M86 Enterprise Reporter

INSTALLATION GUIDE

Models: HL, SL

Software Version: 6.0.10
Document Version: 06.08.10

M86 Enterprise Reporter Installation Guide for HL, SL

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

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

Trademarks

Part# ER-IG-HS-100608

Contents

ER ENTERPRISE REPORTER INTRODUCTION

Thank you for choosing to install M86 Security's ER Enterprise Reporter. The ER is designed to readily obtain information about end users' Internet activity via log files (text files containing Web access data) from a source device such as the M86's Web Filter.

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

The ER is comprised of the ER server and client application. Once the ER server is configured and log files have populated the database, an administrator can use the ER client reporting application to virtually generate an unlimited number of queries and reports from data in the database. This data shows which end user is accessing which site, the duration of each site visit, and the frequency of these visits, and can help administrators identify Internet usage abusers, develop policies, and target sites to be filtered, in order to maximize bandwidth utilization and productivity. The client gives the administrator the ability to interrogate massive datasets through flexible drill-down technology, until the desired view is obtained, and then memorize and save the view to a user-defined report menu for repetitive, scheduled execution and distribution.

Quick setup procedures—to implement the best reporting practices using the ER client—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 ER 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 ER in your network environment
- **Install the Server -** This section explains how to configure the ER for reporting
- **Conclusion** - This section indicates that the installation steps have been completed
- **Best Reporting Practices** - This section includes reporting scenarios and instructions for implementing the best reporting practices to capture a snapshot of end user activity on your network that tells you whether or not policies are being enforced
- **Evaluation Mode -** This section gives information on using the ER in the evaluation mode
- **LED Indicators and Buttons** - This section explains how to read LED indicators and use LED buttons for troubleshooting the unit
- **Regulatory Specifications and Disclaimers -** This section cites safety and emissions compliance information for the ER models referenced in this document
- **Appendices -** Appendix A provides an alternate way of installing the Web Filter by using a crossover cable. Appendix B explains how to set up the optional NAS (Fibre Channel Connected Storage Device or “SAN”) unit
- **Index -** An alphabetized list of some topics included in this document

Conventions Used in this Document

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

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

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

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

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

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

SERVICE INFORMATION

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

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

M86 Security Corporate Headquarters (USA)

Local	:	714.282.6111
Domestic US	:	1.888.786.7999
International	:	+1.714.282.6111

M86 Security Taiwan

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

Procedures

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

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

PRELIMINARY SETUP PROCEDURES

Unpack the Unit from the Carton

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

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

The carton should contain the following items:

- 1 Enterprise Reporter (ER)
- 1 Bezel to be installed on the front of the chassis
- 1 AC Power Cord, 2 AC Power Cords for HL servers
- 1 Serial Port Cable
- 1 CAT-5E Crossover Cable
- Rack Mount Brackets (2)
- 1 CD-ROM containing supplemental product applications and EULA

  User guides can be obtained at **http://www.m86security.com/support/Enterprise-Reporter/documentation.asp**

NOTES*: A spare parts kit is included with the ER unit. For HL servers, this kit contains a hard drive and power supply. For SL servers, this kit contains a hard drive. Please refer to the appendix of the user guide for information on replacing a hard drive or power supply. If you have purchased the optional NAS (Fibre Channel Connected Storage Device or “SAN”) unit, an additional five-foot CAT-5E crossover cable is also included in the carton, and this unit also comes with a spare parts kit.*

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

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

Select a Site for the Server

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

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

Rack Mount the Server

Rack Setup Precautions

⚠ ***WARNING****:*

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

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

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

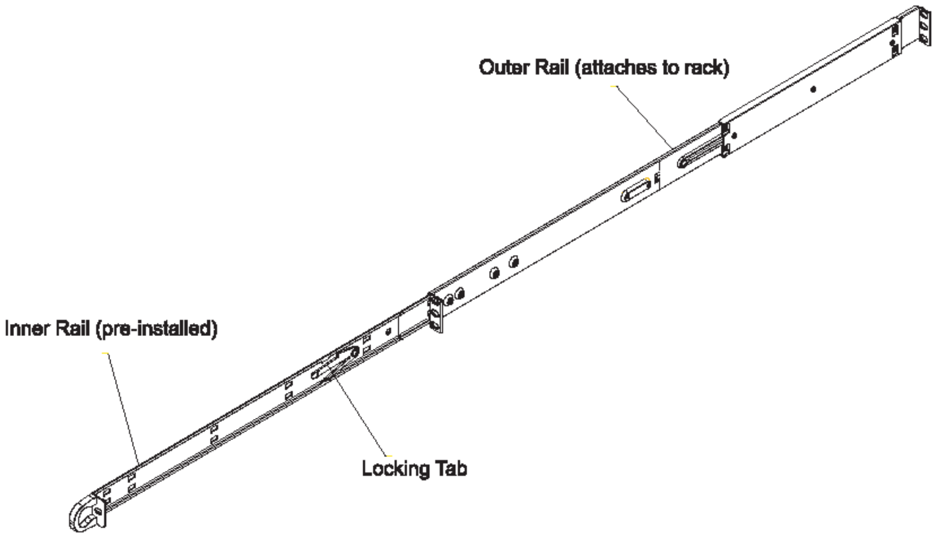
Rack Mount Instructions for HL Servers

Rack Setup Suggestions

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

Identify the Sections of the Rack Rails

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



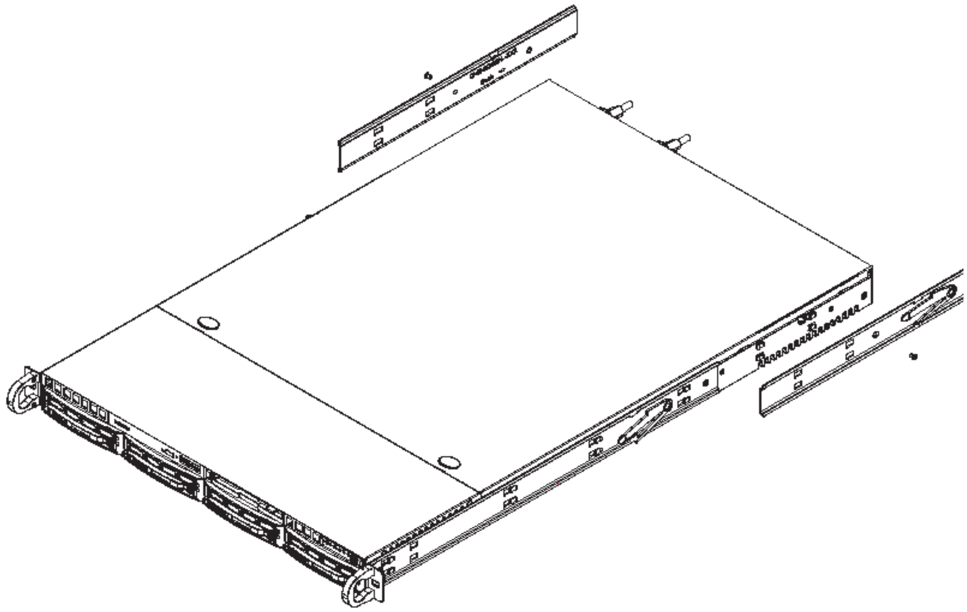
Install the Inner Rails

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

Install the Outer Rails

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

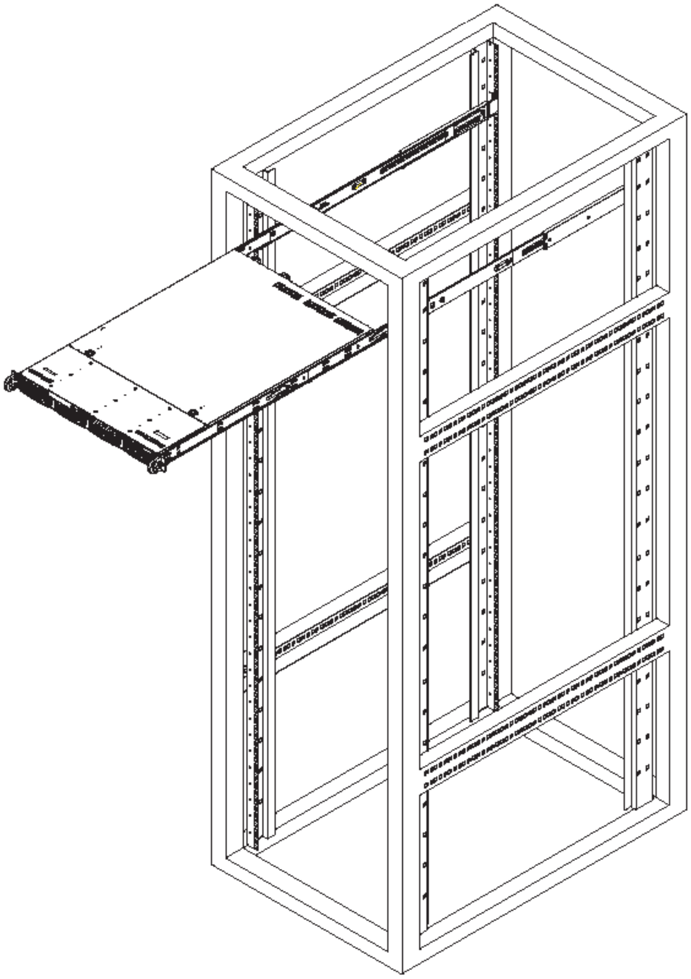
Locking Tabs: Both chassis rails have a locking tab, which serves two functions. The first is to lock the server into place when installed and pushed fully into the rack, which is its normal position. Secondly, these tabs also lock the server in place when fully extended from the rack. This prevents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



Install the Server into the Rack

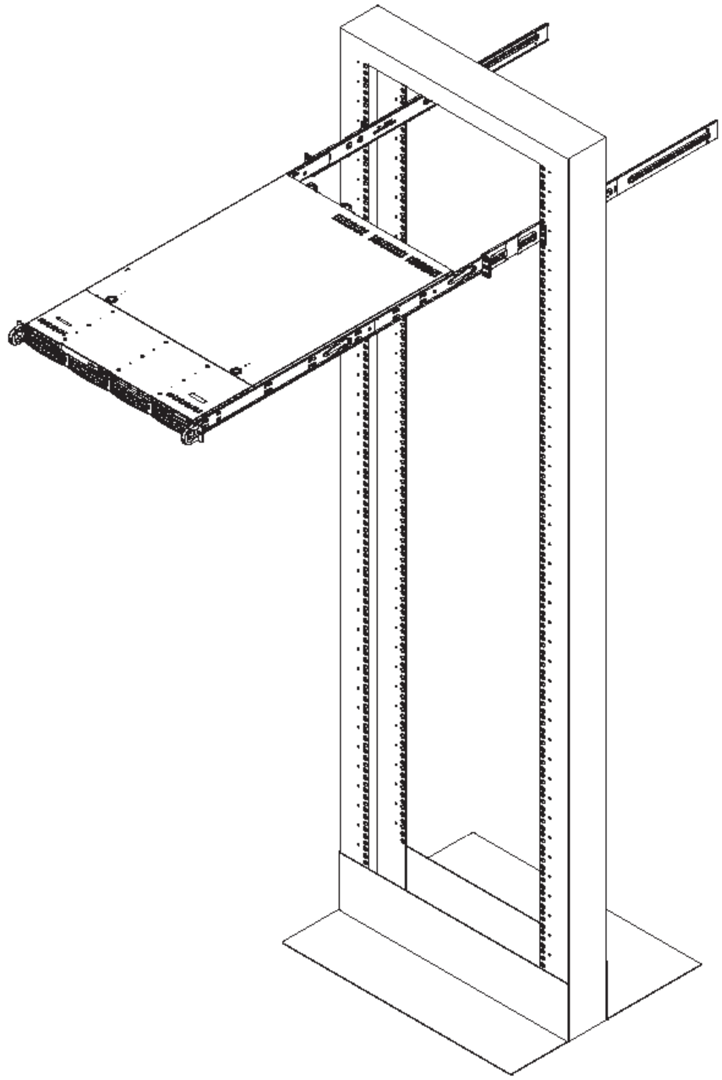
You should now have rails attached to both the chassis and the rack unit. The next step is to install the server chassis into the rack. Do this by lining up the rear of the chassis rails with the front of the rack rails. Slide the chassis rails into the rack rails, keeping the pressure even on both sides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

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



Install the Server into a Telco Rack

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



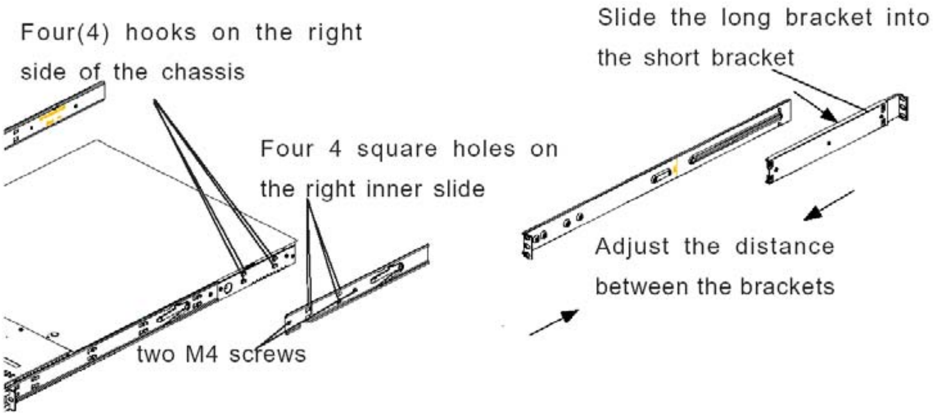
Rack Mount Instructions for SL Servers

Rack Setup Suggestions

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

Install the Inner Slides

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

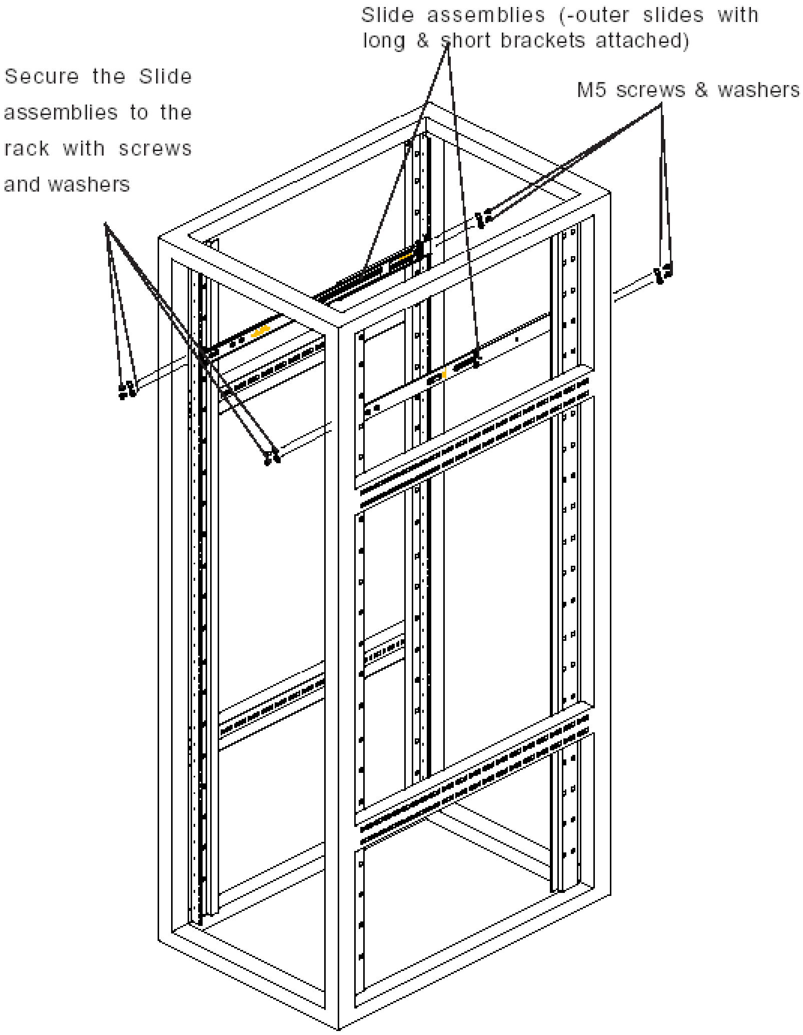

Four(4) hooks on the right side of the chassis
Four 4 square holes on the right inner slide
two M4 screws
Slide the long bracket into the short bracket
Adjust the distance between the brackets

Install the Outer Slides

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

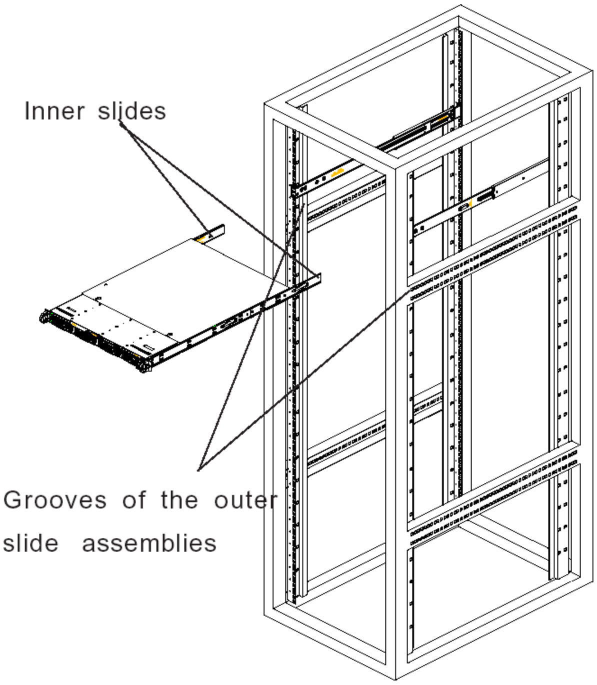
Install the Slide Assemblies to the Rack

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

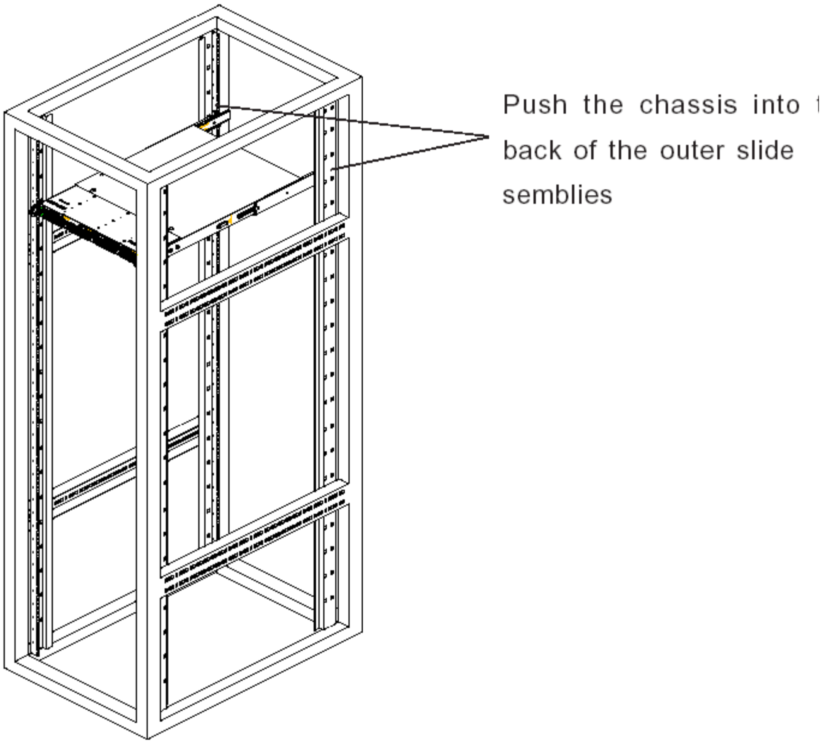

Slide assemblies (-outer slides with long & short brackets attached)
Secure the Slide assemblies to the rack with screws and washers
M5 screws & washers

Install the Chassis into the Rack

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



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



Install the SL or HL Server Bezel

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

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

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

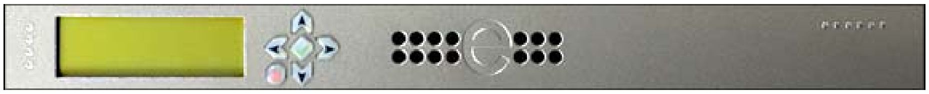


Fig. 1 - Front of bezel

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

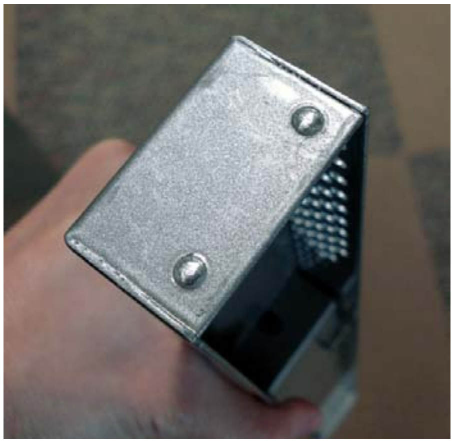


Fig. 2 - Bumps on right end of bezel

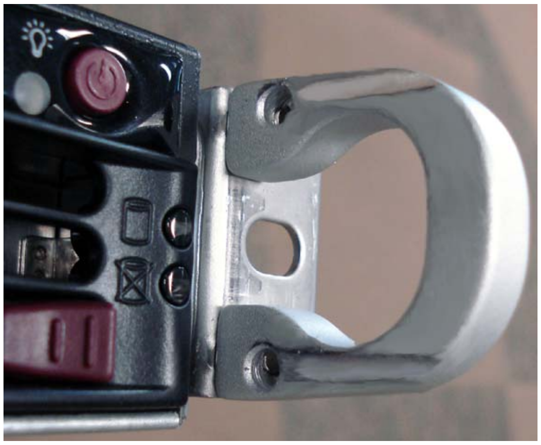


Fig. 3 - Grooves in right U-shaped handle

C. Align these bumps along the two parallel grooves inside each U-shaped aluminum chassis handle affixed to the front end of the chassis rail (Fig. 3).

D. Push the bezel towards the front of the chassis, inserting the USB B-type plug on the back of the bezel (Fig. 4) into the USB port on the chassis.

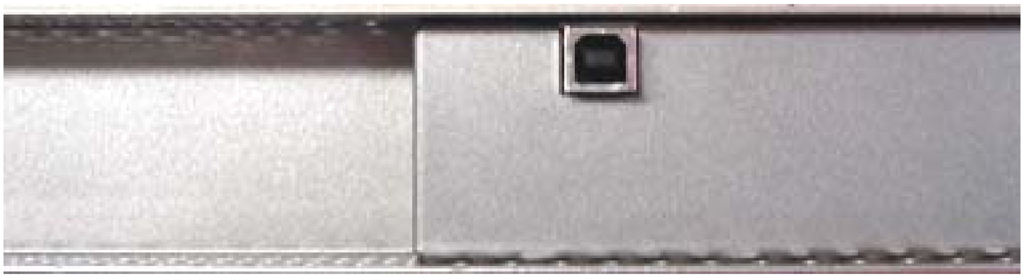


Fig. 4 - Section of back of bezel with USB B-type plug

Check the Power Supply

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

Power Supply Precautions

⚠ ***WARNING**:*

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

General Safety Information

Server Operation and Maintenance Precautions

WARNING*:*

Observe the following safety precautions during server operation and maintenance:

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

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

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

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

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

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

AC Power Cord and Cable Precautions

***WARNING**:*

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

Electrical Safety Precautions

***WARNING**:*

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

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

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

Motherboard Battery Precautions

CAUTION:

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

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

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

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

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

Quick Start Setup Requirements

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

- ER 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)

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

Administrator Console Setup Requirements

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

- ER with AC power cord(s)
- CAT-5E crossover cable
- PC laptop computer, or PC monitor with AC power cord and keyboard

Go to Appendix A to execute Console Setup Procedures.

