default gateway)
- **Configure host name** specified in screen 7 (Configure Host Name)
- **DNS server IP address(es)** specified in screen 6 (Configure Domain Name Servers)
- Current status of the Threat Analysis Reporter
- Current Version of the Threat Analysis Reporter software



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

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 Threat Analysis Reporter.
- Proceed to Step 2: Physically Connect the Unit to the Network.

Step 1B: LCD Panel Setup Procedures

- A. Connect the AC power cord(s) to the back of the chassis and plug the cord(s) into a UPS power supply unit.
- B. Power on the server by dropping down the face plate and pressing the large button at the right of the front panel.

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

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

LCD Menu

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



NOTE: On the LCD Menu, press "X" to toggle the display between the main menu and the following information: "Threat Analysis Reporter (software version number)" and "Data-base Status (Active, Inactive)".

Main Menu

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

- Current Patch Level
- IP / LAN1 > *
- IP / LAN2 > *
- Gateway *
- DNS 1 > *
- DNS 2 > *
- Host Name > *
- Regional Setting (Time Zone, date, time) *
- Admin Console Wizard User *
- Reboot >
- Shutdown >



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



TIPS: Navigation tips in the main menu:

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

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

IP / LAN1 and LAN2

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

- Configure LAN 1 (2) IP
 - Change LAN1 (2) Netmask
- A. Choose **Configure LAN 1 (2) IP** and press the checkmark key to go to the Configure LAN 1 (2) IP screen.
 - B. Use the up / down keys to increase / decrease the current value, and the left / right arrow keys to navigate across the line.
 - C. Press the checkmark key to accept your entry and to return to the previous screen.
 - D. Choose **Change LAN1 (2) Netmask** and press the checkmark key to go to the Change LAN1 (2) Netmask screen.
 - E. Use the up / down keys to increase / decrease the current value, and the left / right arrow keys to navigate across the line.
 - F. Press the checkmark key to accept your entry and to return to the previous screen.
 - G. Press the “X” key to return to the main menu.

Gateway

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

- A. Choose **Configure Gateway IP** and press the checkmark key to go to the Configure Gateway IP screen.
- B. Use the up / down keys to increase / decrease the current value, and the left / right arrow keys to navigate across the line.
- C. Press the checkmark key to accept your entry and to return to the previous screen.
- D. Press the “X” key to return to the main menu.

DNS 1 and 2

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

- A. Choose **Configure DNS IP 1 (2)** and press the checkmark key to go to the Configure DNS IP 1 (2) screen.
- B. Use the up / down keys to increase / decrease the current value, and the left / right arrow keys to navigate across the line.
- C. Press the checkmark key to accept your entry and to return to the previous screen.
- D. Press the “X” key to return to the main menu.

Host Name

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

- A. Choose **Configure Hostname** and press the checkmark key to go to the Configure Hostname screen.
- B. Use the arrow keys to navigate the menu. Press the right arrow key to view the alphabets in first uppercase and then lowercase, numbers from 0-9, and lastly the symbol characters.



NOTE: Navigation tips:

- If the down arrow key is pressed first—instead of the right arrow key—the symbol characters display first.
 - Press the “X” key to remove a character and move the cursor to the first position in the line.
- C. Press the checkmark key to return to the previous screen.
 - D. Press the “X” key to return to the main menu.

Regional Setting (Time Zone, date, time)

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

- A. Choose **Region**, and use the left / right arrow keys to view the available region selections.
- B. After making a selection, press the checkmark key to display the Choose a Location screen.
- C. Choose **Location**, and use the left / right arrow keys to view the available location selections.
- D. After making a selection, press the checkmark key to display the Save Changes? screen:
 - Choose **Yes** to save your changes and to return to the main menu.
 - Choose **No** to return to the previous screen.

Admin Console Wizard User

When the Admin Console Wizard User option is selected, the Admin Console Wizard User screen displays with two menu selections:

- Choose **Reset TAR setup wizard username** to reset the username and to return to the main menu.
- Choose **Reset TAR setup wizard password** to reset the password and to return to the main menu.

Non-Quick Start procedures or settings

Current Patch Level

When the Current Patch Level option is selected, “Threat Analysis Reporter” and the version number of the currently installed build displays.

Reboot

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

A. Choose one of two options:

- **Yes, reboot now!!!** - This selection reboots the Threat Analysis Reporter.
- **No, cancel reboot** - This selection returns you to the previous screen.

B. Press the “X” key to return to the main menu.

Shutdown

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

A. Choose one of two options:

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

B. Press the “X” key to return to the main menu.

LCD Options menu

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

- Heartbeat
- Backlight
- LCD Controls >

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

Heartbeat

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

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

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

- B. After making your selection, press the “X” key to return to the previous screen.

Backlight

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

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

LCD Controls

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

- A. Choose one of the menu selections and press the checkmark key to go to that screen:
- **Contrast** - In the Contrast screen, use the left / right arrow keys to decrease / increase the text and screen contrast.
 - **On Brightness** - In the On Brightness screen, use the left / right arrow keys to decrease / increase the brightness of a screen with a feature that is enabled.
 - **Off Brightness** - In the Off Brightness screen, use the left / right arrow keys to decrease / increase the brightness of a screen with a feature that is disabled.
- B. After making your selection, press the “X” key to return to the previous screen.
- C. Proceed to Step 2: Physically Connect the Unit to the Network.

Step 2: Physically Connect the Unit to the Network

After performing initial setup procedures for the Threat Analysis Reporter, the unit needs to be physically connected to the network. This step requires a standard CAT-5E cable to connect the unit to the network. An additional CAT-5E cable is required if the Ethernet Tap unit will be installed for bandwidth monitoring.

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



Fig. 1 - Portion of SL and MSA chassis rear

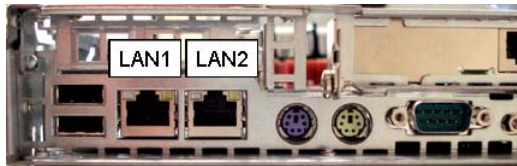


Fig. 2 - Portion of HL chassis rear

- B. Plug the other end of the CAT-5E cable into an open port on the network switch.
- C. Reboot the server by using the Reboot system option (as described in Step 1A: Quick Start Setup Procedures), or by using the Reboot option on the LCD panel (as described in Step 1B: LCD Panel Setup Procedures).
- D. Proceed to Bandwidth Management or Step 3.

Bandwidth Management

If you choose to install the Ethernet Tap for bandwidth monitoring, you will need to connect it to the Threat Analysis Reporter at this point. Refer to Appendix A at the end of this document for instructions on how to connect the Ethernet Tap unit.

Step 3: Register TAR and its Applications

Next you will register the Threat Analysis Reporter and its applications online. For this step you will need your network administrator to provide you the IP range and netmask of machines on the network the Threat Analysis Reporter application will use for monitoring bandwidth on your network.

Access TAR via its LAN 1 IP Address

A. Launch an Internet supported browser:

- Firefox 3.5
- Internet Explorer 7 or 8
- Safari 4.0

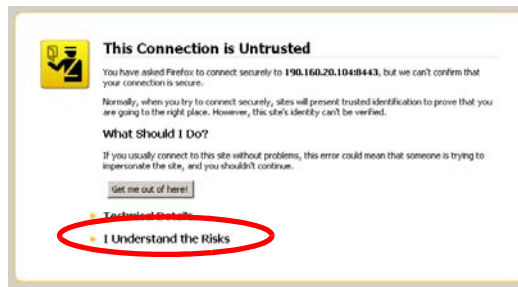
B. In the address field, type in the LAN 1 IP address you assigned to the Threat Analysis Reporter unit in Step 1A (Configure Network Interface screen) or Step 1B (IP / LAN1 and 2). Be sure to use “https” and port **:8443** for a secure connection, appended by “/8e6tar”. For example, if the Threat Analysis Reporter server was assigned an IP address of 10.10.10.10, you would enter **https://10.10.10.10:8443/8e6tar/** in the browser’s address field.

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

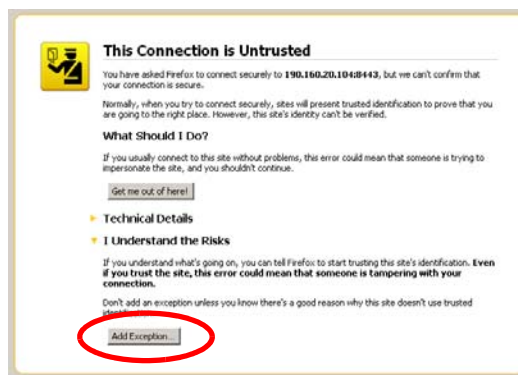
- If using Firefox, proceed to Accept the Security Certificate in Firefox.
- If using IE, proceed to Temporarily Accept the Security Certificate in IE.
- If using Safari, proceed to Accept the Security Certificate in Safari.
- If the security issue page does not display in your browser, verify the following:
 - The Threat Analysis Reporter appliance is powered on.
 - Can the administrator workstation normally connect to the Internet?
 - Is the administrator workstation able to ping the Threat Analysis Reporter’s LAN 1 IP address? (To ping the Threat Analysis Reporter using the Command Prompt in Windows XP, Vista, and 7, go to **Start > All Programs > Accessories > Command Prompt**, type in **Ping** and the IP address using the x.x.x.x format—in which each ‘x’ represents an octet—and then press **Enter**.)
 - If pinging the IP address of the Threat Analysis Reporter is unsuccessful, try restarting the network service or rebooting the server.
 - If still unsuccessful, contact an M86 Security solutions engineer or technical support representative.

