M86 Security Reporter Virtual

INSTALLATION GUIDE

Software Version: 3.1.10
Document Version: 09.19.11

M86 SECURITY REPORTER VIRTUAL INSTALLATION GUIDE

© 2011 M86 Security

All rights reserved. Printed in the United States of America

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

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

Trademarks

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

Part# SR-VIG-110919

CONTENTS

M86 SR VIRTUAL INTRODUCTION 1

About this Document. 2

Conventions Used in this Document. 2

SERVICE INFORMATION 3

M86 Technical Support Call Procedures. 3

PRELIMINARY SETUP PROCEDURES 4

Network Requirements. 4

Download and Install the SR software image. 4

Important Virtual Machine Message. 5

INSTALL AND CONFIGURE SR VIRTUAL 7

Step 1: Quick Start Setup Procedures. 7

Login screen 7
Quick Start menu screen 7
Quick Start setup 8
Configure network interface LAN1 8
Configure network interface LAN2 9
Configure default gateway 9
Configure DNS servers 9
Configure host name 9
Time Zone regional setting 9
Configure setup wizard user 10
Non-Quick Start procedures or settings 10
Reboot system 10
Change Quick Start password 10
Reset Admin account 10
System Status screen 11
Log Off 11

Step 2: Connect Peripheral Devices to the Host. 12

Storage Device Setup (for Attached Storage Units) 12
Bandwidth Management 12

Step 3: Access the SR and its Applications Online. 13

Access the SR via its LAN 1 IP Address 13
Accept the Security Certificate in Firefox 14
Temporarily Accept the Security Certificate in IE 16
Accept the Security Certificate in Safari 17
Accept the Security Certificate in Chrome 18
Accept the End User License Agreement 19
Log in to the Security Reporter Wizard 20
Use the SR Wizard to Specify Application Settings 20
Enter Main Administrator Criteria 21
For Web Filters: Go to Bandwidth Range and Web Filter Setup 21

Enter Bandwidth Range 21
Enter Web Filter Setup Criteria 21
For SWGs: Go to Secure Web Gateway Setup 22
Save settings 22

Step 4: Generate SSL Certificate. 23
Generate a Self-Signed Certficate for the SR 23
IE Security Certificate Installation Procedures 25
Accept the Security Certificate in IE 25
Windows XP or Vista with IE 8 25
Windows 7 with IE 8 29
Map the SR's IP Address to the Server's Hostname 30

Step 5: Add Web Filter, SWG to Device Registry. 32
Add a Web Filter Device 32
Add an SWG Device 33

Step 6: Set up Web Filter, SWG Log Transfers. 34
Web Filter Setup 34
Web Filter Configuration 34
Web Filter Log Transfer Verification 35
Set Self-Monitoring 36
SWG Setup 37
SWG Configuration for Software Version 10.0 37
Configure SWG to Send Logs to the SR 37
Policy Settings 38
SWG Configuration for Software Version 9.2.5 39
Configure SWG to Send Logs to the SR 39
Policy Settings 40

Single Sign-On Access, Default Username/Password. 41
Single Sign-On Access 41
Default Usernames and Passwords 41

CONCLUSION 42

BEST REPORTING PRACTICES 43

Productivity Reports Usage Scenarios. 44
I. Summary Report and Drill Down Report exercise 44
Step A: Use Summary Reports for a high level activity overview 44
Step B: Further investigate using a Summary Drill Down Report 45
Step C: Create a new report using yesterday's date scope 47
Step D: Create a report grouped by two report types 47
Step E: Create a Detail Drill Down Report to obtain a list of URLs 48
II. 'Group By' Report and Export Report exercise 50
Step A: Drill down to view the most visited sites in a category 50
Step B: Modify the report view to only display top 10 site records 51
Step C: Export the report view in the PDF output format 52
III. Save and schedule a report exercise 53
Step A. Save a report 53
Step B. Schedule a recurring time for the report to run 54
IV. Create a Custom Category Group and generate reports 55
Step A: Create a Custom Category Group 55
Step B: Run a report for a specified Custom Category Group 56
V. Create a custom User Group and generate reports 56