LCD Panel Setup Requirements

The following hardware is required for LCD panel setup procedures:

- ER with AC power cord(s)
- Bezel with LCD panel mounted on chassis front

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

Step 1A: Quick Start Setup Procedures

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 ER, you will need to connect it to the ER at this point. Refer to Appendix B at the end of this document for instructions on how to connect the Fibre Channel Connected Storage Device.

Link the Workstation to the ER

Monitor and Keyboard Setup

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

B. Turn on the PC monitor.

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

D. Power on the ER by dropping down the face plate and pressing the large button at the right of the front panel (see Fig. 3 for an SL unit, and Fig. 4 for an HL unit).

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

Serial Console Setup

A. Using the serial port cable (and USB DB9 serial adapter, if necessary), connect the laptop to the rear of the chassis (see Fig. 1 for an SL unit, and Fig. 2 for an HL unit).

B. Power on the laptop.

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

D. Power on the ER by dropping down the face plate and pressing the large button at the right of the front panel (see Fig. 3 for an SL unit, and Fig. 4 for an HL unit).

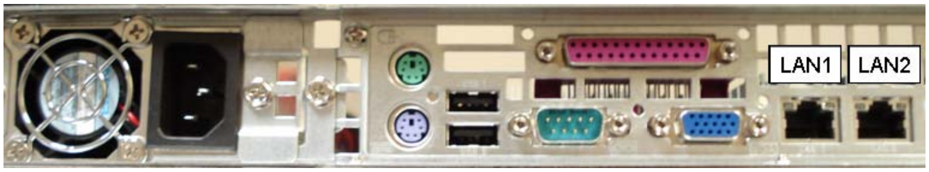


Fig. 1 - Portion of SL chassis rear

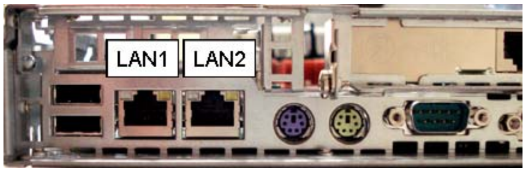


Fig. 2 - Portion of HL chassis rear

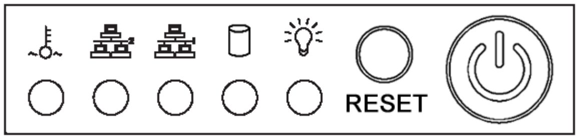


Fig. 3 - Diagram of SL chassis front panel, power button at far right

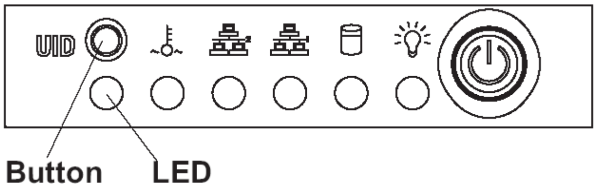


Fig. 4 - Diagram of HL chassis front panel, power button at far right

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

HyperTerminal Setup Procedures

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

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

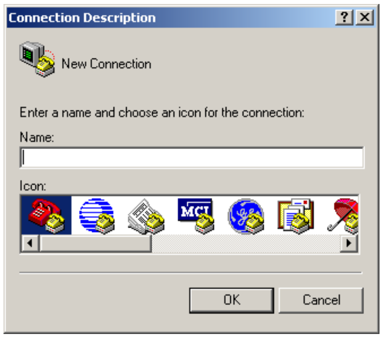
If you are using a Windows Vista or Windows 7 machine to conduct these quick start setup procedures and do not have an equivalent type of terminal emulator program installed on your workstation, Hilgraeve, Inc., the maker of HyperTerminal, offers HyperTerminal Private Edition for Windows Vista and Windows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

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

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

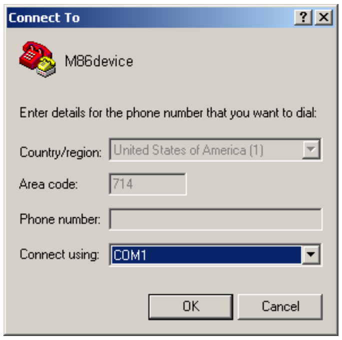
On the Windows XP machine:

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



Enter a name and choose an icon for the connection:

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

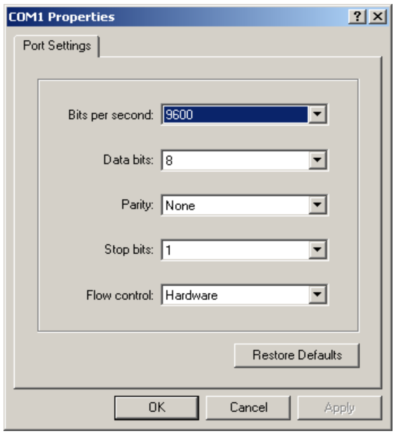


M86device

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

Country/region: United States of America (1)
Area code: 714
Phone number:
Connect using: COM1

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

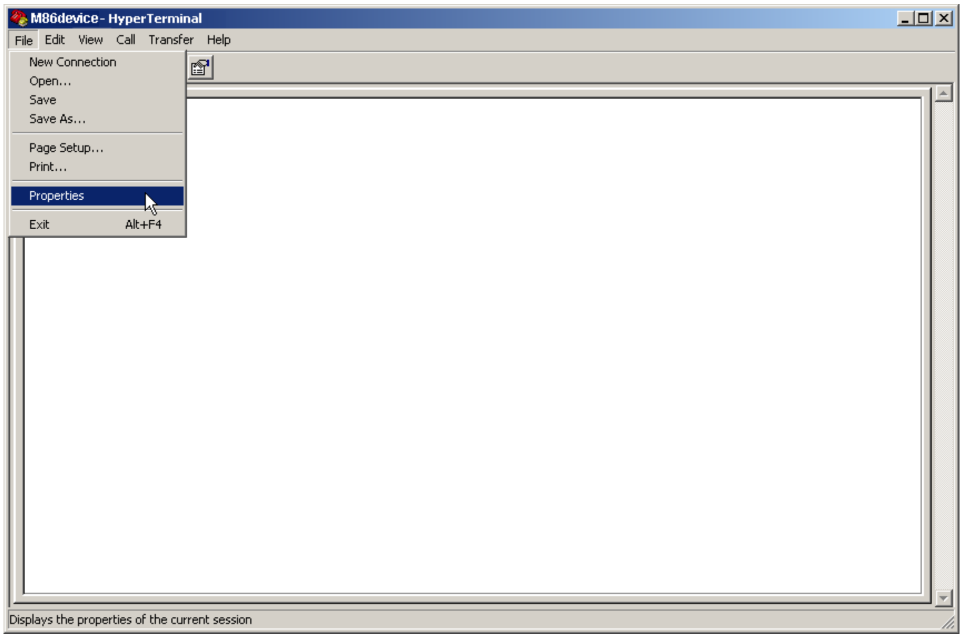


Bits per second: 9600
Data bits: 8
Parity: None
Stop bits: 1
Flow control: Hardware

D. Specify the following session settings:

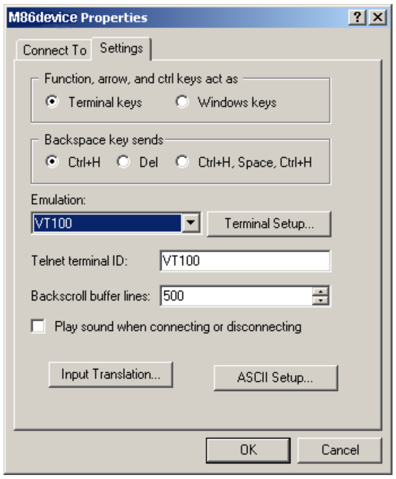
- Bits per second: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: Hardware

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



Displays the properties of the current session

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



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

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

Emulation: VT100

Telnet terminal ID: VT100

Backscroll buffer lines: 500

□ Play sound when connecting or disconnecting

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

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

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

Login screen

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

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

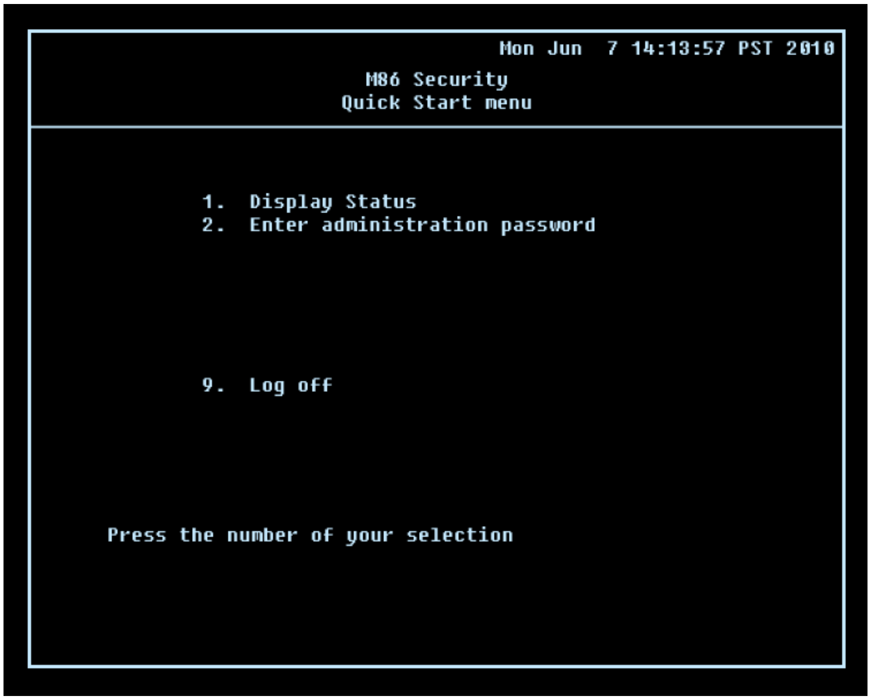
A. At the **login** prompt, type in ***menu***.

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

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

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

Quick Start menu screen



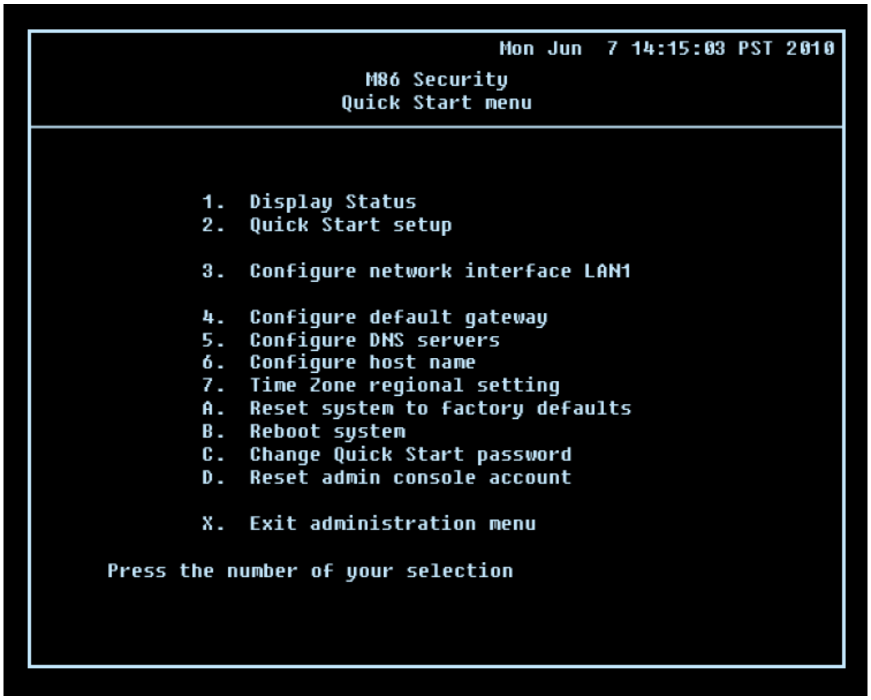
```
                                          Mon Jun  7 14:13:57 PST 2010
                               M86 Security
                             Quick Start menu

              1.  Display Status
              2.  Enter administration password



              9.  Log off



      Press the number of your selection
```

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

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

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

Quick Start menu: administration menu



```
                                        Mon Jun  7 14:15:03 PST 2010
                              M86 Security
                            Quick Start menu


               1.  Display Status
               2.  Quick Start setup

               3.  Configure network interface LAN1

               4.  Configure default gateway
               5.  Configure DNS servers
               6.  Configure host name
               7.  Time Zone regional setting
               A.  Reset system to factory defaults
               B.  Reboot system
               C.  Change Quick Start password
               D.  Reset admin console account

               X.  Exit administration menu

       Press the number of your selection
```

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

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

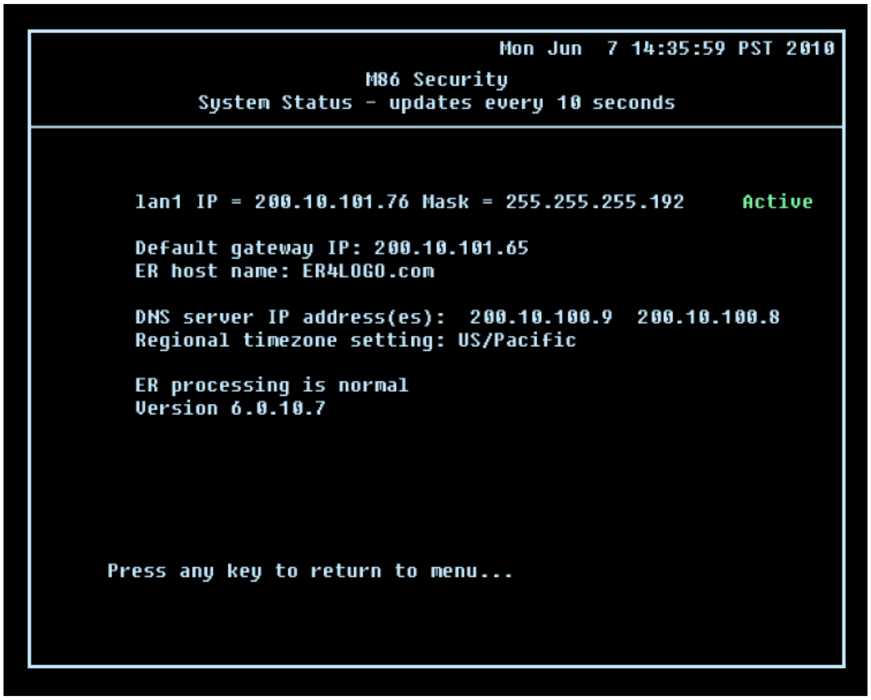
- Configure network interface LAN1
- Configure default gateway
- Configure DNS servers
- Configure host name
- Time Zone regional setting

***NOTE**: See the Network screens for Network Settings, and Regional Setting in Step 1B for content included in the Quick Start setup screens.*

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

***NOTE**: Changing your password using option C, “Change Quick Start password”, will change the password for the console menu but not the ER console login screen. Option A, “Reset system to factory defaults”, should only be used by an M86 Security technical representative. Option D, “Reset admin console account”, should be used for resetting the administrator console username and password to the factory default ‘admin’/’reporter’ and for unlocking all IP addresses currently locked.*

