



8e6® Threat Analysis Reporter

QUICK START GUIDE



Model: TAR

HL-005-004, SL-004-004, MSA-004-004

Release: 1.3.00 / Updated: 03.16.09

8E6 THREAT ANALYSIS REPORTER QUICK START GUIDE

© 2009 8e6 Technologies. All rights reserved.

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 8e6 Technologies.

Every effort has been made to ensure the accuracy of this document. However, 8e6 Technologies makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. 8e6 Technologies 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. The information in this documentation is subject to change without notice.

The Threat Analysis Reporter products have 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.

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# TARul-QSG-090316

CONTENTS

THREAT ANALYSIS REPORTER INTRODUCTION.....	1
About this Document	2
Conventions Used in this Document.....	3
SERVICE INFORMATION	4
PRELIMINARY SETUP PROCEDURES	5
Unpack the Unit from the Carton	5
Select a Site for the Server	6
Rack Mount the Server.....	7
Check the Power Supply.....	24
General Safety Information.....	25
INSTALL THE SERVER	28
Step 1: Initial Setup Procedures	28
Step 1A: Quick Start Setup Procedures	29
Step 1B: LCD Panel Setup Procedures	45
Step 2: Wizard Setup Procedures	51
CONCLUSION	61
BEST USAGE PRACTICES	62
Threat Analysis Reporter Usage Scenarios	62
LED INDICATORS AND BUTTONS.....	77
SL and MSA Units.....	77
HL Unit	78
HL and SL Units	80
REGULATORY SPECIFICATIONS AND DISCLAIMERS.....	81
Declaration of the Manufacturer or Importer	81
APPENDIX: OPTIONAL ETHERNET TAP INSTALLATION.....	84
Preliminary Setup Procedures	84

Install the Ethernet Tap Unit	85
INDEX	87

THREAT ANALYSIS REPORTER INTRODUCTION

Thank you for choosing to evaluate the 8e6 Technologies 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 8e6's R3000 Enterprise Filter, the Threat Analysis Reporter translates end user Internet activity from the R3000'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 8e6 Technologies contact information
- **Preliminary Setup Procedures** - This section includes instructions on how to physically set up the Threat Analysis Reporter unit in your network environment
- **Install the Server** - This section explains how to configure the Threat Analysis Reporter
- **Conclusion** - This section indicates that the quick start steps have been completed
- **Best Usage Practices** - This section includes setup 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 8e6 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 Usage 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 8e6 Technologies solutions engineer or technical support representative.

8e6 Corporate Headquarters (USA)

Local	:	714.282.6111
Domestic US	:	1.888.786.7999
International	:	+1.714.282.6111

8e6 Taiwan

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

Procedures

When calling 8e6 Technologies 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 8e6 Technologies.

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 envelope containing a CD-ROM with a PDF of the Threat Analysis Reporter User Guide. The latest version of the user guide can be obtained from our Web site at http://www.8e6.com/docs/tar_ug.pdf.



NOTES: A coupler is included in the carton if a three-foot CAT-5E crossover cable is packaged with your unit instead of a 14-foot CAT-5E crossover cable. 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.

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



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

Select a Site for the Server

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

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

Rack Mount the Server

Rack Setup Precautions

Warning:

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

- The weight of all units in the rack is evenly distributed. Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- The rack will not tip over when the server is mounted, even when the unit is fully extended from the rack.
- For a single rack installation, stabilizers are attached to the rack.
- For multiple rack installations, racks are coupled together.
- Reliable earthing of rack-mounted equipment is maintained at all times. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).
- A power cord will be long enough to fit into the server when properly mounted in the rack and will be able to supply power to the unit.
- The connection of the server to the power supply will not overload any circuits. Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
- The server is only connected to a properly rated supply circuit. Reliable earthing (grounding) of rack-mounted equipment should be maintained.
- The air flow through the server's fan or vents is not restricted. Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.
- The maximum operating ambient temperature does not exceed 104°F (40°C). If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.

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

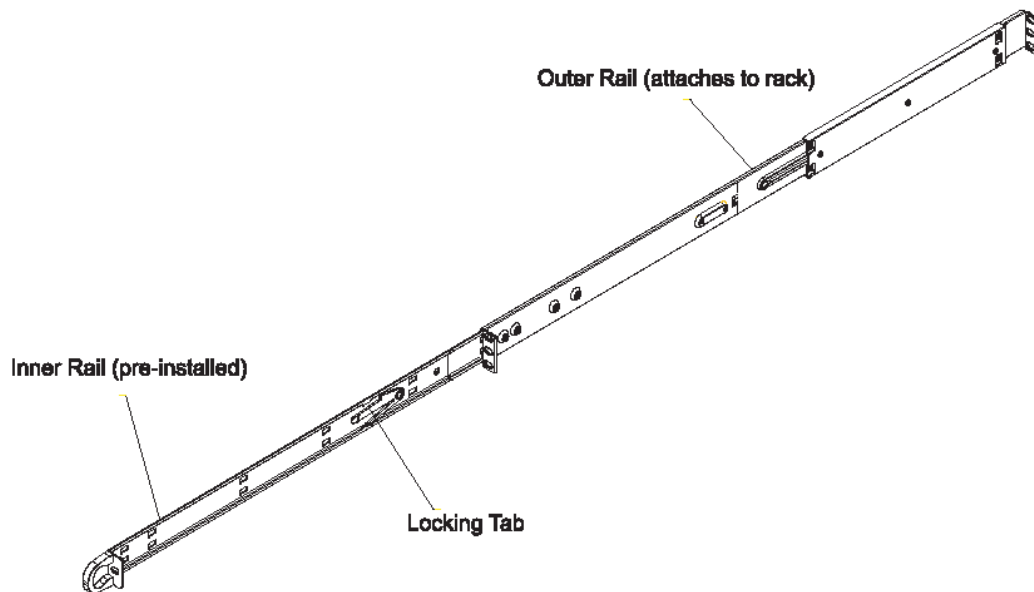
Rack Mount Instructions for HL Servers

Rack Setup Suggestions

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

Identify the Sections of the Rack Rails

You should have received two rack rail assemblies with the 8e6 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.



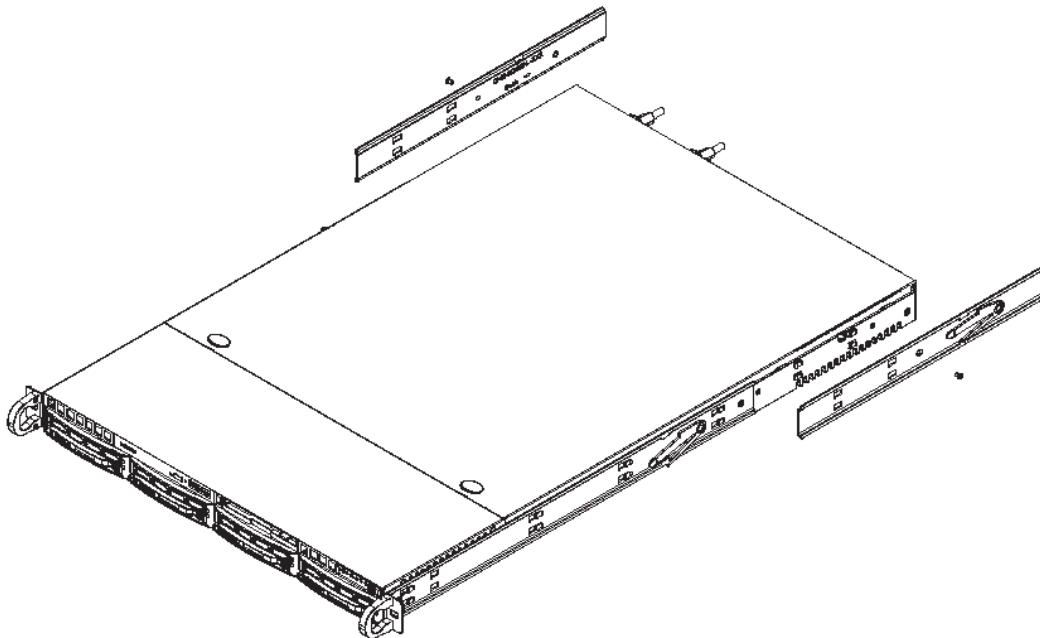
Install the Inner Rails

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 fit 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.

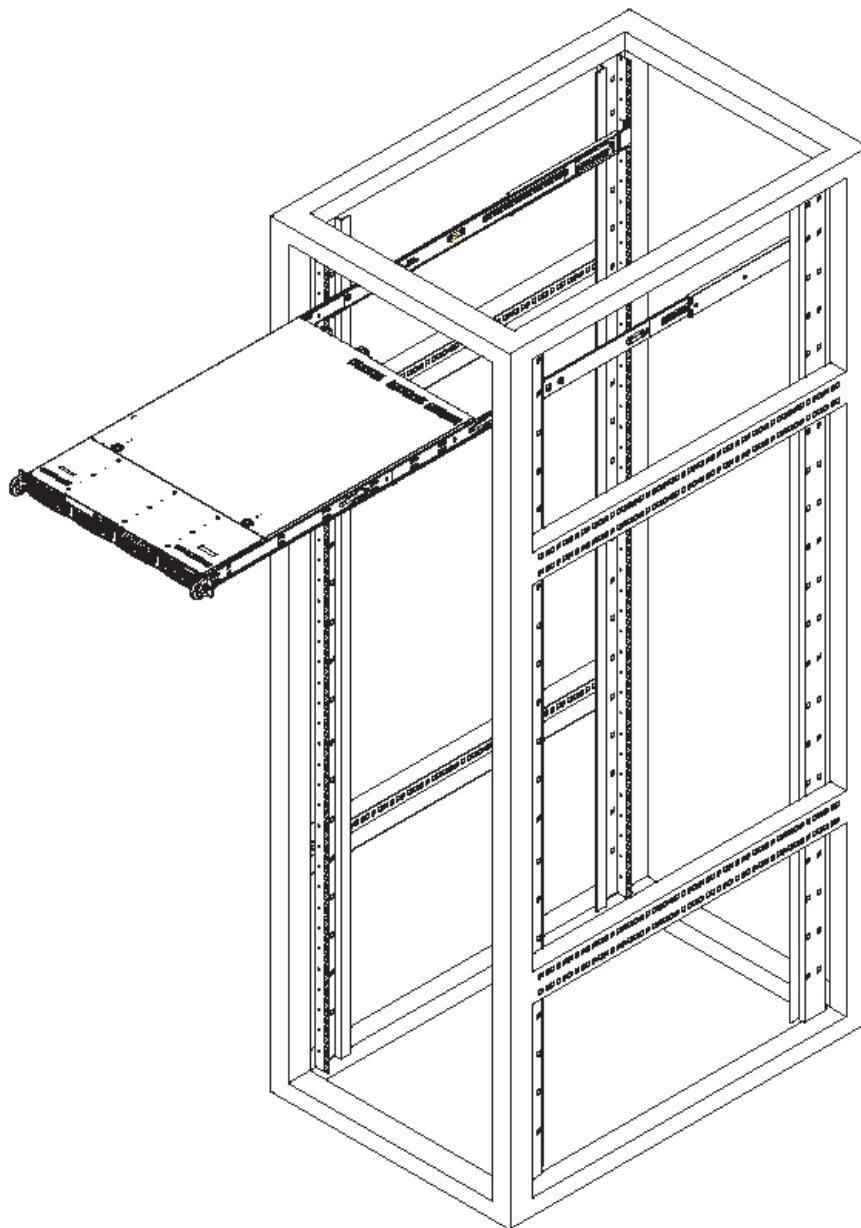
Locking Tabs: Both chassis rails have a locking tab, which serves two functions. The first is to lock the server into place when installed and pushed fully into the rack, which is its normal position. Secondly, these tabs also lock the server in place when fully extended from the rack. This prevents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



Install the Server into the Rack

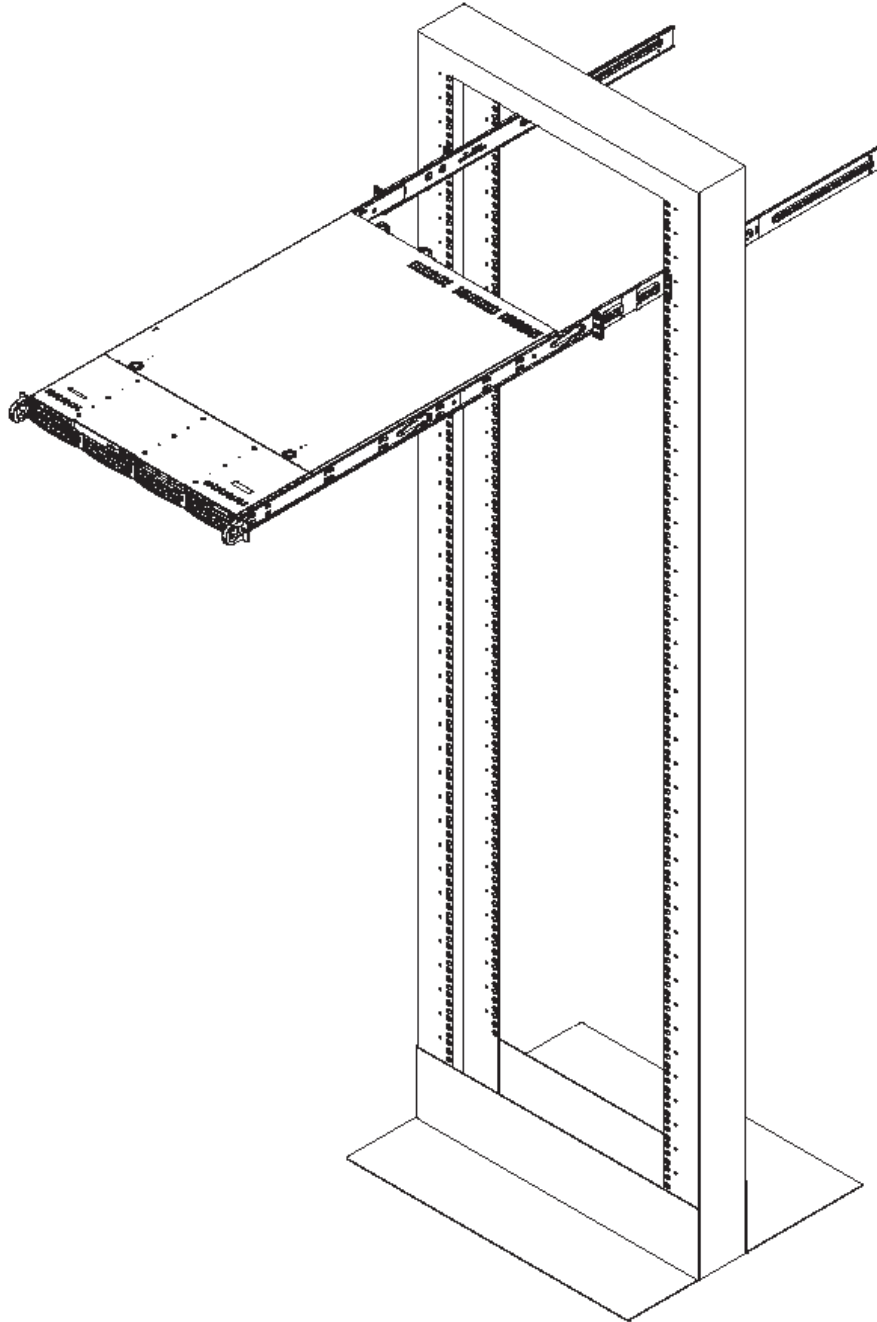
You should now have rails attached to both the chassis and the rack unit. The next step is to install the server chassis into the rack. Do this by lining up the rear of the chassis rails with the front of the rack rails. Slide the chassis rails into the rack rails, keeping the pressure even on both sides (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 8e6 server unit into a Telco type rack, use two L-shaped brackets on either side of the chassis (four total). First, determine how far forward 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.