Accept the Security Certificate in Firefox

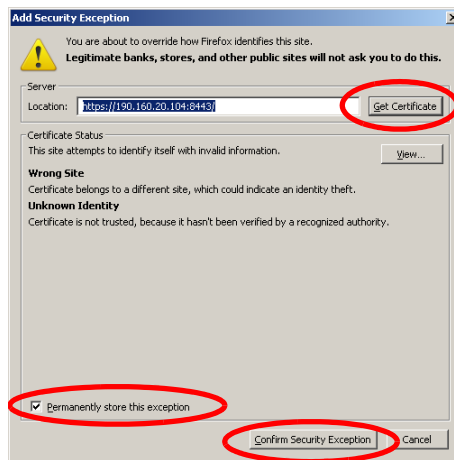
- A. If using a Firefox browser, in the page “This Connection is Untrusted,” click the option **I Understand the Risks**:



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



Clicking Add Exception opens the Add Security Exception window:

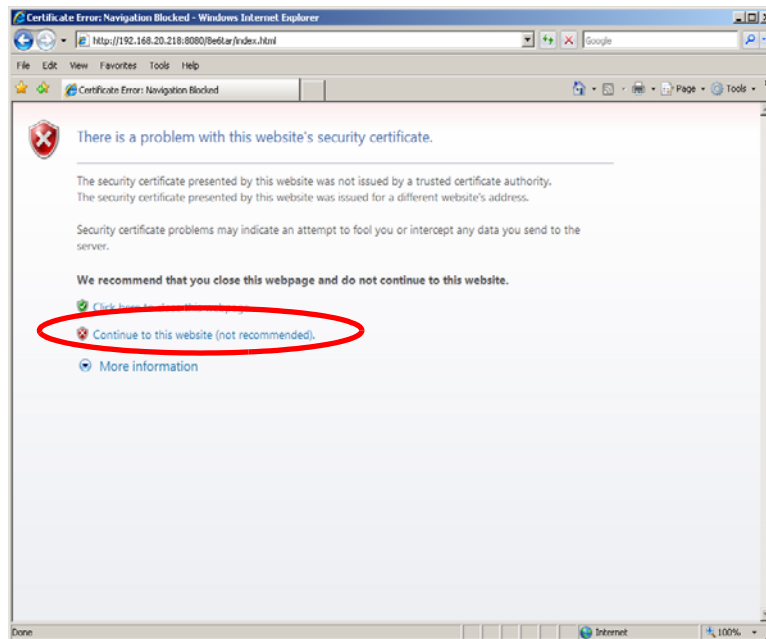


- C. In the Add Security Exception window, click **Get Certificate** and wait a few seconds until the security certificate is obtained by the server.
- D. With the checkbox **Permanently store this exception** selected, click **Confirm Security Exception**.

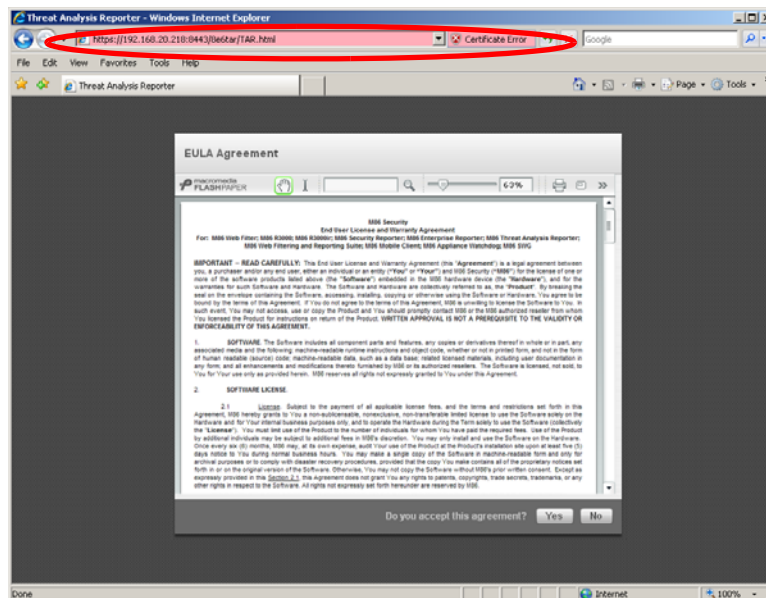
Proceed to Accept the End User License Agreement.

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 Threat Analysis Reporter page's address field and Certificate Error button to the right of the field shaded a reddish color:



Proceed to Accept the End User License Agreement.

Accept the Security Certificate in Safari

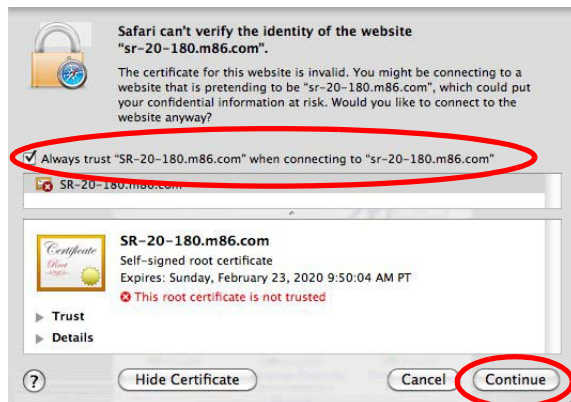
- A. If using a Safari browser, the pop-up window "Safari can't verify the identity of the website..." opens:



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



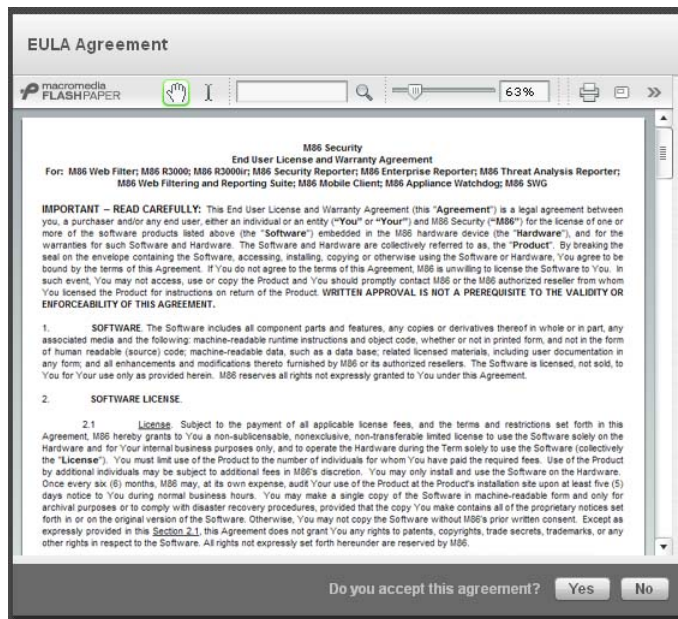
- B. Click the "Always trust..." checkbox and then click **Continue**:



- C. You will be prompted to enter your password in order to install the certificate.
After the security certificate is installed, proceed to Accept the End User License Agreement.

Accept the End User License Agreement

- A. Read the contents of the EULA Agreement dialog:



- B. Click **Yes** to accept the EULA, close the EULA Agreement dialog box, and display the Threat Analysis Reporter Wizard Login window.

Proceed to Log in to the Threat Analysis Reporter Wizard.

Log in to the Threat Analysis Reporter Wizard

- A. In the **Username** field of the Login window, type in the username specified in the Configure Wizard user screen of the Quick Start Setup Procedures (Step 1A), or the Admin Console Wizard User screen in LCD Panel Setup Procedures (Step 1B):



- B. In the **Password** field, type in the password specified in the Configure Wizard user screen of the Quick Start Setup Procedures (Step 1A), or the Admin Console Wizard User screen in LCD Panel Setup Procedures (Step 1B).
- C. Click **Login** to close the login window and to go to the Threat Analysis Reporter wizard screen.

Use the TAR Wizard to Specify Application Settings

Threat Analysis Reporter M86 SECURITY

All fields are required except for ER. A "Source" Web Filter and at least one bandwidth range is required.

Main Administrator
 Register the first administrator for the TAR box. Please make sure you use only alpha-numeric characters.

Username: Email:
 Password: Confirm Password:

Bandwidth Range
 The following IP ranges will be used to monitor the network traffic in your organization.

IP Address: Subnet Mask:

| IP Address | Subnet Mask |
|------------|-------------|
| | |
| | |
| | |
| | |

Web Filter Setup
 These settings are used for communication with TAR agent to retrieve the data logs from Web Filter.

Server Name: Server IP:
☐ Set as Source

| Source | Server Name | Server IP |
|--------|-------------|-----------|
| | | |
| | | |
| | | |
| | | |

Enterprise Reporter
 Do you have an Enterprise Reporter?
☐ Yes ☒ No

Server Name: Server IP:


Click "Save" to finish setting up your TAR >>>

Enter Main Administrator Criteria

- Enter the **Username** the global administrator will use when logging into the Threat Analysis Reporter Administrator console. The global administrator has the highest level of permissions in the Threat Analysis Reporter.
- Enter the **Email** address of the global administrator, who will be notified via email regarding system alerts.
- Enter the **Password** to be used with that username, and enter the same password again in the **Confirm Password** field.