System Status screen



```
                                        Mon Jun  7 14:35:59 PST 2010
                                   M86 Security
                      System Status - updates every 10 seconds

         lan1 IP = 200.10.101.76 Mask = 255.255.255.192     Active

         Default gateway IP: 200.10.101.65
         ER host name: ER4LOGO.com

         DNS server IP address(es):  200.10.100.9  200.10.100.8
         Regional timezone setting: US/Pacific

         ER processing is normal
         Version 6.0.10.7



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

The System Status screen contains the following information:

- **Capturing Interface** specified in screen 3 (Configure network interface LAN1)
- **lan1 IP** address and netmask specified in screen 3, and current status (“Active” or “Inactive”)
- **Default gateway** IP address specified in screen 4 (Configure default gateway)
- **ER host name** specified in screen 6 (Configure host name)
- **DNS server IP address(es)** specified in screen 5 (Configure DNS servers)
- **Regional timezone setting** specified in screen 7 (Time Zone regional setting)
- Current status of the ER
- Current ER software **Version** installed

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

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 ER.

Proceed to Step 2: Physically Connect the ER 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 ER, you will need to connect it to the ER at this point. Refer to Appendix B at the end of this document for instructions on how to connect the Fibre Channel Connected Storage Device.

Power up the ER

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

B. Power on the server by dropping down the face plate and pressing the large button at the right of the front panel.

The ER can be configured using the LCD panel on front of the chassis bezel. When the bezel is placed on the front of the chassis, with the USB plug inserted into the USB port, the default LCD screen displays.

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

LCD Menu

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

***NOTE**: On the LCD Menu, press “X” to toggle the display between the main menu and the following information: “Enterprise Reporter (software version number)” and “Database Status (Active, Inactive)”.*

Main Menu

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

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

***NOTE**: Navigation tips in the main menu:*

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

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

Current Patch Level

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

IP / LAN1

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

- Configure LAN 1 IP
- Change LAN1 Netmask

A. Choose **Configure LAN 1 IP** and press the checkmark key to go to the Configure LAN 1 IP screen.

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

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

D. Choose **Change LAN1 Netmask** and press the checkmark key to go to the Change LAN1 Netmask screen.

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

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

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

Gateway

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

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

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

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

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

DNS 1 and 2

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

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

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

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

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

Host Name

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

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

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

NOTE*: Navigation tips:*

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

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

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

Regional Setting (Time Zone, date, time)

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

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

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

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

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

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

Reset Admin Console Password

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

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

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

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

- Choose **Yes, reset it now!** to reset the password and to return to the main 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 ER.
- **No, cancel reboot** - This selection returns you to the previous screen.

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

Shutdown

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

A. Choose one of two options:

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

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

LCD Options menu

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

- Heartbeat
- Backlight
- LCD Controls >

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

Heartbeat

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

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

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

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

Backlight

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

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

- backlight feature enabled (checkbox populated with “x” and backlight turns on)
- backlight feature disabled (checkbox empty and backlight turns off)
- display the backlight now (checkbox populated with checkmark, and backlight turns on)

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

LCD Controls

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

A. Choose one of the menu selections and press the checkmark key to go to that screen:

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

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

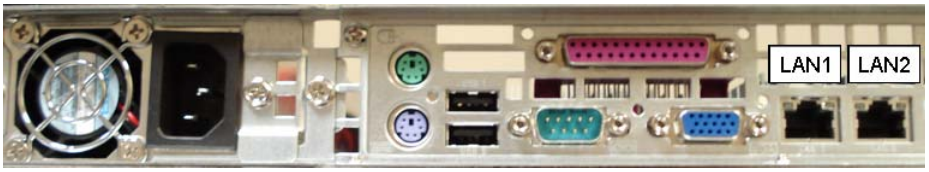
Proceed to Step 2: Physically Connect the ER to the Network.

Step 2: Physically Connect the ER to the Network

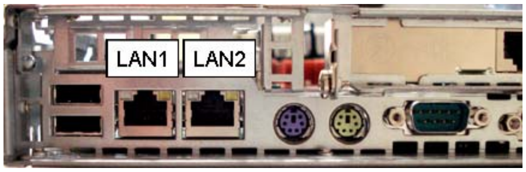
Now that your ER network parameters are set, you can physically connect the unit to your network. This step requires a standard CAT-5E cable.

A. Reboot the server by using the Reboot system option (as described in Step 1A: Quick Start Setup Procedures), or by using the Reboot option on the LCD panel of the SL or HL unit (as described in Step 1B: LCD Panel Setup Procedures).

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



Portion of SL chassis rear



Portion of HL chassis rear

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

D. Wait until the Restart process has completed (indicated by the drive light staying off for 30 seconds. This process may take 5 - 10 minutes), then proceed to Step 3: Access the ER Online.

***NOTE**: To verify that the server is in the process of being restarted, you can try accessing another screen. If you cannot access another screen, the restart process is still in progress.*

Step 3: Access the ER Online

Access the ER via its LAN 1 IP Address

A. Launch an Internet supported browser:

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

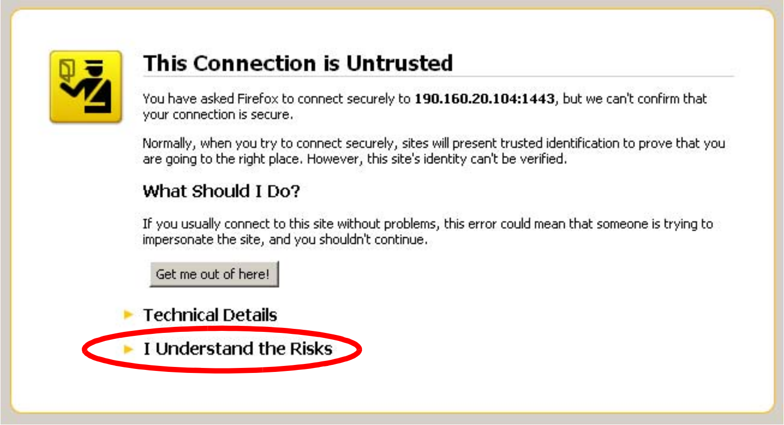
B. In the address field, type in the LAN 1 IP address you assigned to the ER in Step 1A (Quick Start setup) or Step 1B (IP / LAN1 and 2). Be sure to use “https” and port **:8843** for a secure connection. For example, if the ER were assigned an IP address of 10.10.10.10, you would enter **https://10.10.10.10:8843** in the browser’s address field.

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

- If using Firefox, proceed to Accept the Security Certificate in Firefox.
- If using IE, proceed to Temporarily Accept the Security Certificate in IE.
- If using Safari, proceed to Accept the Security Certificate in Safari.
- If the security issue page does not display in your browser, verify the following:
  - The ER is powered on.
  - Can the administrator workstation normally connect to the Internet?
  - Is the administrator workstation able to ping the ER?
  - Did you restart the ER after changing the network settings?
  - If still unsuccessful, contact an M86 Security solutions engineer or technical support representative.

Accept the Security Certificate in Firefox

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



This Connection is Untrusted

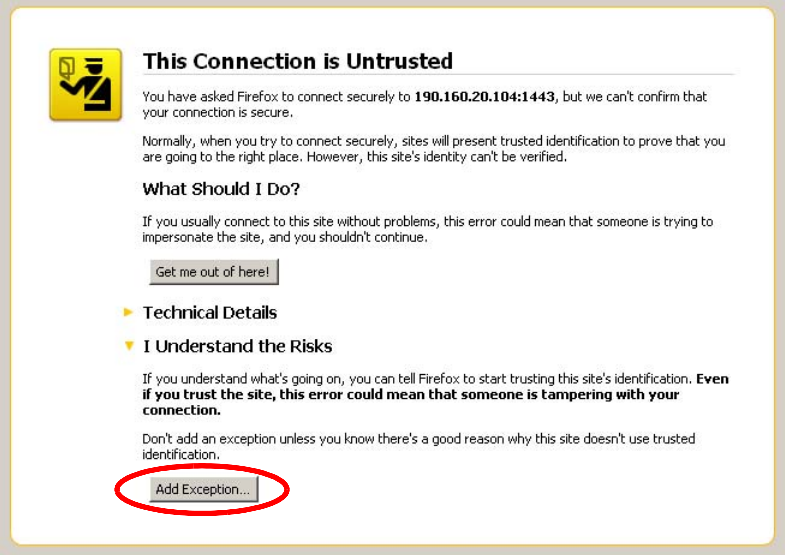
You have asked Firefox to connect securely to **190.160.20.104:1443**, but we can't confirm that your connection is secure.

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

What Should I Do?

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

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



This Connection is Untrusted

You have asked Firefox to connect securely to **190.160.20.104:1443**, but we can't confirm that your connection is secure.

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

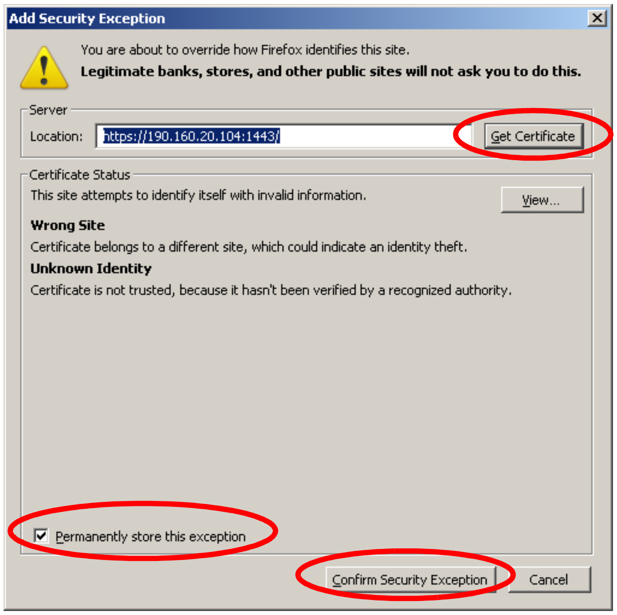
What Should I Do?

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

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

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

Clicking Add Exception opens the Add Security Exception window:



Add Security Exception

You are about to override how Firefox identifies this site.

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

Server

Location: https://190.160.20.104:1443/

Certificate Status

This site attempts to identify itself with invalid information.

Wrong Site

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

Unknown Identity

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

☑ Permanently store this exception

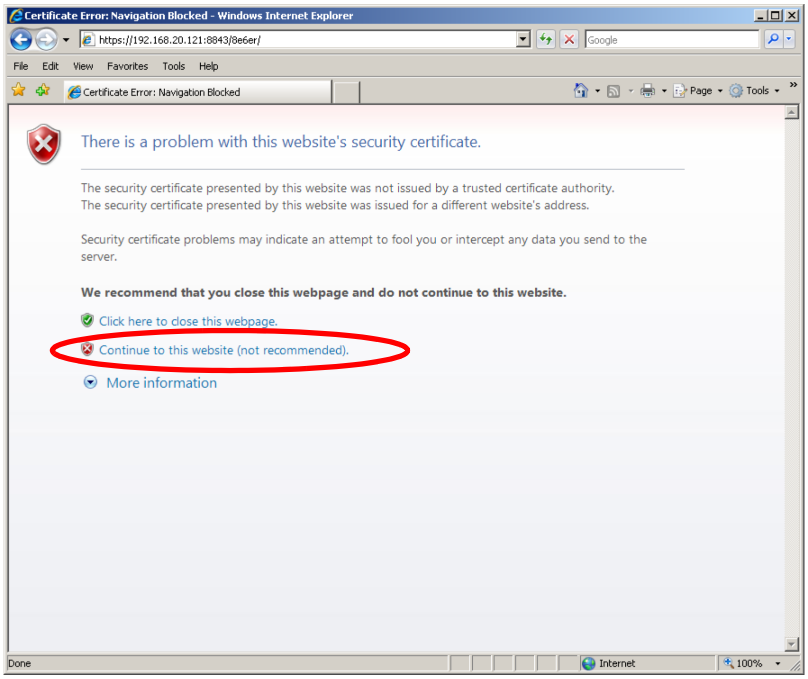
C. In the Add Security Exception window, click **Get Certificate** and wait a few seconds until the security certificate is obtained by the server.

