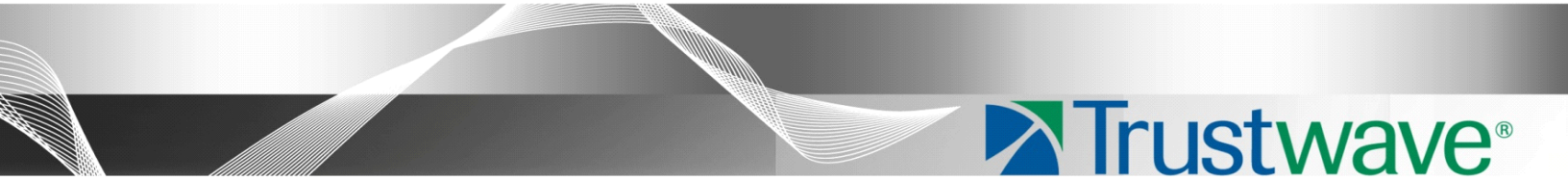


M86 Security Reporter Appliance

Installation Guide

Models: 300, 500, 505, 700, 705, 730, 735

Version 3.2.0

Publication Date: 21 June, 2013

Legal Notice

The most current version of this document may be obtained by contacting:

Trustwave Technical Support:
Phone: +1.800.363.1621
Email: support@trustwave.com

Trademarks

Part# SR-AIG-130621

CONTENTS

M86 SR APPLIANCE INTRODUCTION

Thank you for choosing to install and evaluate the M86 Security Reporter appliance. The Security Reporter (SR) from M86 Security consists of the best in breed of M86 Professional Edition reporting software consolidated into one unit, with the capability to generate productivity reports of end user Internet activity from M86 Web Filter and/or M86 Secure Web Gateway (SWG) appliance(s), and security reports from an SWG.

Using a Web Filter, you have the option to use an Equus SR 300, 500, 700 or 730 model, or an IBM SR 505, 705 or 735 model.

Using an SWG, you have the option to use an IBM SR 505, 705 or 735 model.

Using both a Web Filter and an SWG, you have the option to use an IBM SR 505, 705 or 735 IBM model.

Logs of end user Internet activity from a Web Filter and/or SWG are fed into SR, giving you an overall picture of end user productivity in a bar chart dashboard, and the ability to interrogate massive datasets through flexible drill-down technology, until the desired view is obtained. This “view” can be memorized and saved to a user-defined report menu for repetitive, scheduled execution and distribution.

Web Filter logs provide content for dynamic, real time graphical snapshots of network Internet traffic. Drilling down into the URL categories or bandwidth gauges dashboard quickly identifies the source of user-generated Web threats. SWG logs provide content for bar charts detecting security threats on the network so that prompt action can be taken to terminate them before they become a liability on your network.

Using the SR, threats to your network are readily targeted, 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 and intranet 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 SR 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 specified SR models
- **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.*

***TIP**: The "tip" icon is followed by italicized text giving you hints on how to execute a task more efficiently.*

***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.

Security Reporter Models 505, 705 and 735

Please refer to the appropriate IBM documentation when installing Security Reporter model 505 that uses IBM System x3250 M3 hardware, or model 705 or 735 that uses IBM System x3620 M3 hardware.

NOTE**: Integrated Management Module User's Guide explains how to configure and use the IMM tool to troubleshoot the unit and maintain its health. As of July 2011, this document was made available at **http://www-947.ibm.com/support/entry/portal/docdisplay?Indocid=MIGR-5079770&brandind=5000008

Model 505

System x3250 M3 Installation and User's Guide

IBM System x3250 M3 Types 4251, 4252, and 4261 Installation and User's Guide contains instructions on installing and configuring Security Reporter model 505, and viewing and using LED indicators and buttons on this unit. Also included is technical support, warranty, safety, and emissions compliance information. As of July 2011, this document was made available at **http://www-947.ibm.com/support/entry/portal/docdisplay?Indocid=MIGR-5082564&brandind=5000008**

System x3250 M3 Rack Installation Instructions

See the Rack Installation Instructions document on the IBM System x Documentation CD for complete rack installation and removal instructions.

Models 705 and 735

System x3620 M3 Type 7376 Installation and User's Guide

IBM System x3620 M3 Type 7376 Installation and User's Guide contains instructions on installing and configuring Security Reporter models 705 and 735, and viewing and using LED indicators and buttons on these units. Also included is technical support, warranty, safety, and emissions compliance information. As of July 2011, this document was made available at **http://www-947.ibm.com/support/entry/portal/docdisplay?brand=5000008&Indocid=MIGR-5084233**

System x3620 M3 Rack Installation Instructions

Rack Installation Instructions for IBM System x3620 M3 contains information on rack mounting Security Reporter models 705 and 735. As of July 2011, this document was made available at **http://www-947.ibm.com/support/entry/portal/docdisplay?Indocid=MIGR-5084236&brandind=5000008**

SERVICE INFORMATION

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

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

For technical assistance or warranty repair, please visit **http://www.m86security.com/support/** .

M86 Technical Support Call Procedures

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

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

IBM System Support

If troubleshooting Security Reporter model 505, 705 or 735, visit IBM's Systems Support Web site at **http://www.ibm.com/systems/support/** . Select **IBM System x** and choose **System x3250 M3** for model 505, and **System x3620 M3** for model 705 or 735, and then click **Finish** .

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

***NOTES**:*

For 300 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 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.

For 500 and 700 series models, the following items are also included in the carton:
- *1 AC power cord for 500 models, 2 AC power cords for 700 series models*
- *1 bezel to be installed on the front of the chassis for 700 and 730 models*
- *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 505, 705 and 735 models, the following items are also included in the carton:
- *1 AC power cord for 505 models, 2 AC power cords for 705 and 735 models*
- *1 set of rack mounting rails*

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 Model 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.*

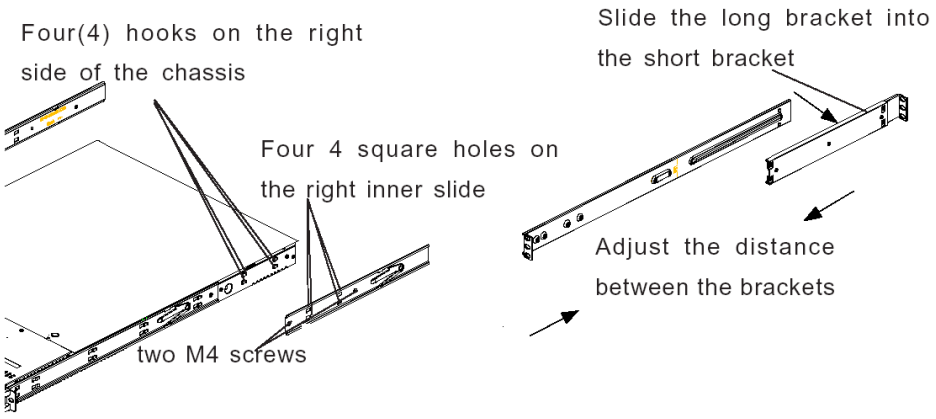
Rack Mount Instructions for 500 Model Servers

Rack Setup Suggestions

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

Install the Inner Slides

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

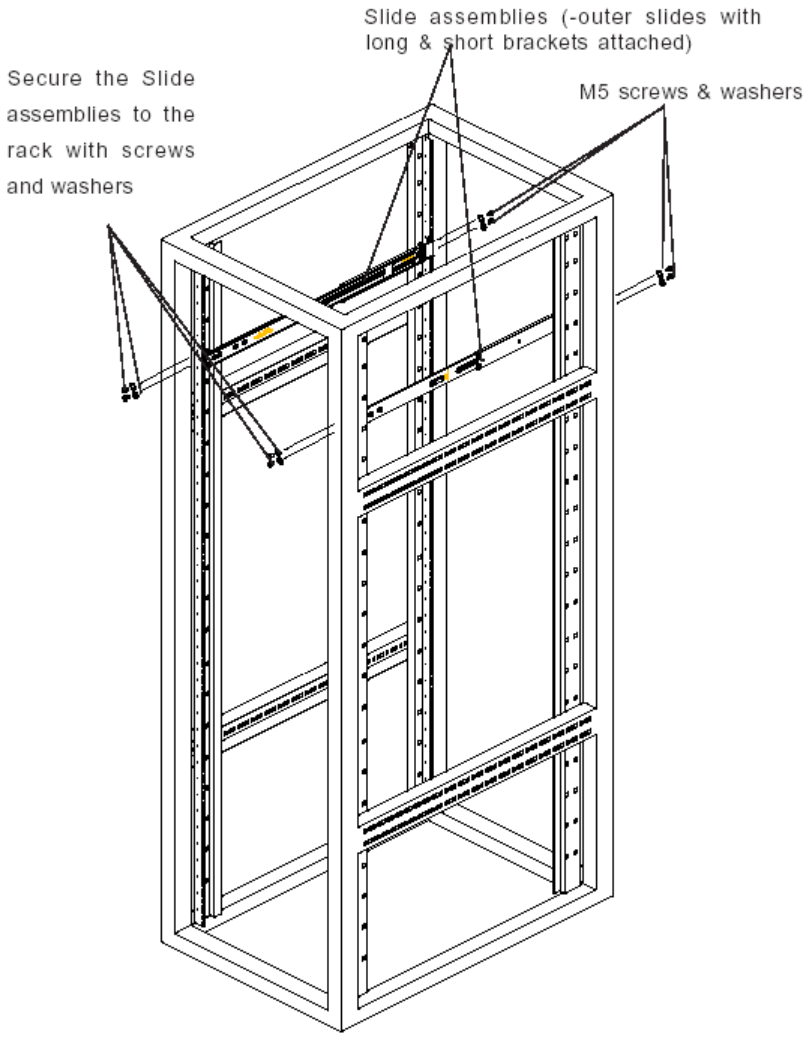


Install the Outer Slides

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

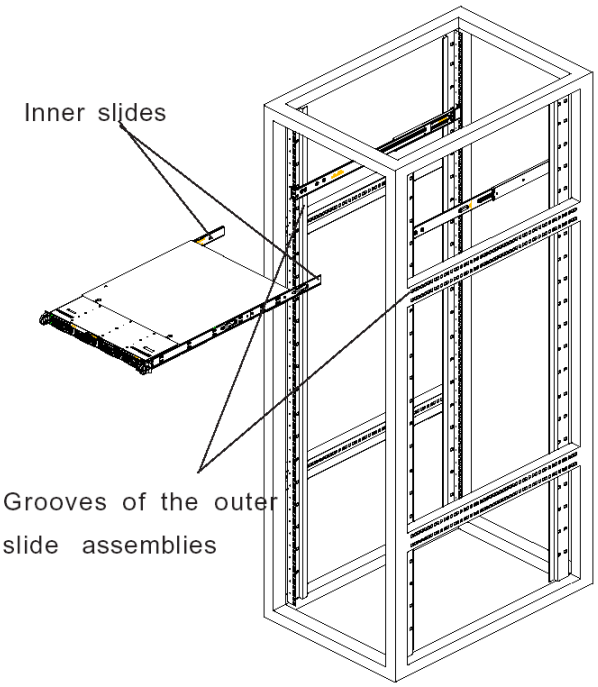
Install the Slide Assemblies to the Rack

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

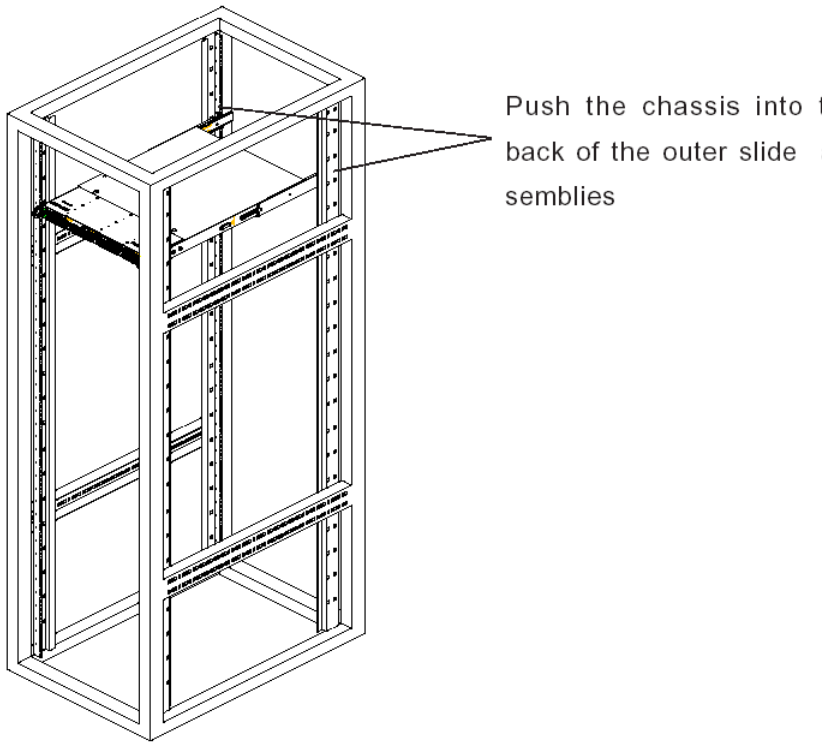


Install the Chassis into the Rack

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



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



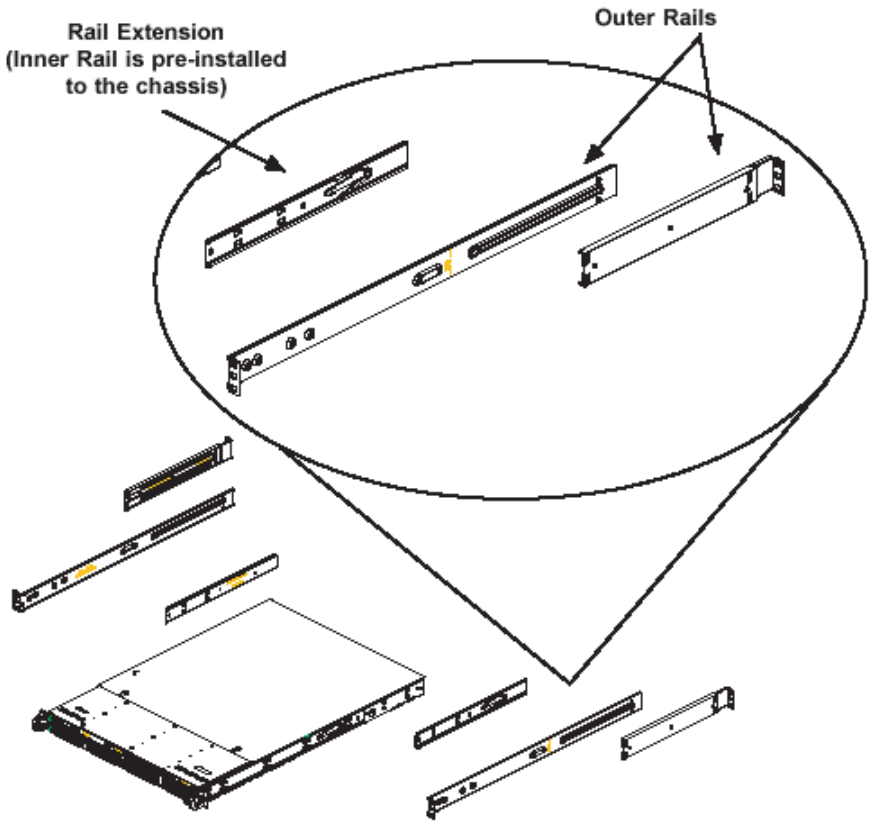
Rack Mount Instructions for 700 and 730 Model Servers

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

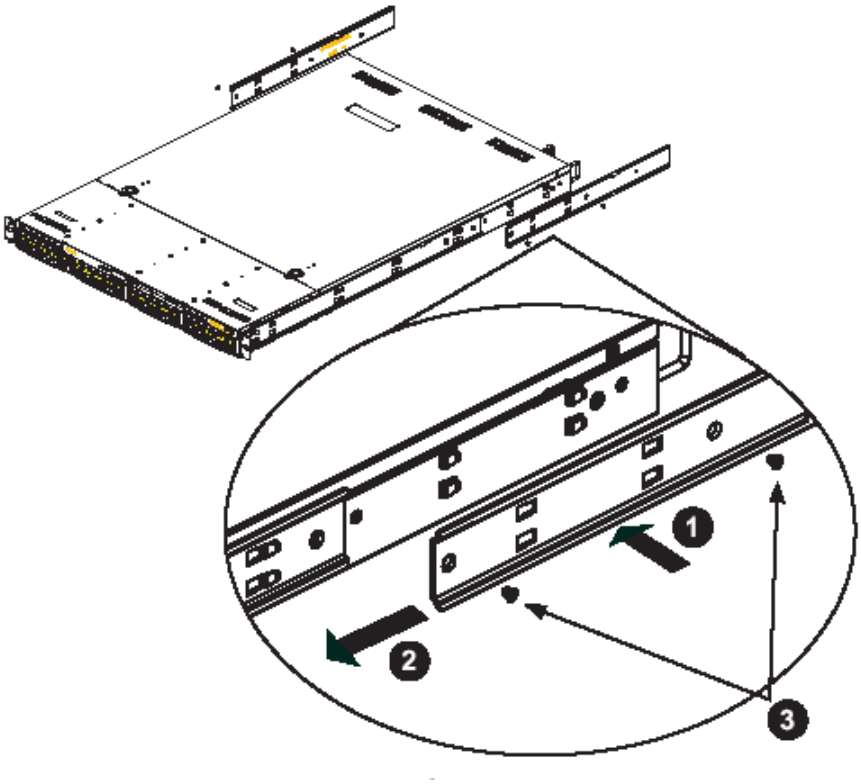
The chassis package includes two rack rail assemblies in the rack mounting kit. Each assembly consists of two sections: an inner fixed chassis rail that secures directly to the server chassis and an outer fixed rack rail that secures directly to the rack itself.



The 700 and 730 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.

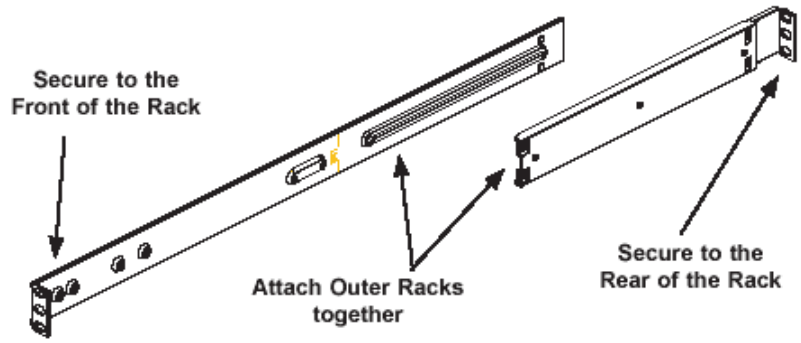
Install the Inner Rails

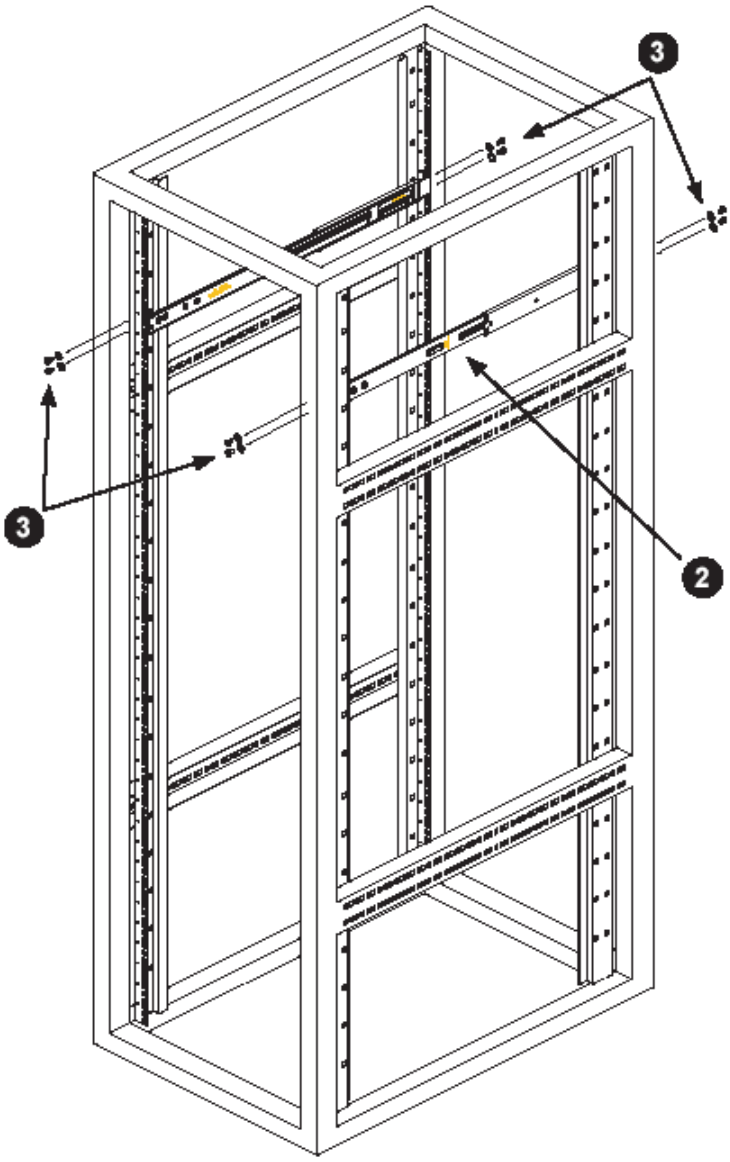
1. Place the inner rack extensions on the side of the chassis aligning the hooks of the chassis with the rail extension holes. Make sure the extension faces "outward" just like the pre-attached inner rail.
2. Slide the extension toward the front of the chassis.
3. Secure the chassis with 2 screws as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



Install the Outer Rails

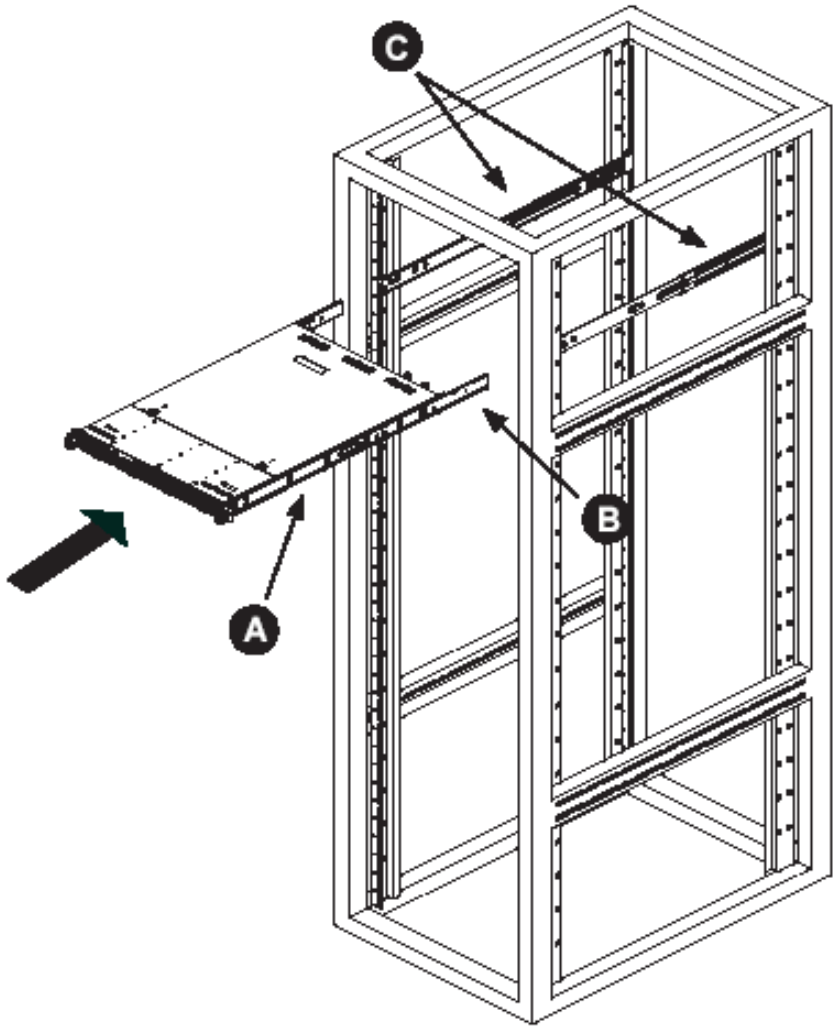
1. Attach the short bracket to the outside of the long bracket. You must align the pins with the slides. Also, both bracket ends must face the same direction.
2. Adjust both the short and long brackets to the proper distance so that the rail fits snugly into the rack.
3. Secure the long bracket to the 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

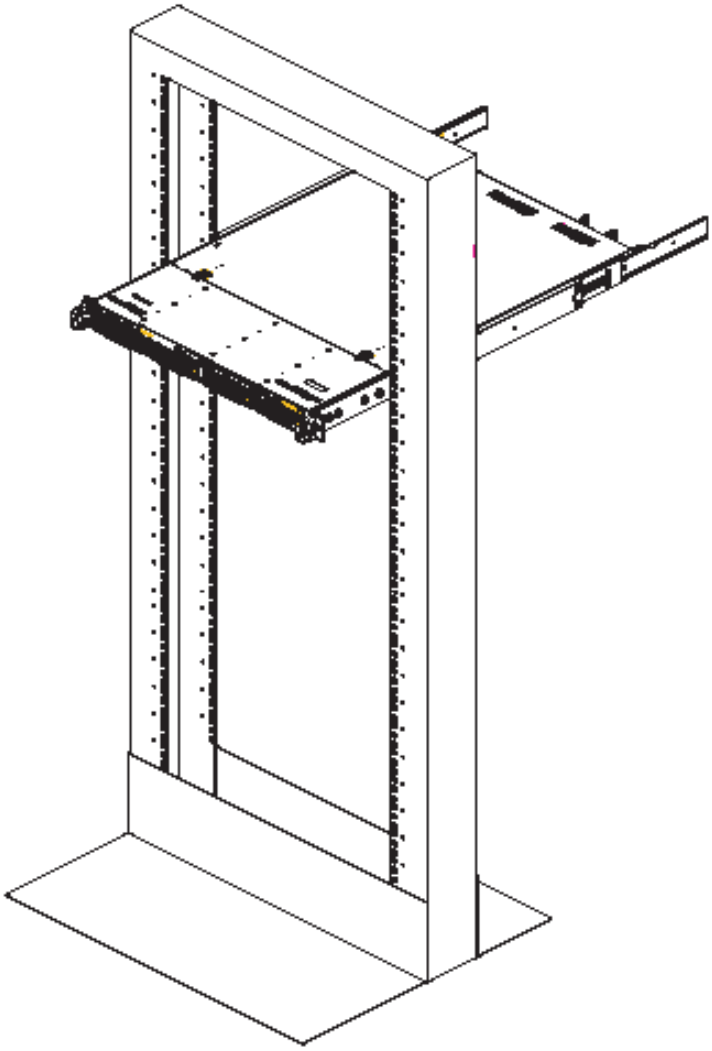
Install the Server into the Rack

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, 700, and 730 Model Chassis

After rack mounting a 500, 700, or 730 model 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).

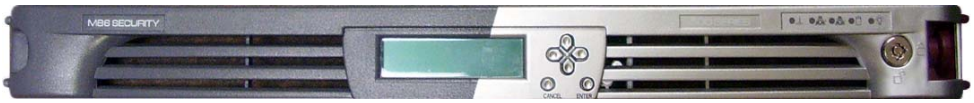


Fig. 1 - Front of bezel

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

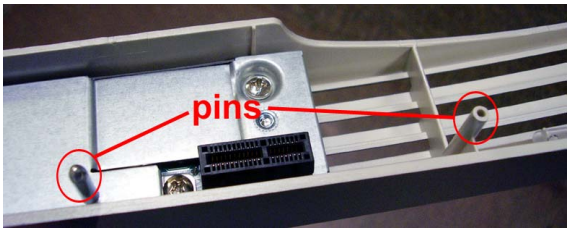


Fig. 3 - Pins on the inside at the top of the bezel

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).

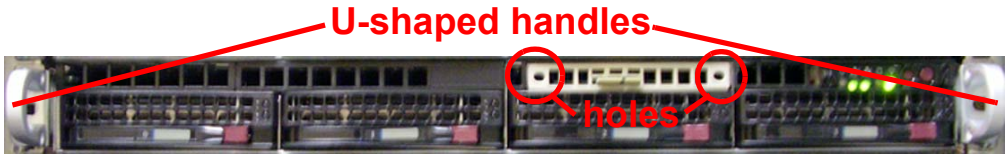


Fig. 4 - Front of chassis with U-shaped handles and holes above third hard drive identified

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

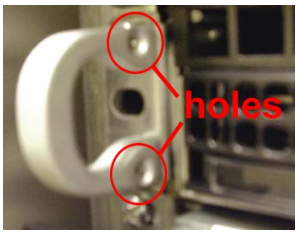


Fig. 5 - Holes in handle

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. If using a 300, 500, 700, or 730 server, 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.

If using a 505, 705 or 735 server, proceed to the text-based Quick Start setup procedures described in Step 1A.

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 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 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 model, Fig. 2 for a 500 model, Fig. 3 for a 700 or 730 model, Fig.4 for a 505 model, and Fig. 5 for a 705 or 735 model).

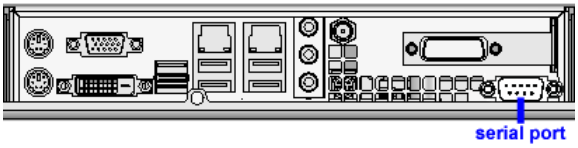


Fig. 1 - Rear of 300 model chassis with serial port identified

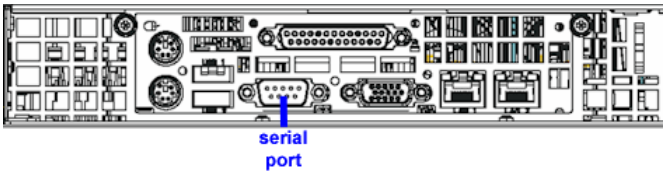


Fig. 2 - Portion of 500 model chassis rear with serial port identified

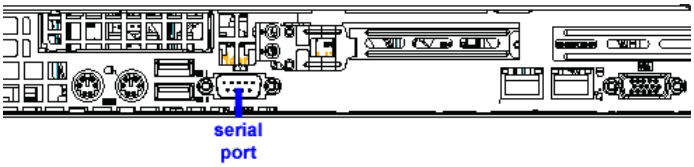


Fig. 3 - Portion of 700 / 730 model chassis rear with serial port identified

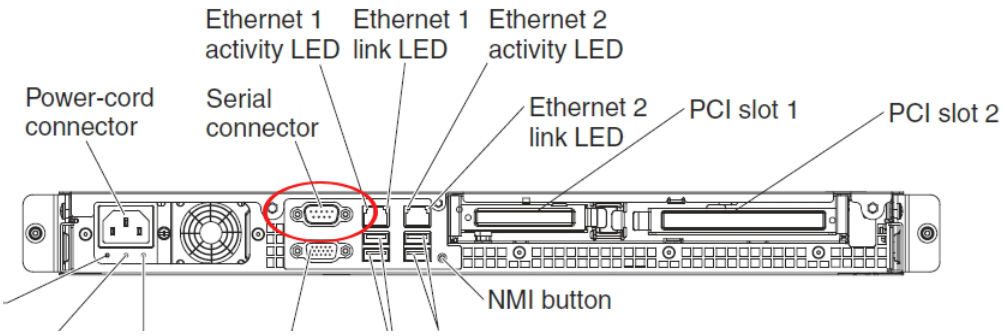


Fig. 4 - Rear of 505 model chassis, serial port circled in red

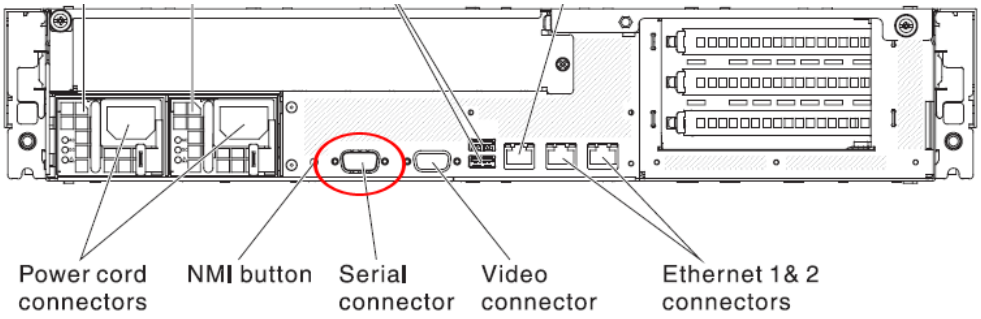


Fig. 5 - Rear of 705 / 735 model chassis, serial port circled in red

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 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. 6).