Enter Bandwidth Range

- Enter the bandwidth **IP Address** range the Threat Analysis Reporter will monitor.
- Enter the **Subnet Mask** for the bandwidth IP range to be monitored, using the dotted decimals notation format.
- Click **Add** to include your entries in the list box below.

 **NOTES:** Additional bandwidth ranges can be included by following steps A through C again. To remove a bandwidth range, select the IP Address from the list box and then click **Remove**.

Enter Web Filter Setup Criteria

- A. Enter the **Server Name** of the Web Filter to be used with the Threat Analysis Reporter, which is any name you wish to associate with that Web Filter.
- B. Enter the **Server IP** address of the Web Filter server to be used with the Threat Analysis Reporter.
- C. Click the “Set as Source” checkbox if this Web Filter will be designated the primary Web Filter to be associated with the Threat Analysis Reporter. Otherwise, leave the checkbox blank.
- D. Click **Add** to include your entries in the list box below.



NOTES:

- *Additional Web Filters can be included by following steps A through D again.*
- *The Source Web Filter is designated by an “X” in the Source column of the list box.*
- *To specify a Source Web Filter server from available entries in the list box, select the Server Name and then click Set as Source.*
- *To remove a Web Filter server from the list, select the Server Name from the list box and then click Remove.*

Enterprise Reporter registration

Respond to the question “Do you have an Enterprise Reporter?” by clicking the radio button corresponding to either “Yes” or “No” to specify whether the Source Web Filter server has an ER application connected to it.

If “Yes” was selected, enter the ER’s:

- **Server Name**
- **Server IP address**

Save settings

Click **Save** at the bottom right of the screen to save your settings and to go to the login window of the Threat Analysis Reporter user interface.

Proceed to Step 4: Generate SSL Certificate.

Step 4: Generate SSL Certificate

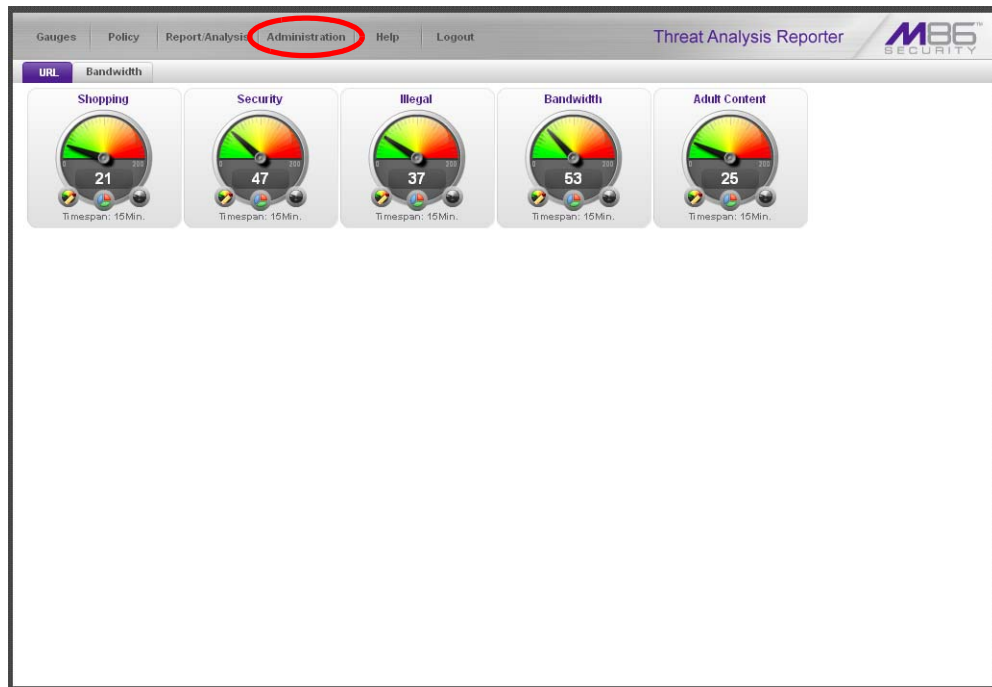
Generate a Self-Signed Certificate for TAR

This step requires you to generate a self-signed certificate for the Threat Analysis Reporter to ensure secure exchanges between the appliance and your browser.

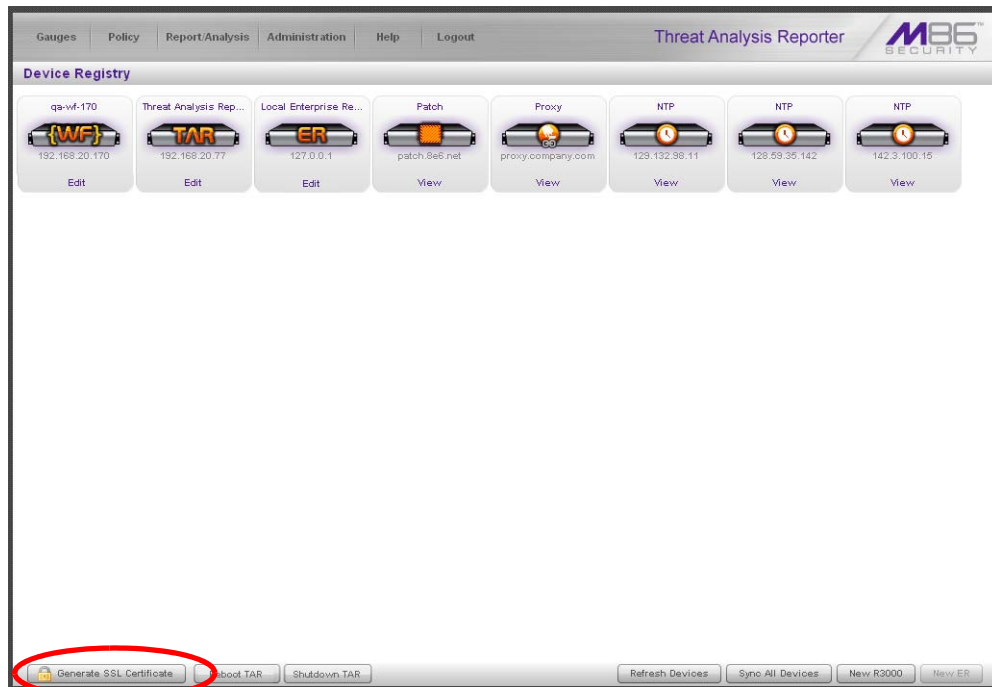
- A. In the Threat Analysis Reporter login window, type in the **Username** and **Password** registered for the TAR Wizard:

The image shows the login interface for the Threat Analysis Reporter (TAR). It features the M86 Security logo in the top right corner. Below the logo, there are two input fields: 'Username' and 'Password'. A 'Login' button is positioned below the password field.


- B. Click **Login** to display the gauges dashboard of the TAR user interface:



- C. Go to the navigation menu bar at the top of the screen and select **Administration > Device Registry** to display the Device Registry screen:



- D. Go to the bottom left corner of the Device Registry screen and click **Generate SSL Certificate** to open the Generate Self-Signed Certificate dialog box with the following message: "Generation of a self-signed certificate might take a long time. Afterwards, this application server would restart. Would you like to continue?"
- E. Click **Yes** to begin the process. Once the self-signed certificate has been generated, you will be logged out of the TAR user interface and the server will be restarted.

 **NOTE:** Although the Threat Analysis Reporter login window may re-display right away, the service will take a few minutes before it starts up again.

If using a Firefox or Safari browser, proceed to Conclusion.