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

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

Temporarily Accept the Security Certificate in IE

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


Certificate Error: Navigation Blocked - Windows Internet Explorer
https://192.168.20.121:8843/8e6er/
Google
File Edit View Favorites Tools Help
Certificate Error: Navigation Blocked
Page Tools
Done
Internet
100%

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

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

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

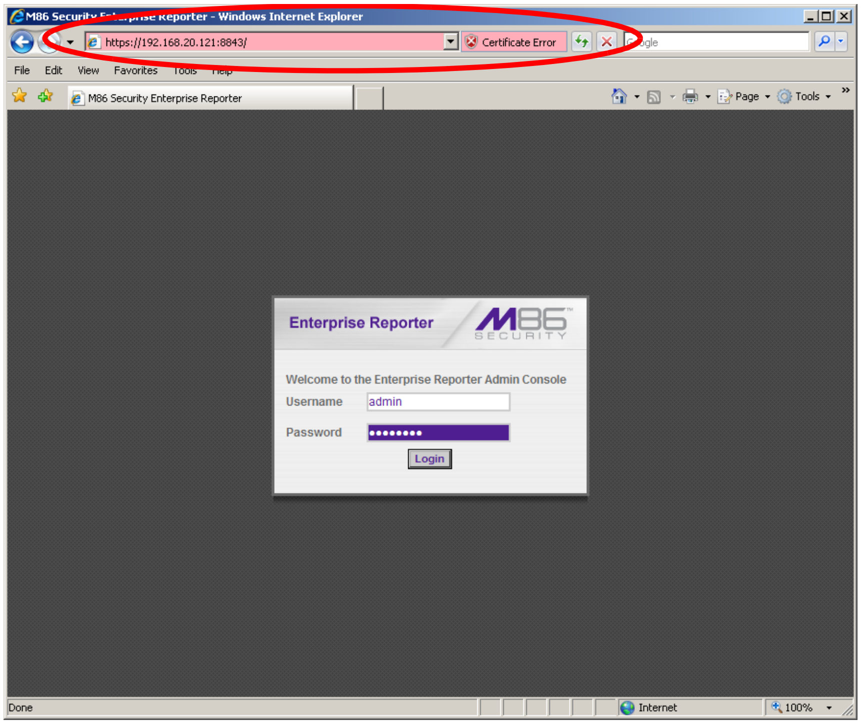
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

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


M86 Security Enterprise Reporter - Windows Internet Explorer
https://192.168.20.121:8843/
Certificate Error
File Edit View Favorites Tools Help
M86 Security Enterprise Reporter
Page Tools
Enterprise Reporter
M86 SECURITY
Login
Done
Internet
100%

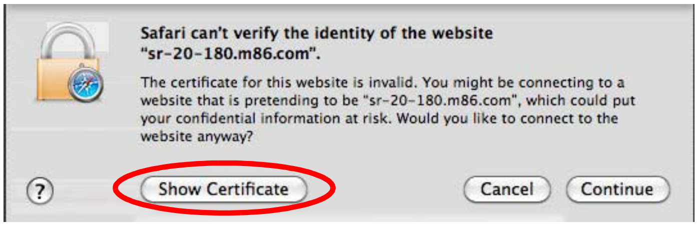
Welcome to the Enterprise Reporter Admin Console

Username admin

Password ••••••••

Accept the Security Certificate in Safari

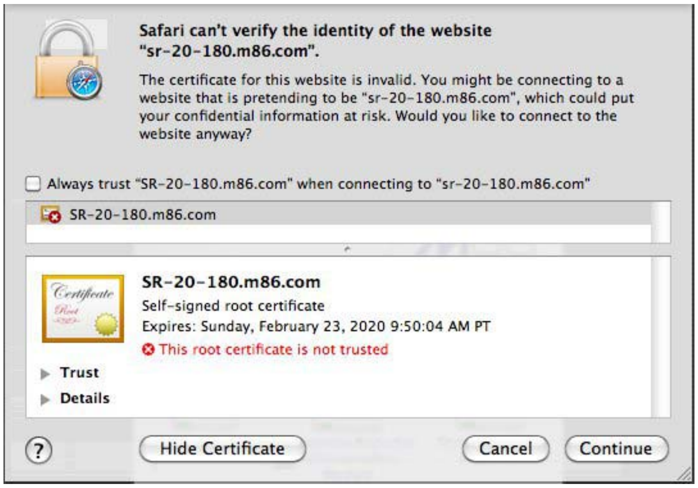
A. If using a Safari browser, the pop-up window "Safari can't verify the identity of the website..." opens:



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

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

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



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

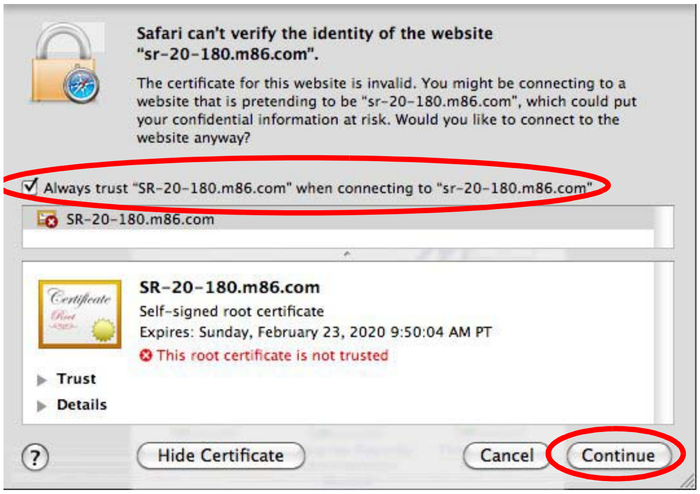
The certificate for this website is invalid. You might be connecting to a website that is pretending to be "sr-20-180.m86.com", which could put your confidential information at risk. Would you like to connect to the website anyway?

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

SR-20-180.m86.com

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

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



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

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

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

SR-20-180.m86.com

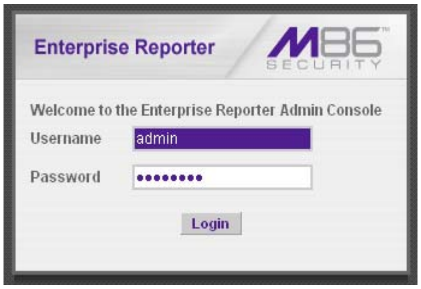
SR-20-180.m86.com
Self-signed root certificate
Expires: Sunday, February 23, 2020 9:50:04 AM PT
This root certificate is not trusted

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

Step 4: Log in, Generate SSL Certificate

Log in to the Administrator Console

A. In the login window, go to the **Username** field and type in ***admin***.



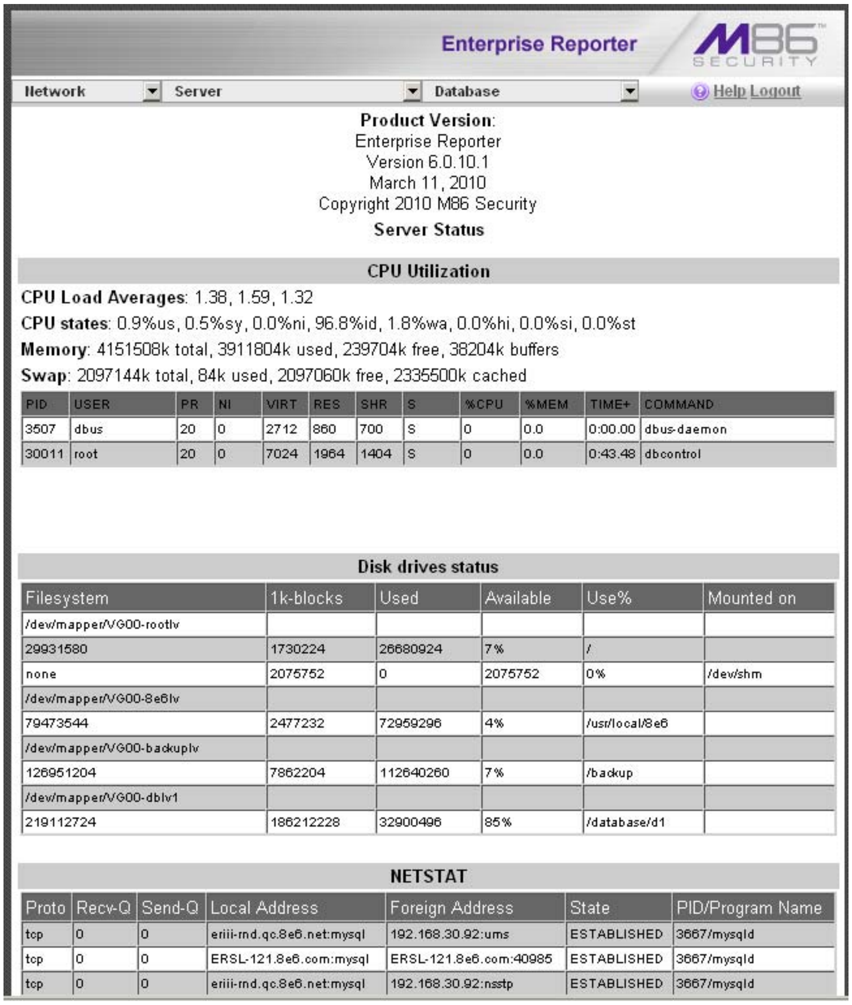
Welcome to the Enterprise Reporter Admin Console

Username: admin

Password: ••••••••

B. In the **Password** field, type in ***reporter***.

C. Click **Login** to go to the Server Status screen of the Administrator console:



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

Server Status

CPU Utilization

CPU Load Averages: 1.38, 1.59, 1.32

CPU states: 0.9%us, 0.5%sy, 0.0%ni, 96.8%id, 1.8%wa, 0.0%hi, 0.0%si, 0.0%st

Memory: 4151508k total, 3911804k used, 239704k free, 38204k buffers

Swap: 2097144k total, 84k used, 2097060k free, 2335500k cached

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
3507	dbus	20	0	2712	860	700	S	0	0.0	0:00.00	dbus-daemon
30011	root	20	0	7024	1964	1404	S	0	0.0	0:43.48	dbcontrol

Disk drives status

Filesystem	1k-blocks	Used	Available	Use%	Mounted on
/dev/mapper/VG00-rootlv					
29931580	1730224	26680924	7%	/	
none	2075752	0	2075752	0%	/dev/shm
/dev/mapper/VG00-8e6lv					
79473544	2477232	72959296	4%	/usr/local/8e6	
/dev/mapper/VG00-backuplv					
126951204	7862204	112640260	7%	/backup	
/dev/mapper/VG00-dblv1					
219112724	186212228	32900496	85%	/database/d1	

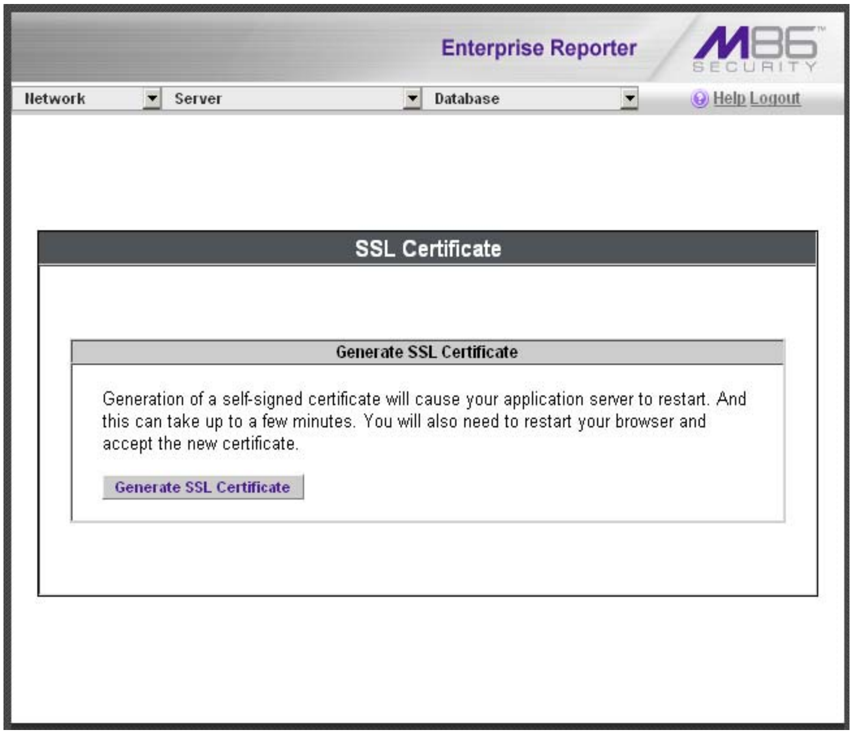
NETSTAT

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

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

Generate SSL Certificate

A. Navigate to **Network > SSL Certificate** to open the SSL Certificate screen:



Generation of a self-signed certificate will cause your application server to restart. And this can take up to a few minutes. You will also need to restart your browser and accept the new certificate.

B. Click **Generate SSL Certificate** to display the page that asks if you wish to continue, which would restart your server.

C. Click **Yes** to generate the SSL certificate and restart the ER Server.

D. Close your browser and wait a few minutes before attempting to access the user interface.

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

If using a Firefox or Safari browser, proceed to Step 5: Change User Name and Password, Set Self-Monitoring.

IE Security Certificate Installation Procedures

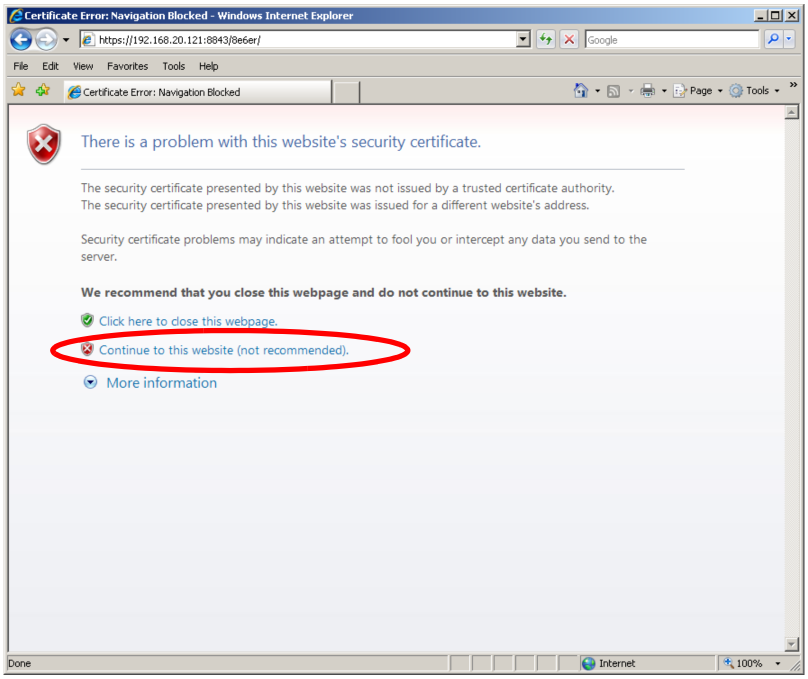
Accept the Security Certificate in IE

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

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

Windows XP or Vista with IE 7 or 8

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


Certificate Error: Navigation Blocked - Windows Internet Explorer
https://192.168.20.121:8843/8e6er/
Google
File
Edit
View
Favorites
Tools
Help
Certificate Error: Navigation Blocked
Page
Tools
Done
Internet
100%

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

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

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

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

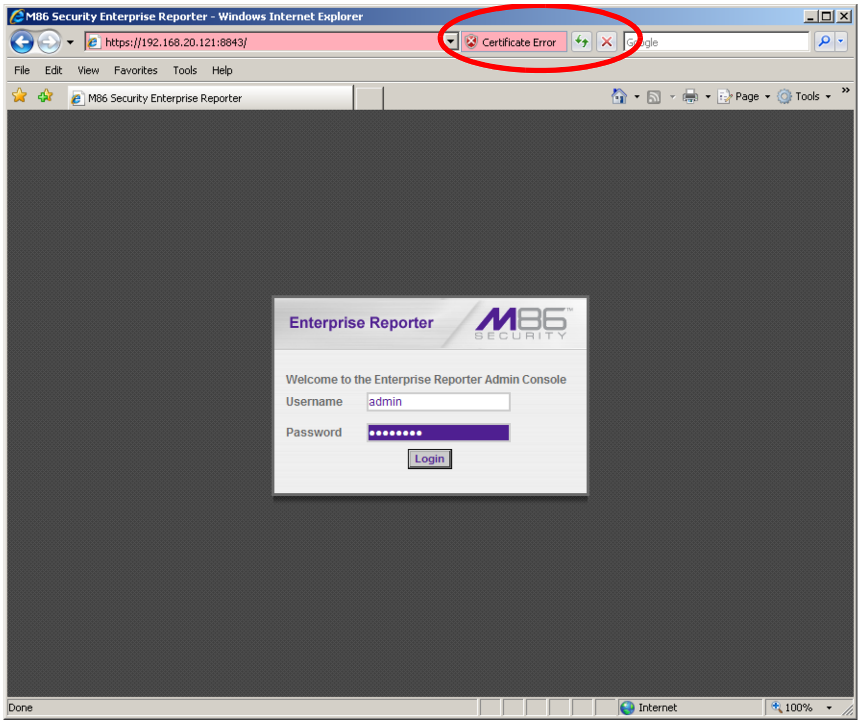
Click here to close this webpage.

Continue to this website (not recommended).

More information

Figure A1: Windows XP, IE 7

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


M86 Security Enterprise Reporter - Windows Internet Explorer
https://192.168.20.121:8843/
Certificate Error
Google
File Edit View Favorites Tools Help
M86 Security Enterprise Reporter
Page
Tools
Enterprise Reporter
M86 SECURITY
Login
Done
Internet
100%

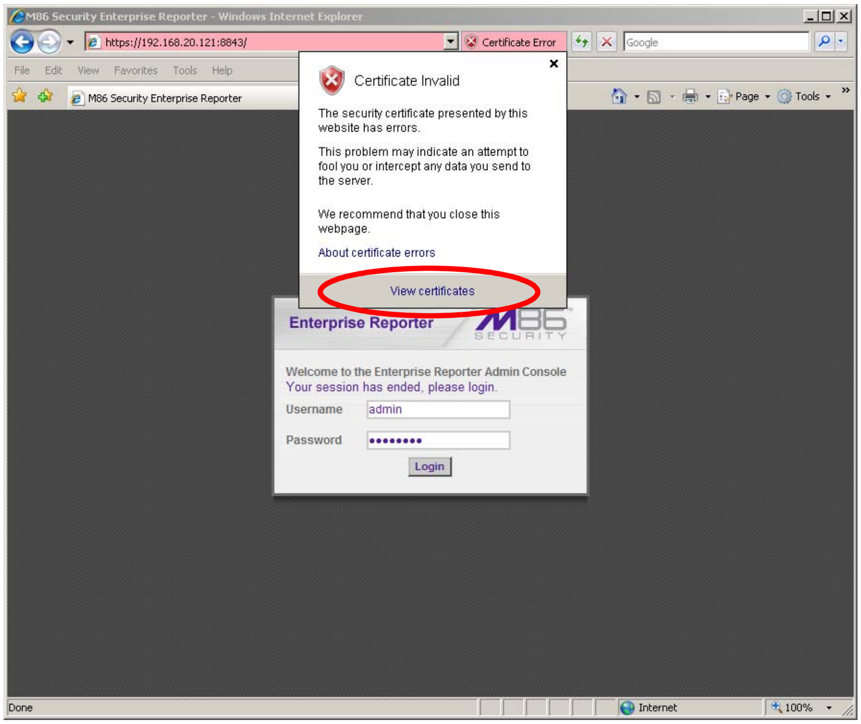
Welcome to the Enterprise Reporter Admin Console

Username admin

Password ••••••••

Figure A2: Windows XP, IE 7

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


M86 Security Enterprise Reporter - Windows Internet Explorer
https://192.168.20.121:8843/
Certificate Error
Google
File Edit View Favorites Tools Help
M86 Security Enterprise Reporter
Page
Tools
View certificates
Enterprise Reporter
M86 SECURITY
Login
Done
Internet
100%

Certificate Invalid

The security certificate presented by this website has errors.

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

We recommend that you close this webpage.

About certificate errors

Welcome to the Enterprise Reporter Admin Console

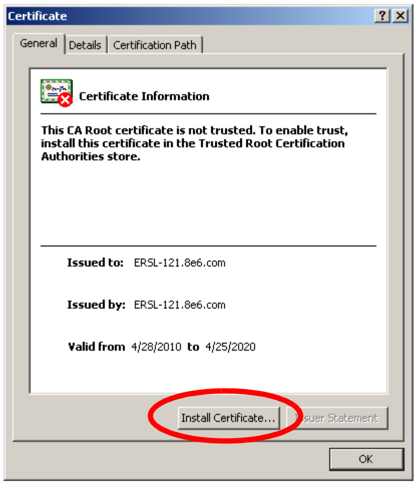
Your session has ended, please login.

Username admin

Password ••••••••

Figure B: Windows XP, IE 7

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



Certificate Information

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

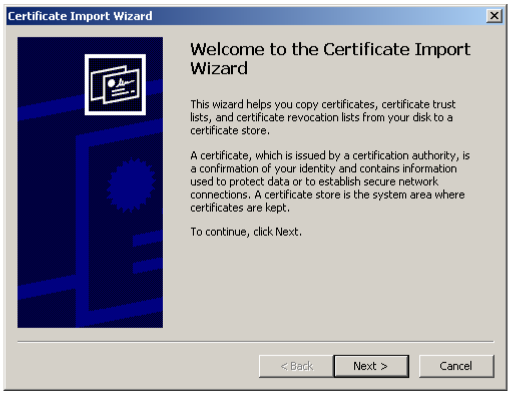
Issued to: ERSL-121.8e6.com

Issued by: ERSL-121.8e6.com

Valid from 4/28/2010 to 4/25/2020

Figure C: Windows XP, IE 7

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



Welcome to the Certificate Import Wizard

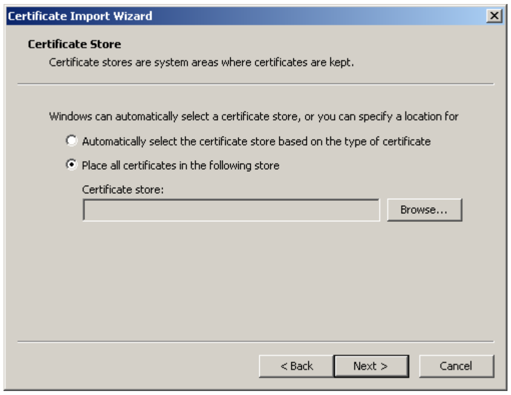
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

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

To continue, click Next.

Figure D: Windows XP, IE 7

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



Certificate Store

Certificate stores are system areas where certificates are kept.

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

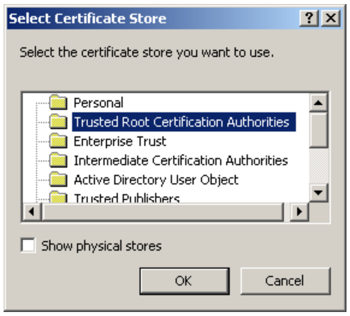
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Figure E: Windows XP, IE 7

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



Select Certificate Store

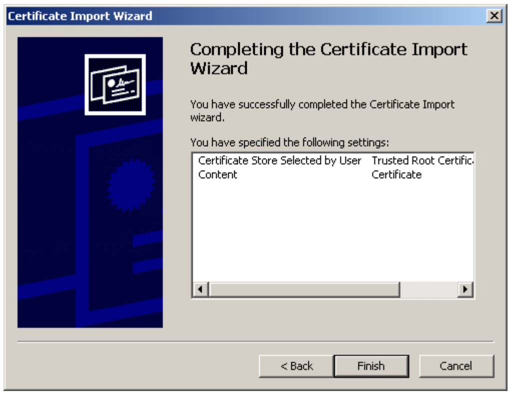
Select the certificate store you want to use.

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Active Directory User Object
- Trusted Publishers

Figure F: Windows XP, IE 7

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

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



Certificate Import Wizard

Completing the Certificate Import Wizard

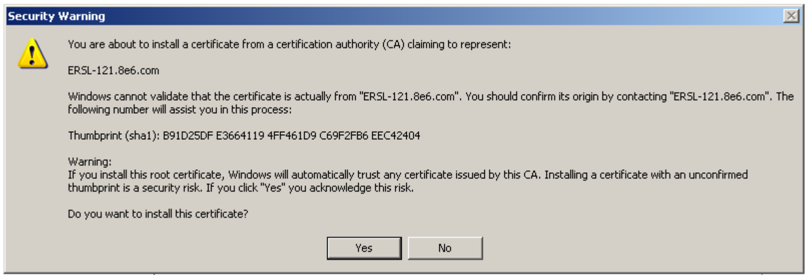
You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certific
Content	Certificate

Figure H: Windows XP, IE 7

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



Security Warning

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

ERSL-121.8e6.com

Windows cannot validate that the certificate is actually from "ERSL-121.8e6.com". You should confirm its origin by contacting "ERSL-121.8e6.com". The following number will assist you in this process:

Thumbprint (sha1): B91D25DF E3664119 4FF461D9 C69F2FB6 EEC42404

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

Do you want to install this certificate?

Figure I: Windows XP, IE 7

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

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

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

Windows 7 with IE 8

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

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

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

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

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

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

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

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

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

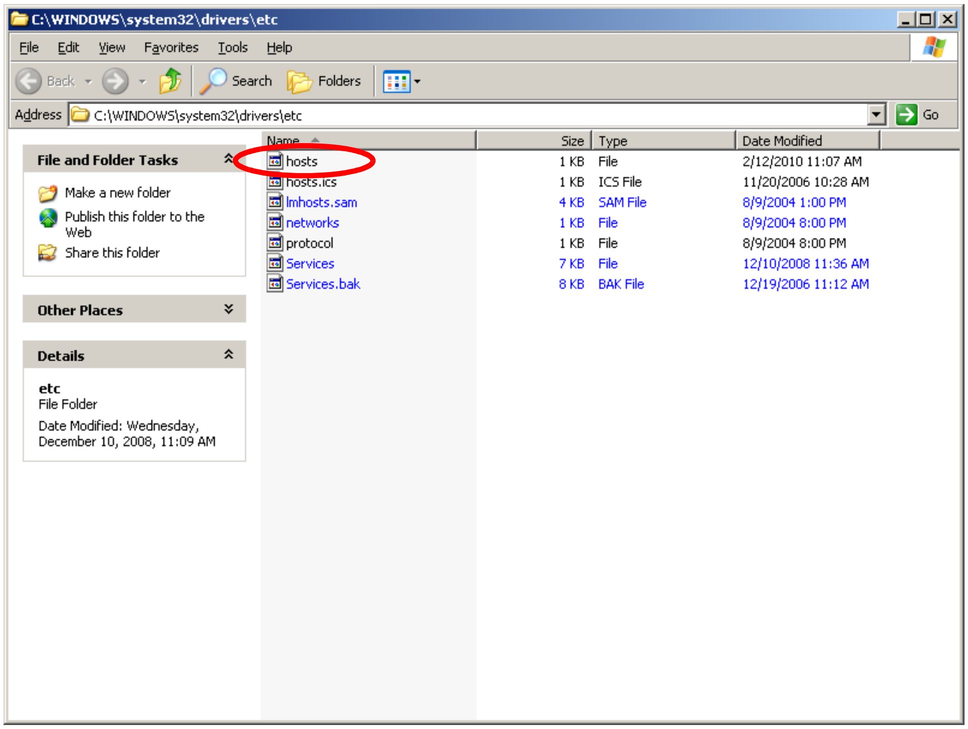
I. Select the Security tab, click **Trusted sites**, and then click **Sites** to open the Trusted sites pop-up box.

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

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

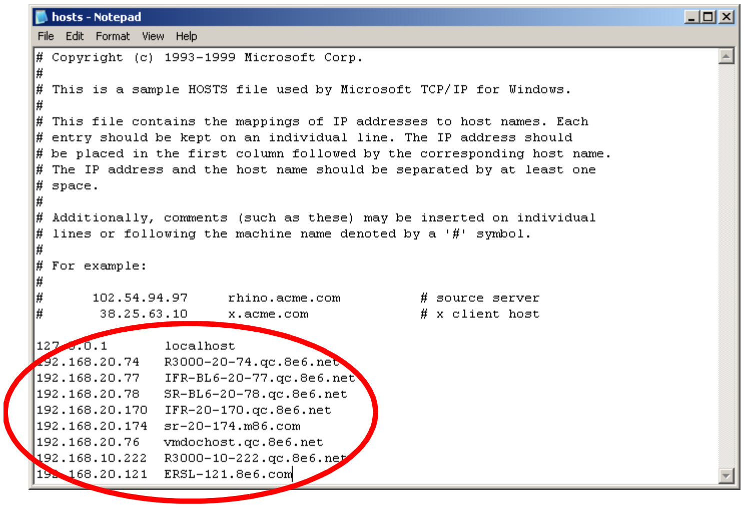
Map the ER’s IP Address to the Server’s Host Name

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


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

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

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



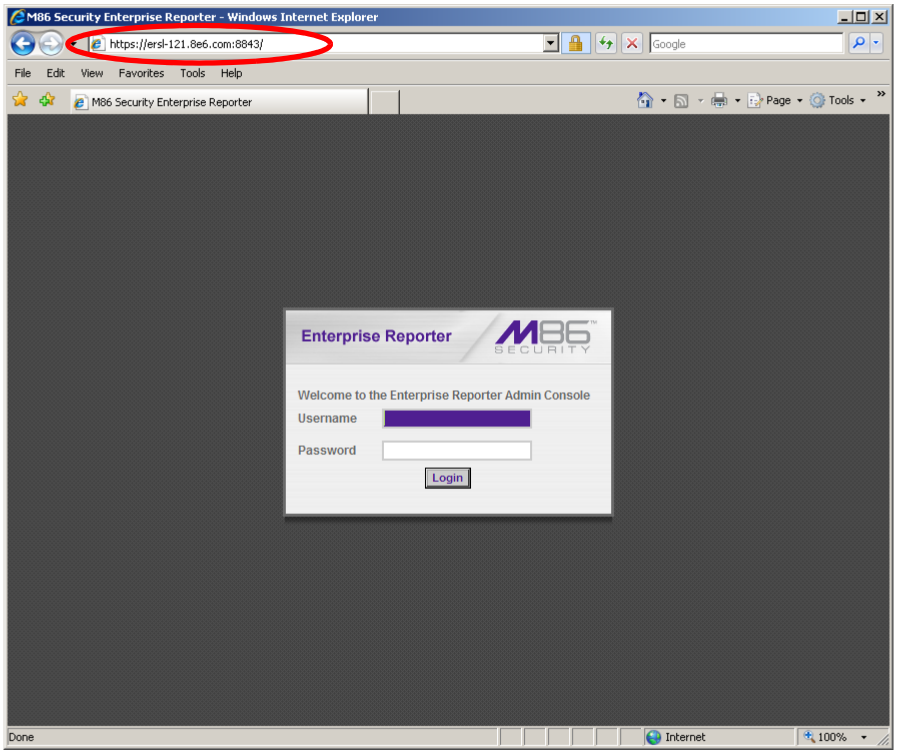
```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the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