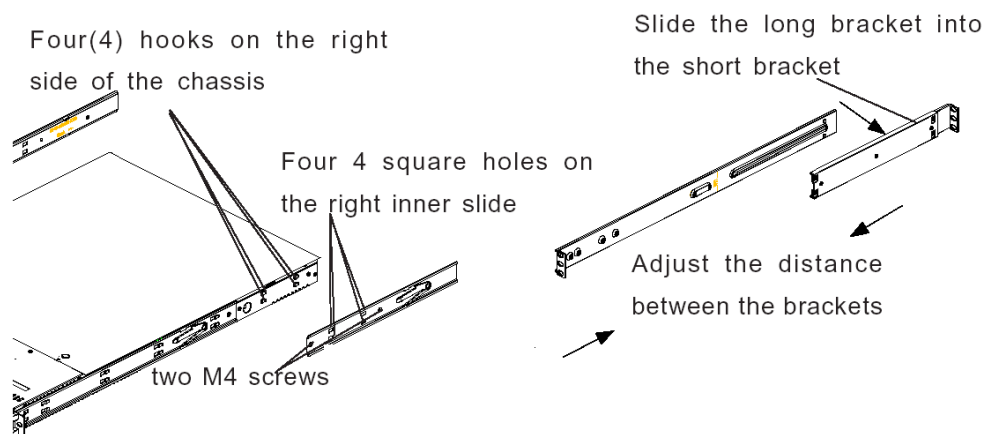
Rack Mount Instructions for SL Servers

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.

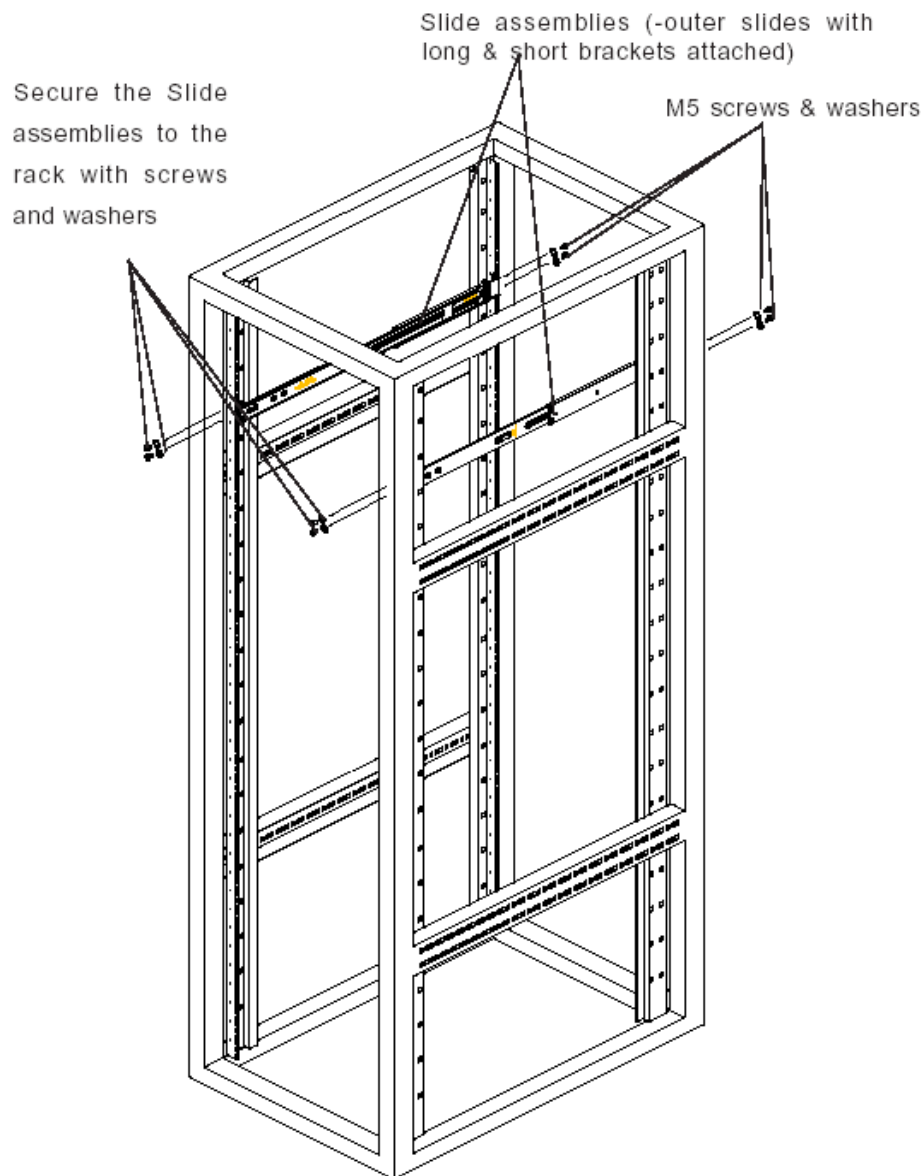


Install the Outer Slides

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.

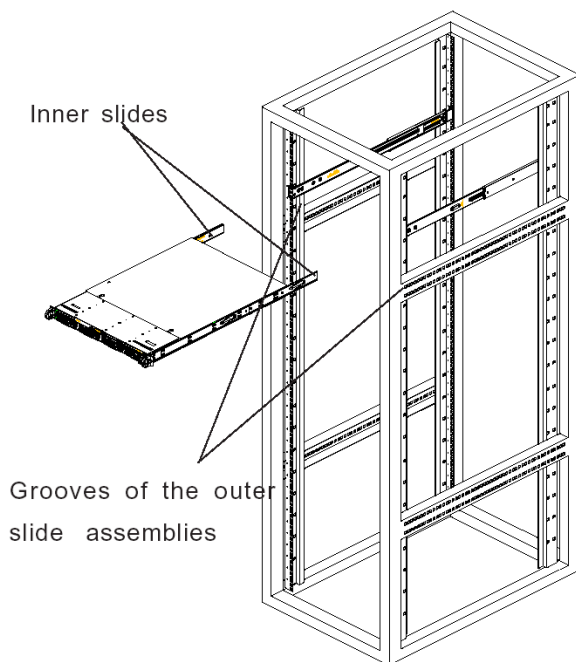
Install the Slide Assemblies to the Rack

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:

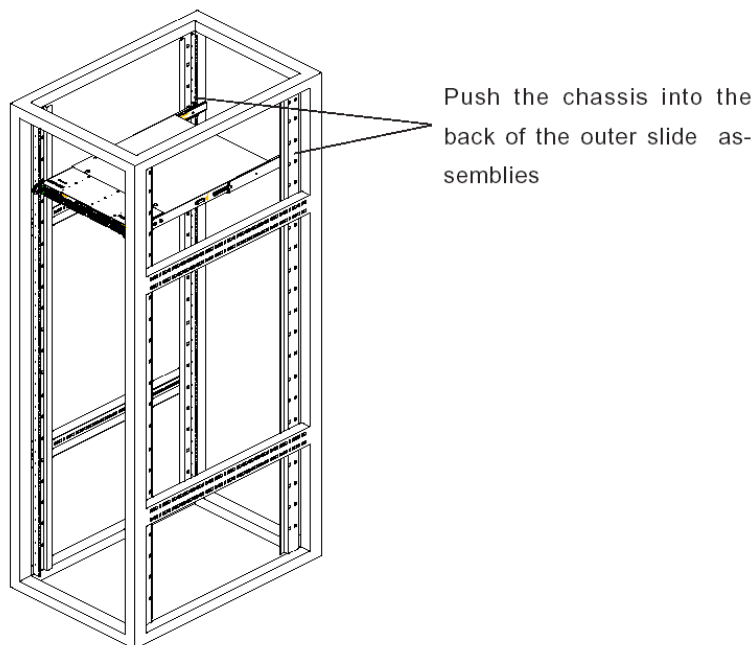


Install the Chassis into the Rack

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:

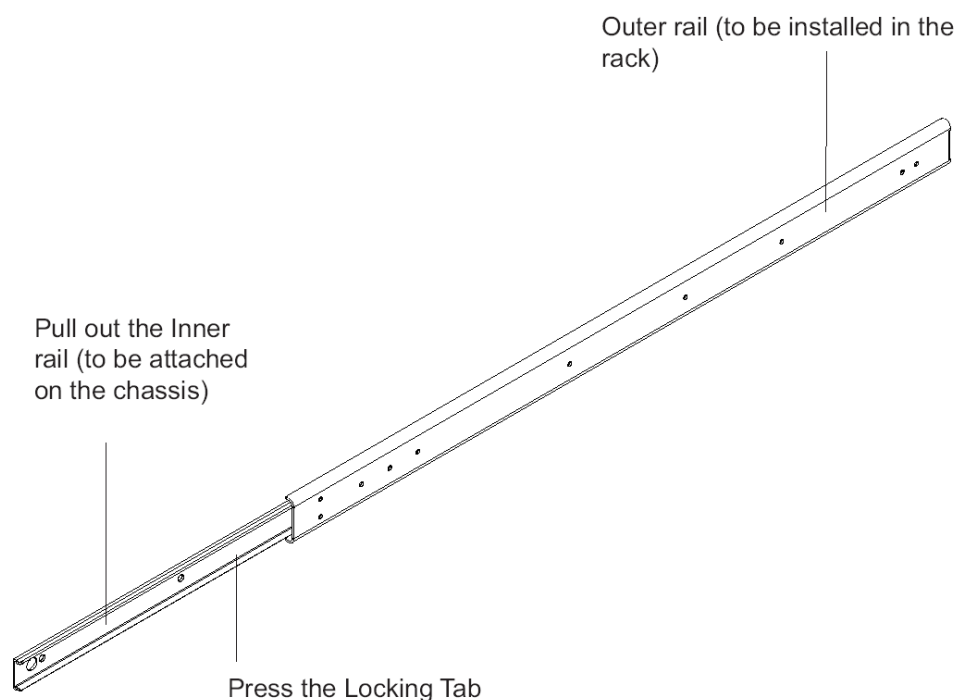
Before installing the chassis rails:

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

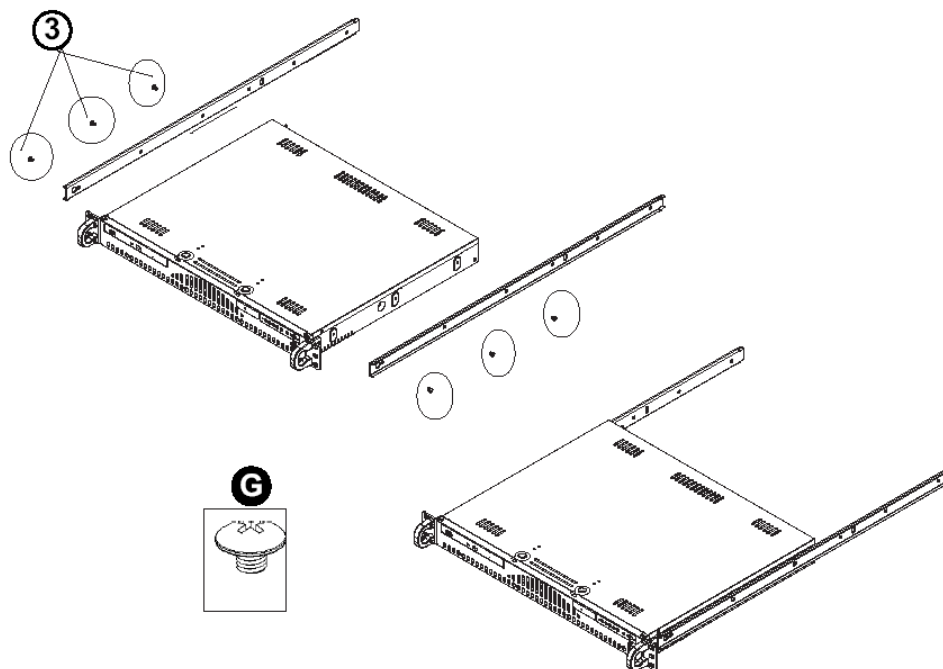
1. Included in the shipping package are a pair of rail assemblies. In each rail assembly, locate the inner rail and the outer rail.
2. Press the locking tab to release the inner rail from its locking position and pull out the inner rail from the rail assembly.



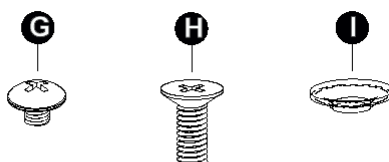
NOTE: The inner rails are to be attached to the chassis and the outer rails are to be installed in the rack.



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.

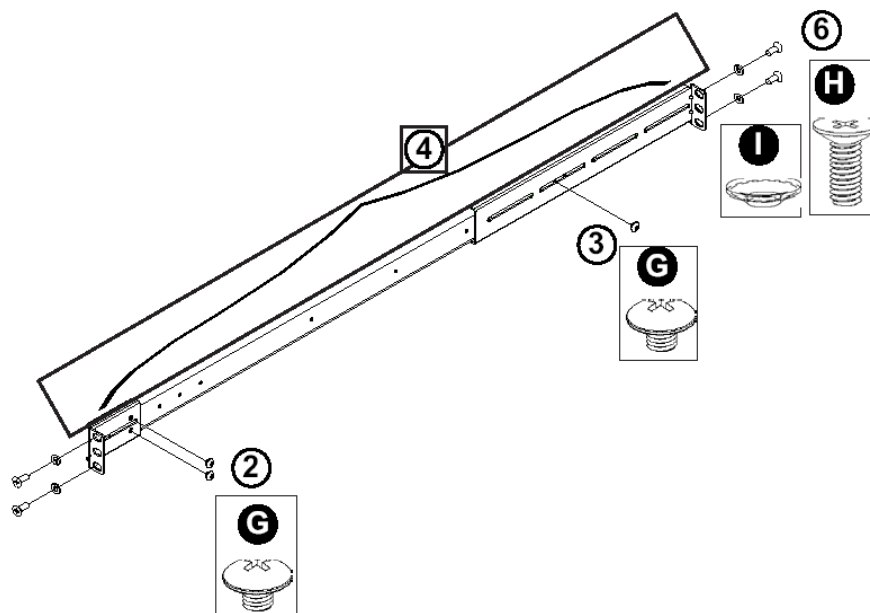
Optional: Install the Traditional UP Racks

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.)