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

IE Security Certificate Installation Procedures

Accept the Security Certificate in IE

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

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

Windows XP or Vista with IE 7 or 8

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

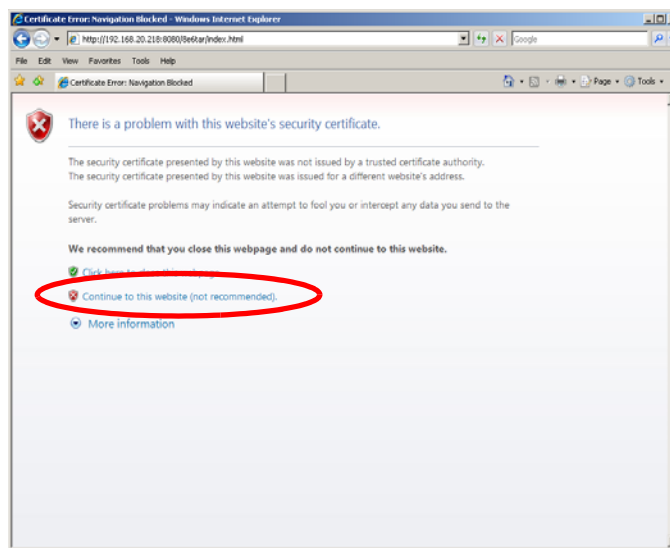


Figure A1: Windows XP, IE 7

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

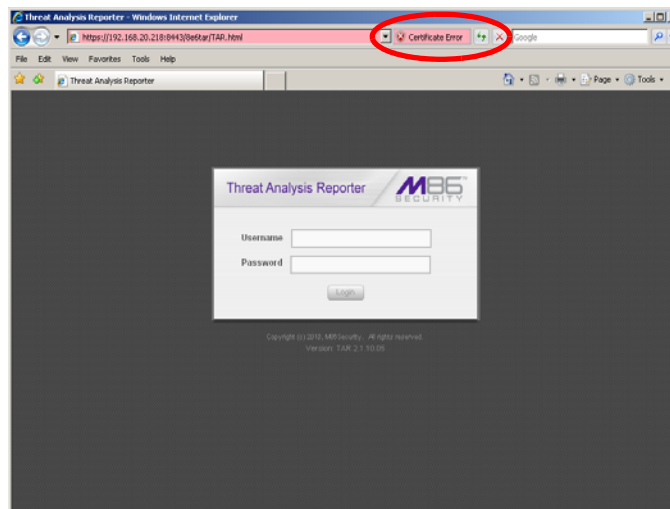


Figure A2: Windows XP, IE 7

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

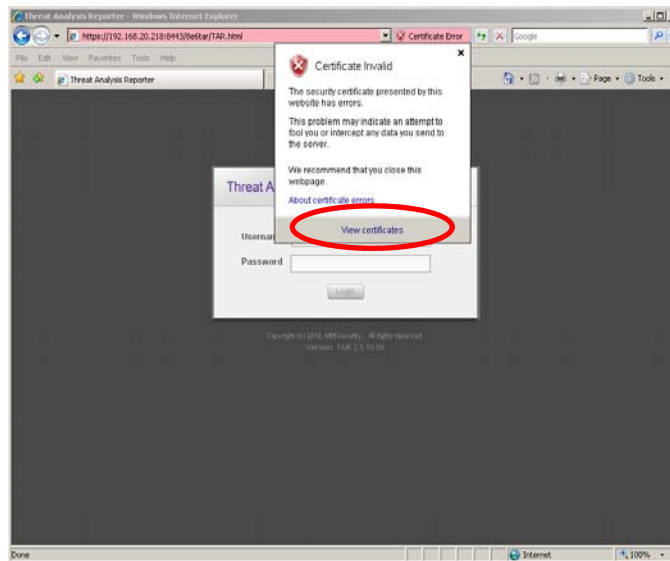


Figure B: Windows XP, IE 7

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



Figure C: Windows XP, IE 7

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

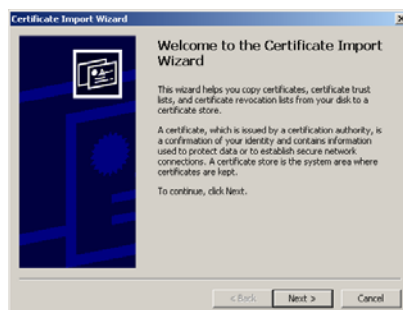


Figure D: Windows XP, IE 7

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

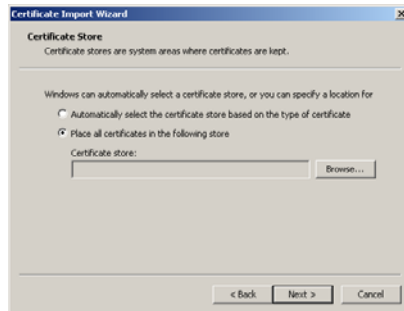


Figure E: Windows XP, IE 7

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



Figure F: Windows XP, IE 7

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



Figure H: Windows XP, IE 7

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

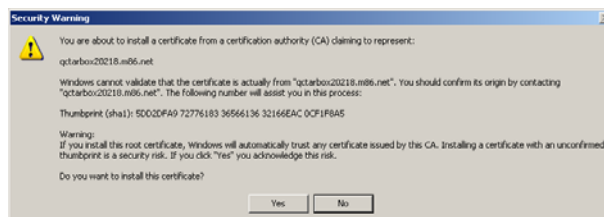


Figure I: Windows XP, IE 7

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

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

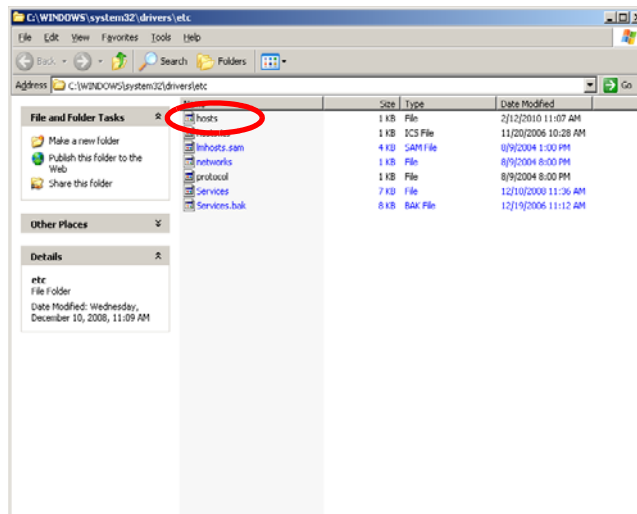
Windows 7 with IE 8

- 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 TAR, and then click **Add** and **Close**.
- E. Click **OK** to close the Internet Options pop-up box.
- F. Refresh the current Web page by pressing the **F5** key on your keyboard.
- G. Follow steps A to K documented in Windows XP or Vista with IE 7 or 8:
 - When the security issue page re-displays with the message: "There is a problem with this website's security certificate.", click **Continue to this website (not recommended)** (see Figure A1). Choosing this option displays the TAR login window with the address field and the Certificate Error button to the right of the field shaded a reddish color (see Figure A2).
 - Click **Certificate Error** to open the Certificate Invalid pop-up box (see Figure B).
 - Click **View certificates** to open the Certificate window that includes the host name you assigned to TAR (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**.

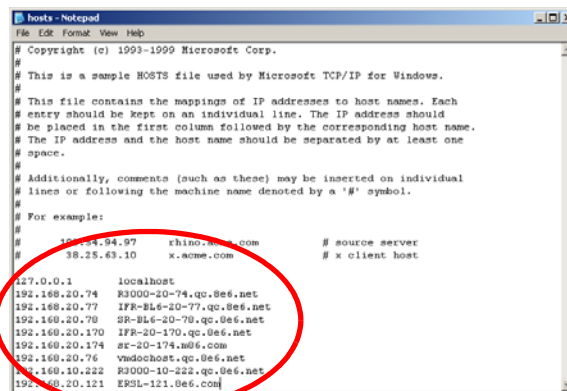
Now that the security certificate is installed, you will need to map TAR's IP address to its host name. Proceed to Map TAR's IP Address to the Server's Host Name.

Map TAR's IP Address to the Server's Host Name

- A. From your workstation, launch Windows Explorer and enter **C:\WINDOWS\system32\drivers\etc** in the Address field to open the folder where the hosts file is located:

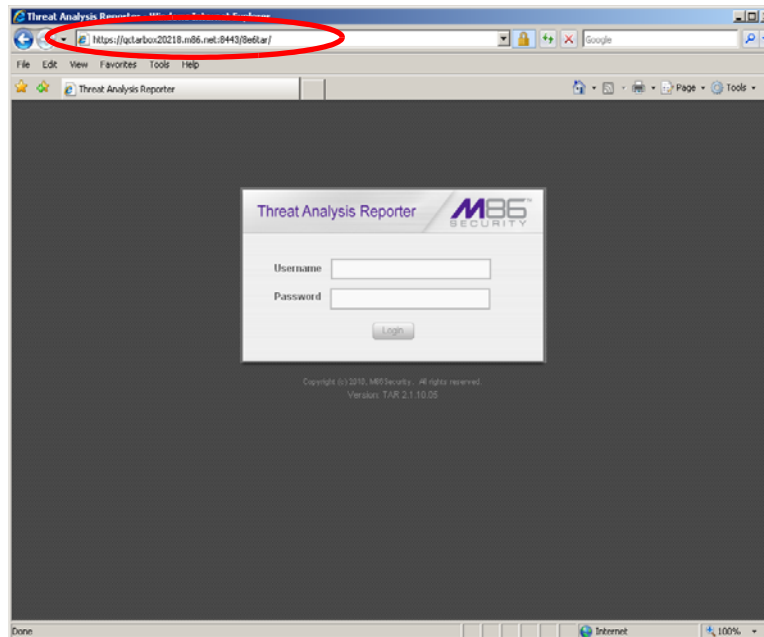


- B. Double-click "hosts" to open a window asking which program you wish to use to open the file. Double-click "Notepad" or "TextPad" to launch the hosts file using that selected program:



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

- D. In the address field of your newly opened IE browser, from now on you will need to use TAR's host name instead of its IP address—that is **https://host-name:8443/8e6tar/** would be used instead of **https://x.x.x.x:8443/8e6tar/**. Click **Go** to open the TAR login window:



CONCLUSION

Congratulations; you have completed the Threat Analysis Reporter installation procedures. Now that the Threat Analysis Reporter is running on your network, the next step is to set up user groups or administrator groups. You will set up and configure gauges thereafter.

Obtain the latest Threat Analysis Reporter User Guide from our Web site at <http://www.m86security.com/support/Threat-Analysis-Reporter/documentation.asp>



IMPORTANT: M86 Security recommends proceeding to the *Best Usage Practices* section for quick setup procedures described within that section.

BEST USAGE PRACTICES

Now that the Threat Analysis Reporter is installed on the network and you have successfully logged into the server, you are ready to begin using the Administrator console. To help you get started, this section provides an overview on some useful setup procedures and tools in the interface that you will use for identifying potential violators of your acceptable Internet usage policy so you can take effective and immediate action.