Fig. 6 - 300 model 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, 700, or 730 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. 7 for a 500 model, and Fig. 8 for a 700 or 730 model).

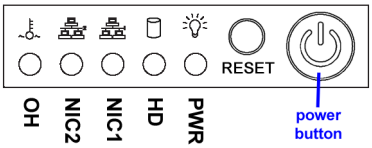


Fig. 7 - 500 model front panel, power button at far right

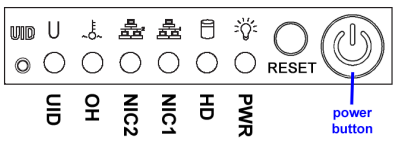


Fig. 8 - 700 / 730 model front panel, power button at far right

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.

Power up a 505 Model

A. Make sure the power cord is plugged into the back of the chassis.

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. Using a stylus or similar tool, depress the small white power button at the left of the front panel (see Fig. 9).

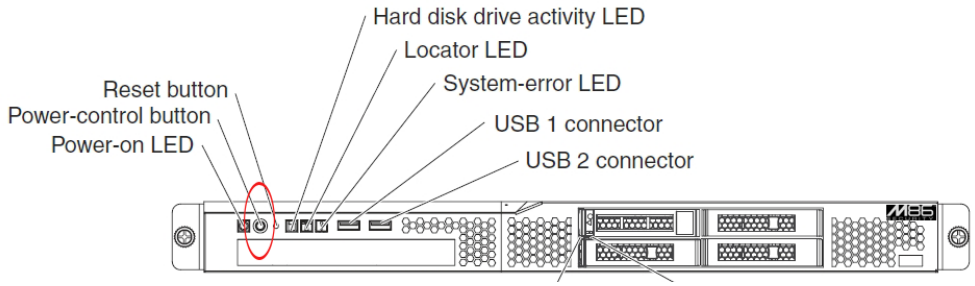


Fig. 9 - 505 model front panel, power button at far left

D. When the server powers up, as indicated by the power supply LED button being steadily lit, 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 705 or 735 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. Using a stylus or similar tool, depress the small white power button at the right of the front panel (see Fig. 10).

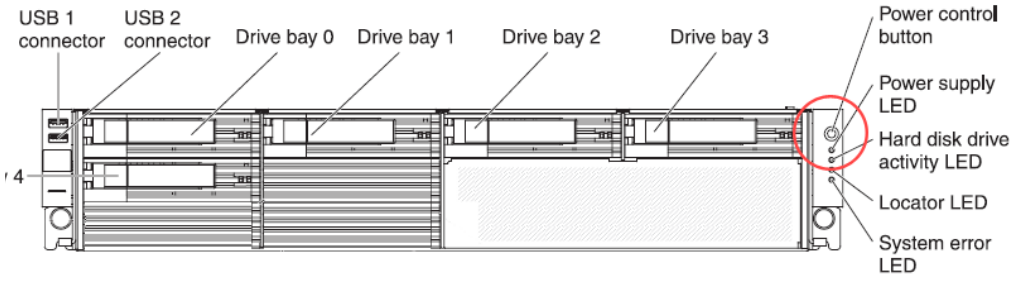


Fig. 10 - 705 / 735 model front panel, power button at far right

D. When the server powers up, as indicated by the green power supply LED button being lit, 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 August 16, 2011), Microsoft states: "HyperTerminal is no longer part of Windows.... If you previously used HyperTerminal to control serial devices, you can usually find a downloadable version of HyperTerminal on the Internet that is free for personal use."*

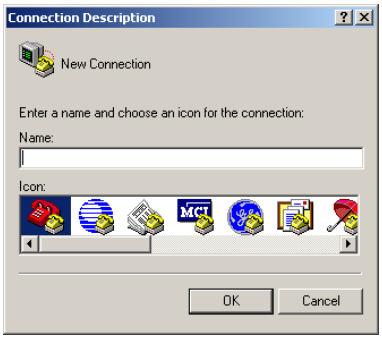
If you are using a Windows Vista or Windows 7 machine to conduct these quick start setup procedures and do not have an equivalent type of terminal emulator program installed on your workstation, Hilgraeve, Inc., the maker of HyperTerminal, offers HyperTerminal Private Edition for Windows Vista and Windows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

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

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

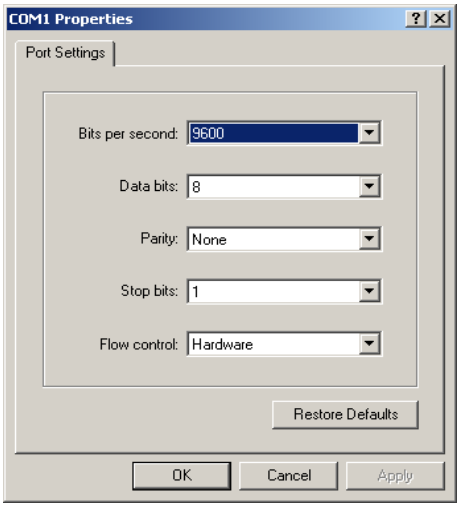
On the Windows XP machine:

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



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

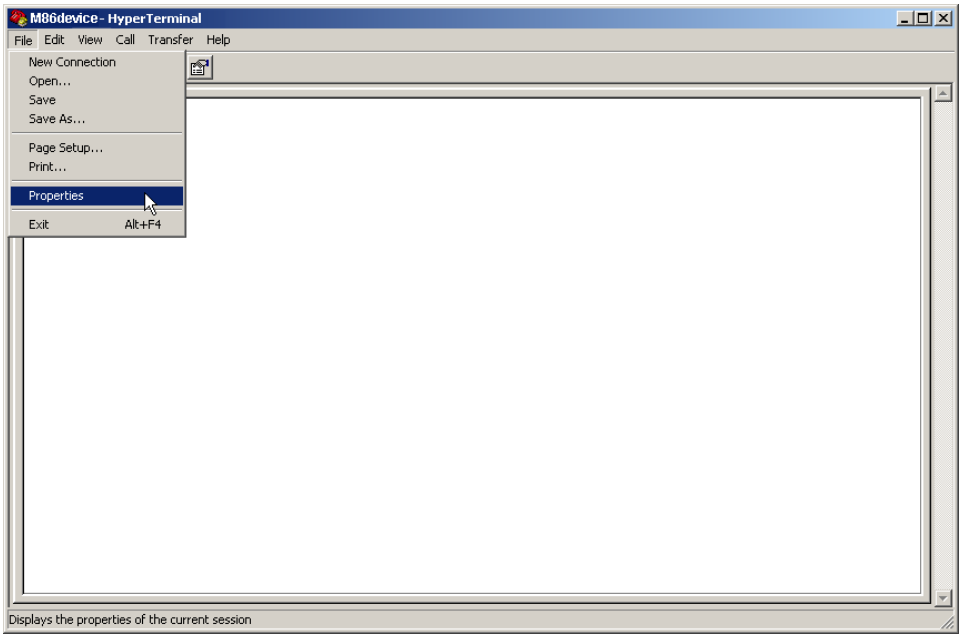
C. At the **Connect using** field, select the COM port assigned to the serial port on the laptop (probably "COM1"), and then click **OK** to open the Properties dialog box, displaying the Port Settings tab:



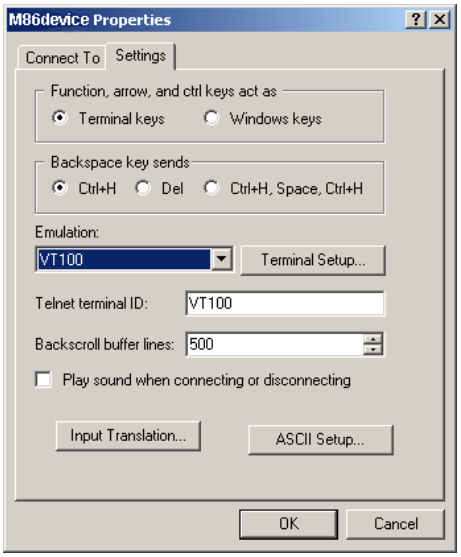
D. Specify the following session settings:

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

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



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



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

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

Login screen

The login screen displays after powering on the 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.*

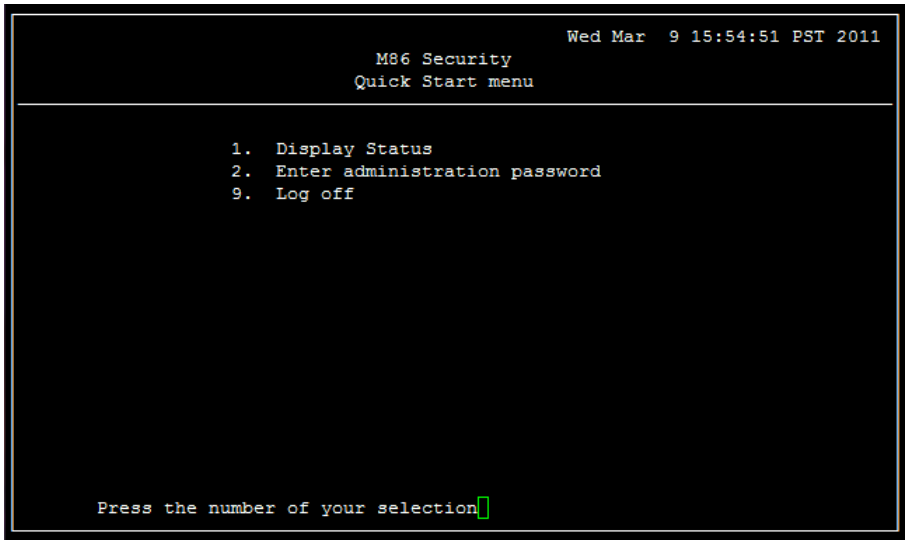
A. At the **login** prompt, type in ***menu***.

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

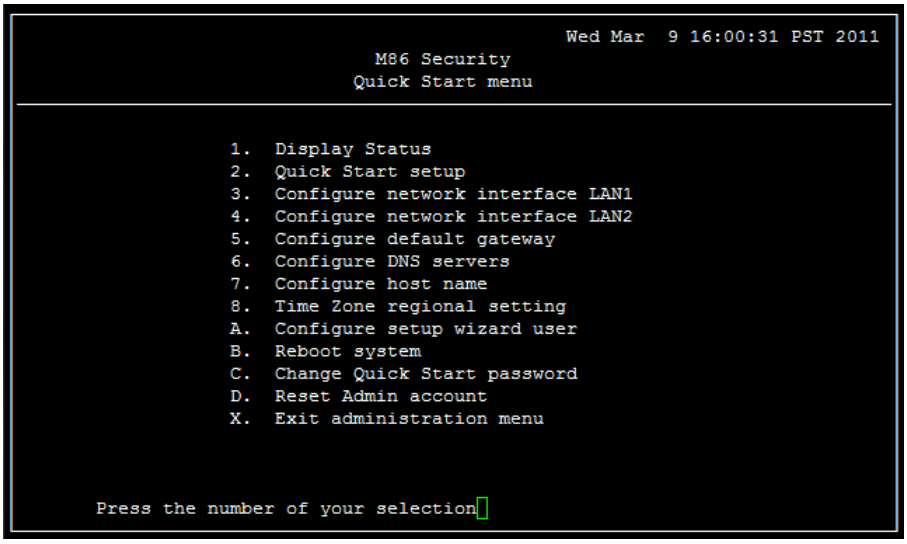


A. At the **Press the number of your selection** prompt, press **2** to select the Quick Start setup process.

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



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 hostname 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 hostname 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.

***NOTE**: After making any change to this menu selection, you must reboot the server to make your settings effective.*

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 by the global administrator for the SR Wizard user setup process and press **Enter**.

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

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

***NOTE**: The username and password you enter and save here will be used by the global administrator for Single Sign-On access in the SR user interface.*

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 is **#s3tup#r3k**) but will not change the global administrator's Single Sign-On password used for accessing the SR user interface via its login window (the default password is 'testpass'). Option D, "Reset Admin account", should be used for resetting the SR login password (the default account reset password is 'reporter1!') 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

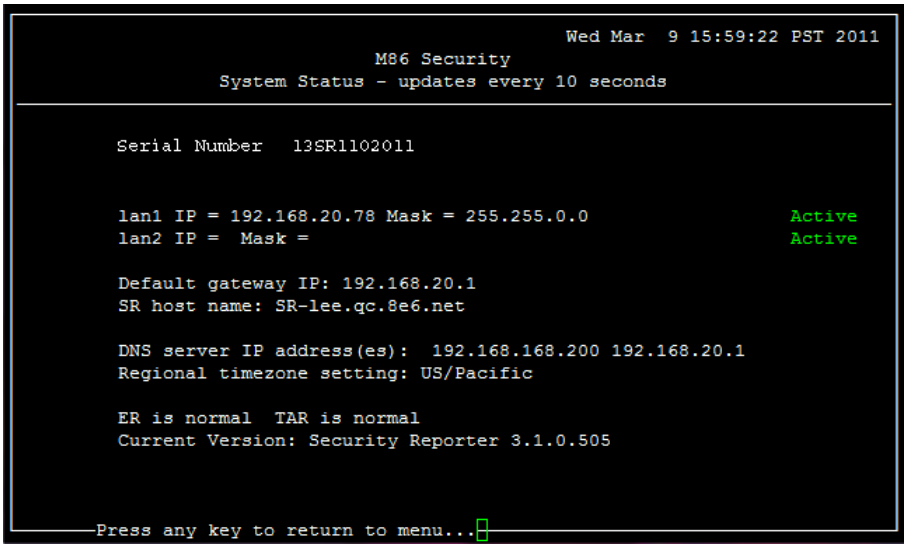
A. From the Quick Start menu, press **D** to go to the Reset admin GUI account confirmation screen that displays the following message:

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

***WARNING**: This option resets the global administrator's Single Sign-On password to 'reporter1!' 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



The System Status screen contains the following information:

- **Serial Number** assigned to the chassis
- **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)
- **SR 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 (System Configuration) and TAR (real time reporting) applications
- **Current 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 model: Up arrow, down arrow, left arrow, right arrow, checkmark, and "X" keys.
- On a 500, 700, or 730 model: Up, down, left, right, CANCEL, and ENTER keys.

300 model keypad at left, 500 and 700 model 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 >
- Serial Number >
- IP / LAN1 > *
- IP / LAN2 > *
- Gateway > *
- DNS 1 > *
- DNS 2 > *
- Host Name > *
- Regional Setting (Time zone, date, time) *
- Configure Setup *
- Reset Admin Account
- 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 hostname you assign to the SR server, as well as the username and password you create for logging into the "SR 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 Host name 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. You must now reboot the server in order for your changes to be effective.
- Choose **No** to return to the previous screen.

Configure Setup Wizard User

When the Configure Setup Wizard User option is selected, the Configure Setup Wizard User screen displays with two menu selections:

- Choose **Change User** to reset the global administrator's Single Sign-On username for accessing the SR login window (this is the username entered and saved during the SR Wizard setup process) and to return to the main menu.

***NOTE**: The username 'admin' cannot be used since it is already the default username. The default Single Sign-On password is 'testpass'.*

- Choose **Change Password** to reset the password for the SR 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.

Serial Number

When the Serial Number option is selected, the serial number of the chassis displays.

Reset Admin Account

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

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

*** WARNING *** The Admin console password will be reset to ‘reporter1!’ 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:

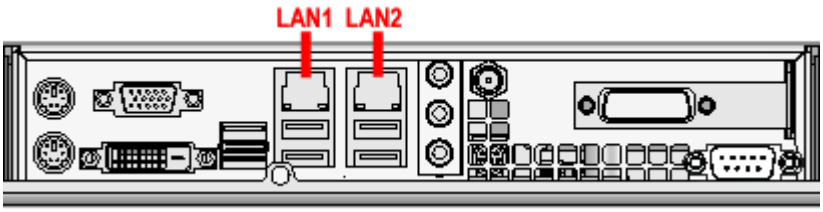
- **Contrast** - In the Contrast screen, use the left / right (arrow) keys to decrease / increase the text and screen contrast.
- **On Brightness** - In the On Brightness screen, use the left / right (arrow) keys to decrease / increase the brightness of a screen with a feature that is enabled.
- **Off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

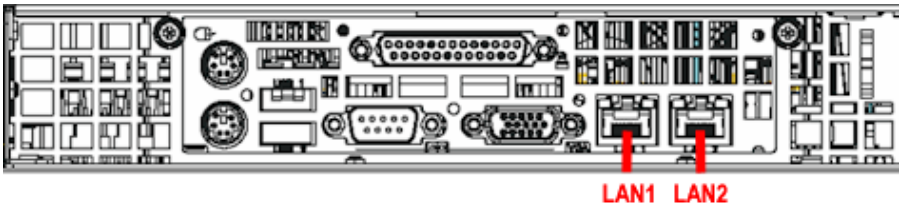
Step 2: Physically Connect the Unit to the Network

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.

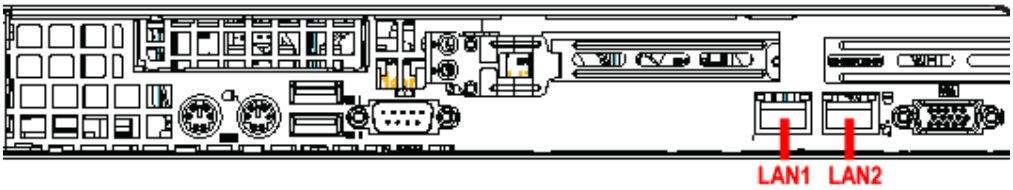
A. Plug one end of a standard CAT-5E cable into the SR's LAN 1 port, the port on the left.



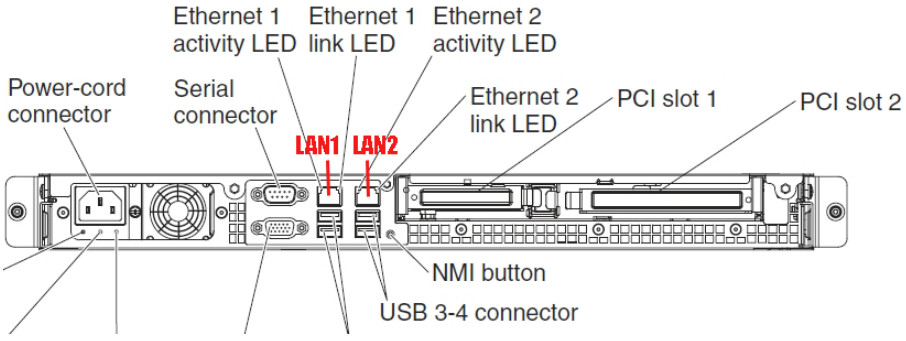
Rear of 300 model chassis with LAN ports identified



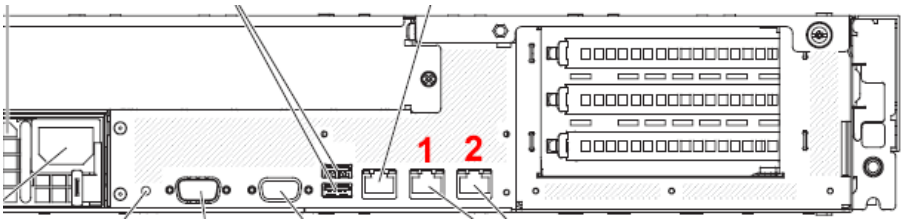
Portion of 500 model chassis rear with LAN ports identified



Portion of 700 / 730 model chassis rear with LAN ports identified



Portion of 505 model chassis rear with LAN ports identified



Portion of 705 / 735 model chassis rear with LAN 1 and LAN 2 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 SWG) 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: Access the SR and its Applications Online

Next you will access the SR and its applications online. For this step you will need your network administrator to provide you the following information:

- If using a Web Filter, IP range and netmask of machines on the network that the Security Reporter application will use for monitoring bandwidth on your network
- Web Filter or SWG IP address, and port number to be used between the Web Filter/SWG and SR

Access the SR via its LAN 1 IP Address

A. Launch an Internet supported browser:

- Firefox 9 or 10
- Internet Explorer 8 or 9
- Safari 5.0 or 5.1
- Google Chrome 16 or 17

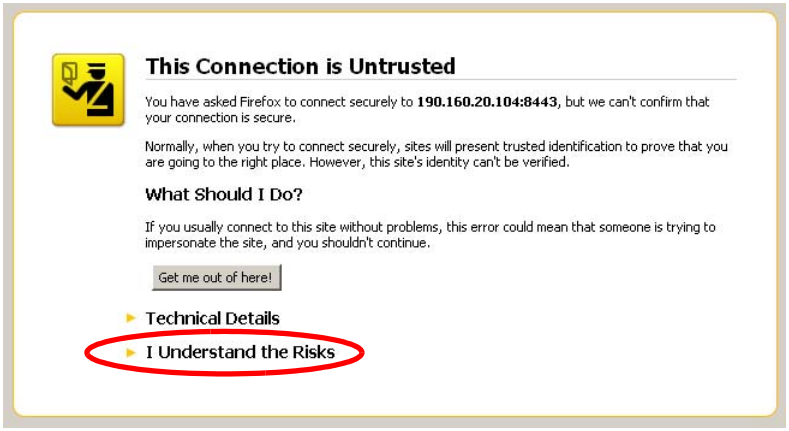
B. In the address field, type in the LAN 1 IP address you assigned to the SR in Step 1A (Quick Start setup) or Step 1B (IP / LAN1 and 2). Be sure to use “https” and port **:8443** for a secure connection, appended by “/SR/”. For example, if the SR were assigned an IP address of 10.10.10.10, you would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

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

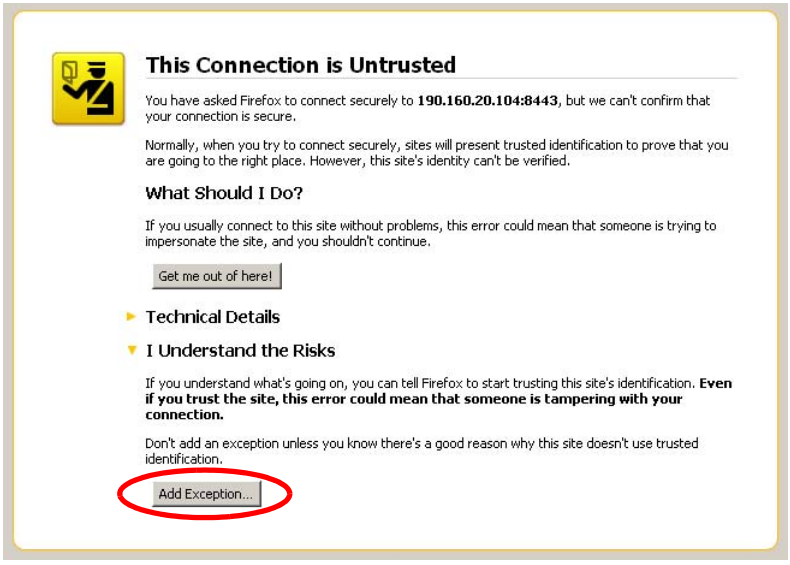
- If using Firefox, proceed to Accept the Security Certificate in Firefox.
- If using IE, proceed to Temporarily Accept the Security Certificate in IE.
- If using Safari, proceed to Accept the Security Certificate in Safari.
- If using Google Chrome, proceed to Accept the Security Certificate in Chrome.
- If the security issue page does not display in your browser, verify the following:
  - The 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

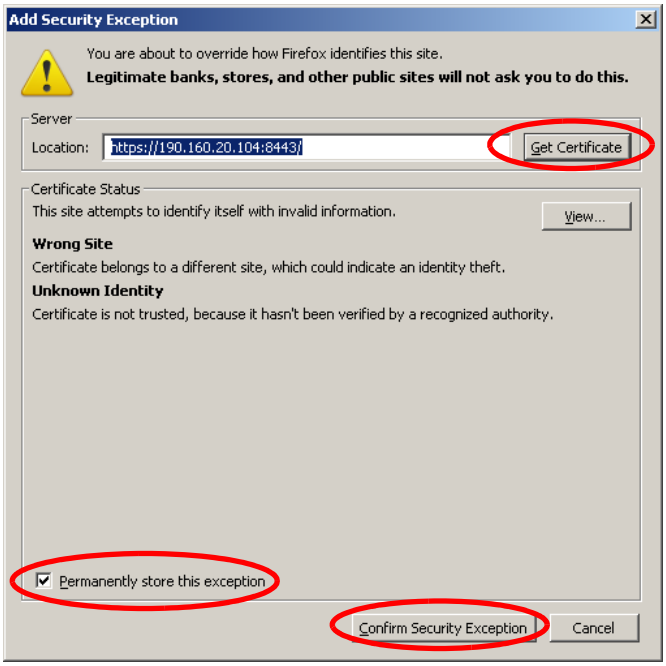
A. If using a Firefox browser, in the page "This Connection is Untrusted," click the option **I Understand the Risks**:



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



Clicking Add Exception opens the Add Security Exception window:



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

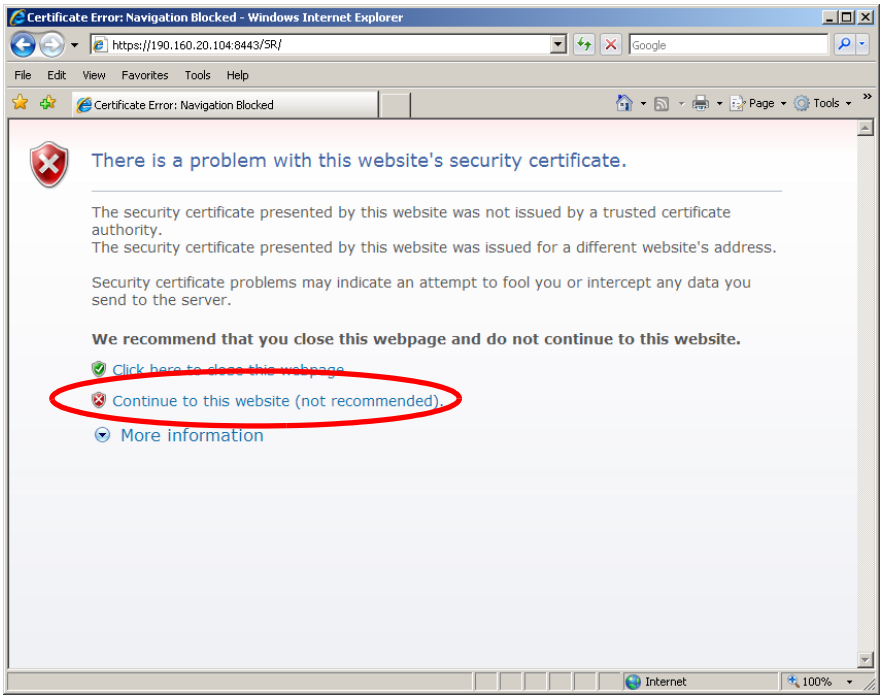
D. With the checkbox **Permanently store this exception** selected, click **Confirm Security Exception** to open the Security Reporter login window:

Proceed to Accept the End User License Agreement.

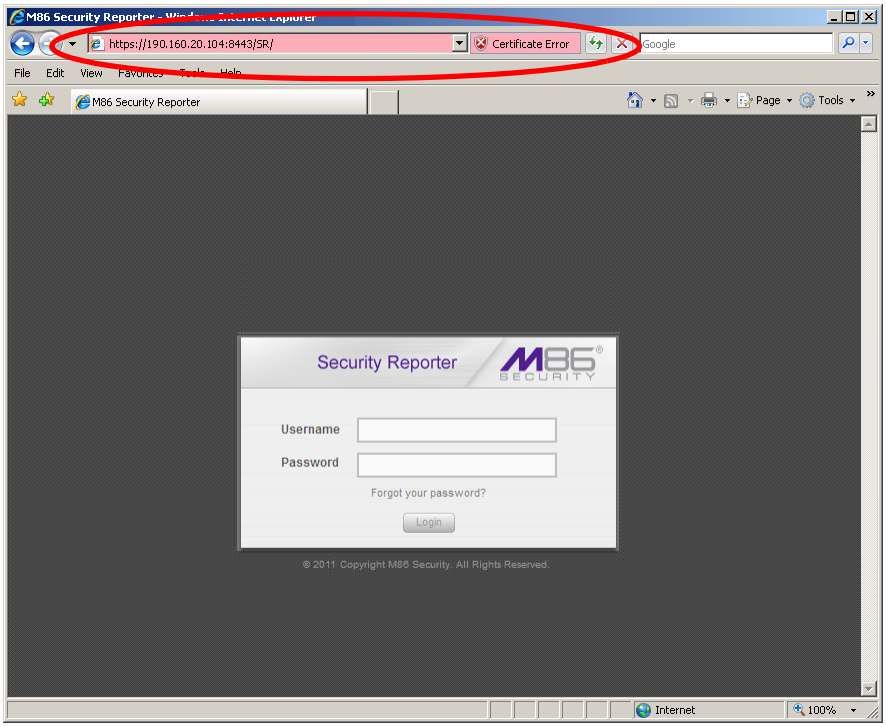
***NOTE**: On a newly installed unit, reports will remain inaccessible until logs are transferred to the SR and the database is built.*

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)**:



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



Proceed to Accept the End User License Agreement.

Accept the Security Certificate in Safari

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

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

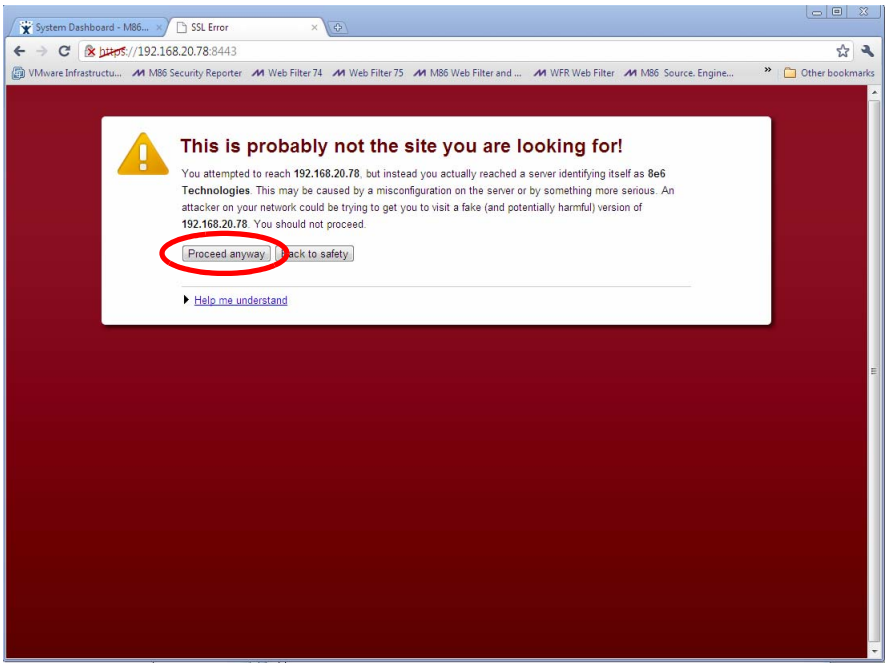
B. Click the "Always trust..." checkbox and then click **Continue**:

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

After the security certificate is installed, the Security Reporter login window displays. Proceed to Accept the End User License Agreement.

