M86 Security Reporter

INSTALLATION GUIDE

Models: 300, 500, 700, 730

Software Version: 2.0.00
Document Version: 04.22.10

M86 Security Reporter Installation Guide for 300, 500, 700, 730 Models

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

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

Trademarks

Part# SR-IG-100422

CONTENTS

M86 SR APPLIANCE INTRODUCTION

Thank you for choosing to install and evaluate the M86 Security Reporter appliance. The Security Reporter (SR) solution consists of the best in breed of the M86 Professional Edition reporting software, consolidated into one unit.

M86's Threat Analysis Reporter (TAR) provides administrators or management personnel dynamic, real time graphical snapshots of network Internet traffic, supported by remediation tools to manage and control user-generated Web threats. Working in conjunction with M86’s Web Filter that tracks users’ online activity, TAR interprets end user Internet activity from the Web Filter’s logs and supplies data that can be viewed via an easy-to-read dashboard of gauges the administrator can drill down into, thereby identifying the source of the threat.

Data from the Web Filter is fed into M86 Security’s Enterprise Reporter (ER), giving you the ability to interrogate massive datasets through flexible drill-down technology, until the desired view is obtained. This “view” can then be memorized and saved to a user-defined report menu for repetitive, scheduled execution and distribution.

Using the SR, threats to your network are quickly identified, thus arming you with the capability to take immediate action to halt the source, secure your network, and protect your organization against lost productivity, network bandwidth issues, and possible legal problems that can result from the misuse of Internet resources.

Quick setup procedures to implement the best reporting practices are included in the Best Reporting 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 SR product and how to use this document
- **Service Information** - This section provides M86 Security contact information
- **Preliminary Setup Procedures** - This section includes instructions on how to physically set up the SR appliance in your network environment
- **Install the Server** - This section explains how to configure the SR for reporting
- **Conclusion** - This section indicates that the installation steps have been completed
- **Best Reporting Practices** - This section includes reporting scenarios and instructions for implementing the best reporting practices to capture a snapshot of end user activity on your network that tells you whether or not policies are being enforced
- **Evaluation Mode** - This section gives information on using the ER applications in the evaluation mode
- **LED Indicators and Buttons** - This section explains how to read LED indicators and use LED buttons for troubleshooting the unit
- **Regulatory Specifications and Disclaimers** - This section cites safety and emissions compliance information for the SR models referenced in this document
- **Appendices** - Appendix A explains how to set up the optional NAS (Fibre Channel Connected Storage Device or “SAN”) unit. Appendix B explains how to install the optional Ethernet Tap device on your network for bandwidth monitoring.
- **Index** - An alphabetized list of some topics included in this document

Conventions Used in this Document

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

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

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

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

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

The “book” icon references the SR User Guide. This icon is found in the Best Reporting Practices section of this document.

SERVICE INFORMATION

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

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

M86 Security Corporate Headquarters (USA)

Local	:	714.282.6111
Domestic US	:	1.888.786.7999
International	:	+1.714.282.6111

M86 Security Taiwan

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

Procedures

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

- Your contact information.
- Serial number or original order number.
- Description of the problem.
- Network environment in which the unit is used.
- State of the unit before the problem occurred.
- Frequency and repeatability of the problem.
- Can the product continue to operate with this problem?
- Can you identify anything that may have caused the problem?

PRELIMINARY SETUP PROCEDURES

Unpack the Unit from the Carton

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

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

The carton should contain the following items:

- 1 Security Reporter appliance (SR)
- 1 serial port cable
- 1 CD-ROM containing supplemental product applications and EULA

***NOTES**:*

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

- *1 AC power cord for 500 series models, 2 AC power cords for 700 series models*
- *1 bezel to be installed on the front of the chassis*
- *1 set of rack mounting rails*
- *Optional: 1 five-foot CAT-5E crossover cable, if you have a 700 series model and have purchased the NAS (Fibre Channel Connected Storage Device or "SAN") unit.*

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

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

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

At your option, a tap kit can be purchased from M86 Security.

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.*

***TIP**: Please consult the Security Reporter User Guide for information about RAID and hardware maintenance. User Guides for the SR product can be obtained from **http://www.m86security.com/support/sr/documentation.asp**.*

Select a Site for the Server

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

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

300 Series Server Setup Procedures

Set Top Applications

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

Optional 1U 2-Unit Tray Kit Applications

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

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

Rack Mount the Server

Rack Setup Precautions

WARNING:

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

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

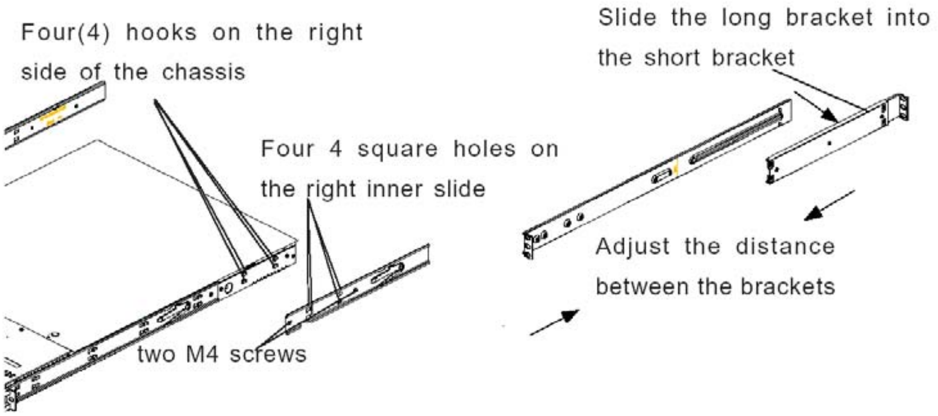
Rack Mount Instructions for 500 Series Servers

Rack Setup Suggestions

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

Install the Inner Slides

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

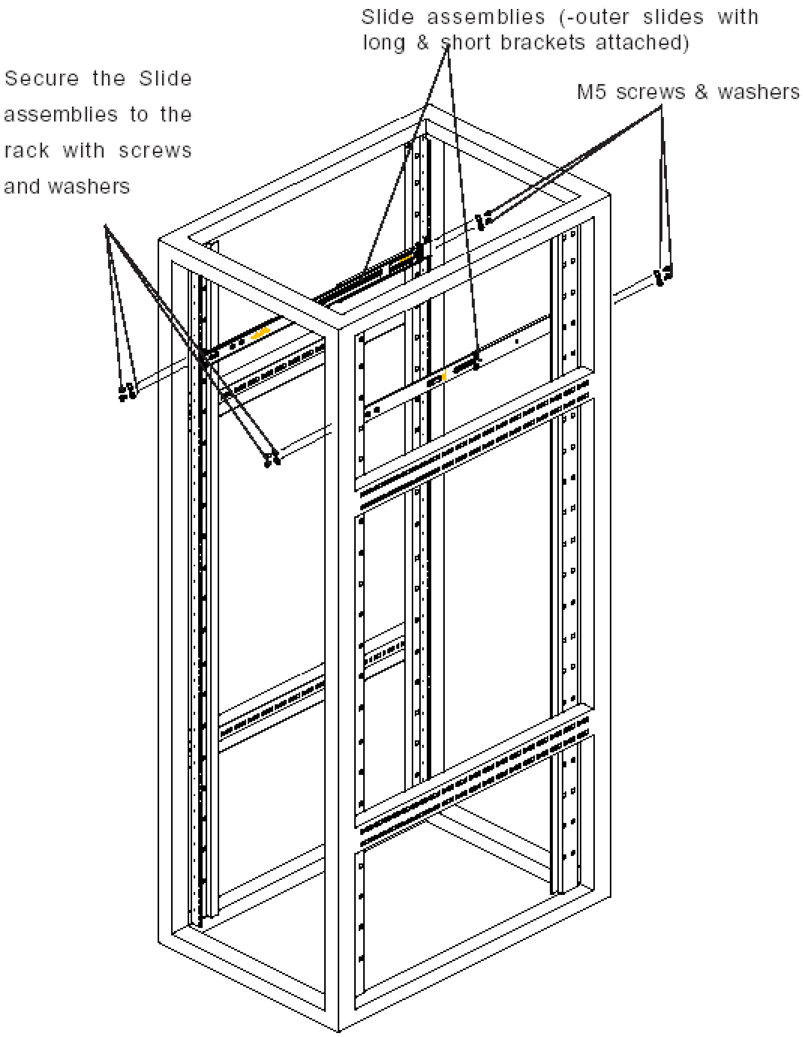

Four(4) hooks on the right side of the chassis
Four 4 square holes on the right inner slide
two M4 screws
Slide the long bracket into the short bracket
Adjust the distance between the brackets

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.

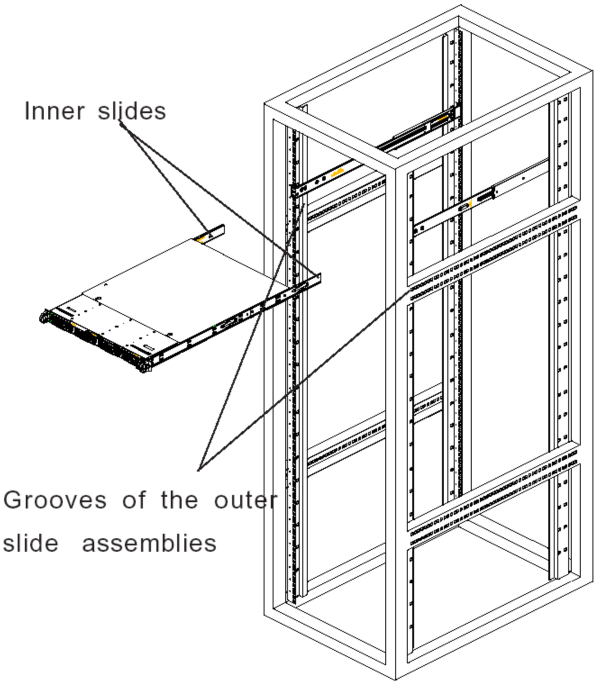
Install the Slide Assemblies to the Rack

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:

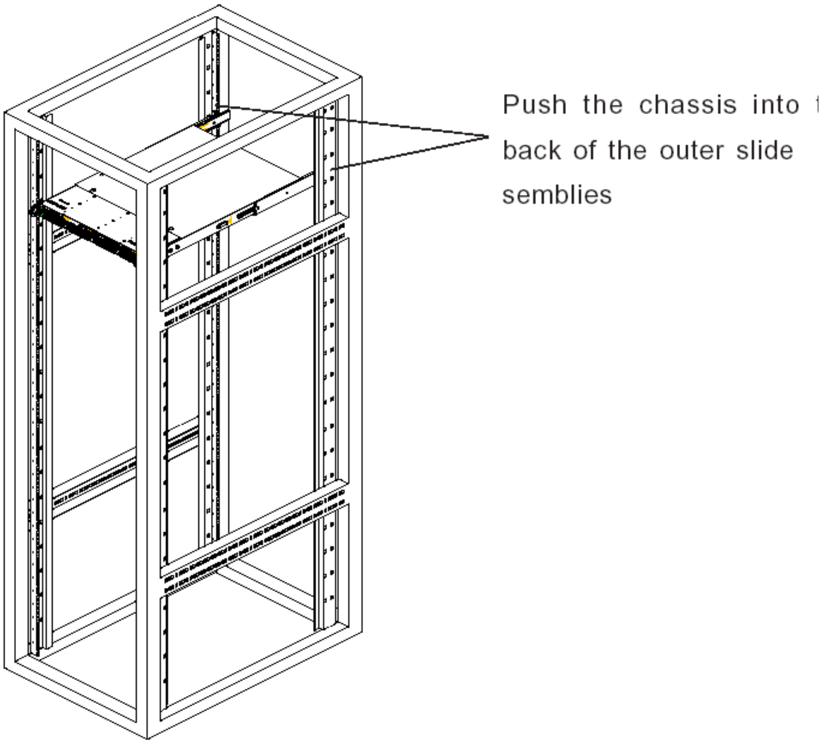

Slide assemblies (-outer slides with long & short brackets attached)
Secure the Slide assemblies to the rack with screws and washers
M5 screws & washers

Install the Chassis into the Rack

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



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



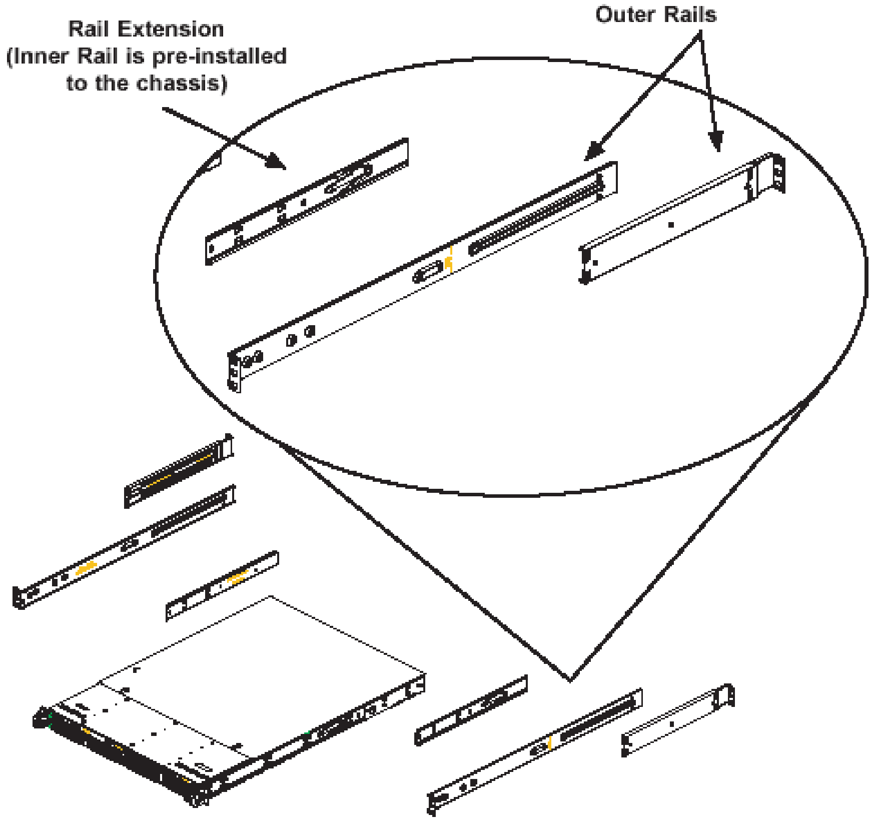
Rack Mount Instructions for 700 Series Servers

Rack Setup Suggestions

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

Identify the Sections of the Rack Rails

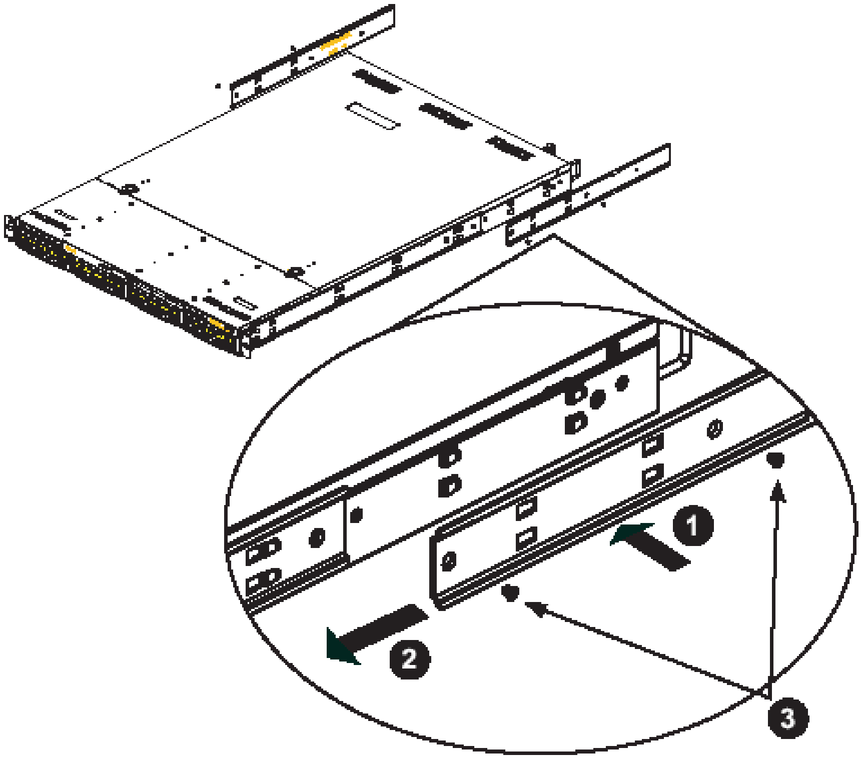
The chassis package includes two rack rail assemblies in the rack mounting kit. Each assembly consists of two sections: an inner fixed chassis rail that secures directly to the server chassis and an outer fixed rack rail that secures directly to the rack itself.



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

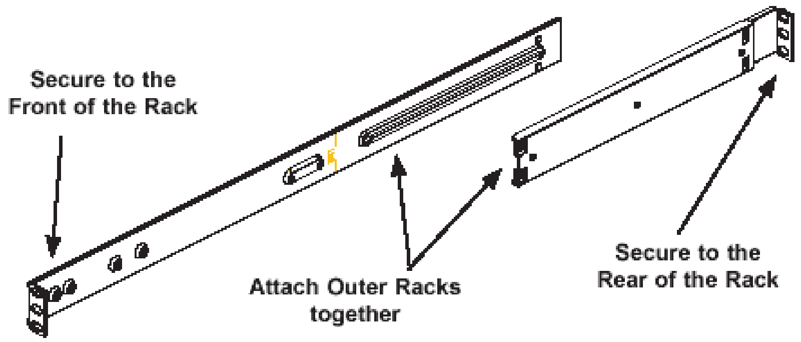
Install the Inner Rails

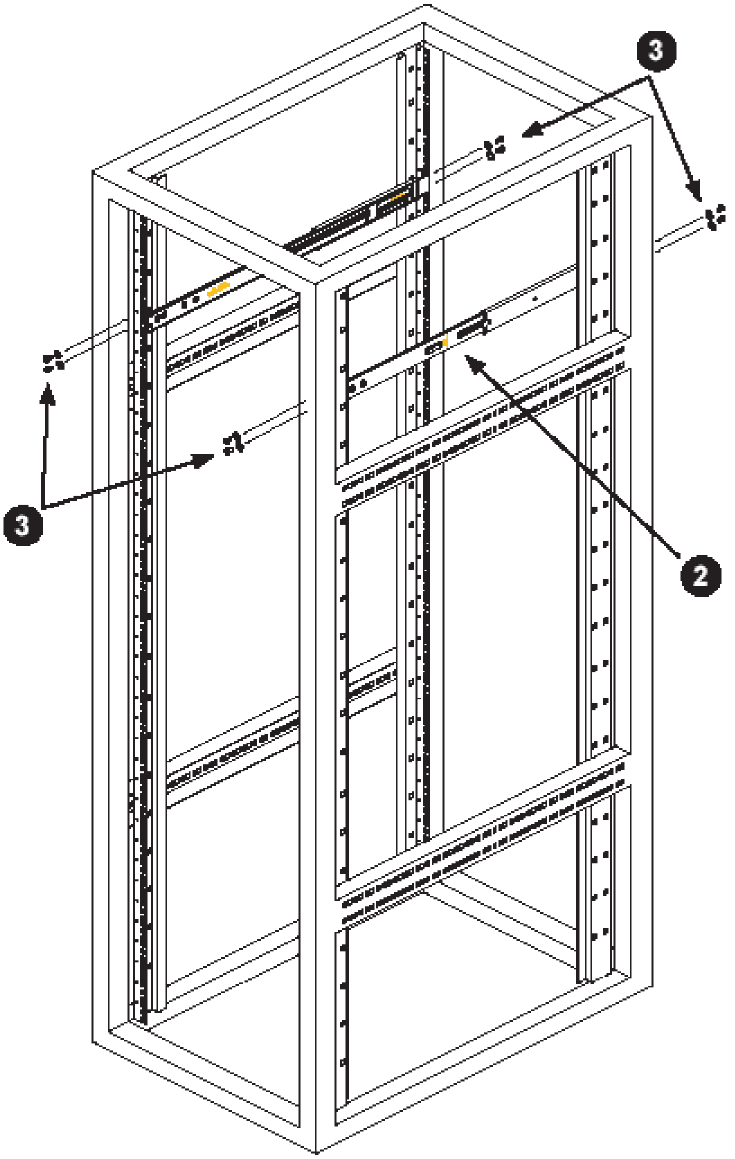
1. Place the inner rack extensions on the side of the chassis aligning the hooks of the chassis with the rail extension holes. Make sure the extension faces "outward" just like the pre-attached inner rail.
2. Slide the extension toward the front of the chassis.
3. Secure the chassis with 2 screws as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



Install the Outer Rails

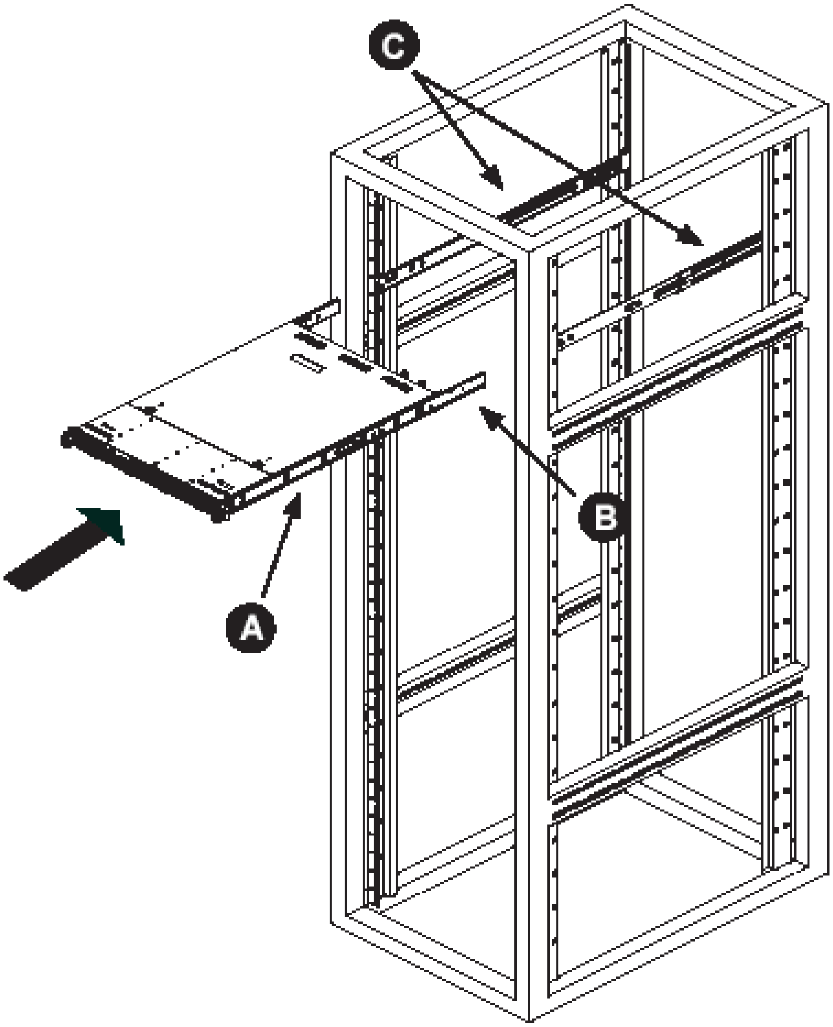
1. Attach the short bracket to the outside of the long bracket. You must align the pins with the slides. Also, both bracket ends must face the same direction.
2. Adjust both the short and long brackets to the proper distance so that the rail fits snugly into the rack.
3. Secure the long bracket to the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


Secure to the
Front of the Rack
Attach Outer Racks
together
Secure to the
Rear of the Rack


3
3
2

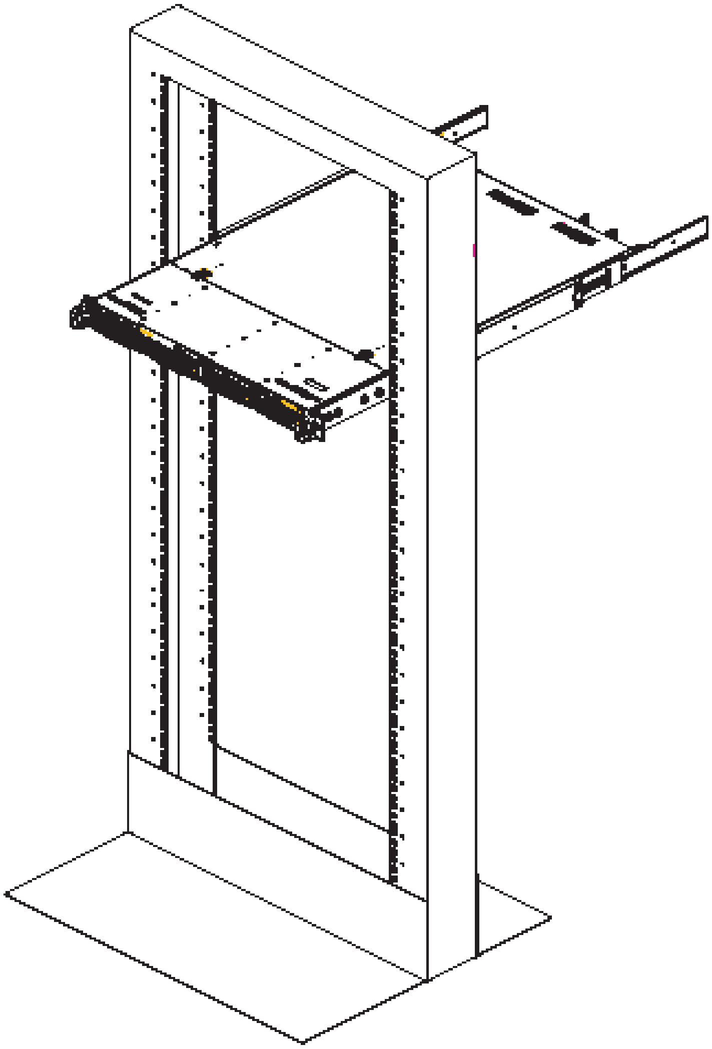
Install the Server into the Rack

1. Confirm that chassis includes the inner rails (A) and rail extensions (B). Also, confirm that the outer rails (C) are installed on the rack.
2. Line chassis rails (A and B) with the front of the rack rails (C).
3. Slide the chassis rails into the rack rails, keeping the pressure even on both sides (you may have to depress the locking tabs when inserting). When the server has been pushed completely into the rack, you should hear the locking tabs "click".
4. (Optional) Insert and tightening the thumbscrews that hold the front of the server to the rack.



Install the Server into a Telco Rack

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



Install the Bezel on the 500 and 700 Series Chassis

After rack mounting a 500 or 700 series server, the bezel should be installed on the front end of the chassis.

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

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

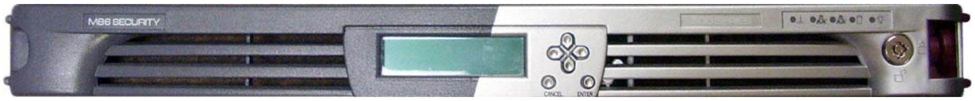


Fig. 1 - Front of bezel

B. Note the short pair of end pins on the left side (Fig. 2), and the longer pair of fixed pins on the inside top towards the middle (Fig. 3).

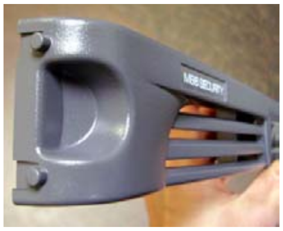


Fig. 2 - Pins on the left end

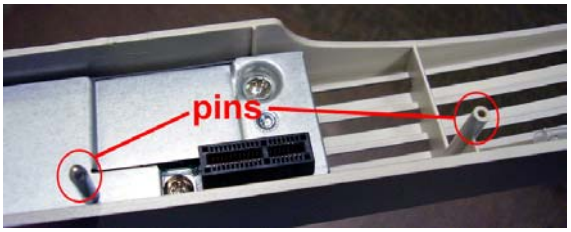


Fig. 3 - Pins on the inside at the top of the bezel

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

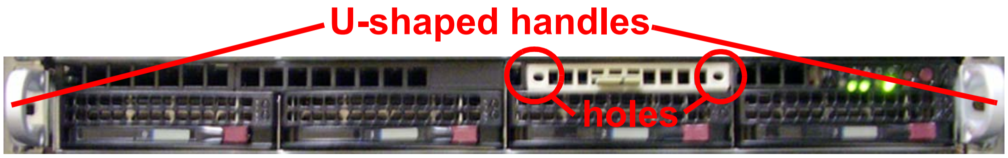


Fig. 4 - Front of chassis with U-shaped handles and holes above third hard drive identified

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

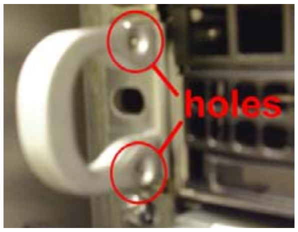


Fig. 5 - Holes in handle

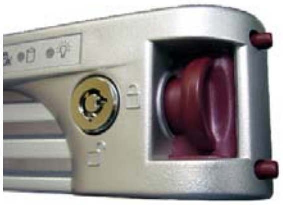


Fig. 6 - Release knob

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

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

Check the Power Supply

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

Power Supply Precautions

WARNING:

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

General Safety Information

Server Operation and Maintenance Precautions

WARNING:

Observe the following safety precautions during server operation and maintenance:

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

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

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

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

WARNING: *In 700 series servers, multiple sources of supply exist. Be sure to disconnect all sources before servicing.*

- Do not insert objects through openings in the chassis. Doing so could result in a short circuit that might cause a fire or an electrical shock.
- Do not operate the server in an explosive atmosphere, in the presence of flammable gases.

- To ensure proper cooling, always operate the server with its covers in place. Do not block any openings on the chassis. Do not place the server near a heater.
- Always exit the software application properly before turning off the server to ensure data integrity.
- Do not expose the server to rain or use near water. If liquids of any kind should leak into the chassis, power down the server, unplug it, and contact M86 Security technical support.
- Disconnect power from the server before cleaning the unit. Do not use liquid or aerosol cleaners.

AC Power Cord and Cable Precautions

⚠ ***WARNING**:*

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

Electrical Safety Precautions

⚠ ***WARNING**:*

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

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

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

Motherboard Battery Precautions

***CAUTION**:*

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

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

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

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

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

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

INSTALL THE SERVER

Step 1: Setup Procedures

This step requires you to set up parameters for the SR to function on the network. You have the option of using the text-based Quick Start setup procedures described in Step 1A, or the LCD panel setup procedures described in Step 1B.

Quick Start Setup Requirements

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

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

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

***NOTE**:*

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

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

LCD Panel Setup Requirements

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

- SR with AC power cord(s) *

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

***NOTE**:*

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

Step 1A: Quick Start Setup Procedures

Storage Device Setup (for Attached Storage Units)

If you have a NAS (Fibre Channel Connected Storage Device or “SAN”) that will be used with the SR, you will need to connect it to the SR at this point. Refer to Appendix A at the end of this document for instructions on how to connect the Fibre Channel Connected Storage Device.