You will learn how to:

- navigate screens to access tools for configuring the Threat Analysis Reporter
- drill down into a dashboard gauge to target sources of unusually high Internet activity
- create a gauge that will monitor a user group's Internet activity
- set up an email alert for notification of potential Internet usage threats on the network

Please review the Threat Analysis Reporter Usage Scenarios sub-section for instructions and tips on using tools in the console to fulfill the scenarios described above.

Threat Analysis Reporter Usage Scenarios

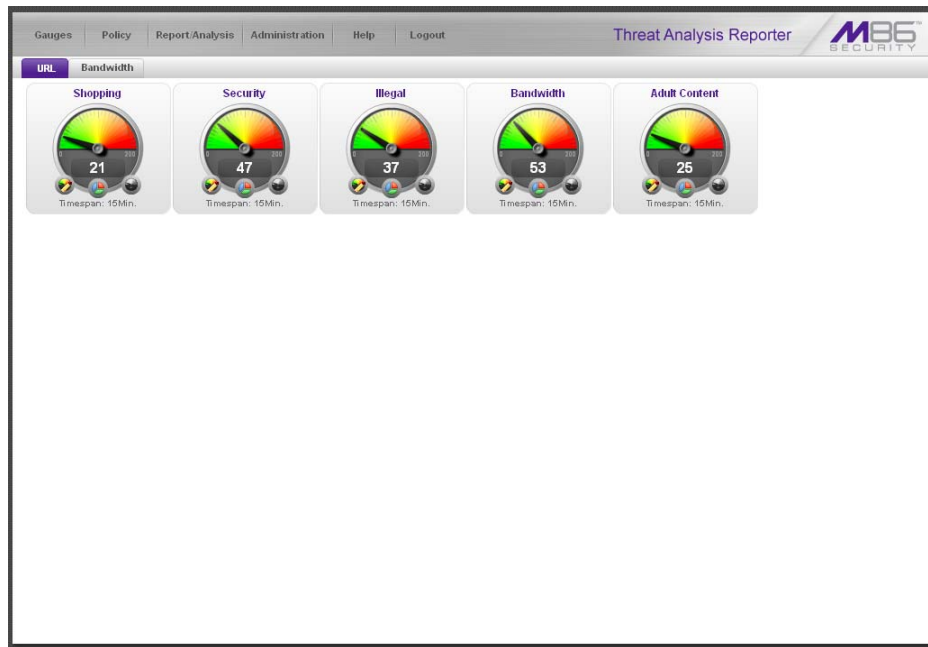
This collection of setup and usage scenarios is designed to help you understand and use basic tools in the console for enforcing your Internet usage policy. Each scenario is followed by console setup information. Please consult the "How to" section in the index of the Threat Analysis Reporter User Guide for pages containing detailed, step-by-step instructions on configuring and/or using the tools and features described in that scenario.

I. Screen navigation exercise

This exercise will familiarize you with the four sections of the user interface and inform you where to go to customize the application to perform a specified task or function.

Step A: Navigate panels in the Gauges section

The URL dashboard displays by default after you log into the console. This main screen is comprised of a banner and dashboard below. The navigation portion of the banner includes six links—the first four links containing a menu of topics used for accessing other panels in the application—and the main panel showing the current status of URL gauges:



Each URL gauge contains a number that represents its current score. This score is derived by activity within that gauge, based on the activities of end users who visited URLs listed in library categories that comprise the gauge.

To view bandwidth gauge activity, click the Bandwidth tab above the URL gauges dashboard to display the bandwidth gauges dashboard. The score for each bandwidth gauge represents the number of bytes of end user bandwidth traffic in ports or protocols that comprise the gauge.

Click any of the topic links from the Gauges menu to display panels used for viewing/configuring URL/bandwidth gauges and/or gauge activity:

- **Dashboard** - view current gauge activity
- **Overall Ranking** - view details about current gauge activity for all end users affecting gauges
- **Lockouts** - prevent the end user from accessing specified URLs, the Internet, or the entire network
- **Add/Edit Gauges** - create and maintain gauges used for monitoring end users' Internet activity
- **Dashboard Settings** - customize the view to only show certain gauges

Step B: Navigate panels in the Policy section

Click the Policy link to display its menu. Click any of the menu topics to display panels used for establishing policies for high threat level threshold management:

- **Alerts** - manage alerts that indicate if gauges are close to—or have reached—their established upper thresholds
- **Alert Logs** - view a list of alert records for the most recent 24-hour time period

Step C: Navigate panels in the Report/Analysis section

Click the Report/Analysis link to display its menu. Click any of the menu topics to display panels used for accessing appliances connected to the Threat Analysis Reporter, to perform a search on user URL/bandwidth activity, or to generate a report showing activity in all URL or bandwidth gauges:

- **Web Filter** - access the Web Filter to configure profiles for end users
- **Enterprise Reporter** - access the ER Web Client to generate reports on end user Internet activity, or access the ER Admin GUI application to configure the ER application
- **Custom Search** - view a list of end users who accessed a specified library category or bandwidth port/protocol
- **Trend Chart** - view a graphical depiction of activity for URL/bandwidth gauges

Now that you've become familiar with the layout of the interface, you will know where you need to go to configure the Threat Analysis Reporter and access real time information.

Step D: Navigate panels in the Administration section

Click the Administration link to display its menu. Click any of the menu topics to display panels used for configuring profiles and maintaining the server:

- **Admin Trails** - view a list of alert records for the most recent time period
- **Device Registry** - view information about devices connected to TAR, synchronize the server with user groups and libraries from the source Web Filter, edit M86 Security appliance criteria, add or delete a Web Filter or ER, reboot or shut down the server, or generate an SSL certificate for TAR
- **User Profiles** - manage a list of end users' logged events
- **Add/Edit Admins** - manage group administrator profiles
- **Admin Groups** - set permissions so that an administrator in your group will only be able to access areas of the Threat Analysis Reporter console that you specify
- **User Groups** - manage user groups whose activity will be monitored by gauges
- **Backup/Restore** - perform a backup and/or restoration of files on the Threat Analysis Reporter application
- **Software Update** - update the server with the latest software version
- **Hardware Detector** - maintain the health of a Threat Analysis Reporter server with RAID installed

Now that you've become familiar with the layout of the interface, you will know where you need to go to configure TAR and access real time information.



In the Threat Analysis Reporter User Guide index, see:

- *How to: navigate the TAR user interface*
-


II. Drill down into a gauge exercise

This exercise will teach you how to drill down into a URL gauge to conduct an investigation on abnormally high Internet activity in a particular filtering category, in order to find out which individuals are driving that gauge's score, and which URLs they are visiting.

Step A: Select the gauge with the highest score

1. In the URL dashboard, select the gauge with the highest score and click it to open the Gauge Ranking table showing columns with names of threats (library categories) that comprise the gauge, and rows of end user records with activity in one or more of these threats:

[illegible]

 **NOTE:** The Gauge Ranking panel is also accessible by right-clicking a dashboard gauge and then selecting View Gauge Ranking from the pop-up menu.

- Find the threat with the highest score, and click that score to open the Threat View User panel:

The screenshot shows the Threat Analysis Reporter interface. At the top, there is a navigation bar with links: Gauges, Policy, Report/Analysis, Administration, Help, and Logout. The title bar indicates the user is 192.168.30.87 and the gauge name is All Threats. The main content area is divided into two panels. The left panel, titled 'Threats', contains a table with two columns: 'Threats' and 'Total'. The right panel, titled 'URLs', contains a table with two columns: 'URLs' and 'Timestamp'.

| Threats | Total |
|-------------------------------------|-------|
| Uncategorized | 74 |
| Banner/Web Ads | 7 |
| General Business | 3 |
| News | 2 |
| Reviewed/Miscellaneous | 1 |
| Social Opinion | 1 |
| Search Engines | 1 |
| Financial Institution | 1 |
| Edge Content Servers/Infrastructure | 1 |

| URLs | Timestamp |
|------|-----------|
|------|-----------|

Note the left side of this panel is populated with rows of records for Threats affected by the selected end user.

Now that you've identified the user affecting the highest scoring gauge, next you will investigate the activity of that user who is driving the gauge's score.



In the Threat Analysis Reporter User Guide index, see:

- *How to: drill down into a gauge*

Step B: Investigate a user's activity in a specified gauge

1. To find out which URLs the top end user visited in the library category associated with the high-scoring threat, select the Threat with the highest score and then click it to display a list of URLs the user visited in the right side of this panel:

[illegible]

2. Choose a URL you wish to view, and then click it to open a separate browser window accessing that URL.

After investigating one or more URLs in the list, you may wish to find out which other gauges that same user is currently affecting.