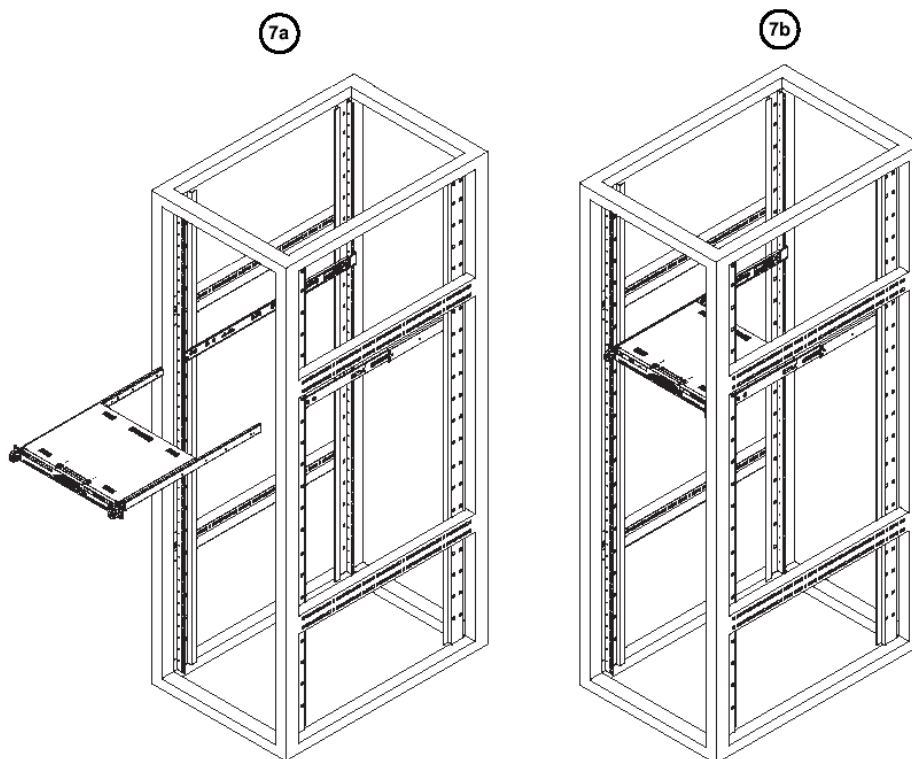


7. Slide the chassis into the rack as shown below.



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.



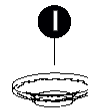
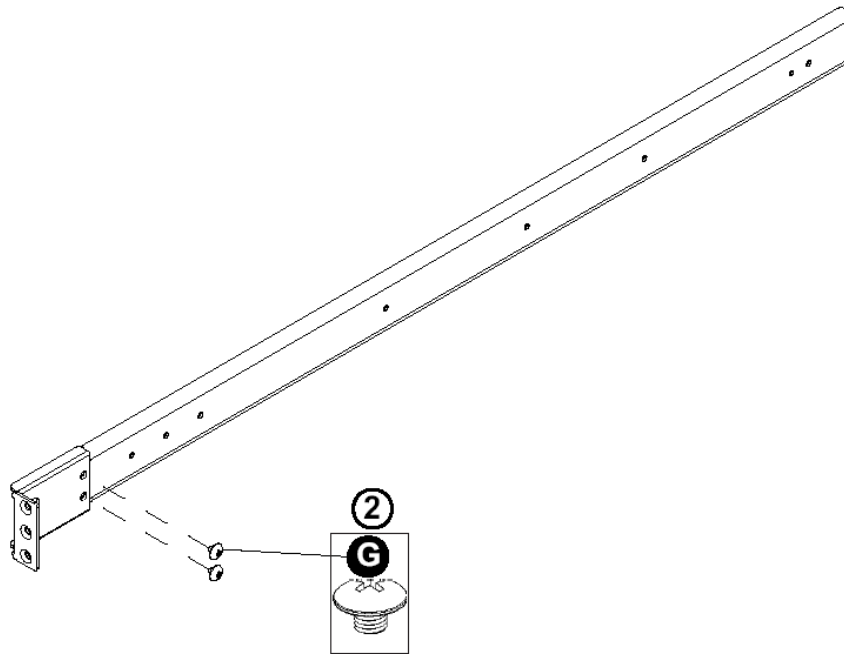
Optional: Install the Open Racks

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.

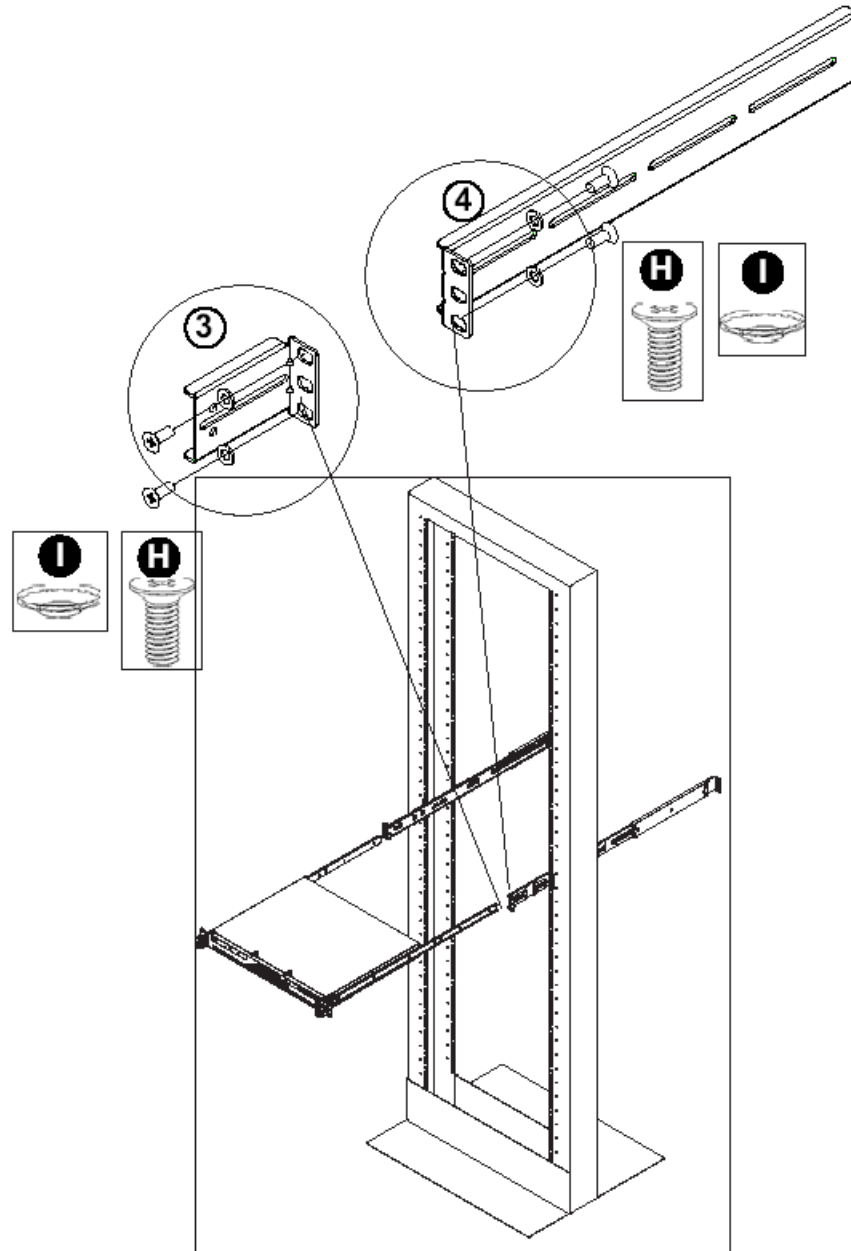


G. Round head M4 x 4 mm [0.157]

H. Flat head M5 x 12 mm [0.472]

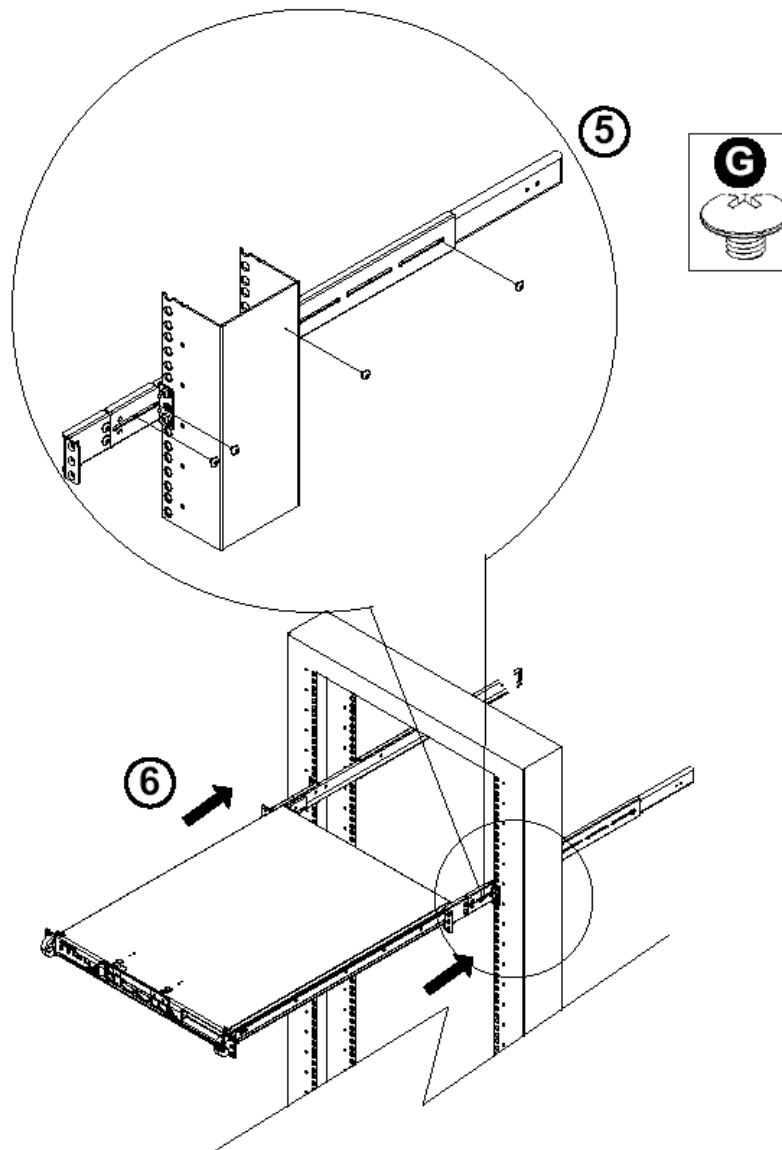
I. Washer for M5

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.



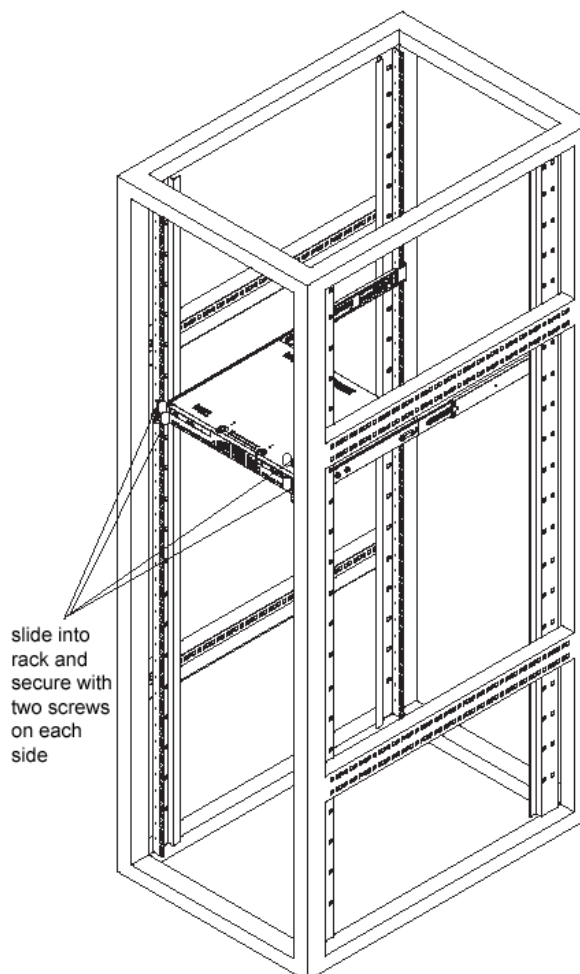
Install the Chassis into the Rack



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, 8e6 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:** *8e6 Technologies 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 8e6 Technologies 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 CONFORMÈMENT 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.

Quick Start Setup Requirements

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



NOTE: Before installing the Threat Analysis Reporter server, the R3000 server to be used with this server must already be installed and running software version 2.0.10 or higher.

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. 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. Power on the Threat Analysis Reporter by pressing the large button on 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

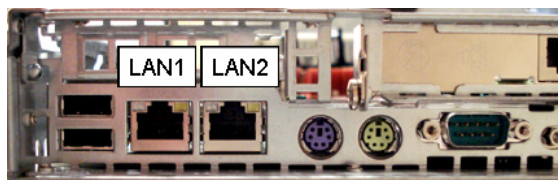


Fig. 2 - Portion of HL chassis rear

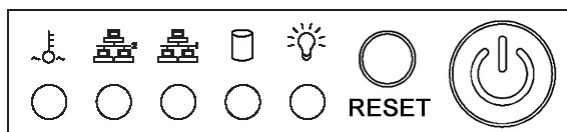


Fig. 3 - Diagram of SL chassis front panel, power button at far right

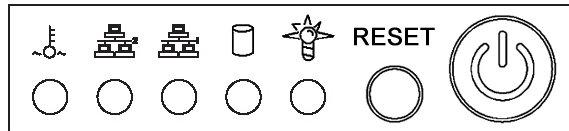


Fig. 4 - Diagram of MSA chassis front panel, power button at far right

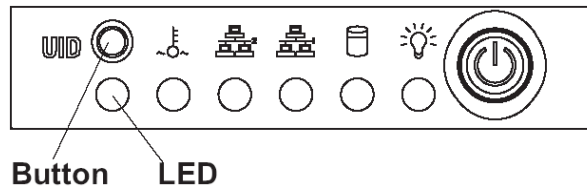


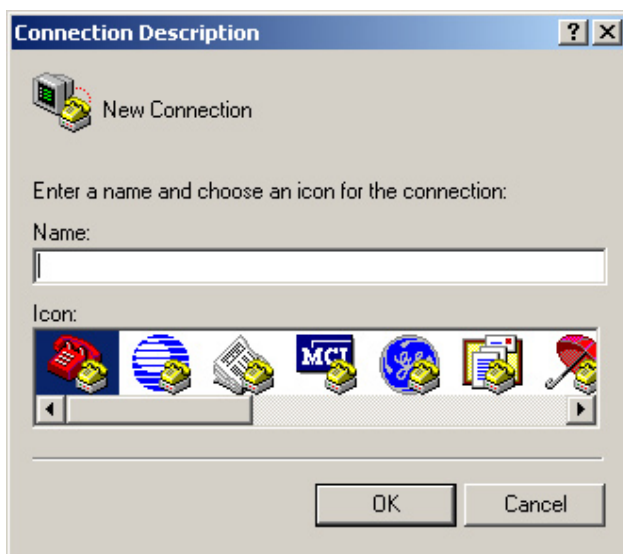
Fig. 5 - Diagram of HL chassis front panel, power button at far right

Once the Threat Analysis Reporter is powered up, proceed to the instructions for Hyper-Terminal Setup Procedures.

HyperTerminal Setup Procedures

If using a serial console, follow these procedures to create a HyperTerminal session on the serial console.