127.0.0.1       localhost
192.168.20.74   R3000-20-74.qc.8e6.net
192.168.20.77   IFR-BL6-20-77.qc.8e6.net
192.168.20.78   SR-BL6-20-78.qc.8e6.net
192.168.20.170  IFR-20-170.qc.8e6.net
192.168.20.174  sr-20-174.m86.com
192.168.20.76   vmdochost.qc.8e6.net
192.168.10.222  R3000-10-222.qc.8e6.net
192.168.20.121  ERSL-121.8e6.com
```

C. Enter a line in the hosts file with the ER’s IP address and its host name, 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 ER’s host name instead of its IP address.

For example, **https://hostname:8443/8e6er/** would be used instead of

https://x.x.x.x:8443/8e6er/, and **https://hostname:8843** would be used instead of **https://x.x.x.x:8843**. Click **Go** to open the ER login window:


M86 Security Enterprise Reporter - Windows Internet Explorer
https://ersl-121.8e6.com:8843/
Google
File
Edit
View
Favorites
Tools
Help
M86 Security Enterprise Reporter
Page
Tools
Enterprise Reporter
M86 SECURITY
Username
Password
Login
Done
Internet
100%

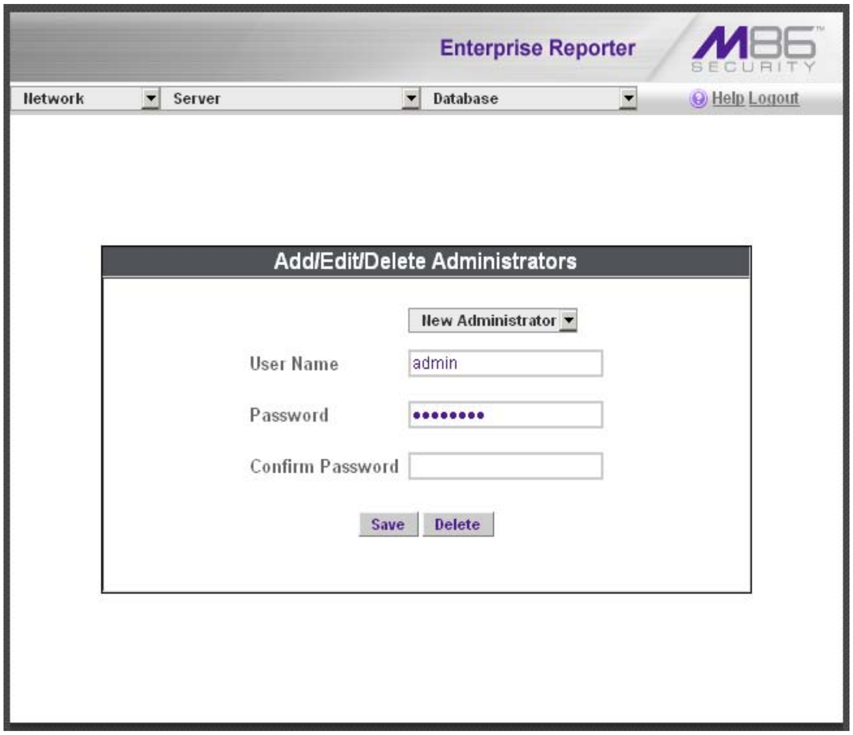
Welcome to the Enterprise Reporter Admin Console

Log in to the user interface and proceed to Step 5.

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

Change User Name and Password

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



User Name: admin

Password: ••••••••

Confirm Password:

B. Select **New Administrators** from the pull-down menu.

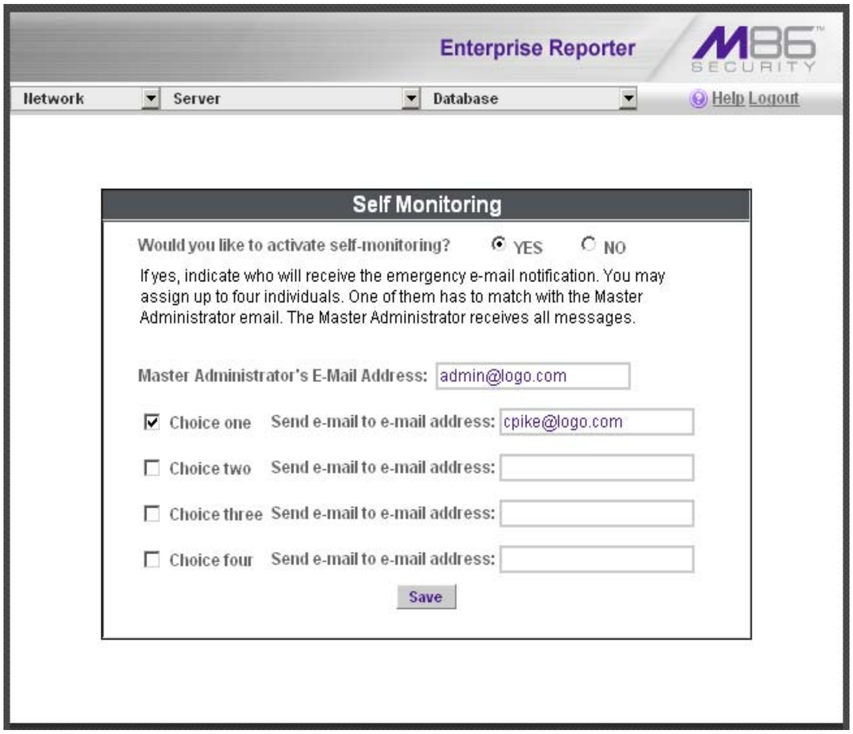
C. Enter a **User Name** and **Password**.

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

E. Click **Save**.

Set Self-Monitoring

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



Self Monitoring

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

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

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

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

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

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

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

B. Choose **YES** to activate monitoring.

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

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

E. Click **Save**.

Step 6: Web Filter Configuration

If you are using M86 Security's Web Filter for your Web-access logging device, this step can be performed any time during ER setup, but must be completed in order for the ER to receive logs from the Web Filter.

A. Access the Administrator console of the Web Filter.

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

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

D. Select **M86 Enterprise Reporter**, and then click **Save**.

E. On the M86 Enterprise Reporter tab, in the **Server** field, enter the LAN 1 IP address you assigned to your ER.

F. Click **Add** to include this IP address in the Remote Server list box. Your Web Filter is now set to transfer its log files to your ER via HTTPS.

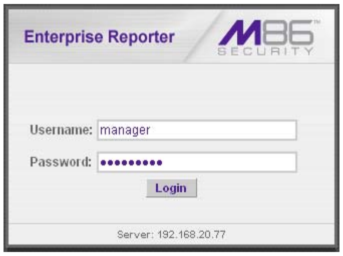
***NOTE**: It is recommended you wait for 1 - 2 hours after the initial installation so sufficient data is available for viewing.*

You can see if log files have transferred by accessing the ER's Administrator console and choosing **Tools** from the Database pull-down menu to display the Tools screen. Choose **File Watch Log** from the Database Status pull-down menu and click **View**. The transfer is working if you see an entry that includes the date, time, and IMPORTING: shadow.log.machine1. The transfer should occur every hour. Once you see an entry, reporting information will be available one hour after the timestamp of the import listing.

Step 7: Launch the ER Client

A. From your workstation, launch a version-supported Internet Explorer, Firefox, or Safari browser window.

B. Enter **https://x.x.x.x:8443/8e6er/** in the address field (in which “x.x.x.x” represents the IP address of the ER server)—or enter **https://hostname:8443/8e6er/** (in which “hostname” represents the host name assigned to the ER server)—and then click Go to access the login window of the ER client:



Username: manager

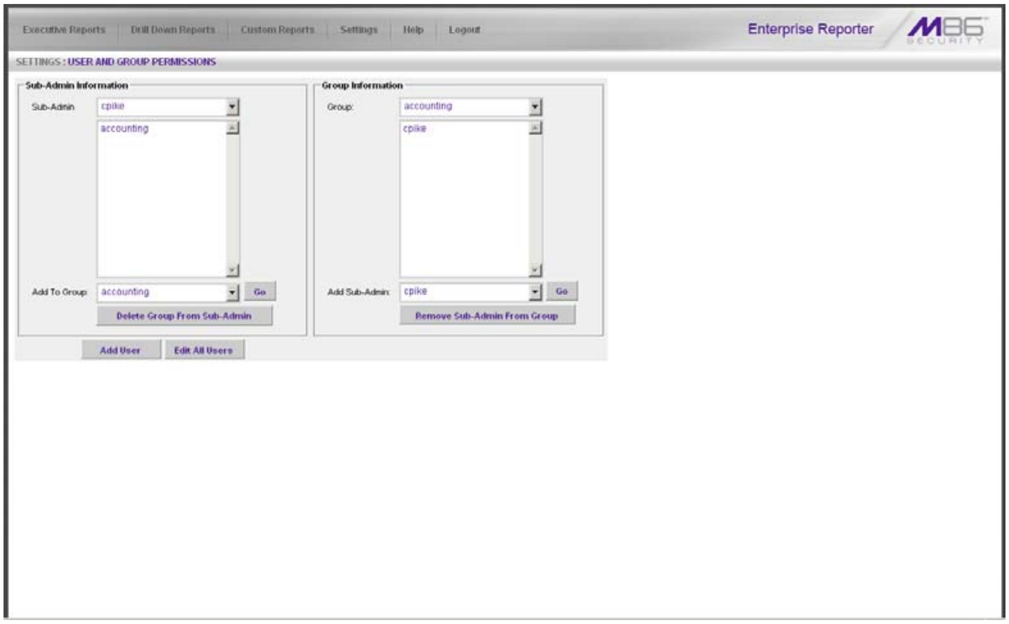
Password: •••••••••

Server: 192.168.20.77

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

***NOTE**: If you do not have your own Username and Password set up in the ER client, the default Username is **manager** and the default Password is 8e6ReporT.*

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



Sub-Admin: cpike

accounting

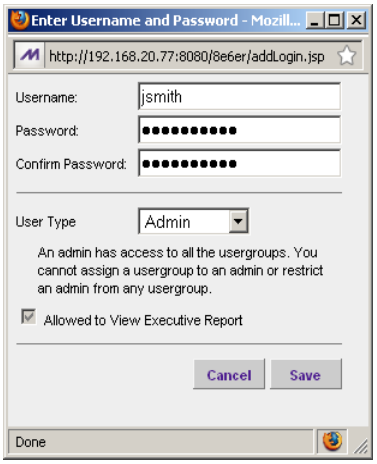
Add To Group: accounting

Group: accounting

cpike

Add Sub-Admin: cpike

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



Enter Username and Password - Mozill...
http://192.168.20.77:8080/8e6er/addLogin.jsp
Cancel
Save
Done

Username: jsmith

Password: ●●●●●●●●●●●

Confirm Password: ●●●●●●●●●●●

User Type: Admin

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

☑ Allowed to View Executive Report

F. Enter the **Username**.

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

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

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

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

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

CONCLUSION

Congratulations; you have completed the ER installation procedures. Now that the ER server is set up on your network and the client can be accessed from your workstation, you will need to be sure the Web-access logging device you are using is sending log files to the ER database. Once the ER database is populated, the client can be used for generating reports.

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

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

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

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

BEST REPORTING PRACTICES

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

You will learn how to:

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

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

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

Reporting Scenarios

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

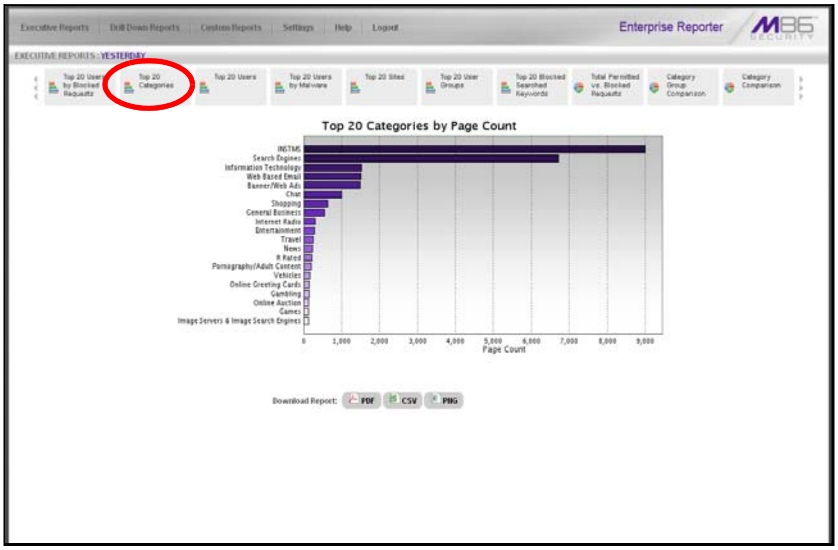
I. Executive Report and Drill Down Report exercise

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

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

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

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



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

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

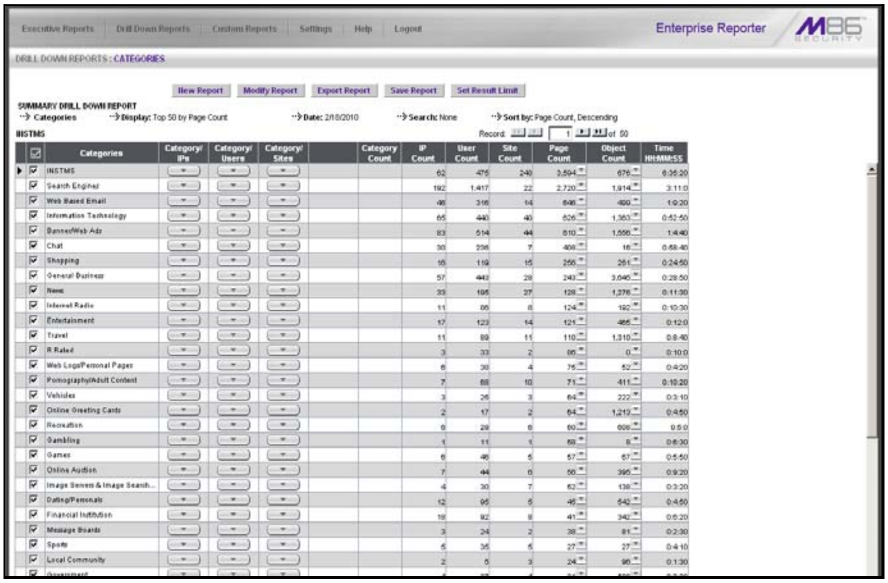
***NOTE**: Click the left or right arrow in the dashboard to view additional thumbnails.*

In the ER Web Client User Guide index, see:
• How to: generate an Executive Report

Step B: Further investigate using a Summary Drill Down Report

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

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



DRILL DOWN REPORTS : CATEGORIES

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

INSTMS

Record: 1 of 50

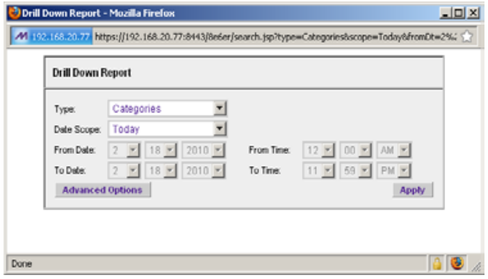
☑	Categories	Category/ IPs	Category/ Users	Category/ Sites		Category Count	IP Count	User Count	Site Count	Page Count	Object Count	Time HH:MM:SS
☑	INSTMS	▾	▾	▾			62	475	240	3,594	676	6:35:20
☑	Search Engines	▾	▾	▾			192	1,417	22	2,720	1,914	3:11:0
☑	Web Based Email	▾	▾	▾			46	316	14	646	490	1:9:20
☑	Information Technology	▾	▾	▾			65	440	40	626	1,363	0:52:50
☑	Banner/Web Ads	▾	▾	▾			83	514	44	610	1,556	1:4:40
☑	Chat	▾	▾	▾			30	236	7	408	16	0:58:40
☑	Shopping	▾	▾	▾			16	119	15	256	261	0:24:50
☑	General Business	▾	▾	▾			57	442	28	243	3,046	0:28:50
☑	News	▾	▾	▾			33	195	27	128	1,276	0:11:30
☑	Internet Radio	▾	▾	▾			11	66	6	124	192	0:10:30
☑	Entertainment	▾	▾	▾			17	123	14	121	465	0:12:0
☑	Travel	▾	▾	▾			11	89	11	110	1,310	0:8:40
☑	R Rated	▾	▾	▾			3	33	2	86	0	0:10:0
☑	Web Logs/Personal Pages	▾	▾	▾			6	38	4	76	52	0:4:20
☑	Pornography/Adult Content	▾	▾	▾			7	68	10	71	411	0:10:20
☑	Vehicles	▾	▾	▾			3	26	3	64	222	0:3:10
☑	Online Greeting Cards	▾	▾	▾			2	17	2	64	1,213	0:4:50
☑	Recreation	▾	▾	▾			6	29	6	60	606	0:5:0
☑	Gambling	▾	▾	▾			1	11	1	58	8	0:6:30
☑	Games	▾	▾	▾			6	46	5	57	67	0:5:50
☑	Online Auction	▾	▾	▾			7	44	6	56	395	0:9:20
☑	Image Servers & Image Search...	▾	▾	▾			4	30	7	62	138	0:3:20
☑	Dating/Personals	▾	▾	▾			12	95	5	46	542	0:4:50
☑	Financial Institution	▾	▾	▾			18	92	8	41	342	0:6:20
☑	Message Boards	▾	▾	▾			3	24	2	38	81	0:2:30
☑	Sports	▾	▾	▾			5	35	5	27	27	0:4:10
☑	Local Community	▾	▾	▾			2	6	3	24	96	0:1:30
☑	Government	▾	▾	▾			[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

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

In the ER Web Client User Guide index, see:
• How to: generate a Drill Down Report

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

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


Drill Down Report - Mozilla Firefox
192.168.20.77
https://192.168.20.77:8443/8e6er/search.jsp?type=Categories&scope=Today&fromDt=2%
Advanced Options
Apply
Done

Drill Down Report

Type: Categories

Date Scope: Today

From Date: 2 18 2010 From Time: 12 00 AM

To Date: 2 18 2010 To Time: 11 59 PM

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

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

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

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

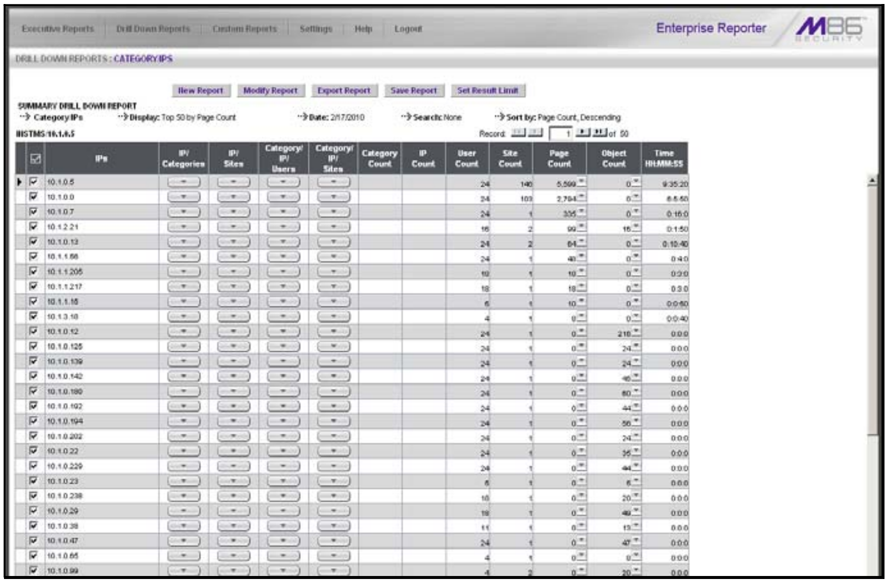
1. To continue this exercise, select the record for the category you wish to further investigate.

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

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

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

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



DRILL DOWN REPORTS : CATEGORY/IPS

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

INSTMS/10.1.0.5   Record: 1 of 50

	☑	IPs	IP/ Categories	IP/ Sites	Category/ IP/ Users	Category/ IP/ Sites	Category Count	IP Count	User Count	Site Count	Page Count	Object Count	Time HH:MM:SS
▶	☑	10.1.0.5	▾	▾	▾	▾			24	140	5,599	0	9:35:20
	☑	10.1.0.0	▾	▾	▾	▾			24	103	2,794	0	6:5:50
	☑	10.1.0.7	▾	▾	▾	▾			24	1	335	0	0:16:0
	☑	10.1.2.21	▾	▾	▾	▾			16	2	99	16	0:1:50
	☑	10.1.0.13	▾	▾	▾	▾			24	2	64	0	0:10:40
	☑	10.1.1.66	▾	▾	▾	▾			24	1	40	0	0:4:0
	☑	10.1.1.205	▾	▾	▾	▾			10	1	10	0	0:3:0
	☑	10.1.1.217	▾	▾	▾	▾			18	1	18	0	0:3:0
	☑	10.1.1.16	▾	▾	▾	▾			6	1	10	0	0:0:50
	☑	10.1.3.18	▾	▾	▾	▾			4	1	0	0	0:0:40
	☑	10.1.0.12	▾	▾	▾	▾			24	1	0	216	0:0:0
	☑	10.1.0.125	▾	▾	▾	▾			24	1	0	24	0:0:0
	☑	10.1.0.139	▾	▾	▾	▾			24	1	0	24	0:0:0
	☑	10.1.0.142	▾	▾	▾	▾			24	1	0	46	0:0:0
	☑	10.1.0.180	▾	▾	▾	▾			24	1	0	60	0:0:0
	☑	10.1.0.192	▾	▾	▾	▾			24	1	0	44	0:0:0
	☑	10.1.0.194	▾	▾	▾	▾			24	1	0	56	0:0:0
	☑	10.1.0.202	▾	▾	▾	▾			24	1	0	24	0:0:0
	☑	10.1.0.22	▾	▾	▾	▾			24	1	0	36	0:0:0
	☑	10.1.0.229	▾	▾	▾	▾			24	1	0	44	0:0:0
	☑	10.1.0.23	▾	▾	▾	▾			6	1	0	6	0:0:0
	☑	10.1.0.238	▾	▾	▾	▾			16	1	0	20	0:0:0
	☑	10.1.0.29	▾	▾	▾	▾			18	1	0	48	0:0:0
	☑	10.1.0.38	▾	▾	▾	▾			11	1	0	13	0:0:0
	☑	10.1.0.47	▾	▾	▾	▾			24	1	0	47	0:0:0
	☑	10.1.0.65	▾	▾	▾	▾			4	1	0	0	0:0:0
	☑	10.1.0.99	▾	▾	▾	▾			4	2	0	20	0:0:0

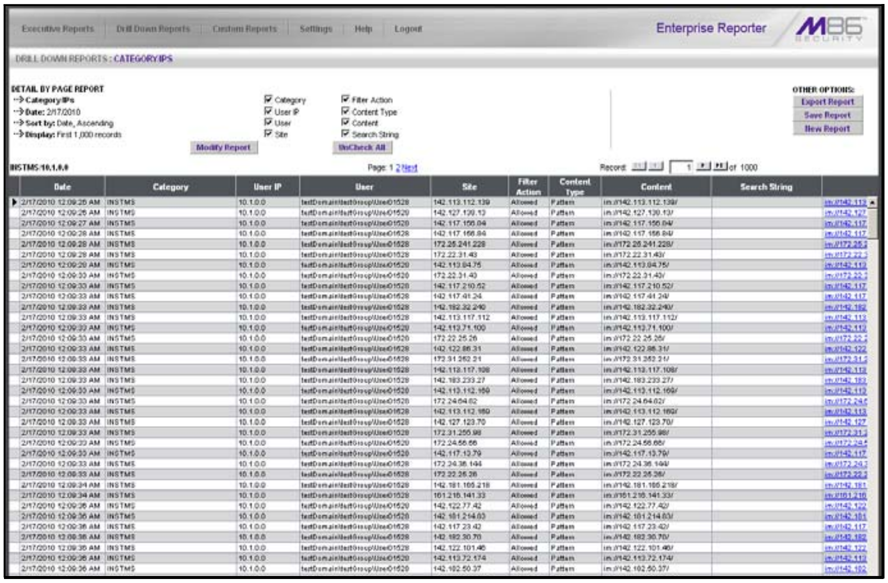
   After executing the last command, note that user IP addresses now display in the first column of the report view instead of categories.

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

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

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

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



DRILL DOWN REPORTS : CATEGORY:IPS

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

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

INSTMS:10.1.0.0

Page: 1 2 Next

Record: 1 of 1000

Date	Category	User IP	User	Site	Filter Action	Content Type	Content	Search String	
2/17/2010 12:09:26 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.113.112.139	Allowed	Pattern	im://142.113.112.139/		im://142.113
2/17/2010 12:09:26 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.127.130.13	Allowed	Pattern	im://142.127.130.13/		im://142.127
2/17/2010 12:09:27 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.117.156.04	Allowed	Pattern	im://142.117.156.04/		im://142.117
2/17/2010 12:09:28 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.117.156.84	Allowed	Pattern	im://142.117.156.84/		im://142.117
2/17/2010 12:09:28 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	172.25.241.228	Allowed	Pattern	im://172.25.241.228/		im://172.25.2
2/17/2010 12:09:28 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	172.22.31.43	Allowed	Pattern	im://172.22.31.43/		im://172.22.3
2/17/2010 12:09:29 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.113.84.75	Allowed	Pattern	im://142.113.84.75/		im://142.113
2/17/2010 12:09:30 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	172.22.31.40	Allowed	Pattern	im://172.22.31.40/		im://172.22.3