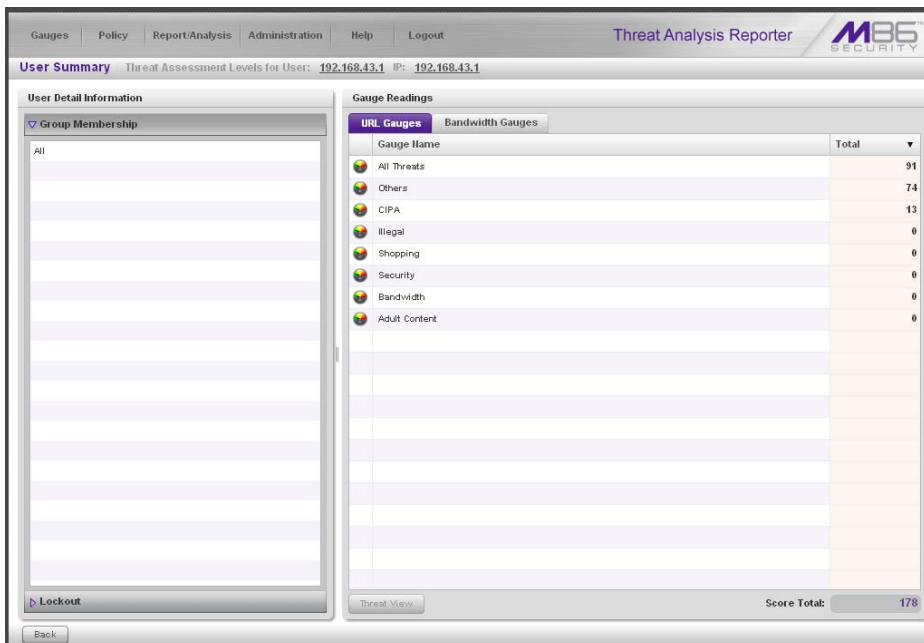


In the Threat Analysis Reporter User Guide index, see:

- *How to: view URLs a user visited in TAR*

Step C: Investigate the user's Internet activity in other gauges

1. To find out which other gauges the same user is currently affecting, return to the Gauge Ranking table by going to the lower left corner of the Threat View User panel and clicking the **Back** button. In the User Name column, click that user's link to display the User Summary panel for that user:



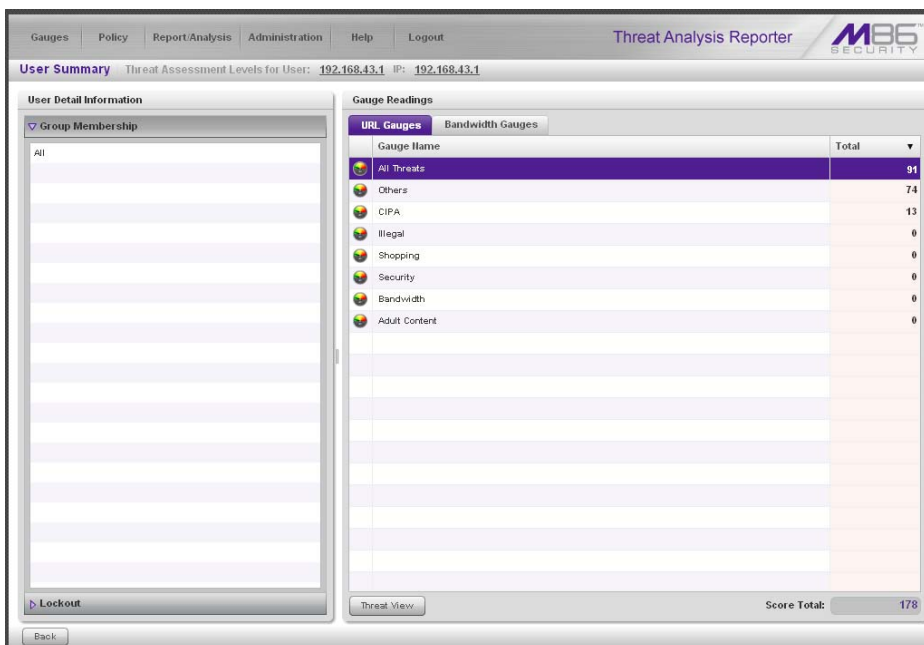
The screenshot shows the 'User Summary' panel for user 192.168.43.1. The 'Gauge Readings' table is as follows:

| Gauge Name | Total |
|---------------|-------|
| All Threats | 91 |
| Others | 74 |
| CIPA | 13 |
| Illegal | 0 |
| Shopping | 0 |
| Security | 0 |
| Bandwidth | 0 |
| Adult Content | 0 |

The 'Score Total' at the bottom right is 178.

Note the Gauge Readings frame to the right with the Total score for each Gauge Name listed.

2. Select a Gauge Name to investigate, which activates the Threat View button below:



The screenshot shows the same 'User Summary' panel, but the 'All Threats' gauge is now selected, highlighted in blue. The 'Threat View' button is now visible at the bottom of the 'Gauge Readings' section.

3. Click **Threat View** to display the Threat View User panel (see Step A2).

4. To find out which URLs the user is viewing in a particular library category, choose the category from the list, and then click the URL in the URLs list (see Step B1).



In the Threat Analysis Reporter User Guide index, see:

- *How to: view end user gauge activity*

You have just learned how to drill down into a gauge to conduct an investigation on identifying the source of unusually high Internet activity. The steps in this exercise demonstrated how to investigate gauge scores in order to find out which end users are driving the score in one or more gauges, and how to view URLs visited by the user.

When you become accustomed to using the Threat Analysis Reporter on a regular basis to conduct these types of investigations, you will eventually want to explore other tools in the interface to restrict or lock out offending users from accessing certain library categories.

III. Create a gauge exercise

This exercise will teach you how to create a URL gauge to be used for monitoring a user group's Internet activity in specified filtering categories.

Step A: Access the Add/Edit Gauges panel

From the Gauges menu, select Add/Edit Gauges to open the Add/Edit Gauges panel:

[illegible]

Note that this panel contains the current Gauge Name list at the left side.

Next, you will specify that you wish to create a new gauge.



In the Threat Analysis Reporter User Guide index, see:

- How to: access the Add/Edit Gauges panel

Step B: Add a URL Gauge

1. Click **New Gauge** at the bottom left of the panel to open the URL Gauge panel:

2. In the Gauge Information frame to the left, specify the following information as necessary:
 - a. **Gauge Name** you wish to use and display for this gauge; this entry must be at least two characters in length.
 - b. **Group Threshold** for the ceiling of gauge activity. For this exercise we will use the default and recommended value, which is 200 for a URL gauge.
 - c. **Timespan (minutes)** for tracking gauge activity (1 - 60 minutes). For this exercise we will use the default and recommended value, which is 15 minutes.
 - d. **Gauge Method** to be used for tracking gauge activity. For this exercise we will use the default "All" gauge method, so you do not need to make any selection from the drop-down menu. The selected "All" method considers all methods users can use to access URLs in library categories included in the gauge.
3. In the Available Threats/Groups list to the right, select one Threat Class/Group, or up to 15 library categories by clicking each one while pressing the **Ctrl** key on your keyboard. When you have made your selection(s) for the gauge to monitor, click the **add >** button to move the choice(s) to the Assigned Threats/Groups list box.
4. Click the User Membership accordion to open it and to display a list of Available User Groups in the list to the left:

5. From the Available User Groups list, select the user group to highlight it.
6. Click **add >** to move the user group to the Assigned User Groups list box.
7. After adding users, click **Save** at the bottom right of the panel to return to the Add/Edit Gauges panel that now includes the name of the gauge you just added:



In the Threat Analysis Reporter User Guide index, see:

- *How to: add new a gauge*

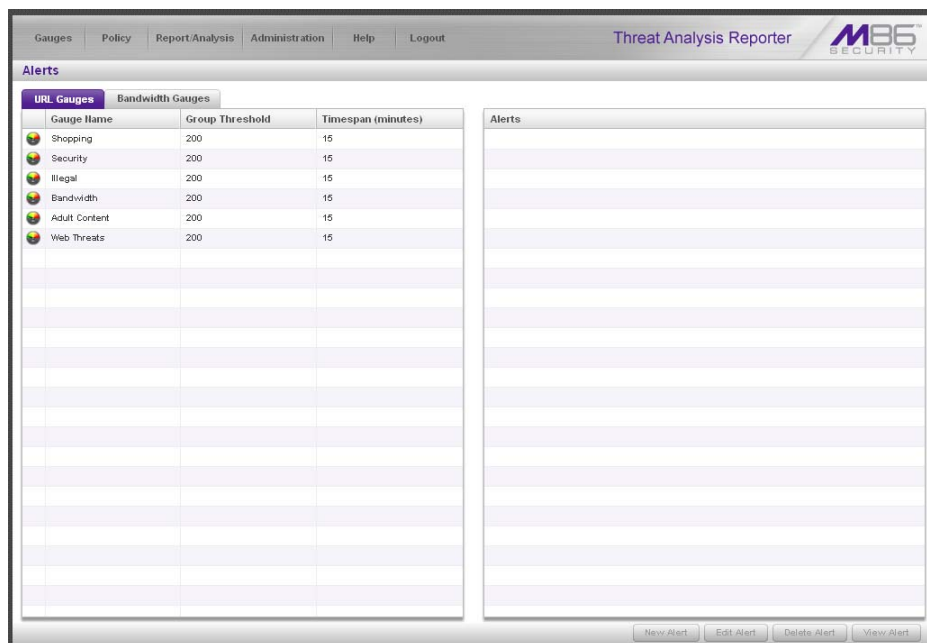
Now that you know the basics of creating a gauge, you will soon be able to create and use gauges to monitor various groups of users who frequent URLs in library categories you wish to restrict, and deal in real time with Internet usage issues that endanger your network and/or consume an excessive amount of bandwidth resources.