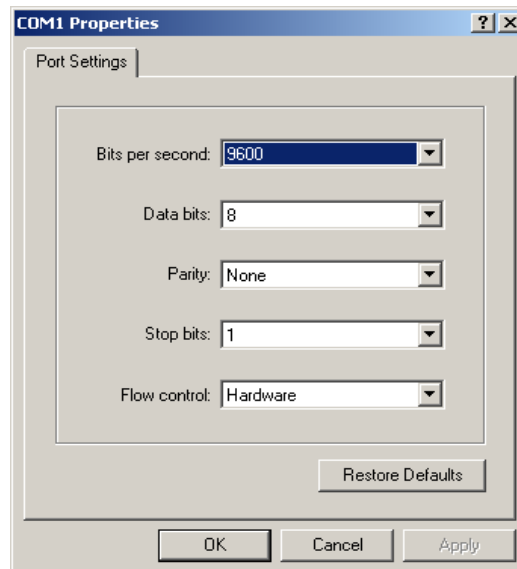
- A. Launch HyperTerminal by going to Start > Programs > Accessories > Communications > HyperTerminal:



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



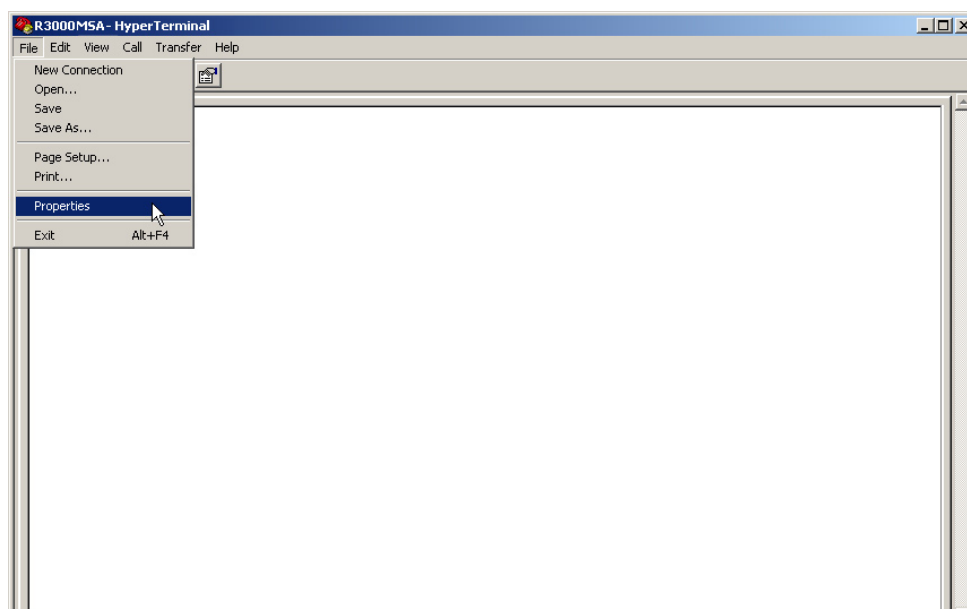
- C. At the **Connect using** field, select the COM port assigned to the serial port on the laptop (probably “COM1”), and then click **OK** to open the Properties dialog box, displaying the Port Settings tab:



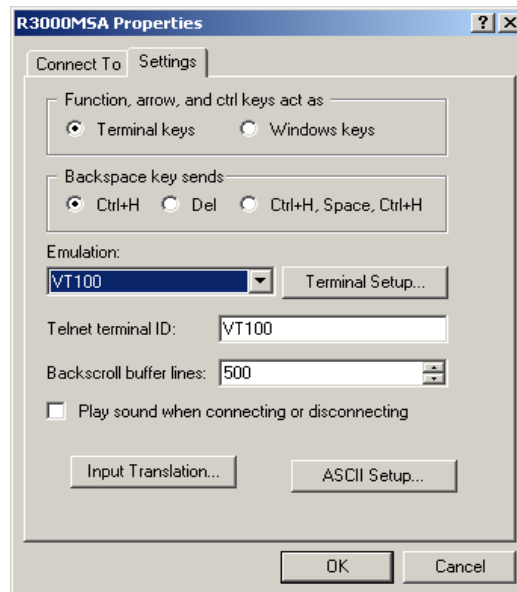
- D. Specify the following session settings:

- 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).

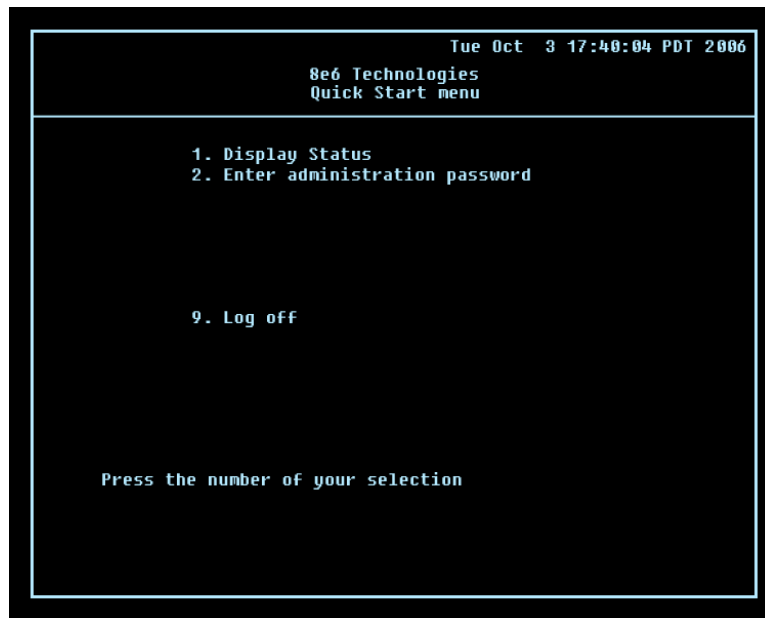
Login screen, password prompts

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

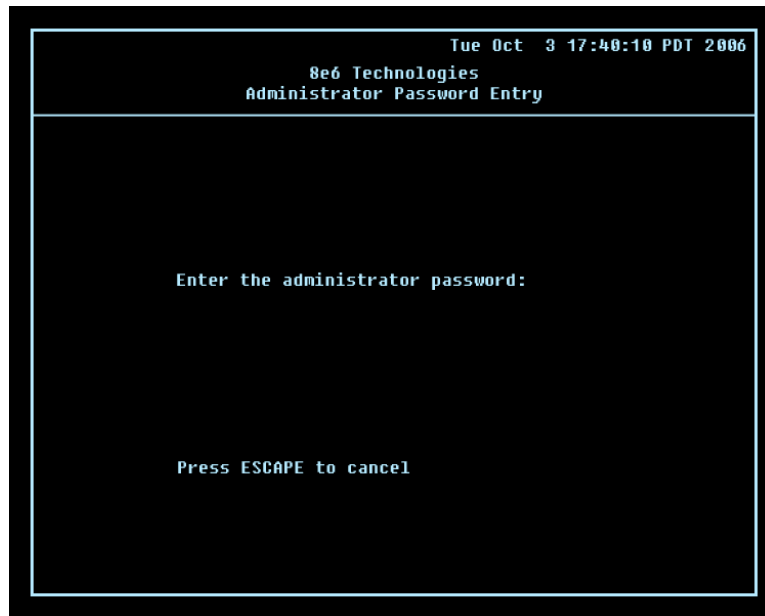


NOTE: If the screensaver currently displays on your screen, press the **Enter** key to display the login screen.

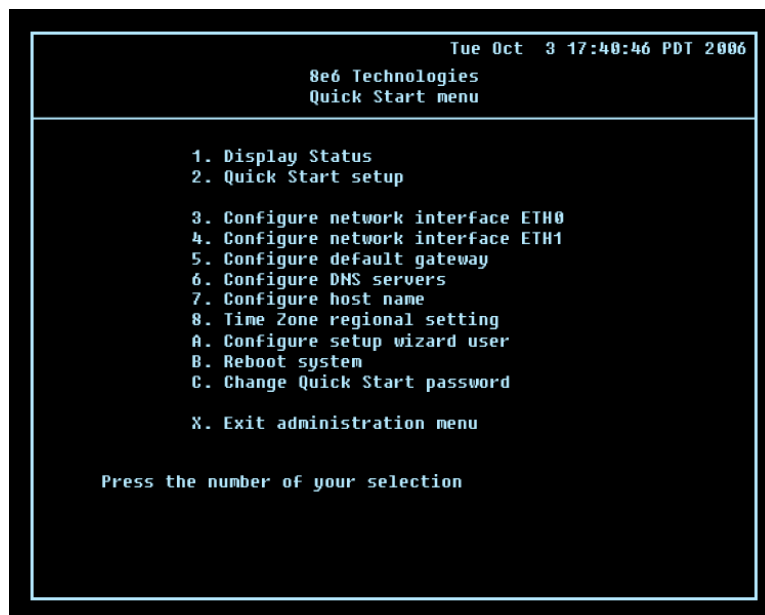
- A. At the **login** prompt, type in **menu**.
- B. Press the **Enter** key to display the Password prompt.
- C. At the **Password** prompt, type in the following: **#s3tup#r3k**
- D. Press **Enter** to display the Quick Start menu screen:



- E. At the **Press the number of your selection** prompt, press **2** to display the Administrator Password Entry screen:

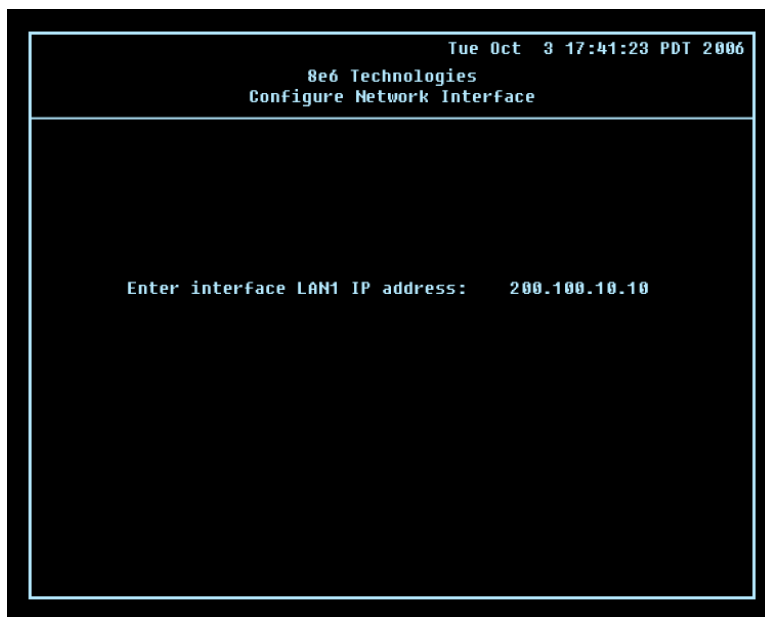


- F. At the **Enter the administrator password** prompt, re-enter your password: **#s3tup#r3k**
- G. Press **Enter** to display the Administration menu where you can begin the Quick Start setup process using the configuration screens:



- 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.

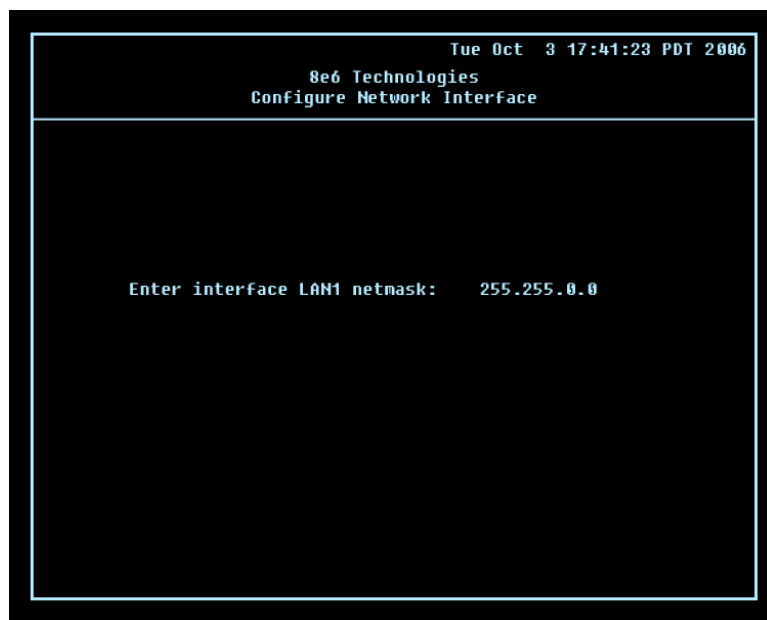
Configure Network Interface screen



Tue Oct 3 17:41:23 PDT 2006
8e6 Technologies
Configure Network Interface

Enter interface LAN1 IP address: 200.100.10.10

- 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.



Tue Oct 3 17:41:23 PDT 2006
8e6 Technologies
Configure Network Interface

Enter interface LAN1 netmask: 255.255.0.0

- 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.

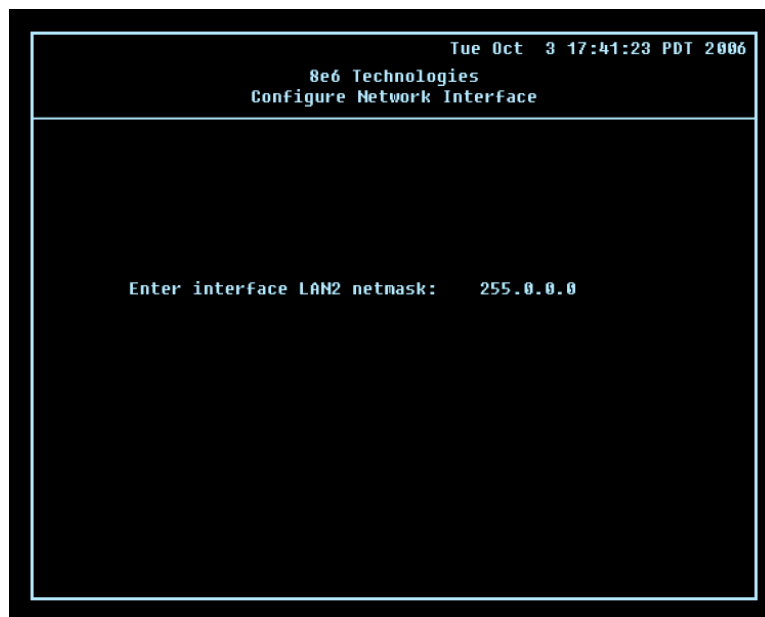


Tue Oct 3 17:41:23 PDT 2006

8e6 Technologies
Configure Network Interface

Enter interface LAN2 IP address: 1.2.3.4

- 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.



Tue Oct 3 17:41:23 PDT 2006

8e6 Technologies
Configure Network Interface

Enter interface LAN2 netmask: 255.0.0.0

- 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

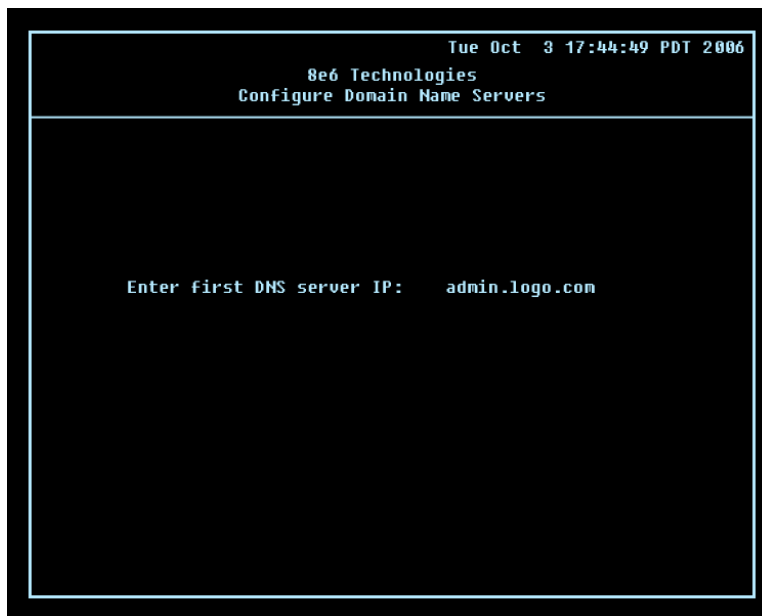


```
Tue Oct 3 17:44:06 PDT 2006
8e6 Technologies
Configure default gateway

Enter default gateway IP: 200.100.10.1
```

- 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.