Accept the Security Certificate in Chrome

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



Clicking this button launches the Security Reporter login window:

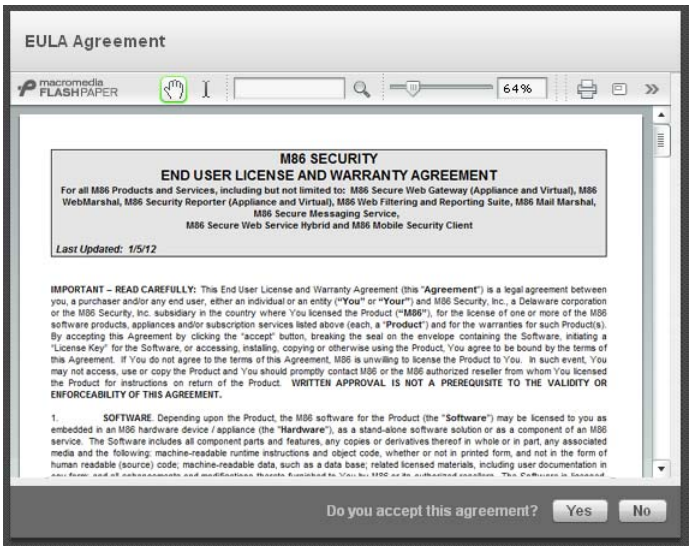
***NOTE**: The Security Certificate must be accepted each time a new browser is launched.*

B. Proceed to Accept the End User License Agreement.

Accept the End User License Agreement

A. In the Security Reporter login window, enter your **Username** and **Password**, and then click **Login** to proceed:

You may be prompted to accept a security exception for the SR application, after which the EULA Agreement dialog box opens:



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

Proceed to Log in to the Security Reporter Wizard.

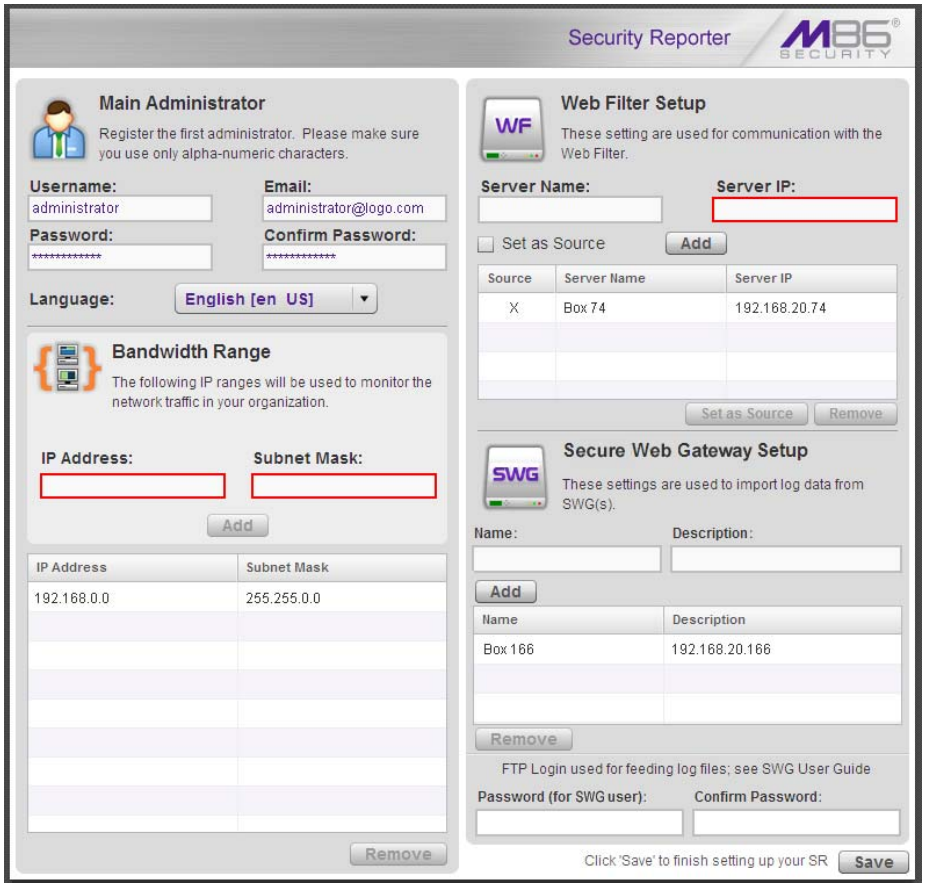
Log in to the Security Reporter Wizard

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 Configure Setup Wizard User screen in LCD Panel Setup Procedures (Step 1B):

B. In the **Password** field, type in the password specified in the wizard screen.

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

Use the SR Wizard to Specify Application Settings



At minimum, the Main Administrator section must be populated and saved. The following section(s) should be populated for the type of Web-access logging device(s) to be used with this SR, if you have the necessary data at this time:

- Bandwidth Range and Web Filter Setup sections, if using one or more Web Filters with this SR.
- Secure Web Gateway Setup section, if using one or more SWG policy servers with this SR.

***NOTE**: If the Web Filter or Secure Web Gateway sections are not populated at this time, the required information will need to be provided in the Device Registry panel of the user interface before the SR can function on your network.*

Enter Main Administrator Criteria

A. Enter the **Username** the global administrator will use when logging into the Security Reporter. 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.

D. Make a selection from the **Language** pull-down menu if you wish to change the language that currently displays in the user interface to another language included in the menu: English, Simplified Chinese, and Traditional Chinese.

***WARNING**: If choosing another language from this menu, the new language will immediately display in the user interface upon saving your entries in this panel.*

***NOTE**: Click **Save** in the lower right corner of this panel after making your entries and settings in this panel.*

For Web Filters: Go to Bandwidth Range and Web Filter Setup

***NOTE**: Bandwidth Range and Web Filter Setup entries are pertinent only to Web Filters to be used with this SR. If one or more Web Filters will be used with this SR, these entries are not required during this Wizard setup process, but if not entered during this process, must be configured in the device registry in order to use the SR on your network.*

Enter Bandwidth Range

A. Enter the bandwidth **IP Address** range the Security 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 Security 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 Security Reporter.

C. Click the “Set as Source” checkbox if this Web Filter will be designated the primary Web Filter to be associated with the Security 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.*

For SWGs: Go to Secure Web Gateway Setup

***NOTE**: Secure Web Gateway Setup entries are pertinent only to SWG Policy Servers to be used with this SR. If one or more Policy Servers will be used with this SR, these entries are not required during this Wizard setup process, but if not entered during this process, must be configured in the device registry in order to use the SR on your network.*

A. In the Secure Web Gateway Setup section, type in the **Name** and/or **Description** for the SWG.

B. Click **Add** to include the server criteria in the list box below.

***TIP**: To remove the SWG from the list box, select it and then click **Remove**.*

C. Type in the **Password (for SWG user)**—which is the password to be used by this SR and any SWG added to this SR’s device registry—and type this same password again in the **Confirm Password** field. The password entered in these fields will be used by all SWG Policy Servers set up in the Device Registry panel, so the SWGs can send logs to this SR.

***NOTE**: The password entered in this field must be added in the user interface of each SWG that will send logs to this SR.*

Save settings

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

Step 4: Generate SSL Certificate

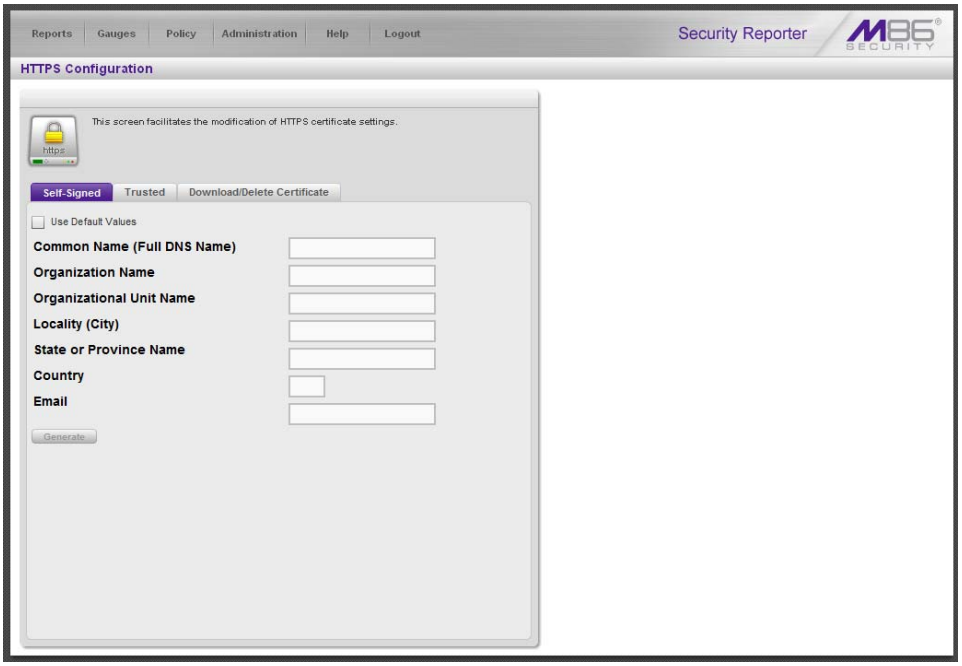
Generate a Self-Signed Certficate for the SR

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

A. In the Security Reporter login window, type in the **Username** and **Password** set up during the SR wizard.

B. Click **Login** to access the Report Manager application.

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



On the Self-Signed tab, you generate a Secure Socket Layer certificate that ensures secure exchanges between the SR and group administrator workstation browsers.

***WARNING**: Generating the self-signed certificate will restart the Report Manager. If the DNS name of the SR changes, a new certificate must be created and possibly added to each client workstation's trusted certificate list.*

D. Do the following:

- click the checkbox corresponding to **Use Default Values** to grey-out the tab, or
- make entries in these fields:
  a. **Common Name (Full DNS Name)** - hostname of the server, such as ***logo.com***.
  b. **Organization Name** - Name of your organization, such as ***Logo***.
  c. **Organizational Unit Name** - Name of your department, such as ***Administration***.

d. **Locality (City)** - Name of your organization's city or principality, such as ***Orange***.

e. **State or Province Name** - Full name of your state or province, such as ***California***.

f. **Country** - Two-character code for your country, such as ***US***.

g. **Email** - Your email address.

E. Click **Create** to generate the SSL certificate to be stored on the SR, and to restart the Report Manager. Thereafter, group administrators must accept the security certificate on their workstations in order for their machines to communicate with the Report Manager and/or System Configuration administrator console.

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

If using a Firefox, Safari, or Chrome browser, proceed to Step 5: Add Web Filter, SWG to Device Registry.

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 8 or 9
- Windows 7 with IE 8 or 9

Windows XP or Vista with IE 8 or 9

A. If using an IE 8 or 9 browser on a Windows XP or Vista machine, in the page "There is a problem with this website's security certificate.", click **Continue to this website (not recommended)**:

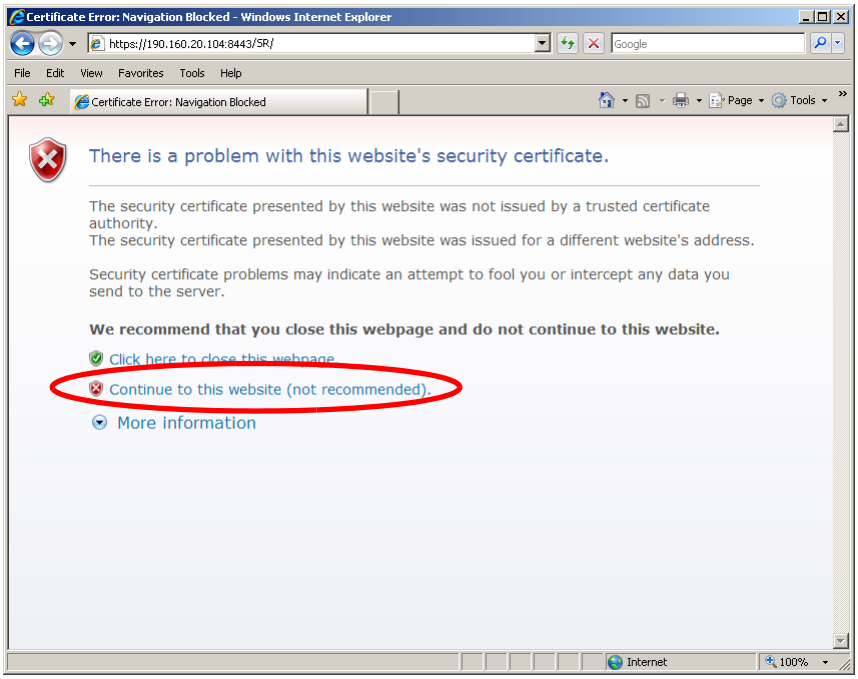


Figure A1: Windows XP, IE 8

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

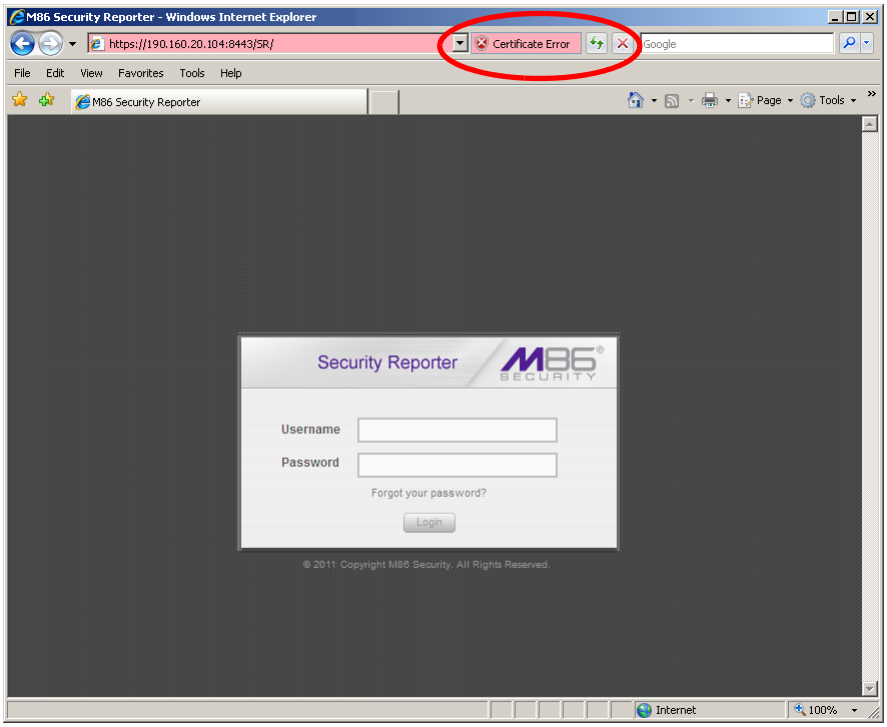


Figure A2: Windows XP, IE 8

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

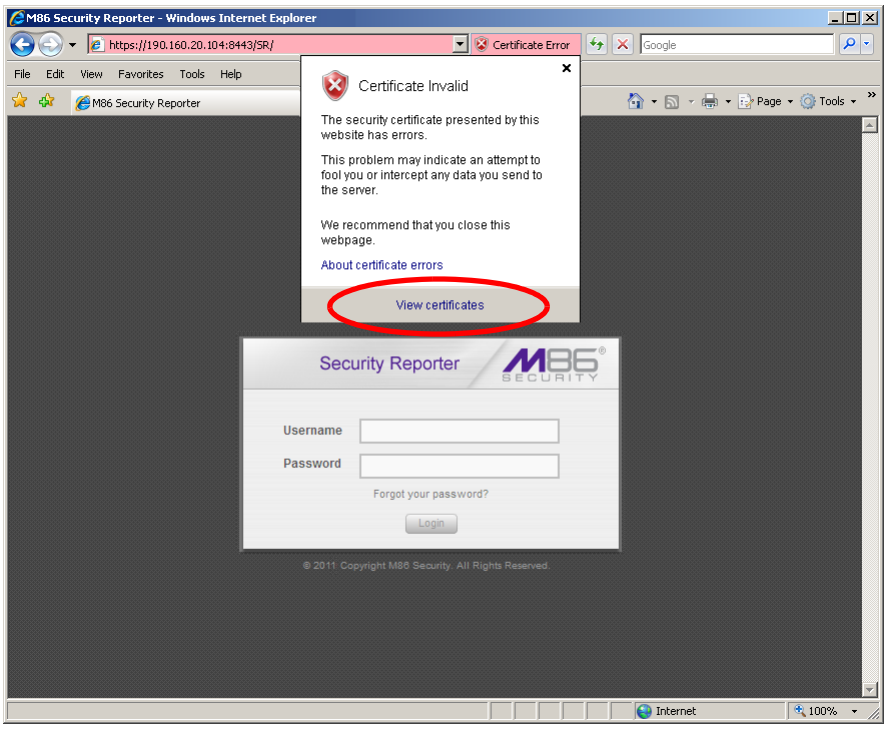


Figure B: Windows XP, IE 8

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

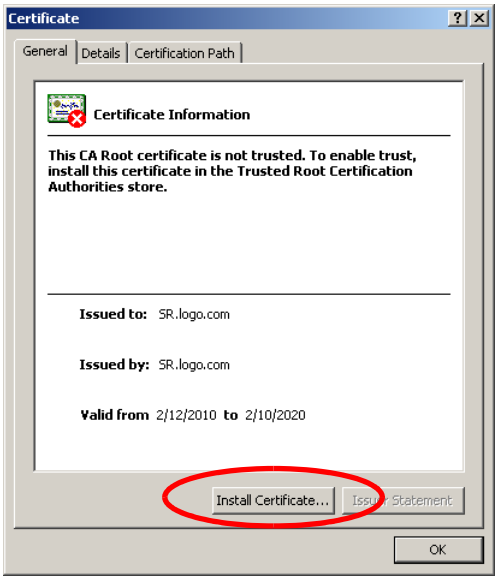


Figure C: Windows XP, IE 8

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

Figure D: Windows XP, IE 8

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

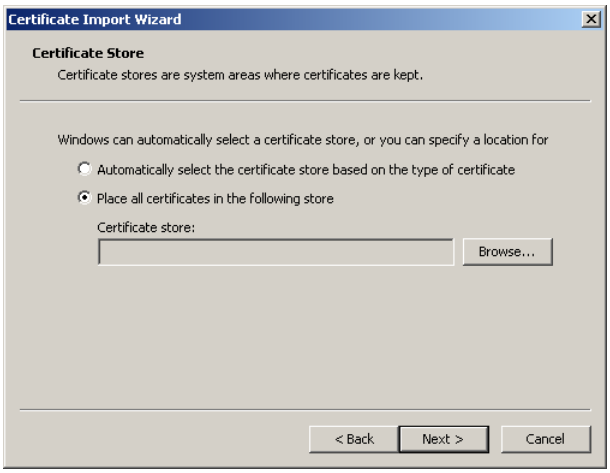


Figure E: Windows XP, IE 8

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

Figure F: Windows XP, IE 8

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

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

Figure H: Windows XP, IE 8

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

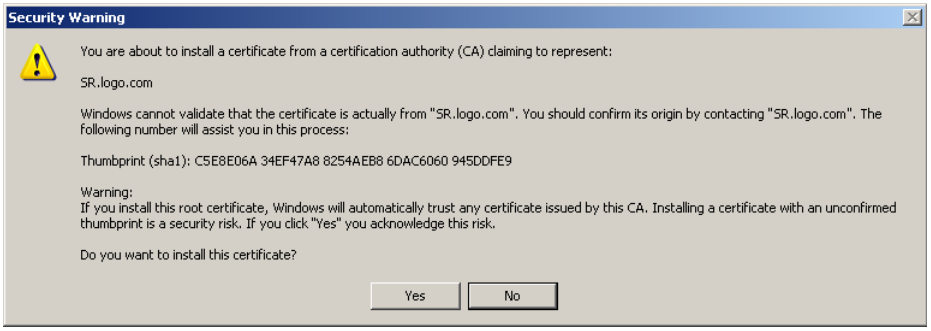


Figure I: Windows XP, IE 8

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

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

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

Windows 7 with IE 8 or 9

A. If using an IE 8 or 9 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 box.

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

D. In the Trusted sites 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 box.

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

G. Follow steps A to K documented in Windows XP or Vista with IE 8 or 9:

- 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 box (see Figure B).
- Click **View certificates** to open the Certificate window that includes the hostname 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 box (see Figure F).
- Choose "Trusted Root Certification Authorities" and then click **OK** to close the 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 box.

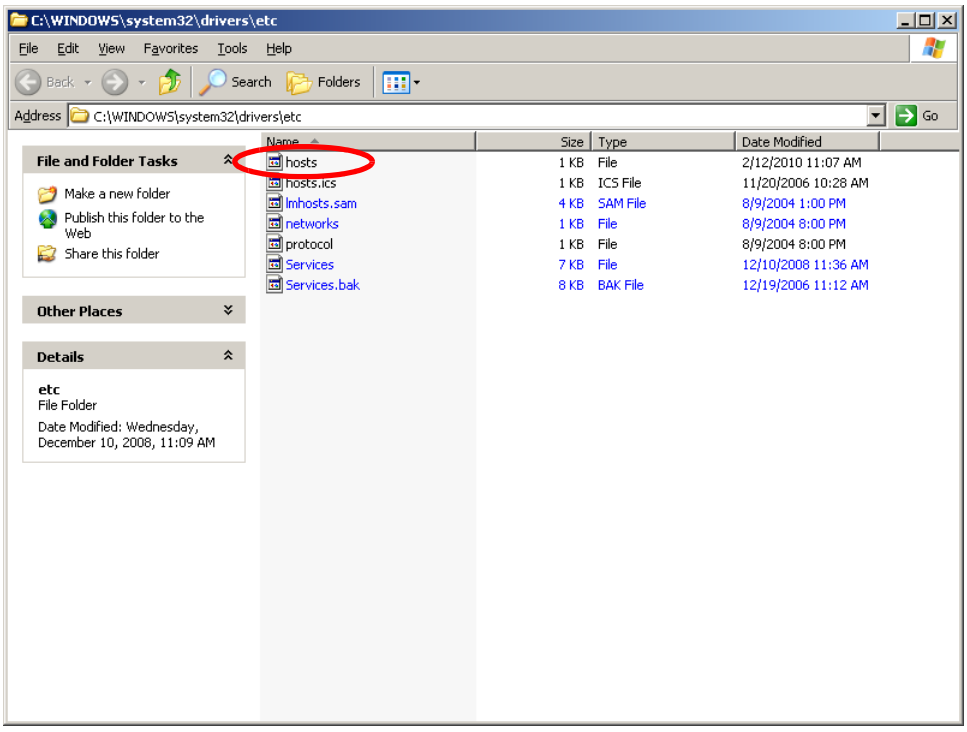
I. Select the Security tab, click **Trusted sites**, and then click **Sites** to open the Trusted sites box.

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

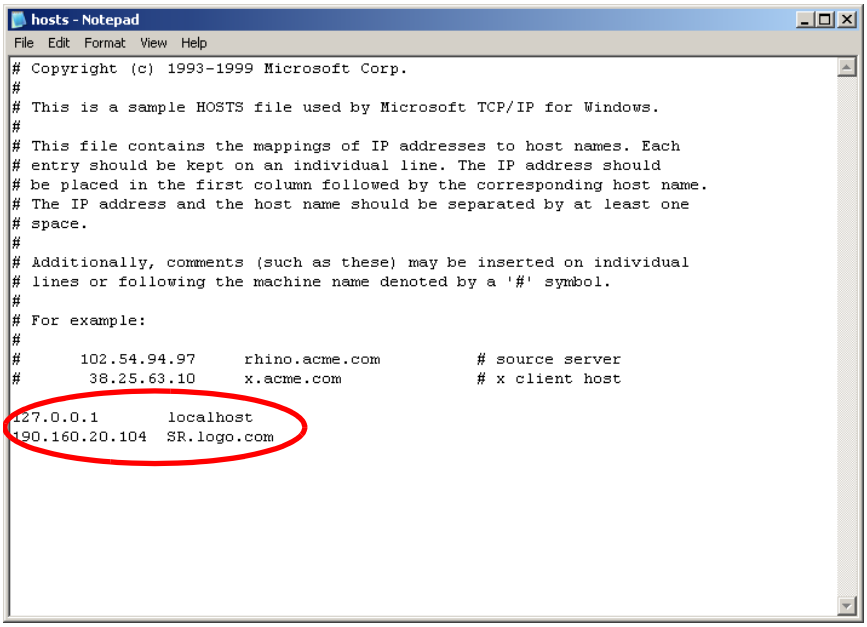
Now that the security certificate is installed, you will need to map the SR's IP address to its hostname. Proceed to Map the SR's IP Address to the Server's Hostname.

Map the SR's IP Address to the Server's Hostname

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

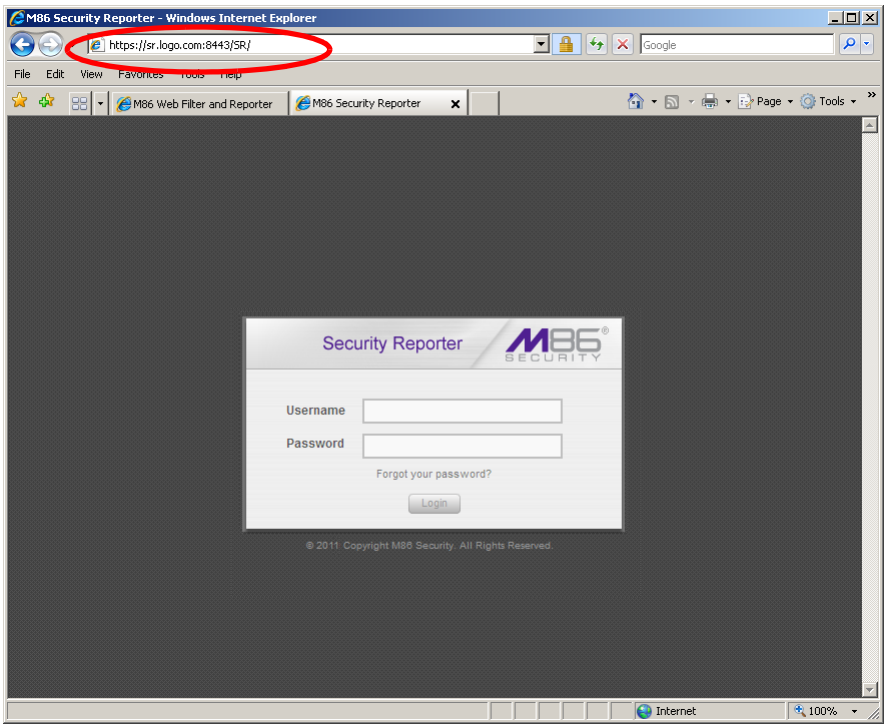


B. Double-click "hosts" to open a window asking which program you wish to use to open the file. Double-click "Notepad" or "TextPad" to launch the hosts file using that selected program:



C. Enter a line in the hosts file with the SR's IP address and its hostname—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 hostname instead of its IP address—that is **https://hostname:8443/SR/** would be used instead of **https://x.x.x.x:8443/SR/**. Click **Go** to open the SR Welcome window:

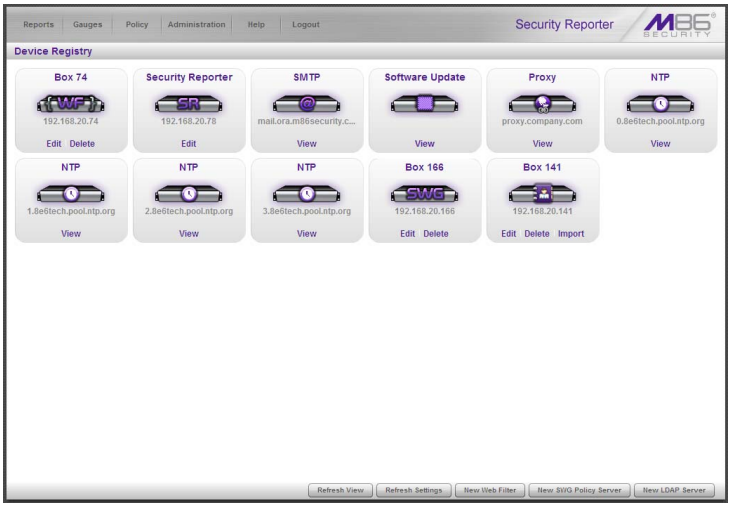


Proceed to Step 5: Add Web Filter, SWG to Device Registry.

Step 5: Add Web Filter, SWG to Device Registry

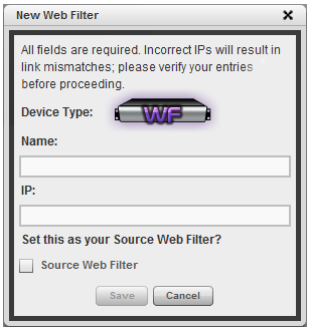
Before you begin configuring the Web Filter and/or SWG to send logs to the SR, you will need to add the Web Filter/SWG in the SR's Device Registry panel if the device(s) was/were not added during the SR Wizard installation process in Step 3.

A. In the navigation toolbar, with the Administration tab selected, click **Device Registry** to display the Device Registry panel:



Add a Web Filter Device

A. At the bottom of the Device Registry panel, click **New Web Filter** to open the New Web Filter window:



B. Type in the server **Name**.

C. Type in the **IP** address of the server.

D. If this Web Filter will be the source server, click the **Source Web Filter** checkbox.

E. Click **Save** to save and process your information, and to return to the Device Registry panel where an icon representing the Web Filter device you added now displays.

Add an SWG Device

A. At the bottom of the Device Registry panel, click **New SWG Policy Server** to open the New SWG Policy Server window:

The following information displays and cannot be edited: Path, Device Type (SWG).

***NOTE**: Make a note of the Path. You will need to enter this information in the SWG to allow the SWG to transfer logs to this SR (step 6, below). The Path consists of the IP address of the SR, and a unique number for each configured SWG policy server.*

B. Enter a **Name** for the device and/or a **Description** for the device.

C. Click **Save** to save and process your information, and to return to the Device Registry panel where an icon representing the SWG device you added now displays.

All SWG devices use the common password that you configured in the Secure Web Gateway Setup section of the SR Wizard. To change this password if required, edit any configured SWG device and click **Change Common Password**.

Step 6: Set up Web Filter, SWG Log Transfers

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 and/or SWG.

Web Filter Setup

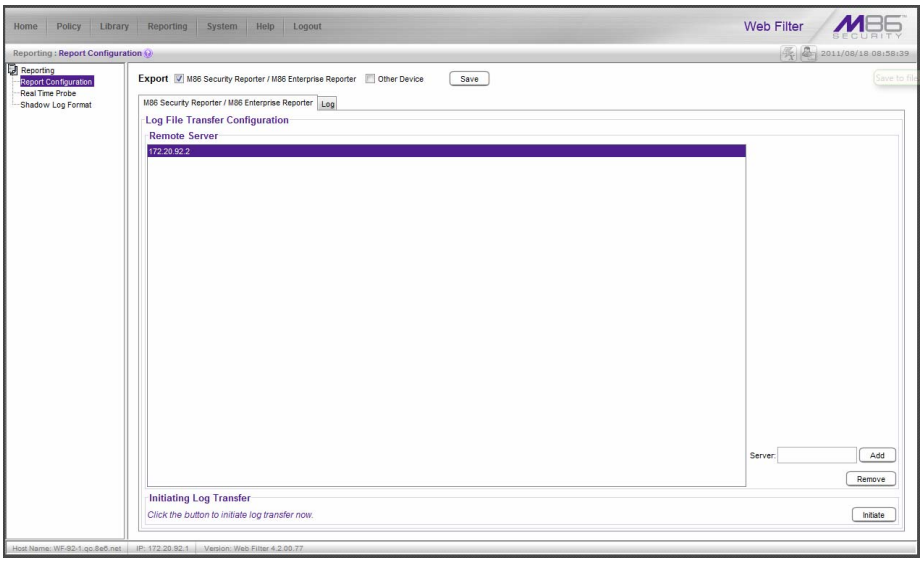
Web Filter Configuration

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 Security Reporter / M86 Enterprise Reporter** to display the M86 Security Reporter / 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.