Link the Workstation to the SR

Monitor and Keyboard Setup

A. Connect the PC monitor and keyboard cables to the rear of the SR chassis.

B. Turn on the PC monitor.

C. Proceed to the next set of instructions: Power on the SR.

Serial Console Setup

A. Using the serial port cable (and USB DB9 serial adapter, if necessary), connect the laptop to the rear of the chassis (see “serial port” in Fig. 1 for a 300 series unit, Fig. 2 for a 500 series unit, and Fig. 3 for a 700 series unit).

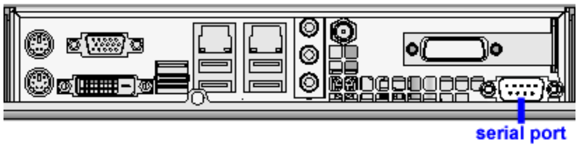


Fig. 1 - Rear of 300 series chassis with serial port identified

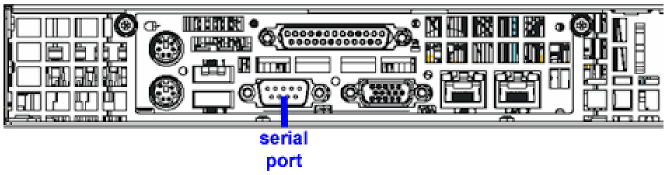


Fig. 2 - Portion of 500 series chassis rear with serial port identified

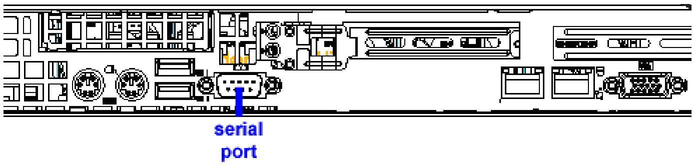


Fig. 3 - Portion of 700 series chassis rear with serial port identified

B. Power on the laptop.

C. Proceed to the next set of instructions: Power on the SR.

Power on the SR

Power up a 300 Series Model

A. Make sure the power adapter is plugged into the back of the chassis and connected to the power cord.

B. Plug the power cord into a power source with an appropriate rating.

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

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

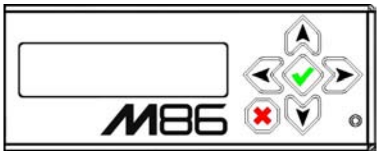


Fig. 4 - 300 series LCD panel and keypad

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

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

Power up a 500 or 700 Series Model

A. Make sure the power cord(s) is/are plugged into the back of the chassis.

B. Plug the power cord(s) into a power source with an appropriate rating.

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

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

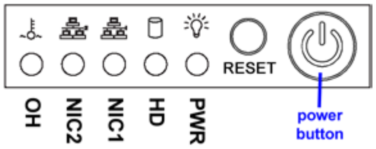


Fig. 5 - 500 series chassis front panel, power button at far right

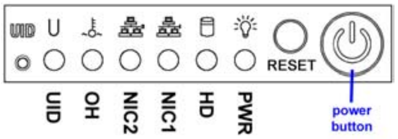


Fig. 6 - 700 series chassis front panel, power button at far right

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

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

HyperTerminal Setup Procedures

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

NOTE*: HyperTerminal is no longer included with Windows as of Microsoft’s Vista system. Please note on Microsoft’s Web page “What happened to HyperTerminal?” at http://windows.microsoft.com/en-us/windows-vista/What-happened-to-HyperTerminal (accessed February 10, 2010), Microsoft states: “HyperTerminal is no longer part of Windows.... If you previously used HyperTerminal to control serial devices, you can usually find a downloadable version of HyperTerminal on the Internet that is free for personal use.”*

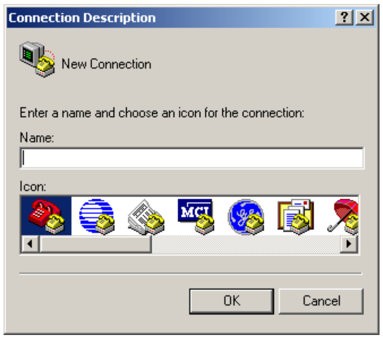
If you are using a Windows Vista or Windows 7 machine to conduct these quick start setup procedures and do not have an equivalent type of terminal emulator program installed on your workstation, Hilgraeve, Inc., the maker of HyperTerminal, offers HyperTerminal Private Edition for Windows Vista and Windows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

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

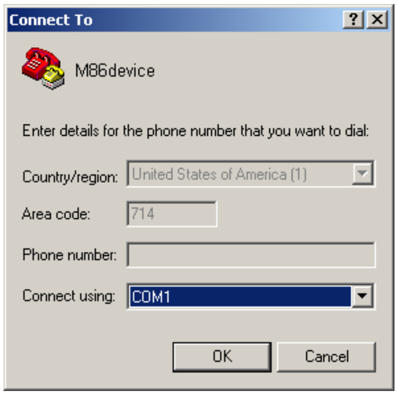
- *9600 bits per second*
- *8 data bits*
- *no parity*
- *1 stop bit*
- *hardware flow control*
- *VT100 emulation settings*

On the Windows XP machine:

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



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



Connect To

M86device

Enter details for the phone number that you want to dial:

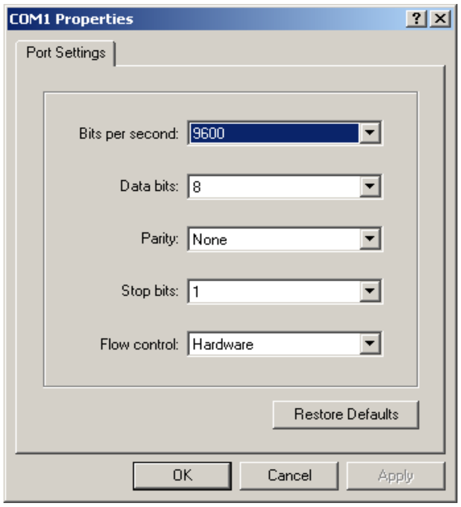
Country/region: United States of America (1)

Area code: 714

Phone number:

Connect using: COM1

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:



COM1 Properties

Port Settings

Bits per second: 9600

Data bits: 8

Parity: None

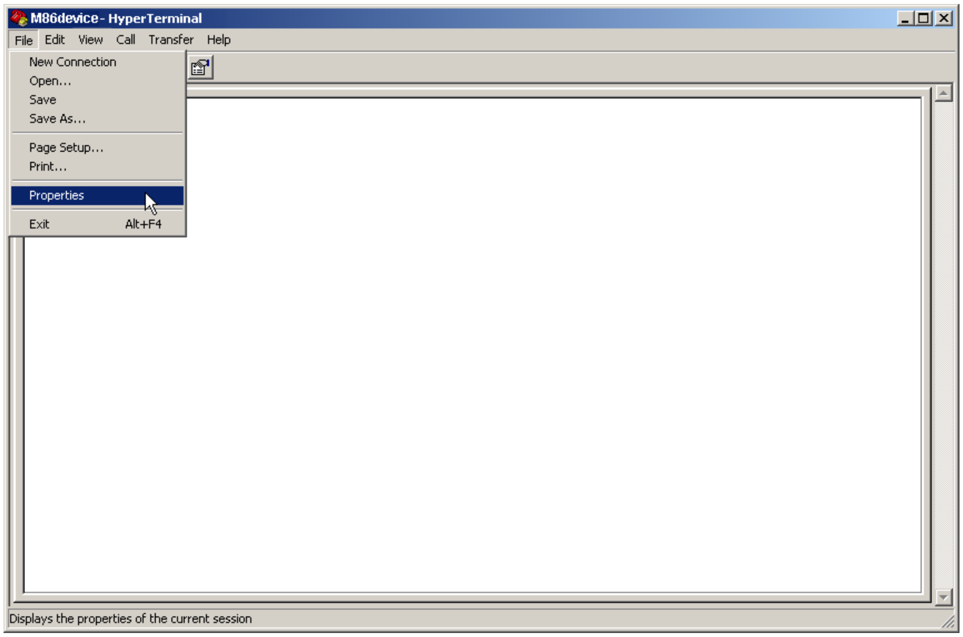
Stop bits: 1

Flow control: Hardware

D. Specify the following session settings:

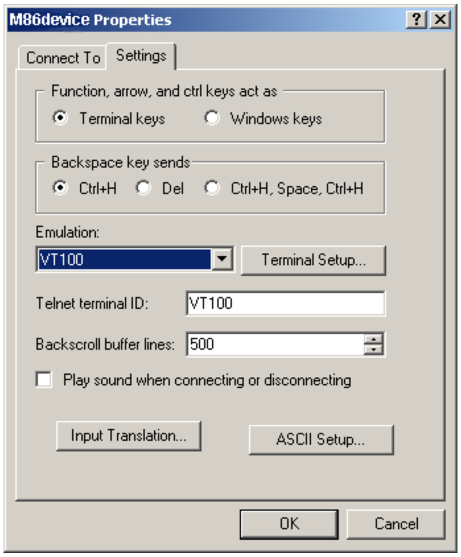
- Bits per second: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: Hardware
- VT100 emulation settings

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



Displays the properties of the current session

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



Function, arrow, and ctrl keys act as
● Terminal keys ○ Windows keys

Backspace key sends
● Ctrl+H ○ Del ○ Ctrl+H, Space, Ctrl+H

Emulation: VT100

Telnet terminal ID: VT100

Backscroll buffer lines: 500

□ Play sound when connecting or disconnecting

G. Click the Settings tab, and at the **Emulation** menu select “VT100”.

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

Login screen

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

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

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

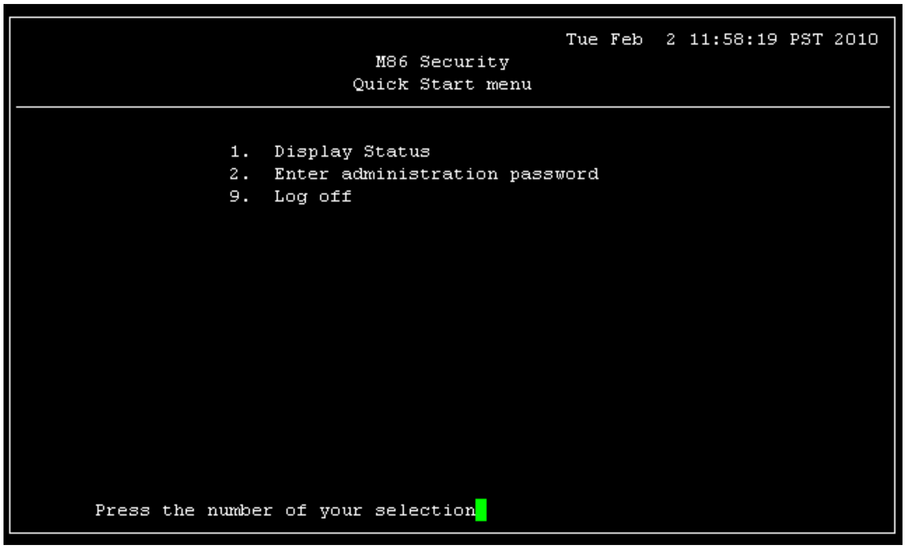
A. At the **login** prompt, type in ***menu***.

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

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

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

Quick Start menu screen



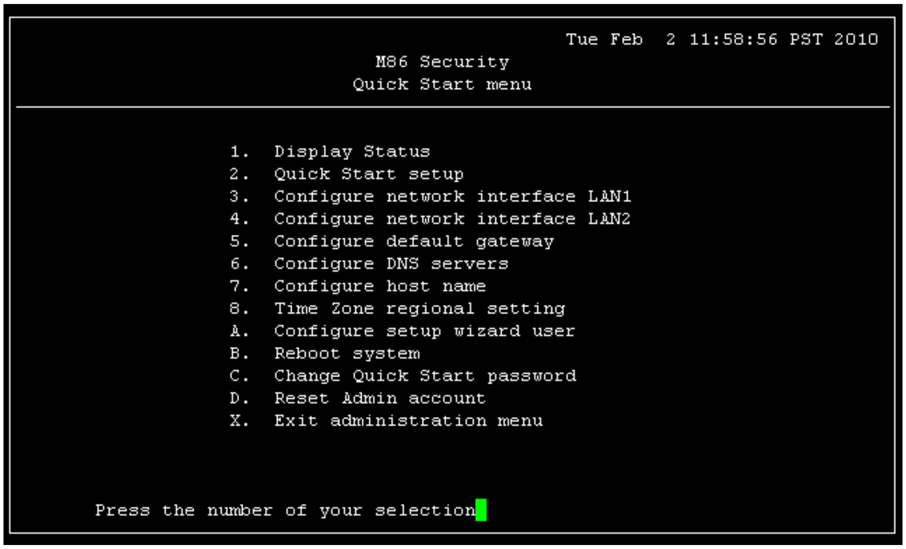
```
                                                        Tue Feb  2 11:58:19 PST 2010
                                          M86 Security
                                        Quick Start menu

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

        Press the number of your selection
```

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

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

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

Quick Start setup



```
                                                   Tue Feb  2 11:58:56 PST 2010
                              M86 Security
                            Quick Start menu
---------------------------------------------------------------------------------

                   1.  Display Status
                   2.  Quick Start setup
                   3.  Configure network interface LAN1
                   4.  Configure network interface LAN2
                   5.  Configure default gateway
                   6.  Configure DNS servers
                   7.  Configure host name
                   8.  Time Zone regional setting
                   A.  Configure setup wizard user
                   B.  Reboot system
                   C.  Change Quick Start password
                   D.  Reset Admin account
                   X.  Exit administration menu



       Press the number of your selection
```

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

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

- Configure network interface LAN1
- Configure network interface LAN2
- Configure default gateway
- Configure DNS servers
- Configure host name
- Time Zone regional setting
- Configure setup wizard user

***NOTE**: Please make a note of the LAN 1 and LAN 2 IP address and host name you assign to the SR server, as well as the username and password you create for logging into the “setup wizard”, as you will need to use this information in later steps of the installation procedure.*

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

***NOTE**: To configure an individual screen from the Quick Start menu, press the number or alphabet corresponding to that menu option, as described in the following sub-sections.*

Configure network interface LAN1

A. From the Quick Start menu, press **3** to go to the Configure Network Interface screen for LAN1.

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

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

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

Configure network interface LAN2

A. From the Quick Start menu, press **4** to go to the Configure Network Interface screen for LAN2.

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

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

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

Configure default gateway

A. From the Quick Start menu, press **5** to go to the Configure default gateway screen.

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

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

Configure DNS servers

A. From the Quick Start menu, press **6** to go to the Configure Domain Name Servers screen.

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

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

Configure host name

A. From the Quick Start menu, press **7** to go to the Configure host name screen.

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

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

Time Zone regional setting

A. From the Quick Start menu, press **8** to go to the Time Zone regional configuration screen.

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

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

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

Configure setup wizard user

A. From the Quick Start menu, press **A** to go to the Configure Wizard user screen.

B. At the **Enter wizard user name** prompt, type in the new username to be used for the Threat Analysis Reporter Quick Start Wizard (TAR GUI Wizard User) setup and press **Enter**.

***NOTE**: The username ‘admin’ cannot be used since it is already the default username.*

C. At the **Enter wizard password** prompt, type in the new password for the username you entered and press **Enter**.

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

Non-Quick Start procedures or settings

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

Reboot system

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

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

Change Quick Start password

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

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

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

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

Reset Admin account

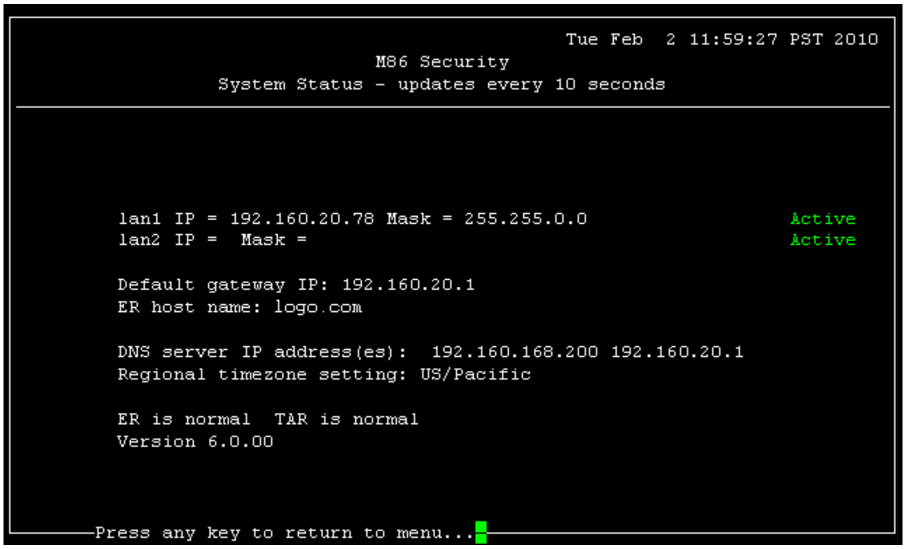
A. From the Quick Start menu, press **D** to go to the Reset admin GUI account confirmation screen that displays the following message:

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

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

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

System Status screen



```
                                              Tue Feb  2 11:59:27 PST 2010
                              M86 Security
                 System Status - updates every 10 seconds
─────────────────────────────────────────────────────────────────────────



         lan1 IP = 192.160.20.78 Mask = 255.255.0.0                Active
         lan2 IP =  Mask =                                         Active

         Default gateway IP: 192.160.20.1
         ER host name: logo.com

         DNS server IP address(es):  192.160.168.200 192.160.20.1
         Regional timezone setting: US/Pacific

         ER is normal  TAR is normal
         Version 6.0.00



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

The System Status screen contains the following information:

- **lan1 IP** address and netmask specified in screen 3, and current status (“Active” or “Inactive”)
- **lan2 IP** address and netmask specified in screen 4, and current status (“Active” or “Inactive”)
- **Default gateway IP** address specified in screen 5 (Configure default gateway)
- **host name** specified in screen 7 (Configure host name)
- **DNS server IP address(es)** specified in screen 6 (Configure DNS servers)
- **Regional timezone setting** specified in screen 8 (Time Zone regional setting)
- current status of ER and TAR applications
- **Version** of software installed

NOTE*: Modifications can be made at any time by returning to the specific screen of the Quick Start setup procedures. To access the System Status screen from the Quick Start setup screen, press* ***1*** *and then* ***Enter****.*

Log Off, Disconnect the Peripherals

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

B. Disconnect the peripherals from the SR.

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

Step 1B: LCD Panel Setup Procedures

Storage Device Setup (for Attached Storage Units)

If you have a NAS (Fibre Channel Connected Storage Device or “SAN”) that will be used with the SR, you will need to connect it to the SR at this point. Refer to Appendix A at the end of this document for instructions on how to connect the Fibre Channel Connected Storage Device.

LCD Panel

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

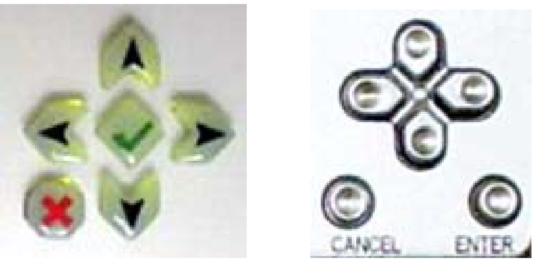
B. Power on the server following the instructions at Step 1A: Quick Start Setup Procedures, Power on the SR.

LCD panel keypad

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

The keypad consists of the following keys:

- On a 300 series model: Up arrow, down arrow, left arrow, right arrow, check-mark, and “X” keys.
- On a 500 or 700 series model: Up, down, left, right, CANCEL, and ENTER keys.



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

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

LCD Menu

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

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

The menu tree displays an arrow to the left of the currently selected menu item. Use the up or down (arrow) keys to navigate the menu. After making your menu selection, press the checkmark / ENTER key to accept your selection.

M86 menu

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

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

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

Please make a note of the LAN 1 and LAN 2 IP address and host name you assign to the SR server, as well as the username and password you create for logging into the "TAR GUI Wizard", as you will need to use this information in later steps of the installation procedure.

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

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

IP / LAN1 and 2

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

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

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

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

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

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

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

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

G. Press the “X” / CANCEL key to return to the M86 menu.

Gateway

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

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

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

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

D. Press the “X” / CANCEL key to return to the M86 menu.

DNS 1 and 2

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

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

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

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

D. Press the “X” / CANCEL key to return to the M86 menu.

Host Name

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

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

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

***NOTE**: Navigation tips:*

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

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

D. Press the "X" / CANCEL key to return to the M86 menu.

Regional Setting (Time Zone, date, time)

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

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

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

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

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

- Choose **Yes** to save your changes and to return to the M86 menu.
- Choose **No** to return to the previous screen.

TAR GUI Wizard User

When the TAR GUI Wizard User option is selected, the TAR GUI Wizard User screen displays with two menu selections:

- Choose **Change User** to reset the username for accessing the Threat Analysis Reporter login window (this is the username entered and saved during the TAR Wizard process) and to return to the main menu.

***NOTE**: The username 'admin' cannot be used since it is already the default username.*

- Choose **Change Password** to reset the password for the TAR Wizard username and to return to the M86 menu.

Non-Quick Start procedures or settings

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

SR Patch Level

When the SR Patch Level option is selected, “Security Reporter” and the version number of the currently installed software build displays.

Reset ER Admin Console Password

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

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

*** WARNING *** The Admin console username/password will be reset to ‘admin’/’reporter’ and all locked IPs will be unlocked.

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

- Choose **Yes, reset it now!** to reset the password and to return to the M86 menu.
- Choose **No, cancel reset** to return to the previous screen.

Reboot

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

A. Choose one of two options:

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

B. Press the “X” / CANCEL key to return to the M86 menu.

Shutdown

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

A. Choose one of two options:

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

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

LCD Options menu

When “**LCD Options >**” is selected, the following menu items display on the screen: Heartbeat, Backlight, LCD Controls >. Make a selection from the menu, and press the checkmark / ENTER key to go to that screen.

Heartbeat

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

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

- heartbeat feature enabled (populated field)
- heartbeat feature disabled (empty field)
- check for a heartbeat now (blinking heartbeat symbol displayed in the line above)

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

Backlight

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

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

- backlight feature enabled (populated field, backlight turns on)
- backlight feature disabled (empty field, backlight turns off)
- display the backlight now (populated field, backlight turns on)

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

LCD Controls

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

A. Choose one of the menu selections and press the checkmark / ENTER or right (arrow) key to go to that screen:

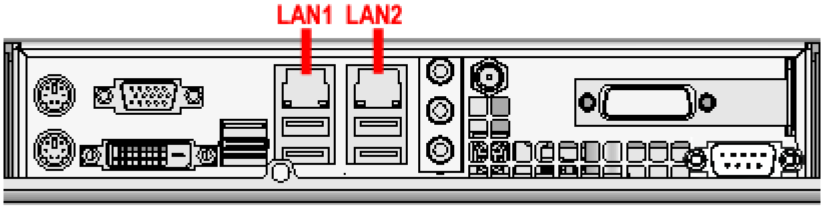
- **Contrast -** In the Contrast screen, use the left / right (arrow) keys to decrease / increase the text and screen contrast.
- **On Brightness -** In the On Brightness screen, use the left / right (arrow) keys to decrease / increase the brightness of a screen with a feature that is enabled.
- **Off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

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

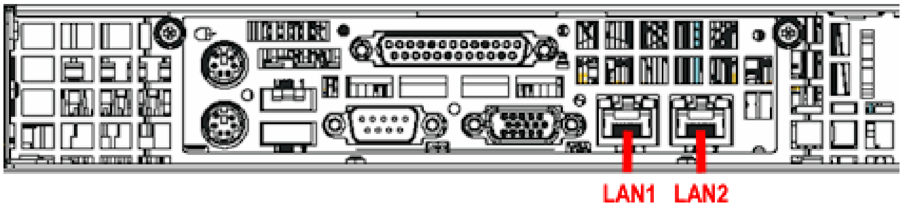
Step 2: Physically Connect the Unit to the Network

Now that your SR network parameters are set, you can physically connect the unit to your network. This step requires a standard CAT-5E cable. An additional CAT-5E cable is required if an Ethernet Tap unit will be installed for bandwidth monitoring.

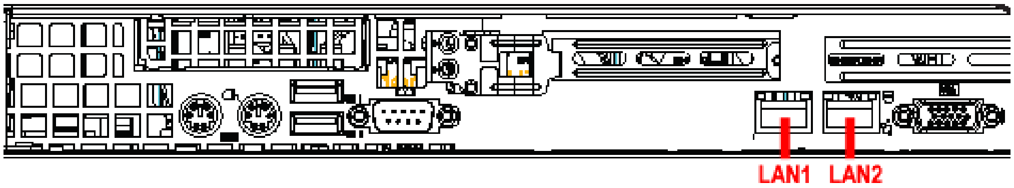
A. Plug one end of a standard CAT-5E cable into the SR's LAN 1 port, the port on the left.



Rear of 300 series chassis with LAN ports identified



Portion of 500 series chassis rear with LAN ports identified



Portion of 700 series chassis rear with LAN ports identified

B. Plug the other end of the CAT-5E cable into an open port on the network hub to which the Web-access logging device (Web Filter or equivalent type of unit) is connected.

Bandwidth Management

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

***NOTE**: In order to monitor bandwidth on the SR, both inbound and outbound traffic must be sent to the SR through use of a port span, tap, or other similar device.*

Step 3: Register the SR and its Applications

Next you will register the SR and its applications online. 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 application will use for monitoring bandwidth on your network
- Web Filter IP address, and port number to be used between the Web Filter and SR

Access the SR via its LAN 1 IP Address

A. Launch an Internet supported browser:

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

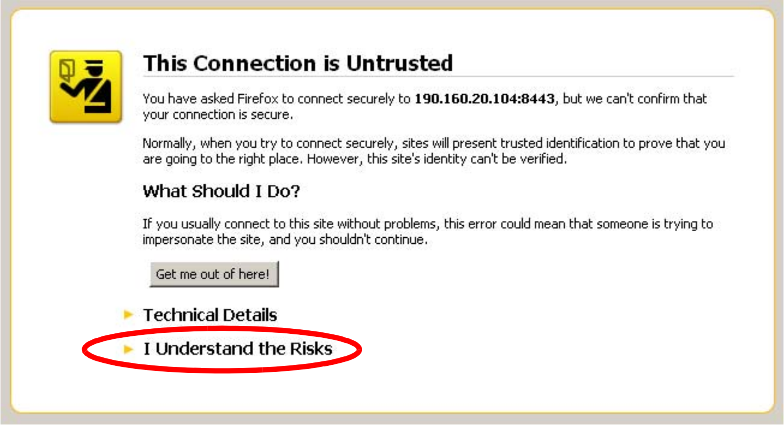
B. In the address field, type in the LAN 1 IP address you assigned to the SR in Step 1A (Quick Start setup) or Step 1B (IP / LAN1 and 2). Be sure to use “https” and port **:8443** for a secure connection. For example, if the SR were assigned an IP address of 10.10.10.10, you would enter **https://10.10.10.10:8443** in the browser’s address field.

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

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

Accept the Security Certificate in Firefox

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



This Connection is Untrusted

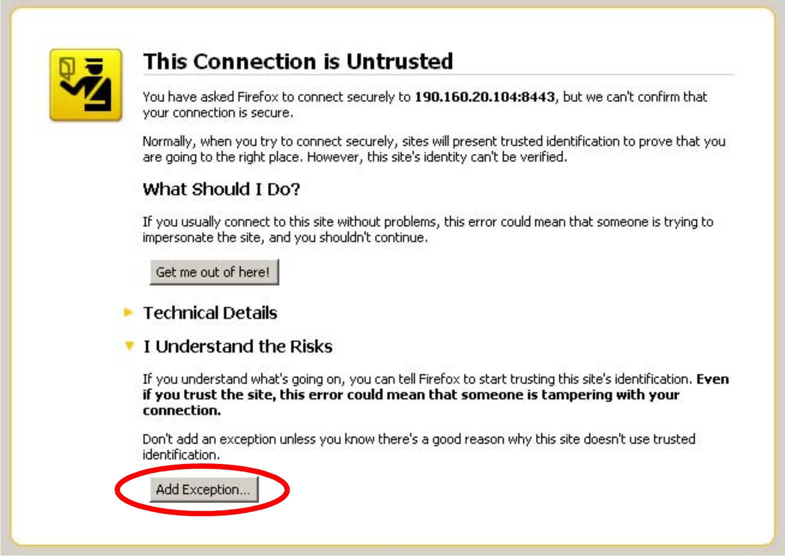
You have asked Firefox to connect securely to **190.160.20.104:8443**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

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



This Connection is Untrusted

You have asked Firefox to connect securely to **190.160.20.104:8443**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

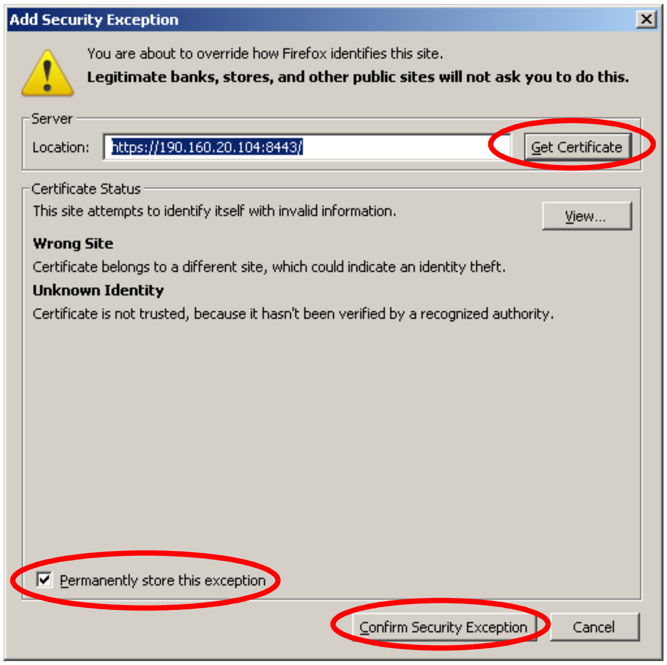
What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

Clicking Add Exception opens the Add Security Exception window:



Add Security Exception

You are about to override how Firefox identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://190.160.20.104:8443/

Certificate Status

This site attempts to identify itself with invalid information.

Wrong Site

Certificate belongs to a different site, which could indicate an identity theft.

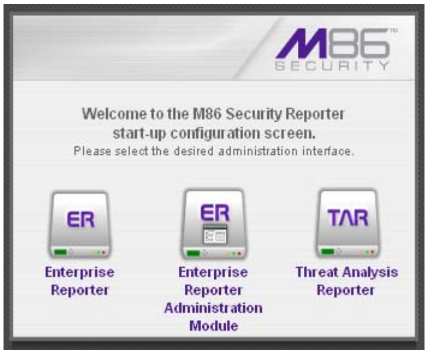
Unknown Identity

Certificate is not trusted, because it hasn't been verified by a recognized authority.

☑ Permanently store this exception

C. In the Add Security Exception window, click **Get Certificate** and wait a few seconds until the security certificate is obtained by the server.

D. With the checkbox **Permanently store this exception** selected, click **Confirm Security Exception** to open the SR Welcome window:



Welcome to the M86 Security Reporter start-up configuration screen.

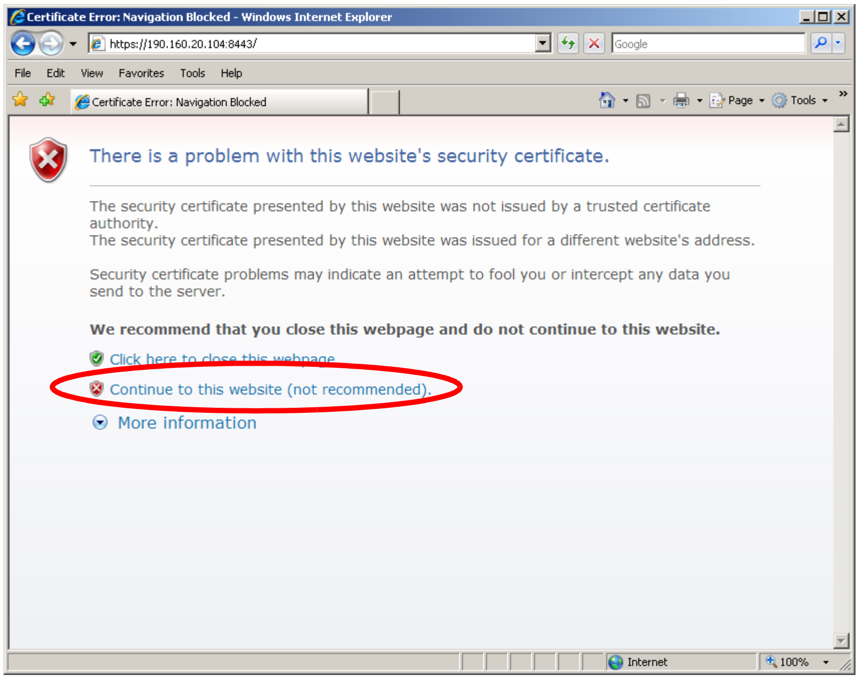
Please select the desired administration interface.

Proceed to Accept the End User License Agreement.

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

Temporarily Accept the Security Certificate in IE

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


Certificate Error: Navigation Blocked - Windows Internet Explorer
https://190.160.20.104:8443/
Google
File Edit View Favorites Tools Help
Certificate Error: Navigation Blocked
Page Tools
Internet
100%

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

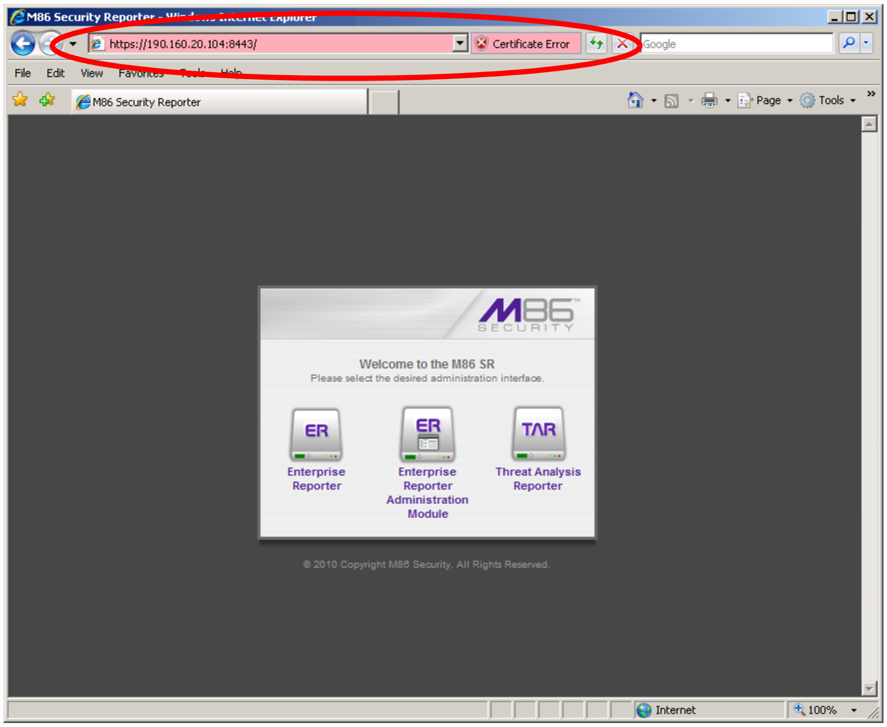
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

Selecting this option displays the SR Welcome window with the address field and the Certificate Error button to the right of the field shaded a reddish color:


M86 Security Reporter - Windows Internet Explorer
https://190.160.20.104:8443/
Certificate Error
Google
File Edit View Favorites Tools Help
M86 Security Reporter
Page Tools
M86 SECURITY
ER
Enterprise Reporter
ER
Enterprise Reporter Administration Module
TAR
Threat Analysis Reporter
Internet
100%

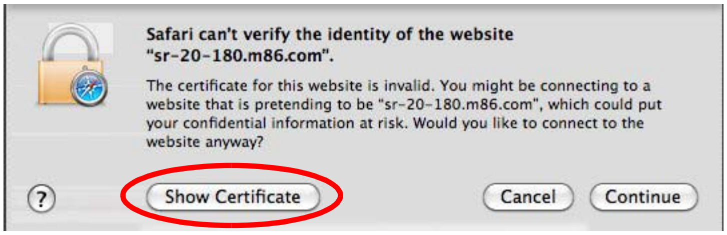
Welcome to the M86 SR
Please select the desired administration interface.

© 2010 Copyright M86 Security. All Rights Reserved.

Proceed to Accept the End User License Agreement.

Accept the Security Certificate in Safari

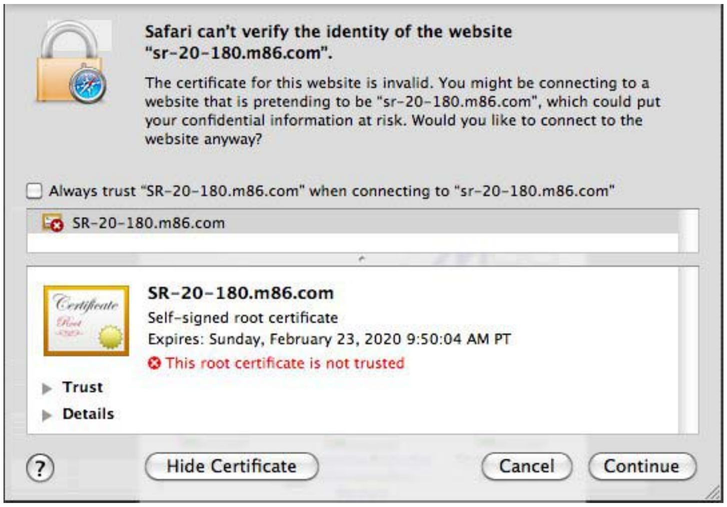
A. If using a Safari browser, the pop-up window "Safari can't verify the identity of the website..." opens:



Safari can't verify the identity of the website "sr-20-180.m86.com".

The certificate for this website is invalid. You might be connecting to a website that is pretending to be "sr-20-180.m86.com", which could put your confidential information at risk. Would you like to connect to the website anyway?

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



Safari can't verify the identity of the website "sr-20-180.m86.com".

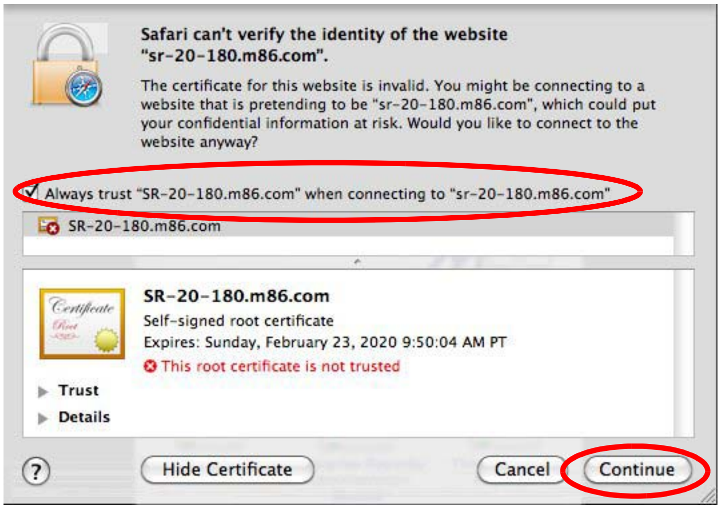
The certificate for this website is invalid. You might be connecting to a website that is pretending to be "sr-20-180.m86.com", which could put your confidential information at risk. Would you like to connect to the website anyway?

□ Always trust "SR-20-180.m86.com" when connecting to "sr-20-180.m86.com"

SR-20-180.m86.com

SR-20-180.m86.com
Self-signed root certificate
Expires: Sunday, February 23, 2020 9:50:04 AM PT
☒ This root certificate is not trusted

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



Safari can't verify the identity of the website "sr-20-180.m86.com".

The certificate for this website is invalid. You might be connecting to a website that is pretending to be "sr-20-180.m86.com", which could put your confidential information at risk. Would you like to connect to the website anyway?

☑ Always trust "SR-20-180.m86.com" when connecting to "sr-20-180.m86.com"

SR-20-180.m86.com

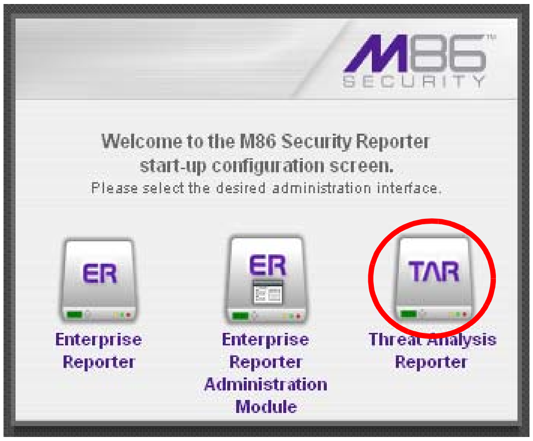
SR-20-180.m86.com
Self-signed root certificate
Expires: Sunday, February 23, 2020 9:50:04 AM PT
☒ This root certificate is not trusted

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

After the security certificate is installed, the SR Welcome window displays. Proceed to Accept the End User License Agreement.

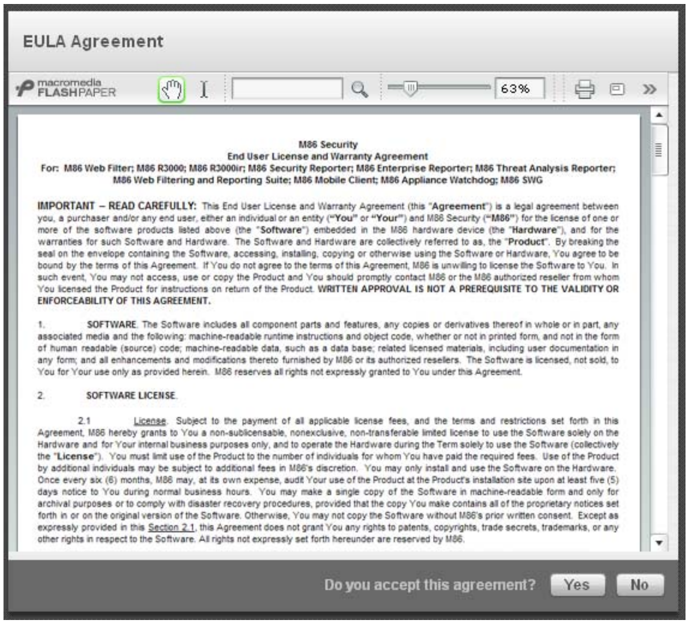
Accept the End User License Agreement

A. In the SR Welcome window, click the TAR icon:



Welcome to the M86 Security Reporter
start-up configuration screen.
Please select the desired administration interface.

After clicking the TAR icon—and accepting a security exception for the TAR application, if necessary—the EULA Agreement dialog box opens:



M86 Security
End User License and Warranty Agreement
For: M86 Web Filter; M86 R3000; M86 R3000ir; M86 Security Reporter; M86 Enterprise Reporter; M86 Threat Analysis Reporter; M86 Web Filtering and Reporting Suite; M86 Mobile Client; M86 Appliance Watchdog; M86 SWG

IMPORTANT – READ CAREFULLY: This End User License and Warranty Agreement (this "**Agreement**") is a legal agreement between you, a purchaser and/or any end user, either an individual or an entity (**"You"** or **"Your"**) and M86 Security (**"M86"**) for the license of one or more of the software products listed above (the "**Software**") embedded in the M86 hardware device (the "**Hardware**"), and for the warranties for such Software and Hardware. The Software and Hardware are collectively referred to as, the "**Product**". By breaking the seal on the envelope containing the Software, accessing, installing, copying or otherwise using the Software or Hardware, You agree to be bound by the terms of this Agreement. If You do not agree to the terms of this Agreement, M86 is unwilling to license the Software to You. In such event, You may not access, use or copy the Product and You should promptly contact M86 or the M86 authorized reseller from whom You licensed the Product for instructions on return of the Product. **WRITTEN APPROVAL IS NOT A PREREQUISITE TO THE VALIDITY OR ENFORCEABILITY OF THIS AGREEMENT.**

1. **SOFTWARE**. The Software includes all component parts and features, any copies or derivatives thereof in whole or in part, any associated media and the following: machine-readable runtime instructions and object code, whether or not in printed form, and not in the form of human readable (source) code; machine-readable data, such as a data base; related licensed materials, including user documentation in any form; and all enhancements and modifications thereto furnished by M86 or its authorized resellers. The Software is licensed, not sold, to You for Your use only as provided herein. M86 reserves all rights not expressly granted to You under this Agreement.

2. **SOFTWARE LICENSE**.

2.1 License. Subject to the payment of all applicable license fees, and the terms and restrictions set forth in this Agreement, M86 hereby grants to You a non-sublicensable, nonexclusive, non-transferable limited license to use the Software solely on the Hardware and for Your internal business purposes only, and to operate the Hardware during the Term solely to use the Software (collectively the "**License**"). You must limit use of the Product to the number of individuals for whom You have paid the required fees. Use of the Product by additional individuals may be subject to additional fees in M86's discretion. You may only install and use the Software on the Hardware. Once every six (6) months, M86 may, at its own expense, audit Your use of the Product at the Product's installation site upon at least five (5) days notice to You during normal business hours. You may make a single copy of the Software in machine-readable form and only for archival purposes or to comply with disaster recovery procedures, provided that the copy You make contains all of the proprietary notices set forth in or on the original version of the Software. Otherwise, You may not copy the Software without M86's prior written consent. Except as expressly provided in this Section 2.1, this Agreement does not grant You any rights to patents, copyrights, trade secrets, trademarks, or any other rights in respect to the Software. All rights not expressly set forth hereunder are reserved by M86.

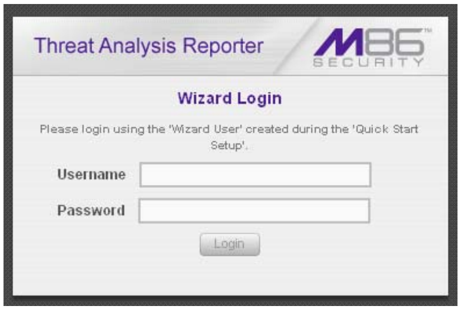
Do you accept this agreement? Yes No

B. After reading the End User License Agreement, click **Yes** to accept the EULA, close the EULA Agreement dialog box, and open the Threat Analysis Reporter Wizard Login window.

Proceed to Log in to the Threat Analysis Reporter Wizard.

Log in to the Threat Analysis Reporter Wizard

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

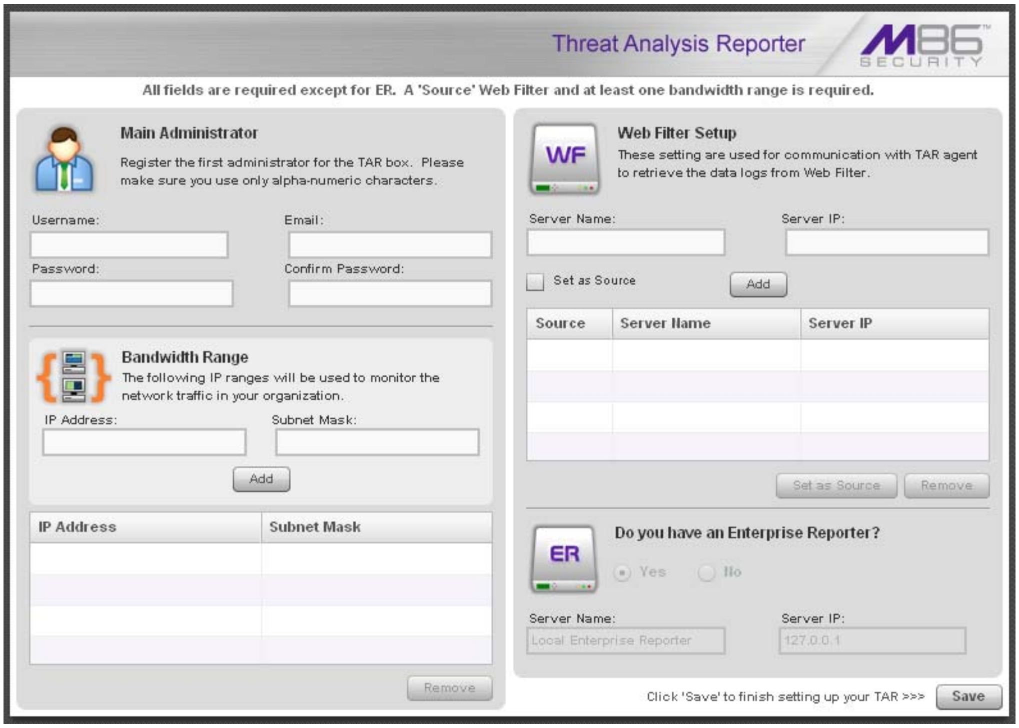


Please login using the 'Wizard User' created during the 'Quick Start Setup'.

B. In the **Password** field, type in the password specified in the Configure setup wizard user screen of the Quick Start Setup Procedures (Step 1A), or the TAR GUI Wizard screen in LCD Panel Setup Procedures (Step 1B).

C. Click **Login** to close the login window and to go to the Threat Analysis Reporter wizard screen.

Use the TAR Wizard to Specify Application Settings



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

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

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

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

○ Yes ○ No

Server Name: Local Enterprise Reporter

Server IP: 127.0.0.1

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

Enter Main Administrator Criteria

A. 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 all user applications in SR.

B. Enter the **Email** address of the global administrator, who will be notified via email regarding system alerts.

C. Enter the **Password** to be used with that username, and enter the same password again in the **Confirm Password** field.

Enter Bandwidth Range

A. Enter the bandwidth **IP Address** range the Threat Analysis Reporter will monitor.

B. Enter the **Subnet Mask** for the bandwidth IP range to be monitored, using the dotted decimals notation format.

C. Click **Add** to include your entries in the list box below.

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

Enter Web Filter Setup Criteria

A. Enter the **Server Name** of the Web Filter to be used with the Threat Analysis Reporter, which is any name you wish to associate with that Web Filter.

B. Enter the **Server IP** address of the Web Filter server to be used with the Threat Analysis Reporter.

C. Click the “Set as Source” checkbox if this Web Filter will be designated the primary Web Filter to be associated with the Threat Analysis Reporter. Otherwise, leave the checkbox blank.

D. Click **Add** to include your entries in the list box below.

***NOTES**:*

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

Enterprise Reporter registration, Save settings

The section of the wizard asking “Do you have an Enterprise Reporter?” is greyed-out since the ER is already installed on the SR appliance.

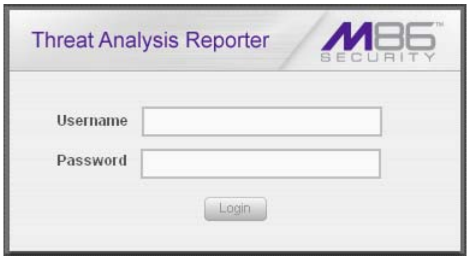
Click **Save** at the bottom right of the screen to save your settings and to go to the login window of the Threat Analysis Reporter user interface (see Step 4).

Step 4: Generate SSL Certificate

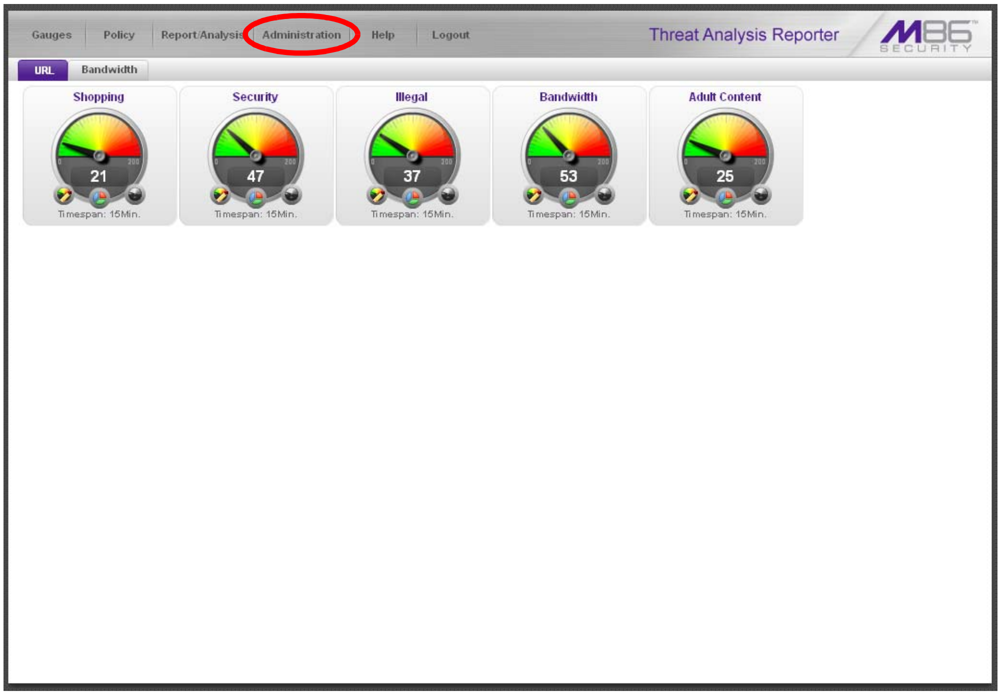
Generate a Self-Signed Certficate for the SR

This step requires you to generate a self-signed certificate so your browser will recognize the SR as an accepted device.

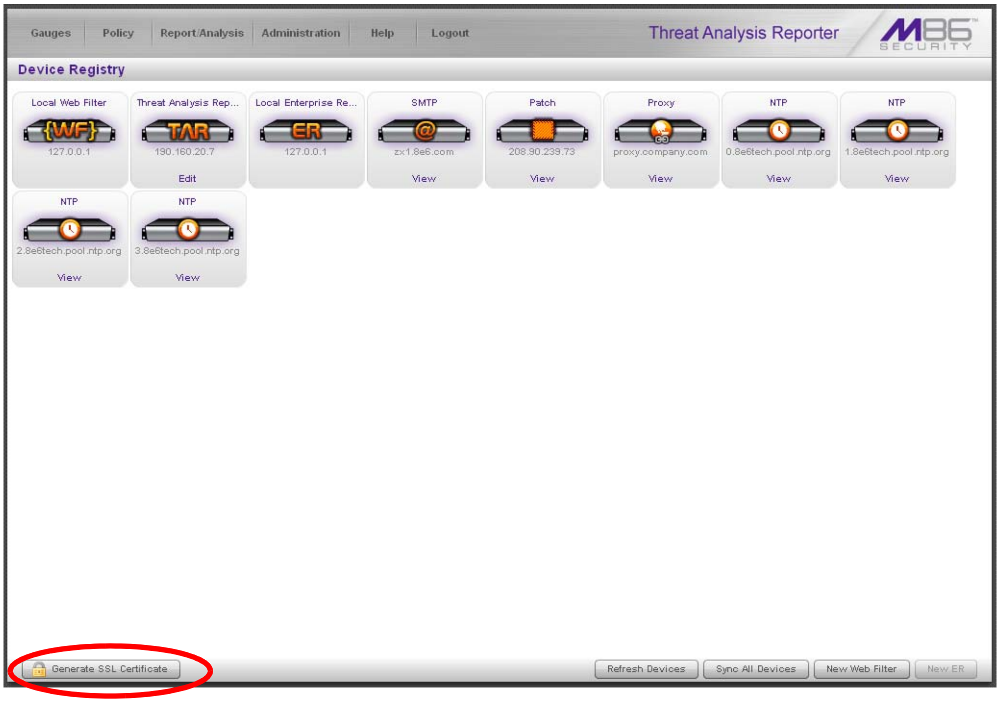
A. In the Threat Analysis Reporter login window, type in the **Username** and **Password** registered for the TAR Wizard:



B. Click **Login** to display the gauges dashboard of the TAR application:



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



D. Go to the bottom left corner of the Device Registry screen and click **Generate SSL Certificate** to open the Generate Self-Signed Certificate dialog box with the following message: "Generation of a self-signed certificate might take a long time. Afterwards, this application server would restart. Would you like to continue?"

E. Click **Yes** to begin the process. Once the self-signed certificate has been generated, you will be logged out of TAR and the SR server will be restarted.

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

If using a Firefox or Safari browser, proceed to Step 5: Set Self-Monitoring.

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

IE Security Certificate Installation Procedures

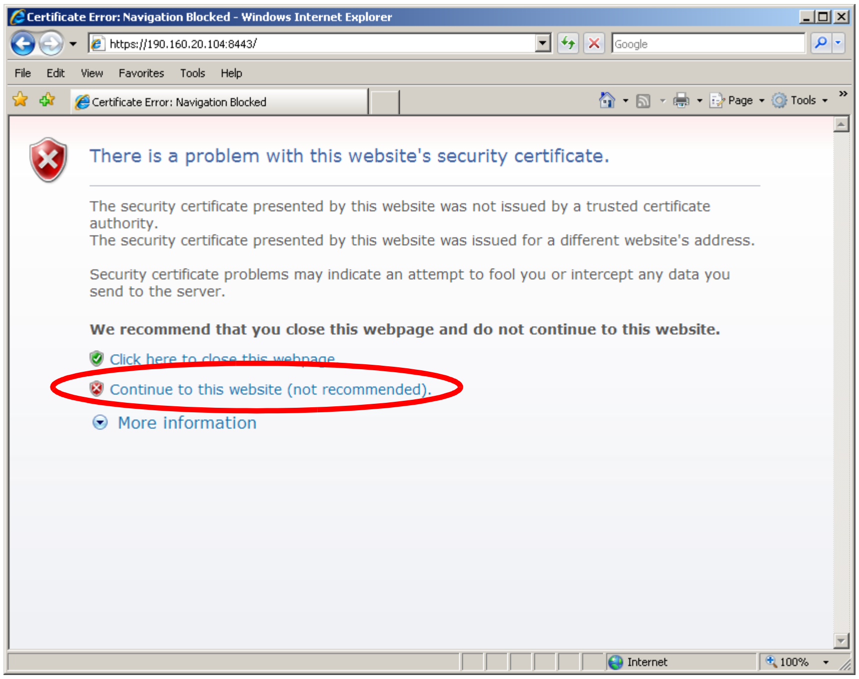
Accept the Security Certificate in IE

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

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

Windows XP or Vista with IE 7 or 8

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



Certificate Error: Navigation Blocked - Windows Internet Explorer
https://190.160.20.104:8443/
Google
File Edit View Favorites Tools Help
Certificate Error: Navigation Blocked
Page
Tools
Internet
100%

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

Figure A1: Windows XP, IE 7

Selecting this option displays the SR Welcome window with the address field and the Certificate Error button to the right of the field shaded a reddish color:

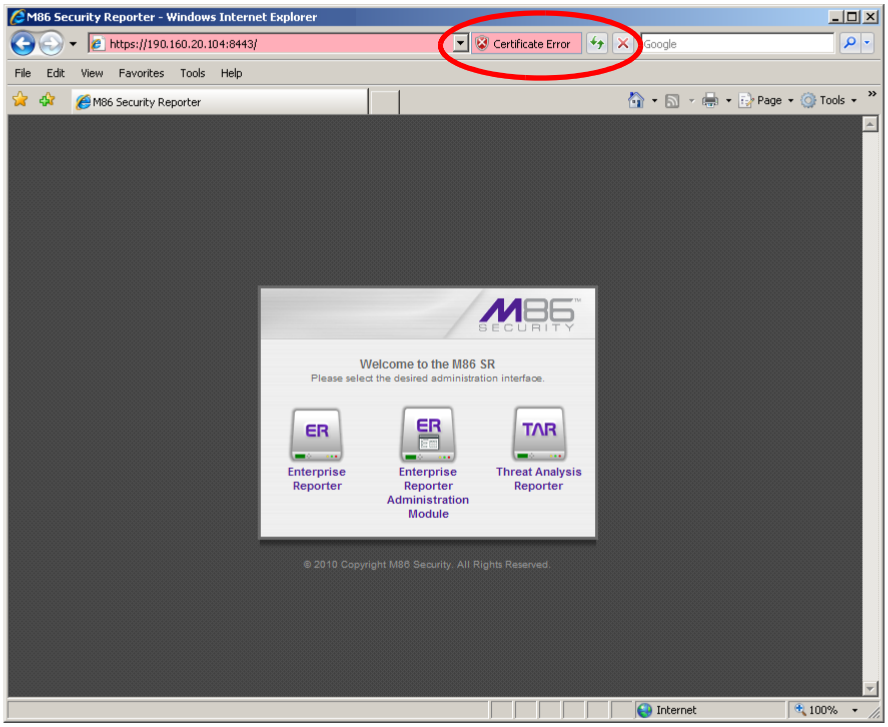
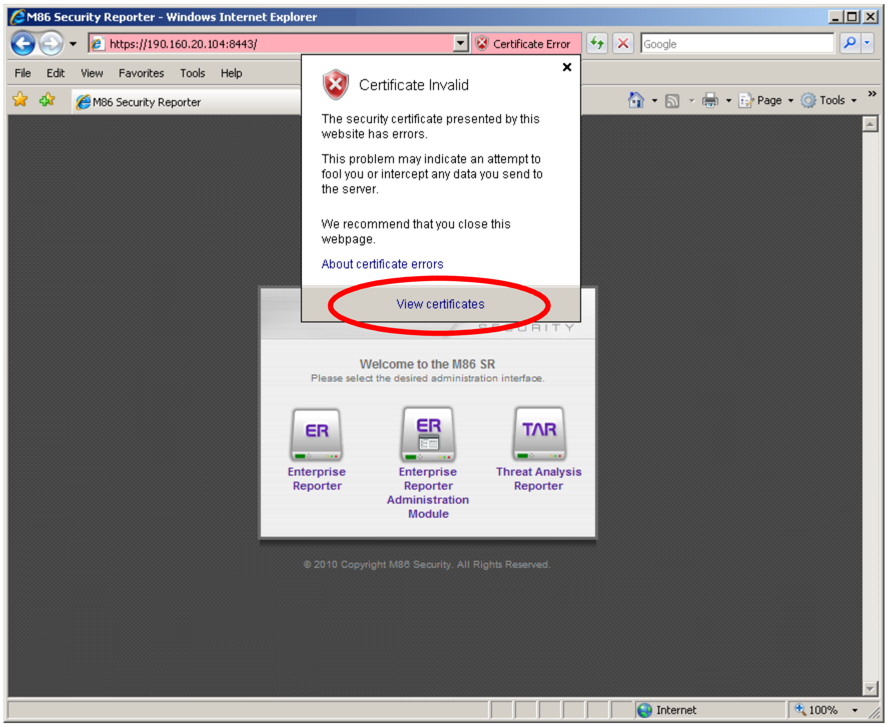

M86 Security Reporter - Windows Internet Explorer
https://190.160.20.104:8443/
Certificate Error
Google
File Edit View Favorites Tools Help
M86 Security Reporter
Page Tools
M86 SECURITY
Welcome to the M86 SR
Please select the desired administration interface.
ER
Enterprise Reporter
ER
Enterprise Reporter Administration Module
TAR
Threat Analysis Reporter
© 2010 Copyright M86 Security. All Rights Reserved.
Internet
100%

Figure A2: Windows XP, IE 7

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


M86 Security Reporter - Windows Internet Explorer
https://190.160.20.104:8443/
Certificate Error
Google
File Edit View Favorites Tools Help
M86 Security Reporter
Page Tools
Welcome to the M86 SR
Please select the desired administration interface.
ER
Enterprise Reporter
ER
Enterprise Reporter Administration Module
TAR
Threat Analysis Reporter
© 2010 Copyright M86 Security. All Rights Reserved.
Internet
100%

Certificate Invalid

The security certificate presented by this website has errors.

This problem may indicate an attempt to fool you or intercept any data you send to the server.

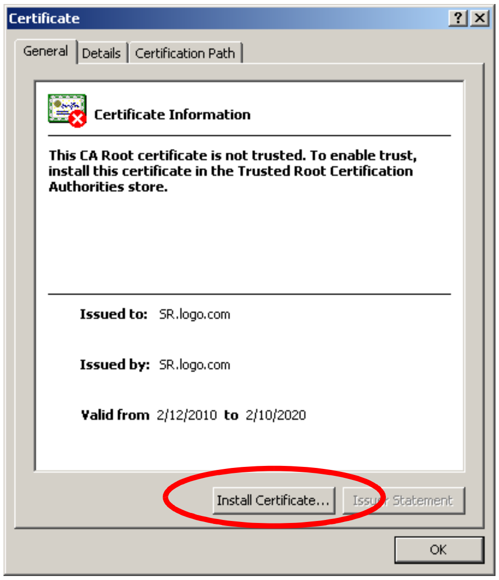
We recommend that you close this webpage.

About certificate errors

View certificates

Figure B: Windows XP, IE 7

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



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

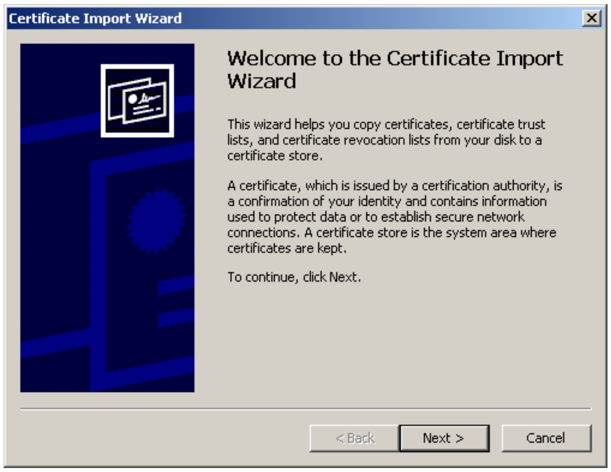
Issued to: SR.logo.com

Issued by: SR.logo.com

Valid from 2/12/2010 to 2/10/2020

Figure C: Windows XP, IE 7

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



Welcome to the Certificate Import Wizard

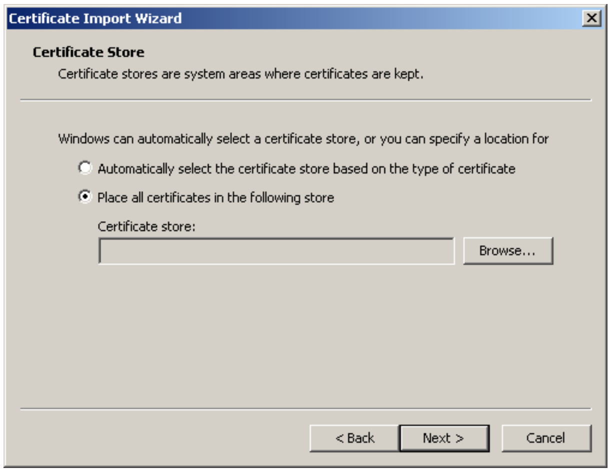
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Figure D: Windows XP, IE 7

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



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

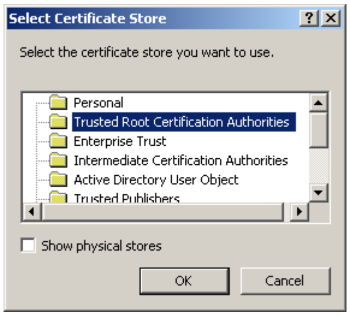
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Figure E: Windows XP, IE 7

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

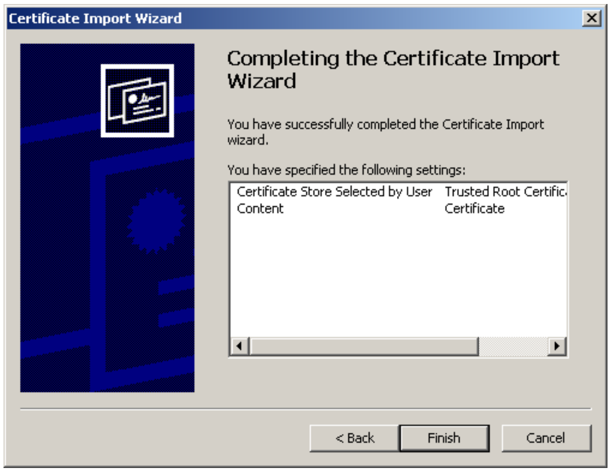


Select Certificate Store
Select the certificate store you want to use.
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
☐ Show physical stores
OK
Cancel

Figure F: Windows XP, IE 7

G. Choose “Trusted Root Certification Authorities” and then click **OK** to close the pop-up box.

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



Certificate Import Wizard

Completing the Certificate Import Wizard

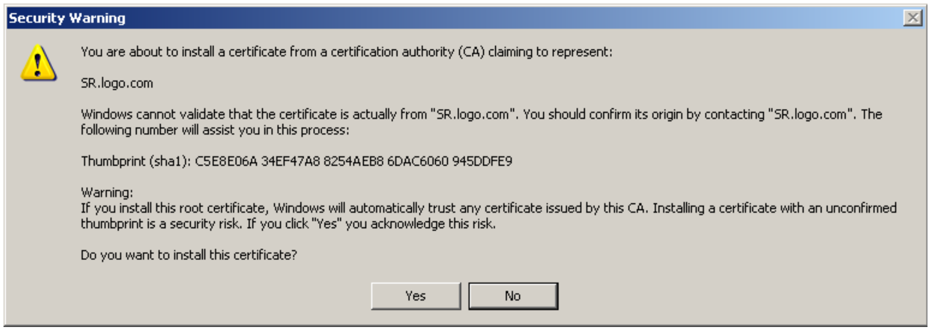
You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certific
Content	Certificate

Figure H: Windows XP, IE 7

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



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

SR.logo.com

Windows cannot validate that the certificate is actually from "SR.logo.com". You should confirm its origin by contacting "SR.logo.com". The following number will assist you in this process:

Thumbprint (sha1): C5E8E06A 34EF47A8 8254AEB8 6DAC6060 945DDFE9

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

Figure I: Windows XP, IE 7

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

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

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

Windows 7 with IE 8

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

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

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

D. In the Trusted sites pop-up box, confirm the URL displayed in the field matches the IP address of the SR, and then click **Add** and **Close**.

E. Click **OK** to close the Internet Options pop-up box.

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

G. Follow steps A to K documented in Windows XP or Vista with IE 7 or 8:

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

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

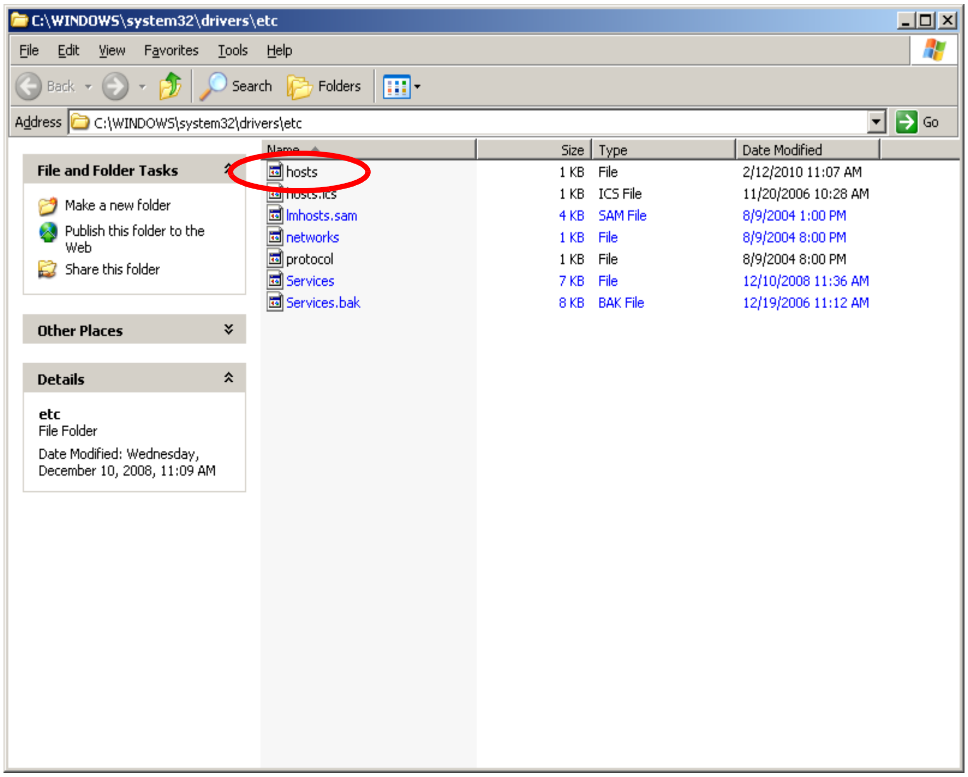
I. Select the Security tab, click **Trusted sites**, and then click **Sites** to open the Trusted sites pop-up box.

J. Select the URL you just added, click **Remove**, and then click **Close**.

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

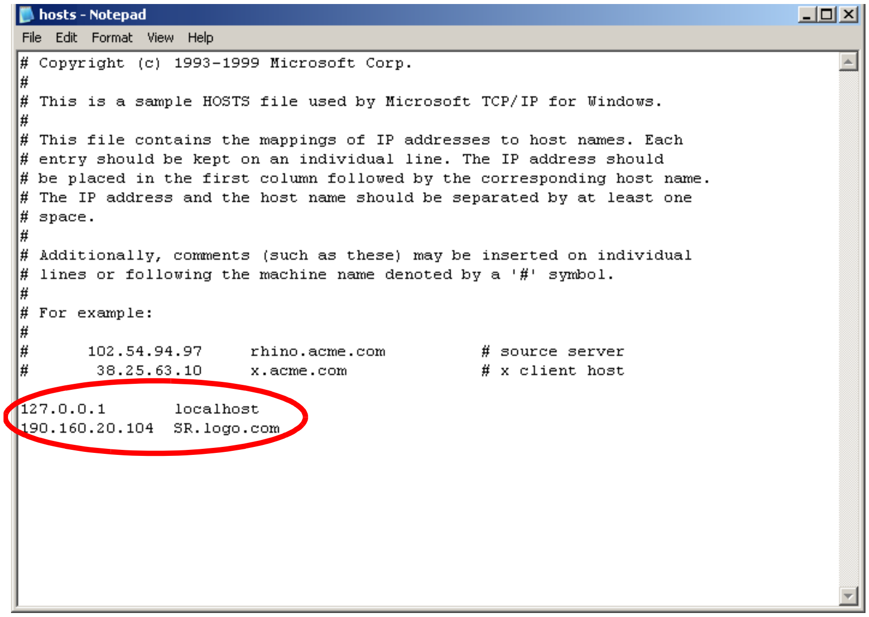
Map the SR's IP Address to the Server's Host Name

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


C:\WINDOWS\system32\drivers\etc
File
Edit
View
Favorites
Tools
Help
Back
Search
Folders
Address
C:\WINDOWS\system32\drivers\etc
Go
File and Folder Tasks
Make a new folder
Publish this folder to the Web
Share this folder
Other Places
Details
etc
File Folder
Date Modified: Wednesday, December 10, 2008, 11:09 AM

Name	Size	Type	Date Modified
hosts	1 KB	File	2/12/2010 11:07 AM
hosts.ics	1 KB	ICS File	11/20/2006 10:28 AM
lmhosts.sam	4 KB	SAM File	8/9/2004 1:00 PM
networks	1 KB	File	8/9/2004 8:00 PM
protocol	1 KB	File	8/9/2004 8:00 PM
Services	7 KB	File	12/10/2008 11:36 AM
Services.bak	8 KB	BAK File	12/19/2006 11:12 AM

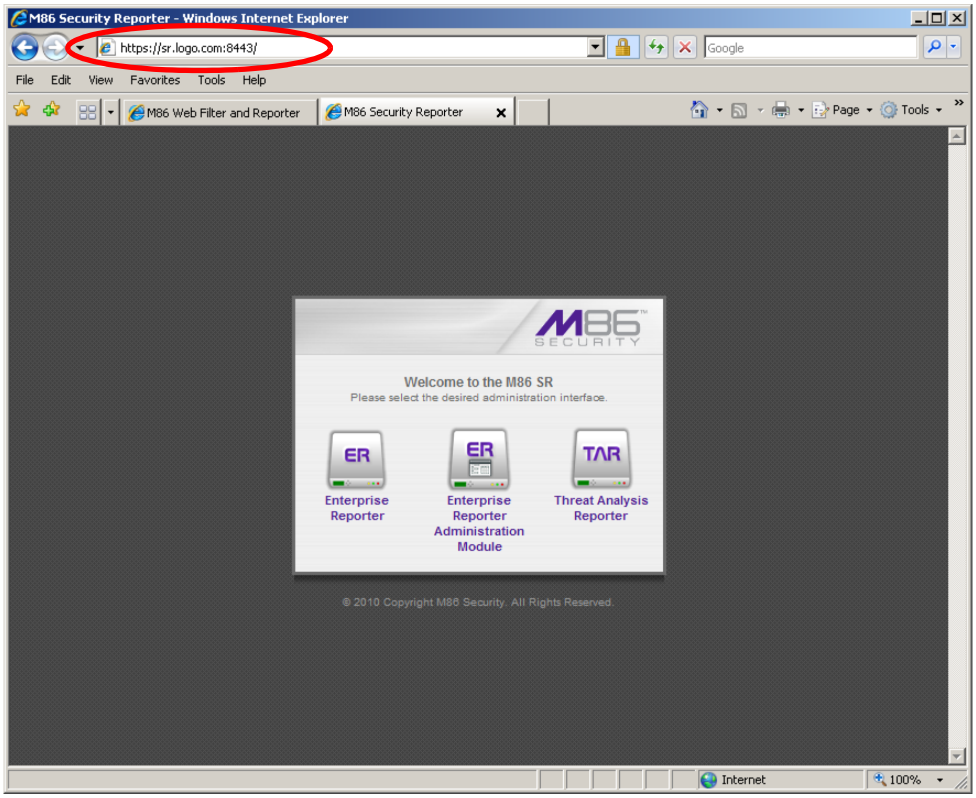
B. Double-click "hosts" to open a window asking which program you wish to use to open the file. Double-click "Notepad" or "TextPad" to launch the hosts file using that selected program:



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

127.0.0.1       localhost
190.160.20.104  SR.logo.com
```