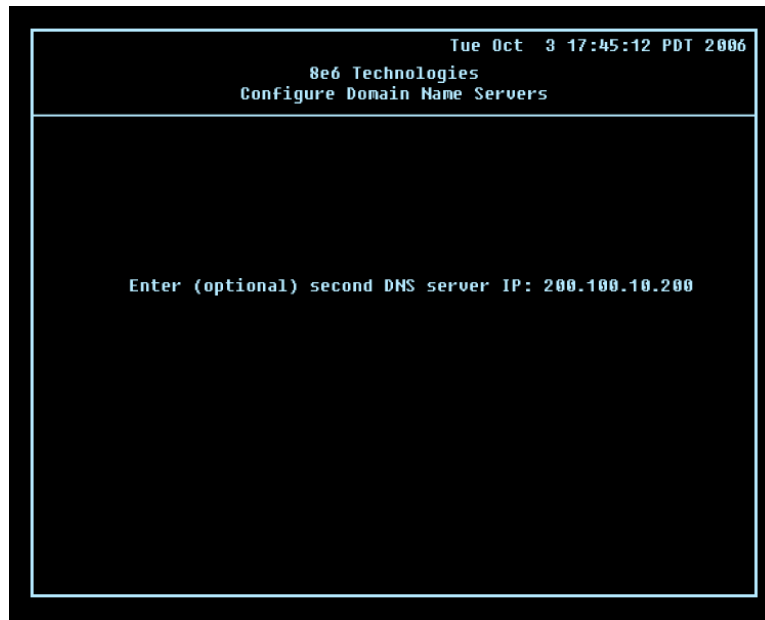
Configure Domain Name Servers screen



```
Tue Oct 3 17:44:49 PDT 2006
8e6 Technologies
Configure Domain Name Servers

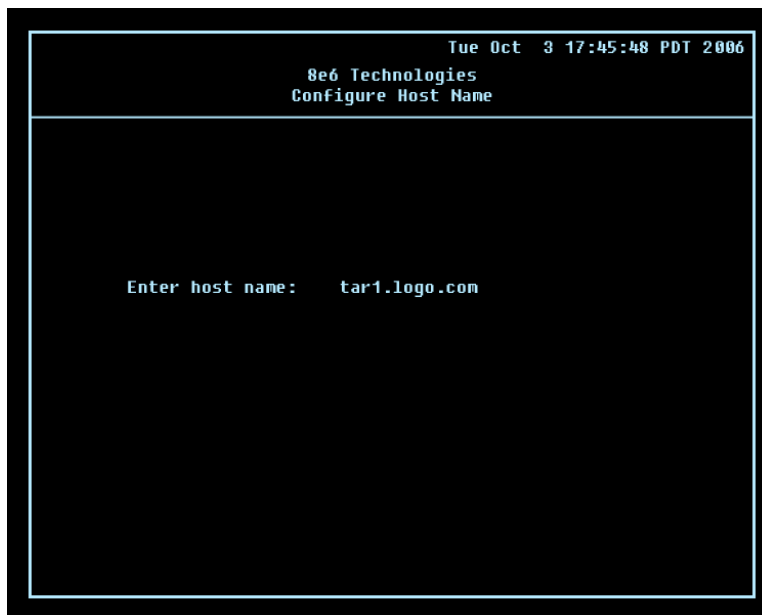
Enter first DNS server IP: admin.logo.com
```

- 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.

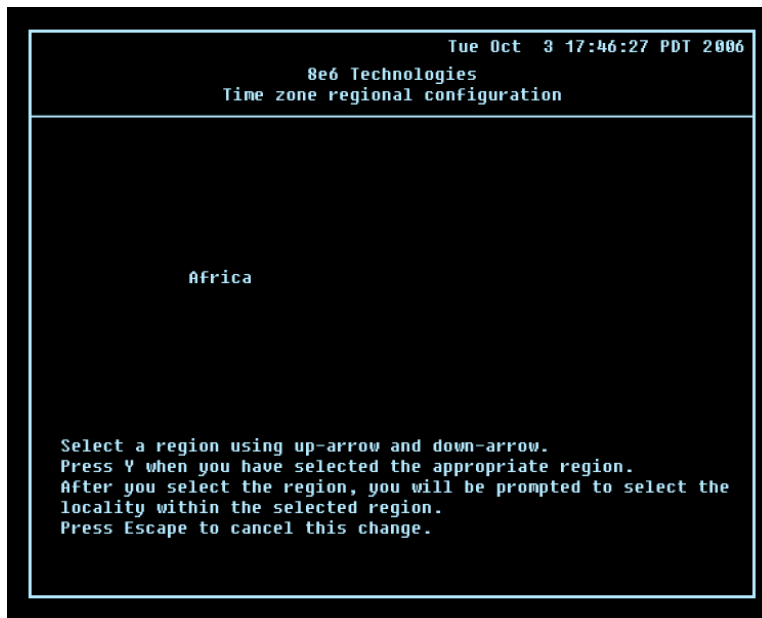
Configure Host Name screen



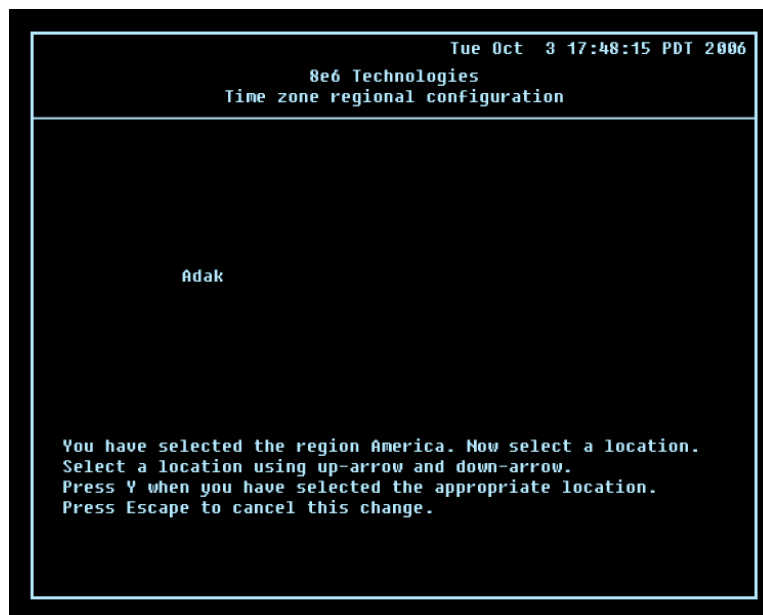
- A. At the **Enter host name** field, enter the host name of the server. Press **Enter** to display the confirmation prompt.

- 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.

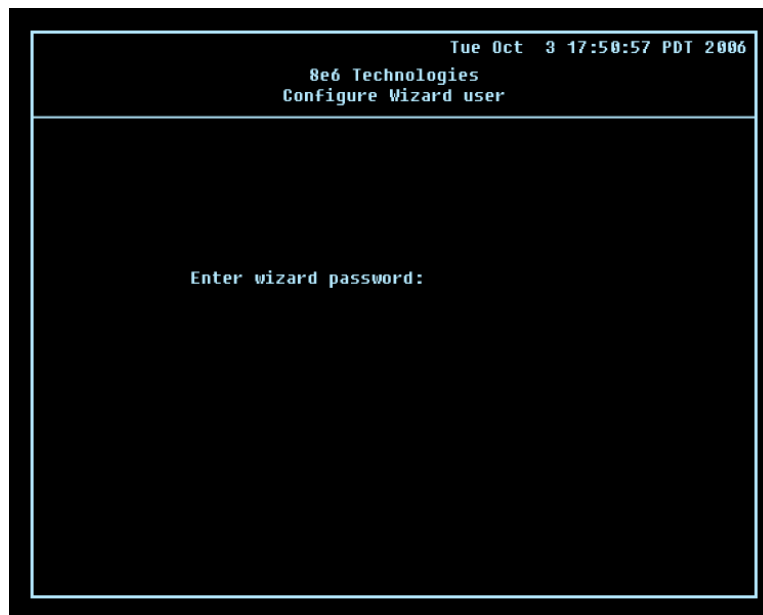
Configure Wizard user screen



```
Tue Oct 3 17:49:26 PDT 2006
8e6 Technologies
Configure Wizard user

Enter wizard user name: taruser
```

- 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.

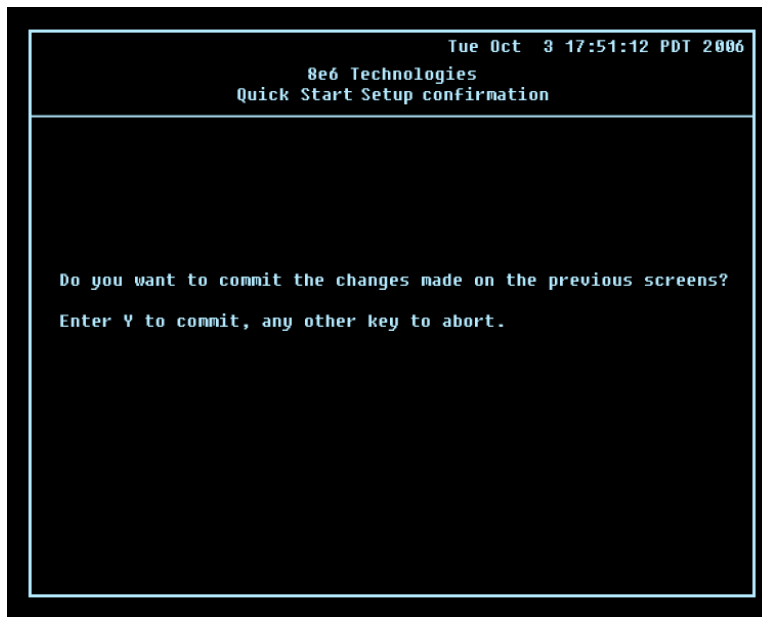


```
Tue Oct 3 17:50:57 PDT 2006
8e6 Technologies
Configure Wizard user

Enter wizard password:
```

- 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 Oct  3 17:40:04 PDT 2006
                        8e6 Technologies
                System Status - updates every 10 seconds

LAN1 interface for web access and R3000 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 R3000 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 Physically Connect the Unit to the Network.

Physically Connect the Unit to the Network

After performing initial setup procedures for the Threat Analysis Reporter, the unit should 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

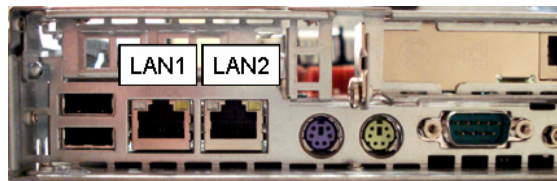


Fig. 2 - Portion of HL chassis rear

- B. Plug the other end of the CAT-5E cable into an open port on the network switch.

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 1B: LCD Panel Setup Procedures

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 with the following message:

8e6 Technologies

**Display Initializing
Please Wait**

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 "Database Status (Active, Inactive)".

8e6 menu

When "8e6 >" 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: *Navigation tips in the 8e6 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.

Current Patch Level

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

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
- Choose **Configure LAN 1 (2) IP** and press the checkmark key to go to the Configure LAN 1 (2) IP screen.
 - Use the up / down keys to increase / decrease the current value, and the left / right arrow keys to navigate across the line.
 - Press the checkmark key to accept your entry and to return to the previous screen.
 - Choose **Change LAN1 (2) Netmask** and press the checkmark key to go to the Change LAN1 (2) Netmask screen.
 - Use the up / down keys to increase / decrease the current value, and the left / right arrow keys to navigate across the line.
 - Press the checkmark key to accept your entry and to return to the previous screen.
 - Press the “X” key to return to the 8e6 menu.

Gateway

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

- Choose **Configure Gateway IP** and press the checkmark key to go to the Configure Gateway IP screen.
- 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 8e6 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 8e6 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 8e6 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 8e6 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 8e6 menu.
- Choose **Reset TAR setup wizard password** to reset the password and to return to the 8e6 menu.

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 8e6 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 8e6 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.

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.

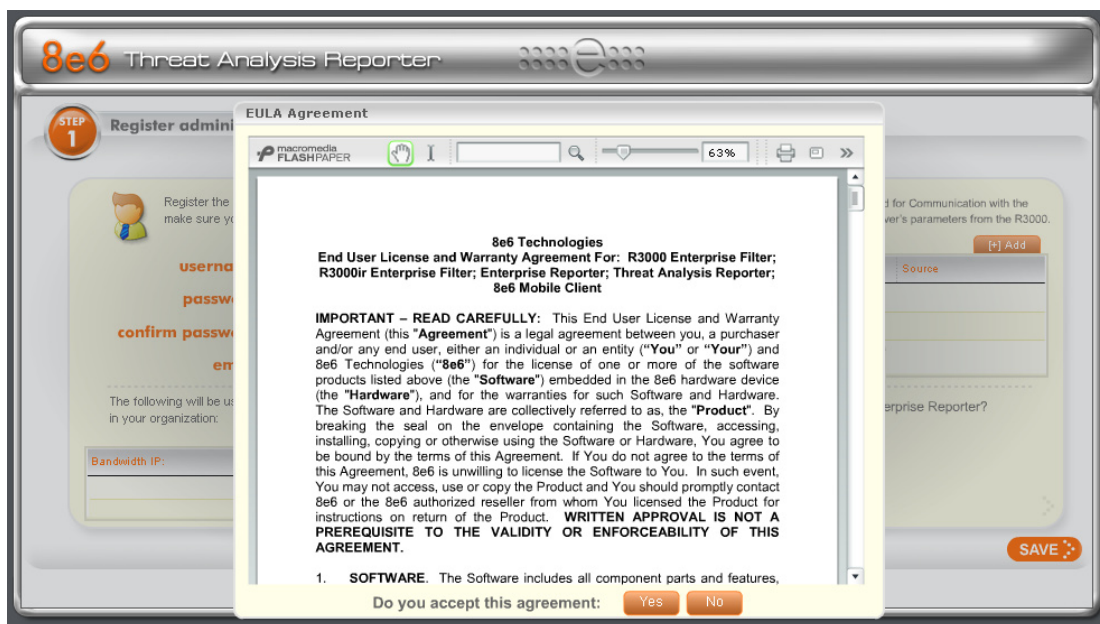
Step 2: Wizard Setup Procedures

For this step, you will need your network administrator to provide you the following information:

- IP range and netmask of machines on the network the Threat Analysis Reporter server will be monitoring
- R3000 IP address, and port number to be used between the R3000 and Threat Analysis Reporter
- 8e6 Enterprise Reporter server IP address and server name, if an ER unit is connected to the R3000

Access the Threat Analysis Reporter Administrator Console

- Launch Internet Explorer.
- In the address field, type in **http://x.x.x.x:8080/8e6tar/wizard.html** (in which “x.x.x.x” represents the eth0 (LAN1) IP address entered in the Connect Network Interface screen of the Quick Start Setup Procedures). In our example, this entry would be: **http://200.100.10.10:8080/8e6tar/wizard.html**.
- Click **Go** to open the Threat Analysis Reporter interface and the EULA Agreement dialog box:



- After reading the End User License Agreement, you have the option to do either of the following:
 - Click **No** to close both the EULA Agreement dialog box and the Threat Analysis Reporter interface. You will not be able to enable the Threat Analysis Reporter for use in your environment.