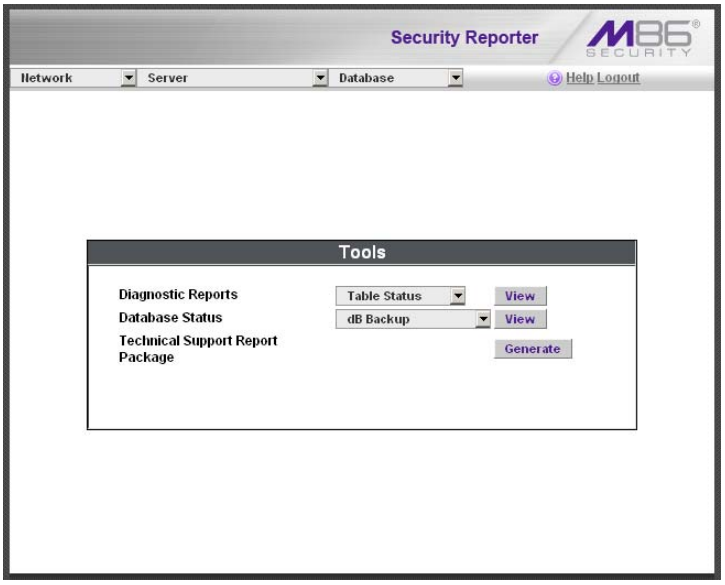
***NOTE**: It is recommended you wait for 1 - 2 hours after the initial installation so sufficient data is available for viewing.*

Web Filter Log Transfer Verification

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

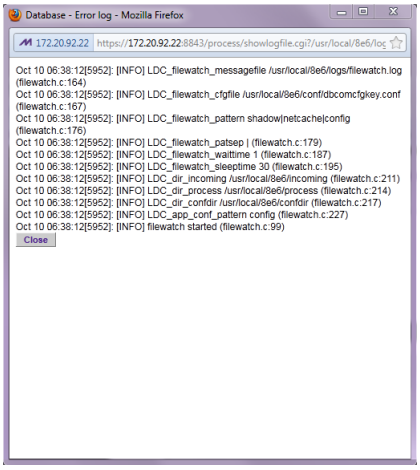
A. Access the System Configuration administrator console.

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



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

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

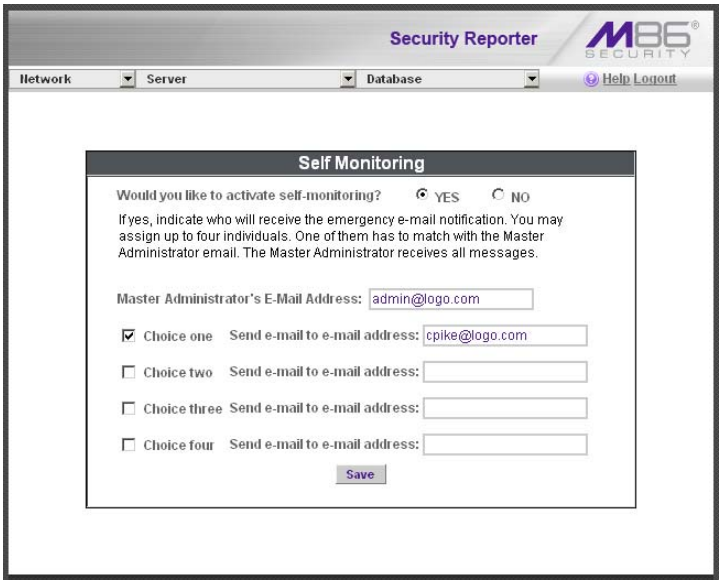


The transfer is working if you see an entry that includes the date and time for incoming shadow logs. The transfer should occur every hour. Once you see an entry, reporting information will be available one hour after the timestamp of the import listing.

Set Self-Monitoring

A. In the SR Report Manager navigation toolbar, select **Administration > System Configuration** to display the Server Status panel screen of the System Configuration administrator console.

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



C. Choose **YES** to activate monitoring.

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

E. Click **Choice one** and enter an e-mail address of an individual in your organization that you would like notified if the SR 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.

F. Click **Save**.

Use Single Sign-On Access

Single Sign-On Access

If using a Web Filter, the Single Sign-On (SSO) access feature is available for the global administrator account set up during the wizard hardware installation process. To enable this feature, be sure this same username and password combination is saved in the Web Filter (System > Administrator) for an 'Admin' account type. Also be sure the hostname for the SR server and Web Filter are entered in the hosts file. Thereafter, whenever accessing the Web Filter via the menu link in the SR user interface, the Web Filter splash screen displays, bypassing the Web Filter login window.

Default Usernames and Passwords

Without setting up Single Sign-On access for the global administrator account, default usernames and passwords for the SR application and Web Filter are as follows:

Application	Username	Password
Security Reporter	admin	testpass
Web Filter	admin	user3

Note that since the default username for both the Security and Web Filter are identical (*admin*), but the passwords are dissimilar, the SSO feature will not function. Thus, in order to use SSO, M86 recommends setting up an administrator account in the Web Filter that matches the global administrator account set up in the SR.

SWG Setup

Setup instructions differ depending on the SWG software version to be used with the SR (10.0 or 9.2.5).

SWG Configuration for Software Version 10.0

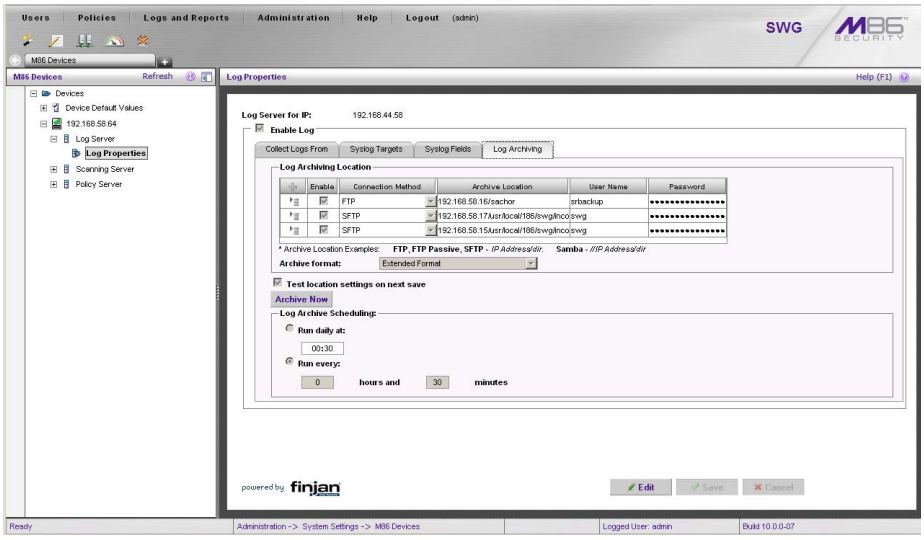
Configure SWG to Send Logs to the SR

A. Access the SWG user interface.

B. Navigate to **Administration > System Settings > M86 Devices**.

C. In the Devices tree, find the SWG's IP address and drill down to **Log Server > Log Properties**.

D. In the Log Properties panel, click the **Log Archiving** tab:



E. Click **Edit** to activate the elements in this tab.

F. In Log Archiving Location, click the '**+**' (plus character) in the table header to add a new row in the table, and specify the following criteria to the right of the checkmark in the Enable column:

- **Connection Method**: Select "SFTP" from the pull-down menu.
- **Archive Location**: Type in the Path information that you noted when setting up this SWG in the SR Device Registry. Do not include the leading //. For example: ***200.260.10.56/2***.
- **User Name**: Type in the SWG's Username from the Device Registry, which is ***swg*** (in lower case characters).
- **Password**: Type in the common password for SWG transfer as configured on the SR.

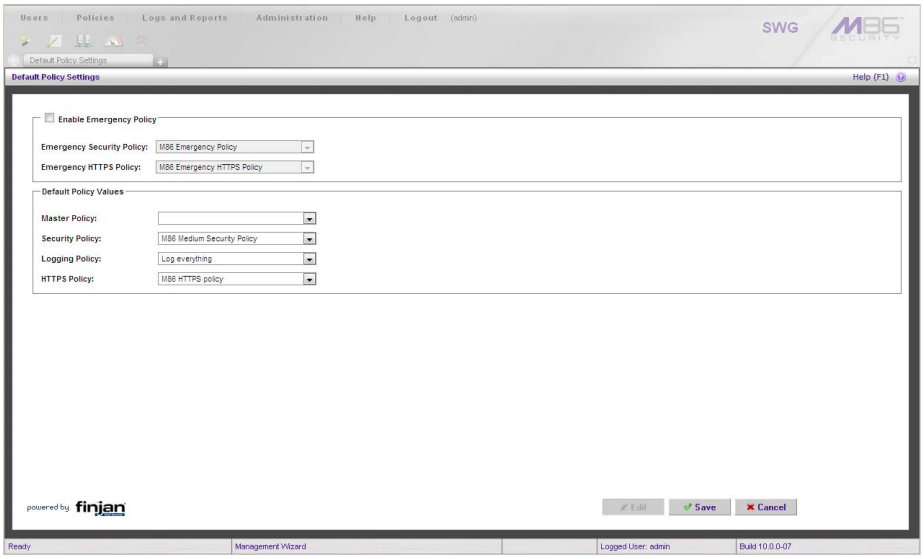
***NOTE**: Be sure "Extended Format" is selected for Archive format, and Log Archive Scheduling specifies the correct interval you wish to use for sending logs from the SWG to the SR.*

G. Click **Save** to save your settings.

Policy Settings

A. Navigate to **Policies > Default Policy Settings** and verify if the settings in Enable Emergency Policy and Default Policy Values are the ones you wish to use for sending logs to the SR.

B. To modify any settings, click **Edit** to activate all elements in this panel:



C. Make your selections from the pull-down menu(s).

D. Click **Save** to save your edit(s).

SWG Configuration for Software Version 9.2.5

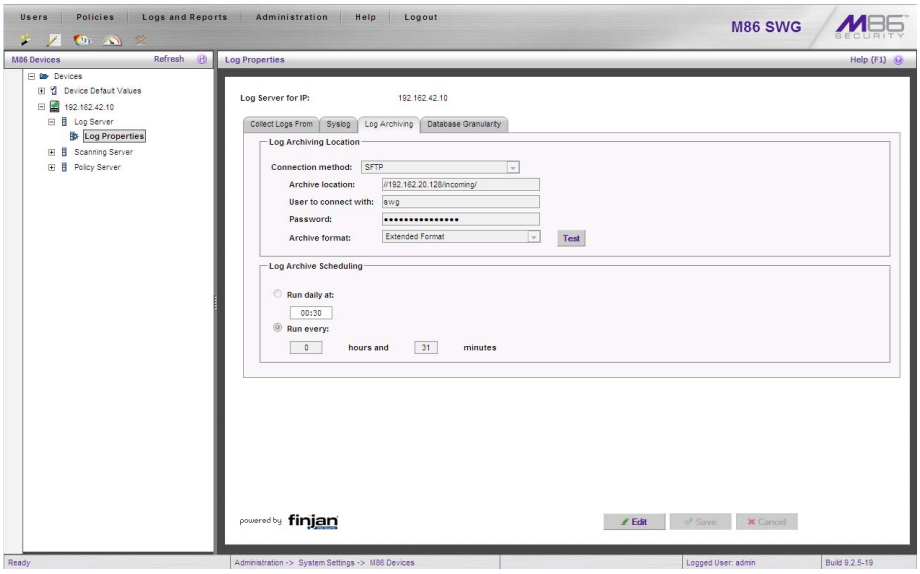
Configure SWG to Send Logs to the SR

A. Access the SWG user interface.

B. Navigate to **Administration > System Settings > M86 Devices**.

C. In the Devices tree, find the SWG's IP address and drill down to **Log Server > Log Properties**.

D. In the Log Properties panel, click the **Log Archiving** tab:



E. Click **Edit** to activate the elements in this tab.

F. In Log Archiving Location, be sure the following is specified:

- **Connection Method**: "SFTP" is selected from the pull-down menu.
- **Archive Location**: The Path information that you noted when setting up this SWG in the SR Device Registry. The Path will begin with a double backslash (//). For example: ***//200.260.10.56/2***.
- **Password**: The common password for SWG transfer as configured on the SR.
- **Archive Format**: "Extended" is selected from the pull-down menu.

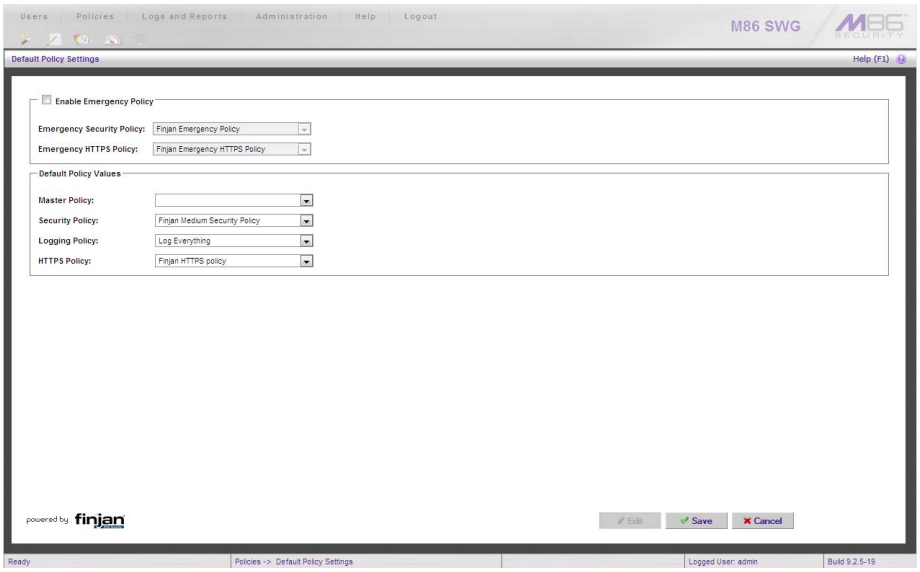
***NOTE**: Be sure Log Archive Scheduling specifies the correct interval you wish to use for sending logs from the SWG to the SR.*

G. Click **Save** to save your settings.

Policy Settings

A. Navigate to **Policies > Default Policy Settings** and verify if the settings in Enable Emergency Policy and Default Policy Values are the ones you wish to use for sending logs to the SR.

B. To modify any settings, click **Edit** to activate all elements in this panel:



C. Make your selections from the pull-down menu(s).

D. Click **Save** to save your edit(s).

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 SR database. Once the SR database is populated—this generally takes a full day—the Report Manager can be used for generating reports.

Initially, you will only be able to report on IP addresses. To implement user names in SR reports using a Web Filter, please consult the System Configuration Section of the Security Reporter User Guide. Refer to the Reports Section, Real Time Reports Section, and Security Reports Section of the Security Reporter User Guide for information on generating reports.

For real time and security reports, the next step is to set up user groups or administrator groups. For real time reports, 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.*

***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 Report Manager user interface. The main areas of focus in this section are productivity reporting, security reporting, and real time reporting.

In the Productivity Reports Usage Scenarios sub-section you will learn how to:

- access Summary 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
- generate a report view grouped by two sets of criteria
- 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 SR must collect data for a full day in order to generate Summary Reports. To use Drill Down Reports, the SR must collect data for a couple of hours. Therefore, it would be best to wait a day after the SR has been installed and fully operational before beginning any of the exercises described in the Productivity Reports Usage Scenarios sub-section.*

In the Security Reports Usage Scenarios sub-section you will learn how to:

- use the four basic reports for an overview of network security threats
- drill down into a Security Report and create a detail report view
- create a customized Security Report
- export a Security Report
- save a Security Report
- schedule a Security Report to run

In the Real Time Reports Usage Scenarios sub-section you will learn how to:

- navigate panels to access tools for configuring the Report Manager
- 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

Productivity Reports Usage Scenarios

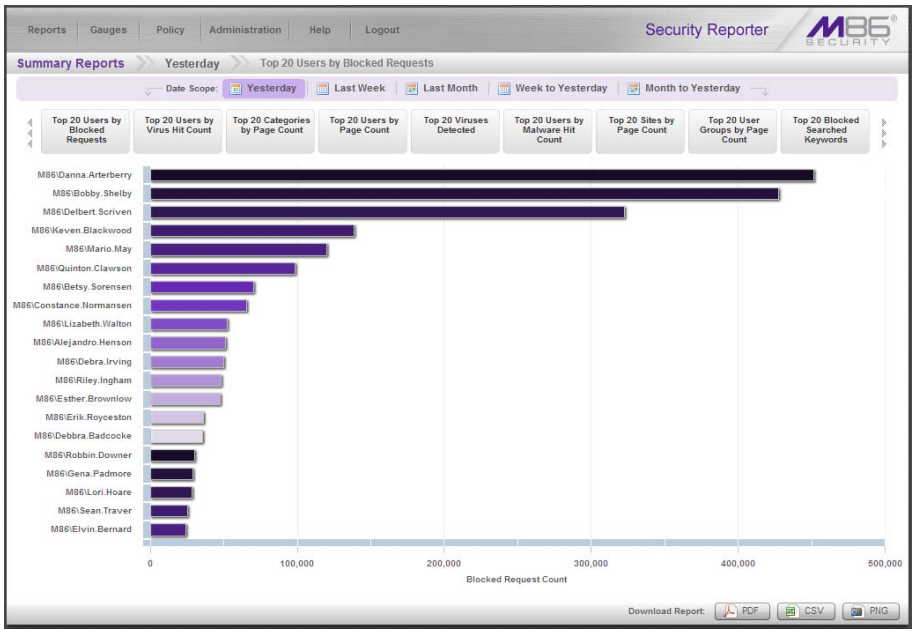
This collection of productivity reporting scenarios is designed to help you use the Report Manager to create typical snapshots of end user Internet activity. Each scenario is followed by setup information. Please consult the “How to” section in the index of the Security Reporter User Guide for pages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

I. Summary Report and Drill Down Report exercise

In this exercise you will learn how to use Summary 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), and various types of reports you can generate for each of these two basic drill down report types.

Step A: Use Summary Reports for a high level activity overview

From the navigation menu, select **Reports > Summary Reports** to display yesterday’s “Top 20 Users by Blocked Requests” Summary 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 Summary Report you wish to view. For this example, click “Top 20 Categories by Page Count”:

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 a Summary 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.

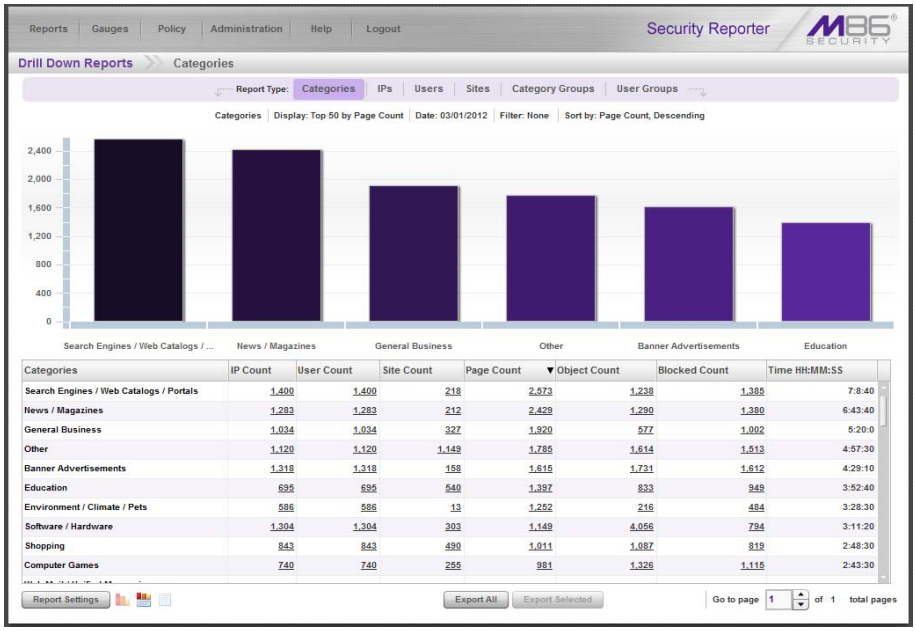
From the navigation menu, go to **Reports > Drill Down Reports > Categories** to display the generated Summary Drill Down Report view, ranking categories in order by the most visited.

Note that tabs for the six Report Types display at the top of the panel. By default, the bar chart beneath these tabs depicts the first six records for the current report type.

***NOTE**: Hovering over a bar in the chart displays the name of the record along with the total count used in that record.*

Beneath the bar chart is a table containing rows of records. Columns of pertinent statistics display for each record.

The bottom portion of the report view panel includes tools for modifying the current report view, exporting or saving the report, and/or scheduling the report to run at a specified time:



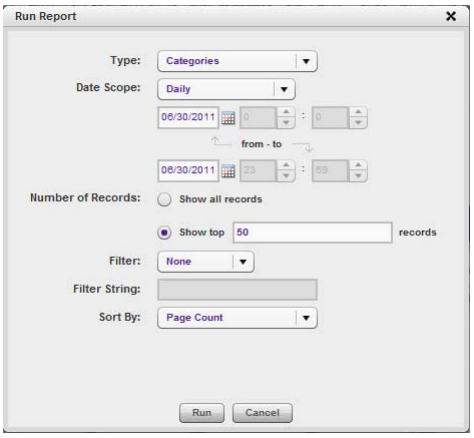
Note that the drill down report view has been generated for today's activity by default.

To continue this investigation using data from yesterday's Summary Report, you must create a new report from this current report view by first changing 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 bottom of the Summary Drill Down Report view, navigate to **Report Settings > Run** to open the Run Report window:



2. By default, "Daily" displays in the **Date Scope** field. Choose "Yesterday" from this menu.
3. Click **Run** to accept your selection and to close the 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 report grouped by two report types

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.*

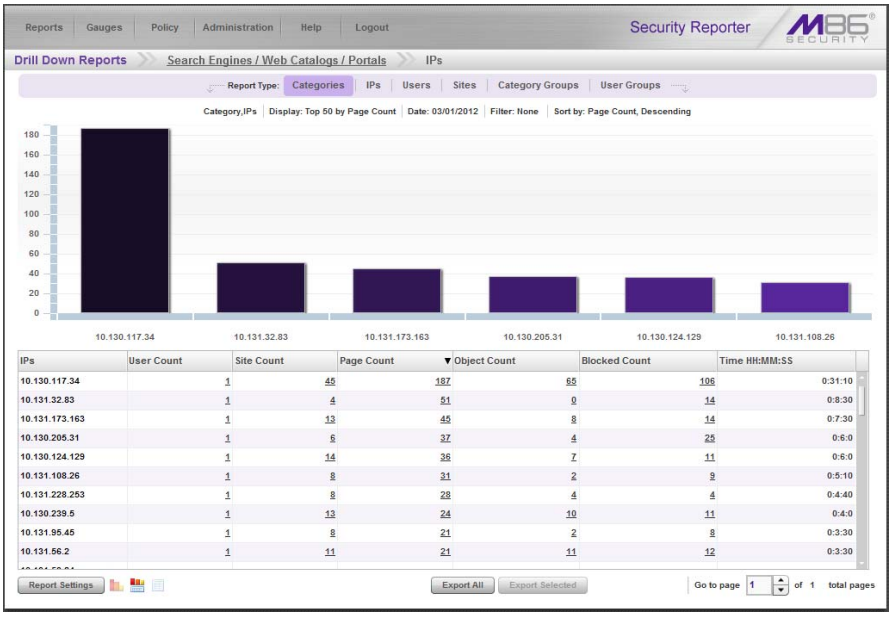
2. Now, to find out who is visiting sites in this category, you will need to identify the user(s).

   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, thereby creating a report view grouped by two report types.

   Note the Count columns to the right of the Categories column, each with click-able links.

***NOTE**: The Bandwidth column displays with GB or MB statistics if using an SWG only with this SR.*

   Click the **IP Count** link corresponding to the targeted category:



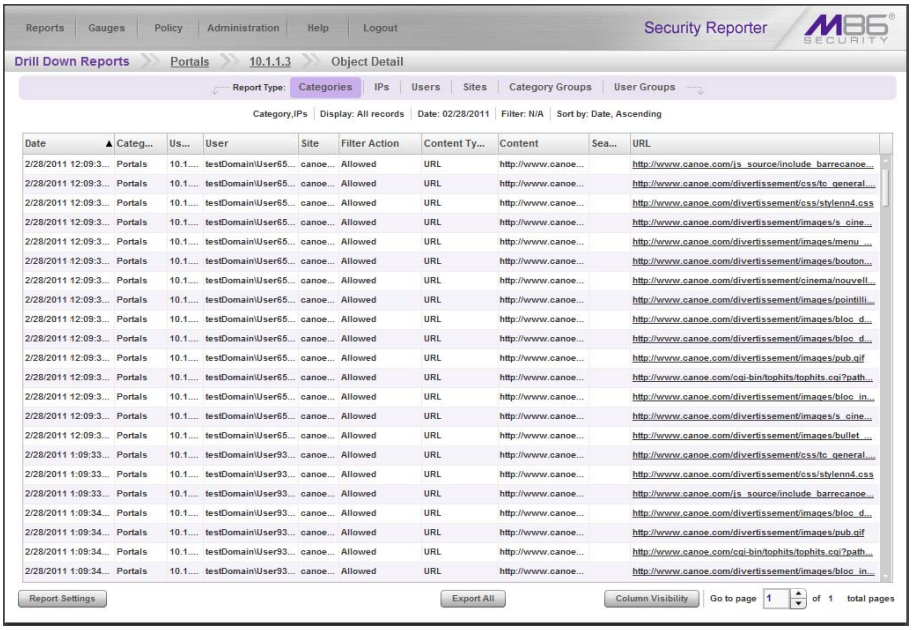
After executing the last command, note that user IP addresses now display in the first column of the report view instead of categories.

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

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 Page Count, Object Count, or Blocked Count link at the far right to show results in the Detail Drill Down Report view that now displays:



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

You have now learned how to access Summary 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 report view grouped by two report types, and drill down into the current summary report view to create a detail report view.

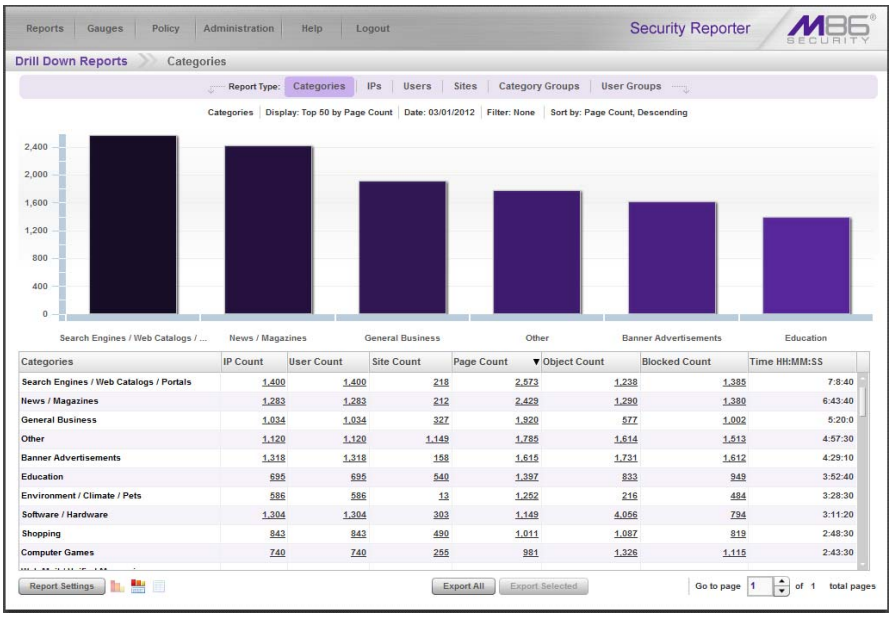
These tools and other tools can be used separately or combined to create many different types of reports to fulfill different purposes.

II. 'Group By' Report and Export Report exercise

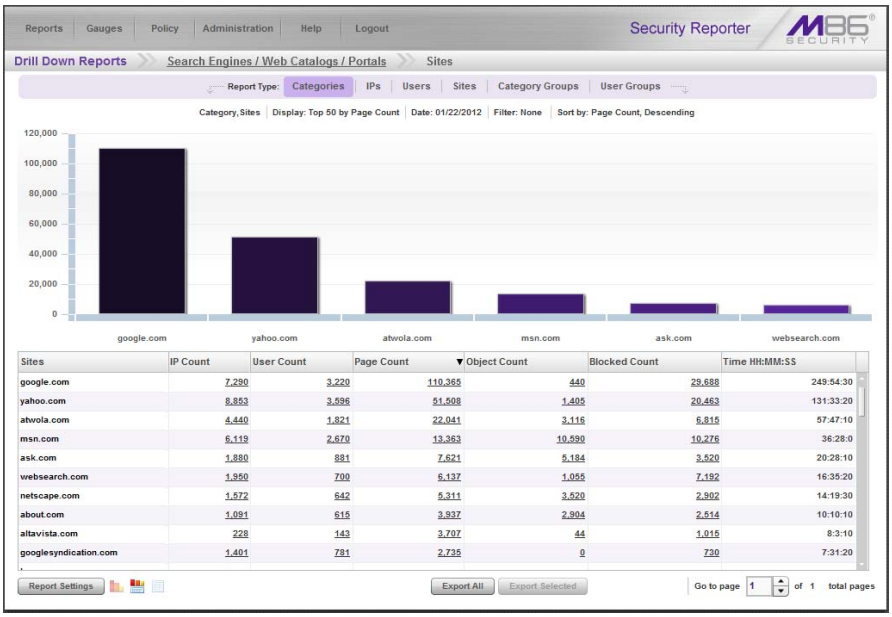
In this exercise you will learn how to display only the top 10 records of a summary drill down 'group by' report view, export that report view in the PDF output format, and then view the results of the generated PDF file.

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

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



2. To find out which sites were visited in a popular category, target the category and then click the **Sites** link corresponding to that category to create a report view grouped by two report types:



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.