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

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


M86 Security Reporter - Windows Internet Explorer
https://sr.logo.com:8443/
Google
File Edit View Favorites Tools Help
M86 Web Filter and Reporter
M86 Security Reporter
Page
Tools
M86 SECURITY
ER
Enterprise Reporter
ER
Enterprise Reporter Administration Module
TAR
Threat Analysis Reporter
Internet
100%

Welcome to the M86 SR

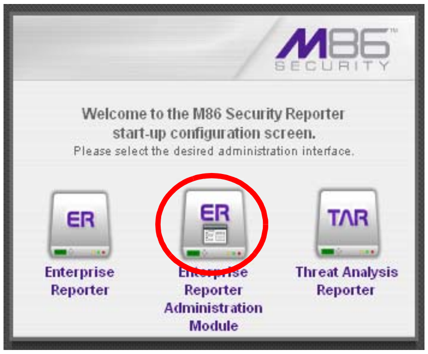
Please select the desired administration interface.

© 2010 Copyright M86 Security. All Rights Reserved.

Proceed to Step 5: Set Self-Monitoring.

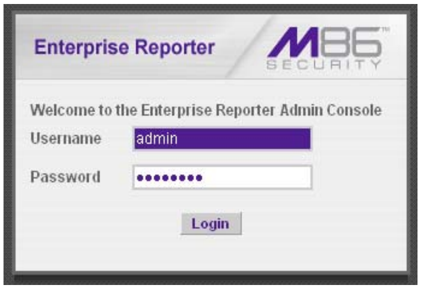
Step 5: Set Self-Monitoring

A. In the SR Welcome window, click the icon corresponding to Enterprise Reporter Administration Module:



Welcome to the M86 Security Reporter start-up configuration screen.
Please select the desired administration interface.

After clicking the ER Admin Module icon—and accepting a security exception for the ER Admin Module application, if necessary—the ER Administrator console login window opens:

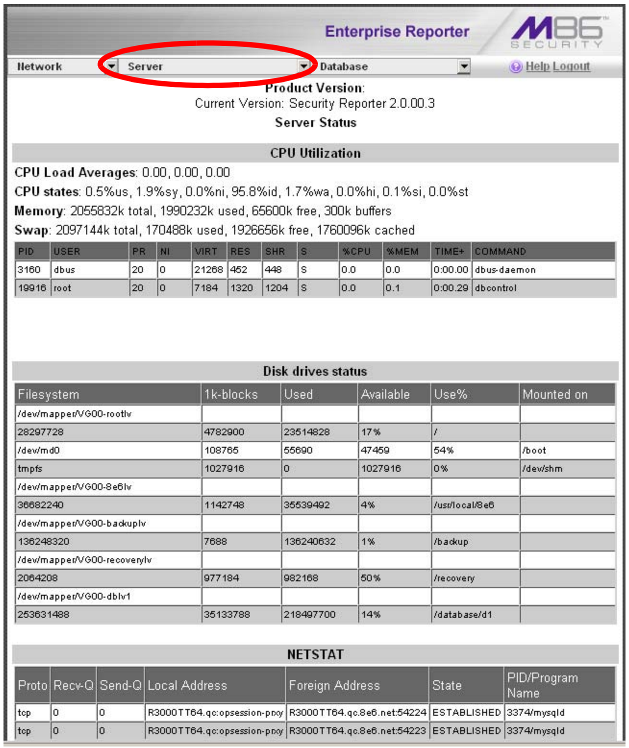


Welcome to the Enterprise Reporter Admin Console

Username: admin

Password: ••••••••

B. Type in the **Username** (***admin***) and **Password** (***reporter***), and then click **Login** to display the ER Admin console Server Status window:



Product Version:
Current Version: Security Reporter 2.0.00.3

Server Status

CPU Utilization

CPU Load Averages: 0.00, 0.00, 0.00
CPU states: 0.5%us, 1.9%sy, 0.0%ni, 95.8%id, 1.7%wa, 0.0%hi, 0.1%si, 0.0%st
Memory: 2055832k total, 1990232k used, 65600k free, 300k buffers
Swap: 2097144k total, 170488k used, 1926656k free, 1760096k cached

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
3160	dbus	20	0	21268	452	448	S	0.0	0.0	0:00.00	dbus-daemon
19916	root	20	0	7184	1320	1204	S	0.0	0.1	0:00.29	dbcontrol

Disk drives status

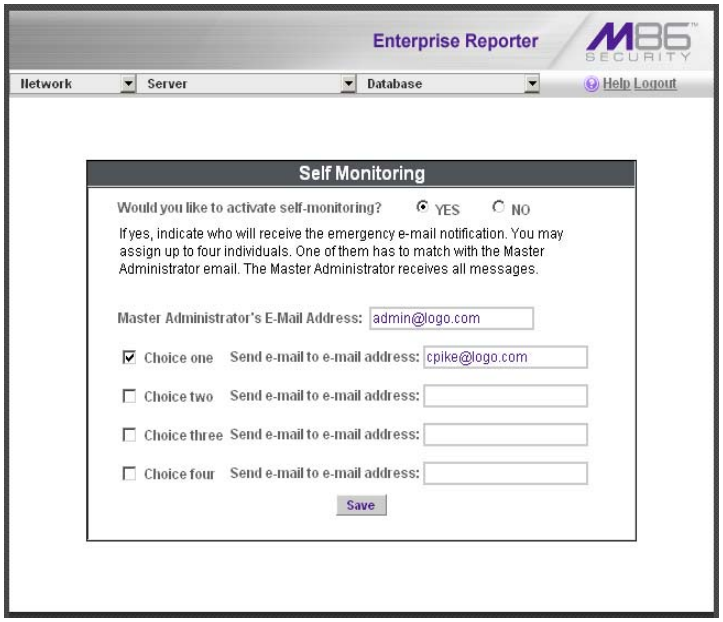
Filesystem	1k-blocks	Used	Available	Use%	Mounted on
/dev/mapper/VG00-rootlv					
28297728	4782900	23514828	17%	/	
/dev/md0	108765	55690	47459	54%	/boot
tmpfs	1027916	0	1027916	0%	/dev/shm
/dev/mapper/VG00-8e6lv					
36682240	1142748	35539492	4%	/usr/local/8e6	
/dev/mapper/VG00-backuplv					
136248320	7688	136240632	1%	/backup	
/dev/mapper/VG00-recoverylv					
2064208	977184	982168	50%	/recovery	
/dev/mapper/VG00-dblv1					
253631488	35133788	218497700	14%	/database/d1	

NETSTAT

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program Name
tcp	0	0	R3000TT64.qc:opsession-prxy	R3000TT64.qc.8e6.net:54224	ESTABLISHED	3374/mysqld
tcp	0	0	R3000TT64.qc:opsession-prxy	R3000TT64.qc.8e6.net:54223	ESTABLISHED	3374/mysqld

***NOTE**: On a new server, the ER Status pop-up window opens after you log in to the user interface of the ER Administration Module. This pop-up window will continue to open each time you log in until the ER is no longer in the evaluation mode. See the section Important Information about using the ER in the Evaluation Mode for more details about the evaluation mode.*

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



Self Monitoring

Would you like to activate self-monitoring? ● YES ○ NO

If yes, indicate who will receive the emergency e-mail notification. You may assign up to four individuals. One of them has to match with the Master Administrator email. The Master Administrator receives all messages.

Master Administrator's E-Mail Address: admin@logo.com

☑ Choice one Send e-mail to e-mail address: cpike@logo.com

□ Choice two Send e-mail to e-mail address:

□ Choice three Send e-mail to e-mail address:

□ Choice four Send e-mail to e-mail address:

D. Choose **YES** to activate monitoring.

E. Enter the **Master Administrator's E-Mail Address**.

F. Click **Choice one** and enter an e-mail address of an individual in your organization that you would like notified if the ER Admin Module detects any problems when processing data. This can be the same e-mail address entered in the previous field. Enter up to four e-mail addresses.

G. Click **Save**.

Step 6: Set up Web Filter Log Transfer

This step can be performed any time during SR setup, but must be completed in order for the SR to receive logs from the Web Filter.

Web Filter Configuration

A. Access the user interface of the Web Filter.

B. Choose the **Reporting** link at the top of the screen to display the Reporting section of the Administrator console.

C. From the navigation panel at the left of the screen, choose Report Configuration to display the Report Configuration window.

D. Select **M86 Enterprise Reporter** to display the M86 Enterprise Reporter tab.

E. In the **Server** field, enter the LAN 1 IP address you assigned to your SR, and then click **Add** to include this IP address in the Remote Server list box.

F. Click **Save**. Your Web Filter is now set to transfer its log files to your SR via HTTPS.

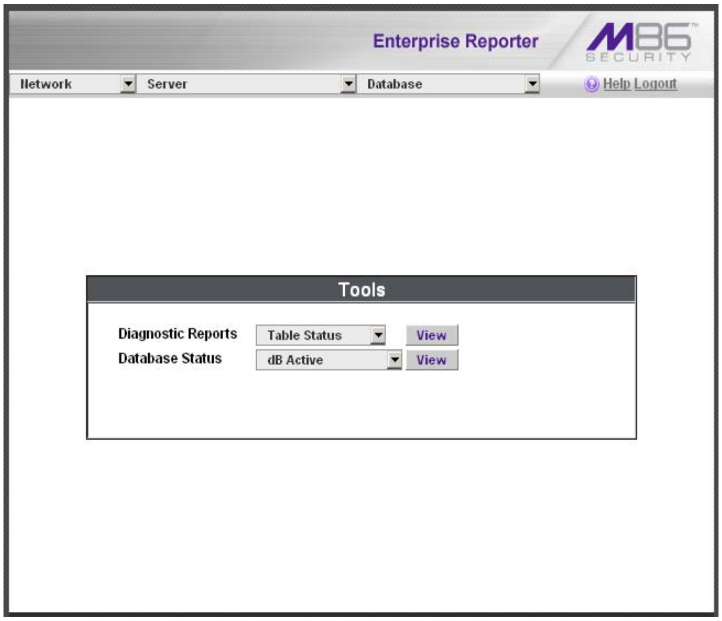
***NOTE**: It is recommended you wait for 1 - 2 hours after the initial installation so sufficient data is available for viewing.*

Log Transfer Verification

You can see if log files have transferred by following these steps:

A. Access the ER Administrator console.

B. Go to the Database pull-down menu and choose **Tools** to display the Tools screen:

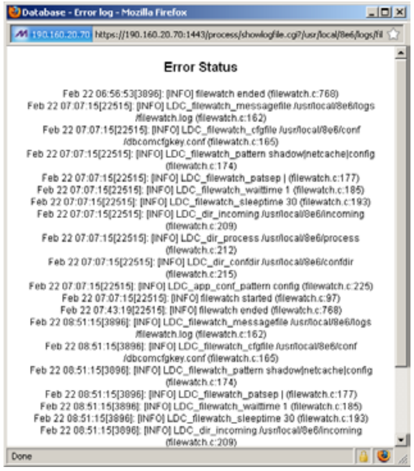


Diagnostic Reports: Table Status

Database Status: dB Active

C. From the **Database Status** menu, select **File Watch Log**.

D. Click **View** to open the Database log:



Database - Error log - Mozilla Firefox
190.160.20.70 https://190.160.20.70:1443/process/showlogfile.cgi?/usr/local/8e6/logs/fil
Done

Error Status

```
Feb 22 06:56:53[3896]: [INFO] filewatch ended (filewatch.c:768)
Feb 22 07:07:15[22515]: [INFO] LDC_filewatch_messagefile /usr/local/8e6/logs
/filewatch.log (filewatch.c:162)
Feb 22 07:07:15[22515]: [INFO] LDC_filewatch_cfgfile /usr/local/8e6/conf
/dbcomcfgkey.conf (filewatch.c:165)
Feb 22 07:07:15[22515]: [INFO] LDC_filewatch_pattern shadow|netcache|config
(filewatch.c:174)
Feb 22 07:07:15[22515]: [INFO] LDC_filewatch_patsep | (filewatch.c:177)
Feb 22 07:07:15[22515]: [INFO] LDC_filewatch_waittime 1 (filewatch.c:185)
Feb 22 07:07:15[22515]: [INFO] LDC_filewatch_sleeptime 30 (filewatch.c:193)
Feb 22 07:07:15[22515]: [INFO] LDC_dir_incoming /usr/local/8e6/incoming
(filewatch.c:209)
Feb 22 07:07:15[22515]: [INFO] LDC_dir_process /usr/local/8e6/process
(filewatch.c:212)
Feb 22 07:07:15[22515]: [INFO] LDC_dir_confdir /usr/local/8e6/confdir
(filewatch.c:215)
Feb 22 07:07:15[22515]: [INFO] LDC_app_conf_pattern config (filewatch.c:225)
Feb 22 07:07:15[22515]: [INFO] filewatch started (filewatch.c:97)
Feb 22 07:43:19[22515]: [INFO] filewatch ended (filewatch.c:768)
Feb 22 08:51:15[3896]: [INFO] LDC_filewatch_messagefile /usr/local/8e6/logs
/filewatch.log (filewatch.c:162)
Feb 22 08:51:15[3896]: [INFO] LDC_filewatch_cfgfile /usr/local/8e6/conf
/dbcomcfgkey.conf (filewatch.c:165)
Feb 22 08:51:15[3896]: [INFO] LDC_filewatch_pattern shadow|netcache|config
(filewatch.c:174)
Feb 22 08:51:15[3896]: [INFO] LDC_filewatch_patsep | (filewatch.c:177)
Feb 22 08:51:15[3896]: [INFO] LDC_filewatch_waittime 1 (filewatch.c:185)
Feb 22 08:51:15[3896]: [INFO] LDC_filewatch_sleeptime 30 (filewatch.c:193)
Feb 22 08:51:15[3896]: [INFO] LDC_dir_incoming /usr/local/8e6/incoming
(filewatch.c:209)
```

The transfer is working if you see an entry that includes the date, time, and IMPORTING: shadow.log.machine1. The transfer should occur every hour. Once you see an entry, reporting information will be available one hour after the timestamp of the import listing.

Single Sign-On Access, Default Username/Password

Access SR Applications from the TAR User Interface

By logging in to the Threat Analysis Reporter using the TAR Wizard username and password, the ER Web Client and ER Administrator console are accessible to you via the TAR user interface. This single sign-on option eliminates the process of choosing each application from the SR Welcome window and then logging in to each one.

To use the single sign-on option:

1. Log in to TAR using the TAR Wizard username and password.
2. Go to the navigation links at the top of the screen and select:
   - **Report/Analysis > Enterprise Reporter > Web Client** to access the Web Client user interface
   - **Report/Analysis > Enterprise Reporter > Admin GUI** to access the ER Administrator console

Default Usernames and Passwords for SR Applications

Default usernames and passwords for SR applications are as follows:

Application	**Username**	**Password**
ER Web Client	manager	8e6ReporT
ER Administration Module	admin	reporter
Threat Analysis Reporter	admin	testpass

***NOTE**: On a newly installed unit, you will not be able to log in to the ER Web Client until Web Filter logs are transferred to the ER Administration Module and the ER database is built. This process generally takes 24 hours.*

CONCLUSION

Congratulations; you have completed the SR installation procedures. Now that the SR server is set up on your network you will need to be sure the Web-access logging device you are using is sending log files to the ER database. Once the ER database is populated—this generally takes a full day—the ER Web Client can be used for generating reports.

Initially, you will only be able to report on IP addresses. To implement user names in ER reporting, please consult the ER Administrator portion of the Security Reporter User Guide. Refer to the ER Web Client portion of the Security Reporter User Guide for information on generating reports.

For the Threat Analysis Reporter, the next step is to set up user groups or administrator groups. You will set up and configure gauges thereafter.

Obtain the latest Security Reporter User Guide at **http://www.m86security.com/support/sr/documentation.asp** .

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

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

BEST REPORTING PRACTICES

This Best Reporting Practices section is provided to help you get started using the Threat Analysis Reporter and Enterprise Reporter Web Client applications. Each of the two applications has its own sub-section with scenarios for configuring and using basic tools in the user interface of each product.