2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.117.210.52	Allowed	Pattern	im://142.117.210.52/		im://142.117
2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.117.41.24	Allowed	Pattern	im://142.117.41.24/		im://142.117
2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.182.32.240	Allowed	Pattern	im://142.182.32.240/		im://142.182
2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.113.117.112	Allowed	Pattern	im://142.113.117.112/		im://142.113
2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.113.71.100	Allowed	Pattern	im://142.113.71.100/		im://142.113
2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	172.22.25.26	Allowed	Pattern	im://172.22.25.26/		im://172.22.2
2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.122.86.31	Allowed	Pattern	im://142.122.86.31/		im://142.122
2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	172.31.252.21	Allowed	Pattern	im://172.31.252.21/		im://172.31.2
2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.113.117.108	Allowed	Pattern	im://142.113.117.108/		im://142.113
2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.183.233.27	Allowed	Pattern	im://142.183.233.27/		im://142.183
2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.113.112.169	Allowed	Pattern	im://142.113.112.169/		im://142.113
2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	172.24.64.62	Allowed	Pattern	im://172.24.64.62/		im://172.24.6
2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.113.112.160	Allowed	Pattern	im://142.113.112.160/		im://142.113
2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.127.123.70	Allowed	Pattern	im://142.127.123.70/		im://142.127
2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	172.31.255.98	Allowed	Pattern	im://172.31.255.98/		im://172.31.2
2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	172.24.56.66	Allowed	Pattern	im://172.24.56.66/		im://172.24.5
2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.117.13.79	Allowed	Pattern	im://142.117.13.79/		im://142.117
2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	172.24.36.144	Allowed	Pattern	im://172.24.36.144/		im://172.24.3
2/17/2010 12:09:33 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	172.22.26.26	Allowed	Pattern	im://172.22.26.26/		im://172.22.2
2/17/2010 12:09:34 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.181.165.218	Allowed	Pattern	im://142.181.165.218/		im://142.181
2/17/2010 12:09:34 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	161.216.141.33	Allowed	Pattern	im://161.216.141.33/		im://161.216
2/17/2010 12:09:36 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.122.77.42	Allowed	Pattern	im://142.122.77.42/		im://142.122
2/17/2010 12:09:36 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.181.214.03	Allowed	Pattern	im://142.181.214.03/		im://142.181
2/17/2010 12:09:36 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.117.23.42	Allowed	Pattern	im://142.117.23.42/		im://142.117
2/17/2010 12:09:36 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.182.30.70	Allowed	Pattern	im://142.182.30.70/		im://142.182
2/17/2010 12:09:36 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.122.101.46	Allowed	Pattern	im://142.122.101.46/		im://142.122
2/17/2010 12:09:36 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.113.72.174	Allowed	Pattern	im://142.113.72.174/		im://142.113
2/17/2010 12:09:36 AM	INSTMS	10.1.0.0	testDomain\testGroup\User01528	142.182.50.37	Allowed	Pattern	im://142.182.50.37/		im://142.182

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

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

In the ER Web Client User Guide index, see:
- *How to: create a detail Page Count report from a summary report*

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

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

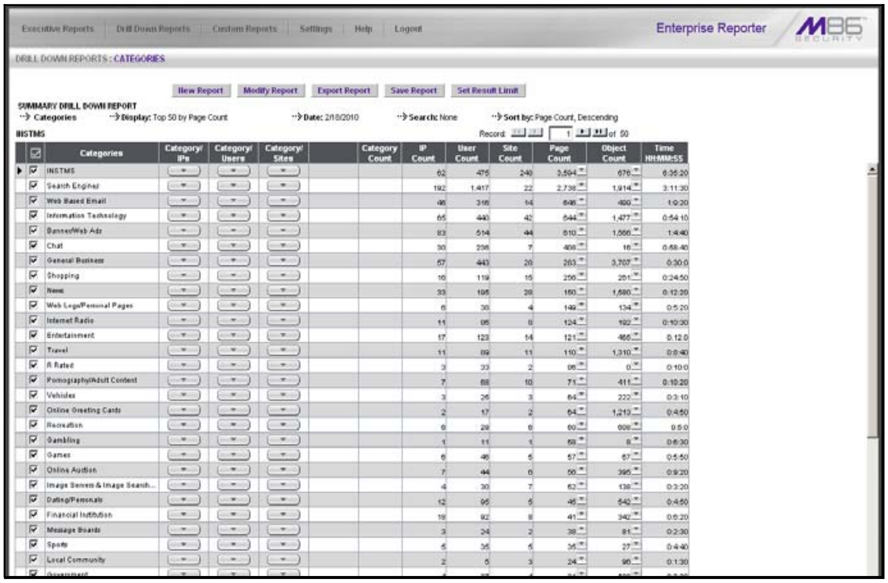
These tools and other tools can be used separately or combined to create many different types of reports to fulfill different purposes.

II. Double-break Report and Export Report exercise

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

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

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



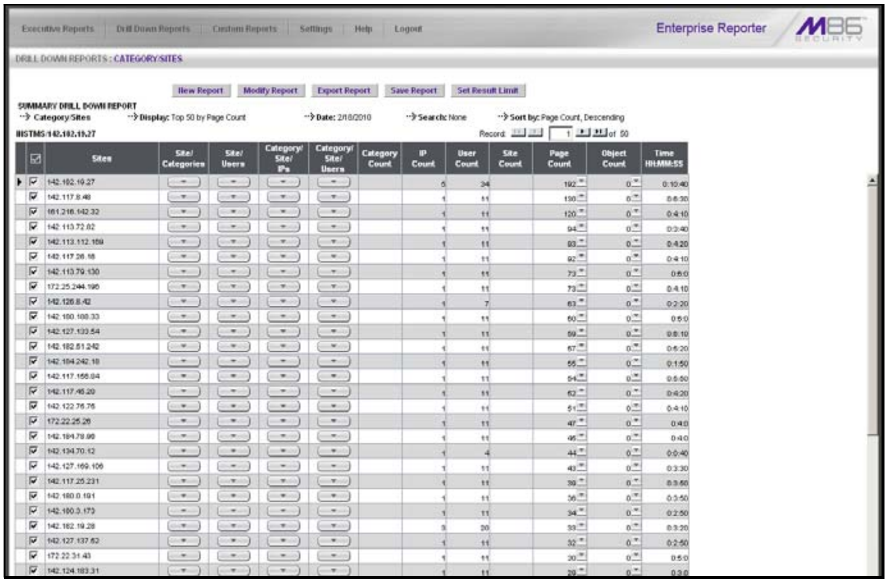
DRILL DOWN REPORTS : CATEGORIES

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

INSTMS   Record 1 of 50

☑	Categories	Category/ IPs	Category/ Users	Category/ Sites		Category Count	IP Count	User Count	Site Count	Page Count	Object Count	Time HH:MM:SS
☑	INSTMS	▾	▾	▾			62	475	240	3,594	676	6:35:20
☑	Search Engines	▾	▾	▾			192	1,417	22	2,738	1,914	3:11:30
☑	Web Based Email	▾	▾	▾			46	316	14	646	400	1:9:20
☑	Information Technology	▾	▾	▾			65	440	42	644	1,477	0:54:10
☑	Banner/Web Ads	▾	▾	▾			83	514	44	610	1,566	1:4:40
☑	Chat	▾	▾	▾			30	236	7	408	16	0:58:40
☑	General Business	▾	▾	▾			57	443	20	263	3,707	0:30:0
☑	Shopping	▾	▾	▾			16	119	15	256	251	0:24:50
☑	News	▾	▾	▾			33	195	29	160	1,680	0:12:20
☑	Web Logs/Personal Pages	▾	▾	▾			6	30	4	149	134	0:5:20
☑	Internet Radio	▾	▾	▾			11	95	8	124	192	0:10:30
☑	Entertainment	▾	▾	▾			17	123	14	121	466	0:12:0
☑	Travel	▾	▾	▾			11	89	11	110	1,310	0:0:40
☑	R Rated	▾	▾	▾			3	33	2	96	0	0:10:0
☑	Pornography/Adult Content	▾	▾	▾			7	68	10	71	411	0:10:20
☑	Vehicles	▾	▾	▾			3	26	3	64	222	0:3:10
☑	Online Greeting Cards	▾	▾	▾			2	17	2	64	1,219	0:4:50
☑	Recreation	▾	▾	▾			6	29	6	60	608	0:5:0
☑	Gambling	▾	▾	▾			1	11	1	58	8	0:6:30
☑	Games	▾	▾	▾			6	46	5	57	67	0:5:50
☑	Online Auction	▾	▾	▾			7	44	6	56	395	0:9:20
☑	Image Servers & Image Search...	▾	▾	▾			4	30	7	52	138	0:3:20
☑	Dating/Personals	▾	▾	▾			12	95	5	46	542	0:4:50
☑	Financial Institution	▾	▾	▾			19	92	8	41	342	0:6:20
☑	Message Boards	▾	▾	▾			3	24	2	38	81	0:2:30
☑	Sports	▾	▾	▾			5	35	5	36	27	0:4:40
☑	Local Community	▾	▾	▾			2	5	3	24	96	0:1:30

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



DRILL DOWN REPORTS : CATEGORY/SITES

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

INSTMS/142.192.19.27   Record 1 of 50

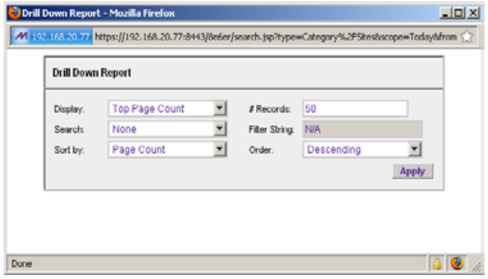
☑	Sites	Site/ Categories	Site/ Users	Category/ Site/ IPs	Category/ Site/ Users	Category Count	IP Count	User Count	Site Count	Page Count	Object Count	Time HH:MM:SS
☑	142.192.19.27	▾	▾	▾	▾		5	34		192	0	0:10:40
☑	142.117.8.48	▾	▾	▾	▾		1	11		130	0	0:6:30
☑	161.216.142.32	▾	▾	▾	▾		1	11		120	0	0:4:10
☑	142.113.72.82	▾	▾	▾	▾		1	11		94	0	0:3:40
☑	142.113.112.169	▾	▾	▾	▾		1	11		93	0	0:4:20
☑	142.117.26.18	▾	▾	▾	▾		1	11		92	0	0:4:10
☑	142.113.79.130	▾	▾	▾	▾		1	11		73	0	0:6:0
☑	172.25.244.195	▾	▾	▾	▾		1	11		73	0	0:4:10
☑	142.126.8.42	▾	▾	▾	▾		1	7		63	0	0:2:20
☑	142.180.180.33	▾	▾	▾	▾		1	11		60	0	0:6:0
☑	142.127.133.54	▾	▾	▾	▾		1	11		59	0	0:8:10
☑	142.182.51.242	▾	▾	▾	▾		1	11		57	0	0:6:20
☑	142.184.242.18	▾	▾	▾	▾		1	11		55	0	0:1:50
☑	142.117.156.84	▾	▾	▾	▾		1	11		54	0	0:5:50
☑	142.117.46.20	▾	▾	▾	▾		1	11		52	0	0:4:20
☑	142.122.76.76	▾	▾	▾	▾		1	11		51	0	0:4:10
☑	172.22.25.26	▾	▾	▾	▾		1	11		47	0	0:4:0
☑	142.184.78.96	▾	▾	▾	▾		1	11		46	0	0:4:0
☑	142.134.70.12	▾	▾	▾	▾		1	4		44	0	0:0:40
☑	142.127.169.106	▾	▾	▾	▾		1	11		43	0	0:3:30
☑	142.117.25.231	▾	▾	▾	▾		1	11		38	0	0:3:50
☑	142.180.0.191	▾	▾	▾	▾		1	11		36	0	0:3:50
☑	142.180.3.173	▾	▾	▾	▾		1	11		34	0	0:2:50
☑	142.182.19.28	▾	▾	▾	▾		3	20		33	0	0:3:20
☑	142.127.137.62	▾	▾	▾	▾		1	11		32	0	0:2:50
☑	172.22.31.43	▾	▾	▾	▾		1	11		30	0	0:5:0
☑	142.124.183.31	▾	▾	▾	▾		1	11		29	0	0:3:0

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

In the ER Web Client User Guide index, see:
• How to: generate a Drill Down Report
• How to: use filter columns and buttons

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

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



Drill Down Report - Mozilla Firefox

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

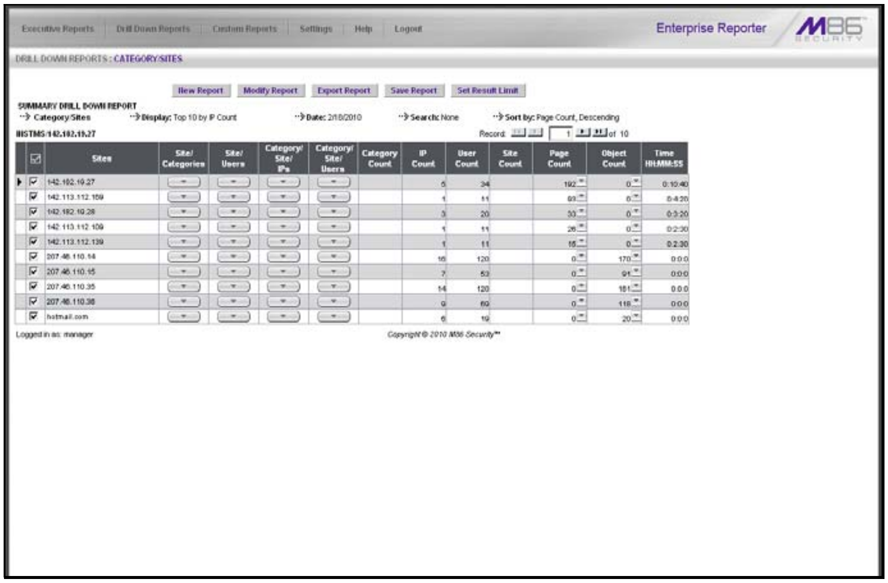
Drill Down Report

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

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

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

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



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

IISTMS/142.192.19.27 Record: 1 of 10

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

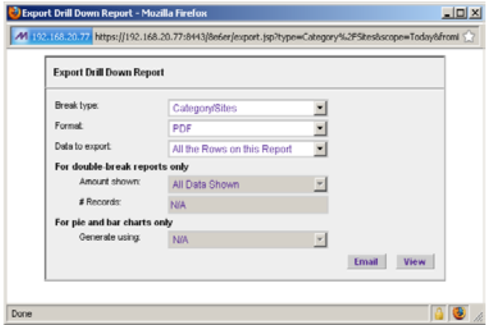
Logged in as: manager

Copyright © 2010 M86 Security™

In the ER Web Client User Guide index, see:
• How to: modify a Drill Down Report
• How to: display only a specified number of records

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

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



Export Drill Down Report - Mozilla Firefox

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

Export Drill Down Report

Break type: Category/Sites

Format: PDF

Data to export: All the Rows on this Report

For double-break reports only

Amount shown: All Data Shown

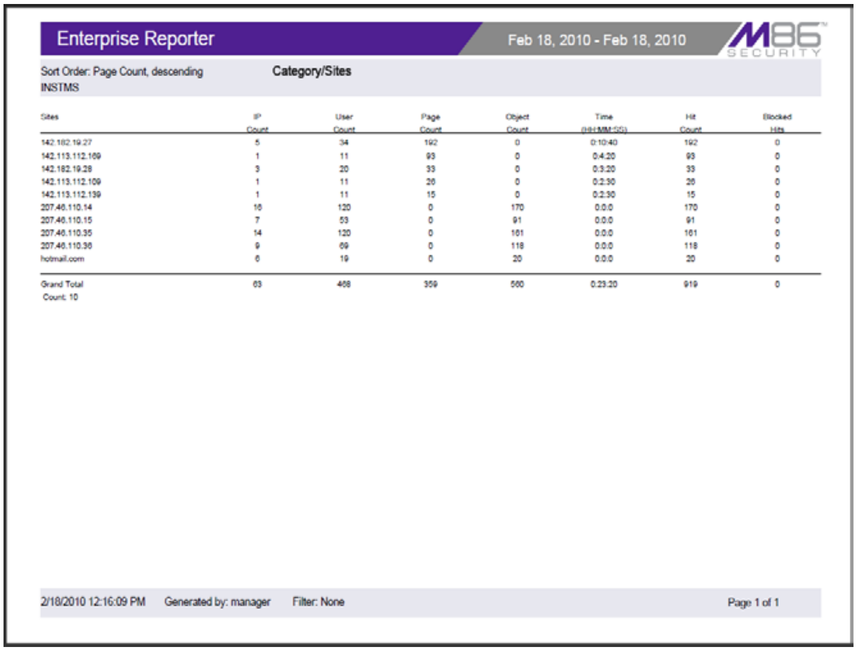
Records: N/A

For pie and bar charts only

Generate using: N/A

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

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



Enterprise Reporter

Feb 18, 2010 - Feb 18, 2010

Sort Order: Page Count, descending
INSTMS

Category/Sites

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

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

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

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

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

In the ER Web Client User Guide index, see:
• How to: export a summary Drill Down Report
• How to: view and print a Web Client report

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

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

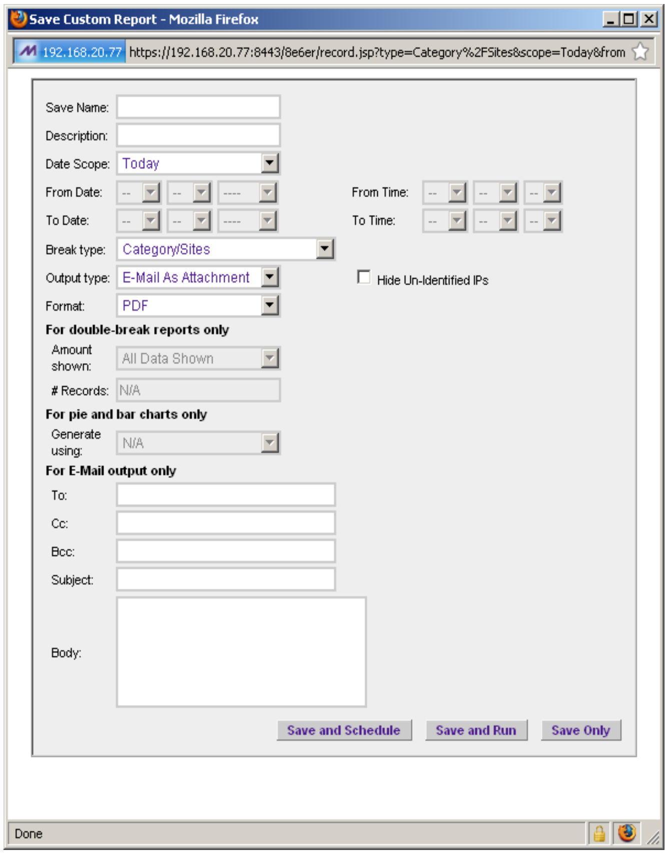
Variations of this exercise can be performed to generate and export countless reports using criteria of your specifications.

III. Save and schedule a report exercise

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

Step A. Save a report

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



Save Custom Report - Mozilla Firefox

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

Save Name:

Description:

Date Scope: Today

From Date: -- -- ----

From Time: -- -- --

To Date: -- -- ----

To Time: -- -- --

Break type: Category/Sites

Output type: E-Mail As Attachment

□ Hide Un-Identified IPs

Format: PDF

For double-break reports only

Amount shown: All Data Shown

Records: N/A

For pie and bar charts only

Generate using: N/A

For E-Mail output only

To:

Cc:

Bcc:

Subject:

Body:

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

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

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

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

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

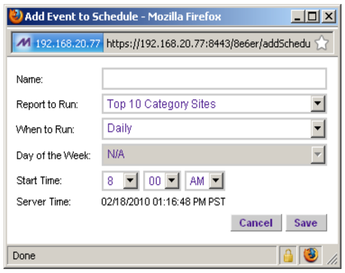
In the ER Web Client User Guide index, see:
• How to: save a custom report

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

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

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

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

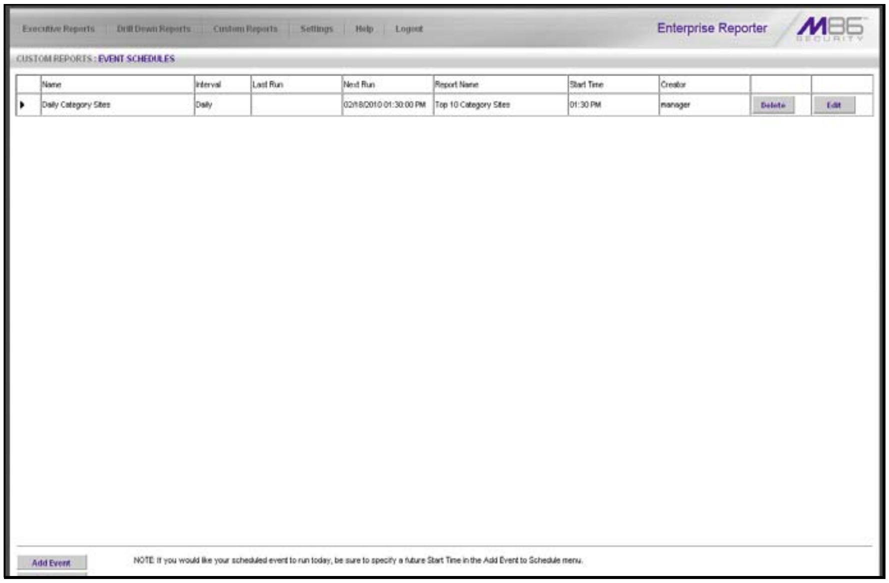


Add Event to Schedule - Mozilla Firefox

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

Name:
Report to Run: Top 10 Category Sites
When to Run: Daily
Day of the Week: N/A
Start Time: 8 00 AM
Server Time: 02/18/2010 01:16:48 PM PST

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



CUSTOM REPORTS : EVENT SCHEDULES

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

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

In the ER Web Client User Guide index, see:
• How to: schedule a report to run

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

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

IV. Create a custom category group and generate reports

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

Step A: Create a custom category group

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

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

Step B: Run a report for a specified category group

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

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

V. Create a custom user group and generate reports

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

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

Step A: Create a custom user group

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

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

Step B: Generate a report for a custom user group

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

Summary Report

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

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

Detail Report

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

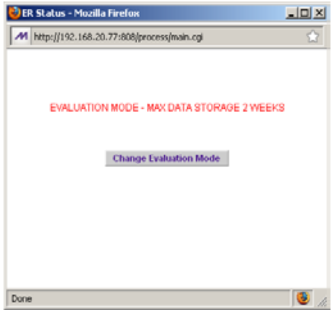
In the ER Web Client User Guide index, see:
• How to: generate a custom Web Client report