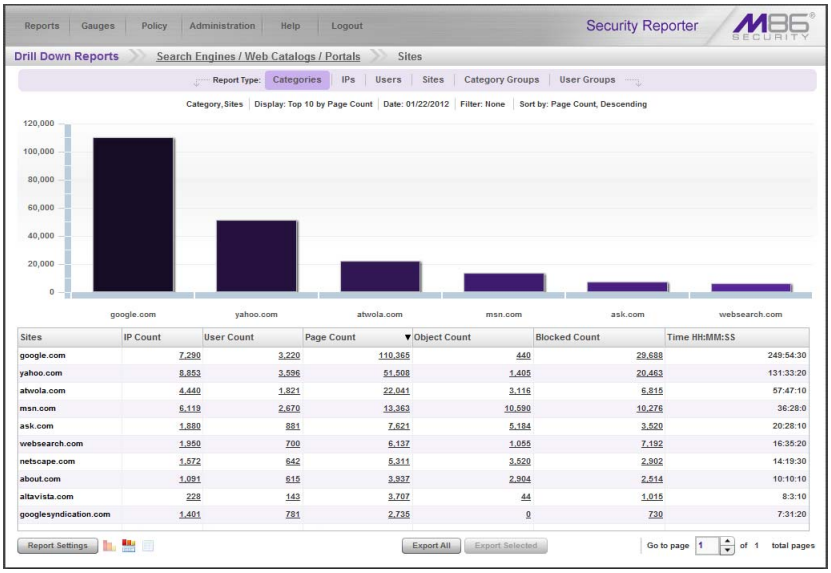
In the Security Reporter User Guide index, see:
- *How to: generate a Drill Down Report*
- *How to: use count columns and links*

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, navigate to **Report Settings > Run** to open the Run Report window in which you make customizations to display in the current report view:

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

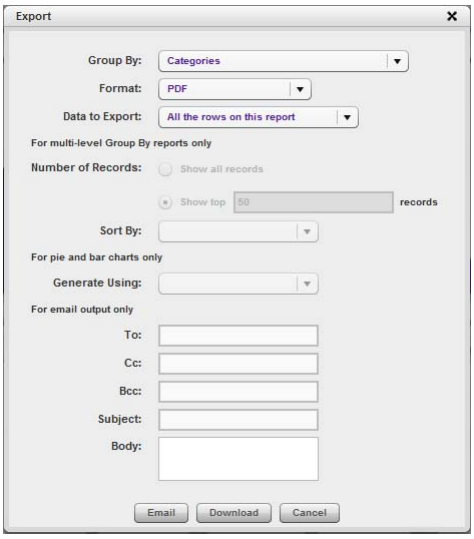
2. At the **Number of Records** field, select "Show top" and and type in ***10*** records.
3. Select **Sort By** "IP Count".
4. Click **Run** to close the window and to display the report view showing only the top 10 site records for the selected category:



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

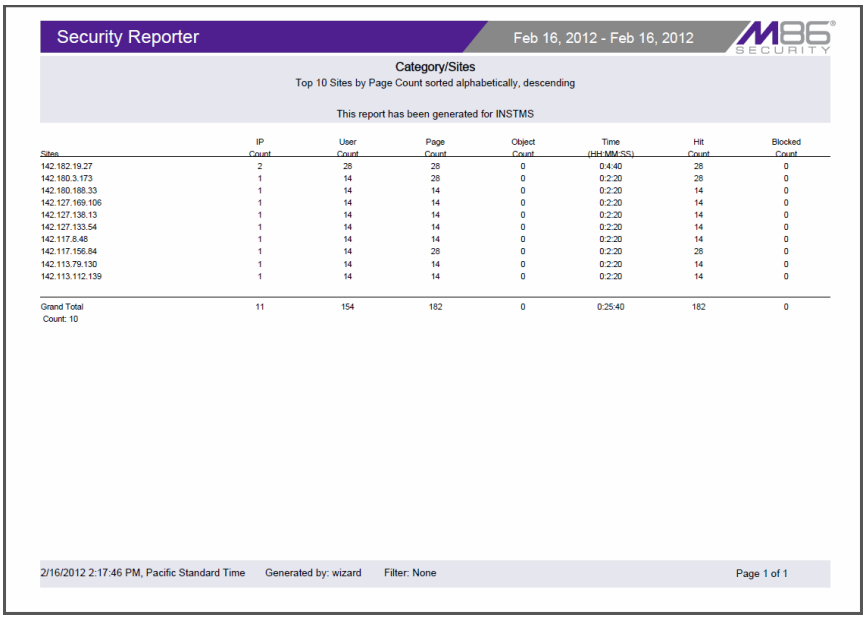
Step C: Export the report view in the PDF output format

1. To export the current report view in the PDF format, at the bottom of the report view click **Export All** to open the Export window:



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

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



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, Bandwidth (if using an SWG only), Page, Object, Time (HH:MM:SS), Hit, and Blocked. The Grand Total and total Count display at the end of the report.

***NOTE**: Notice that the report is sorted by IP Count, the selection made in the Run Report 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 report

See also:
• How to: export a detail report
• How to: email a Drill Down report

You have now learned how to modify a Summary Drill Down Report view grouped by two report types to include only the top 10 records, and then export that content for viewing in the PDF format.

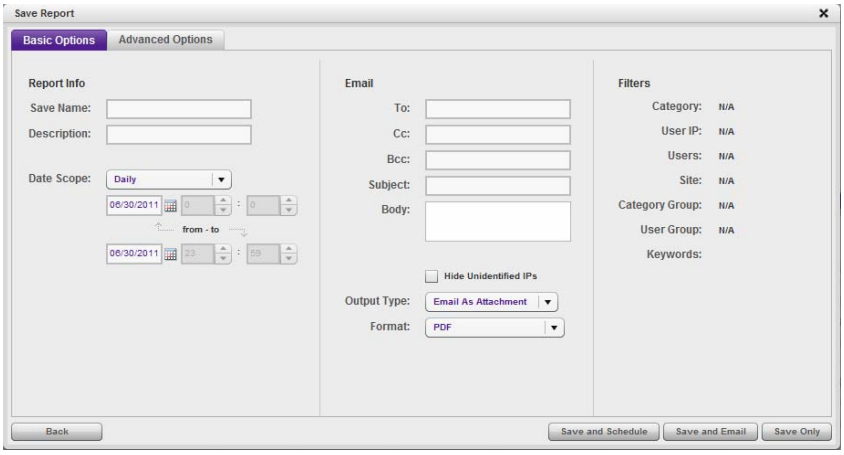
Variations of this exercise can be performed to generate and export countless reports using criteria of your specifications.

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, navigate to **Report Settings >Save** at the bottom of the report view to open the Save Report window:



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

2. For this exercise, make entries in the following fields:
   - Report Info - **Save Name**, **Description**
   - Email **- To**, **Subject**

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 Email** - this option lets you save criteria from the current report view and then email the 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 Reports > Saved Reports, and then choosing the report from the **Reports list**.*

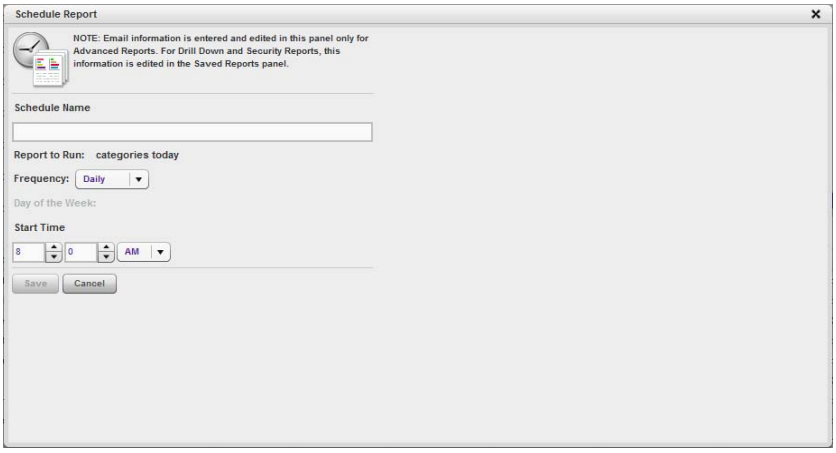
In the Security Reporter User Guide index, see:
• How to: save a Drill Down report

See also:
• How to: use saved Drill Down reports
• How to: edit a saved Drill Down report

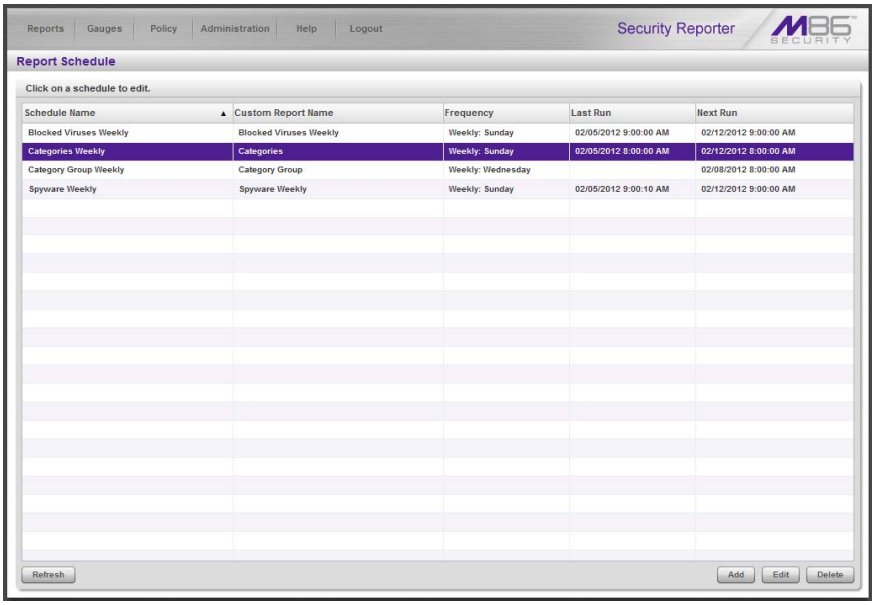
Step B. Schedule a recurring time for the report to run

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 with the message confirming the report was successfully saved.
2. Click **OK** to close this alert box and to display the Schedule Report window:



3. In the Schedule Report window, enter a **Schedule Name**, select the run **Frequency** (Daily, Weekly, Monthly), and specify Day and Start Time criteria.
4. Click **Save** to save your settings and close the window, and to open the alert box with the message confirming the run event was successfully added.
5. Click **OK** to close the alert box and to display the Report Schedule panel with the run event added to the schedule:



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

You have now learned how to save a report and schedule the report to run at a designated time.

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 Custom Category Group, choose **Administration > Custom Category Groups** from the navigation menu.
2. Type in the **Category Group Name** to be used.
3. Specify whether the **Service Type** for reporting is "URL" or "Bandwidth"; if "Bandwidth" is selected, this action affects the Member Categories section below:
   - For a URL Service Type: Choose the Available Categories and click **Add** to include each category in the Assigned Categories list box.
   - For a Bandwidth Service Type: Specify the Port Number(s) and click **Add Port** to include each port in the Assigned Ports list box.
4. Click **Save** to save your settings and to display the name of the group you added in the Custom Category Group list box.

In the Security Reporter User Guide index, see:
• How to: add a Custom Category Group

Step B: Run a report for a specified Custom Category Group

1. To create a report for a Custom Category Group, choose **Reports > Drill Down Reports > Category Groups** from the navigation menu.
2. In the Drill Down Reports > Category Groups report view:
   - For a summary report, click the first column of the custom category group you just added, and then click **Export Selected**.
   - For a detail report, click **Export All**.
3. In the Export window:
   - For a summary report, specify for Data to Export **Only selected rows on this page**, and then click **Download** to generate the report.
   - For a detail report, click **Download** to generate the report.

In the Security Reporter User Guide index, see:
• How to: generate a Custom Category Group report

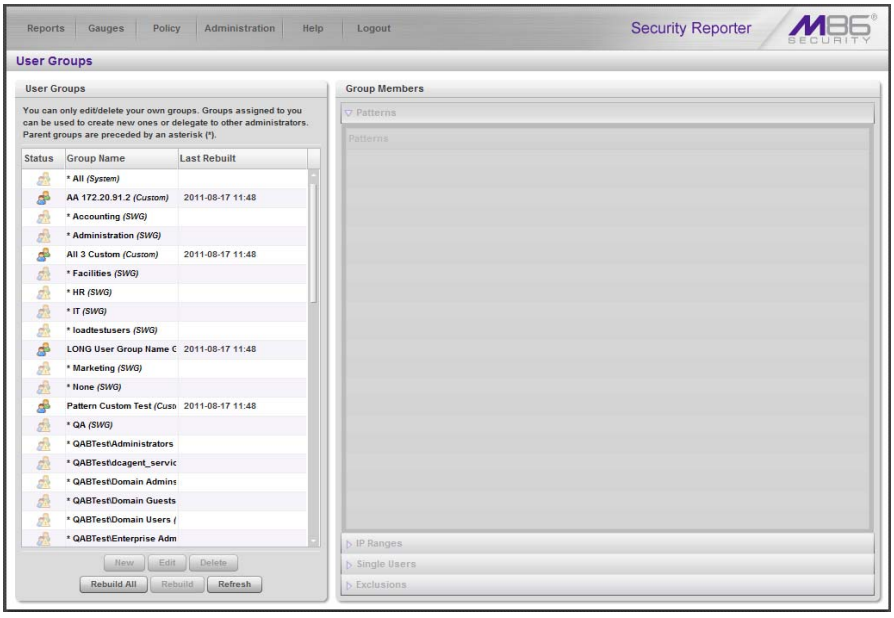
V. Create a custom User Group and generate reports

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.

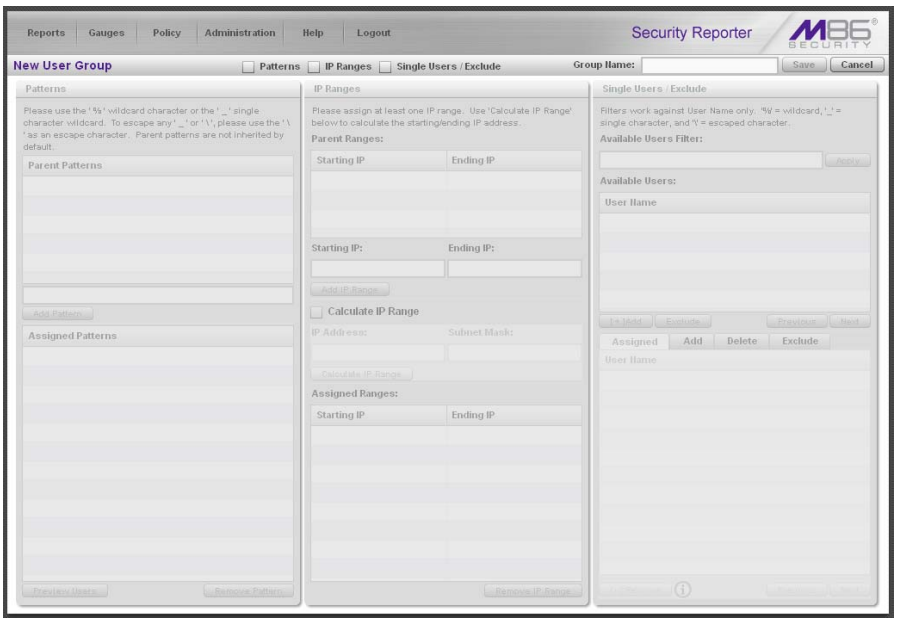
***NOTE**: In order to generate reports for a custom user group, the user group must be created a day in advance, since the list of users is updated each day automatically based on group definitions and latest usage data.*

Step A: Create a custom User Group

1. To create a user group, navigate to **Administration > User Groups**:



2. Choose an existing user group from the User Groups list and then click **New** to display the New User Groups panel:



3. Type in the **Group Name** and check the box(es) corresponding to “Patterns”, “IP Ranges”, and/or “Single Users/Exclude” to activate the section(s) below. For this example, select “IP Ranges”.
4. Specify criteria for the group. In this example, enter an IP address within the range of the parent group.
5. Click **Save** to save your settings and to return to the User Groups panel. Note the group you added now displays in the User Groups list.

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

Step B: Generate a report for a custom User Group

Once the custom User Group is recognized by the SR (on the following day), reports can be generated.

There are two ways to generate a summary or detail report for a custom User Group. You can use the **Reports > Drill Down Reports > Report Wizard** option, or you can use the **Reports > Drill Down Reports > User Groups** option.

- **Report Wizard** - In the Report Wizard panel:

  1. Specify “Summary Report” or “Detail Report”. For a summary report, choose the report **Type** for the results (Categories, IPs, Users, Sites, Category Groups).
  2. Select the User Group name from the “By User Group” accordion, and then click **Run** to generate the report.

  Once the report view displays in the panel, click **Export Selected** for a summary report or **Export All** for a detail report, and then click **Download** to generate the report in the PDF format.

- **Drill Down Reports > User Groups** - In the Drill Down Reports > User Groups panel the list of user groups displays.

  1. For a summary report, select only the user group you wish to use by clicking the first column for that record. For a detail report, select only the user group you wish to use, and then click the **Page Count**, **Object Count**, or **Blocked Count** link.
  2. Once the report view displays in the panel, click **Export Selected** for a summary report or **Export All** for a detail report, and then click **Download** to generate the report in the PDF format.

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

Security Reports Usage Scenarios

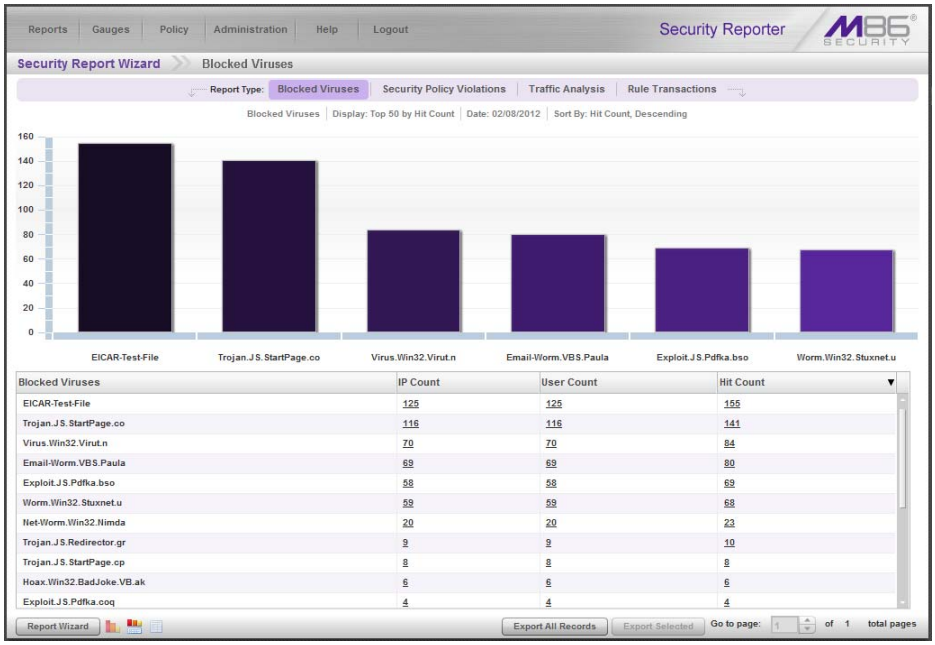
This collection of reporting scenarios is tailored towards familiarizing you with tools for generating, exporting, saving, and scheduling basic security reports. Each scenario is followed by user interface access information. Please consult the "How to" section in the index of the Security Reporter User Guide for pages containing instructions on using the tools and features described in that scenario.

I. Explore the four basic Security Reports types

The four basic security reports are accessible by navigating to **Reports > Security Reports** and selecting the report type from the menu: Blocked Viruses, Security Policy Violations, Traffic Analysis, and Rule Transactions. These reports are also accessible by clicking the tab for the Report Type at the top of a security report panel.

Step A: Navigate to the Blocked Viruses report

Navigate to **Reports > Security Reports > Blocked Viruses** to display the current Blocked Viruses report view:



This report includes details for each instance of each blocked virus detected from end user Internet/network activity.

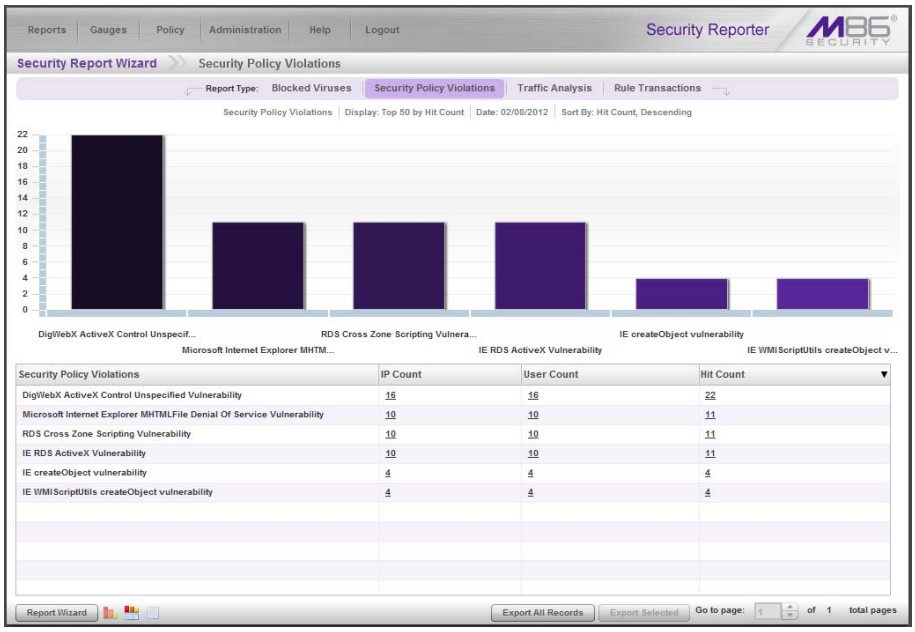
Note the tabs for the four Report Types at the top of the panel. By default, the bar chart beneath these tabs depicts the first six records for the current report type.

***NOTE**: Hovering over a bar in the chart displays the name of the record along with the total hit count or bandwidth used in that record. The Rule Transactions report also includes Actions and Policies information.*

By default, the bottom portion of the report view contains a table that includes rows of records. Columns of pertinent statistics display for each record.

Step B: Navigate to the Security Policy Violations report

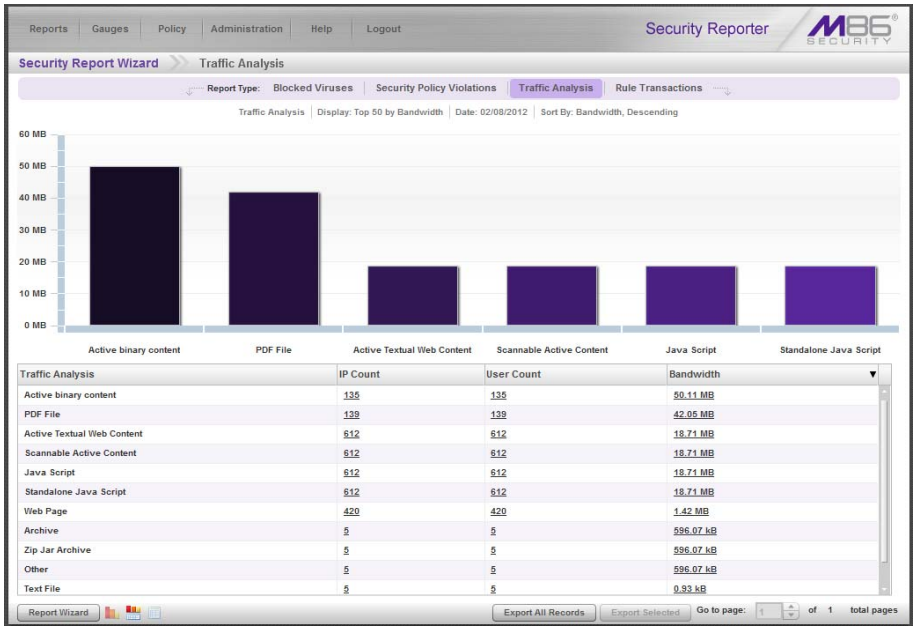
Click the **Security Policy Violations** tab to display the the Security Policy Violations report view:



This report provides information on each instance in which an end user breached a security policy.

Step C: Navigate to the Traffic Analysis report

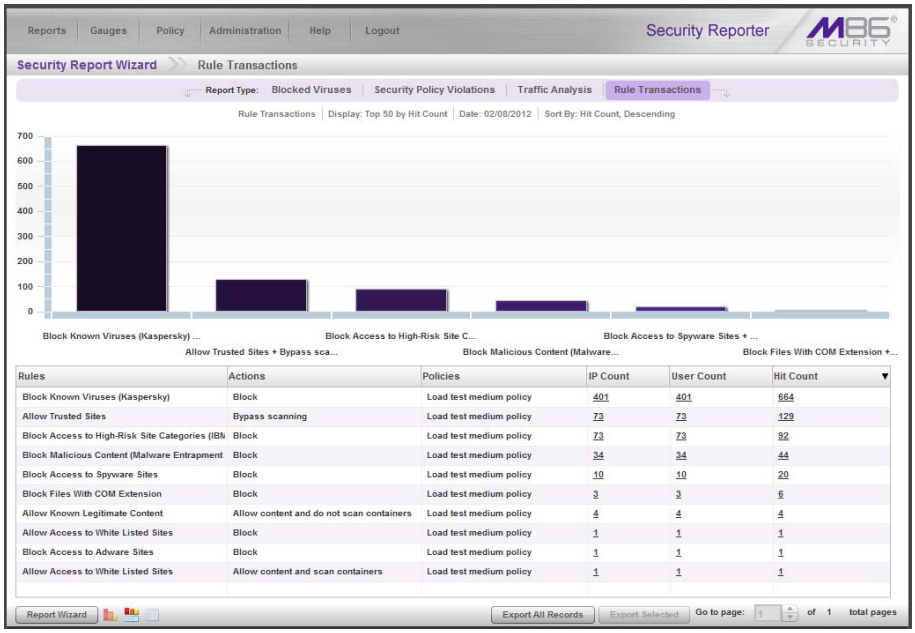
Click the **Traffic Analysis** tab to display the Traffic Analysis report view:



This report shows activity for end user access of objects utilizing an excessive amount of network bandwidth.

Step D: Navigate to the Rule Transactions report

Click the **Rule Transactions** tab to display the Rule Transactions report view:



This report includes each instance in which an end user triggered a threshold in an SWG Security Policy.

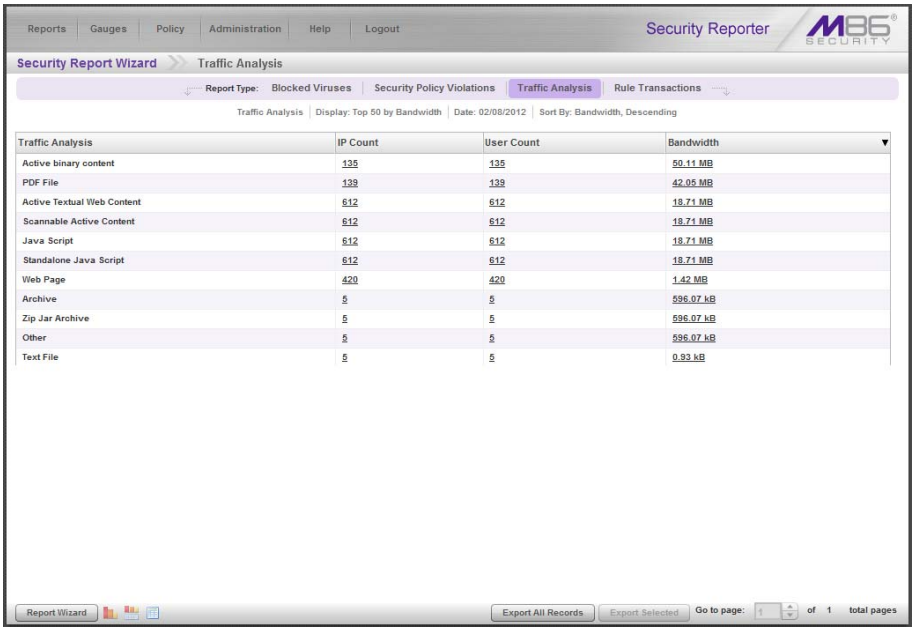
Step E: Modify the current report view

Now that you have viewed the four basic report types, you will learn how to modify the current report view. With a security report view displayed, go to the icons at the bottom left of the panel and do the following:

-  Click this icon to display only the top six bars in the chart:

- Click this icon to re-display the top six graphs and table of records (the default view)

- Click this icon to display the table of records only:



In the Security Reporter User Guide index, see:
• How to: use the four basic Security Report types
• How to: use Security Report tools

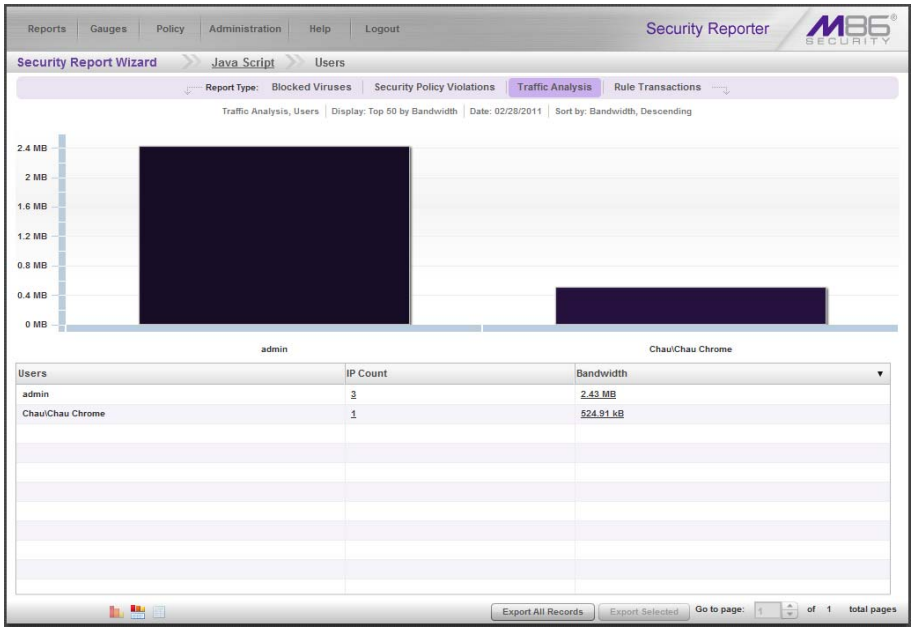
II. Create a drill down Security Report view

As with productivity reports, you can drill down into a security report to obtain more information about a record. In this manner, you can create multi-group reports by drilling down into two or three different columns, or generate a detail report by clicking a Bandwidth or Hit Count column link.

Exercise A: Create a report view that includes two report types

From a basic security report view, click an IP Count or User Count column link for a record to create a report view that includes two report types combined.

The example below shows the result of a Traffic Analysis report view in which the User Count was clicked for the selected record:



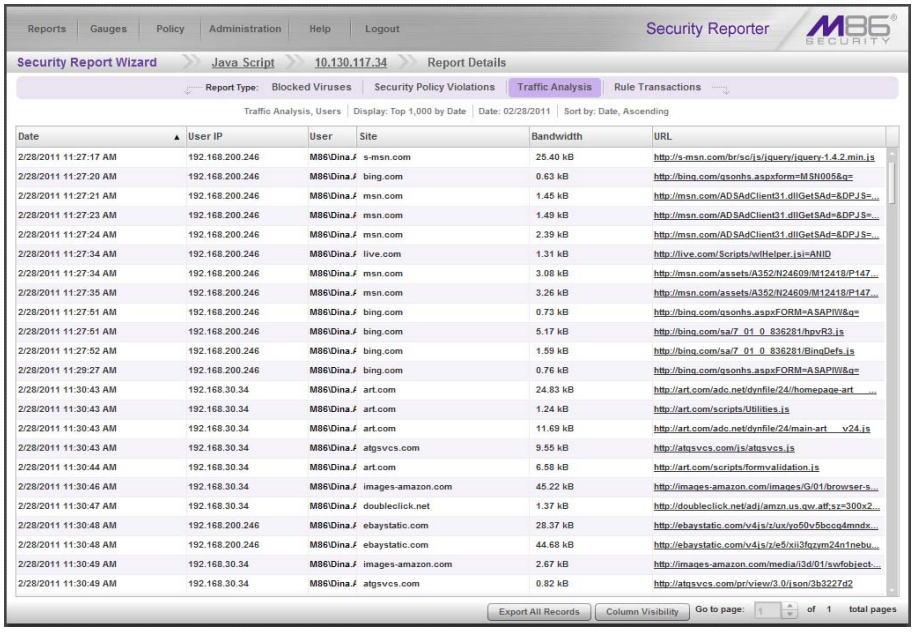
Note that this report view looks similar to a basic security report view, with the following exceptions:

- breadcrumb trail beneath the navigation toolbar shows the path of the current report view
- first column of report view corresponds to the column selection you made to create this report view
- Report Wizard menu options are not available at the bottom left of the panel

***NOTE**: More about Report Wizard menu options are discussed in the following pages in this sub-section.*

Exercise B: Create a detail report view

From the current security report view you created, click the Bandwidth or Hit Count column in a selected record to display the detail report view:



The detail report view shows a table of records with columns for Date, User IP, User name path, Site name, Bandwidth (if clicking a Bandwidth link), and URL.