In the Threat Analysis Reporter Usage Scenarios sub-section 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

In the Enterprise Reporter Usage Scenarios sub-section you will learn how to:

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

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

Threat Analysis Reporter Usage Scenarios

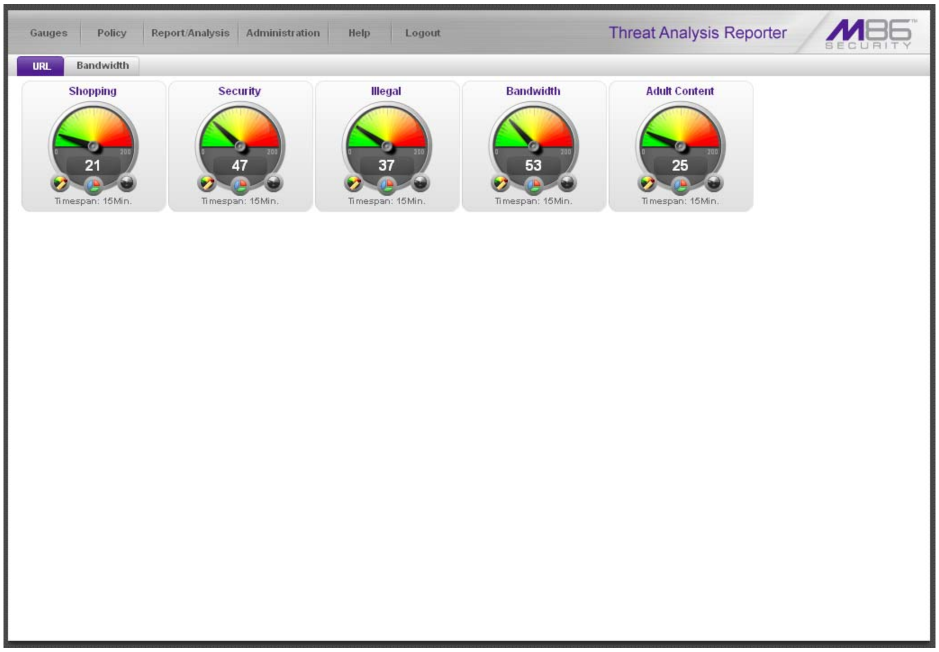
This collection of setup and usage scenarios is designed to help you understand and use basic tools in the console for enforcing your Internet usage policy. Each scenario is followed by console setup information. Please consult the “How to” section in the index of the Security Reporter User Guide for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

I. Screen navigation exercise

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

Step A: Navigate panels in the Gauges section

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



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

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

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

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

Step B: Navigate panels in the Policy section

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

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

Step C: Navigate panels in the Report/Analysis section

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

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

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

Step D: Navigate panels in the Administration section

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

- **Admin Trails** - view a list of alert records for the most recent time period
- **Device Registry** - view information about devices connected to the SR, edit M86 Security appliance criteria, add or delete a Web Filter from the device registry, generate an SSL certificate for the SR server, and synchronize the Threat Analysis Reporter user groups and library categories

- **User Profiles** - manage a list of end users' logged events
- **Add/Edit Admins** - manage group administrator profiles
- **Admin Groups** - set permissions so that an administrator in your group will only be able to access areas of the Threat Analysis Reporter console that you specify
- **User Groups** - manage user groups whose activity will be monitored by gauges
- **Backup/Restore** - perform a backup and/or restoration of files on the Threat Analysis Reporter application

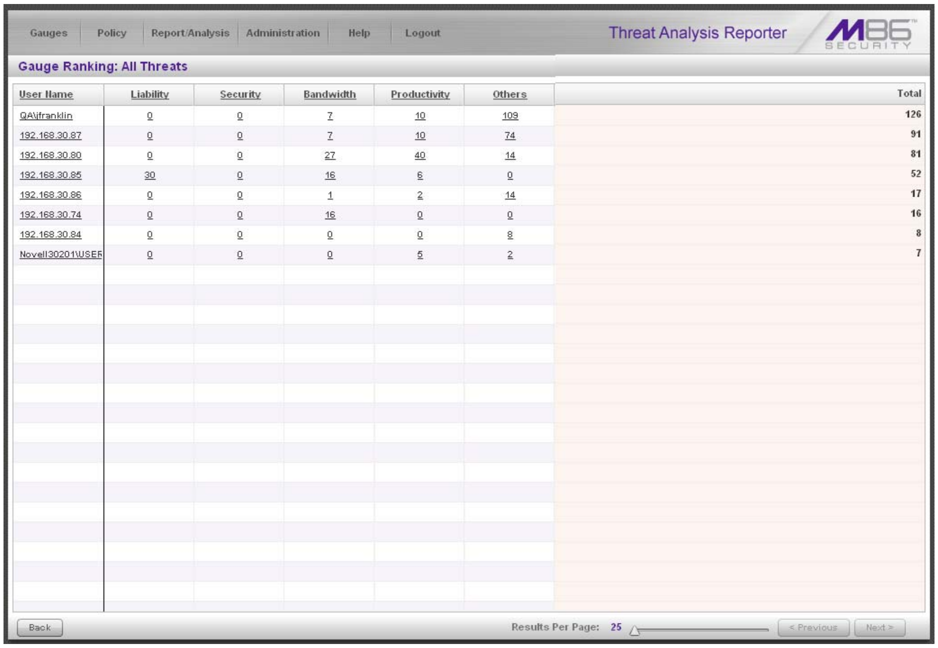
In the Security Reporter User Guide index, see:
• How to: navigate the TAR user interface

II. Drill down into a gauge exercise

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

Step A: Select the gauge with the highest score

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



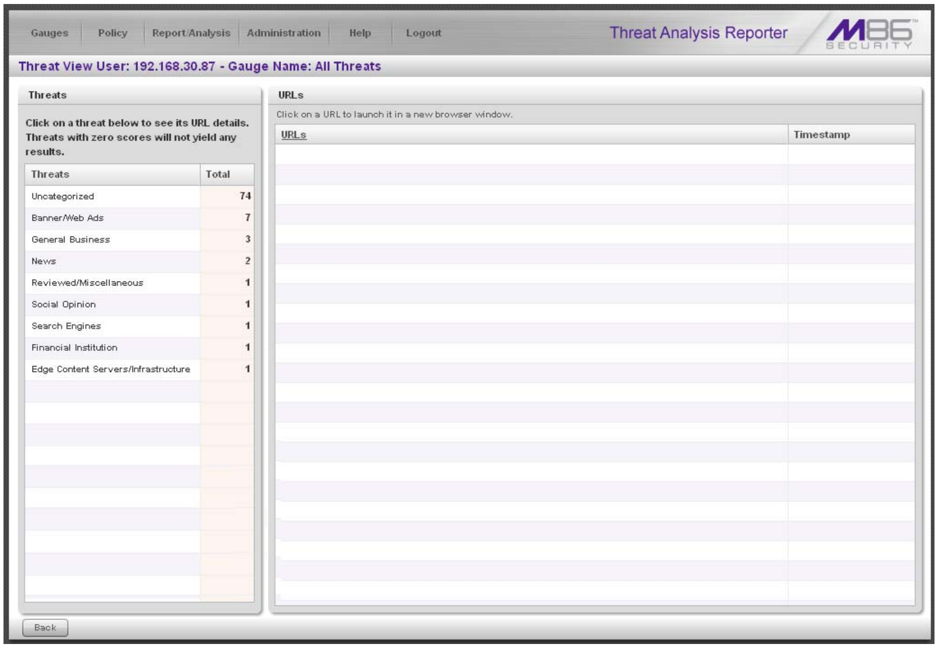
Gauge Ranking: All Threats

User Name	Liability	Security	Bandwidth	Productivity	Others	Total
QA\jfranklin	0	0	7	10	109	126
192.168.30.87	0	0	7	10	74	91
192.168.30.80	0	0	27	40	14	81
192.168.30.85	30	0	16	6	0	52
192.168.30.86	0	0	1	2	14	17
192.168.30.74	0	0	16	0	0	16
192.168.30.84	0	0	0	0	8	8
Novell30201\USER	0	0	0	5	2	7

Results Per Page: 25

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

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



Threat View User: 192.168.30.87 - Gauge Name: All Threats

Threats

Click on a threat below to see its URL details. Threats with zero scores will not yield any results.

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

URLs

Click on a URL to launch it in a new browser window.

URLs	Timestamp

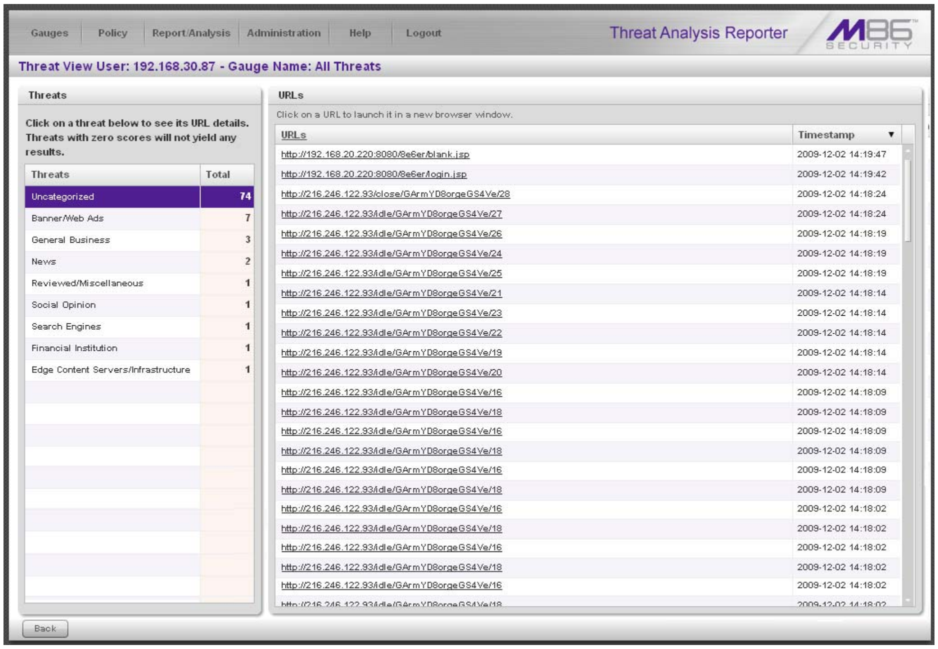
Note the left side of this panel is populated with rows of records for Threats affected by the selected end user.

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

In the Security Reporter User Guide index, see:
• How to: drill down into a gauge

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

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



Threat View User: 192.168.30.87 - Gauge Name: All Threats

Threats

Click on a threat below to see its URL details. Threats with zero scores will not yield any results.

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

URLs

Click on a URL to launch it in a new browser window.

URLs	Timestamp ▼
http://192.168.20.220:8080/8e6er/blank.jsp	2009-12-02 14:19:47
http://192.168.20.220:8080/8e6er/login.jsp	2009-12-02 14:19:42
http://216.246.122.93/close/GArmYD8orgeGS4Ve/28	2009-12-02 14:18:24
http://216.246.122.93/idle/GArmYD8orgeGS4Ve/27	2009-12-02 14:18:24
http://216.246.122.93/idle/GArmYD8orgeGS4Ve/26	2009-12-02 14:18:19
http://216.246.122.93/idle/GArmYD8orgeGS4Ve/24	2009-12-02 14:18:19
http://216.246.122.93/idle/GArmYD8orgeGS4Ve/25	2009-12-02 14:18:19
http://216.246.122.93/idle/GArmYD8orgeGS4Ve/21	2009-12-02 14:18:14
http://216.246.122.93/idle/GArmYD8orgeGS4Ve/23	2009-12-02 14:18:14
http://216.246.122.93/idle/GArmYD8orgeGS4Ve/22	2009-12-02 14:18:14
http://216.246.122.93/idle/GArmYD8orgeGS4Ve/19	2009-12-02 14:18:14
http://216.246.122.93/idle/GArmYD8orgeGS4Ve/20	2009-12-02 14:18:14
http://216.246.122.93/idle/GArmYD8orgeGS4Ve/16	2009-12-02 14:18:09
http://216.246.122.93/idle/GArmYD8orgeGS4Ve/18	2009-12-02 14:18:09
http://216.246.122.93/idle/GArmYD8orgeGS4Ve/16	2009-12-02 14:18:09
http://216.246.122.93/idle/GArmYD8orgeGS4Ve/18	2009-12-02 14:18:09
http://216.246.122.93/idle/GArmYD8orgeGS4Ve/16	2009-12-02 14:18:09
http://216.246.122.93/idle/GArmYD8orgeGS4Ve/18	2009-12-02 14:18:09
http://216.246.122.93/idle/GArmYD8orgeGS4Ve/16	2009-12-02 14:18:02
http://216.246.122.93/idle/GArmYD8orgeGS4Ve/18	2009-12-02 14:18:02
http://216.246.122.93/idle/GArmYD8orgeGS4Ve/16	2009-12-02 14:18:02
http://216.246.122.93/idle/GArmYD8orgeGS4Ve/18	2009-12-02 14:18:02
http://216.246.122.93/idle/GArmYD8orgeGS4Ve/16	2009-12-02 14:18:02
http://216.246.122.93/idle/GArmYD8orgeGS4Ve/18	2009-12-02 14:18:02

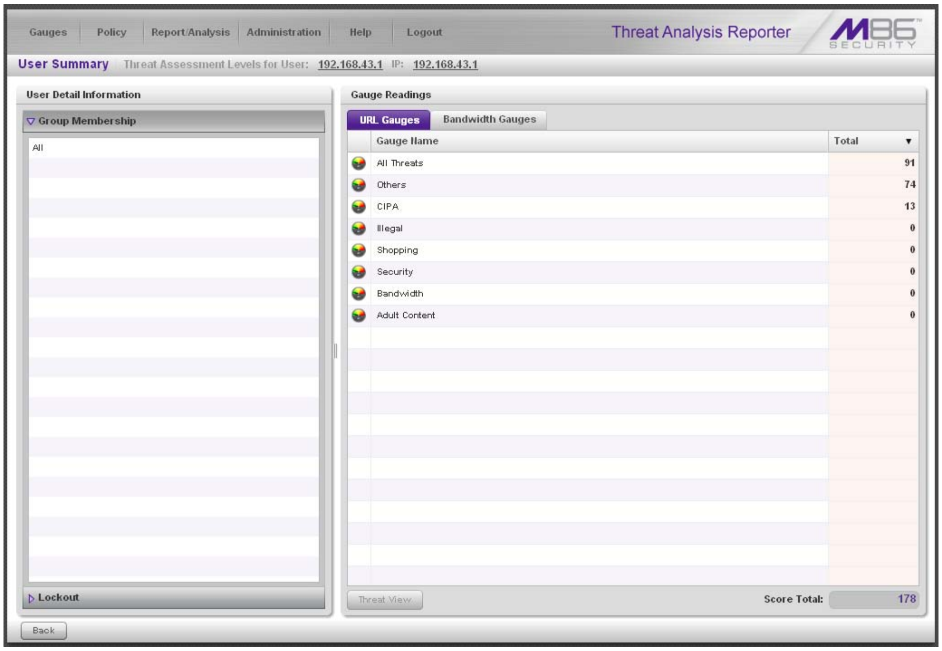
2. Choose a URL you wish to view, and then click it to open a separate browser window accessing that URL.

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

In the Security Reporter User Guide index, see:
• How to: view URLs a user visited in TAR

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

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



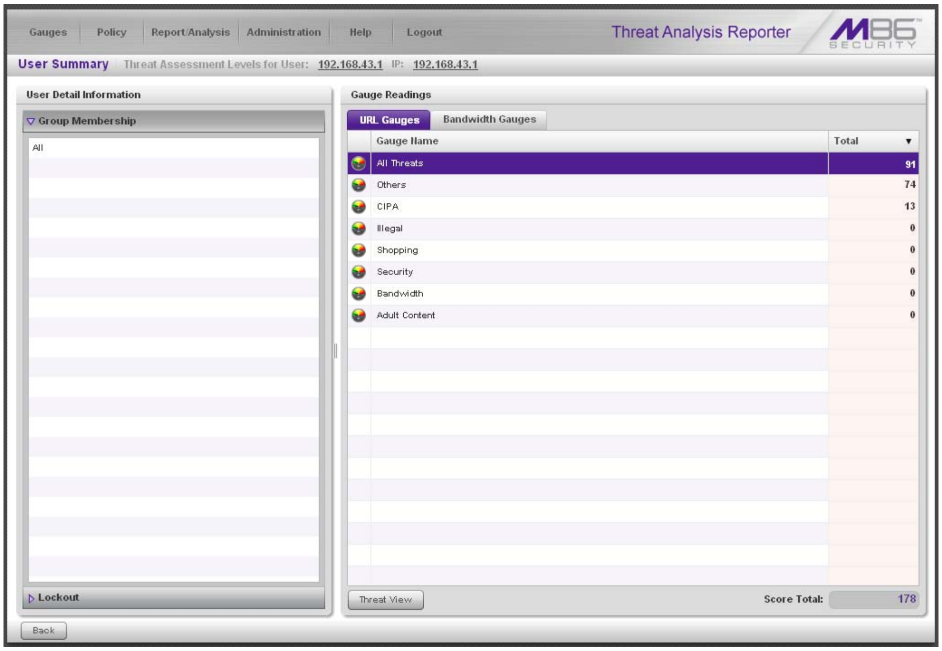
Threat Assessment Levels for User: 192.168.43.1 IP: 192.168.43.1

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

Score Total: 178

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

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



Threat Assessment Levels for User: 192.168.43.1 IP: 192.168.43.1

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

Score Total: 178

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

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

In the Security Reporter User Guide index, see:
• How to: view end user gauge activity

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

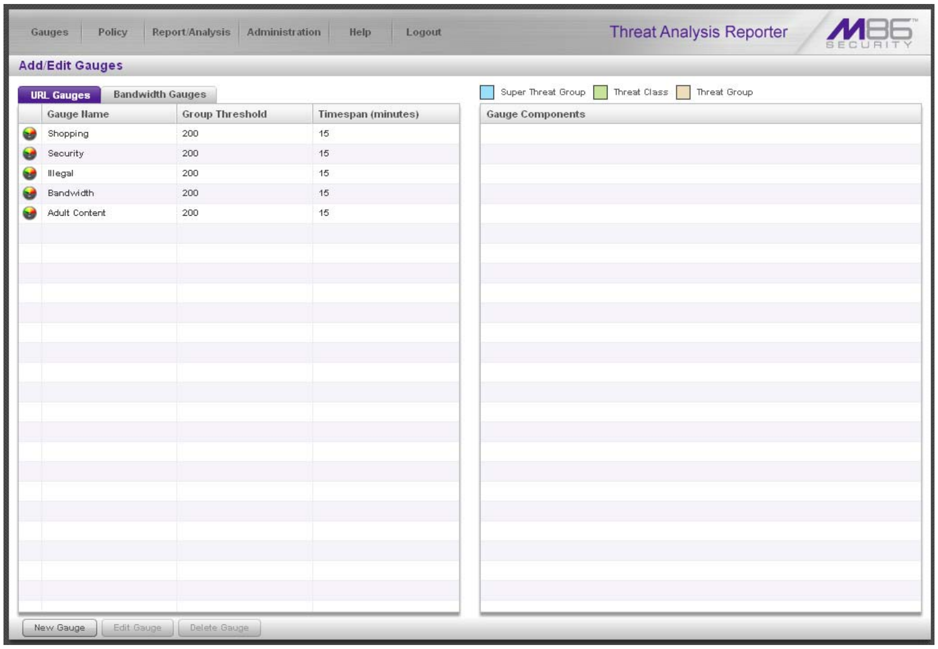
When you become accustomed to using the Threat Analysis Reporter on a regular basis to conduct these types of investigations, you will eventually want to explore other tools in the interface to restrict or lock out offending users from accessing certain library categories.

III. Create a gauge exercise

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

Step A: Access the Add/Edit Gauges panel

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



Add/Edit Gauges

🟦 Super Threat Group 🟩 Threat Class 🟨 Threat Group

	Gauge Name	Group Threshold	Timespan (minutes)
●	Shopping	200	15
●	Security	200	15
●	Illegal	200	15
●	Bandwidth	200	15
●	Adult Content	200	15

Gauge Components

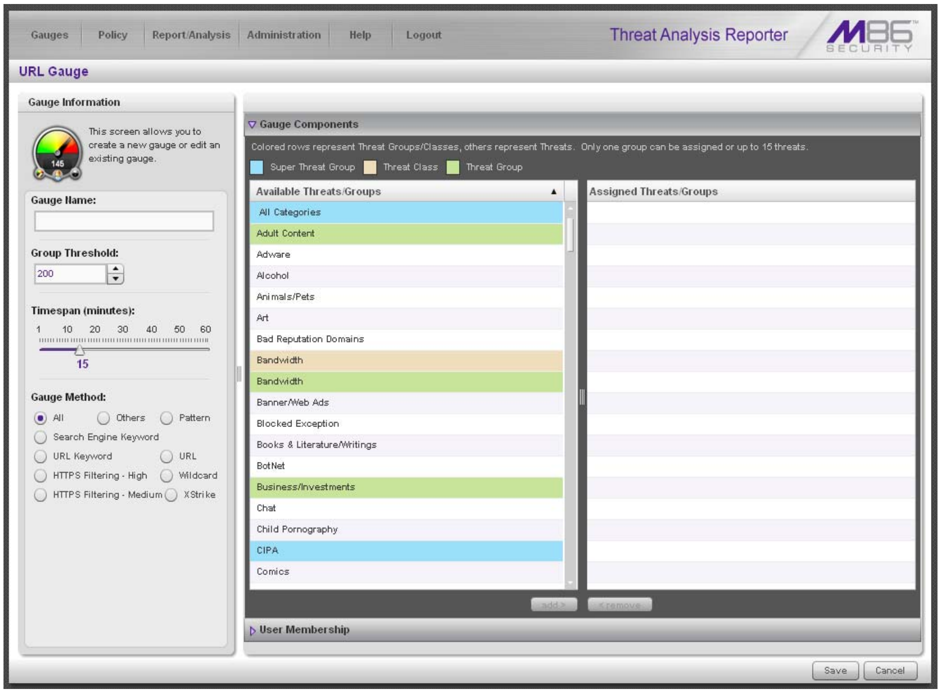
Note that this panel contains the current Gauge Name list at the left side.

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

In the Security Reporter User Guide index, see:
• How to: access the Add/Edit Gauges panel

Step B: Add a URL Gauge

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



Gauge Information

This screen allows you to create a new gauge or edit an existing gauge.

Gauge Name:

Group Threshold: 200

Timespan (minutes): 1 10 20 30 40 50 60 — 15

Gauge Method:

● All ○ Others ○ Pattern
○ Search Engine Keyword
○ URL Keyword ○ URL
○ HTTPS Filtering - High ○ Wildcard
○ HTTPS Filtering - Medium ○ XStrike

▽ Gauge Components

Colored rows represent Threat Groups/Classes, others represent Threats. Only one group can be assigned or up to 15 threats.

🟦 Super Threat Group 🟧 Threat Class 🟩 Threat Group

Available Threats/Groups ▲	Assigned Threats/Groups
All Categories	
Adult Content	
Adware	
Alcohol	
Animals/Pets	
Art	
Bad Reputation Domains	
Bandwidth	
Bandwidth	
Banner/Web Ads	
Blocked Exception	
Books & Literature/Writings	
BotNet	
Business/Investments	
Chat	
Child Pornography	
CIPA	
Comics	

▷ User Membership

2. In the Gauge Information frame to the left, specify the following information as necessary:

   a. **Gauge Name** you wish to use and display for this gauge; this entry must be at least two characters in length.

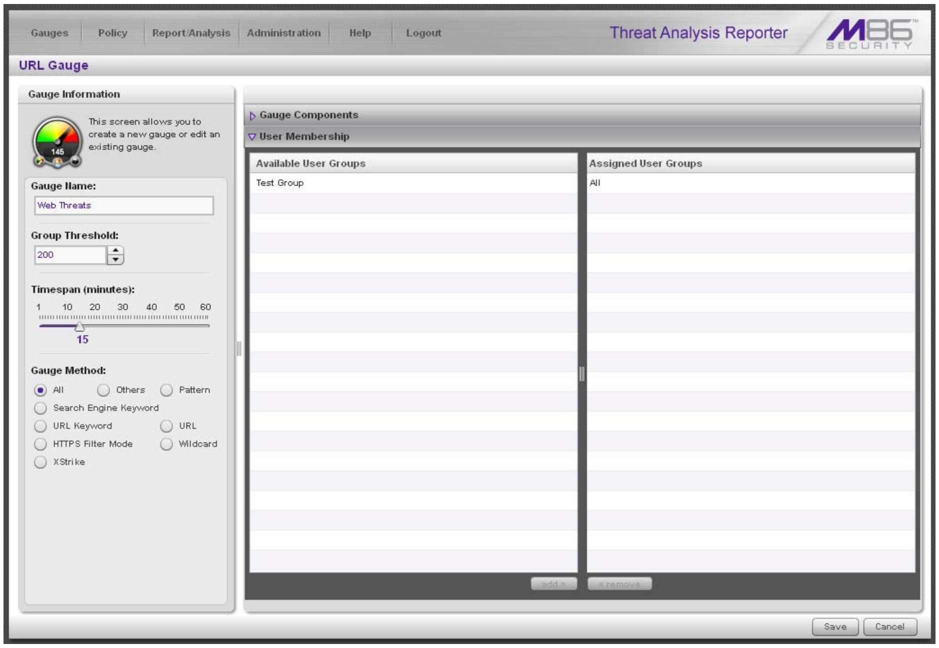
   b. **Group Threshold** for the ceiling of gauge activity. For this exercise we will use the default and recommended value, which is 200 for a URL gauge.

   c. **Timespan (minutes)** for tracking gauge activity (1 - 60 minutes). For this exercise we will use the default and recommended value, which is 15 minutes.

   d. **Gauge Method** to be used for tracking gauge activity. For this exercise we will use the default “All” gauge method, so you do not need to make any selection from the drop-down menu. The selected “All” method considers all methods users can use to access URLs in library categories included in the gauge.

3. In the Available Threats/Groups list to the right, select one Threat Class/Group, or up to 15 library categories by clicking each one while pressing the **Ctrl** key on your keyboard. When you have made your selection(s) for the gauge to monitor, click the **add >** button to move the choice(s) to the Assigned Threats/ Groups list box.

4. Click the User Membership accordion to open it and to display a list of Available User Groups in the list to the left:



URL Gauge

Gauge Information

This screen allows you to create a new gauge or edit an existing gauge.

Gauge Name: Web Threats

Group Threshold: 200

Timespan (minutes): 1 10 20 30 40 50 60 — 15

Gauge Method:

● All ○ Others ○ Pattern
○ Search Engine Keyword
○ URL Keyword ○ URL
○ HTTPS Filter Mode ○ Wildcard
○ XStrike

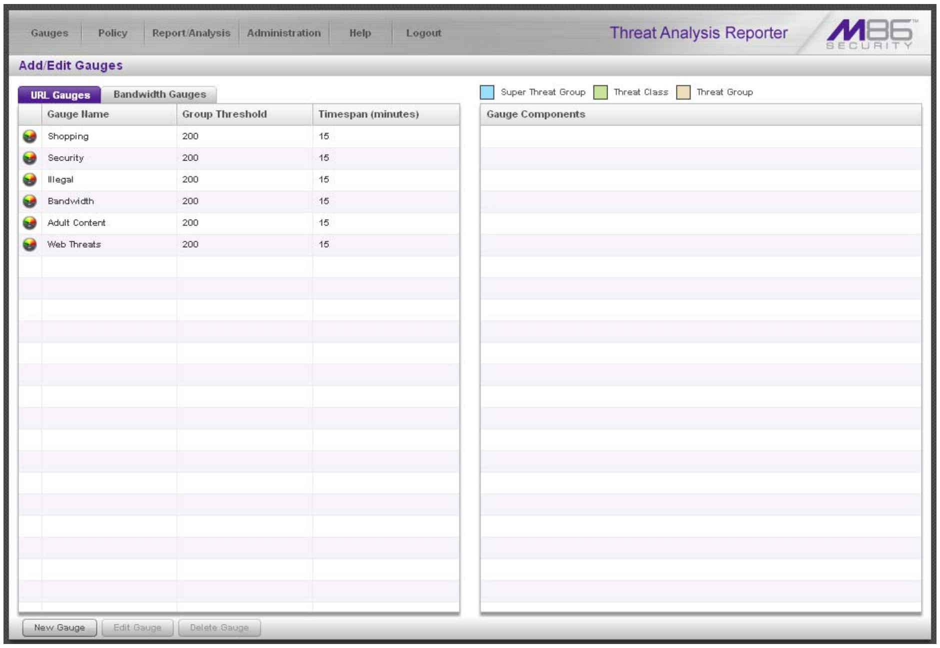
User Membership

Available User Groups	Assigned User Groups
Test Group	All

5. From the Available User Groups list, select the user group to highlight it.

6. Click **add >** to move the user group to the Assigned User Groups list box.

7. After adding users, click **Save** at the bottom right of the panel to return to the Add/Edit Gauges panel that now includes the name of the gauge you just added:



Add/Edit Gauges

Gauge Name	Group Threshold	Timespan (minutes)
Shopping	200	15
Security	200	15
Illegal	200	15
Bandwidth	200	15
Adult Content	200	15
Web Threats	200	15

In the Security Reporter User Guide index, see:
• How to: add new a gauge

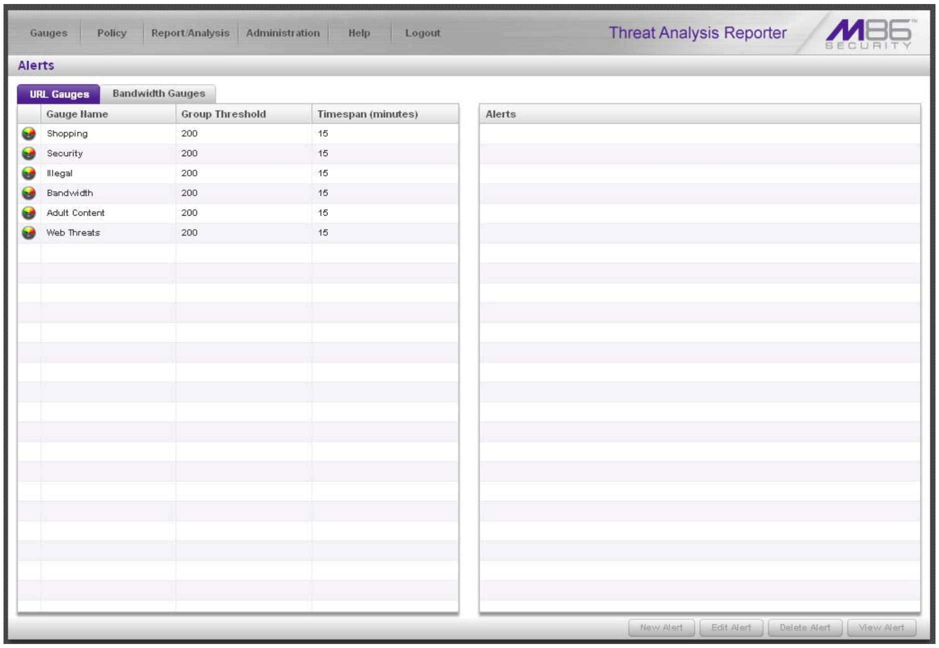
Now that you know the basics of creating a gauge, you will soon be able to create and use gauges to monitor various groups of users who frequent URLs in library categories you wish to restrict, and deal in real time with Internet usage issues that endanger your network and/or consume an excessive amount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