IV. Create an email alert exercise

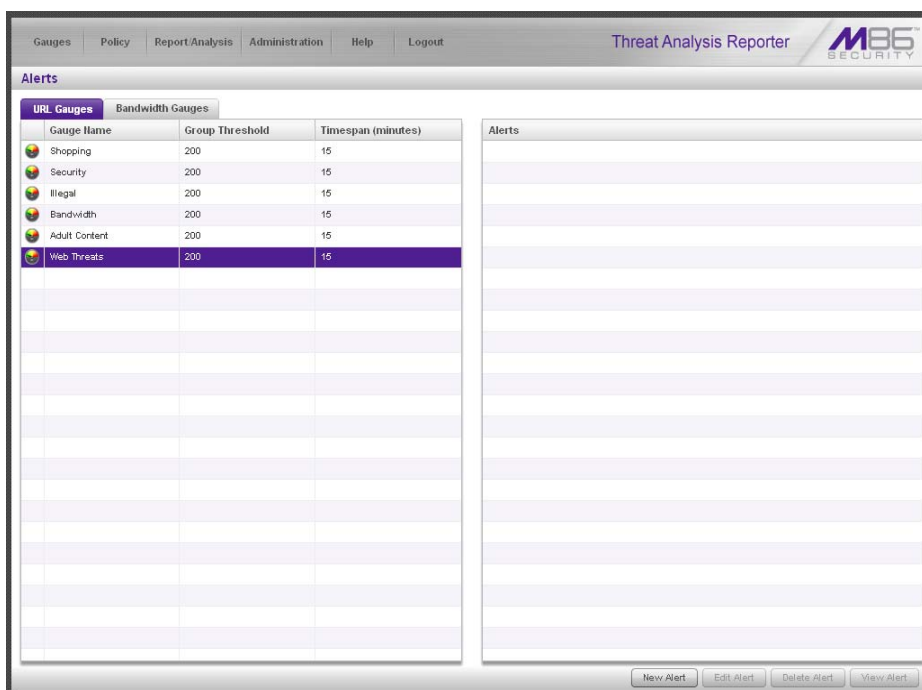
This exercise will teach you how to set up an email alert so you will be notified when a gauge reaches the high end of its established threshold.

Step A: Add a new alert

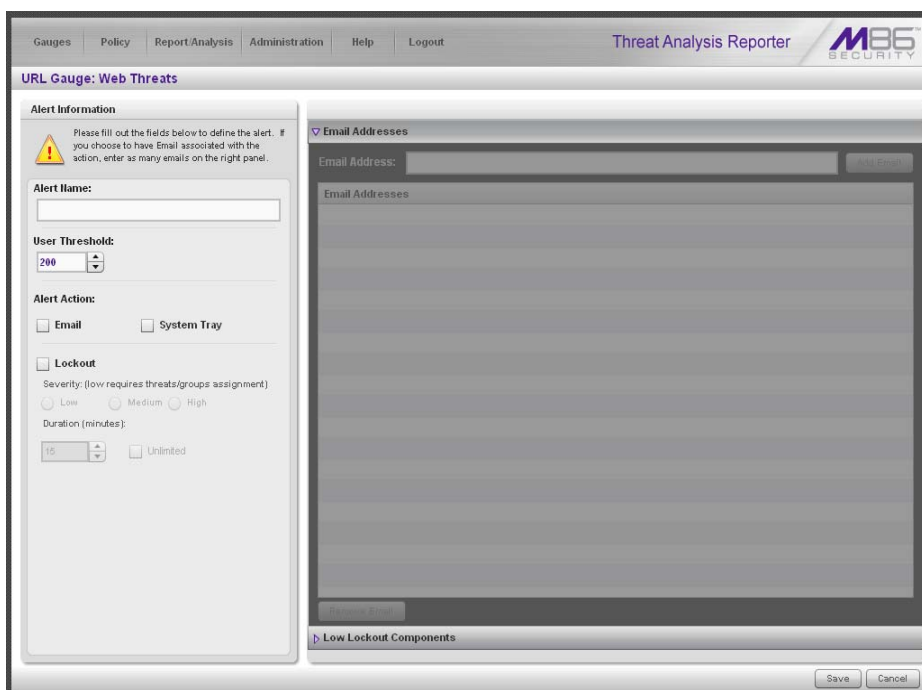
1. From the Policy menu, select Alerts to open the Alerts panel:



2. In the left frame, select the gauge for which an alert will be created; this action activates the New Alert button:



- Click **New Alert** to open a panel that displays the Alert Information frame to the left and the greyed-out target panel to the right containing the Email Addresses and Low Lockout Components accordions:



- Type in the **Alert Name** to be used for the alert that will be delivered to the group administrator.
- Specify the **User Threshold** ceiling of gauge activity that will trigger the alert. The default and recommended value is 200 for a URL gauge.
- Specify the **Alert Action** method(s) to be used for alert notifications:

- **Email** - An email alert notifies a group administrator via email if an end user has reached the threshold limit set up in a gauge alert.
- **System Tray** - A TAR Alert message notifies a group administrator via his/her workstation's System Tray if an end user has reached the threshold limit set up in a gauge alert.
- **Lockout** - The Lockout function locks out an end user from Internet/network access if he/she reaches the threshold limit set up in a gauge alert.

For this exercise, however, you will only want to select Email, as described in the next step.



In the *Threat Analysis Reporter User Guide index*, see:

- *How to: add a new alert*

Step C: Select Email Alert Action

1. In the Alert Action section, choose the “Email” alert notification option.

Note that this action opens and activates the Email Addresses accordion at the right side of the panel.

2. In the **Email Address** field, type in the email address to which the alert will be sent, and then click **Add Email** to include the email address in the list box above.
3. Click **Save** at the bottom right of the panel to save your entries and to display the Alerts panel.

Next you will learn what to expect when an email alert is sent to your mailbox.

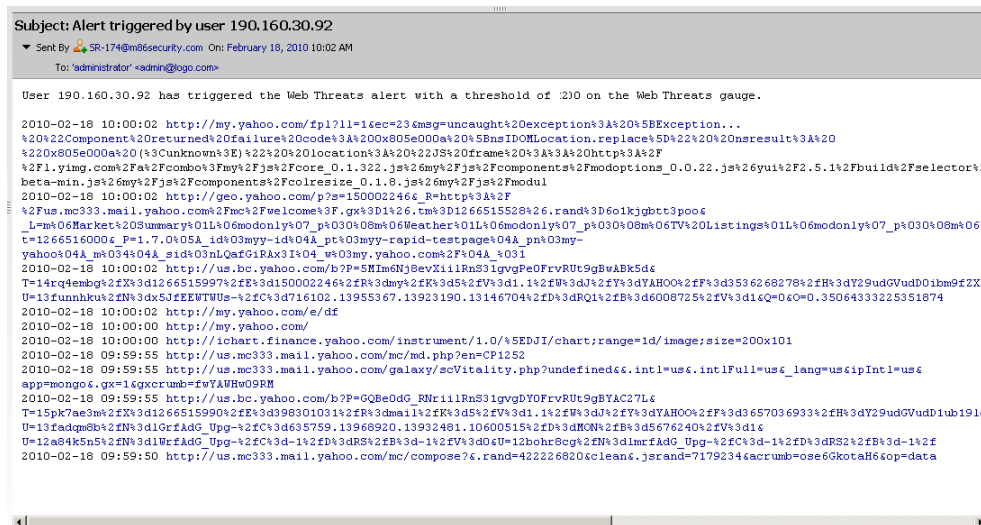


In the Threat Analysis Reporter User Guide index, see:

- *How to: set up email alert notifications in TAR*

Step D: Receiving an email alert

When an end user's activity in a gauge reaches the threshold limit established for an alert, it triggers an alert notification. If the email alert option was selected, an email is sent to the email address that was specified:



The email alert identifies the end user who triggered the alert, and includes a list of URLs the user visited, along with the date and time each URL was accessed. Clicking any of the URLs in the email opens a browser window containing the contents of that URL.



In the Threat Analysis Reporter User Guide index, see:

- *How to: view an email alert in TAR*

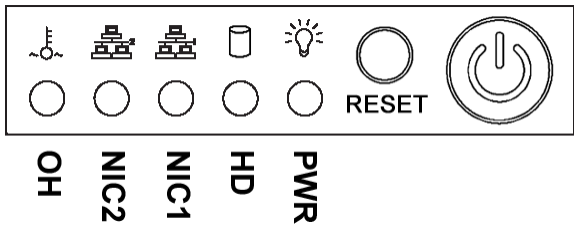
Now that you know how to create an email alert for a gauge, you will quickly identify users who are misusing their Internet access privileges, giving you knowledge about policy violations in real time so you can immediately take action to protect your resources.

LED INDICATORS AND BUTTONS

SL and MSA Units

Front LED Indicators and Buttons for Hardware Status Monitoring

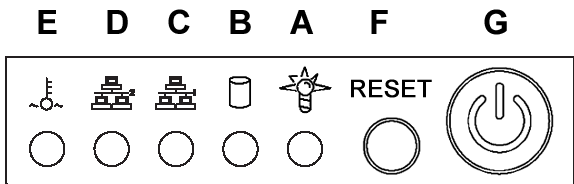
LED indicators and buttons for hardware status monitoring display on the front panel, located on the right side of the SL and MSA chassis (see diagrams below).