Note the following buttons are available at the bottom right of the panel:

- **Export All Records** - clicking this button gives you options for exporting records shown in the current report view
- **Column Visibility** - clicking this button gives you options for displaying specified columns in the current report view

---

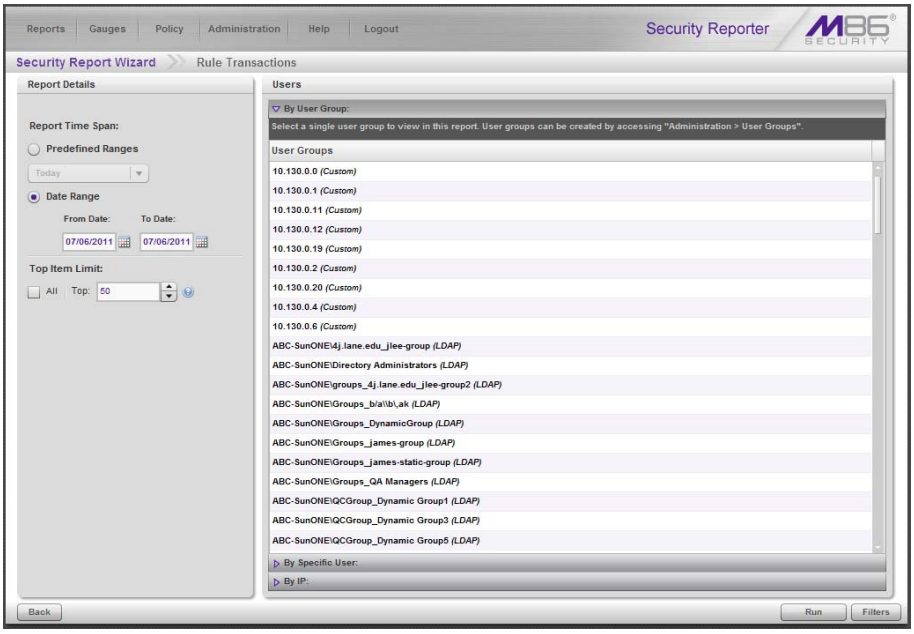
In the Security Reporter User Guide index, see:
• How to: drill down into a Security Report
• How to: use Security Report tools

III. Create a customized Security Report

Once you become familiar with the basic four security reports and their reporting tools, you may want to create your own customized reports. This exercise will show you two different methods for running security reports. One method is by using the **Report Wizard > Run** feature, and the other is by generating a report view using the Report Wizard.

Exercise A: Use the current view to generate a custom report

1. From a basic security report view, go to the bottom left of the panel, hover over **Report Wizard**, and choose **Run** to display the Security Report Wizard panel for that report:



2. In Report Details, specify the **Report Time Span** by choosing one of two options:
   - **Predefined Ranges** - If choosing this option, make a selection from the pull-down menu: “Today” (default), “Month to Date”, “Year to Date”, “Yesterday”, “Month to Yesterday”, “Year to Yesterday”, “Last Week”, “Last Weekend”, “Current Week”, “Last Month”.
   - **Date Range** - This option is selected by default. For this option, use the calendar icons to set the date range.
3. Set the **Top Item Limit** for the report by either specifying the “Top” number of records to be returned in the results, or by choosing “All” records.

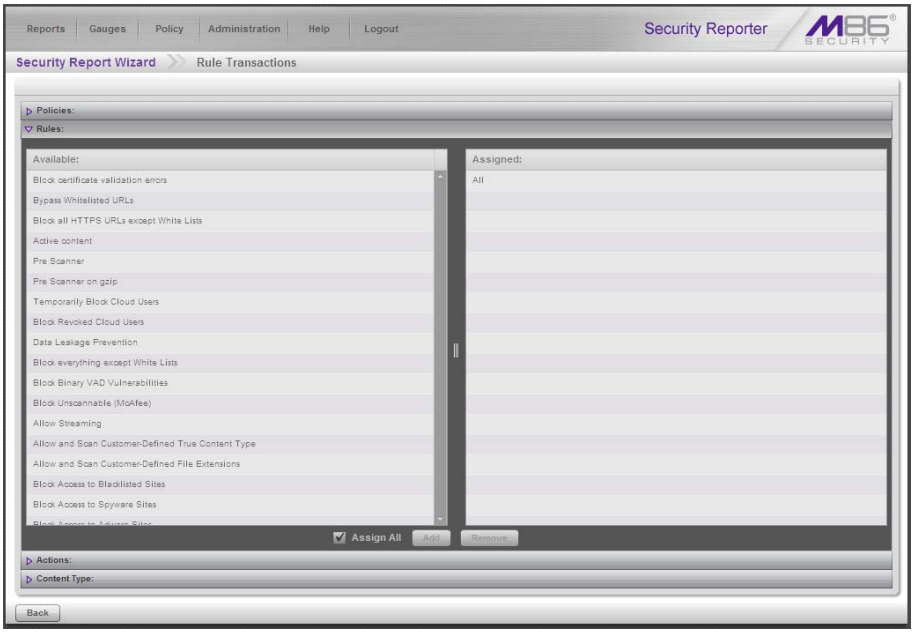
***NOTE**: Choosing “All” records may take a long time for the report to generate, depending on the number of records to be included.*

4. In Users, select one of the accordions and indicate criteria to include in the report to be generated:
   - **By User Group** - If selecting this option, choose the User Group for your report query results.

- **By Specific User** - If selecting this option, enter the end user name—using the '%' wildcard to return multiple usernames—and then click **Preview Users** to display query results in the list box below.
- **By IP** - If selecting this option, enter the end user IP address for filtering your results—using the '%' wildcard to return multiple IP addresses—and then click **Preview Users** to display query results in the list box below.

For a Traffic Analysis or Rule Transactions report, you can narrow your search result by including filters:

a. Click **Filters** at the bottom right of the panel to display the filter results panel:

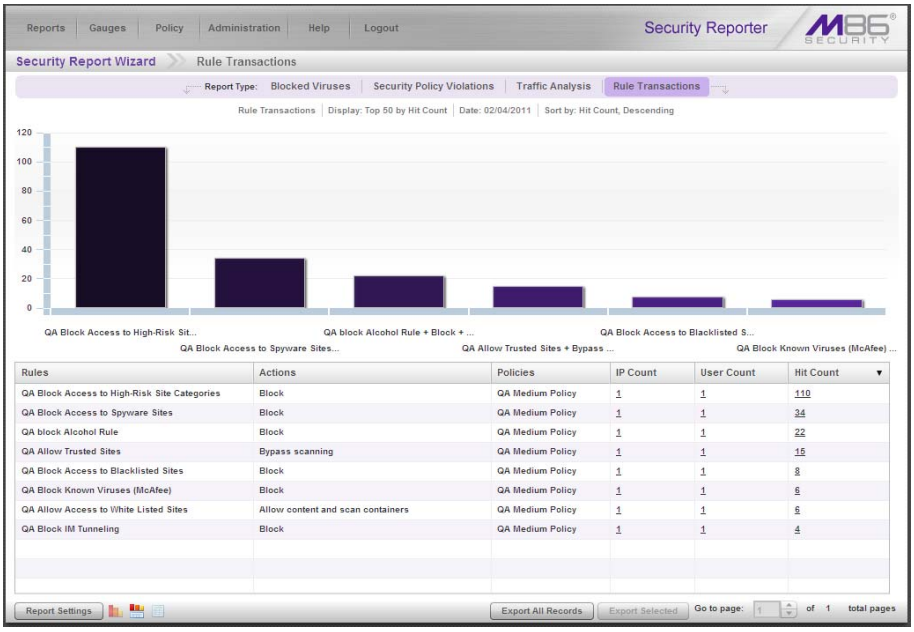


b. Choose a filter type from an available accordion (Policies, Rules, Action, Content Type) and indicate criteria to use in the filter.

By default the "Assign All" checkbox is populated, and the filter panel greyed-out. Uncheck this checkbox to select specific records from the Available list box, and then click **Add** to move the record(s) to the Assigned list box.

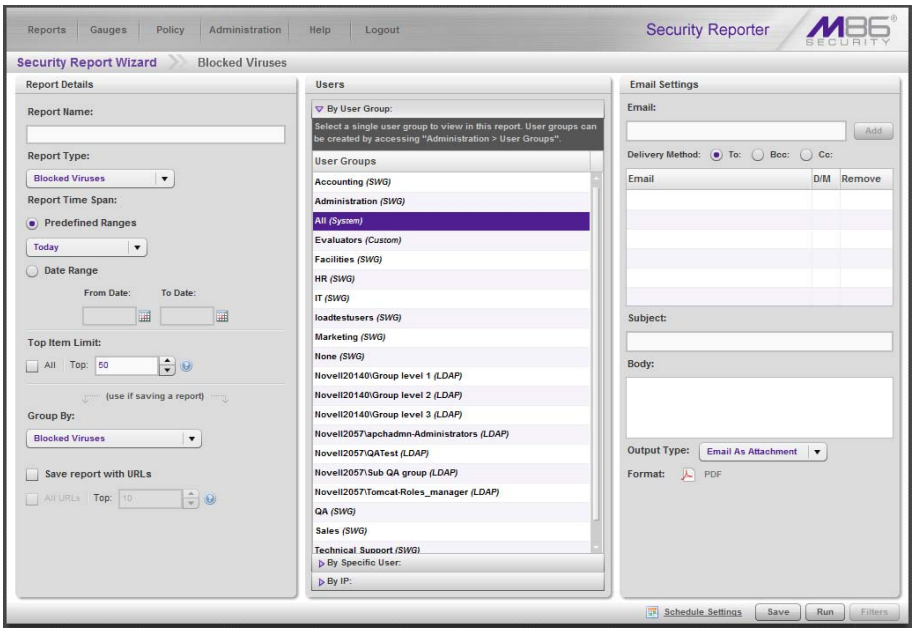
c. Click **Back** to return to the Security Report Wizard panel.

5. Click **Run** to generate the security report view:



Exercise B: Use the Report Wizard to run a custom report

1. Navigate to **Reports > Security Reports > Report Wizard** to display the Security Report Wizard panel where you specify criteria to include in the report you wish to generate:



2. In Report Details, choose the **Report Type** from the pull-down menu (“Blocked Viruses”, “Security Policy Violations”, “Traffic Analysis”, “Rule Transactions”); by default “Blocked Viruses” displays.
3. Specify the **Report Time Span** by choosing one of two options:

- **Predefined Ranges** - If choosing this default option, make a selection from the pull-down menu: “Today” (default), “Month to Date”, “Year to Date”, “Yesterday”, “Month to Yesterday”, “Year to Yesterday”, “Last Week”, “Last Weekend”, “Current Week”, “Last Month”.
- **Date Range** - For this option, use the calendar icons to set the date range.

4. Indicate the **Top Item Limit** to be included in the report. By default, the **Top** number of items specified in “Default Top ‘N’ Value” from Administration > Default Report Settings displays.

***NOTE**: Choosing “All” records may take a long time for the report to generate, depending on the number of records to be included.*

5. Specify the **Group By** selection from available choices in the pull-down menu.
6. By default, **Save report with URLs** is de-selected. Click this checkbox to select this option, and then specify the number of URLs to save:
   - **All URLs** - Check this checkbox to save all URLs
   - **Top** - Specify the number of top URLs to be saved
7. Follow steps 4 - 5 in Exercise A to complete the remaining steps for this exercise.

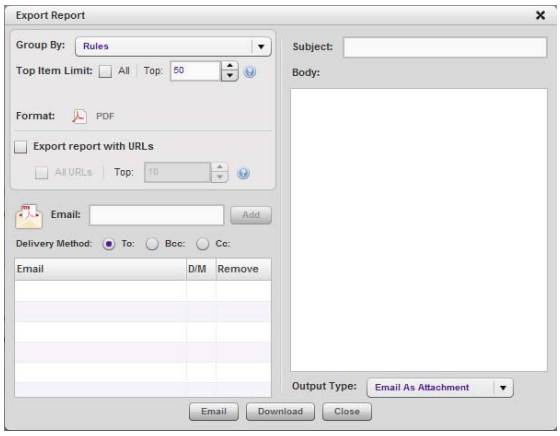
In the Security Reporter User Guide index, see:
• How to: run a Security Report

IV. Export a Security Report

In this exercise you will learn how to export the current basic security report view in the PDF format.

Step A: Specify records to include in the report

With a basic security report generated, go to the bottom right of the panel and either click **Export All Records**, or choose specific records from the table and then click **Export Selected**. Clicking either button opens the Export Report window displaying different options, depending on your export selection:



Export Report window, Export All Records option

Step B: Specify 'Group By' and URL limitation criteria

1. In the Export Report window, specify the **Group By** selection from the available choices in the pull-down menu.
2. At **Top Item Limit**:
   - If the Export All Records option was selected, the **Top** number of items specified in the "Default Top 'N' Value" field from Administration > Default Report Settings displays and can be modified by either editing the displayed value or choosing "All".

***NOTE**: "All" records may take a long time for the report to generate, depending on the number of records to be included.*

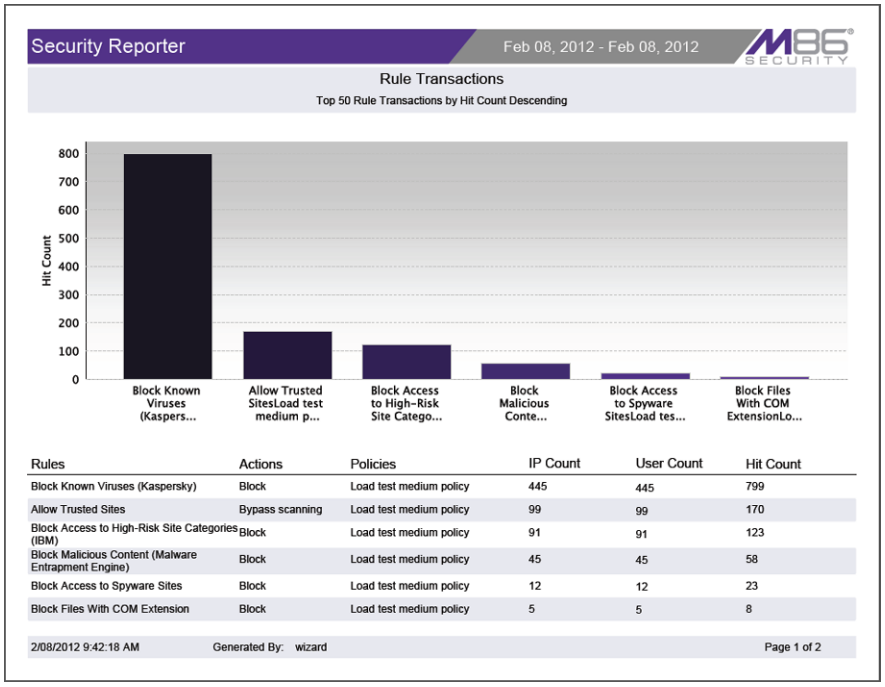
   - If the Export Selected option was selected, "All" is greyed-out. Specify the **Top** number of items to be included in the exported report.
3. By default, **Export report with URLs** is de-selected. Click this checkbox to select this option, and then specify the number of URLs to export:
   - **All URLs** - Check this checkbox to export all URLs
   - **Top** - Specify the number of top URLs to be exported

Step C: Download the report

To download the report in PDF format, click **Download**. The PDF file can be printed, saved, or emailed.

Step D: View the exported Security Report

The generated basic Security Report PDF file includes the following information:

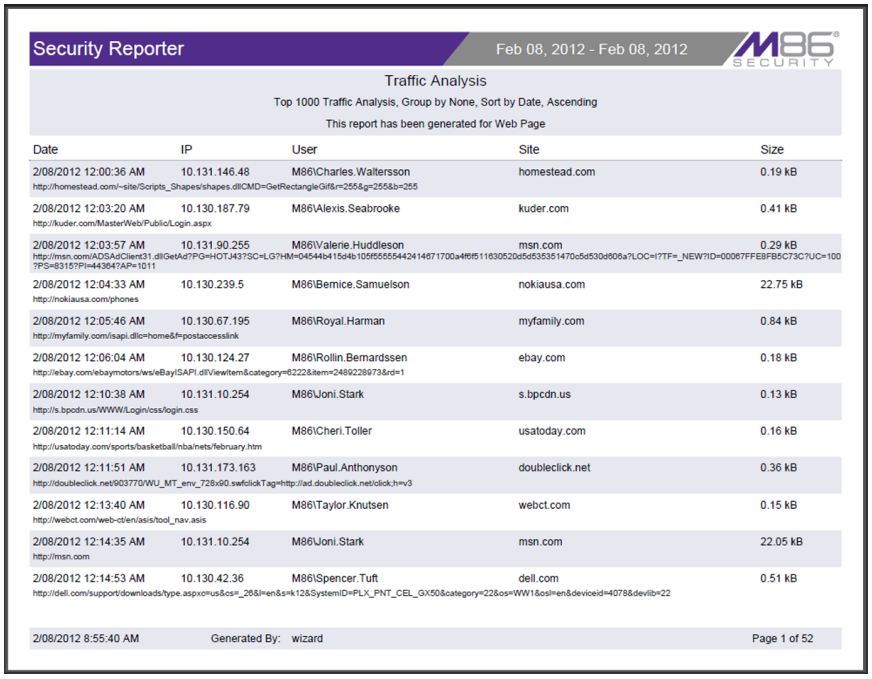


The header of the generated report includes the date range, report type, and report criteria, and report description.

The footer of the report includes the date and time the report was generated (M/D/YY, HH:MM:SS AM/PM), administrator login ID (Generated By), and Page number and page range.

The body of a basic report includes a bar chart showing the top six graphs with count indicators, and the report name. Following the bar chart is a list of records, with the corresponding Item Count for each record. For Rule Transaction reports, Actions and Policies column data precede Item Count column data.

For Bandwidth or Hit Count detail report views, the body of the report includes columns set up to be visible. These columns might include Date (M/DD/YYYY H:MM:SS AM/PM format), IP, User name path, Site, bandwidth Size (e.g. kB), and URL, as in the following sample report:



Security Reporter — Feb 08, 2012 - Feb 08, 2012

Traffic Analysis

Top 1000 Traffic Analysis, Group by None, Sort by Date, Ascending

This report has been generated for Web Page

Date	IP	User	Site	Size
2/08/2012 12:00:36 AM http://homestead.com/~site/Scripts_Shapes/shapes.dll?CMD=GetRectangleGif&r=255&g=255&b=255	10.131.146.48	M86\Charles.Waltersson	homestead.com	0.19 kB
2/08/2012 12:03:20 AM http://kuder.com/MasterWeb/Public/Login.aspx	10.130.187.79	M86\Alexis.Seabrooke	kuder.com	0.41 kB
2/08/2012 12:03:57 AM http://msn.com/ADSAdClient31.dll/GetAd?PG=HOTJ437SC=LG?HM=04544b415d4b105f5555544241467170 0a4f6f511630520d5d53535147 0c5d530d606a?LOC=I?TF=_NEW?ID=00067FFE8FB5C73C?UC=100?PS=8315?PI=44364?AP=1011	10.131.90.255	M86\Valerie.Huddleson	msn.com	0.29 kB
2/08/2012 12:04:33 AM http://nokiausa.com/phones	10.130.239.5	M86\Bernice.Samuelson	nokiausa.com	22.75 kB
2/08/2012 12:05:46 AM http://myfamily.com/isapi.dll/c=home&f=postaccesslink	10.130.67.195	M86\Royal.Harman	myfamily.com	0.84 kB
2/08/2012 12:06:04 AM http://ebay.com/ebaymotors/ws/eBayISAPI.dll?ViewItem&category=6222&item=2489228973&rd=1	10.130.124.27	M86\Rollin.Bernardssen	ebay.com	0.18 kB
2/08/2012 12:10:38 AM http://s.bpcdn.us/WWW/Login/css/login.css	10.131.10.254	M86\Joni.Stark	s.bpcdn.us	0.13 kB
2/08/2012 12:11:14 AM http://usatoday.com/sports/basketball/nba/nets/february.htm	10.130.150.64	M86\Cheri.Toller	usatoday.com	0.16 kB
2/08/2012 12:11:51 AM http://doubleclick.net/903770/WU_MT_env_728x90.swf&clickTag=http://ad.doubleclick.net/click;h=v3	10.131.173.163	M86\Paul.Anthonyson	doubleclick.net	0.36 kB
2/08/2012 12:13:40 AM http://webct.com/web-ct/en/asis/tool_nav.asis	10.130.116.90	M86\Taylor.Knutsen	webct.com	0.15 kB
2/08/2012 12:14:35 AM http://msn.com	10.131.10.254	M86\Joni.Stark	msn.com	22.05 kB
2/08/2012 12:14:53 AM http://dell.com/support/downloads/type.aspx?c=us&cs=_26&l=en&s=k12&SystemID=PLX_PNT_CEL_GX50&category=22&os=WW1&osl=en&deviceid=4078&devlib=22	10.130.42.36	M86\Spencer.Tuft	dell.com	0.51 kB

2/08/2012 8:55:40 AM Generated By: wizard Page 1 of 52

At the end of the report, the Total Items display for all records.

In the Security Reporter User Guide index, see:
• How to: export a Security Report

V. Save a Security Report

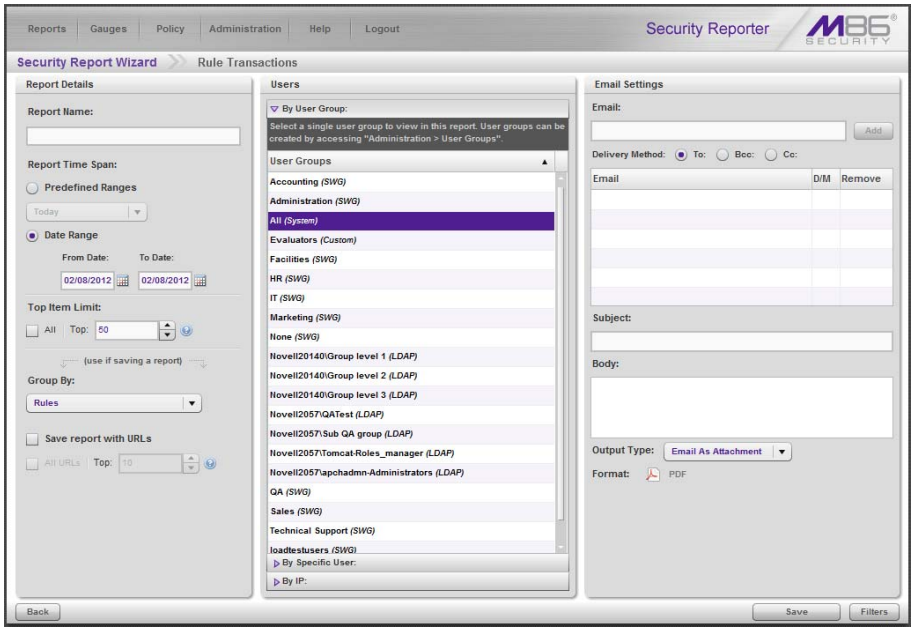
A basic security report is saved by using the Security Report Wizard. The Wizard is accessible by either creating a report view and then selecting **Report Wizard > Save**, or by navigating to **Security Reports > Report Wizard**.

In this exercise, you will save a report view using the **Report Wizard > Save** option.

After saving the report, the report can be edited at any time by going to Saved Reports, as you will see at the end of this exercise.

Step A: Select Report Wizard, Save option

From a basic security report view, navigate to the bottom left of the panel, hover over **Report Wizard**, and choose **Save** to display the Security Report Wizard panel for that report:



Step B: Specify criteria in Report Details

1. In Report Details, type in the **Report Name**.
2. Specify the **Report Time Span** by choosing one of two options:
   - **Predefined Ranges** - If choosing this option, make a selection from the pull-down menu: “Today” (default), “Month to Date”, “Year to Date”, “Yesterday”, “Month to Yesterday”, “Year to Yesterday”, “Last Week”, “Last Weekend”, “Current Week”, “Last Month”.
   - **Date Range** - This option is selected by default. If choosing this option, use the calendar icons to set the date range.
3. Specify the **Group By** selection from available choices in the pull-down menu.
4. Indicate the **Top Item Limit** to be included in the report. By default, the **Top** number of items specified in “Default Top ‘N’ Value” from Administration > Default Report Settings displays.

***NOTE**: Choosing “All” records may take a long time for the report to generate, depending on the number of records to be included.*

5. Specify the **Group By** selection from available choices in the pull-down menu.
6. By default, **Save report with URLs** is de-selected. Click this checkbox to select this option, and then specify the number of URLs to save:
   - **All URLs** - Check this checkbox to save all URLs
   - **Top** - Specify the number of top URLs to be saved

Step C: Select the users or group in Users

In Users, select one of the accordions and indicate criteria to include in the report to be generated:

- **By User Group** - If selecting this option, choose the User Group for your report query results.
- **By Specific User** - If selecting this option, enter the end user name—using the '%' wildcard to return multiple usernames—and then click **Preview Users** to display query results in the list box below.
- **By IP** - If selecting this option, enter the end user IP address for filtering your results—using the '%' wildcard to return multiple IP addresses—and then click **Preview Users** to display query results in the list box below.

For a Traffic Analysis or Rule Transactions report, you can narrow your search result by including filters:

1. Click **Filters** at the bottom right of the panel to display the filter results panel.
2. Choose a filter type from an available accordion (Policies, Rules, Action, Content Type) and indicate criteria to use in the filter.

   By default the "Assign All" checkbox is populated, and the filter panel greyed-out. Uncheck this checkbox to select specific records from the Available list box, and then click **Add** to move the record(s) to the Assigned list box.
3. Click **Back** to return to the Security Report Wizard panel.

Step D: Populate Email Settings

1. In Email Settings, enter at least one **Email** address and then click **Add** to include the email address in the list box below.
2. Specify the **Delivery Method** for the email address: "To" (default), "Bcc", or "Cc".
3. Type in the **Subject** for the email message.
4. If you wish, enter text to be included in the **Body** of the message.
5. Specify the **Output Type** for the email: "Email As Attachment" or "Email As Link".

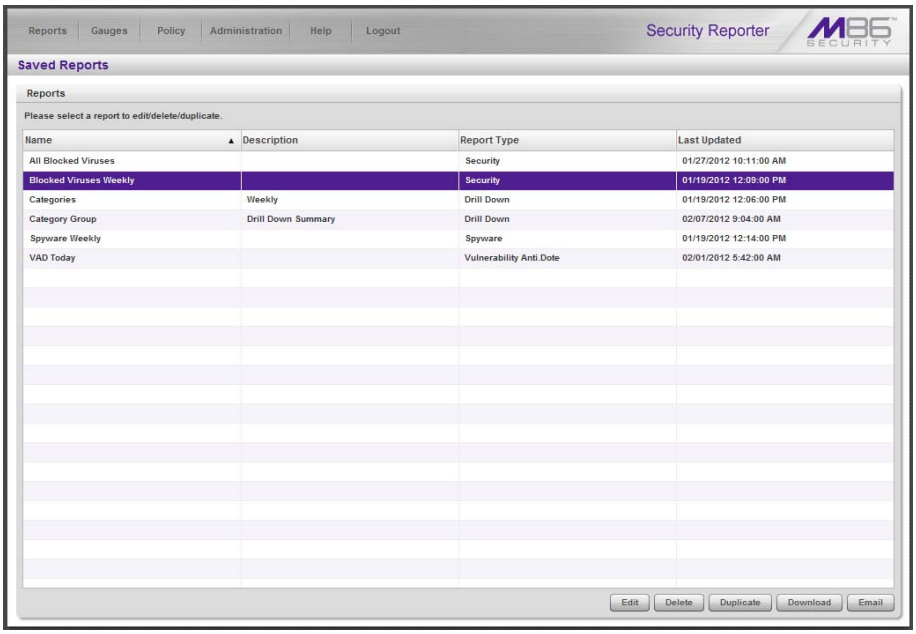
Step E: Save the report

Click **Save** at the bottom of the Security Report Wizard panel to save your settings and to add the report to the Saved Reports panel.

Access the Saved Reports panel

A saved security report can be edited any time as follows:

1. Navigate to **Reports > Saved Reports**.
2. Select the report name from the list:



3. Click **Edit** to go to the Security Report Wizard panel where the report can be updated and saved.

In the Security Reporter User Guide index, see:
- *How to: save a Security Report*
- *How to: edit a saved Security Report*

VI. Schedule a Security Report to run

A basic security report is scheduled to run by using either the Schedule Settings window in the Security Report Wizard, or the Report Schedule panel.

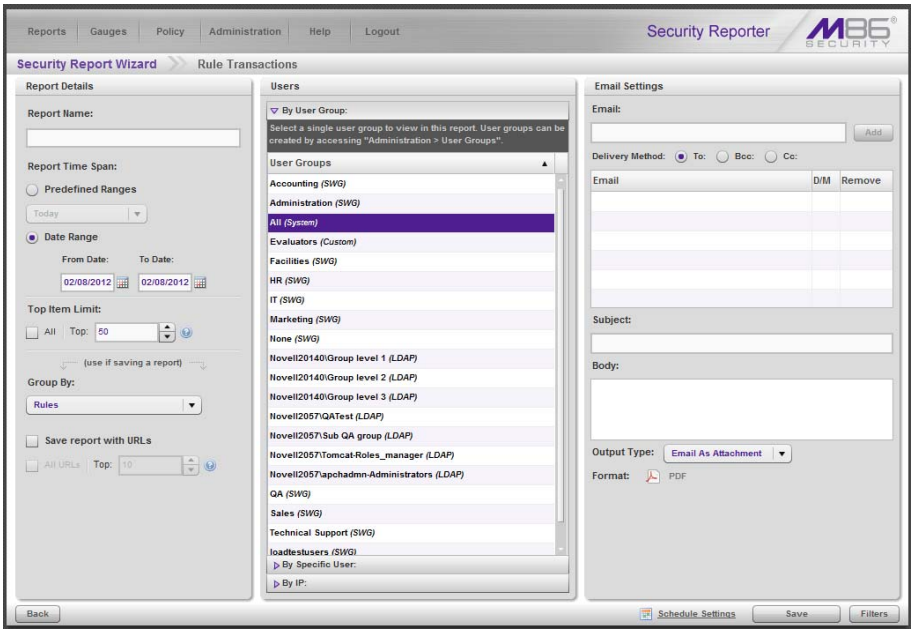
The Schedule Settings window is accessible via **Report Wizard > Schedule** or **Security Reports > Report Wizard**, and the Report Schedule panel is accessible by navigating to **Reports > Report Schedule**.

In this exercise, you will use the **Report Wizard > Schedule** option to save several steps, since the panel will be pre-populated with data from the current report view.

After scheduling the report to run, the report can be edited at any time by going to Report Schedule, as you will see at the end of this exercise.

Exercise A: Use the current view to schedule a report to run

1. In the current security report view, hover over **Report Wizard** and choose **Schedule** to display the Security Report Wizard panel for that report:



2. In Report Details, type in the **Report Name**.
3. Specify the **Report Time Span** by choosing one of two options:
   - **Predefined Ranges** - If choosing this option, make a selection from the pull-down menu: “Today” (default), “Month to Date”, “Year to Date”, “Yesterday”, “Month to Yesterday”, “Year to Yesterday”, “Last Week”, “Last Weekend”, “Current Week”, “Last Month”.
   - **Date Range** - This option is selected by default. For this option, use the calendar icons to set the date range.
4. Indicate the **Top Item Limit** to be included in the report. By default, the **Top** number of items specified in “Default Top ‘N’ Value” from Administration > Default Report Settings displays.