IV. Create an email alert exercise

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

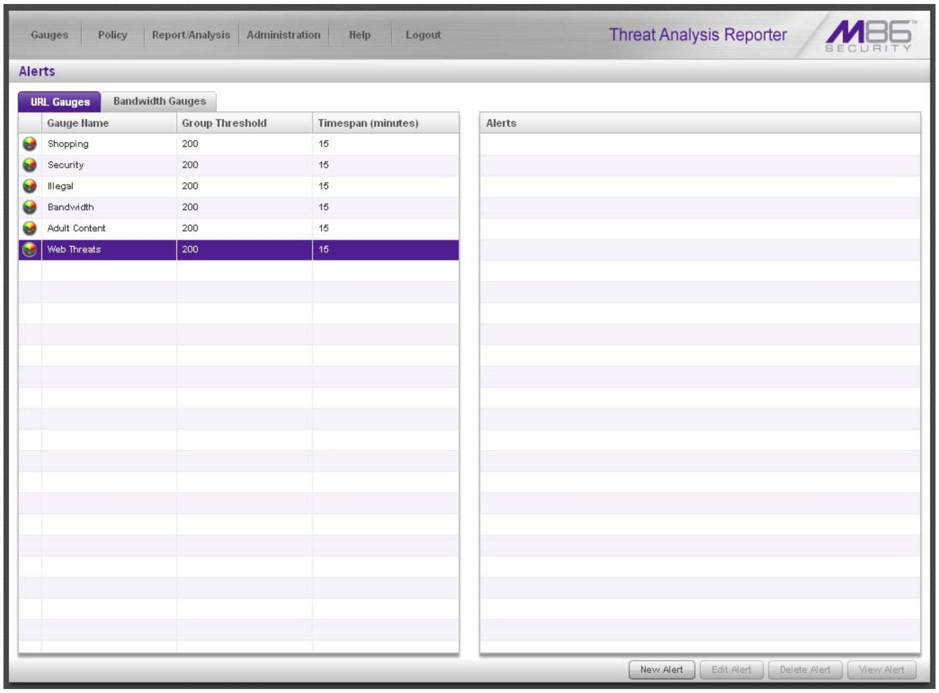
Step A: Add a new alert

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



Gauge Name	Group Threshold	Timespan (minutes)
Shopping	200	15
Security	200	15
Illegal	200	15
Bandwidth	200	15
Adult Content	200	15
Web Threats	200	15

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



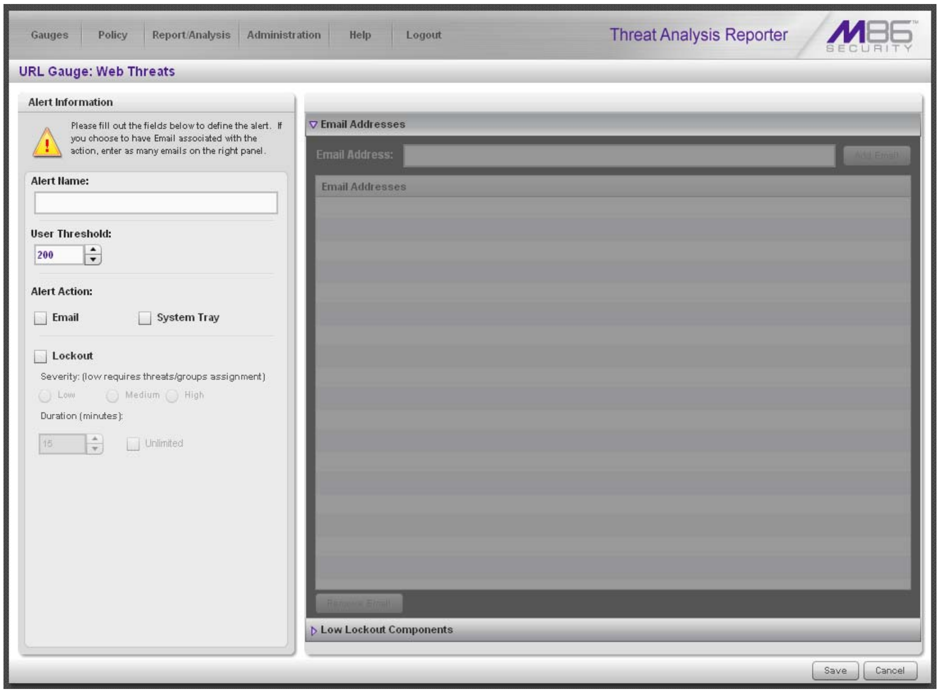
Alerts

URL Gauges | Bandwidth Gauges

Gauge Name	Group Threshold	Timespan (minutes)
Shopping	200	15
Security	200	15
Illegal	200	15
Bandwidth	200	15
Adult Content	200	15
Web Threats	200	15

Alerts

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



URL Gauge: Web Threats

Alert Information

Please fill out the fields below to define the alert. If you choose to have Email associated with the action, enter as many emails on the right panel.

Alert Name:

User Threshold: 200

Alert Action:

□ Email □ System Tray

□ Lockout

Severity: (low requires threats/groups assignment)

○ Low ○ Medium ○ High

Duration (minutes):

15 □ Unlimited

▽ Email Addresses

Email Address:

Email Addresses

▷ Low Lockout Components

4. Type in the **Alert Name** to be used for the alert that will be delivered to the group administrator.

5. Specify the **User Threshold** ceiling of gauge activity that will trigger the alert. The default and recommended value is 200 for a URL gauge.

6. Specify the **Alert Action** method(s) to be used for alert notifications:

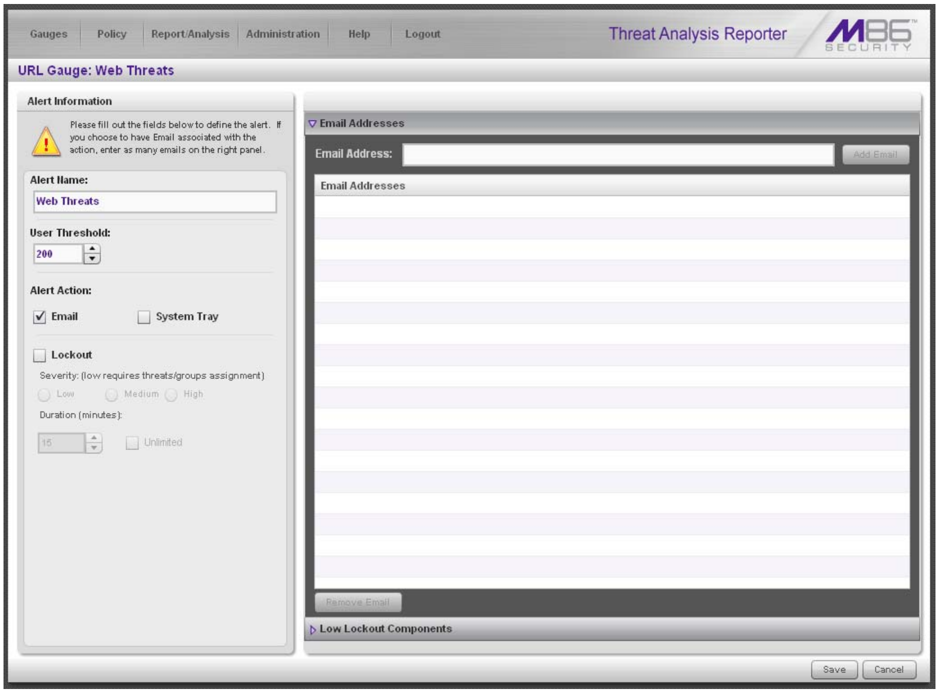
- **Email** - An email alert notifies a group administrator via email if an end user has reached the threshold limit set up in a gauge alert.
- **System Tray** - A TAR Alert message notifies a group administrator via his/her workstation's System Tray if an end user has reached the threshold limit set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

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

In the Security 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.



URL Gauge: Web Threats

Alert Information

Please fill out the fields below to define the alert. If you choose to have Email associated with the action, enter as many emails on the right panel.

Alert Name: Web Threats

User Threshold: 200

Alert Action:

☑ Email ☐ System Tray

☐ Lockout

Severity: (low requires threats/groups assignment)

○ Low ○ Medium ○ High

Duration (minutes): 15 ☐ Unlimited

Email Address:

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

2. In the **Email Address** field, type in the email address to which the alert will be sent, and then click **Add Email** to include the email address in the list box above.

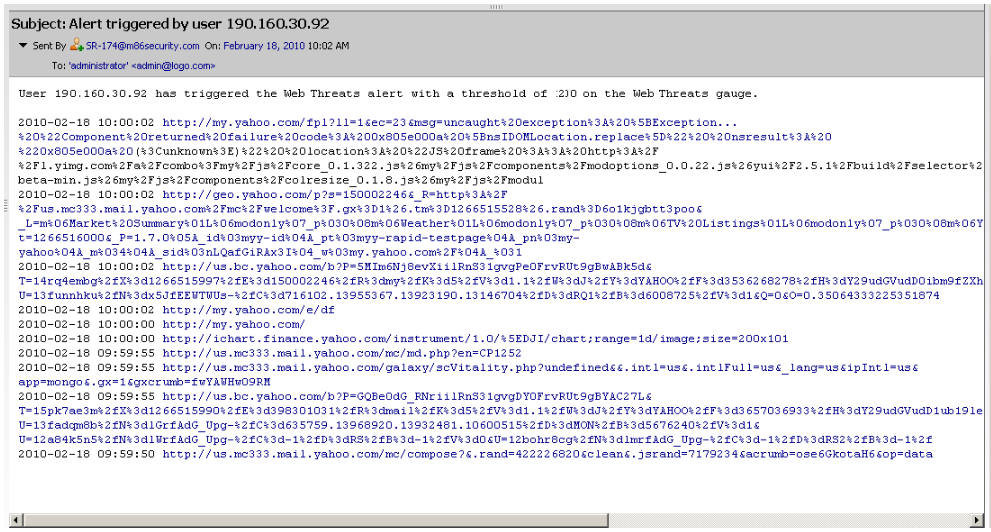
3. Click **Save** at the bottom right of the panel to save your entries and to display the Alerts panel.

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

In the Security Reporter User Guide index, see:
• How to: set up email alert notifications in TAR

Step D: Receiving an email alert

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



Subject: Alert triggered by user 190.160.30.92
Sent By SR-174@m86security.com On: February 18, 2010 10:02 AM
To: 'administrator' <admin@logo.com>

```
User 190.160.30.92 has triggered the Web Threats alert with a threshold of :2)0 on the Web Threats gauge.

2010-02-18 10:00:02 http://my.yahoo.com/fp1?ll=1&ec=23&msg=uncaught%20exception%3A%20%5BException...
%20%22Component%20returned%20failure%20code%3A%200x805e000a%20%5BnsIDOMLocation.replace%5D%22%20%20nsresult%3A%20
%220x805e000a%20(%3Cunknown%3E)%22%20%20location%3A%20%22JS%20frame%20%3A%3A%20http%3A%2F
%2Fl.yimg.com%2Fa%2Fcombo%3Fmy%2Fjs%2Fcore_0.1.322.js%26my%2Fjs%2Fcomponents%2Fmodoptions_0.0.22.js%26yui%2F2.5.1%2Fbuild%2Fselector%2
beta-min.js%26my%2Fjs%2Fcomponents%2Fcolresize_0.1.8.js%26my%2Fjs%2Fmodul
2010-02-18 10:00:02 http://geo.yahoo.com/p?s=150002246&_R=http%3A%2F
%2Fus.mc333.mail.yahoo.com%2Fmc%2Fwelcome%3F.gx%3D1%26.tm%3D1266515528%26.rand%3D6o1kjgbtt3poo&
_L=m%06Market%20Summary%01L%06modonly%07_p%030%08m%06Weather%01L%06modonly%07_p%030%08m%06TV%20Listings%01L%06modonly%07_p%030%08m%06Y
t=1266516000&_P=1.7.0%05A_id%03myy-id%04A_pt%03myy-rapid-testpage%04A_pn%03my-
yahoo%04A_m%034%04A_sid%03nLQafGiRAx3I%04_w%03my.yahoo.com%2F%04A_%031
2010-02-18 10:00:02 http://us.bc.yahoo.com/b?P=5MIm6Nj8evXiilRnS31gvgPeOFrvRUt9gBwABk5d&
T=14rq4embg%2fX%3d1266515997%2fE%3d150002246%2fR%3dmy%2fK%3d5%2fV%3d1.1%2fW%3dJ%2fY%3dYAHOO%2fF%3d3536268278%2fH%3dY29udGVudD0ibm9fZXh
U=13funnhku%2fN%3dx5JfEEWTWUs-%2fC%3d716102.13955367.13923190.13146704%2fD%3dRQ1%2fB%3d6008725%2fV%3d1&Q=0&O=0.3506433225351874
2010-02-18 10:00:02 http://my.yahoo.com/e/df
2010-02-18 10:00:00 http://my.yahoo.com/
2010-02-18 10:00:00 http://ichart.finance.yahoo.com/instrument/1.0/%5EDJI/chart;range=1d/image;size=200x101
2010-02-18 09:59:55 http://us.mc333.mail.yahoo.com/mc/md.php?en=CP1252
2010-02-18 09:59:55 http://us.mc333.mail.yahoo.com/galaxy/scVitality.php?undefined&&.intl=us&.intlFull=us&_lang=us&ipIntl=us&
app=mongo&.gx=1&gxcrumb=fwYAWHwO9RM
2010-02-18 09:59:55 http://us.bc.yahoo.com/b?P=GQBeOdG_RNriilRnS31gvgDYOFrvRUt9gBYAC27L&
T=15pk7ae3m%2fX%3d1266515990%2fE%3d398301031%2fR%3dmail%2fK%3d5%2fV%3d1.1%2fW%3dJ%2fY%3dYAHOO%2fF%3d3657036933%2fH%3dY29udGVudD1ub19le
U=13fadqm8b%2fN%3dlGrfAdG_Upg-%2fC%3d635759.13968920.13932481.10600515%2fD%3dMON%2fB%3d5676240%2fV%3d1&
U=12a84k5n5%2fN%3dlWrfAdG_Upg-%2fC%3d-1%2fD%3dRS%2fB%3d-1%2fV%3d0&U=12bohr8cg%2fN%3dlmrfAdG_Upg-%2fC%3d-1%2fD%3dRS2%2fB%3d-1%2f
2010-02-18 09:59:50 http://us.mc333.mail.yahoo.com/mc/compose?&.rand=422226820&clean&.jsrand=7179234&acrumb=ose6GkotaH6&op=data
```

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 Security Reporter User Guide index, see:
• How to: view an email alert in TAR

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

Enterprise Reporter Usage Scenarios

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

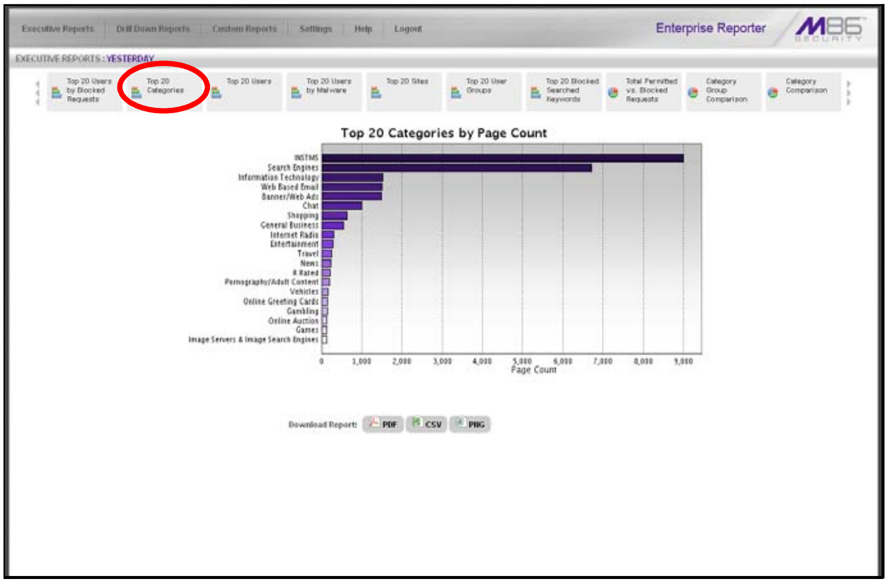
I. Executive Report and Drill Down Report exercise

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

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

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

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



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

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

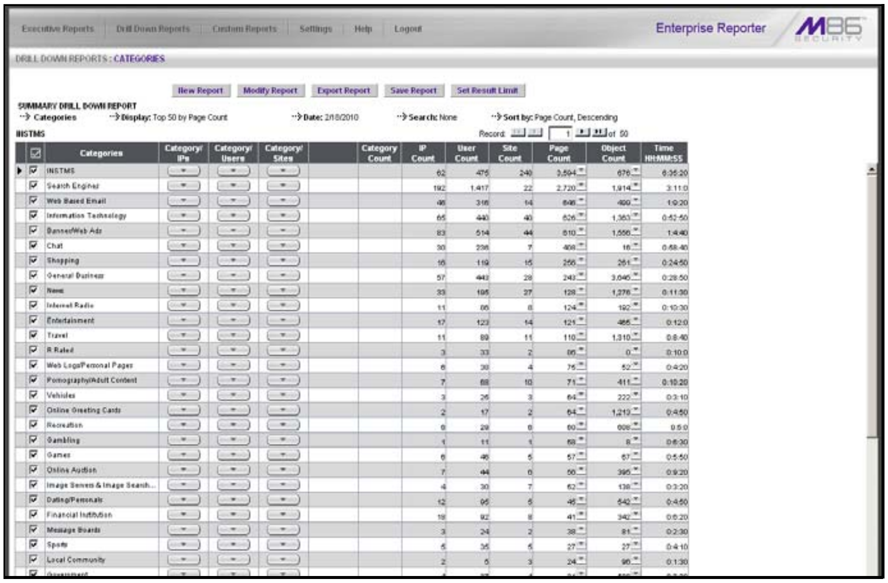
***NOTE**: Click the left or right arrow in the dashboard to view additional thumbnails.*

In the Security Reporter User Guide index, see:
• How to: generate an Executive Report

Step B: Further investigate using a Summary Drill Down Report

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

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



DRILL DOWN REPORTS : CATEGORIES

SUMMARY DRILL DOWN REPORT
→ Categories → Display: Top 50 by Page Count → Date: 2/18/2010 → Search: None → Sort by: Page Count, Descending

INSTMS Record: 1 of 50

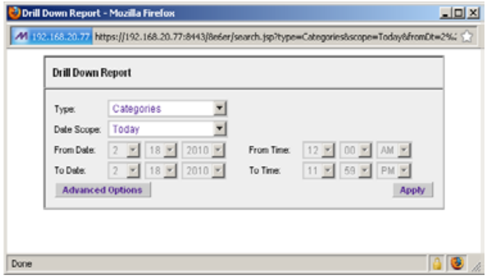
☑	Categories	Category/ IPs	Category/ Users	Category/ Sites		Category Count	IP Count	User Count	Site Count	Page Count	Object Count	Time HH:MM:SS
☑	INSTMS	▾	▾	▾			62	475	240	3,594	676	6:35:20
☑	Search Engines	▾	▾	▾			192	1,417	22	2,720	1,914	3:11:0
☑	Web Based Email	▾	▾	▾			46	316	14	646	490	1:0:20
☑	Information Technology	▾	▾	▾			65	440	40	626	1,363	0:52:50
☑	Banner/Web Ads	▾	▾	▾			83	514	44	610	1,556	1:4:40
☑	Chat	▾	▾	▾			30	236	7	408	16	0:58:40
☑	Shopping	▾	▾	▾			16	119	15	256	261	0:24:50
☑	General Business	▾	▾	▾			57	442	28	243	3,046	0:28:50
☑	News	▾	▾	▾			33	195	27	128	1,276	0:11:30
☑	Internet Radio	▾	▾	▾			11	66	8	124	192	0:10:30
☑	Entertainment	▾	▾	▾			17	123	14	121	466	0:12:0
☑	Travel	▾	▾	▾			11	89	11	110	1,310	0:8:40
☑	R Rated	▾	▾	▾			3	33	2	86	0	0:10:0
☑	Web Logs/Personal Pages	▾	▾	▾			6	38	4	76	52	0:4:20
☑	Pornography/Adult Content	▾	▾	▾			7	68	10	71	411	0:10:20
☑	Vehicles	▾	▾	▾			3	26	3	64	222	0:3:10
☑	Online Greeting Cards	▾	▾	▾			2	17	2	64	1,213	0:4:50
☑	Recreation	▾	▾	▾			6	29	6	60	606	0:5:0
☑	Gambling	▾	▾	▾			1	11	1	58	8	0:6:30
☑	Games	▾	▾	▾			6	46	5	57	67	0:5:50
☑	Online Auction	▾	▾	▾			7	44	6	56	395	0:9:20
☑	Image Servers & Image Search...	▾	▾	▾			4	30	7	52	138	0:3:20
☑	Dating/Personals	▾	▾	▾			12	96	5	46	542	0:4:50
☑	Financial Institution	▾	▾	▾			18	92	8	41	342	0:6:20
☑	Message Boards	▾	▾	▾			3	24	2	38	81	0:2:30
☑	Sports	▾	▾	▾			5	35	5	27	27	0:4:10
☑	Local Community	▾	▾	▾			2	5	3	24	96	0:1:30
☑	Government	▾	▾	▾			[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

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

In the Security Reporter User Guide index, see:
• How to: generate a Drill Down Report

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

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



https://192.168.20.77:8443/8e6er/search.jsp?type=Categories&scope=Today&fromDt=2%

Type: Categories
Date Scope: Today
From Date: 2 18 2010 From Time: 12 00 AM
To Date: 2 18 2010 To Time: 11 59 PM

2. By default, "Today" displays in the **Date Scope** field. Choose "Yesterday" from this menu.
3. Click **Apply** to accept your selection and to close the pop-up window. The regenerated report now displays yesterday's data in the Summary Drill Down Report view.

In the Security Reporter User Guide index, see:
• How to: create a New Report from the current report view

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

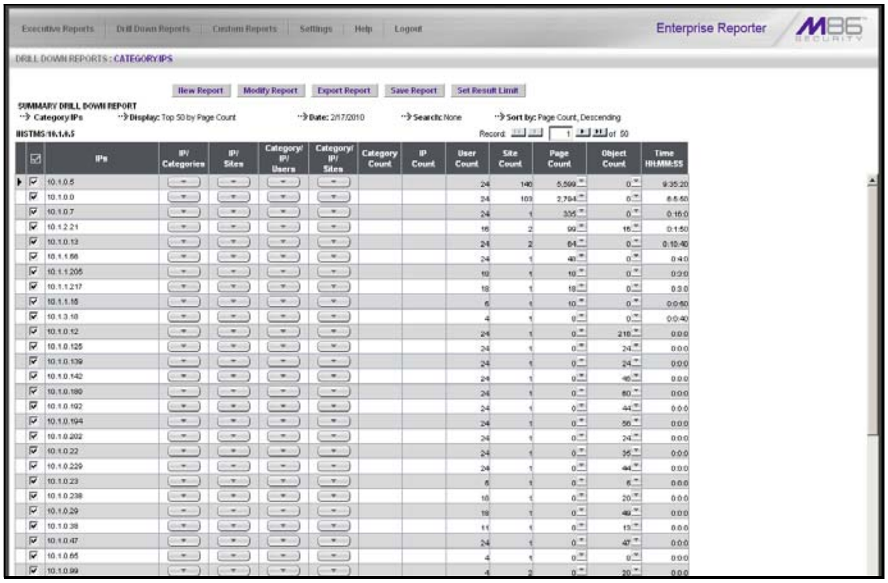
1. To continue this exercise, select the record for the category you wish to further investigate.

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

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

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

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



DRILL DOWN REPORTS : CATEGORY:IPS

SUMMARY DRILL DOWN REPORT
→ Category IPs → Display: Top 50 by Page Count → Date: 2/17/2010 → Search: None → Sort by: Page Count, Descending

INSTMS:10.1.0.5 Record: 1 of 50

	☑	IPs	IP/ Categories	IP/ Sites	Category/ IP/ Users	Category/ IP/ Sites	Category Count	IP Count	User Count	Site Count	Page Count	Object Count	Time HH:MM:SS
▶	☑	10.1.0.5	▾	▾	▾	▾			24	140	5,599 ▾	0 ▾	9:35:20
	☑	10.1.0.0	▾	▾	▾	▾			24	103	2,794 ▾	0 ▾	6:5:50
	☑	10.1.0.7	▾	▾	▾	▾			24	1	335 ▾	0 ▾	0:16:0
	☑	10.1.2.21	▾	▾	▾	▾			16	2	99 ▾	16 ▾	0:1:50
	☑	10.1.0.13	▾	▾	▾	▾			24	2	64 ▾	0 ▾	0:10:40
	☑	10.1.1.66	▾	▾	▾	▾			24	1	40 ▾	0 ▾	0:4:0
	☑	10.1.1.205	▾	▾	▾	▾			10	1	10 ▾	0 ▾	0:3:0
	☑	10.1.1.217	▾	▾	▾	▾			18	1	18 ▾	0 ▾	0:3:0
	☑	10.1.1.16	▾	▾	▾	▾			6	1	10 ▾	0 ▾	0:0:50
	☑	10.1.3.10	▾	▾	▾	▾			4	1	0 ▾	0 ▾	0:0:40
	☑	10.1.0.12	▾	▾	▾	▾			24	1	0 ▾	216 ▾	0:0:0
	☑	10.1.0.125	▾	▾	▾	▾			24	1	0 ▾	24 ▾	0:0:0
	☑	10.1.0.139	▾	▾	▾	▾			24	1	0 ▾	24 ▾	0:0:0
	☑	10.1.0.142	▾	▾	▾	▾			24	1	0 ▾	46 ▾	0:0:0
	☑	10.1.0.180	▾	▾	▾	▾			24	1	0 ▾	60 ▾	0:0:0
	☑	10.1.0.192	▾	▾	▾	▾			24	1	0 ▾	44 ▾	0:0:0
	☑	10.1.0.194	▾	▾	▾	▾			24	1	0 ▾	56 ▾	0:0:0
	☑	10.1.0.202	▾	▾	▾	▾			24	1	0 ▾	24 ▾	0:0:0
	☑	10.1.0.22	▾	▾	▾	▾			24	1	0 ▾	36 ▾	0:0:0
	☑	10.1.0.229	▾	▾	▾	▾			24	1	0 ▾	44 ▾	0:0:0
	☑	10.1.0.23	▾	▾	▾	▾			6	1	0 ▾	6 ▾	0:0:0
	☑	10.1.0.238	▾	▾	▾	▾			16	1	0 ▾	20 ▾	0:0:0
	☑	10.1.0.29	▾	▾	▾	▾			18	1	0 ▾	48 ▾	0:0:0
	☑	10.1.0.38	▾	▾	▾	▾			11	1	0 ▾	13 ▾	0:0:0
	☑	10.1.0.47	▾	▾	▾	▾			24	1	0 ▾	47 ▾	0:0:0
	☑	10.1.0.65	▾	▾	▾	▾			4	1	0 ▾	0 ▾	0:0:0
	☑	10.1.0.99	▾	▾	▾	▾			4	2	0 ▾	20 ▾	0:0:0

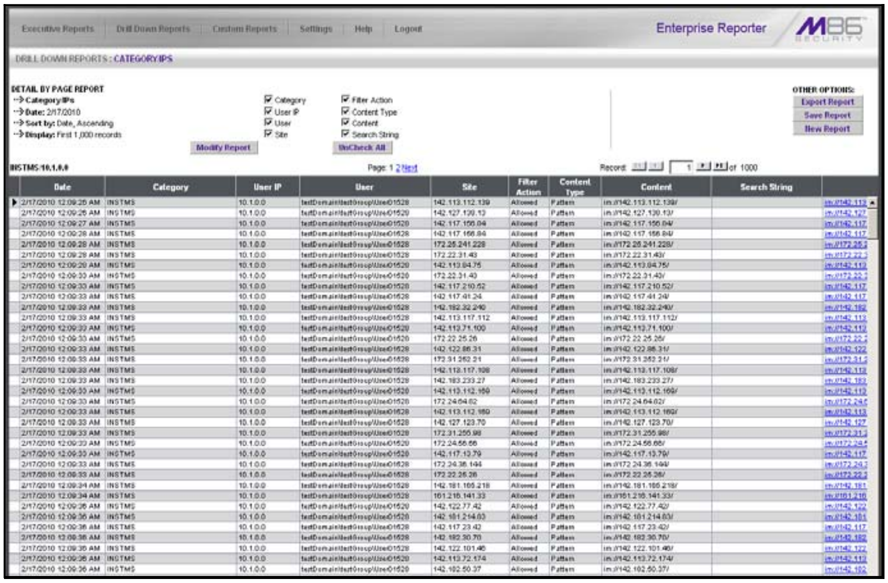
After executing the last command, note that user IP addresses now display in the first column of the report view instead of categories.