Step A: Create a custom User Group 56
Step B: Generate a report for a custom User Group 58

Security Reports Usage Scenarios. 59
I. Explore the four basic Security Reports types 59
Step A: Navigate to the Blocked Viruses report 59
Step B: Navigate to the Security Policy Violations report 60
Step C: Navigate to the Traffic Analysis report 60
Step D: Navigate to the Rule Transactions report 61
Step E: Modify the current report view 61
II. Create a drill down Security Report view 62
Exercise A: Create a report view that includes two report types 62
Exercise B: Create a detail report view 63
III. Create a customized Security Report 65
Exercise A: Use the current view to generate a custom report 65
Exercise B: Use the Report Wizard to run a custom report 67
IV. Export a Security Report 69
Step A: Specify records to include in the report 69
Step B: Specify 'Group By' and URL limitation criteria 69
Step C: Download the report 69
Step D: View the exported Security Report 70
V. Save a Security Report 71
Step A: Select Report Settings, Save option 71
Step B: Specify criteria in Report Details 72
Step C: Select the users or group in Users 73
Step D: Populate Email Settings 73
Step E: Save the report 73
VI. Schedule a Security Report to run 74
Exercise A: Use the current report view to schedule a run event 74
Exercise B: Use the Wizard to create and schedule reports 76
Access the Report Schedule panel 77
View Details for a Scheduled Report Run Event 77

Real Time Reports Usage Scenarios 79
I. Screen navigation exercise 79
Step A: Navigate panels in the Gauges section 79
Step B: Navigate panels in the Policy section 80
II. Drill down into a gauge exercise 80
Step A: Select the gauge with the highest score 80
Step B: Investigate a user's activity in a specified gauge 82
Step C: Investigate the user's Internet activity in other gauges 83
III. Create a gauge exercise 84
Step A: Access the Add/Edit Gauges panel 84
Step B: Add a URL Gauge 85
IV. Create an email alert exercise 87
Step A: Add a new alert 87
Step B: Select Email Alert Action 89
Step C: Receiving an email alert 90

IMPORTANT INFORMATION ABOUT USING THE SR IN THE EVALUATION MODE ..91

Report Manager. 91
Server Information Panel 91

System Configuration. 92
Evaluation Mode Pop-Up 92
Expiration screen 92

APPENDIX A: BANDWIDTH MONITORING 93

Initial Setup on the ESXi Server..... 93

Steps to Set Up the VM to Use Bandwidth Monitoring..... 93

APPENDIX B: OPTIONAL ETHERNET TAP INSTALLATION 94

Preliminary Setup Procedures..... 94
Unpack the Ethernet Tap Unit from the Box 94
Other Required Installation Items 94

Install the Ethernet Tap Unit. 95

INDEX 97

M86 SR VIRTUAL INTRODUCTION

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

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

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

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

Quick setup procedures to implement the best reporting practices are included in the Best Reporting Practices section that follows the Conclusion of this guide.

About this Document

This document is divided into the following sections:

- **Introduction** - This section is comprised of an overview of the SR product and how to use this document
- **Service Information** - This section provides M86 Security contact information
- **Preliminary Setup Procedures** - This section includes instructions on how to prepare your environment for the inclusion of SR Virtual on your network
- **Install and Configure SR Virtual** - This section explains how to install and configure the SR for reporting
- **Conclusion** - This section indicates that the installation steps have been completed
- **Best Reporting Practices** - This section includes reporting scenarios and instructions for implementing the best reporting practices to capture a snapshot of end user activity on your network that tells you whether or not policies are being enforced
- **Evaluation Mode** - This section gives information on using the SR in the evaluation mode
- **Appendices** - Appendix A explains how to configure bandwidth monitoring. Appendix B explains how to install the optional Ethernet Tap device on your network for bandwidth monitoring.
- **Index** - An alphabetized list of some topics included in this document