***NOTE**: Choosing “All” records may take a long time for the report to generate, depending on the number of records to be included.*

5. Specify the **Group By** selection from available choices in the pull-down menu.
6. By default, **Save report with URLs** is de-selected. Click this checkbox to select this option, and then specify the number of URLs to save:
   - **All URLs** - Check this checkbox to save all URLs
   - **Top** - Specify the number of top URLs to be saved
7. In Users, select one of the accordions and indicate criteria to include in the report to be generated:
   - **By User Group** - If selecting this option, choose the User Group for your report query results.
   - **By Specific User** - If selecting this option, enter the end user name—using the '%' wildcard to return multiple usernames—and then click **Preview Users** to display query results in the list box below.
   - **By IP** - If selecting this option, enter the end user IP address for filtering your results—using the '%' wildcard to return multiple IP addresses—and then click **Preview Users** to display query results in the list box below.

   For a Traffic Analysis or Rule Transactions report, you can narrow your search result by including filters:

   a. Click **Filters** at the bottom right of the panel to display the filter results panel.

   b. Choose a filter type from an available accordion (Policies, Rules, Action, Content Type) and indicate criteria to use in the filter.

   By default the "Assign All" checkbox is populated, and the filter panel greyed-out. Uncheck this checkbox to select specific records from the Available list box, and then click **Add** to move the record(s) to the Assigned list box.

   c. Click **Back** to return to the Security Report Wizard panel.
8. In Email Settings:

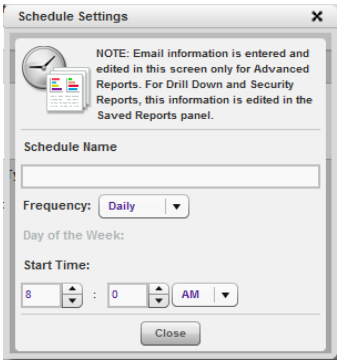
   a. Enter at least one **Email** address and then click **Add** to include the email address in the list box below.

   b. Specify the **Delivery Method** for the email address: "To" (default), "Bcc", or "Cc".

   c. Type in the **Subject** for the email message.

   d. If you wish, enter text to be included in the **Body** of the message.

   e. Specify the **Output Type** for the email: "Email As Attachment" or "Email As Link".
9. Go to the lower right corner of the panel and click **Schedule Settings** to open the Schedule Settings window:



a. Enter a **Schedule Name**.

b. Select the **Frequency** to run the report from the pull-down menu (Daily, Weekly, or Monthly).

If Weekly, specify the **Day of the Week** from the pull-down menu (Sunday - Saturday).

If Monthly, specify the **Day of the Month** from the pull-down menu (1 - 31).

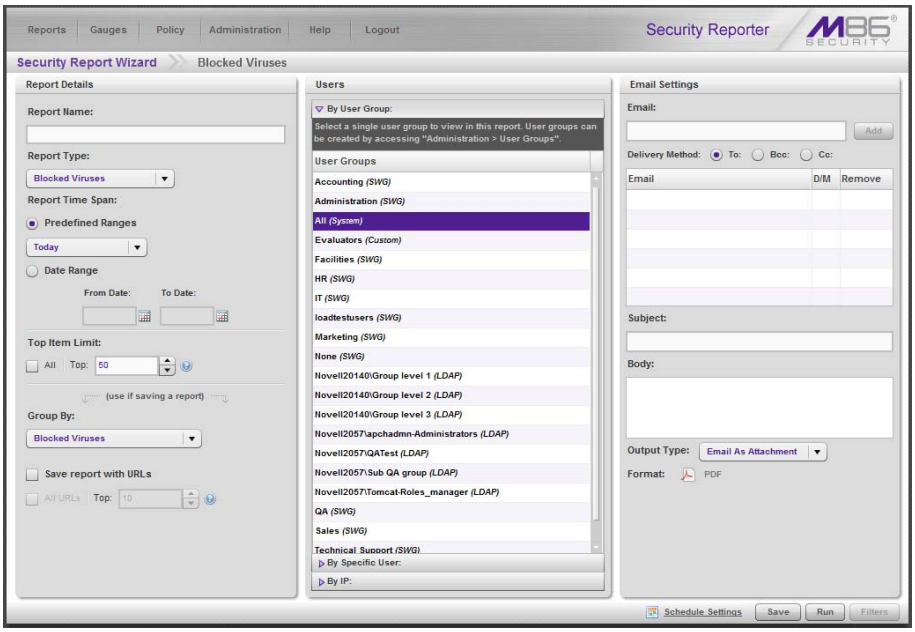
c. Select the **Start Time** for the report: 1 - 12 for the hour, 0 - 59 for the minutes, and AM or PM.

d. Click **Close** to save your settings and close the window.

10. Click **Save** at the bottom of the Security Report Wizard panel to save your settings and to add the report to the schedule to be run.

Exercise B: Use the Wizard to create and schedule reports

1. Navigate to **Reports > Security Reports > Report Wizard** to open the Security Report Wizard panel:

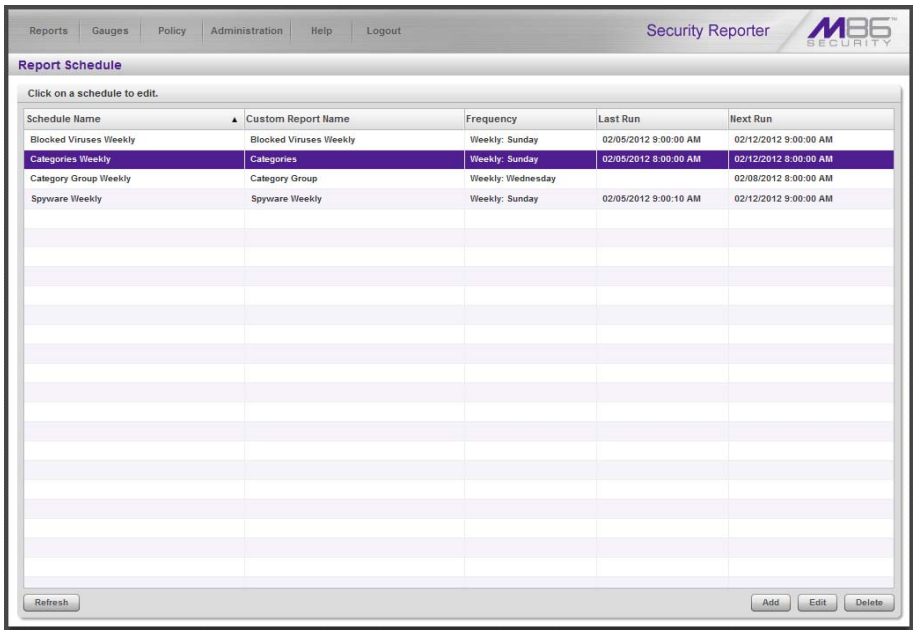


2. In Report Details, type in the **Report Name**.

3. Choose the **Report Type** from the pull-down menu (“Blocked Viruses”, “Security Policy Violations”, “Traffic Analysis”, “Rule Transactions”); by default “Blocked Viruses” displays.
4. Specify the **Report Time Span** by choosing one of two options:
   - **Predefined Ranges** - This option is selected by default. For this option, make a selection from the pull-down menu: “Today” (default), “Month to Date”, “Year to Date”, “Yesterday”, “Month to Yesterday”, “Year to Yesterday”, “Last Week”, “Last Weekend”, “Current Week”, “Last Month”.
   - **Date Range** - If choosing this option, use the calendar icons to set the date range.
5. Follow steps 4 - 10 for Exercise A in this section to complete the remainder of this exercise.

Access the Report Schedule panel

To access the Report Schedule panel that includes all reports scheduled to run—both productivity and security reports—navigate to **Reports > Report Schedule**:



Reports scheduled to be run display as rows of records. The following information is included for each record: Schedule Name, Custom Report Name, Frequency for running the report, and Last Run and Next Run date and time.

The schedule for the report can be edited or deleted, or a new schedule for a report added here.

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

Real Time Reports Usage Scenarios

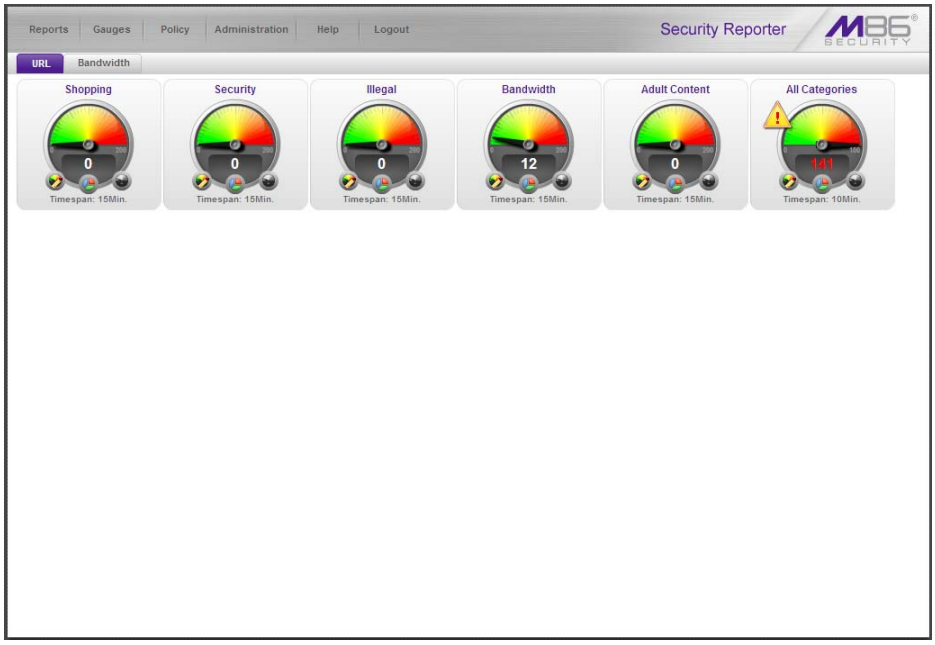
This collection of setup and usage scenarios is designed to help you understand and use basic tools in the console for enforcing your Internet usage policy. Each scenario is followed by console setup information. Please consult the “How to” section in the index of the Security Reporter User Guide for 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 Gauges Dashboard displays by default when you select Gauges in the navigation toolbar:



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:

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

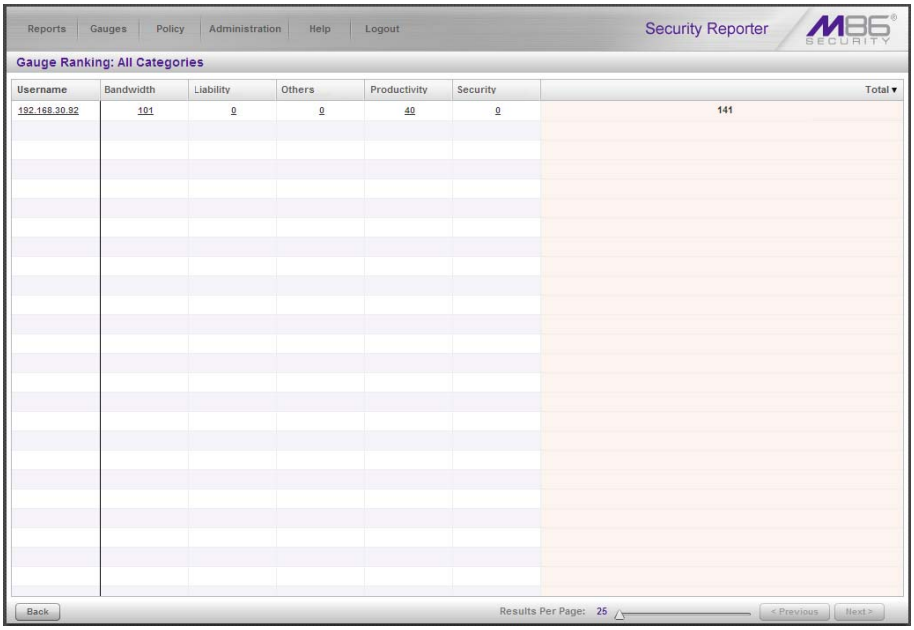
In the Security Reporter User Guide index, see:
• How to: use Gauges and Policy menu selections

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.

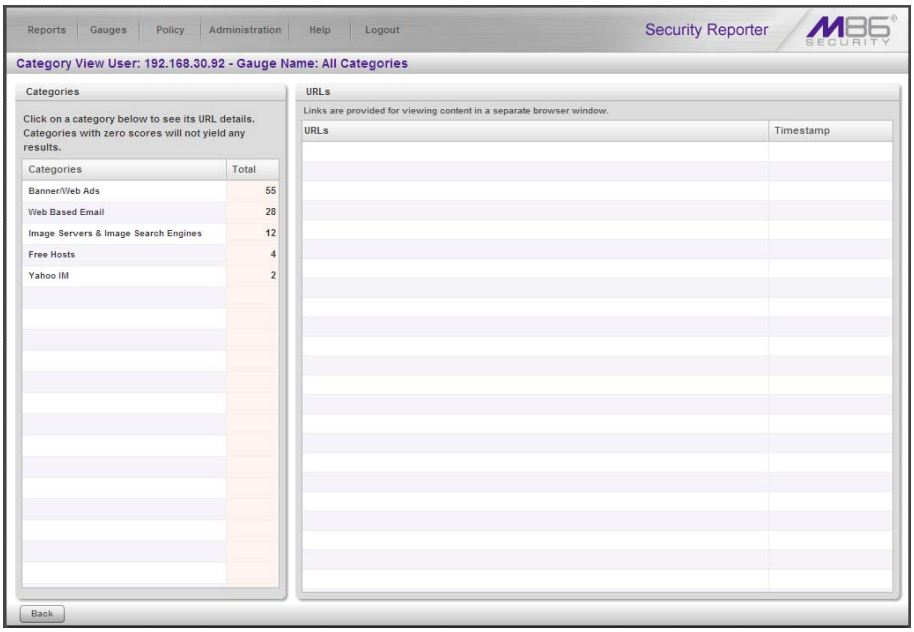
Step A: Select the gauge with the highest score

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 library categories that comprise the gauge, and rows of end user records with activity in one or more of these library categories:



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

2. Find the library category with the highest score, and click that score to open the Category View User panel:



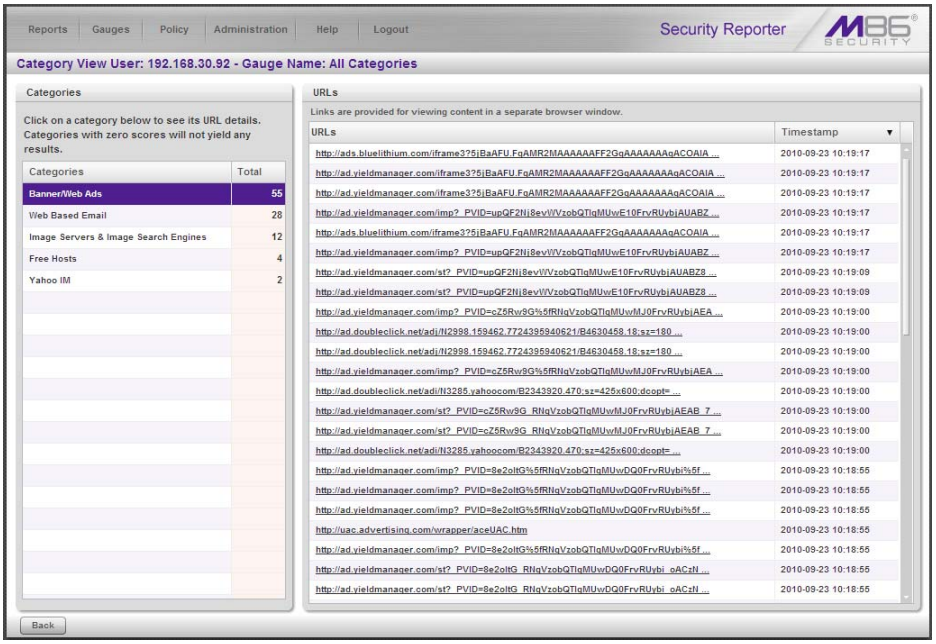
Note the left side of this panel is populated with rows of records for Categories affected by the selected end user.

Now that you've identified the user affecting the highest scoring gauge, next you will investigate the activity of the user driving that 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 high-scoring library category, select the category with the highest score and then click it to display a list of URLs the user visited in the right side of this panel:



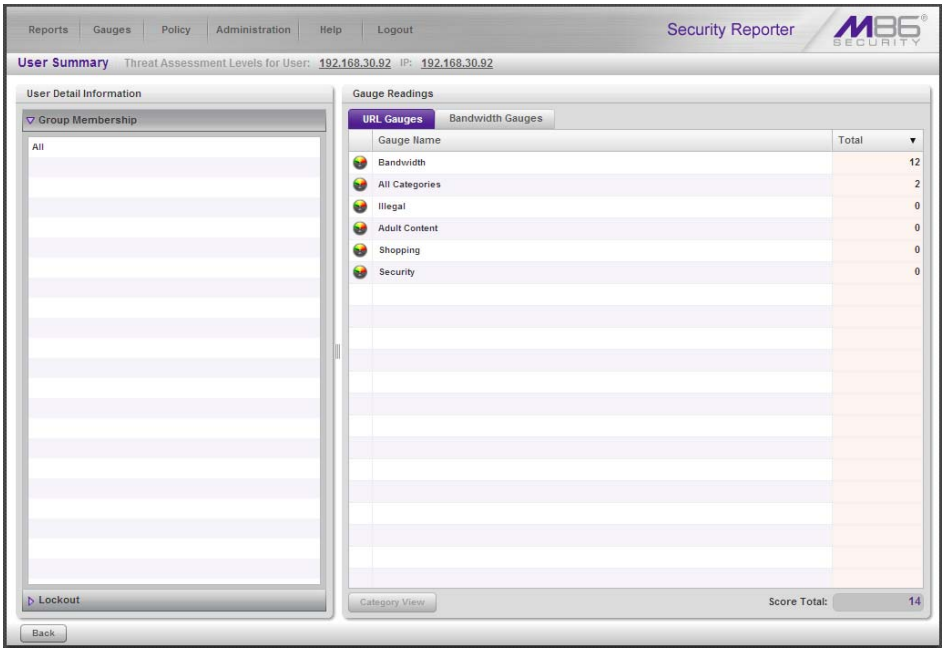
2. Choose a URL you wish to view, and then click it to open a separate browser window accessing that URL.

   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

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

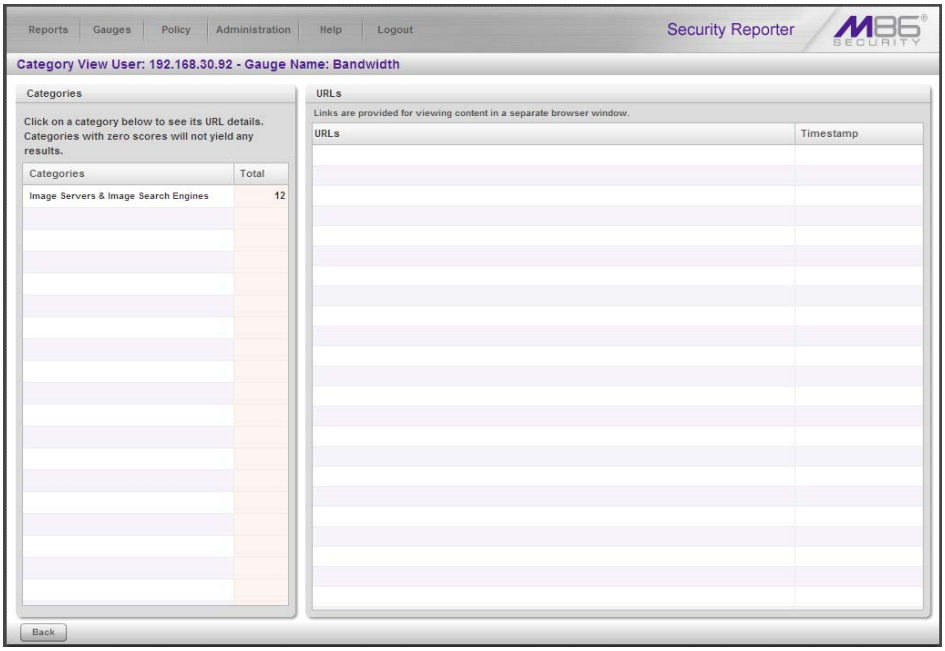
1. To find out which other gauges the same user is currently affecting, return to the Gauge Ranking table by going to the lower left corner of the Category View User panel and clicking the **Back** button. In the Username column, click that user's link to display the User Summary panel for that user:



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

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

3. Click **Category View** to display the Category View User panel:



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.

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.

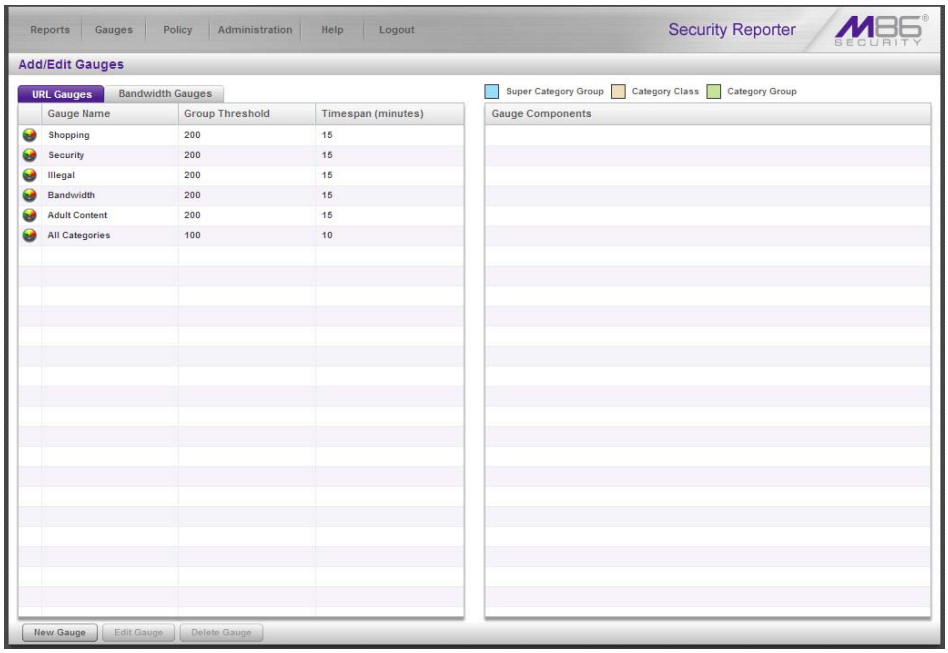
When you become accustomed to using the gauges on a regular basis to conduct these types of investigations, you will eventually want to explore other tools in the interface to restrict or lock out offending users from accessing certain library categories.

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:



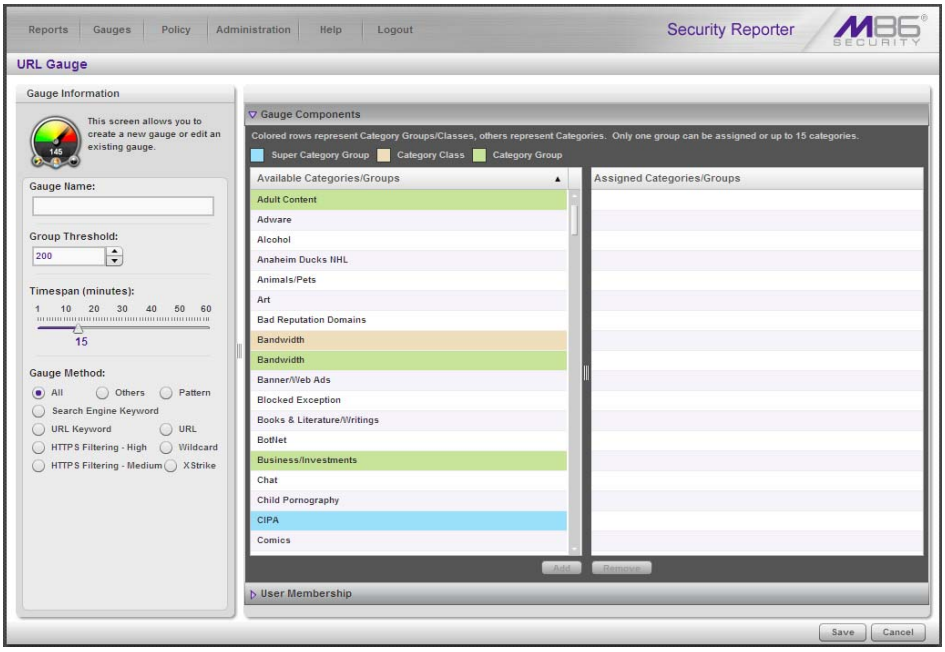
Note that this panel contains the current Gauge Name list at the left side.

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:



2. In Gauge Information 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.

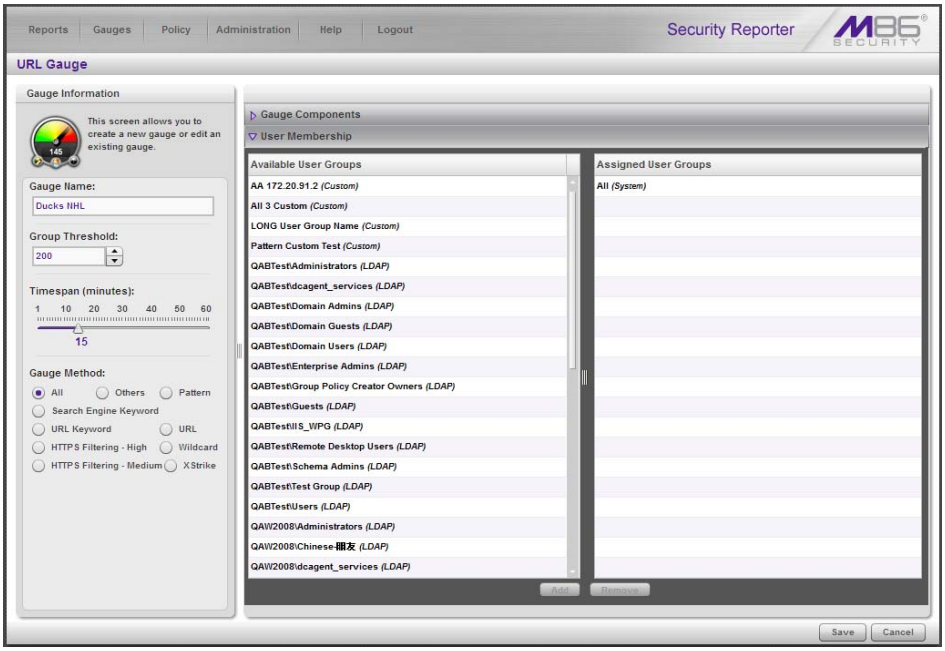
   b. **Group Threshold** for the ceiling of gauge activity. For this exercise we will use the default and recommended value, which is 200 for a URL gauge.

   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.

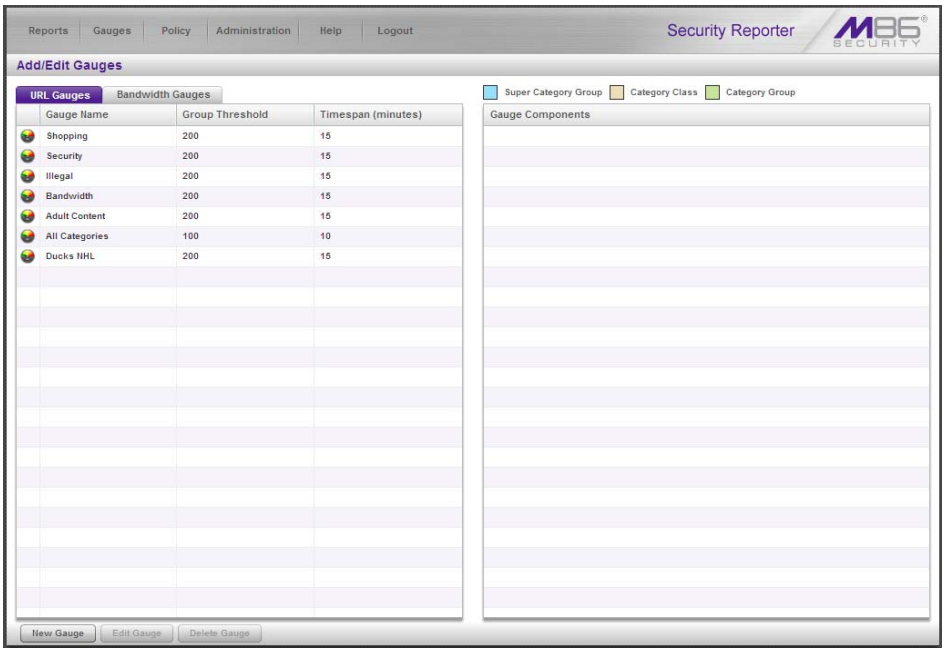
   d. **Gauge Method** to be used for tracking gauge activity. For this exercise we will use the default “All” gauge method, so you do not need to make any selection from the drop-down menu. The selected “All” method considers all methods users can use to access URLs in library categories included in the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

3. In the Available Categories/Groups list to the right, select one Category 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 Categories/Groups list box.

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



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



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

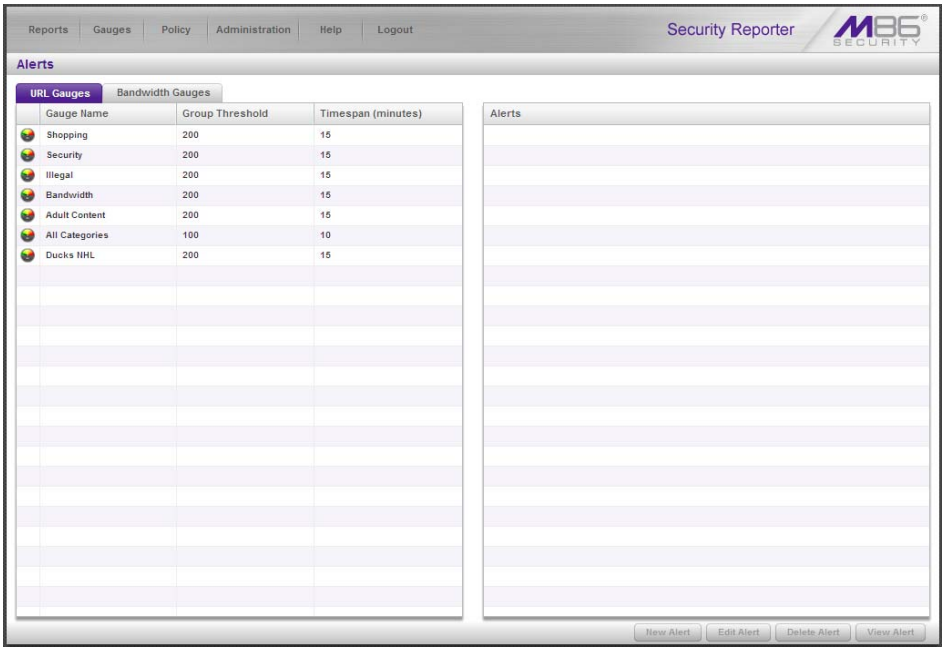
Now that you know the basics of creating a gauge, you will soon be able to create and use gauges to monitor various groups of users who frequent URLs in library categories you wish to restrict, and deal in real time with Internet usage issues that endanger your network and/or consume an excessive amount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

IV. Create an email alert exercise

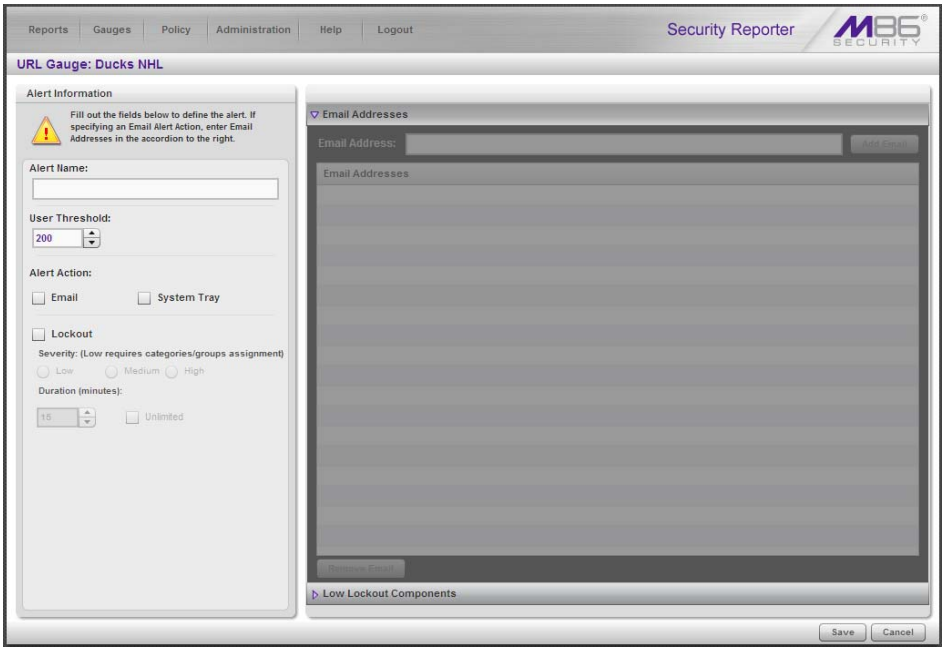
This exercise will teach you how to set up an email alert so you will be notified when a gauge reaches the high end of its established threshold.