In the Security Reporter User Guide index, see:
- *How to: use filter columns and buttons*

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

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

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



DRILL DOWN REPORTS : CATEGORY:IPS

DETAIL BY PAGE REPORT
→ Category:IPs
→ Date: 2/17/2010
→ Sort by: Date, Ascending
→ Display: First 1,000 records

☑ Category
☑ User IP
☑ User
☑ Site
☑ Filter Action
☑ Content Type
☑ Content
☑ Search String

INSTMS:10.1.0.0 Page: 1 2 Next Record: 1 of 1000

	Date	Category	User IP	User	Site	Filter Action	Content Type	Content	Search String	
▶	2/17/2010 12:09:26 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.113.112.139	Allowed	Pattern	im://142.113.112.139/		im://142.113
	2/17/2010 12:09:26 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.127.130.13	Allowed	Pattern	im://142.127.130.13/		im://142.127
	2/17/2010 12:09:27 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.117.156.84	Allowed	Pattern	im://142.117.156.84/		im://142.117
	2/17/2010 12:09:28 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.117.156.84	Allowed	Pattern	im://142.117.156.84/		im://142.117
	2/17/2010 12:09:28 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	172.25.241.228	Allowed	Pattern	im://172.25.241.228/		im://172.25.2
	2/17/2010 12:09:28 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	172.22.31.43	Allowed	Pattern	im://172.22.31.43/		im://172.22.3
	2/17/2010 12:09:29 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.113.84.75	Allowed	Pattern	im://142.113.84.75/		im://142.113
	2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	172.22.31.43	Allowed	Pattern	im://172.22.31.43/		im://172.22.3
	2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.117.210.52	Allowed	Pattern	im://142.117.210.52/		im://142.117
	2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.117.41.24	Allowed	Pattern	im://142.117.41.24/		im://142.117
	2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.182.32.240	Allowed	Pattern	im://142.182.32.240/		im://142.182
	2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.113.117.112	Allowed	Pattern	im://142.113.117.112/		im://142.113
	2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.113.71.100	Allowed	Pattern	im://142.113.71.100/		im://142.113
	2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	172.22.25.26	Allowed	Pattern	im://172.22.25.26/		im://172.22.2
	2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.122.86.31	Allowed	Pattern	im://142.122.86.31/		im://142.122
	2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	172.31.252.21	Allowed	Pattern	im://172.31.252.21/		im://172.31.2
	2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.113.117.108	Allowed	Pattern	im://142.113.117.108/		im://142.113
	2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.183.233.27	Allowed	Pattern	im://142.183.233.27/		im://142.183
	2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.113.112.169	Allowed	Pattern	im://142.113.112.169/		im://142.113
	2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	172.24.64.62	Allowed	Pattern	im://172.24.64.62/		im://172.24.6
	2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.113.112.169	Allowed	Pattern	im://142.113.112.169/		im://142.113
	2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.127.123.70	Allowed	Pattern	im://142.127.123.70/		im://142.127
	2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	172.31.255.98	Allowed	Pattern	im://172.31.255.98/		im://172.31.2
	2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	172.24.56.66	Allowed	Pattern	im://172.24.56.66/		im://172.24.5
	2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.117.13.79	Allowed	Pattern	im://142.117.13.79/		im://142.117
	2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	172.24.36.144	Allowed	Pattern	im://172.24.36.144/		im://172.24.3
	2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	172.22.26.26	Allowed	Pattern	im://172.22.26.26/		im://172.22.2
	2/17/2010 12:09:34 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.181.165.218	Allowed	Pattern	im://142.181.165.218/		im://142.181
	2/17/2010 12:09:34 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	161.216.141.33	Allowed	Pattern	im://161.216.141.33/		im://161.216
	2/17/2010 12:09:36 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.122.77.42	Allowed	Pattern	im://142.122.77.42/		im://142.122
	2/17/2010 12:09:36 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.181.214.83	Allowed	Pattern	im://142.181.214.83/		im://142.181
	2/17/2010 12:09:36 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.117.23.42	Allowed	Pattern	im://142.117.23.42/		im://142.117
	2/17/2010 12:09:36 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.182.30.70	Allowed	Pattern	im://142.182.30.70/		im://142.182
	2/17/2010 12:09:36 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.122.101.46	Allowed	Pattern	im://142.122.101.46/		im://142.122
	2/17/2010 12:09:36 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.113.72.174	Allowed	Pattern	im://142.113.72.174/		im://142.113
	2/17/2010 12:09:36 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.182.50.37	Allowed	Pattern	im://142.182.50.37/		im://142.182

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

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

In the Security Reporter User Guide index, see:
• How to: create a detail Page Count report from a summary report

See also:
• How to: create a detail Object Count report from a summary report

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

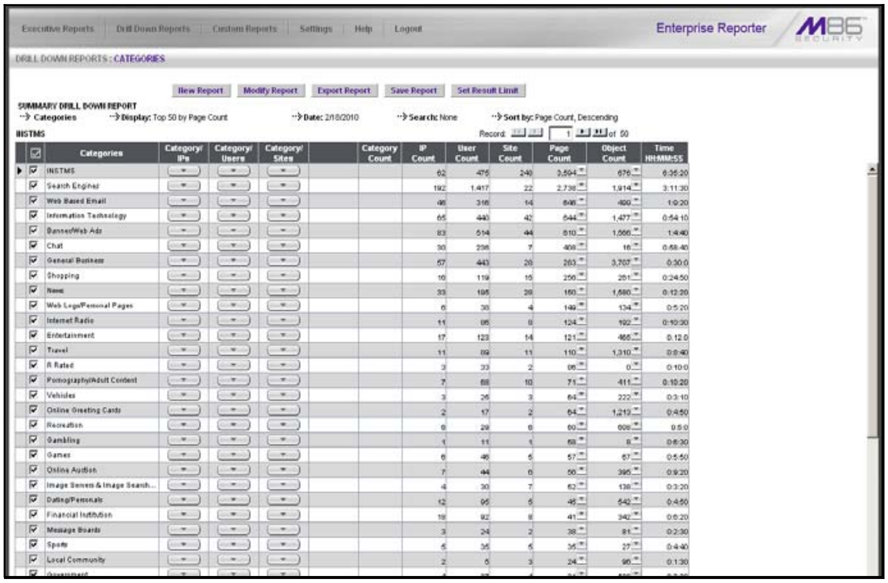
These tools and other tools can be used separately or combined to create many different types of reports to fulfill different purposes.

II. Double-break Report and Export Report exercise

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

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

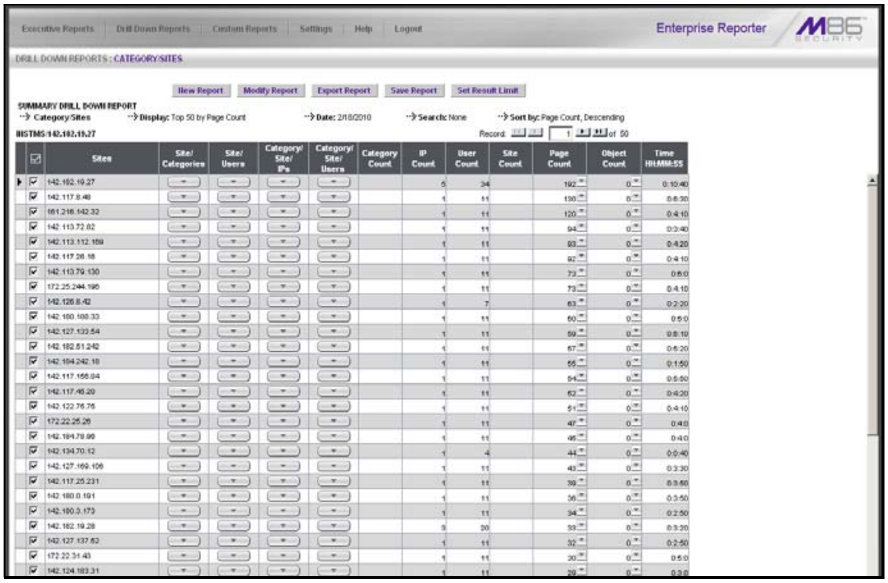
1. From the top panel, go to **Drill Down Reports > Categories** to generate a Summary Drill Down Report view, ranking categories in order by the most visited to the least visited:



SUMMARY DRILL DOWN REPORT
→ Categories →Display: Top 50 by Page Count →Date: 2/18/2010 →Search: None →Sort by: Page Count, Descending
INSTMS Record: 1 of 50

☑	Categories	Category/ IPs	Category/ Users	Category/ Sites		Category Count	IP Count	User Count	Site Count	Page Count	Object Count	Time HH:MM:SS
☑	INSTMS	▾	▾	▾			62	475	240	3,594	676	6:35:20
☑	Search Engines	▾	▾	▾			192	1,417	22	2,738	1,914	3:11:30
☑	Web Based Email	▾	▾	▾			46	316	14	646	400	1:0:20
☑	Information Technology	▾	▾	▾			65	440	42	644	1,477	0:54:10
☑	Banner/Web Ads	▾	▾	▾			83	514	44	610	1,566	1:4:40
☑	Chat	▾	▾	▾			30	236	7	408	16	0:58:40
☑	General Business	▾	▾	▾			57	443	20	203	3,707	0:30:0
☑	Shopping	▾	▾	▾			16	119	15	256	251	0:24:50
☑	News	▾	▾	▾			33	195	20	160	1,680	0:12:20
☑	Web Logs/Personal Pages	▾	▾	▾			6	30	4	149	134	0:5:20
☑	Internet Radio	▾	▾	▾			11	95	8	124	192	0:10:30
☑	Entertainment	▾	▾	▾			17	123	14	121	466	0:12:0
☑	Travel	▾	▾	▾			11	89	11	110	1,310	0:0:40
☑	R Rated	▾	▾	▾			3	33	2	96	0	0:10:0
☑	Pornography/Adult Content	▾	▾	▾			7	68	10	71	411	0:10:20
☑	Vehicles	▾	▾	▾			3	26	3	64	222	0:3:10
☑	Online Greeting Cards	▾	▾	▾			2	17	2	64	1,213	0:4:50
☑	Recreation	▾	▾	▾			6	29	6	60	609	0:5:0
☑	Gambling	▾	▾	▾			1	11	1	58	8	0:6:30
☑	Games	▾	▾	▾			6	46	5	57	67	0:5:50
☑	Online Auction	▾	▾	▾			7	44	6	56	395	0:9:20
☑	Image Servers & Image Search...	▾	▾	▾			4	30	7	62	138	0:3:20
☑	Dating/Personals	▾	▾	▾			12	95	5	46	542	0:4:50
☑	Financial Institution	▾	▾	▾			19	92	8	41	342	0:6:20
☑	Message Boards	▾	▾	▾			3	24	2	38	81	0:2:30
☑	Sports	▾	▾	▾			5	35	5	35	27	0:4:40
☑	Local Community	▾	▾	▾			2	5	3	24	96	0:1:30
☑	Government	▾	▾	▾								

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



DRILL DOWN REPORTS : CATEGORY/SITES

SUMMARY DRILL DOWN REPORT
→ Category/Sites → Display: Top 50 by Page Count → Date: 2/18/2010 → Search: None → Sort by: Page Count, Descending

INSTMS/142.182.19.27 Record: 1 of 50

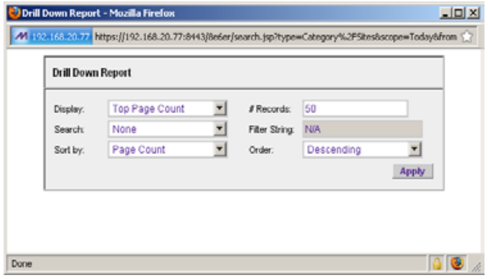
☑	Sites	Site/ Categories	Site/ Users	Category/ Site/ IPs	Category/ Site/ Users	Category Count	IP Count	User Count	Site Count	Page Count	Object Count	Time HH:MM:SS
☑	142.182.19.27	▼	▼	▼	▼		5	34		192	0	0:10:40
☑	142.117.8.48	▼	▼	▼	▼		1	11		130	0	0:6:30
☑	161.216.142.32	▼	▼	▼	▼		1	11		120	0	0:4:10
☑	142.113.72.82	▼	▼	▼	▼		1	11		94	0	0:3:40
☑	142.113.112.169	▼	▼	▼	▼		1	11		93	0	0:4:20
☑	142.117.26.18	▼	▼	▼	▼		1	11		92	0	0:4:10
☑	142.113.79.130	▼	▼	▼	▼		1	11		73	0	0:6:0
☑	172.25.244.196	▼	▼	▼	▼		1	11		73	0	0:4:10
☑	142.126.8.42	▼	▼	▼	▼		1	7		63	0	0:2:20
☑	142.180.188.33	▼	▼	▼	▼		1	11		60	0	0:6:0
☑	142.127.133.54	▼	▼	▼	▼		1	11		59	0	0:8:10
☑	142.182.51.242	▼	▼	▼	▼		1	11		57	0	0:6:20
☑	142.184.242.18	▼	▼	▼	▼		1	11		55	0	0:1:50
☑	142.117.156.84	▼	▼	▼	▼		1	11		54	0	0:5:50
☑	142.117.46.20	▼	▼	▼	▼		1	11		52	0	0:4:20
☑	142.122.76.76	▼	▼	▼	▼		1	11		51	0	0:4:10
☑	172.22.25.26	▼	▼	▼	▼		1	11		47	0	0:4:0
☑	142.184.78.90	▼	▼	▼	▼		1	11		46	0	0:4:0
☑	142.134.70.12	▼	▼	▼	▼		1	4		44	0	0:0:40
☑	142.127.169.106	▼	▼	▼	▼		1	11		43	0	0:3:30
☑	142.117.25.231	▼	▼	▼	▼		1	11		39	0	0:3:50
☑	142.180.0.191	▼	▼	▼	▼		1	11		36	0	0:3:50
☑	142.180.3.173	▼	▼	▼	▼		1	11		34	0	0:2:50
☑	142.182.19.28	▼	▼	▼	▼		3	20		33	0	0:3:20
☑	142.127.137.62	▼	▼	▼	▼		1	11		32	0	0:2:50
☑	172.22.31.43	▼	▼	▼	▼		1	11		30	0	0:5:0
☑	142.124.183.31	▼	▼	▼	▼		1	11		29	0	0:3:0

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

In the Security Reporter User Guide index, see:
- *How to: generate a Drill Down Report*
- *How to: use filter columns and buttons*

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

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



https://192.168.20.77:8443/8e6er/search.jsp?type=Category%2FSites&scope=Today&from

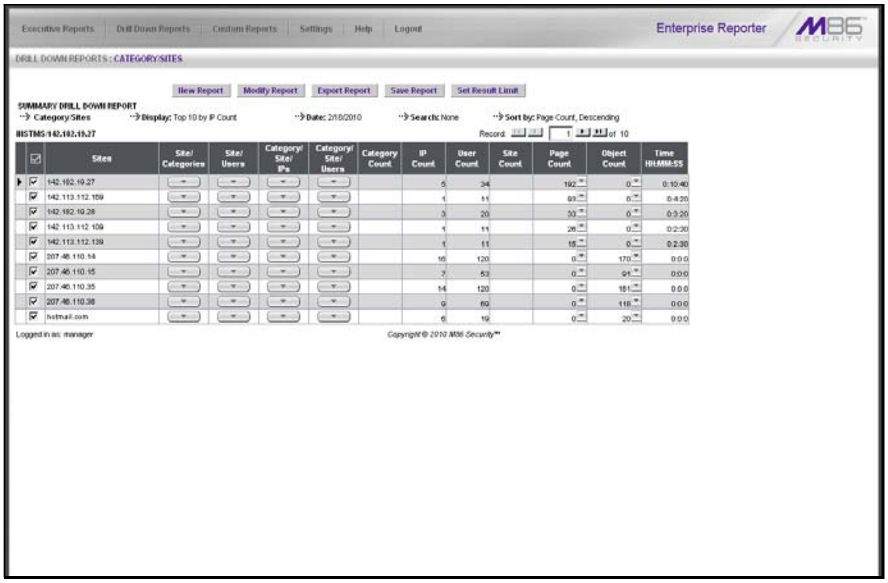
Drill Down Report

Display: Top Page Count
Search: None
Sort by: Page Count
Records: 50
Filter String: N/A
Order: Descending

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

2. Select "Top IP Count" from the Display drop-down menu, and type in ***10*** in the **# Records** field.

3. Click **Apply** to close the pop-up window and to display the report view showing only the top 10 site records for the selected category:



SUMMARY DRILL DOWN REPORT
→ Category/Sites → Display: Top 10 by IP Count → Date: 2/18/2010 → Search: None → Sort by: Page Count, Descending

IISTMS/142.192.19.27

Record: 1 of 10

☑	Sites	Site/ Categories	Site/ Users	Category/ Site/ IPs	Category/ Site/ Users	Category Count	IP Count	User Count	Site Count	Page Count	Object Count	Time HH:MM:SS
☑	142.192.19.27	▾	▾	▾	▾		5	34		192	0	0:10:40
☑	142.113.112.159	▾	▾	▾	▾		1	11		93	0	0:4:20
☑	142.192.19.28	▾	▾	▾	▾		3	20		33	0	0:3:20
☑	142.113.112.109	▾	▾	▾	▾		1	11		26	0	0:2:30
☑	142.113.112.139	▾	▾	▾	▾		1	11		16	0	0:2:30
☑	207.46.110.14	▾	▾	▾	▾		16	120		0	170	0:0:0
☑	207.46.110.15	▾	▾	▾	▾		7	53		0	91	0:0:0
☑	207.46.110.35	▾	▾	▾	▾		14	120		0	181	0:0:0
☑	207.46.110.38	▾	▾	▾	▾		9	69		0	118	0:0:0
☑	hotmail.com	▾	▾	▾	▾		6	19		0	20	0:0:0

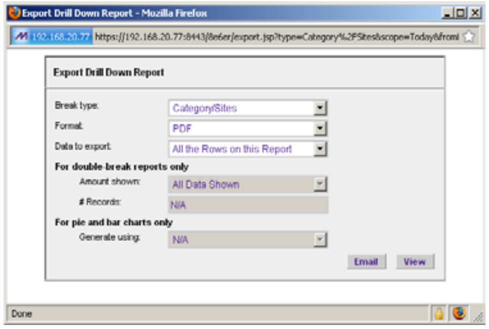
Logged in as: manager

Copyright © 2010 M86 Security™

In the Security Reporter User Guide index, see:
- *How to: modify a Drill Down Report*
- *How to: display only a specified number of records*

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

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



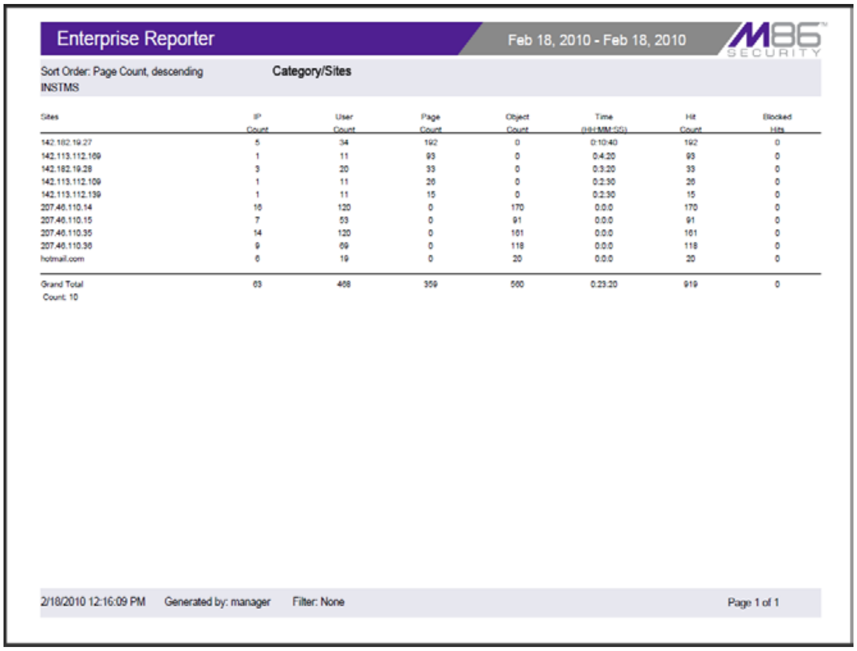
192.168.20.77 https://192.168.20.77:8443/8e6er/export.jsp?type=Category%2FSites&scope=Today&from

Export Drill Down Report

Break type: Category/Sites
Format: PDF
Data to export: All the Rows on this Report
For double-break reports only
Amount shown: All Data Shown
Records: N/A
For pie and bar charts only
Generate using: N/A

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

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



Enterprise Reporter Feb 18, 2010 - Feb 18, 2010

Sort Order: Page Count, descending
INSTMS

Category/Sites

Sites	IP Count	User Count	Page Count	Object Count	Time (HH:MM:SS)	Hit Count	Blocked Hits
142.182.19.27	5	34	192	0	0:10:40	192	0
142.113.112.169	1	11	93	0	0:4:20	93	0
142.182.19.28	3	20	33	0	0:3:20	33	0
142.113.112.109	1	11	26	0	0:2:30	26	0
142.113.112.139	1	11	15	0	0:2:30	15	0
207.46.110.14	16	120	0	170	0:0:0	170	0
207.46.110.15	7	53	0	91	0:0:0	91	0
207.46.110.35	14	120	0	161	0:0:0	161	0
207.46.110.36	9	69	0	118	0:0:0	118	0
hotmail.com	6	19	0	20	0:0:0	20	0
Grand Total Count: 10	63	468	359	560	0:23:20	919	0

2/18/2010 12:16:09 PM Generated by: manager Filter: None Page 1 of 1

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

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

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

In the Security Reporter User Guide index, see:
- *How to: export a summary Drill Down Report*
- *How to: view and print a Web Client report*

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

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

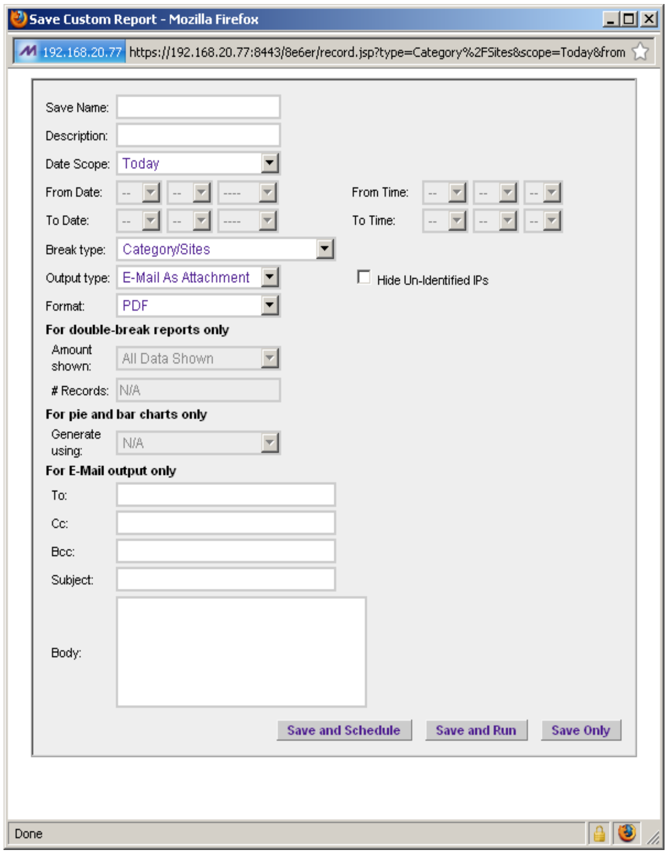
Variations of this exercise can be performed to generate and export countless reports using criteria of your specifications.

III. Save and schedule a report exercise

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

Step A. Save a report

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



Save Custom Report - Mozilla Firefox

192.168.20.77 https://192.168.20.77:8443/8e6er/record.jsp?type=Category%2FSites&scope=Today&from

Save Name:

Description:

Date Scope: Today

From Date: -- -- ----

From Time: -- -- --

To Date: -- -- ----

To Time: -- -- --

Break type: Category/Sites

Output type: E-Mail As Attachment

□ Hide Un-Identified IPs

Format: PDF

For double-break reports only

Amount shown: All Data Shown

Records: N/A

For pie and bar charts only

Generate using: N/A

For E-Mail output only

To:

Cc:

Bcc:

Subject:

Body:

Save and Schedule | Save and Run | Save Only

Done

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

2. For this exercise, make entries in the following fields: **Save Name**, **Description**, and **For E-Mail output only** (**To** and **Subject** fields).

3. Choose the **Save and Schedule** option from the “Save” options at the bottom of the window. The three “Save” options are as follows:

   - **Save and Schedule -** this option lets you save criteria from the current report view and then set up a schedule to run the report using that criteria.
   - **Save and Run -** this option lets you save criteria from the current report view and then automatically generate a report in the specified output format.
   - **Save Only -** this option lets you save criteria from the current report view.

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

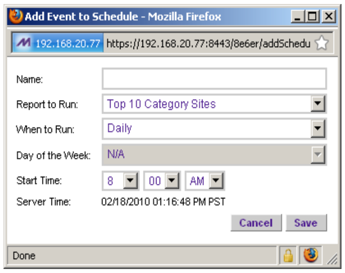
In the Security Reporter User Guide index, see:
- *How to: save a custom report*

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

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

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

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



Add Event to Schedule - Mozilla Firefox

192.168.20.77 https://192.168.20.77:8443/8e6er/addSchedu

Name:

Report to Run: Top 10 Category Sites

When to Run: Daily

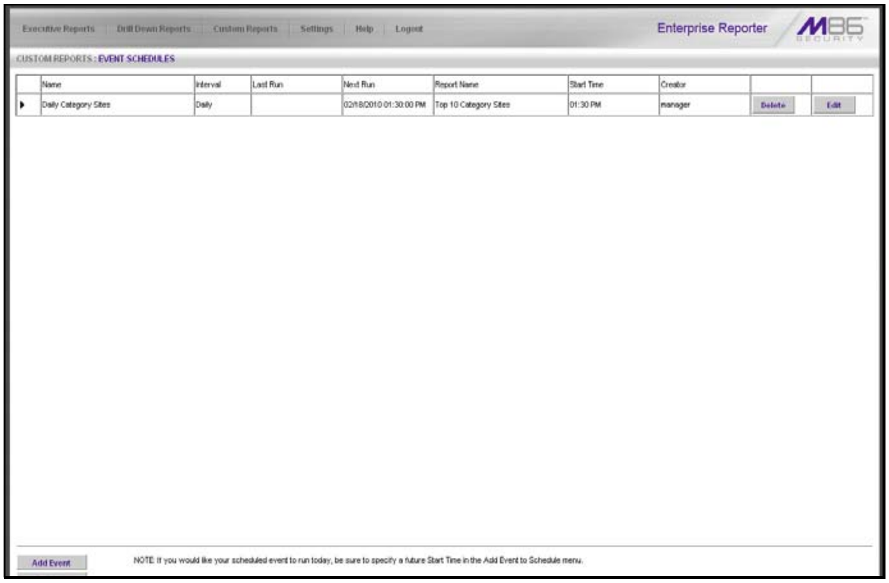
Day of the Week: N/A

Start Time: 8 00 AM

Server Time: 02/18/2010 01:16:48 PM PST

Done

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



	Name	Interval	Last Run	Next Run	Report Name	Start Time	Creator		
▶	Daily Category Sites	Daily		02/18/2010 01:30:00 PM	Top 10 Category Sites	01:30 PM	manager	Delete	Edit

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

In the Security Reporter User Guide index, see:
• How to: schedule a report to run

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

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

IV. Create a custom category group and generate reports

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

Step A: Create a custom category group

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

In the Security Reporter User Guide index, see:
• How to: add a category group in the Web Client

Step B: Run a report for a specified category group

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

In the Security Reporter User Guide index, see:
• How to: generate a custom Web Client report

V. Create a custom user group and generate reports

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

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

Step A: Create a custom user group

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

In the Security Reporter User Guide index, see:
• How to: add a user group in the Web Client

Step B: Generate a report for a custom user group

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

Summary Report

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

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

Detail Report

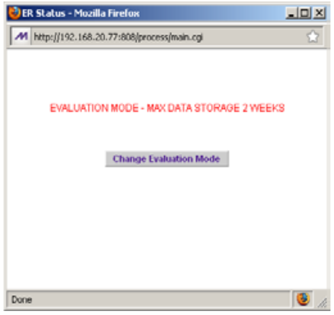
Specific User Detail by Page/Object - To use this option, choose Custom Reports from the left panel, select Custom Report Wizard, and then specify **Specific User Detail by Page/Object**. Click the **Next** button, choose the **User Group** name, and then click the **View Drill Down Results** button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

In the Security Reporter User Guide index, see:
• How to: generate a custom Web Client report
• How to: generate a Single User Group Report

IMPORTANT INFORMATION ABOUT USING THE ER IN THE EVALUATION MODE

Evaluation Mode Pop-Ups

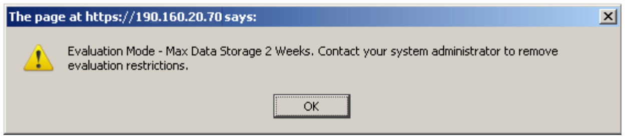
When evaluating the SR and using the ER applications in the evaluation mode, the ER Status pop-up box opens after logging in to the ER Administrator console:


ER Status - Mozilla Firefox
http://192.168.20.77:808/process/main.cgi
Change Evaluation Mode
Done

EVALUATION MODE - MAX DATA STORAGE 2 WEEKS

ER Status pop-up box

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



Evaluation Mode - Max Data Storage 2 Weeks. Contact your system administrator to remove evaluation restrictions.

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

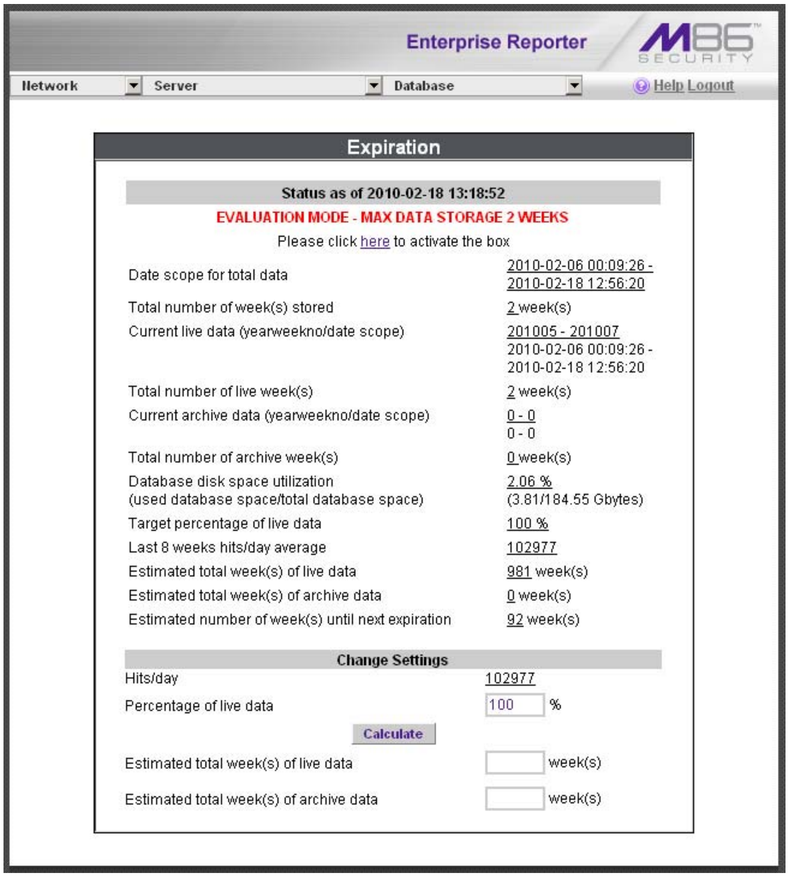
These two pop-up boxes will continue to open in the user interfaces until the ER is in the activated mode.

***NOTE**: In theSecurity Reporter User Guide, see ER Server Appendix Section and ER Web Client Appendix Section for information about changing the ER's mode from evaluation to activated.*

In the evaluation mode, the Expiration screen in the ER Administrator console and the ER Server Statistics window in the ER Web Client will display and function differently than they do in the activated (standard) mode (described respectively in the ER Administrator Section and ER Web Client Section of the Security Reporter User Guide).