Conventions Used in this Document

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

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

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

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

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

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

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

SERVICE INFORMATION

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

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

M86 Technical Support Call Procedures

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

- Your contact information.
- Original order number.
- Description of the problem.
- Network environment in which the virtual appliance hosting SR Virtual software is used.
- State of SR Virtual software 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

Network Requirements

The following items are required for using SR Virtual:

- Host appliance on your network that supports Virtualization Technology
- VMware ESXi 4.1 server
- VMware ESXi 4.1 vSphere Client
- SR Virtual product downloaded to your appliance, which includes the following items:
  - SR software image
  - End User License Agreement
  - link to Security Reporter documentation page at M86 Security's Web site: **http://www.m86security.com/support/sr/documentation.asp**

The following optional devices can be used with SR Virtual:

- One or more attached "NAS" storage devices (e.g. Ethernet connected, SCSI/ Fibre Channel connected "SAN")
- An Ethernet Tap device connected to the virtual server for monitoring bandwidth

Download and Install the SR software image

1. Download the SR software image to your appliance from a link on this page: **http://www.m86security.com/support/sr/virtual-product-upgrade.asp**

***NOTE**: Contact your M86 Security account representative or an M86 solutions engineer if you need assistance accessing the URL or downloading the SR image. Before installing the software image on your machine, be sure you have reviewed the End User License Agreement.*

2. Lauch the vSphere Client on your workstation.
3. Import the SR software image into the ESXi server.

***IMPORTANT**: M86 recommends selecting "Thick provisioned format" for your datastore. See Important Virtual Machine Message on the next page for important information about selecting "Thin provisioned format".*

4. With the SR powered on, access the vSphere Client's Console panel and proceed to the next section of this Installation Guide that requires you to set up parameters for the SR to function on the network.