Step A: Add a new alert

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



2. Select the gauge for which an alert will be created; this action activates the New Alert button.
3. Click **New Alert** to open a panel that displays Alert Information to the left and the greyed-out target panel to the right containing the Email Addresses and Low Lockout Components accordions:



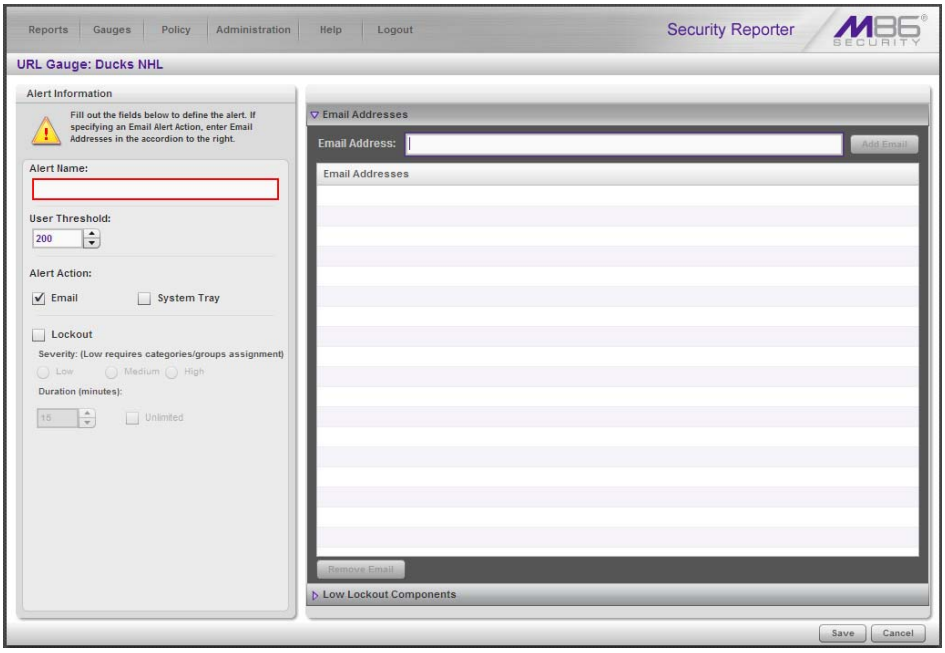
4. Type in the **Alert Name** to be used for the alert that will be delivered to the group administrator.
5. Specify the **User Threshold** ceiling of gauge activity that will trigger the alert. The default and recommended value is 200 for a URL gauge.
6. Specify the **Alert Action** method(s) to be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

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



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

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

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

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

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

Step C: Receiving an email alert

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

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

In the Security Reporter User Guide index, see:
• How to: view an email alert

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

IMPORTANT INFORMATION ABOUT USING THE SR IN THE EVALUATION MODE

Evaluation mode pertains to the state of an SR in which a maxmum of three weeks of data is stored on the server.

When evaluating the SR in evaluation mode, the Report Manager user interface and Expiration screen from the System Configuration administrator console display differently than they do in registered (standard) mode.

***NOTE**: See the System Configuration Section and Report Manager Administration Section of the Security Reporter User Guide for information about using panels/screens in registered mode.*

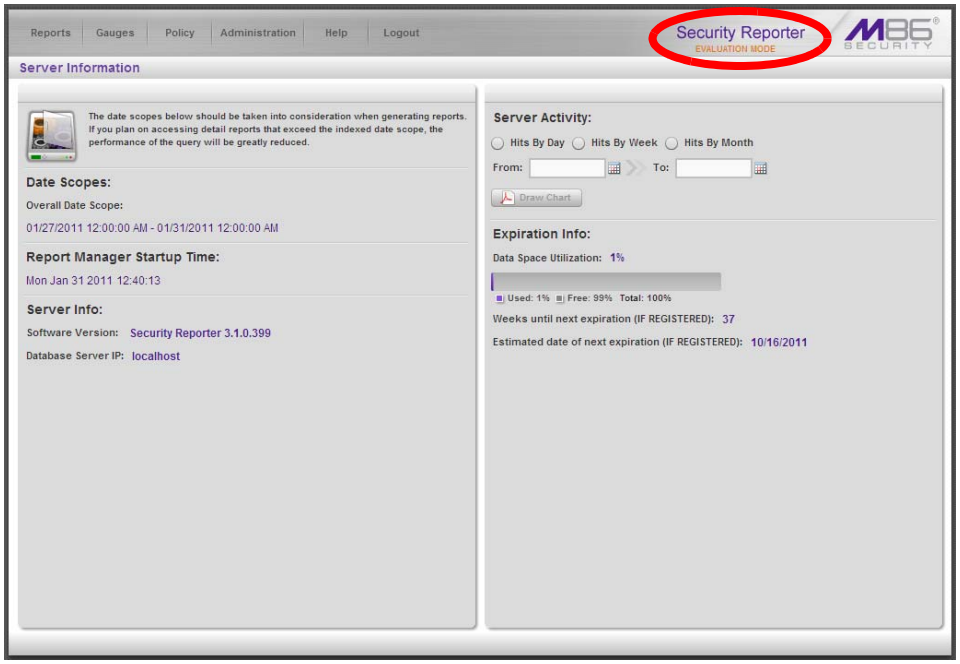
Report Manager

In evaluation mode, the Report Manager banner displays 'EVALUATION MODE' beneath the Security Reporter name/link as shown in the sample panel below.

Hover over the '**EVALUATION MODE**' link to display a definition of 'Evaluation Mode'. Click this link to launch the SR Server Status screen of the System Configuration administrator console and Status pop-up box (see more about the pop-up box on the next page).

Server Information Panel

Information about the server's status can be viewed in the Server Information panel (shown below). The Expiration Info section at the bottom right of the panel displays the amount of data space allocated to the SR and used by the SR, as well as data expiration criteria calculated for this SR, if activated in registered mode.

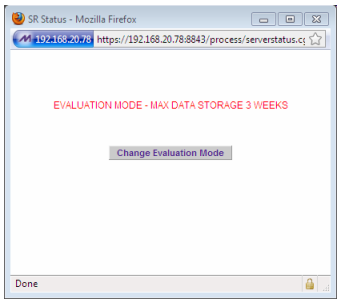


System Configuration

***NOTE**: See Appendix C: Evaluation Mode in the Security Reporter User Guide for information about changing the SR's mode from evaluation to registered.*

Evaluation Mode Pop-Up

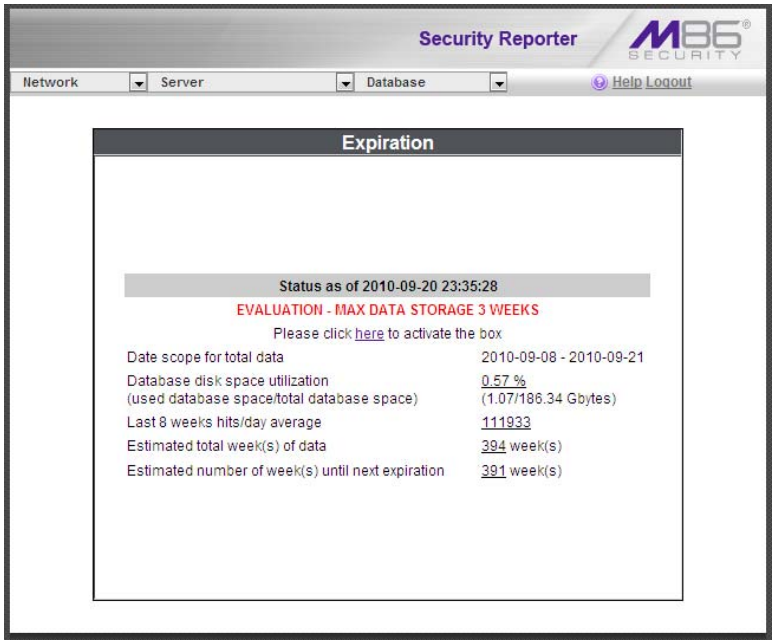
In evaluation mode, the SR Status pop-up box opens when accessing the System Configuration administrator console:



Until the SR is in registered mode, this pop-up box will continue to open whenever accessing the System Status screen of the System Configuration administrator console.

Expiration screen

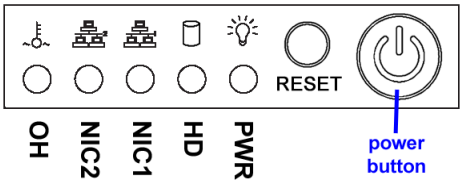
In evaluation mode, the Expiration screen includes the following message beneath the Status bar: "EVALUATION – MAX DATA STORAGE 'X' WEEKS" (in which 'X' represents the maximum number of weeks in the SR's data storage scope).



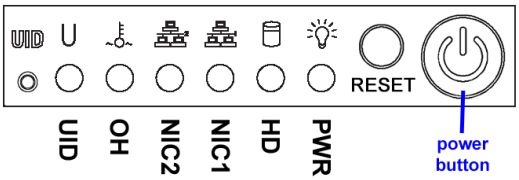
LED INDICATORS AND BUTTONS

Front Control Panels on 500, 700 and 730 Models

Control panel buttons, icons, and LED indicators display on the right side of a 500, 700 and 730 model's 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 model chassis front panel



700 / 730 model chassis front panel

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

UID (button) and **U** icon – On a 700 and 730 model, 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 model, 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 model, 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 and 730 Model

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 and 730 model 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.

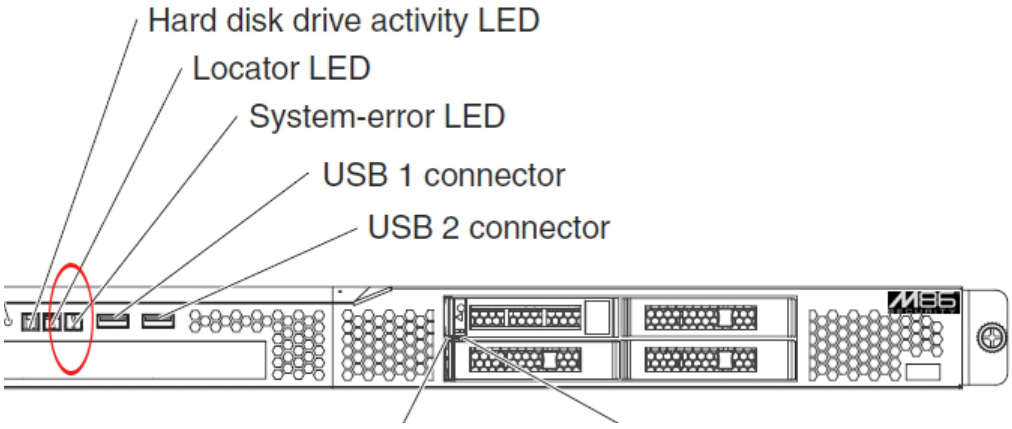
Front Control Panel on a 300 Model

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.

Chassis Panel on a 505 Model

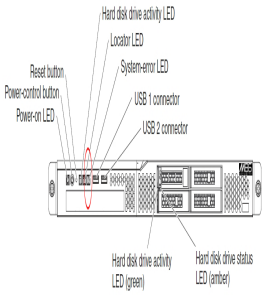
For diagrams and descriptions of the 505 model's front and rear panel components and their usage, please see "Server controls, LEDs, and power" in the IBM System x3250 M3 Types 4251, 4252, and 4261 Installation and User's Guide. As of July 2011, this manual can be downloaded from **http://www-947.ibm.com/support/entry/portal/docdisplay?Indocid=MIGR-5082564&brandind=5000008**



NOTE**: A lit System-error amber LED (located on the left side of the front panel) indicates one or more system error issues. System errors are troubleshooted via IBM's Integrated Management Module (IMM). Please consult IBM's Integrated Management Module User's Guide for information on configuring and using IMM. As of July 2011, this document was made available at **http://www-947.ibm.com/support/entry/portal/docdisplay?Indocid=MIGR-5079770&brandind=5000008

Chassis Panels on 705 and 735 Models

For diagrams and descriptions of the 705 and 735 model's front and rear panel components and their usage, please see "Server controls, LEDs, and power" in the IBM System x3620 M3 Type 7376 Installation and User's Guide. As of July 2011, this document can be downloaded from **http://www-947.ibm.com/support/entry/portal/docdisplay?brand=5000008&lndocid=MIGR-5084233**



NOTE: A lit System-error amber LED (located on the right side of the front panel) indicates one or more system error issues. System errors are troubleshooted via IBM's Integrated Management Module (IMM). Please consult IBM's Integrated Management Module User's Guide for information on configuring and using IMM. As of July 2011, this document was made available at **http://www-947.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5079770&brandind=5000008**

REGULATORY SPECIFICATIONS AND DISCLAIMERS

The information in this section pertains to SR models 300, 500, 700, and 730.

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 Item

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

- 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:

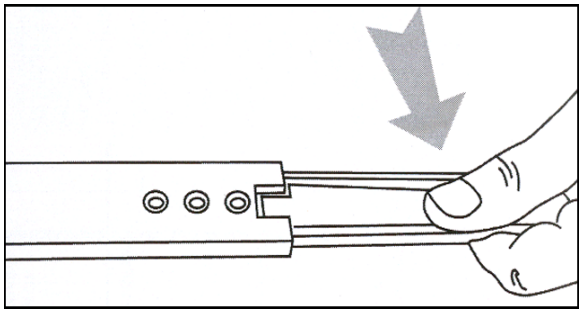
- The weight of all units in the rack is evenly distributed. Hazardous conditions may be created by an uneven weight distribution.
- The rack will not tip over when the unit is mounted, even when the unit is fully extended from the rack.
- For a single rack installation, stabilizers are attached to the 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.*

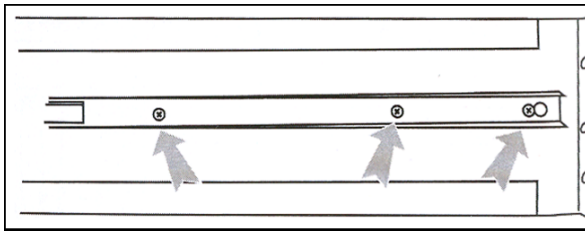
Step 1

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.

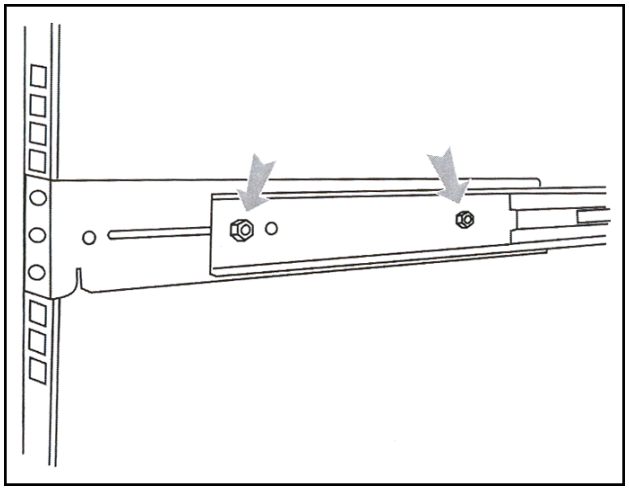


***NOTE**: When attaching the extended brackets, attach them loosely at first. Adjust the length to fit the cabinet, and then tighten.*

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.

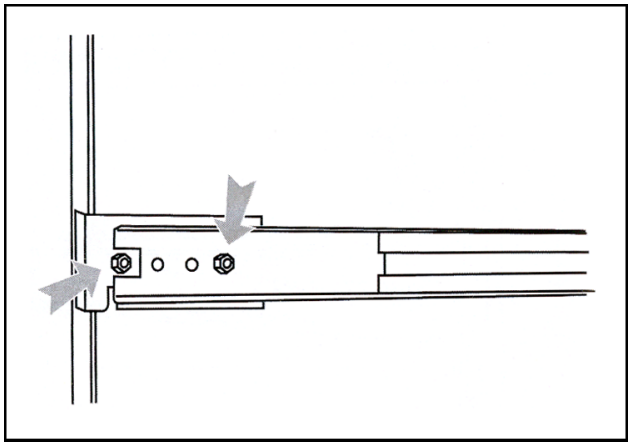
***NOTE**: Make sure the flange is on the bottom edge.*



Step 4

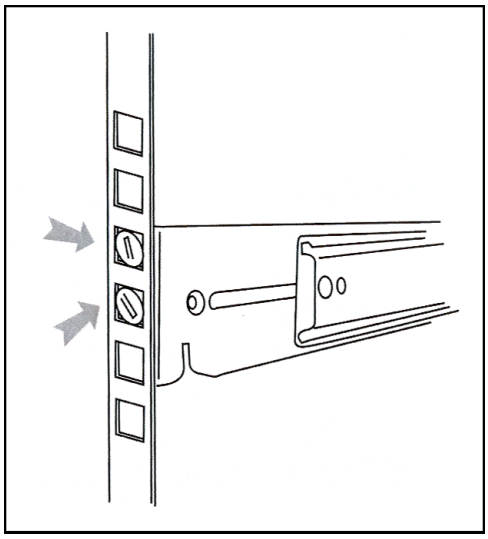
Attach left and right front (short) extended brackets to the outer rail using 2 screws, 2 washers, and 2 nuts for each bracket.

***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.

Step 1: Connect the SR to the Storage Device

Connect a 730 Model

A. Plug one end of the CAT-5E crossover cable into the SR unit's LAN 3 port-—the port to the left, located in the upper right section on the rear of the SR unit (see Figure 1, LAN3 port on a 730 model).

B. Plug the fibre channel cable into the port on the lower right section of the SR unit (see Figure 1, fibre channel port on a 730 model).

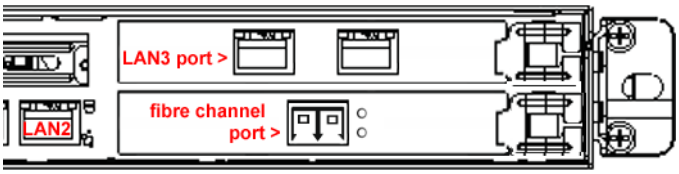


Figure 1: Diagram showing right portion of SR 730 chassis rear

Proceed to Step 2: Connect the Storage Device.

Connect a 735 Model

A. Plug one end of the CAT-5E crossover cable into the SR unit's LAN 2 port (see Figure 2, LAN2 port on a 735 model).

B. Plug the fibre channel cable into the port in the middle slot on the right section of the SR unit (see Figure 2, fibre channel port on a 735 model).

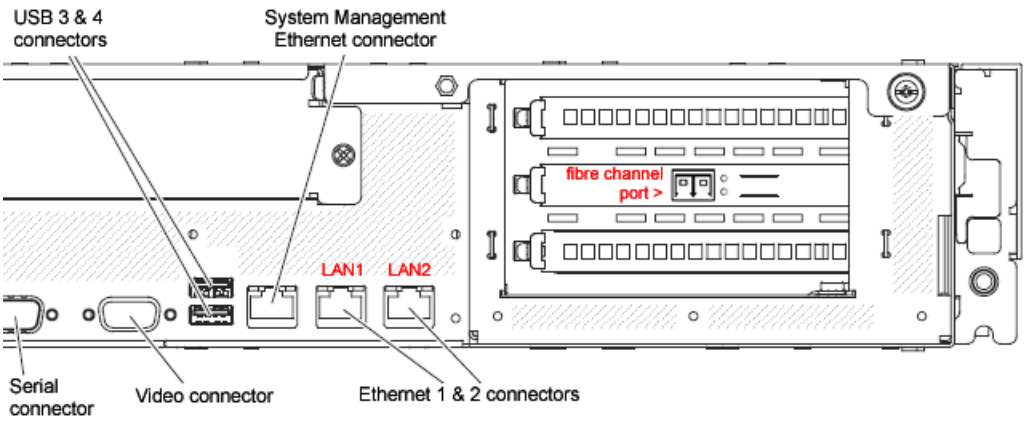


Figure 2: Diagram showing right portion of SR 735 chassis rear

Proceed to Step 2: Connect the Storage Device.

Step 2: Connect the Storage Device

A. Plug the other end of the fibre channel cable into the storage device's HOST "1" channel (see Figure 3, Item A).

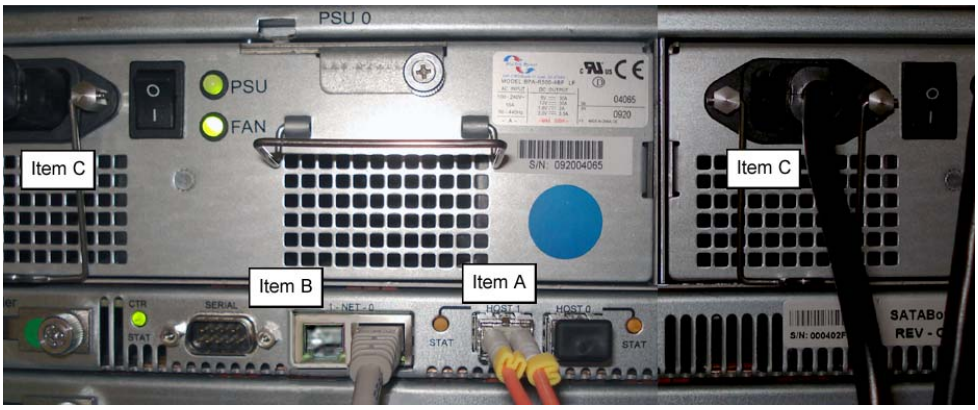


Figure 3: Back of the Nexsan SATABoy

B. Plug the other end of the CAT-5E crossover cable into the storage device's NET "0" (zero) port (see Figure 3, Item B).

C. Plug the storage device's AC power cords into the rear sections of the unit (see Figure 3, Item C).

D. 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.*

E. 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 4).

Figure 4: LED display

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

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

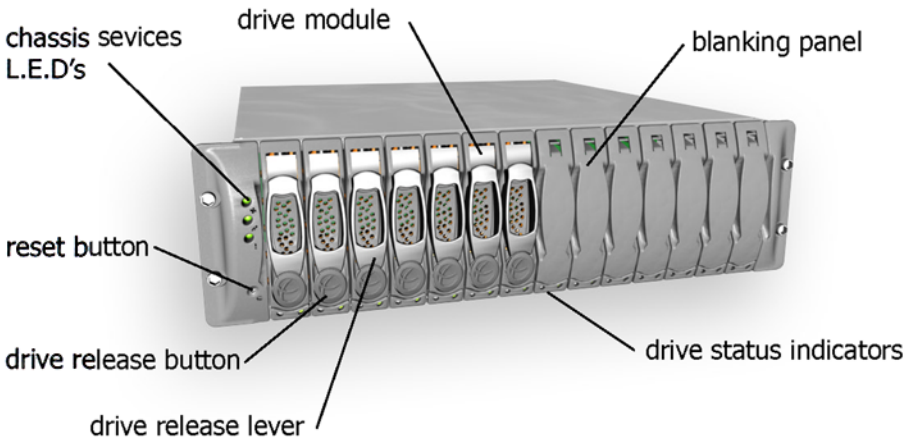
The storage device must be restarted after a power failure. In this instance, the storage device may already be turned on, but needs to be booted up again.

***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.*

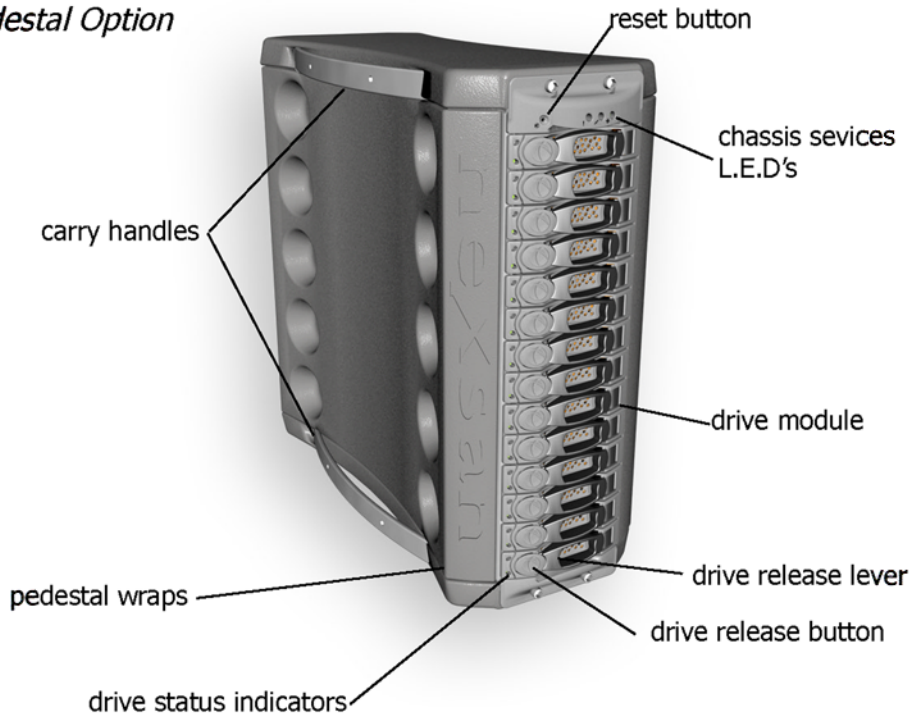
To restart the storage device, press the power button on the front panel. The boot-up process may take up to 5 minutes.

Physical Components

Rack Mount Option

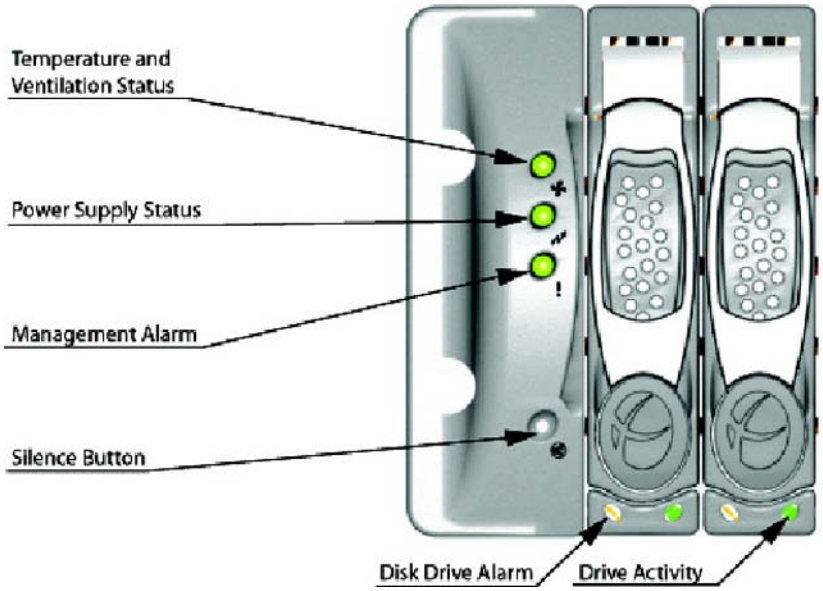


Pedestal Option



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:

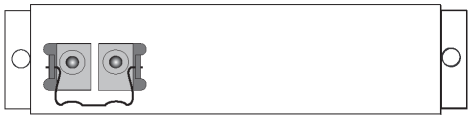
- 1 standard CAT-5E cable

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.

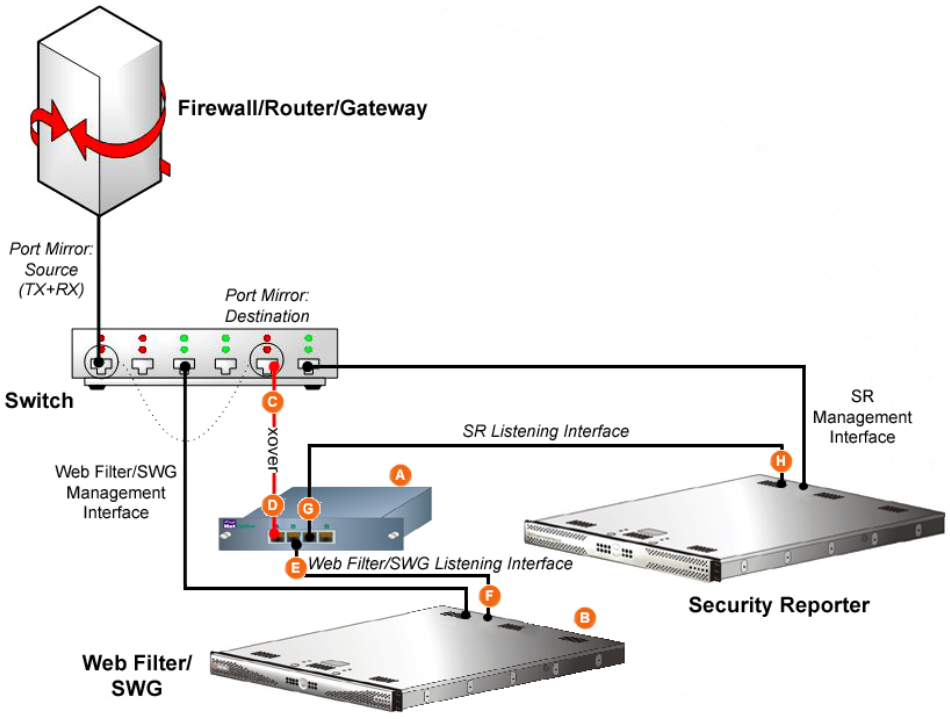


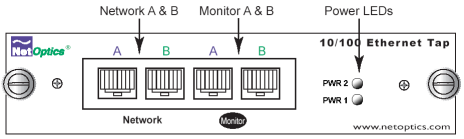
Diagram showing Ethernet Tap installation on the network

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 listening interface of the Web Filter.

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: Access the SR and its Applications Online.

INDEX

U

W

About Trustwave®

Trustwave is a leading provider of information security and compliance management solutions to large and small businesses throughout the world. Trustwave analyzes, protects and validates an organization's data management infrastructure from the network to the application layer—to ensure the protection of information and compliance with industry standards and regulations such as the PCI DSS and ISO 27002, among others. Financial institutions, large and small retailers, global electric exchanges, educational institutions, business service firms and government agencies rely on Trustwave. The company's solutions include on-demand compliance management, managed security services, digital certificates and 24x7 multilingual support. Trustwave is headquartered in Chicago with offices throughout North America, Central and South America, Europe, the Middle East, Africa, and Asia-Pacific.