SL chassis control panel

LED Indicator Key

PWR = Power
 HD = HDD Activity
 NIC1 = LAN 1
 NIC2 = LAN 2
 OH = Overheat



MSA chassis control panel

LED Indicator Key Button Key

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

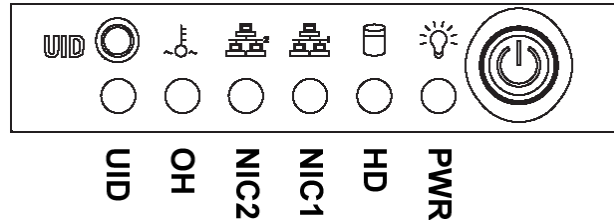
LED indicators alert you to the status of a feature on the unit while buttons let you perform a function on the unit.

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

HL Unit

Front LED Indicators and Buttons for Hardware Status Monitoring

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





LED Indicator Key


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


HL chassis control panel


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


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


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

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

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

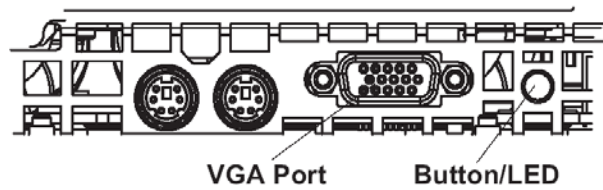
 **HDD** (icon) – In addition to displaying in the control panel, this icon also displays on the front panel on each hard drive carrier. A green LED indicates hard drive activity. An unlit LED on a drive carrier may indicate a hard drive failure.

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

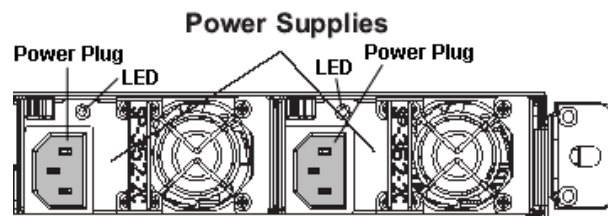
 **Power** (button) – When the power button is pressed, the main power to the server is turned on. When the power button is pressed again, the main power to the server is removed but standby power is still supplied to the server.

Rear LED Indicators for Hardware Status Monitoring

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



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



HL and SL Units

Front LED Indicators for Software and Hardware Status Monitoring

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

| | |
|----------------------------|-------------------------------|
| <input type="radio"/> LOG | LED Indicator Key |
| <input type="radio"/> RAID | LOG = Log Download Status |
| <input type="radio"/> DB | RAID = Hard Drive Status |
| <input type="radio"/> UPDT | DB = Database Status |
| | UPDT = Software Update Status |

left side of the front panel

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

| LED Indicator | Color | Condition | Description |
|---------------|-------|-----------|-------------------------------|
| LOG | Green | On | Downloading a log |
| | -- | Off | No log download detected |
| RAID | Green | On | RAID mode enabled and running |
| | -- | Off | RAID mode is inactive |
| | Red | On | Hard drive fault or failure |
| DB | Green | On | Database is active |
| | Red | On | Database is inactive |
| UPDT | Amber | On | Software update detected |
| | -- | Off | No software update detected |

REGULATORY SPECIFICATIONS AND DISCLAIMERS

Declaration of the Manufacturer or Importer

Safety Compliance

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

Electromagnetic Compatibility (EMC)

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

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

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

FCC Declaration of Conformity

Models: HL-005-004, SL-004-004, MSA-004-004

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): HL-005-004, SL-004-004, MSA-004-004

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: OPTIONAL ETHERNET TAP INSTALLATION

This appendix pertains to the optional installation of the Ethernet Tap unit for bandwidth monitoring.

Preliminary Setup Procedures

Unpack the Ethernet Tap Unit from the Box

Open the NetOptics Ethernet Tap box 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 NetOptics box should contain the following items:

- 1 NetOptics 10/100BaseT Tap
- 2 Power Supply units
- 2 AC Power cords
- 2 Crossover cables
- 2 Straight through cables
- 1 Installation Guide

Other Required Installation Items

In addition to the contents of the NetOptics box, you will need the following item to install the Ethernet Tap unit:

- 1 Standard CAT-5E cable

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

Install the Ethernet Tap Unit

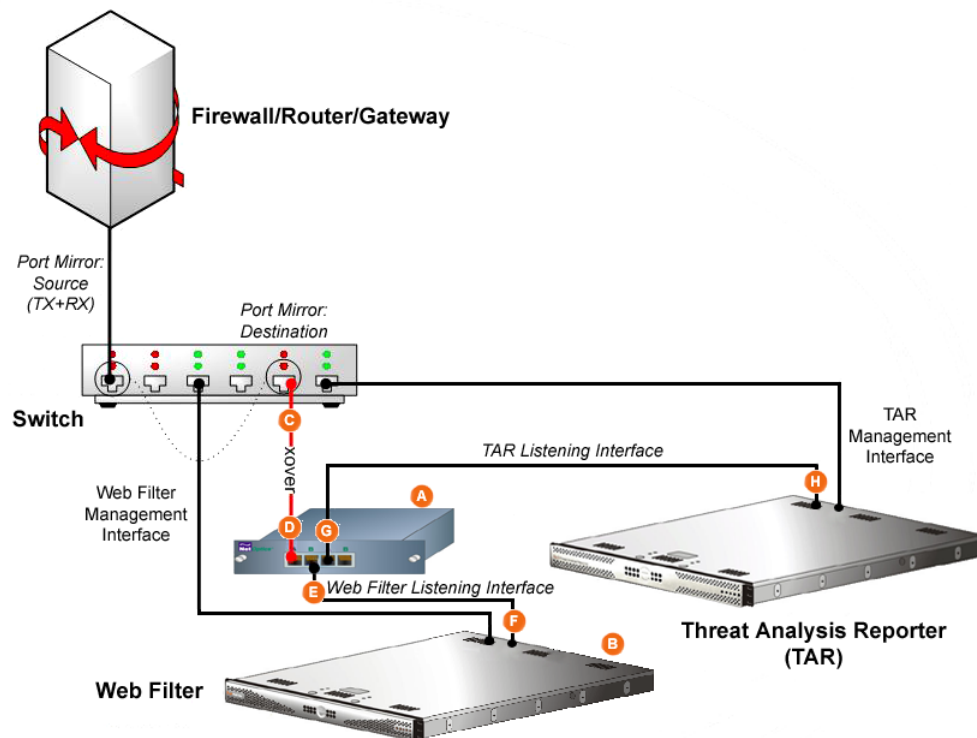


Diagram showing TAR Ethernet Tap installation on the network

This step is a continuation from Physically Connect the Unit to the Network in Step 1A or following setup in Step 1B. The procedures outlined in this step require the use of a CAT-5E cable.

- A. Provide power to the Ethernet Tap by connecting both power cords from the unit to the power source.



AC power in rear panel of NetOptics 10/100BaseT Tap

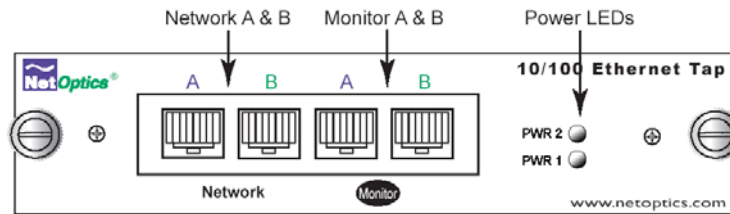
- B. If a designated source Web Filter (to be used with the Threat Analysis Reporter) is already installed on the network, disconnect the cable that connects this Web Filter to the switch.

If the designated Web Filter has not yet been installed, disregard this sub-step and proceed to sub-step C.

- C. Using a crossover cable, connect one end to the Switch's port configured to be the destination port of the Port Mirror.

If adding a Threat Analysis Reporter to an existing installation, this port would be the port that was originally occupied by the listening interface of the Web Filter.

- D. Connect the other end of the crossover cable to the Ethernet Tap's Network A port.



Ports in front panel of NetOptics 10/100BaseT Tap

- E. Using a straight through cable, connect one end to the Ethernet Tap's Network B port.
- F. Connect the other end of the straight through cable to the Web Filter's listening interface.
- G. Using the second straight through cable, connect one end to the Ethernet Tap's Monitor A port.
- H. Connect the other end of the second straight through cable to the Threat Analysis Reporter's listening interface.

Proceed to Step 3: Register TAR and its Applications of the Threat Analysis Reporter installation instructions.

INDEX

A

Admin Console Wizard User 41

B

BSMI 79, 81

C

Change Quick Start password 37
crossover cable 4

E

EMC 79

F

FCC 79

H

HL 4, 7, 22, 24, 28, 29, 44, 76, 77, 78
HyperTerminal Setup 30

I

ICES-003 79, 81
Install Bezel 22
Install Tap 83

L

LCD Panel 27, 39
Login screen 33
LVD 79

M

MSA 28, 29, 44

O

Overheat 75, 76

P

ping the SR 45
Power Supply Precautions 23

Q

Quick Start menu instructions 33

R

Rack Setup Precautions 6
RAID 78
reboot 42
RoHS compliant 82

S

serial port cable 27, 28
shut down 63
SL 11, 22, 28, 29, 44, 75, 78
spare parts kit 4

U

UID 76, 77
UL 79

W

Web Filter 1, 27, 63, 84

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