- Click **Yes** to close the EULA Agreement dialog box and to open the Login dialog box:

Proceed to the next sub-section: Log in to the Threat Analysis Reporter Wizard.

Log in to the Threat Analysis Reporter Wizard

- In the **Username** field of the Login dialog box, type in the username specified in the Configure Wizard user screen of the Quick Start Setup Procedures. In our example, this entry would be: **taruser**.
- In the **Password** field, type in the password specified in the Configure Wizard user screen of the Quick Start Setup Procedures.
- Click **LOGIN** to close the login dialog box and to go to Step 1 of wizard setup procedures in the Threat Analysis Reporter Wizard (see Wizard Step 1: Register administrator).

Wizard Step 1: Register administrator

Step 1 is performed in the left side of the first screen of the wizard:

8e6 Threat Analysis Reporter

STEP 1 Register administrator

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

username :

password :

confirm password :

email :

The following will be used to calculate the bandwidth monitoring in your organization:

Bandwidth IP:	Bandwidth Netmask:

[+] Add

STEP 2 Register R3000 & ER

R3000 // These settings are used for Communication with the TAR agent to retrieve the Patch Server's parameters from the R3000.

IP_Address	Server_Name	Source

[+] Add

ER // Do you have an Enterprise Reporter?

☐ Yes ☐ No

SAVE

Completed Steps 1 2 3

- 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 interface.
- Enter the **password** to be used with that username, and enter the same password again in the **confirm password** field.
- Enter the **email** address of the global administrator, who will be notified via email regarding system alerts.

D. Click the [+] Add tab below to open the IP Range Information dialog box:

The screenshot shows the 8e6 Threat Analysis Reporter interface. It has two main sections: STEP 1 Register administrator and STEP 2 Register R3000 & ER. In STEP 1, there are fields for username (jsmith23), password (masked), confirm password (masked), and email (jsmith23@logo.com). Below these is a section for bandwidth monitoring with fields for Bandwidth IP and Bandwidth Netmask, and a [+] Add button. An IP Range Information dialog box is open, showing the IP address 200.100.10.0 and Netmask 255.255.255.248. In STEP 2, there is a table for R3000 settings with columns IP_Address, Server_Name, and Source, and a [+] Add button. Below the table is a question: ER // Do you have an Enterprise Reporter? with Yes and No radio buttons. A SAVE button is at the bottom right. A progress bar at the bottom shows Completed Steps 1, 2, 3.

E. Enter the **Bandwidth IP** address range for the bandwidth the Threat Analysis Reporter will monitor.

F. Enter the **Bandwidth Netmask** for the bandwidth IP range to be monitored, using the dotted decimals notation format.

G. Click **OK** to close the dialog box and to display your entries in the list box:

This screenshot shows the same interface as the previous one, but the IP Range Information dialog box is closed. In the STEP 1 section, the Bandwidth IP field now contains 200.100.10.0 and the Bandwidth Netmask field contains 255.255.255.248. The rest of the interface remains the same.

 **NOTE:** Additional Bandwidth IP address ranges can be included by clicking the [+] Add tab again and making the entries described in steps E through G above.

To modify an IP address range, double-click the entry in the list box to highlight it and to display the [-] Remove tab to the left of the [+] Add tab:

The screenshot shows the 8e6 Threat Analysis Reporter (TAR) interface. The title bar reads "8e6 Threat Analysis Reporter". The interface is divided into two main sections: "STEP 1 Register administrator" and "STEP 2 Register R3000 & ER".

STEP 1 Register administrator: This section contains a registration form for the first administrator. It includes fields for "username" (jsmith23), "password" (masked with asterisks), "confirm password" (masked with asterisks), and "email" (jsmith23@logo.com). Below the form, there is a note: "The following will be used to calculate the bandwidth monitoring in your organization:". Below this note is a table with two columns: "Bandwidth IP:" and "Bandwidth Netmask:". The table contains two rows: "200.100.10.0" and "255.255.255.248", and "200.100.10.10" and "255.255.255.248". Above the table are buttons for "[-] Remove" and "[+] Add".

STEP 2 Register R3000 & ER: This section contains a registration form for the R3000 agent and the Enterprise Reporter (ER). It includes a table with three columns: "IP_Address", "Server_Name", and "Source". Above the table is a button for "[+] Add". Below the table is a section for the ER, with a question: "ER // Do you have an Enterprise Reporter?". Below this question are two radio buttons: "Yes" and "No". At the bottom right of the section is a "SAVE" button.

At the bottom of the interface, there is a "Completed Steps" section with three steps: 1, 2, and 3. Step 1 is highlighted, indicating it is the current step.

- To modify the entries made for the IP address range, click the [+] Add tab to re-open the IP Range Information dialog box and edit information, as necessary. Click **OK** to close the dialog box and to display the modified information in the list box.
- To remove the entry for the IP address range from the list box, click the [-] Remove tab. Click the [+] Add tab to open the IP Range Information dialog box and make new entries for the IP address range.

Wizard Step 2: Register R3000 & ER

Step 2 is performed in the right side of the first screen of the wizard.

R3000:

Specify information for the R3000 to be used with the Threat Analysis Reporter:

- A. Click the [+] Add tab above the R3000 list box to open the R3000 Information dialog box:



- B. Enter the **IP address** of the R3000 server to be used with the Threat Analysis Reporter. In our example, this is: **200.100.160.74**, which is the LAN 2 IP address of the R3000 server.
- C. Enter the **Server Name** of the R3000 to be used with the Threat Analysis Reporter, which is any name you wish to associate with that R3000. In our example, this is: **R3000LOGO**.
- D. Respond to the question “Is this your Source R3000?” by clicking the “Yes” checkbox, if this R3000 will be designated the primary R3000 to be associated with the Threat Analysis Reporter. Otherwise, leave the checkbox blank.

E. Click **OK** to close the dialog box and to display your entries in the list box:

8e6 Threat Analysis Reporter

STEP 1 Register administrator

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

username : jsmith23
 password : *****
 confirm password : *****
 email : jsmith23@logo.com

The following will be used to calculate the bandwidth monitoring in your organization:

Bandwidth IP:	Bandwidth Netmask:
200.100.10.10	255.255.255.248

[+] Add

STEP 2 Register R3000 & ER

R3000 // These settings are used for Communication with the TAR agent to retrieve the Patch Server's parameters from the R3000.

IP_Address	Server_Name	Source
200.100.160.74	R3000LOGO	Source

[+] Add

ER // Do you have an Enterprise Reporter?

☐ Yes ☐ No

SAVE

Completed Steps 1 2 3

NOTE: Additional R3000 servers can be included by clicking the [+] Add tab again and making the entries described in steps A through E above.

To modify an R3000 entry, double-click the R3000 entry in the list box to highlight it and to display the Set as Source tab and the [-] Remove tab to the left of the [+] Add tab:

8e6 Threat Analysis Reporter

STEP 1 Register administrator

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

username : jsmith23
 password : *****
 confirm password : *****
 email : jsmith23@logo.com

The following will be used to calculate the bandwidth monitoring in your organization:

Bandwidth IP:	Bandwidth Netmask:
200.100.10.10	255.255.255.248

[+] Add

STEP 2 Register R3000 & ER

R3000 // These settings are used for Communication with the TAR agent to retrieve the Patch Server's parameters from the R3000.

Set as Source [-] Remove [+] Add

IP_Address	Server_Name	Source
200.100.160.74	R3000LOGO	Source
200.100.160.77	R3000LOGO2	Source

[+] Add

ER // Do you have an Enterprise Reporter?

☐ Yes ☐ No

SAVE

Completed Steps 1 2 3

- To modify the IP address and Server Name for the R3000 server, click the [+] Add tab to re-open the R3000 Information dialog box, and edit information as necessary. Click **OK** to close the dialog box and to display the modified information in the list box.
- To designate an R3000 as the Source R3000 server, click the entry for the R3000 server in the list box to highlight it, and then click the Set as Source tab to display “Source” in the Source column for that entry in the list box.
- To remove the entry for the R3000 server from the list box, click the [-] Remove tab.

8e6 Threat Analysis Reporter

STEP 1 Register administrator

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

username : jsmith23

password : *****

confirm password : *****

email : jsmith23@logo.com

The following will be used to calculate the bandwidth monitoring in your organization:

Bandwidth IP:	Bandwidth Netmask:
200.100.10.10	255.255.255.248

[+] Add

STEP 2 Register R3000 & ER

R3000 // These settings are used for Communication with the TAR agent to retrieve the Patch Server's parameters from the R3000.

IP_Address	Server_Name	Source
200.100.160.74	R3000LOGO	Source

[+] Add

ER // Do you have an Enterprise Reporter?

☐ Yes ☐ No

SAVE

Completed Steps 1 2 3

ER:

Respond to the question “Do you have an Enterprise Reporter?” by clicking the radio button corresponding to either “Yes” or “No”.

- If “No” was selected, click **SAVE >** at the bottom right of the screen to go to Step 3.
- If “Yes” was selected, the IP address and Server Name fields display in place of the radio buttons. The < Back button displays above the Server Name field.

8e6 Threat Analysis Reporter

STEP 1 Register administrator

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

username : jsmith23

password : *****

confirm password : *****

email : jsmith23@logo.com

The following will be used to calculate the bandwidth monitoring in your organization:

Bandwidth IP:	Bandwidth Netmask:
200.100.10.10	255.255.255.248

STEP 2 Register R3000 & ER

R3000 // These settings are used for Communication with the TAR agent to retrieve the Patch Server's parameters from the R3000.

IP_Address	Server_Name	Source
200.100.160.74	R3000LOGO	Source

ER // Do you have an Enterprise Reporter?

IP address : 200 . 10 . 101 . 76

Server Name: er4logo

SAVE >

Completed Steps 1 2 3

NOTE: To change your answer from “Yes” to “No,” click the < **Back** button to re-display the question “Do you have an Enterprise Reporter?”

- Enter the **IP address** of the ER server to be used with the Threat Analysis Reporter. In our example, this is: **200.10.101.76**.
- Enter the **Server Name** of the ER server to be used with the Threat Analysis Reporter. In our example, this is: **er4logo**.
- Click **SAVE >** at the bottom right of the screen to save all settings entered during the wizard process, and to go to Step 3.

NOTE: Upon clicking **SAVE >** the wizard will verify whether the settings made in Step 1 and Step 2 are correct. If there is an error in any entry made, an orange asterisk flashes beside the field in which the error was made. Correct the error and click **SAVE >** again to go to Step 3.

Step 3: Server Settings

Step 3, the following R3000 server information displays: SMTP Server Settings, Patch Server Settings, PROXY Server Settings, NTP Server Settings:

8e6 Threat Analysis Reporter

STEP 3 Server Settings

SMTP Server Settings :

SMTP [r3214]
 SMTP_Host: popmail.LOGO.com
 SMTP_Port: 25
 SMTP_Base: false
 SMTP_DC: 50

PROXY Server Settings :

Proxy Server [r3214]
 PROXY_Switch: on
 PROXY_Server: 102.108.20.0
 PROXY_Username: test
 PROXY_password: *****
 PROXY_Port: 3128

Patch Server Settings :

Patch Server [r3214]
 PATCH_Server: 200.10.101.104
 PATCH_Username: prodcom
 PATCH_password: *****
 HTTPS: on
 Transfer_Mode: passive

NTP Server Settings :

NTP Server [r3214]
 NTP_Server: 102.108.20.1

PRINT LOGIN

Completed Steps 1 2 3

After reviewing the information in this screen, the following actions can now be performed:

- To print this information, click the **PRINT** button.
- Click **LOGIN** to close the wizard and to open the login dialog box of the Threat Analysis Reporter interface so you can begin using the application.



NOTE: To shut down the Threat Analysis Reporter server, press the power button on the front of the unit to turn off the machine.

CONCLUSION

Congratulations; you have completed the Threat Analysis Reporter quick start 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.8e6.com/docs/tar_ug.pdf**.

 **IMPORTANT:** 8e6 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

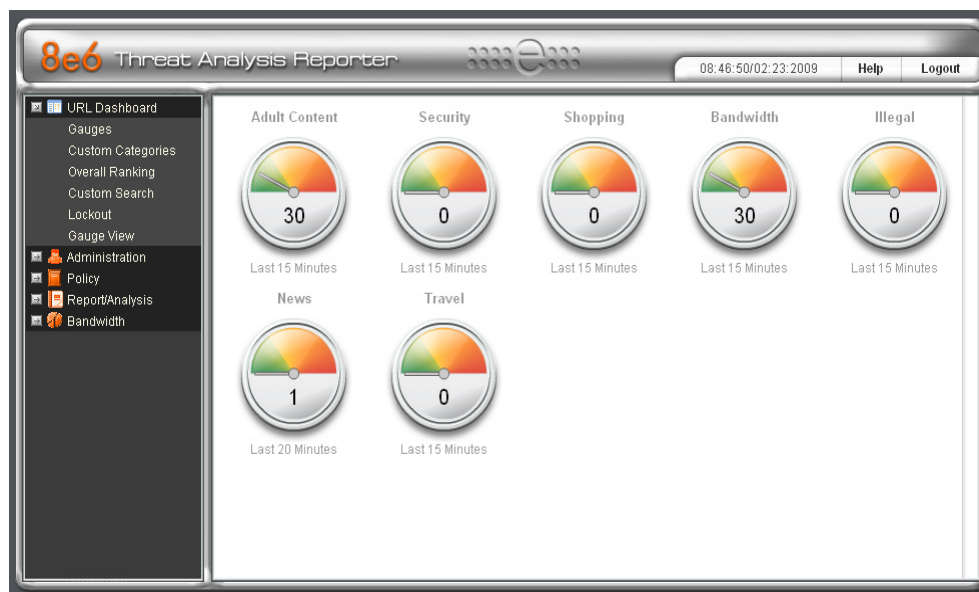
This collection of setup and usage scenarios is designed to help you understand and use basic tools in the console for enforcing your Internet usage policy. Each scenario is followed by console setup information. Please consult the “How to” section in the index of the Threat Analysis Reporter User Guide 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 five sections of the interface and inform you where to go to customize the application to perform a specified task or function.

Step A: Navigate screens and windows of the URL Dashboard menu

The URL Dashboard displays by default after you log into the console. This screen is comprised of a left panel with five menu topics, each with sub-topics used for accessing windows in the application, and a right 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, which is based on factors such as the activities of end users who visited URLs listed in library categories that comprise the gauge, and the threat score assigned to these library categories.