Administrator Console, Expiration Screen

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



Expiration

Status as of 2010-02-18 13:18:52

EVALUATION MODE - MAX DATA STORAGE 2 WEEKS

Please click here to activate the box

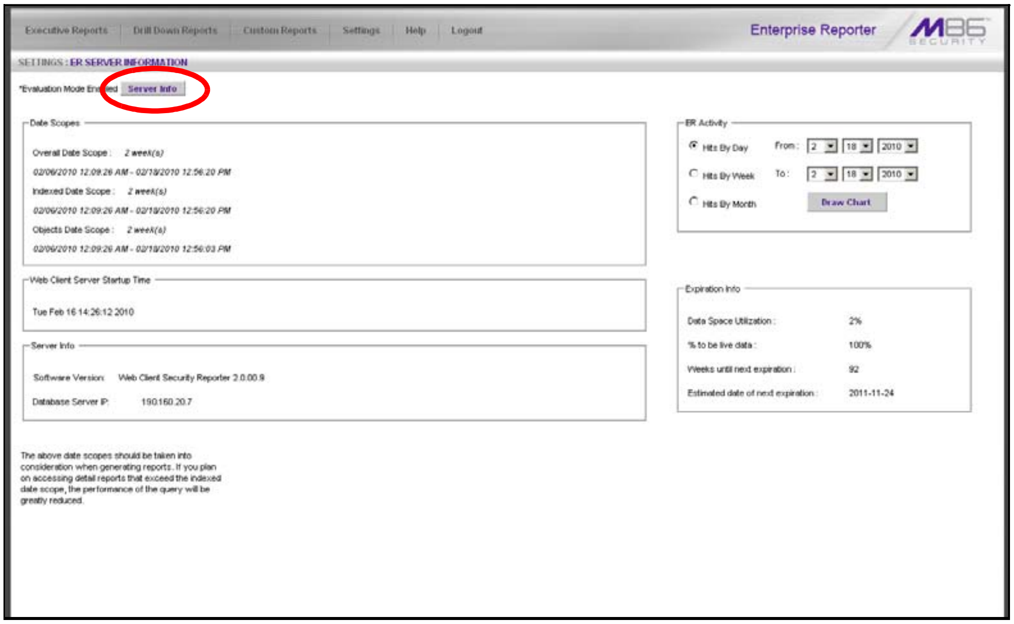
Date scope for total data	2010-02-06 00:09:26 - 2010-02-18 12:56:20
Total number of week(s) stored	2 week(s)
Current live data (yearweekno/date scope)	201005 - 201007 2010-02-06 00:09:26 - 2010-02-18 12:56:20
Total number of live week(s)	2 week(s)
Current archive data (yearweekno/date scope)	0 - 0 0 - 0
Total number of archive week(s)	0 week(s)
Database disk space utilization (used database space/total database space)	2.06 % (3.81/184.55 Gbytes)
Target percentage of live data	100 %
Last 8 weeks hits/day average	102977
Estimated total week(s) of live data	981 week(s)
Estimated total week(s) of archive data	0 week(s)
Estimated number of week(s) until next expiration	92 week(s)

Change Settings

Hits/day	102977
Percentage of live data	100 %
	Calculate
Estimated total week(s) of live data	week(s)
Estimated total week(s) of archive data	week(s)

ER Web Client, ER Server Information Window

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



SETTINGS : ER SERVER INFORMATION

*Evaluation Mode Enabled

Date Scopes

Overall Date Scope : *2 week(s)*

02/06/2010 12:09:26 AM - 02/18/2010 12:56:20 PM

Indexed Date Scope : *2 week(s)*

02/06/2010 12:09:26 AM - 02/18/2010 12:56:20 PM

Objects Date Scope : *2 week(s)*

02/06/2010 12:09:26 AM - 02/18/2010 12:56:03 PM

Web Client Server Startup Time

Tue Feb 16 14:26:12 2010

Server Info

Software Version: Web Client Security Reporter 2.0.00.9

Database Server IP: 190.160.20.7

ER Activity

● Hits By Day From : 2 18 2010

○ Hits By Week To : 2 18 2010

○ Hits By Month

Expiration Info

Data Space Utilization : 2%

% to be live data : 100%

Weeks until next expiration : 92

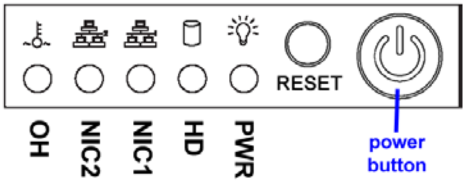
Estimated date of next expiration : 2011-11-24

The above date scopes should be taken into consideration when generating reports. If you plan on accessing detail reports that exceed the indexed date scope, the performance of the query will be greatly reduced.

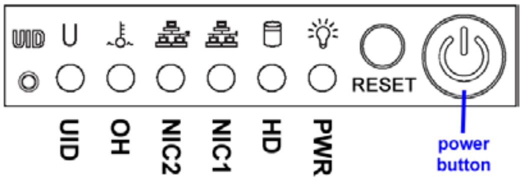
LED Indicators and Buttons

Front Control Panels on 500 and 700 Series Units

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



500 series chassis front panel



700 series chassis front panel

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

UID (button) and **U** icon – On a 700 series unit, when the UID button is pressed, a steady blue LED displays on both the front and rear of the chassis. These indicators are used for easy location of the chassis in a large stack configuration. The LED remains on until the button is pressed a second time.

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

NIC2 (icon) – A flashing green LED indicates network activity on LAN2. On a 500 series unit, the LED is a steady green with link connectivity, and unlit if there with no link connectivity.

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

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

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

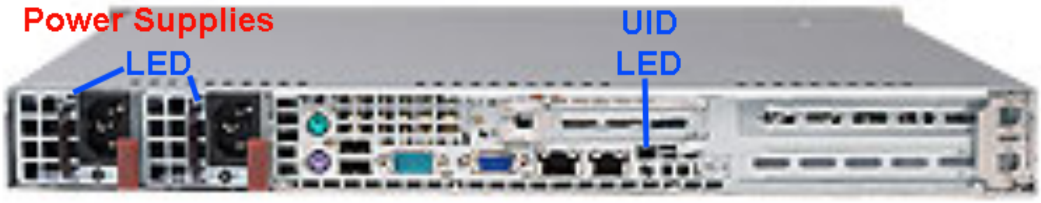
Power (icon) – The LED is unlit when the server is turned off. A steady green LED indicates power is being supplied to the unit's power supplies.

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

Rear Panel on the 700 Series Unit

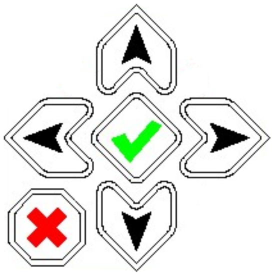
Power Supplies (LED indicators) – The power supplies are located at the right on the rear of the chassis. An LED indicator is located above each of the power plugs.

UID (LED indicator) – On the rear of the 700 series chassis, to the right of the LAN ports, a steady blue UID LED indicator displays when the UID button on the control panel is pressed. This LED remains lit until the UID button is pressed again.



Front Control Panel on a 300 Series Unit

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



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

REGULATORY SPECIFICATIONS AND DISCLAIMERS

Declaration of the Manufacturer or Importer

Safety Compliance

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

Electromagnetic Compatibility (EMC)

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

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

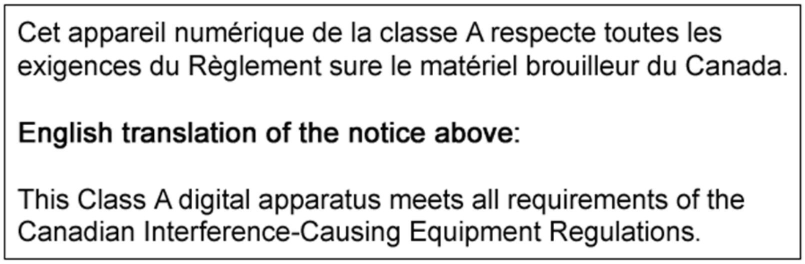
***NOTE**: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment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

FCC Declaration of Conformity

Models: 300-002-007, 500-002-007, 700-001-007, 700-013-007

Electromagnetic Compatibility Class A Notice

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



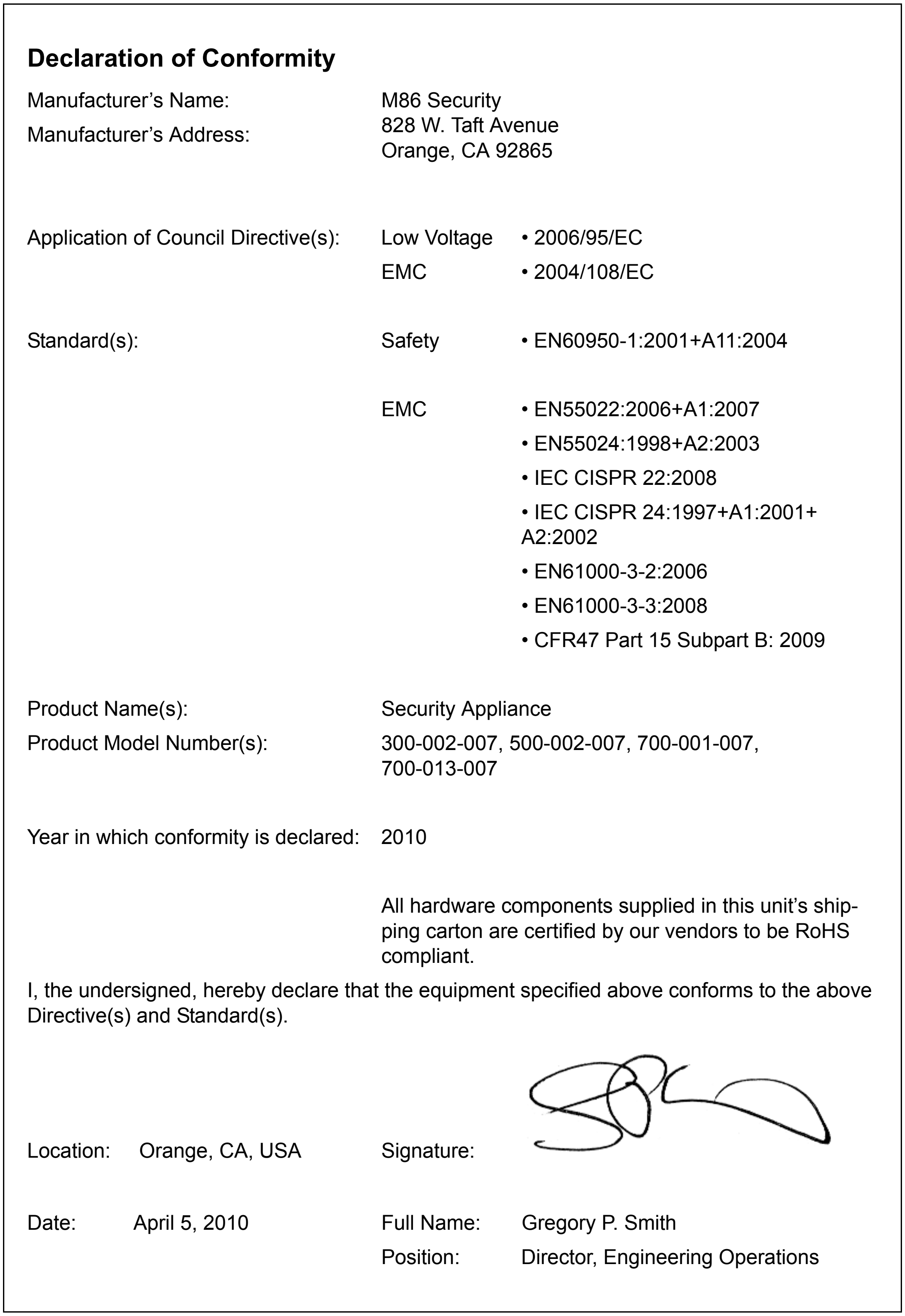
Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sure le matériel brouilleur du Canada.

English translation of the notice above:

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

EC Declaration of Conformity

European Community Directives Requirement (CE)



Declaration of Conformity

Manufacturer’s Name:	M86 Security	
Manufacturer’s Address:	828 W. Taft Avenue Orange, CA 92865	
Application of Council Directive(s):	Low Voltage	• 2006/95/EC
	EMC	• 2004/108/EC
Standard(s):	Safety	• EN60950-1:2001+A11:2004
	EMC	• EN55022:2006+A1:2007
		• EN55024:1998+A2:2003
		• IEC CISPR 22:2008
		• IEC CISPR 24:1997+A1:2001+ A2:2002
		• EN61000-3-2:2006
		• EN61000-3-3:2008
		• CFR47 Part 15 Subpart B: 2009
Product Name(s):	Security Appliance	
Product Model Number(s):	300-002-007, 500-002-007, 700-001-007, 700-013-007	
Year in which conformity is declared:	2010	

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

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

Location:	Orange, CA, USA	Signature:	
Date:	April 5, 2010	Full Name:	Gregory P. Smith
		Position:	Director, Engineering Operations

APPENDIX A: FIBRE CHANNEL CONNECTED STORAGE DEVICE

This appendix pertains to the installation of the optional NAS (Fibre Channel Connected Storage Device or “SAN”) unit.

Preliminary Setup Procedures

Unpack the Unit from the Carton

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

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

The carton should contain the following items:

- 1 Nexsan Technologies unit
- 1 mounting kit
- 1 accessory kit containing:
  - 2 AC power cords
  - 1 fibre channel cable

Other Required Installation Items

In addition to the contents of the Nexsan carton, you will need the following items to install the storage device:

- 1 standard CAT-5E cable
- 1 CAT-5E crossover cable

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

NOTE*: Refer to the SR safety precautions. In addition to being applicable to the SR, this information also applies to this storage device unit.*

Rack Mount the Server

Rack Mount Components

The following items are needed to install rails for rack mounting:

- 1 slide kit and mounting hardware
- 1 pair Accuride slide rails

Rack Setup Precautions

WARNING:

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

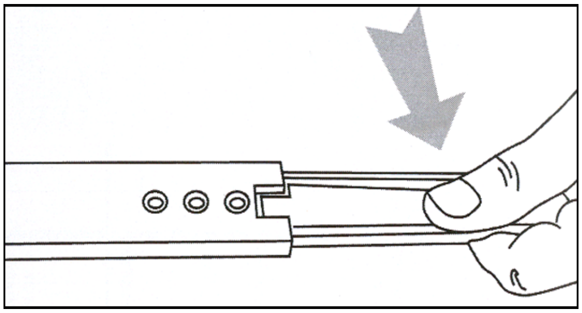
- The weight of all units in the rack is evenly distributed. Hazardous conditions may be created by an uneven weight distribution.
- The rack will not tip over when the unit is mounted, even when the unit is fully extended from the rack.
- For a single rack installation, stabilizers are attached to the rack.
- For multiple rack installations, racks are coupled together.
- The rack is grounded and will maintain a reliable ground at all times.
- A power cord will be long enough to fit into the unit when properly mounted in the rack and will be able to supply power to the unit.
- The connection of the unit to the power supply will not overload any circuits.
- The unit is only connected to a properly rated supply circuit. Reliable earthing (grounding) of rack-mounted equipment should be maintained.
- The air flow through the unit's fan or vents is not restricted.
- The maximum operating ambient temperature does not exceed 104°F (40°C).

NOTE*: Always make sure the rack is stable before extending a component from the rack.*

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

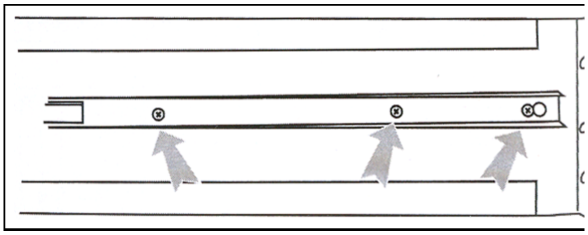
Step 1

Remove inner slide rail as shown. Press down on latch to release.



Step 2

Attach inner slide rail to chassis using 3 screws as shown.

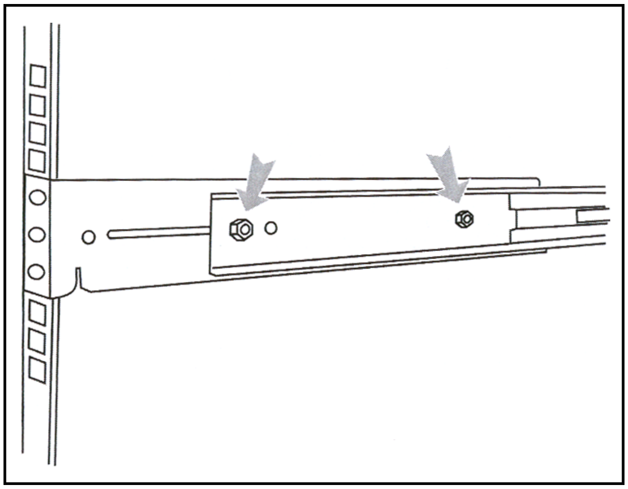


***NOTE**: When attaching the extended brackets, attach them loosely at first. Adjust the length to fit the cabinet, and then tighten.*

Step 3

Attach left and right rear (long) extended brackets to the outer rail using 2 screws, 2 washers, and 2 nuts for each bracket.

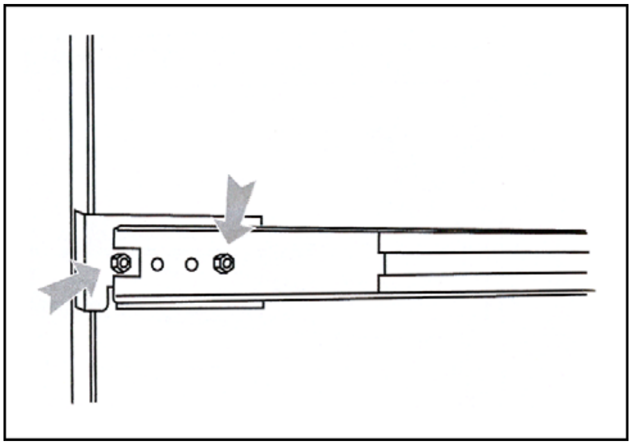
***NOTE**: Make sure the flange is on the bottom edge.*



Step 4

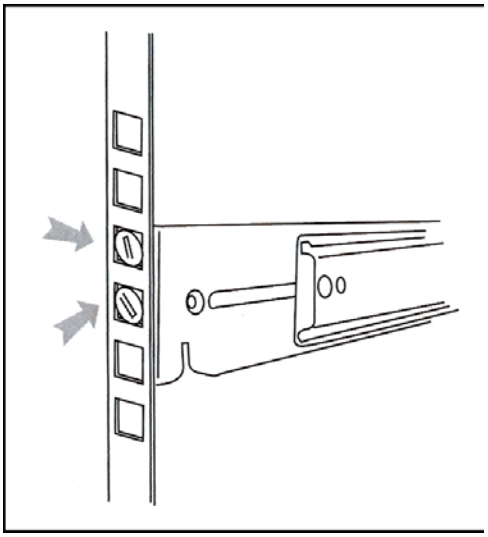
Attach left and right front (short) extended brackets to the outer rail using 2 screws, 2 washers, and 2 nuts for each bracket.

***NOTE**: Make sure the flange is on the bottom edge.*



Step 5

Attach outer rail to chassis using 4 screws and cage nuts per rail, 2 at each end.



Step 6

Slide chassis into outer rail carefully, making sure the chassis is level with the slide.

***NOTE**: It’s easier if the drives and power supplies are removed first before sliding the chassis into the outer rail.*

Install the Unit

Link the SR Unit with the Fibre Channel Connected Device

This step is a continuation from the Storage Device Setup (for Attached Storage Units) portion of Step 1A or 1B in the SR section. The procedures outlined in this step require the use of a CAT-5E crossover cable and the fibre channel cable.

A. Plug one end of the CAT-5E crossover cable into the SR unit's LAN 3 port-—the port on the upper right section on the rear of the SR unit (see Figure 1, LAN3 port).

B. Plug the fibre channel cable into the port on the lower right section on the rear of the SR unit (see Figure 1, fibre channel port).

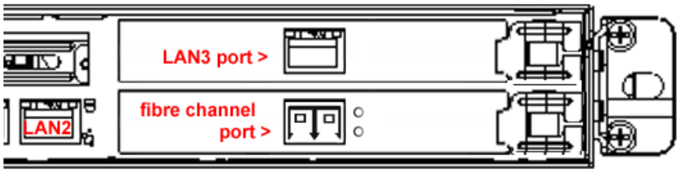


Figure 1: Diagram showing right portion of SR chassis rear

C. Plug the other end of the fibre channel cable into the storage device's HOST "1" channel (see Figure 2, Item A).

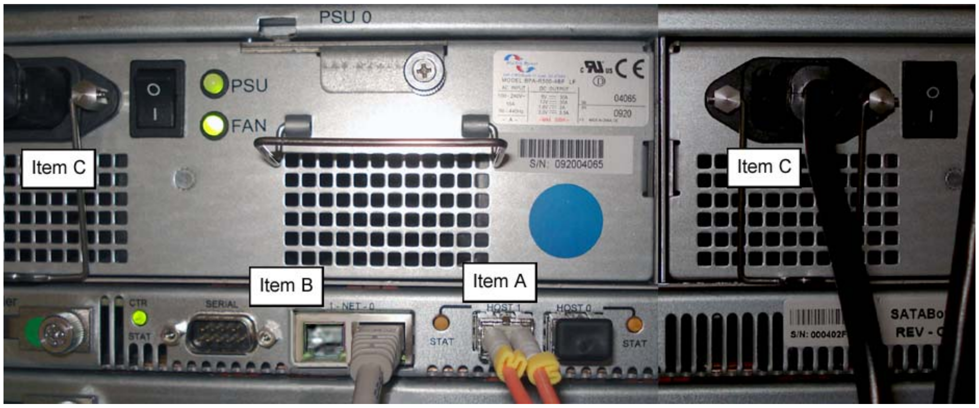


Figure 2: Back of the Nexsan SATABoy

D. Plug the other end of the CAT-5E crossover cable into the storage device's NET "1" port (see Figure 2, Item B).

E. Plug the storage device's AC power cords into the rear sections of the unit (see Figure 2, Item C).

F. Plug the loose ends of the AC power cords into a power source with an appropriate rating. It is strongly suggested you use an uninterruptible power supply.

***WARNING**: Be sure all drives are installed in the storage device unit before powering on the unit. Be sure the SR unit is not powered on.*

G. Turn on the power switches at the back of the storage device, which are positioned to the right of the power cord connectors. The boot-up process may take up to 5 minutes. When the unit is booted up, the three vertical LED lights at the left of the front panel will be lit up (see Figure 3).

Once all LED lights are lit, the SR can be powered on.

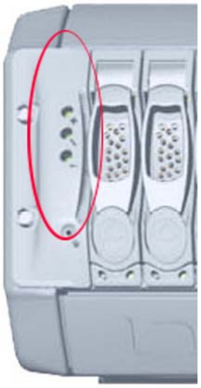


Figure 3: LED display

Proceed to Step 1A: Quick Start Setup Procedures or Step 1B: LCD Panel Setup Procedures, whichever option you chose for configuring SR network parameters.

Shut Down, Restart Procedures

Follow the procedures in this section if you need to shut down or restart the storage device.

Shut Down the Storage Device Unit

If you need to shut down the storage device, always follow these steps:

A. Power off the SR unit first.

***NOTE**: For shut down procedures, refer to the Shutdown instructions in the sub-section Non-Quick Start procedures or settings from Step 1B: LCD Panel Setup Procedures.*

B. Power off the storage device next by turning off both switches in the back of the unit.

Restart the Storage Device Unit

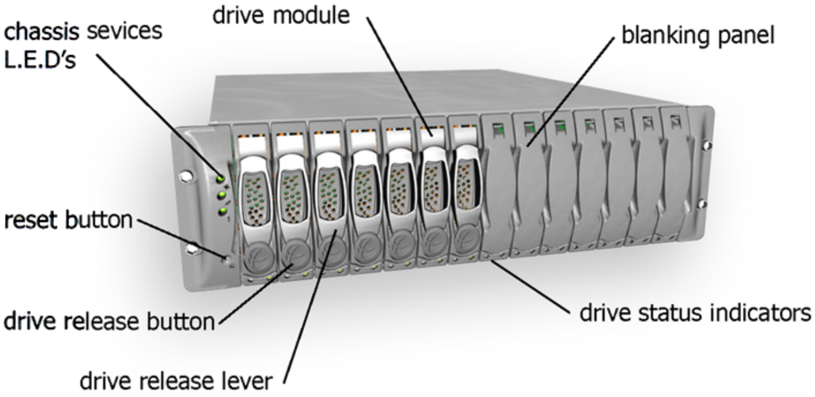
The storage device must be restarted after a power failure. In this instance, the storage device may already be turned on, but needs to be booted up again.

***WARNING**: You must **always** power on the storage device **before** powering on the SR unit. Since the storage device is an information database, if you experience a power interruption or if you power off the storage device without going through the standard shut down procedures, you may lose data and/or damage the file system.*

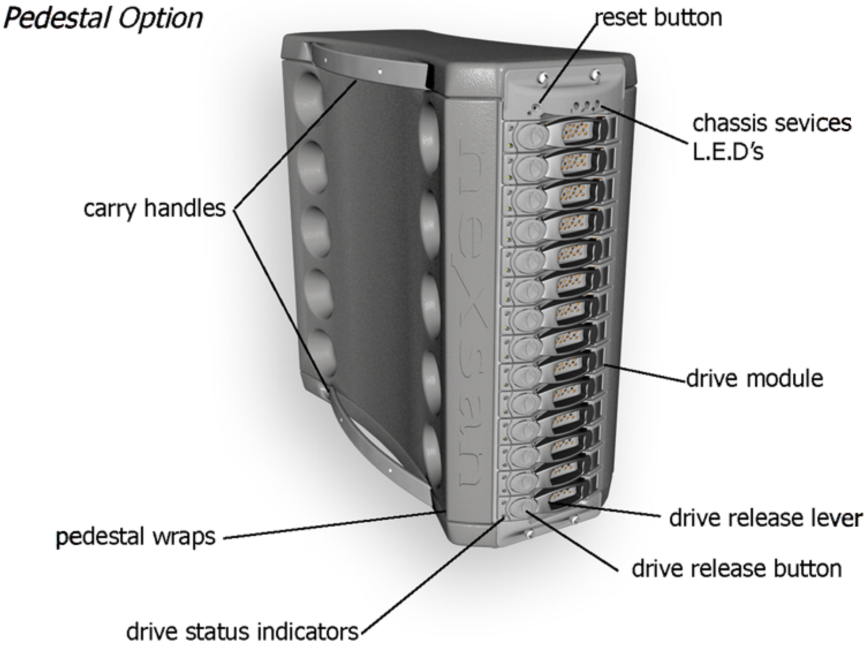
To restart the storage device, press the power button on the front panel. The boot-up process may take up to 5 minutes.

Physical Components

Rack Mount Option

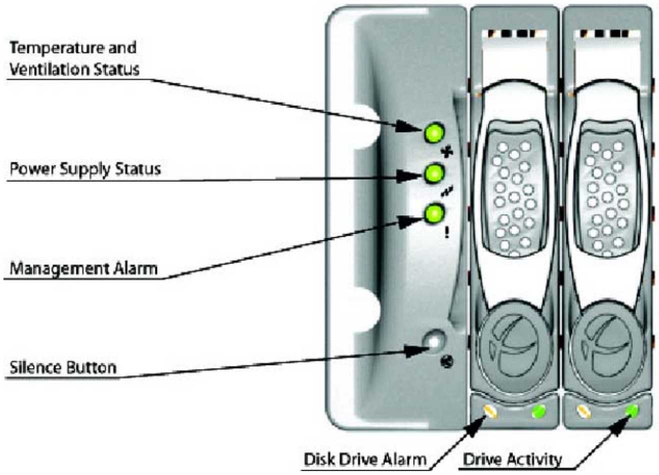


Pedestal Option



LED Display

Temperature and Ventilation Status



When the LED is green, the blowers are operating at an acceptable RPM, and the internal temperature sensors are within acceptable limits.

The LED alternates green and red to indicate a predicted failure of one blower or an alarmingly rapid increase in temperature.

If the LED is red, a blower has failed or the unit is too hot, and an audible alarm will sound.

Power Supply Status

The LED is green if both power supplies are functional.

The LED is red if either power supply has failed, and an audible alarm will sound. In this scenario, an authorized service personnel should examine the LEDs on each power supply module to determine which has failed.

WARNING*: Inadvertently removing the functional, surviving power supply will result in system failure and possible data loss.*

Management Alarm

A green LED indicates nominal status.

A red LED indicates RAID controller or non-PSU/Blower enclosure errors.

Silence Button

Insert a thin object to temporarily silence the audible alarm. This button also is used for confirming creation in the RAID configuration mode.

Disc Drive Alarm

The LED is illuminated yellow if a drive is suspected to be bad.

Disk Drive Activity

The LED is illuminated green when an installed drive is in a “ready” state. During activity, the LED will flicker.

APPENDIX B: OPTIONAL ETHERNET TAP INSTALLATION

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

***NOTE**: In order to monitor bandwidth on the SR, both inbound and outbound traffic must be sent to the SR through use of a port span, tap, or other similar device.*

Preliminary Setup Procedures

The instructions in this section pertain to the use of a NetOptics 10/100BaseT Tap that can be purchased from M86 Security.

Unpack the Ethernet Tap Unit from the Box

Open the NetOptics Ethernet Tap box and verify that all accessories are included. Save all packing materials in the event that the unit needs to be returned to M86 Security.

The NetOptics box should contain the following items:

- 1 NetOptics 10/100BaseT Tap
- 2 power supply units
- 2 AC power cords
- 2 crossover cables
- 2 straight through cables
- 1 installation guide

Other Required Installation Items

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

- 1 standard CAT-5E cable

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

Install the Ethernet Tap Unit

This step is a continuation from Step 2: Physically Connect the Unit to the Network. The procedures outlined in this step require the use of a CAT-5E cable.

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

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

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

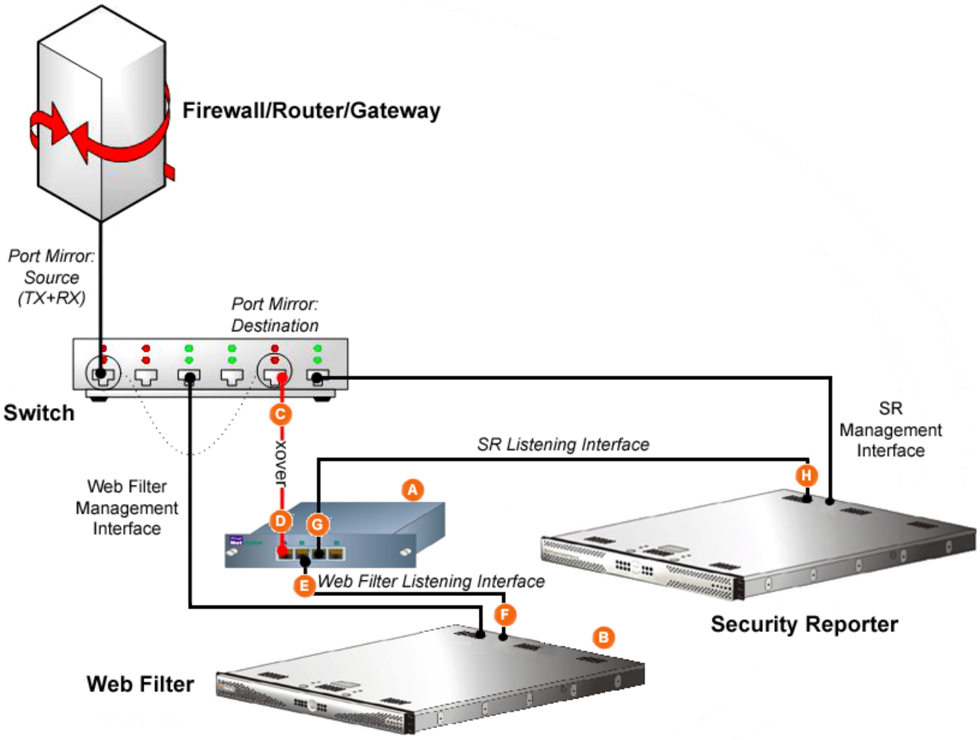


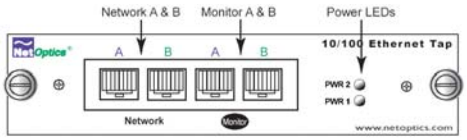
Diagram showing Ethernet Tap installation on the network

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

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

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

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



Ports in front panel of NetOptics 10/100BaseT Tap

E. Using a straight through cable, connect one end to the Ethernet Tap’s Network B port.

F. Connect the other end of the straight through cable to the Web Filter’s listening interface.

G. Using the second straight through cable, connect one end to the Ethernet Tap’s Monitor A port.

H. Connect the other end of the second straight through cable to the Security Reporter’s listening interface.

Proceed to Step 3: Register the SR and its Applications.

INDEX

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