• How to: generate a Single User Group Report

IMPORTANT INFORMATION ABOUT USING THE ER IN THE EVALUATION MODE

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

Evaluation Mode Pop-Ups

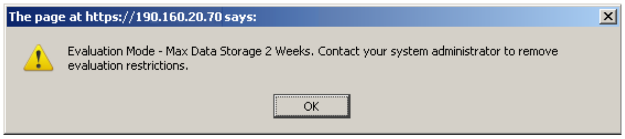
When evaluating the ER in the evaluation mode, the ER Status pop-up box opens after logging in to the ER Administrator console:


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

EVALUATION MODE - MAX DATA STORAGE 2 WEEKS

ER Status pop-up box

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



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

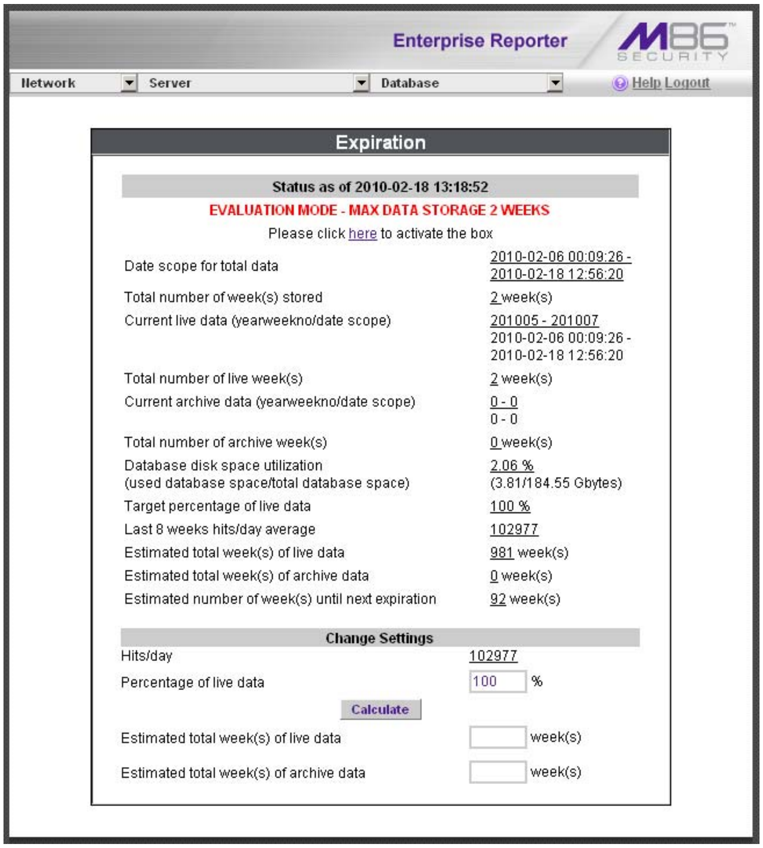
Click **OK** to close this alert pop-up box.

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

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

Administrator Console, Expiration Screen

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



Expiration

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

EVALUATION MODE - MAX DATA STORAGE 2 WEEKS

Please click here to activate the box

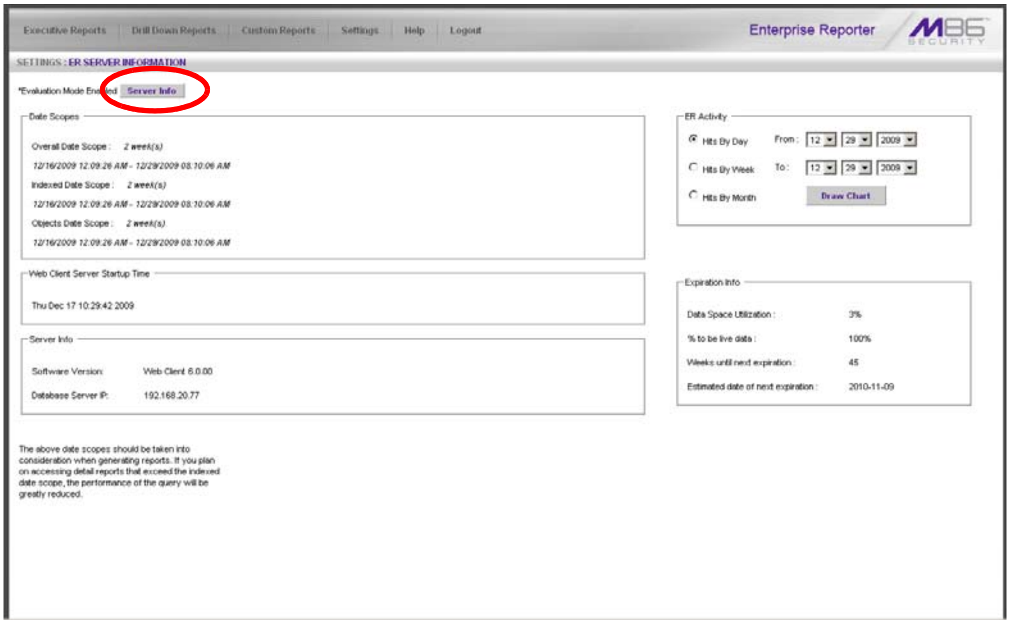
Date scope for total data	2010-02-06 00:09:26 - 2010-02-18 12:56:20
Total number of week(s) stored	2 week(s)
Current live data (yearweekno/date scope)	201005 - 201007 2010-02-06 00:09:26 - 2010-02-18 12:56:20
Total number of live week(s)	2 week(s)
Current archive data (yearweekno/date scope)	0 - 0 0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

Change Settings

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

ER Web Client, ER Server Information Window

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



SETTINGS : ER SERVER INFORMATION

*Evaluation Mode Enabled

Date Scopes

Overall Date Scope : *2 week(s)*
12/16/2009 12:09:26 AM - 12/29/2009 08:10:06 AM
Indexed Date Scope : *2 week(s)*
12/16/2009 12:09:26 AM - 12/29/2009 08:10:06 AM
Objects Date Scope : *2 week(s)*
12/16/2009 12:09:26 AM - 12/29/2009 08:10:06 AM

Web Client Server Startup Time

Thu Dec 17 10:29:42 2009

Server Info

Software Version: Web Client 6.0.00
Database Server IP: 192.168.20.77

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

ER Activity

● Hits By Day From : 12 29 2009
○ Hits By Week To : 12 29 2009
○ Hits By Month

Expiration Info

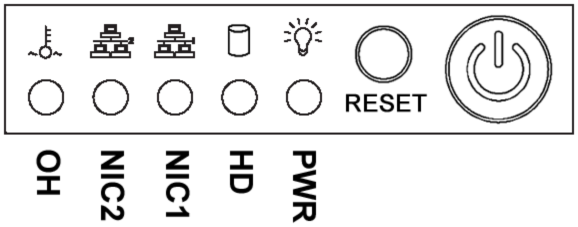
Data Space Utilization :	3%
% to be live data :	100%
Weeks until next expiration :	45
Estimated date of next expiration :	2010-11-09

LED INDICATORS AND BUTTONS

SL Unit

Front LED Indicators and Buttons for Hardware Status Monitoring

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



LED Indicator Key

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

SL chassis control panel

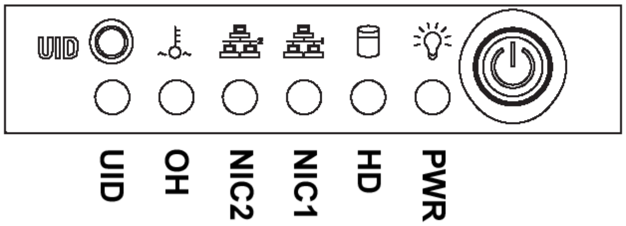
LED indicators alert you to the status of a feature on the unit while buttons let you perform a function on the unit.

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

HL Unit

Front LED Indicators and Buttons for Hardware Status Monitoring

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



LED Indicator Key

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

HL chassis control panel

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

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

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

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

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

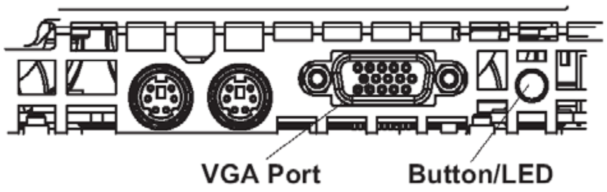
HDD (icon) – In addition to displaying in the control panel, this icon also displays on the front panel on each hard drive carrier. A green LED indicates hard drive activity. An unlit LED on a drive carrier may indicate a hard drive failure.

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

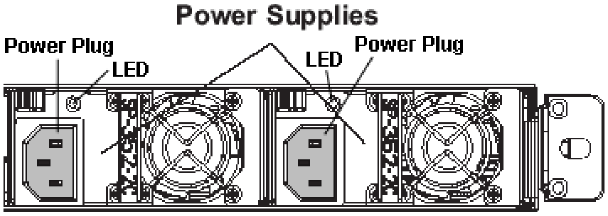
Power (button) – When the power button is pressed, the main power to the server is turned on. When the power button is pressed again, the main power to the server is removed but standby power is still supplied to the server.

Rear LED Indicators for Hardware Status Monitoring

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



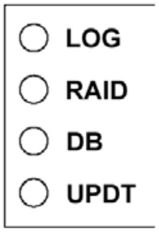
Power Supplies (LED indicators) – The power supplies are located at the right on the rear of the chassis. An LED indicator is located above each of the power plugs.



HL and SL Units

Front LED Indicators for Software and Hardware Status Monitoring

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



LED Indicator Key

LOG = Log Download Status
RAID = Hard Drive Status
DB = Database Status
UPDT = Software Update Status

left side of the front panel

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

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

REGULATORY SPECIFICATIONS AND DISCLAIMERS

Declaration of the Manufacturer or Importer

Safety Compliance

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

Electromagnetic Compatibility (EMC)

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

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

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

FCC Declaration of Conformity

Models: SL-002-002, HL-002-002, HL-022-002, HL-002-006, HL-022-006

Electromagnetic Compatibility Class A Notice

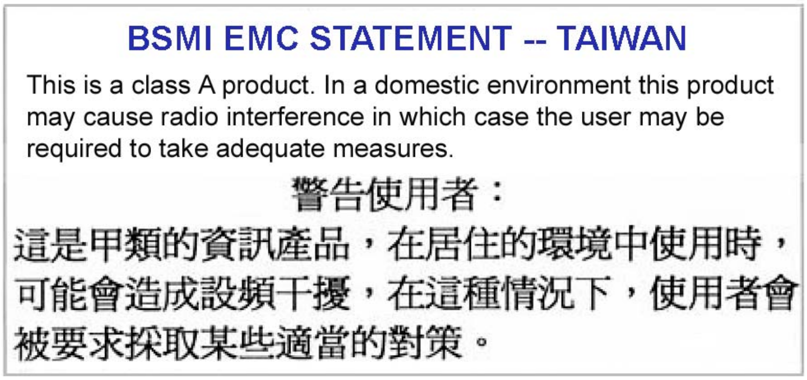
Industry Canada Equipment Standard for Digital Equipment (ICES-003)

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.

Bureau of Standards Metrology and Inspection (BSMI) - Taiwan



BSMI EMC STATEMENT -- TAIWAN

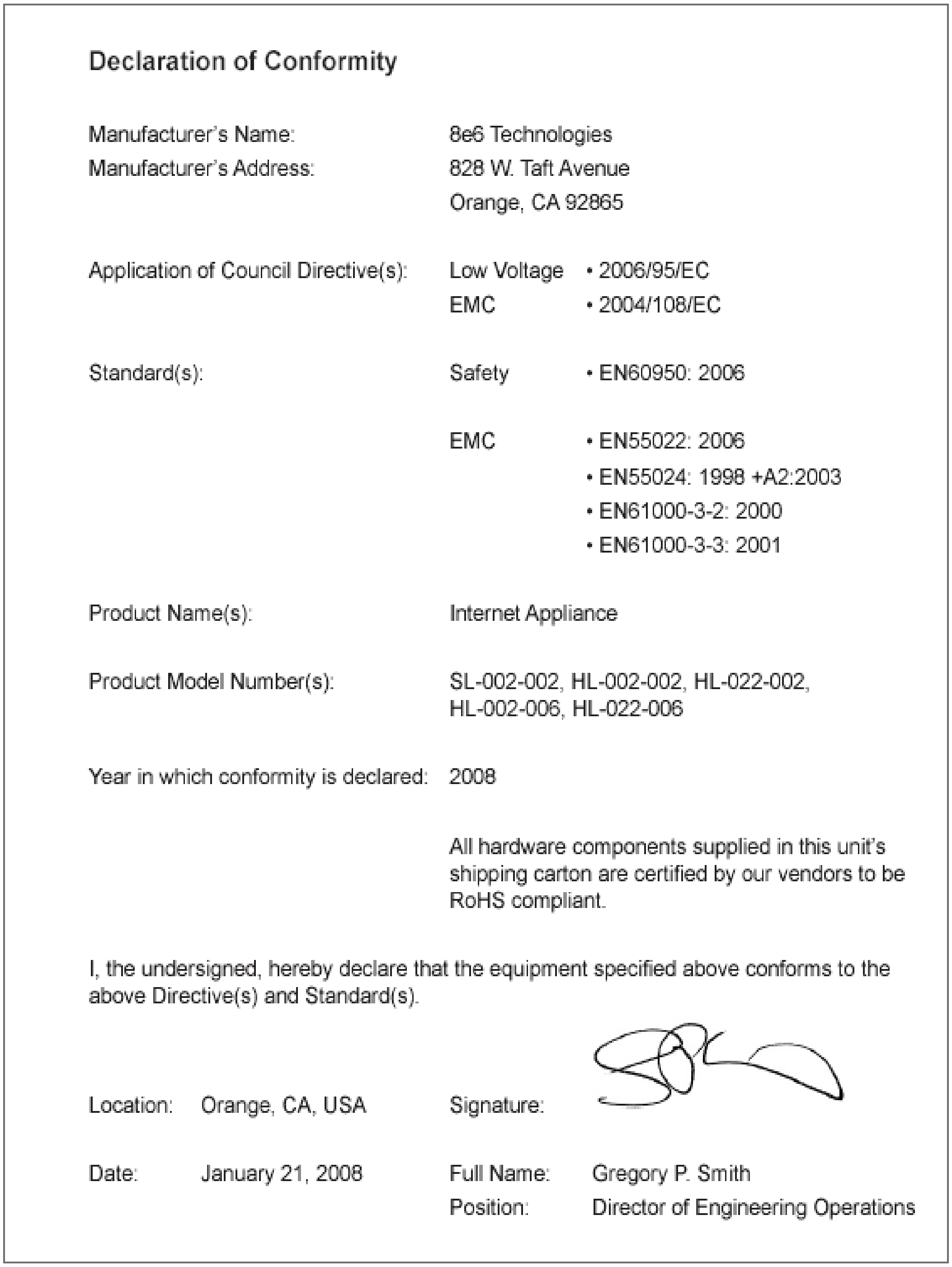
This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

警告使用者：

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

EC Declaration of Conformity

European Community Directives Requirement (CE)



Declaration of Conformity

Manufacturer's Name:	8e6 Technologies	
Manufacturer's Address:	828 W. Taft Avenue Orange, CA 92865	
Application of Council Directive(s):	Low Voltage	• 2006/95/EC
	EMC	• 2004/108/EC
Standard(s):	Safety	• EN60950: 2006
	EMC	• EN55022: 2006 • EN55024: 1998 +A2:2003 • EN61000-3-2: 2000 • EN61000-3-3: 2001
Product Name(s):	Internet Appliance	
Product Model Number(s):	SL-002-002, HL-002-002, HL-022-002, HL-002-006, HL-022-006	
Year in which conformity is declared:	2008	

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

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

Location:	Orange, CA, USA	Signature:	
Date:	January 21, 2008	Full Name:	Gregory P. Smith
		Position:	Director of Engineering Operations

APPENDIX A: CONSOLE SETUP PROCEDURES

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

Configure Setup Workstation

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

A. From the desktop of the setup workstation, while logged in with Administrator privileges, follow the procedures for your machine type:

- **Windows XP**: Go to Start > Control Panel. Open Network Connections. Right-click the link for LAN or High-Speed Internet and choose Properties.
- **Windows Vista**: Go to the start icon > Control Panel > Network and Internet > Network and Sharing Center > Manage network connections. Right-click the Local Area Connection you want to change, then choose Properties.
- **Windows 7**: Go to the start icon > Control Panel. In the search box, type ***adapter***. Under Network and Sharing Center, choose View network connections. Right-click the Local Area Connection you want to change, then choose Properties.

B. On a Windows XP machine, click on **Internet Protocol (TCP/IP)** to highlight it. On a Windows Vista or Windows 7 machine, go to the Networking tab. Under This connection uses the following items, choose **Internet Protocol Version 4 (TCP/IPv4)** to highlight it.

C. Click the **Properties** button.

⚠ ***WARNING**: Be sure to make note of the current network settings on the setup workstation as you will need to return them for further setup procedures.*

D. Choose the option **Use the following IP address**.

E. Type in the **IP address** of 1.2.3.3.

F. Type in the **Subnet mask** (netmask) of 255.0.0.0 and click **OK**.

G. Close the LAN connection properties box.

Storage Device Setup (for Attached Storage Units)

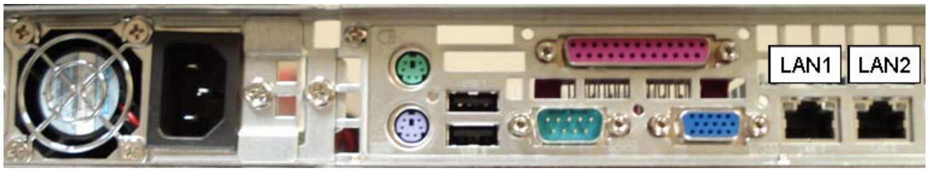
If you have a NAS (Fibre Channel Connected Storage Device or "SAN") that will be used with the ER, you will need to connect it to the ER at this point. Refer to Appendix B at the end of this document for instructions on how to connect the Fibre Channel Connected Storage Device.

Link the Workstation to the ER

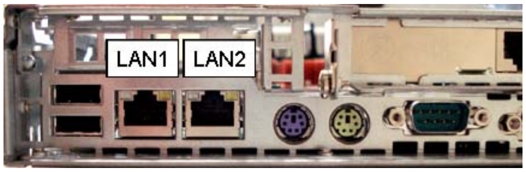
The procedures outlined in this sub-section require the use of the CAT-5E crossover cable.

A. Plug one end of the CAT-5E crossover cable into the ER's **LAN 1** port.

***NOTE**: When facing the rear of the chassis, the LAN 1 port is the port on the left.*



Portion of SL chassis rear



Portion of HL chassis rear

B. Plug the other end of the CAT-5E crossover cable into the setup workstation's network card.

C. Connect the power cable(s) into the back of the ER unit.

D. Plug the power cable(s) into a power source with an appropriate rating.

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

E. Power on the ER by lowering the bezel and pressing the large button at the right of the front panel (see diagrams below):

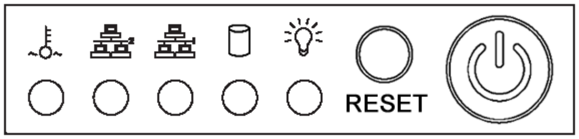


Diagram of SL chassis front panel, power button at far right

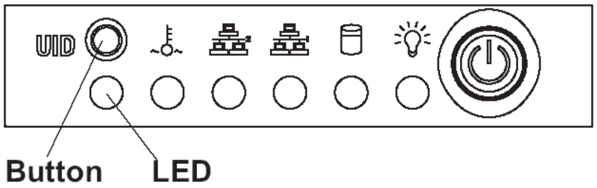


Diagram of HL chassis front panel, power button at far right

***WARNING**: The ER is an information database. If you experience a power interruption or power off the ER in any manner other than from the Web-based interface utility described in the sub-step Physically Connect the ER to the Network, you may lose data and/or damage the file system.*

The Boot Up Process

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

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

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

If you receive a reply, the unit is up.

Security Certificate Acceptance Procedures

A. From the setup workstation, launch an Internet supported browser such as Firefox 3.5, Internet Explorer 7 or 8, or Safari 4.0.

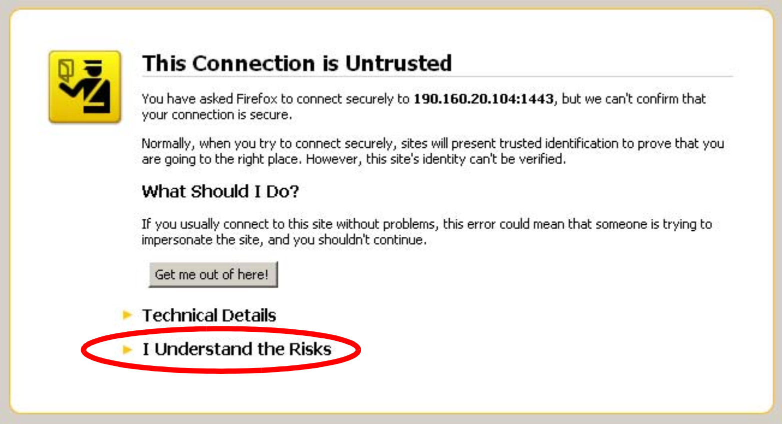
B. Type in **https://1.2.3.4:8843** in the address field.

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

- If using Firefox, proceed to Accept the Security Certificate in Firefox.
- If using IE, proceed to Temporarily Accept the Security Certificate in IE.
- If using Safari, proceed to Accept the Security Certificate in Safari.

Accept the Security Certificate in Firefox

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



This Connection is Untrusted

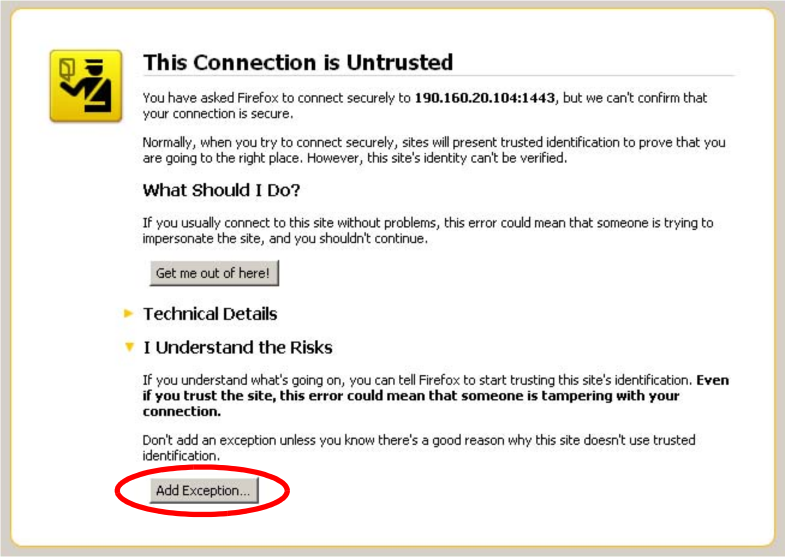
You have asked Firefox to connect securely to **190.160.20.104:1443**, but we can't confirm that your connection is secure.

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

What Should I Do?

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

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



This Connection is Untrusted

You have asked Firefox to connect securely to **190.160.20.104:1443**, but we can't confirm that your connection is secure.

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

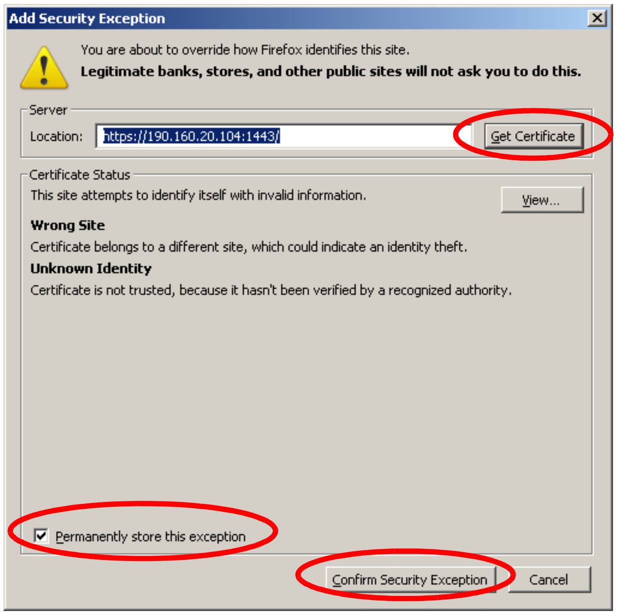
What Should I Do?

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

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

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

Clicking Add Exception opens the Add Security Exception window:



Add Security Exception

You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://190.160.20.104:1443/

Certificate Status

This site attempts to identify itself with invalid information.

Wrong Site

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

Unknown Identity

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

☑ Permanently store this exception

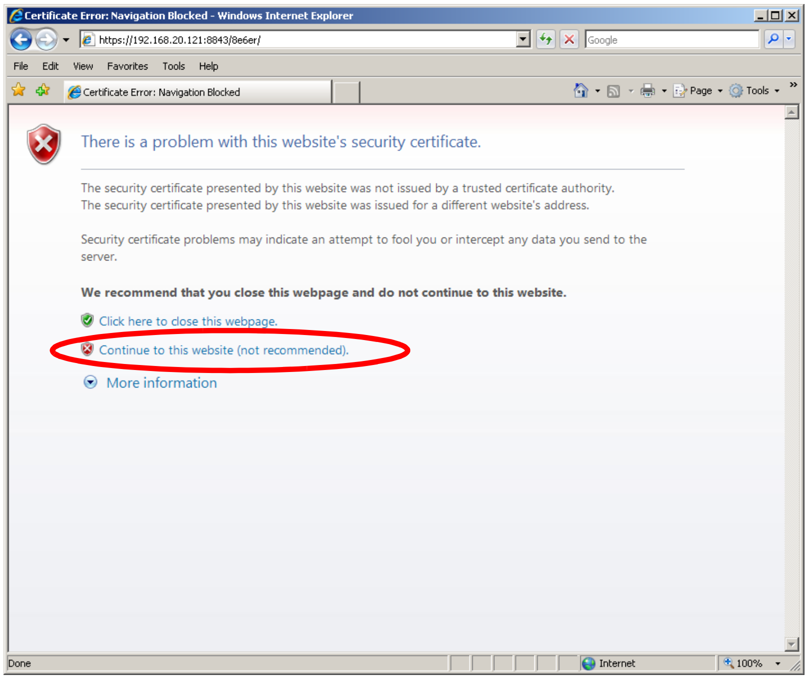
C. In the Add Security Exception window, click **Get Certificate** and wait a few seconds until the security certificate is obtained by the server.

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

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

Temporarily Accept the Security Certificate in IE

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


Certificate Error: Navigation Blocked - Windows Internet Explorer
https://192.168.20.121:8843/8e6er/
Google
File Edit View Favorites Tools Help
Certificate Error: Navigation Blocked
Page Tools
Done
Internet
100%

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

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

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

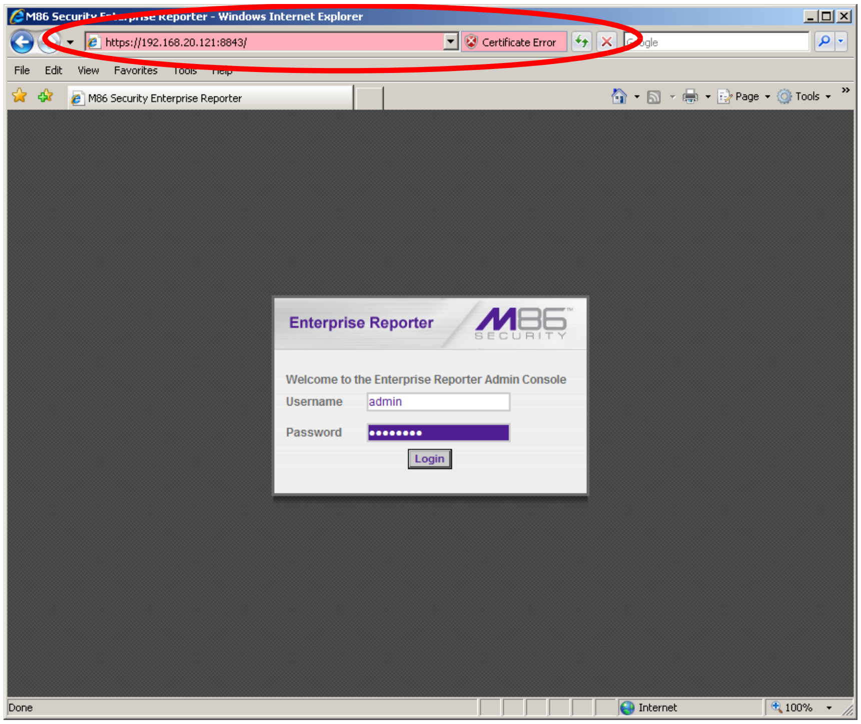
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

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


M86 Security Enterprise Reporter - Windows Internet Explorer
https://192.168.20.121:8843/