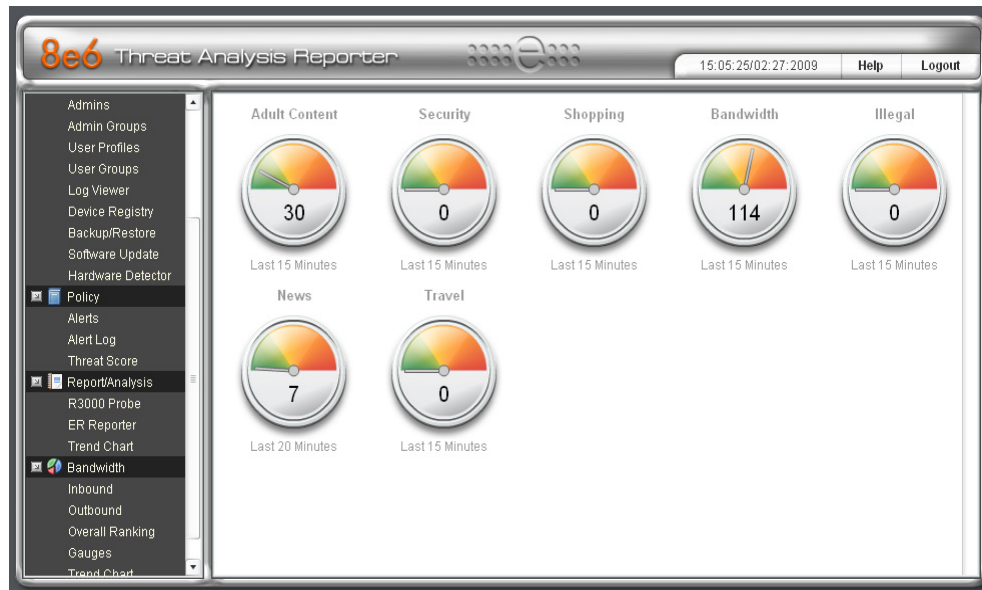
Click any of the menu items to open pop-up windows for configuring URL gauges:

- **Gauges** - create and maintain gauges used for monitoring end users' Internet activity
- **Custom Categories** - maintain the list of custom library categories to be used by gauges, and synchronize the source R3000's custom categories with the Threat Analysis Reporter
- **Overall Ranking** - view details about current gauge activity for all end users affecting gauges
- **Custom Search** - view a list of end users who accessed a specified library category
- **Lockout** - prevent the end user from accessing specified URLs, the Internet, or the entire network

- **Gauge View** - customize the view to only show certain URL gauges and their associated library categories

Step B: Navigate Administration section windows

Click Administration to open its menu. Click any of the menu items to open pop-up windows for configuring profiles and maintaining the server:



- **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 Profiles** - manage a list of end users' logged events
- **User Groups** - manage user groups whose activity will be monitored by gauges
- **Log Viewer** - view a list of alert records for the most recent 24-hour time period
- **Device Registry** - view information about devices connected to the Threat Analysis Reporter, synchronize the server with user groups and libraries from the source R3000, edit 8e6 appliance criteria, and add or delete an R3000 or ER
- **Backup/Restore** - perform a backup and/or restoration on the server
- **Software Update** - update the server with the latest software version
- **Hardware Detector** - maintain the health of a Threat Analysis Reporter server with RAID installed

Step C: Navigate Policy section windows

Click Policy to open its menu. Click any of the menu items to open pop-up windows 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 Log** - view a list of alert records for the most recent 24-hour time period
- **Threat Score** - manage the severity levels for library categories

Step D: Navigate Report/Analysis section windows

Click Report/Analysis to open its menu. Click any of the menu items to open new browser windows or pop-up windows to access appliances connected to the Threat Analysis Reporter, or to generate a report showing activity in all URL gauges:

- **R3000 Probe** - access the R3000 application's Real Time Probe feature that lets you monitor end user Internet usage in real time to verify whether the Internet is being used appropriately
- **ER Reporter** - access the ER application to generate reports on end user Internet activity
- **Trend Chart** - view a graphical depiction of activity for URL gauges

Step E: Navigate Bandwidth section windows

Click Bandwidth to open its menu. Click any of the menu items to open pop-up windows for monitoring bandwidth gauges:

- **Inbound** - view a graphical depiction of inbound activity for bandwidth protocol gauges
- **Outbound** - view a graphical depiction of outbound activity for bandwidth protocol gauges
- **Overall Ranking** - view information on gauges affected by a specified end user
- **Gauges** - monitor and manage bandwidth gauges for inbound and outbound traffic
- **Trend Chart** - view a graphical depiction of activity for 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.



In the Threat Analysis Reporter User Guide index, see:

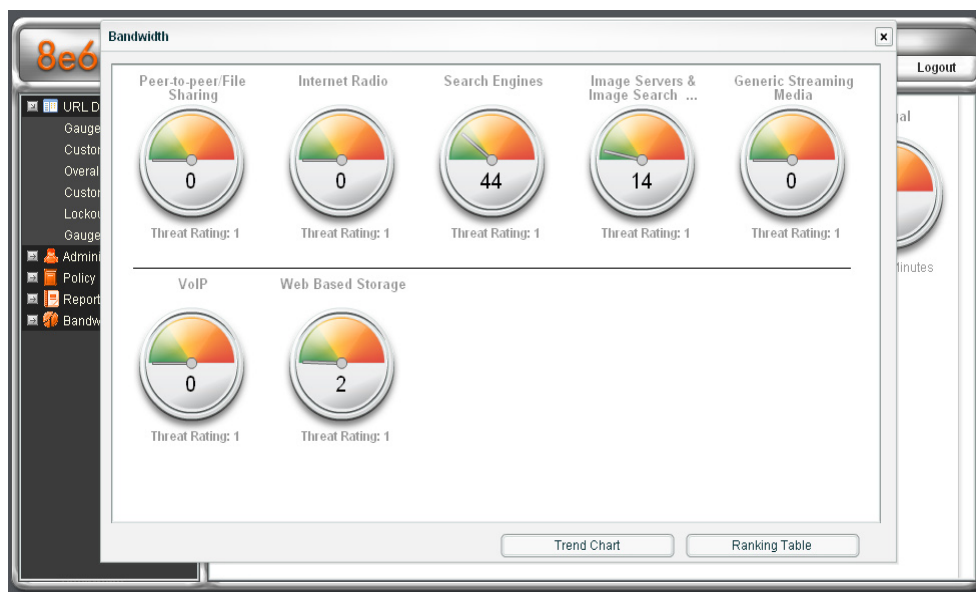
- *How to: navigate the interface*

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 double-click it to open a pop-up window with "child" gauges corresponding to library categories that comprise the "parent" gauge:



2. Find the child gauge with the highest score and double-click it to open a pop-up window that shows the scores of users affecting that gauge's score, ranked in order by the highest to lowest score:

The screenshot shows a pop-up window titled 'Search Engines'. It contains a table with two columns: 'Name' and 'Score'. The table lists the following data:

Name	Score
202.168.200.76	22
202.168.200.74	20
QAtsun	1
Goa	1

At the bottom of the window are navigation arrows and two buttons: 'URL Details' and 'User Summary'.

Now that you've identified the users affecting the highest scoring child gauge, next you will investigate the activity of the top user who is driving that 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 child gauge, return to the child gauge's pop-up window that lists users and their scores. Select the top user and then click **URL Details** to open the View Details pop-up window:

URL	Timestamp
http://www.google.com/url?sa=T&source=web&ct=res&cd=1&url=http://www.ocregister.com	2009-02-23 08:50:05
http://www.google.com/csi?v=3&s=GWS&action=search&tran=undefined&ei=ttOISbLNHpg	2009-02-23 08:50:05
http://www.google.com/search?q=ocregister&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-U	2009-02-23 08:50:00
http://suggestqueries.google.com/complete/search?output=firefox&client=firefox&hl=en-US	2009-02-23 08:50:00
http://www.google.com/url?sa=T&source=web&ct=res&cd=1&url=http://money.cnn.com/&ei	2009-02-23 08:49:20
http://www.google.com/csi?v=3&s=GWS&action=search&tran=undefined&ei=idOISd-KLaC	2009-02-23 08:49:15
http://www.google.com/search?q=cnn+money&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-	2009-02-23 08:49:15
http://suggestqueries.google.com/complete/search?output=firefox&client=firefox&hl=en-US	2009-02-23 08:49:15
http://fe.shortcuts.search.yahoo.com/modules/validate?id=hw_1235407610_1&entity=Mardi	2009-02-23 08:46:59
http://www.google.com/url?sa=T&source=web&ct=res&cd=1&url=http://mail.yahoo.com/&ei	2009-02-23 08:45:45
http://www.google.com/csi?v=3&s=GWS&action=search&tran=undefined&ei=tdKISayLipGL	2009-02-23 08:45:45
http://www.google.com/search?hl=en&q=yahoo+mail&btnG=Google+Search&aq=1&oq=ya	2009-02-23 08:45:45
http://clients1.google.com/generate_204	2009-02-23 08:45:26

Open URL

2. This window lists the user's visited URLs that are included in the library category corresponding to the child gauge. Choose a URL you wish to view, and then click **Open URL** 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.

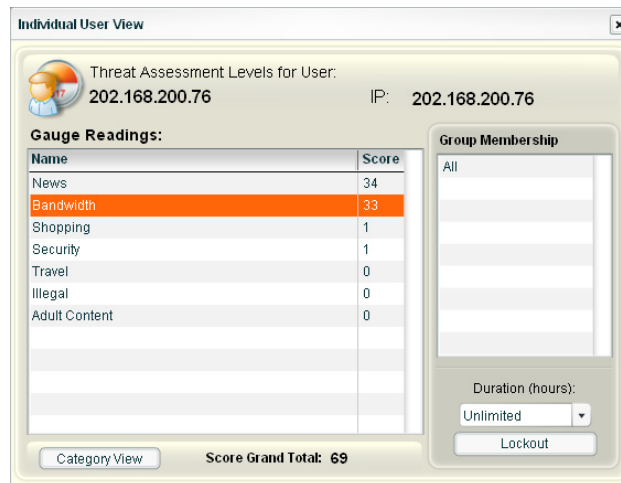


In the Threat Analysis Reporter User Guide index, see:

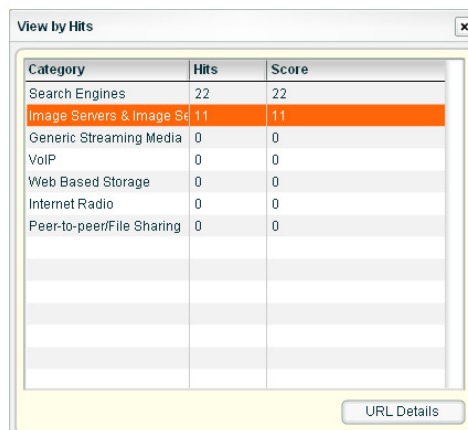
- *How to: view URLs a user visited*

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

1. To find out which other gauges the same user is currently affecting, in the child gauge's pop-up window—the one in which you previously clicked the URL Details button—with the same user still selected, click **User Summary** to open the Individual User View pop-up window:



2. Choose a parent gauge from this list box and then click **Category View** to open the View by Hits pop-up window:



This window shows you a list of library categories that comprise the parent gauge, and the user's corresponding hits and scores in each category.

3. To find out which URLs the user is viewing in a particular library category, choose the category from the list and then click **URL Details** to open the View Details pop-up window again that shows you a list of URLs you can view.



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 view parent and child gauges 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.

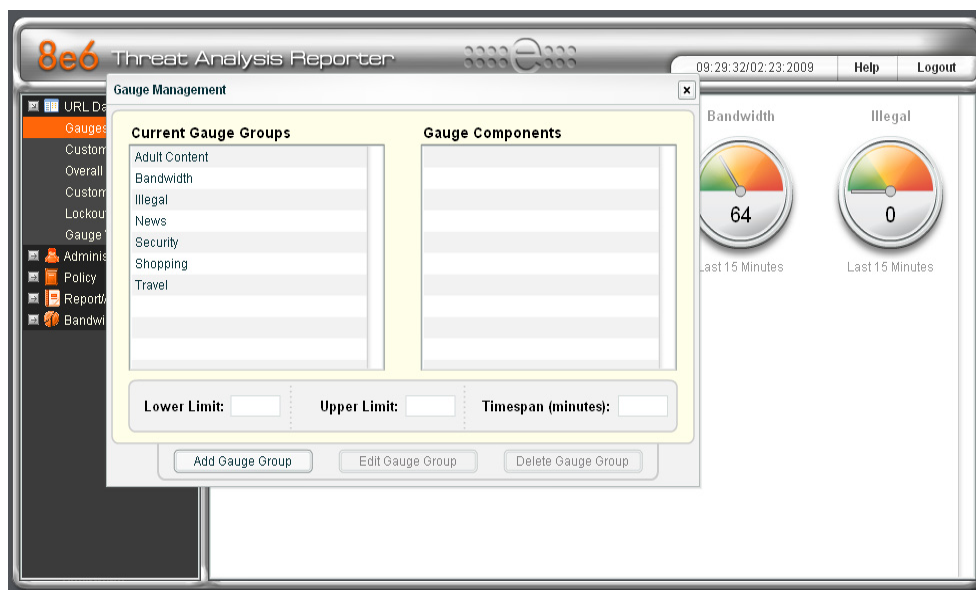
When you become accustomed to using the Threat Analysis Reporter on a regular basis to conduct these types of investigations, you will eventually want to explore other tools in the interface to restrict or lock out offending users from accessing certain library categories.

III. Create a gauge exercise

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

Step A: Access the Gauge Management window

In the URL Dashboard menu, click Gauges to open the Gauge Management pop-up window:



Note that this pop-up window contains a list of Current Gauge Groups 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 Gauge Management window*

Step B: Add a Gauge Group

1. Click **Add Gauge Group** at the bottom of this window to open the Add a new Gauge Group pop-up window:

2. In the Gauge Information frame to the left, type in the following information:
 - a) **Group Name** you wish to use and display for this gauge; this must be at least four characters in length.
 - b) **Lower Limit Value** to be used as the floor for gauge activity—this can be any number; the recommended value is “**0**” (zero).
 - c) **Upper Limit Value** to be used as the ceiling for gauge activity; the recommended value is **200**.
 - d) **Timespan in minutes (1-60 Only)** to designate the amount of time for tracking gauge activity; usually **15** minutes. The timespan will always keep pace with the current time period, so that if a timespan of 15 minutes is specified, the gauge will always reflect the most recent end user activity from the past 15 minutes.
3. In the Available Categories list box, select up to 15 library categories by clicking each one while pressing the **Ctrl** key on your keyboard. When you have selected all the categories you want the gauge to monitor, click the **Add** button to move these categories to the Assigned Categories list box.

4. Click **Next** at the bottom right of the window to open the pop-up window that lets you review the current components of the gauge and their threshold values, and specify the method(s) by which users will affect the gauge:

	Lower Limit	Upper Limit
Flash Video	0	200
Intranet/Internal Servers	0	200
Peer-to-peer/File Sharing	0	200
Portals	0	200

Set a gauge method: All

Next

Note the values in the Lower Limit and Upper Limit boxes are all the same since these values reflect the entries made in the Lower Limit Value and Upper Limit Value fields in the prior pop-up window. You can modify these figures if you want some of the library categories to carry less or more weight when affecting the gauge's score.

For this exercise, leave the values of the library categories untouched.

5. Note that the **Set a gauge method** drop-down menu includes the following options from which to select that will be used for triggering the gauge's movement:
 - **All** - choosing this option will consider all methods users can use to access URLs in library categories included in the gauge
 - **Keyword** - choosing this option will only consider user entries of URL keywords that have been categorized in any library category included in the gauge
 - **URL** - choosing this option will only consider user entries of URLs that have been categorized in any library category included in the gauge
 - **Others** - choosing this option will only consider user entries of Passed categories that have been categorized in any library category included in the gauge

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.

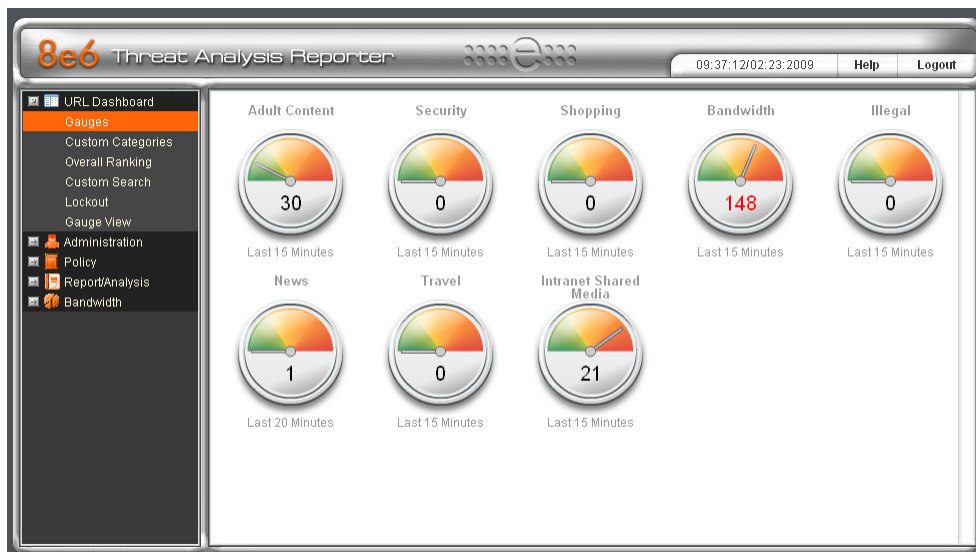


In the Threat Analysis Reporter User Guide index, see:

- *How to: add new a gauge*

Step C: Add the gauge group

In the Add a new Gauge Group window, click the **Next** button at the bottom of the window to close all pop-up windows that were opened during this exercise, and to add the new gauge to the group:



In the Threat Analysis Reporter User Guide index, see:

- *How to: add a new gauge in the dashboard*

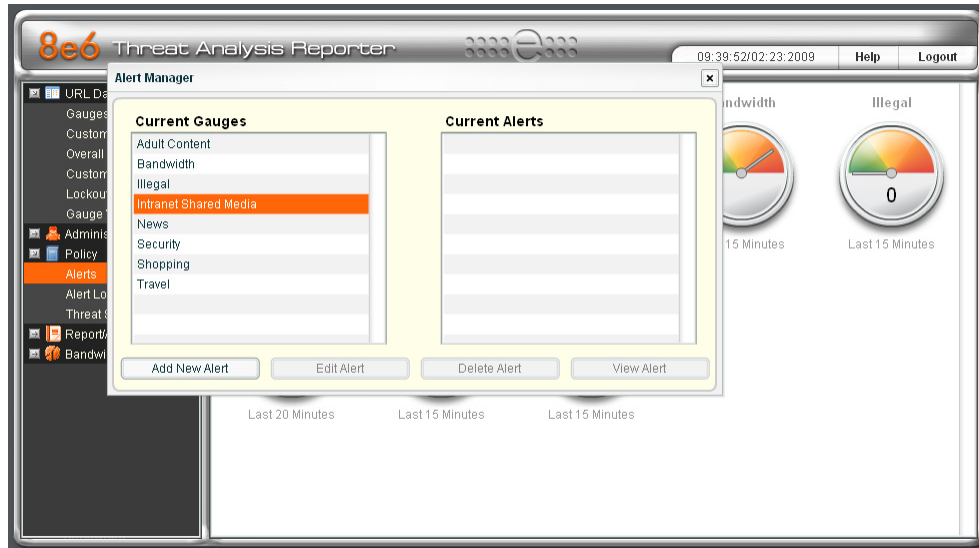
Now that you know the basics of creating a gauge, you will soon be able to create and use gauges to monitor various groups of users who frequent URLs in library categories you wish to restrict, and deal in real time with Internet usage issues that endanger your network and/or consume an excessive amount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

1. In the navigation panel, click Policy to open that menu.
2. Click Alerts to open the Alert Manager pop-up window:



In the next step you will specify that you wish to create a new alert.



In the Threat Analysis Reporter User Guide index, see:

- *How to: access the Alert Manager window*

Step B: Add a new Alert

1. At the bottom left of the Alert Manager window, click **Add New Alert** to open the Add a new Alert pop-up window where you indicate which gauge you wish to monitor and the method(s) by which you want to be notified when the gauge's activity reaches its ceiling:

2. In the Current Gauge frame, choose the gauge you wish to monitor.
3. At the bottom left of the window, enter the **Alert Name** to be used for notification of an alert.
4. At the bottom right, enter the value of the **Threshold** that will trigger the alert.

Next, you will specify which type(s) of alert notification(s) you wish to receive by choosing from any or all of the following notification options:

- **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.
- **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.
- **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.

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.

Add a new Alert

Please fill out the fields below to define the alert. If you choose to have Email associated with the action, enter as many email addresses as required.

Current Gauge

- Adult Content
- Bandwidth
- Illegal
- Intranet Shared Media**
- News
- Security
- Shopping
- Travel

Alert Action

☒ Email

☐ Lockout

☐ System Tray

Email Addresses

- admin@logo.com

Remove Email Add Email

Severity: Medium

Duration (hours): Unlimited

Threshold: 15

Alert Name: Intranet Shared Media alert

Submit

Note that this action activates the Email Addresses list box, field, and buttons at the right side of the window.

2. In the Email Addresses section, enter 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 **Submit** at the bottom right of the window to close the Add a new Alert window.

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*

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*

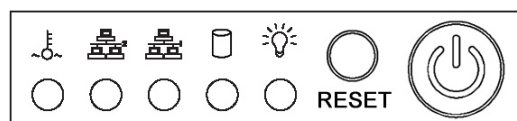
Now that you know how to create an email alert for a gauge, you will quickly identify users who are misusing their Internet access privileges, giving you knowledge about policy violations in real time so you can immediately take action to protect your resources.

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).



OH
NIC2
NIC1
HD
PWR

SL chassis control panel

LED Indicator Key

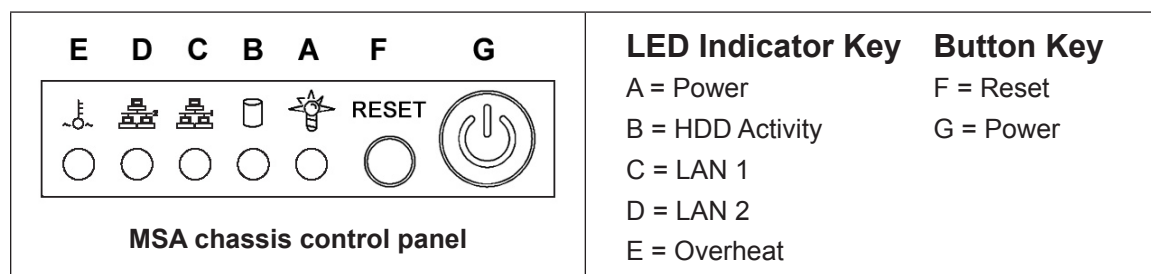
PWR = Power

HD = HDD Activity

NIC1 = LAN 1

NIC2 = LAN 2

OH = Overheat



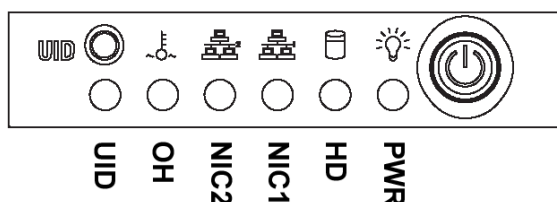
LED indicators alert you to the status of a feature on the unit while buttons let you perform a function on the unit.

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:



HL chassis control panel

LED Indicator Key

PWR = Power

HD = HDD Activity

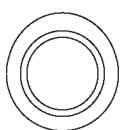
NIC1 = LAN 1

NIC2 = LAN 2

OH = Overheat

UID = Unique IDentifier

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.



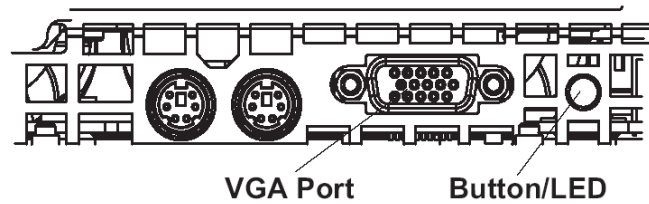
Power (icon) – The LED is unlit when the server is turned off. A steady green LED indicates power is being supplied to the unit's power supplies. (See also Rear of Chassis.) A steady amber LED—or an unlit LED—may indicate a disconnected or loose power supply cord.



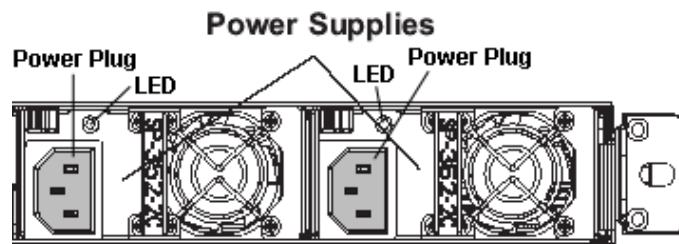
Power (button) – When the power button is pressed, the main power to the server is turned on. When the power button is pressed again, the main power to the server is removed but standby power is still supplied to the server.

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.



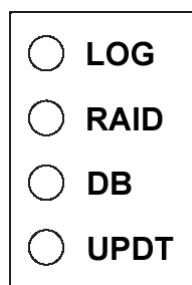
Power Supplies (LED indicators) – The power supplies are located at the right on the rear of the chassis. An LED indicator is located above each of the power plugs.



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:



left side of the
front panel

LED Indicator Key

LOG = Log Download Status

RAID = Hard Drive Status

DB = Database Status

UPDT = Software Update Status

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 in 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 8e6 Technologies.

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

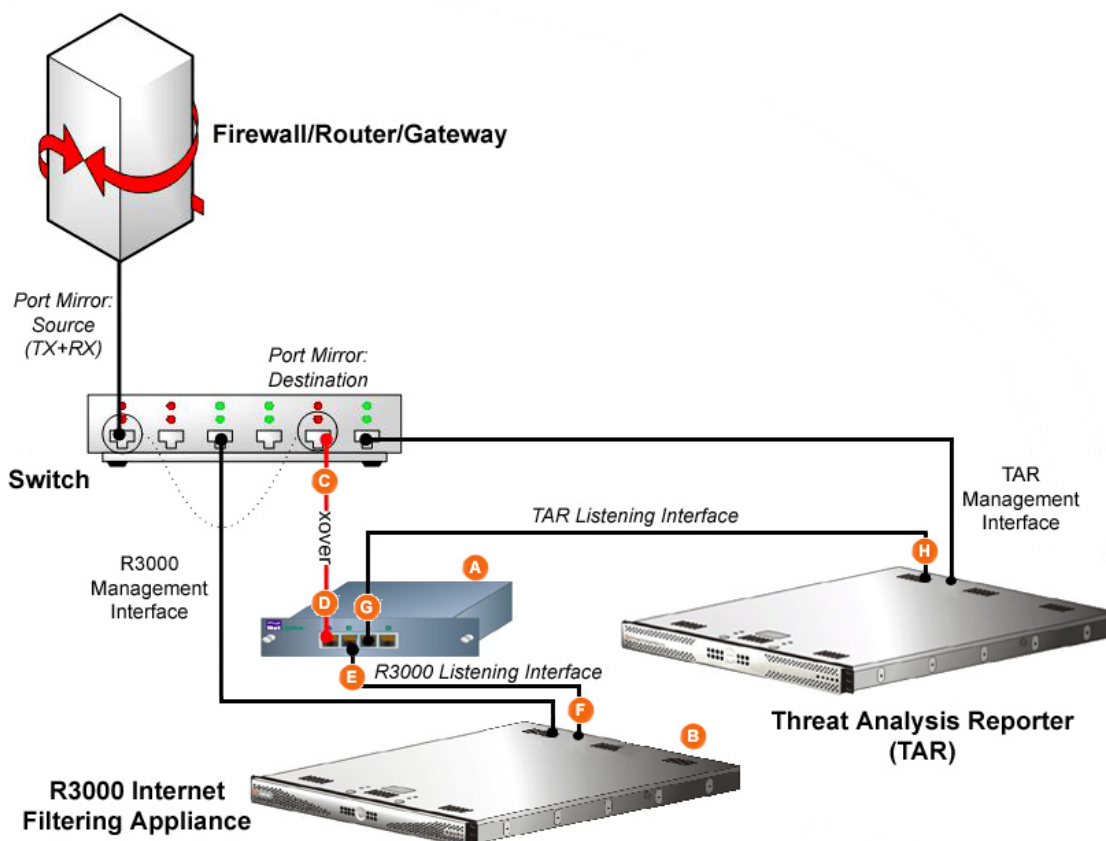


Diagram showing TAR Ethernet Tap installation on the network

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

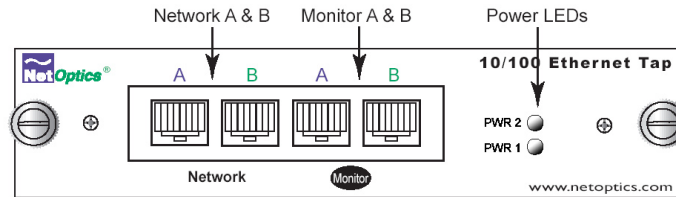
- B. If a designated source R3000 (to be used with the Threat Analysis Reporter) is already installed on the network, disconnect the cable that connects this R3000 to the switch.

If the designated R3000 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 R3000.

- 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 R3000'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 2: Wizard Setup Procedures of the Threat Analysis Reporter installation instructions.

INDEX

B

BSMI 81, 82

C

Change Quick Start password 42
crossover cable 84, 86

E

EMC 81, 83

F

FCC 81

H

HL 1, 5, 8, 23, 25, 28, 29, 30, 44, 45, 78, 79, 80, 81, 83
HyperTerminal Setup 31

I

ICES-003 81, 82
Install Bezel 23
Install TAP 84

L

LCD Panel 28
Login screen 34
LVD 81

M

MSA 15, 29, 30, 44, 77, 83

O

Overheat 77

P

Power Supply Precautions 24

Q

Quick Start menu 29, 34, 42, 43

R

R3000 1, 28, 43, 51, 56, 57, 58, 85, 86
Rack Setup Precautions 7
RAID 1, 80
reboot 45, 48
RoHS compliant 83

S

serial port cable 28, 29
shut down 49
SL 1, 5, 12, 23, 28, 29, 44, 45, 77, 80, 81, 83
spare parts kit 5

U

UID 78, 79
UL 81

8e6 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)

Satellite Office:
8e6 Taiwan: 7 Fl., No. 1, Sec. 2, Ren-Ai Rd., Taipei 10055, Taiwan, R.O.C.
Tel: 886-2-2397-0300 • Fax: 886-2-2397-0306