Certificate Error
Google
File Edit View Favorites Tools Help
M86 Security Enterprise Reporter
Page Tools
Enterprise Reporter
M86 SECURITY
Login
Done
Internet
100%

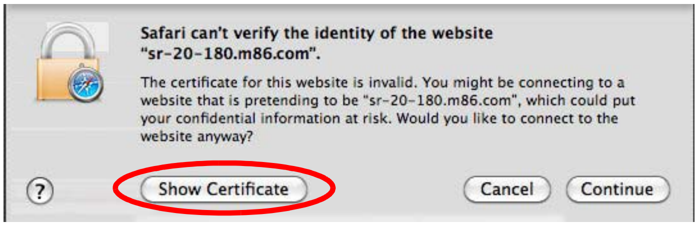
Welcome to the Enterprise Reporter Admin Console

Username admin

Password ••••••••

Accept the Security Certificate in Safari

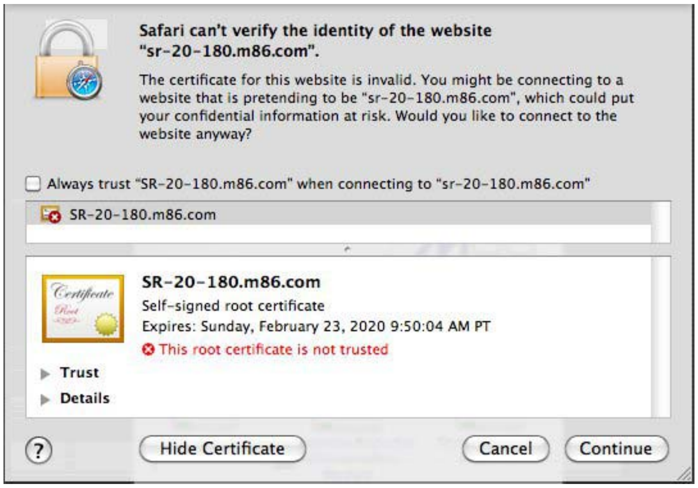
A. If using a Safari browser, the pop-up window "Safari can't verify the identity of the website..." opens:



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

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

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



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

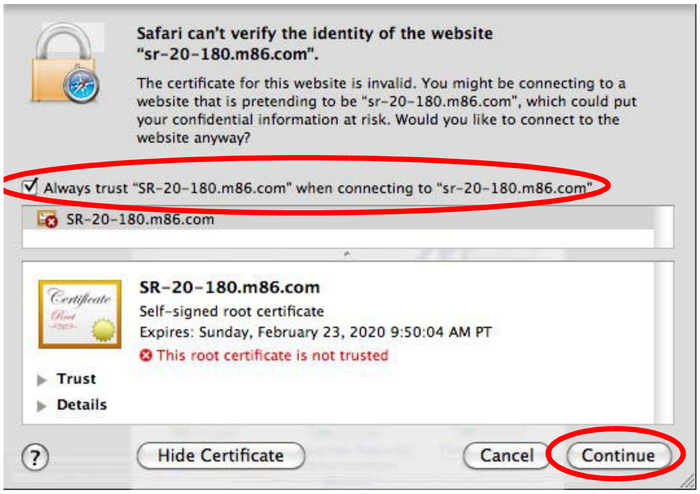
The certificate for this website is invalid. You might be connecting to a website that is pretending to be "sr-20-180.m86.com", which could put your confidential information at risk. Would you like to connect to the website anyway?

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

SR-20-180.m86.com

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

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



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

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

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

SR-20-180.m86.com

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

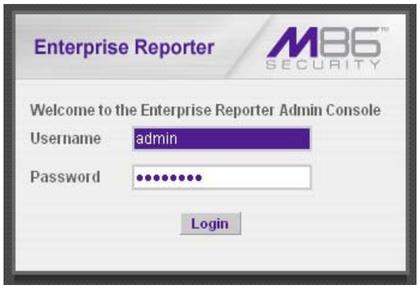
C. You will be prompted to enter your password in order to install the certificate.

Network Setup

For this step, you will need your network administrator to provide you the host name, gateway address, and one unused IP address.

Log in to the Administrator Console

In the ER login window, enter the generic Username and Password:



Welcome to the Enterprise Reporter Admin Console

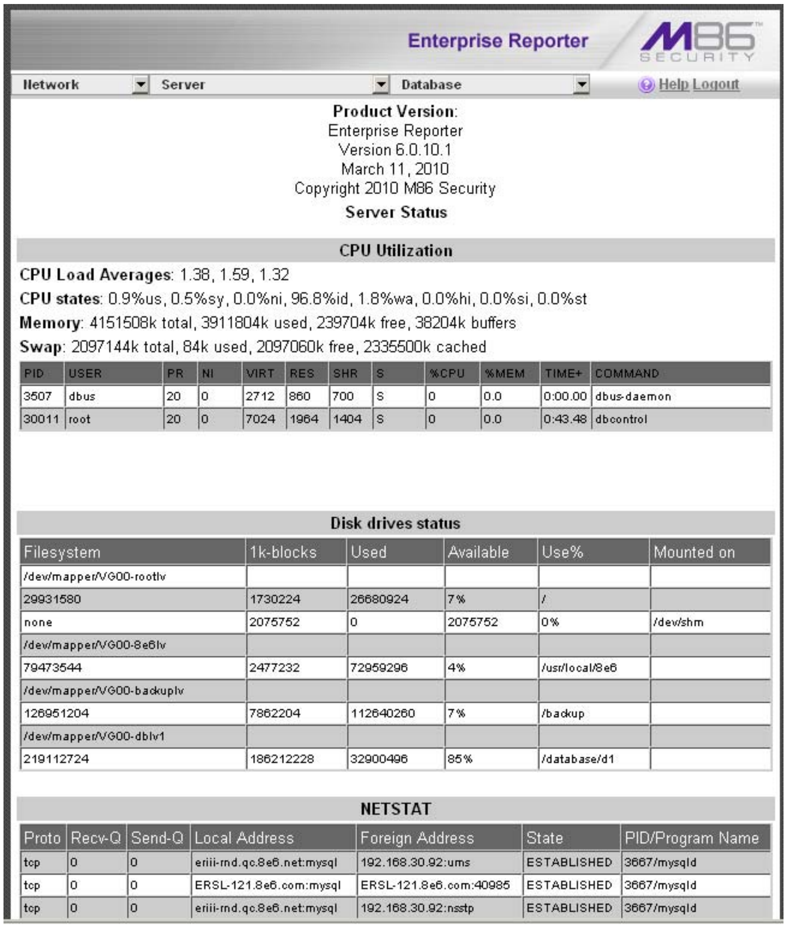
Username: admin

Password: ••••••••

A. In the **Username** field, type in ***admin***.

B. In the **Password** field, type in ***reporter***.

C. Click **Login** to go to the Server Status screen of the Administrator console:



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

Server Status

CPU Utilization

CPU Load Averages: 1.38, 1.59, 1.32

CPU states: 0.9%us, 0.5%sy, 0.0%ni, 96.8%id, 1.8%wa, 0.0%hi, 0.0%si, 0.0%st

Memory: 4151508k total, 3911804k used, 239704k free, 38204k buffers

Swap: 2097144k total, 84k used, 2097060k free, 2335500k cached

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
3507	dbus	20	0	2712	860	700	S	0	0.0	0:00.00	dbus-daemon
30011	root	20	0	7024	1964	1404	S	0	0.0	0:43.48	dbcontrol

Disk drives status

Filesystem	1k-blocks	Used	Available	Use%	Mounted on
/dev/mapper/VG00-rootlv					
29931580	1730224	26680924	7%	/	
none	2075752	0	2075752	0%	/dev/shm
/dev/mapper/VG00-8e6lv					
79473544	2477232	72959296	4%	/usr/local/8e6	
/dev/mapper/VG00-backuplv					
126951204	7862204	112640260	7%	/backup	
/dev/mapper/VG00-dblv1					
219112724	186212228	32900496	85%	/database/d1	

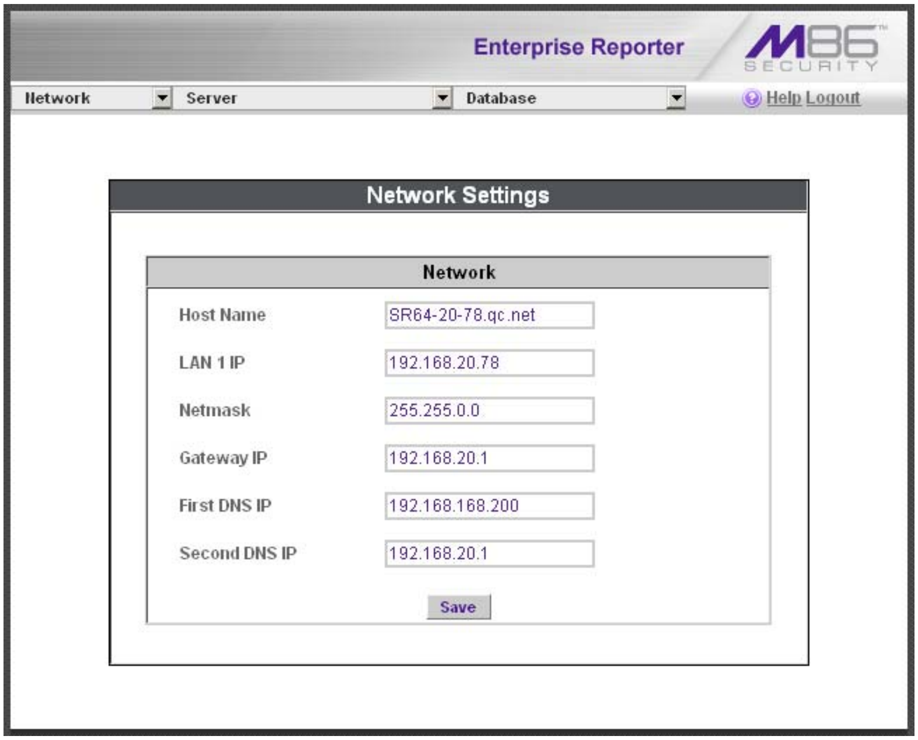
NETSTAT

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

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

Network Settings

A. From the Network menu at the top left of the screen, choose **Network Setting** to display the Network Settings screen in which you enter LAN settings the ER will use on your network:



Network Settings

Network	
Host Name	SR64-20-78.qc.net
LAN 1 IP	192.168.20.78
Netmask	255.255.0.0
Gateway IP	192.168.20.1
First DNS IP	192.168.168.200
Second DNS IP	192.168.20.1

B. Enter the **Host Name** that includes your domain name. For example: er.myserver.com. This must be a valid DNS entry.

C. Enter the **LAN 1 IP** address of the ER server. This IP address must be HTTPS-accessible via the Web access logging device, and via port 3306 from the client workstation that will run the reports.

D. Enter the **Netmask** (subnet) that will define the traffic designated for the LAN.

E. Enter the **Gateway IP** address for the default router or firewall that is the main gateway for the entire network segment.

F. Enter the **First DNS IP** address of the primary Domain Name System (name server). The server will use this IP address to identify IP addresses on the network.

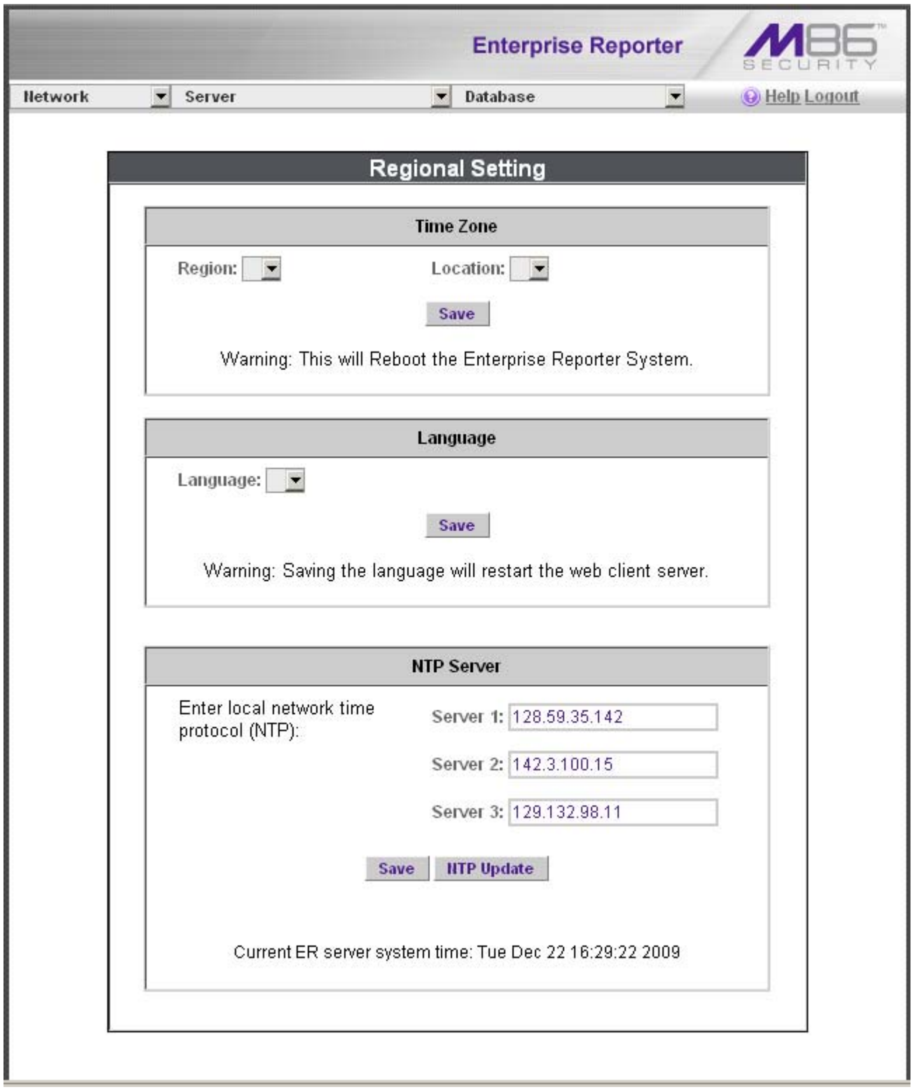
G. Enter the **Second DNS IP** address of the fallback DNS.

⚠ ***WARNING****: Be sure to make note of the IP addresses and host name you assigned to the ER. It is strongly suggested you document and save a copy of these entries since they are now the only way to communicate with the ER.*

H. Click **Save**.

Regional Setting: Time Zone

A. From the Network menu, choose **Regional Setting** to display the Regional Setting screen in which you specify the geographic region of the ER, select the language set to display in the console, and then select the Network Time Protocol (NTP) servers the ER will use for time synchronization with Internet clocks:



Regional Setting

Time Zone

Region:

Location:

Warning: This will Reboot the Enterprise Reporter System.

Language

Language:

Warning: Saving the language will restart the web client server.

NTP Server

Enter local network time protocol (NTP):

Server 1: 128.59.35.142

Server 2: 142.3.100.15

Server 3: 129.132.98.11

Current ER server system time: Tue Dec 22 16:29:22 2009

B. At the **Region** pull-down menu, select your country from the available choices.

C. At the **Location** pull-down menu, select the time zone for the specified region.

D. Click **Save**.

Regional Setting: Language

A. If necessary, select a language set from the **Language** pull-down menu to display that text in the console.

B. Click **Save**.

Regional Setting: NTP Servers

A. In the **Server 1** field on the Time Settings screen, enter the IP address of the primary NTP server you wish to use for clock settings on your server.

B. In the **Server 2** field, enter the IP address of the secondary NTP server. The time from this server will be used by your server if the IP address for the primary server fails to be accessed by your server.

C. In the **Server 3** field, enter the IP address of the tertiary NTP server. The time from this server will be used by your server if the IP addresses for the primary and secondary servers fail to be accessed by your server.

D. Click **Save**.

Physically Connect the ER to the Network

Now that your ER network parameters are set, you can physically connect the unit to your network. This step requires a standard CAT-5E cable (*not* the CAT-5E crossover cable supplied with the ER).

***NOTE**: This section requires you to restart the ER. If you wish to relocate the ER before connecting it to the network, you must first shut down the server instead of restarting it. To shut down the ER, go to the Server menu, select Shut Down, and then choose Shutdown Hardware. Once the server is shut down, you must power on the ER and then log back into the Administrator console.*

***WARNING**:*

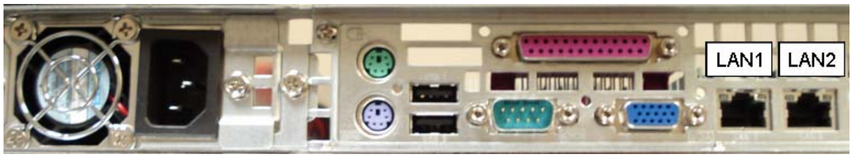
A. Restart the machine using the steps below. ***Never*** reset by using the power or reset buttons as this can corrupt the database and result in lost data.

1. From the Server menu, select **Shut Down**.
2. On the Shut Down screen, choose **Restart Hardware**.
3. Click **Apply**.
4. When the Warning screen displays, click **Restart**.

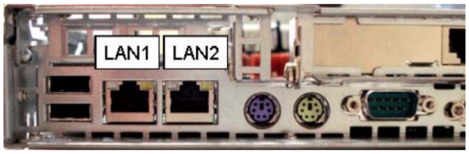
***NOTE**: From the time you click Restart Hardware, you have approximately 2 minutes to perform steps B through E while the ER goes through the Restart process.*

B. Disconnect the crossover cable from the ER.

C. Plug one end of a standard CAT-5E cable into the ER’s LAN 1 port.



Portion of SL chassis rear



Portion of HL chassis rear

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

E. Wait until the Restart process has completed (indicated by the drive light staying off for 30 seconds. This process may take 5 - 10 minutes).

NOTE*: To verify that the server is in the process of being restarted, you can try accessing another screen. If you cannot access another screen, the restart process is still in progress.*

F. Restore the setup workstation you used for the Network Setup to its original settings, and connect it to the network hub to create an “administrator workstation.” (You could also use another workstation already on the network that you want to designate as the administrator workstation.)

G. Launch your Internet browser on the administrator workstation.

H. In the address field, enter the LAN 1 IP address you assigned to the ER. Be sure to use “https” and port **:8843** for a secure connection. For example, if the ER were assigned an IP address of 10.10.10.10, you would enter **https://10.10.10.10:8843** in the browser’s address field.

Proceed to Step 4: Log in, Generate SSL Certificate from the Install the Server portion of this Installation Guide.

APPENDIX B: FIBRE CHANNEL CONNECTED STORAGE DEVICE

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

Preliminary Setup Procedures

Unpack the Unit from the Carton

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

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

The carton should contain the following items:

- 1 Nexsan Technologies unit
- 1 Mounting Kit
- 1 Accessory Kit containing:
  - 2 AC Power Cords
  - 1 Fibre Channel cable

Other Required Installation Items

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

- 1 Standard CAT-5E cable
- 1 CAT-5E crossover cable (from the ER server carton)

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

***NOTE**: Refer to the ER safety precautions. In addition to being applicable to the ER, 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 x 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:

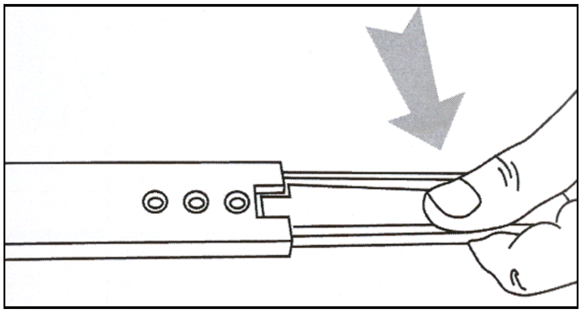
- The weight of all units in the rack is evenly distributed. Hazardous conditions may be created by an uneven weight distribution.
- The rack will not tip over when the unit is mounted, even when the unit is fully extended from the rack.
- For a single rack installation, stabilizers are attached to the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

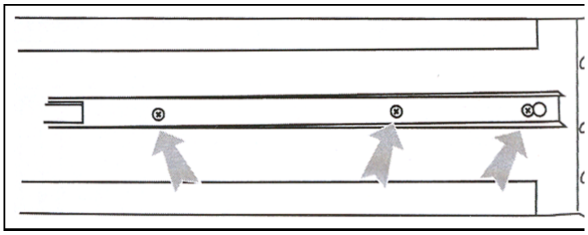
Step 1

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.

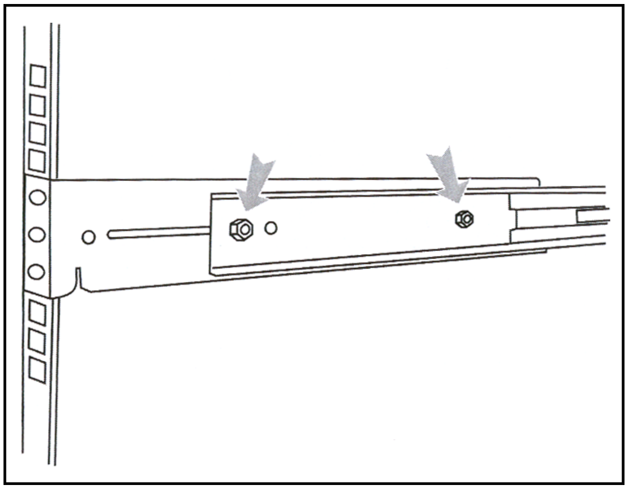


***NOTE**: When attaching the extended brackets, attach them loosely at first. Adjust the length to fit the cabinet, and then tighten.*

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.

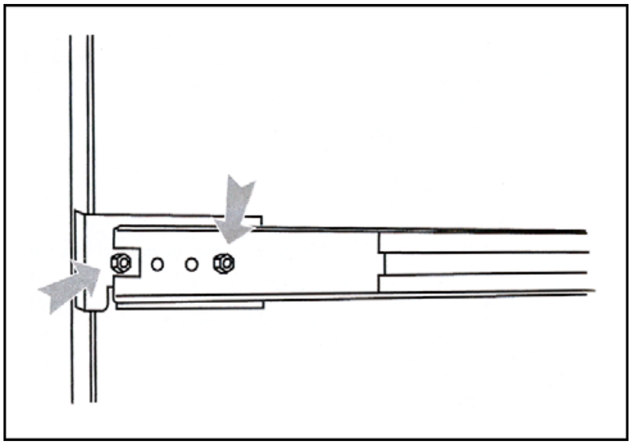
***NOTE**: Make sure the flange is on the bottom edge.*



Step 4

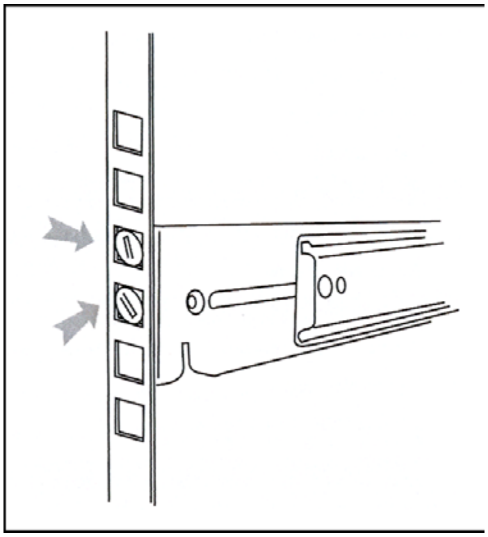
Attach left and right front (short) extended brackets to the outer rail using 2 screws, 2 washers, and 2 nuts for each bracket.

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 ER 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 ER section. The procedures outlined in this step require the use of the CAT-5E crossover cable and the Fibre Channel cable.

A. Plug the Fibre Channel cable into the slot on the upper middle section on the rear of the ER unit (see Figure 1, Item A).

B. Plug one end of the CAT-5E crossover cable into the ER unit's LAN 2 port-—the port to the right (see Figure 1, Item B).

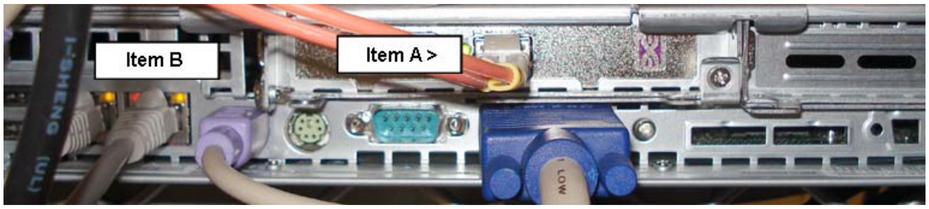


Figure 1: Back of the ER unit

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

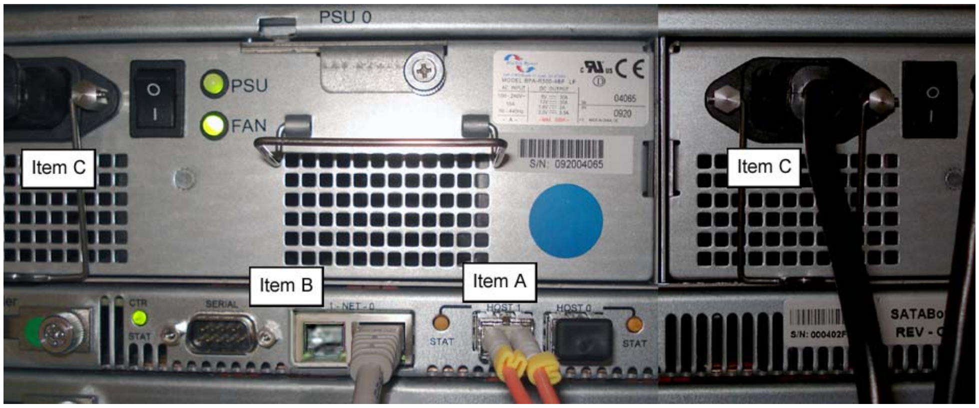


Figure 2: Back of the Nexsan SATABoy

D. Plug the other end of the CAT-5E crossover cable into the storage device's NET "0" port (see Figure 2, Item B).

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

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

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

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

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

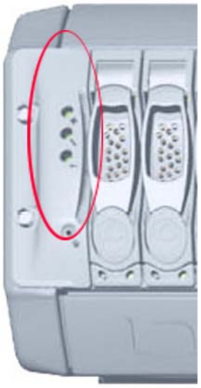


Figure 3: LED display

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 ER unit first. (Refer to the Physically Connect the ER to the Network sub-step in Step 1B of the ER section for shut down procedures.)

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

Restart the Storage Device Unit

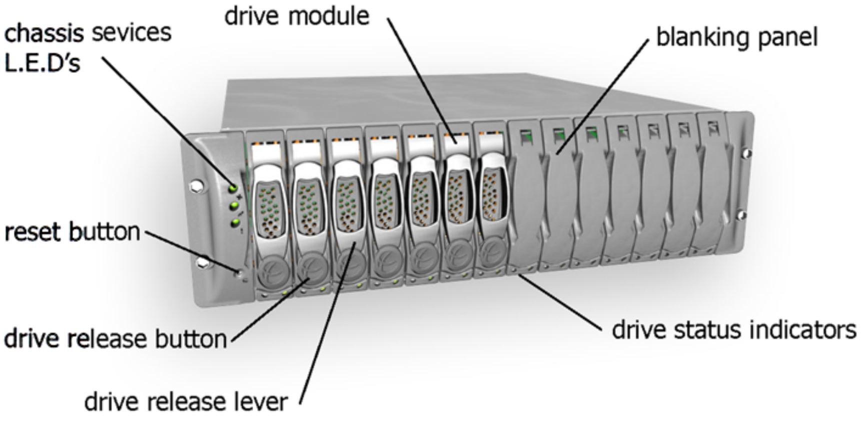
The storage device must be restarted after a power failure. In this instance, the storage device may already be turned on, but needs to be booted up again.

⚠ ***WARNING**: You must **always** power on the storage device **before** powering on the ER 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.*

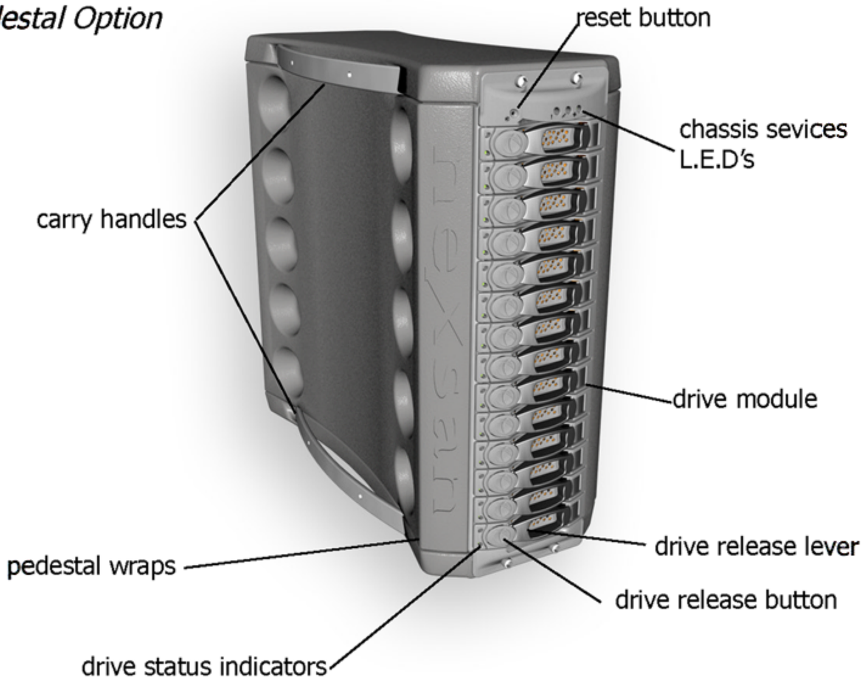
To restart the storage device, press the power button on the front panel. The boot-up process may take up to 5 minutes.

Physical Components

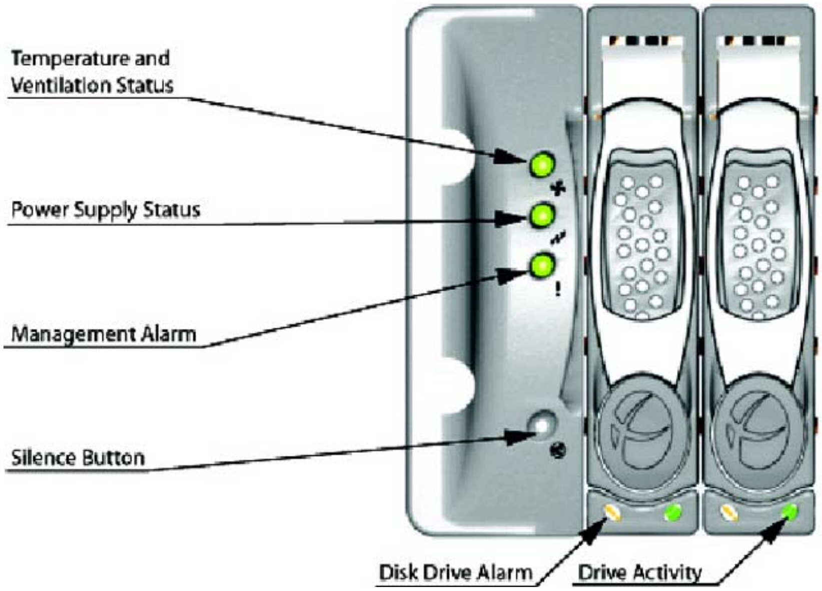
Rack Mount Option



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.

INDEX

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