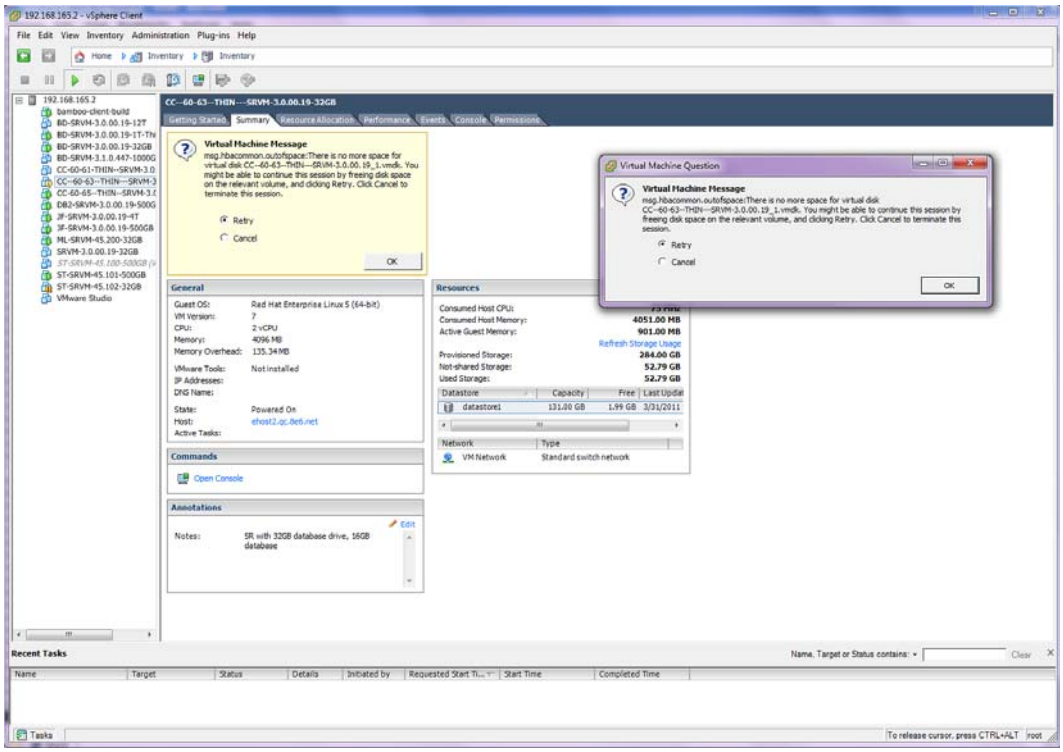
Important Virtual Machine Message

M86 recommends selecting “Thick provisioned format” since the system will automatically allocate appropriate disk space to the SR Virtual image and you will not need to monitor the amount of disk space being used by the datastore.

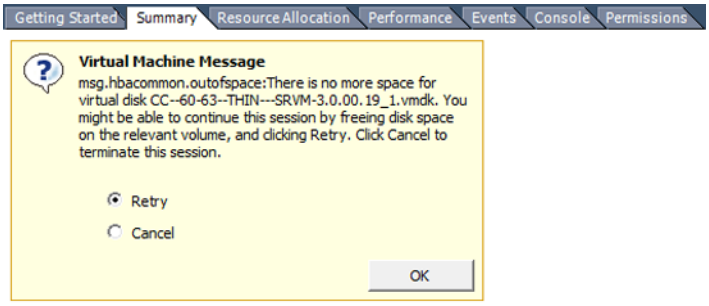
If “Thin provisioned format” is selected, you will need to monitor the amount of disk space available for SR data storage.

If data storage space runs out, the machine will run out of memory and freeze up, and the following Virtual Machine Message will display in the vSphere Client Console’s Summary tab and in a pop-up window: “There is no more space for virtual disk name.vmdk (in which ‘name’ represents the name of the virtual machine). You might be able to continue this session by freeing disk space on the relevant volume, and clicking Retry. Click Cancel to terminate this session.”

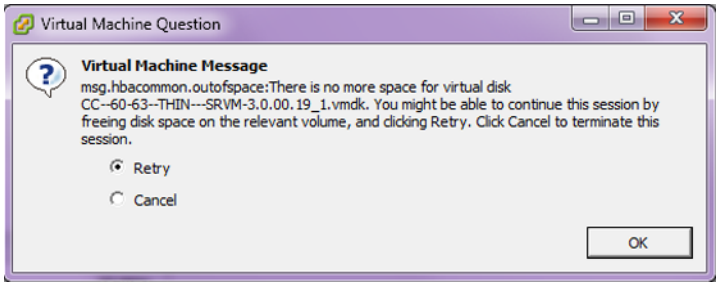
Sample images on this page and the next page illustrate this scenario:



vSphere Client Console showing Virtual Machine Messages



Summary tab showing Virtual Machine Message



Pop-up window showing Virtual Machine Message

To proceed, you will need to free up space on the disk, and then click “Retry” and **OK** to continue.

INSTALL AND CONFIGURE SR VIRTUAL

Step 1: Quick Start Setup Procedures

Login screen

In the Console panel of the vSphere Client:

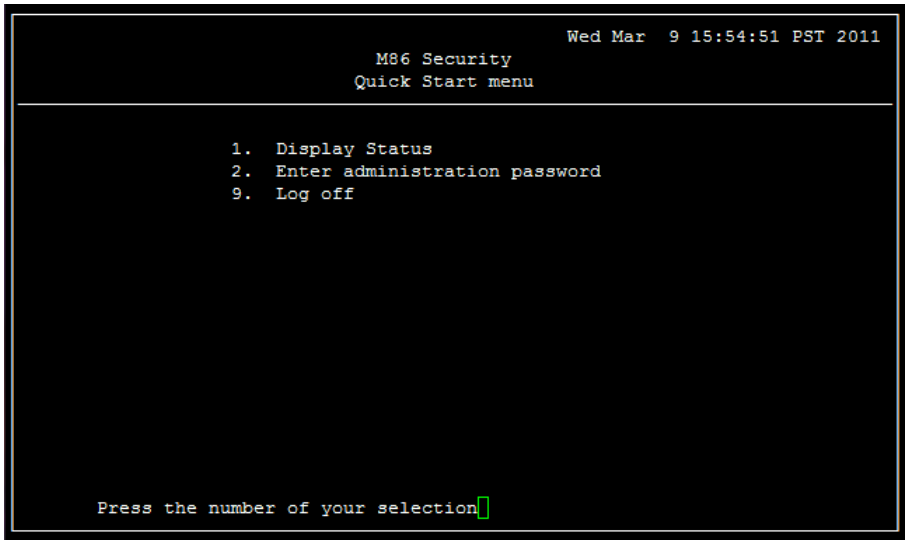
A. At the **login** prompt, type in ***menu***.

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

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

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

Quick Start menu screen

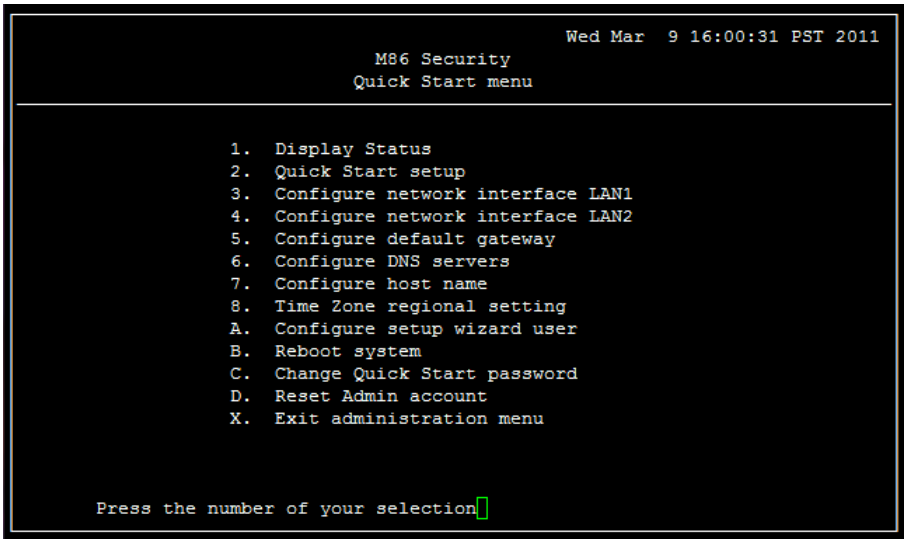


A. At the **Press the number of your selection** prompt, press **2** to select the Quick Start setup process.

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

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

Quick Start setup



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

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

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

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

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

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

Configure network interface LAN1

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

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

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

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

Configure network interface LAN2

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

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

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

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

Configure default gateway

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

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

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

Configure DNS servers

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

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

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

Configure host name

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

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

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

Time Zone regional setting

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

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

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

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

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

Configure setup wizard user

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

B. At the **Enter wizard user name** prompt, type in the new username to be used by the global administrator for the SR Wizard user setup process and press **Enter**.

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

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

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

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

Non-Quick Start procedures or settings

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

Reboot system

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

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

Change Quick Start password

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

***NOTE**: This option will change the password used for accessing the Quick Start menu (the default password is **#s3tup#r3k**) but will not change the global administrator's Single Sign-On password used for accessing the SR user interface via its login window (the default password is 'testpass'). Option D, "Reset Admin account", should be used for resetting the SR login password (the default account reset password is 'reporter1!') and for unlocking all IP addresses currently locked.*

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

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

Reset Admin account

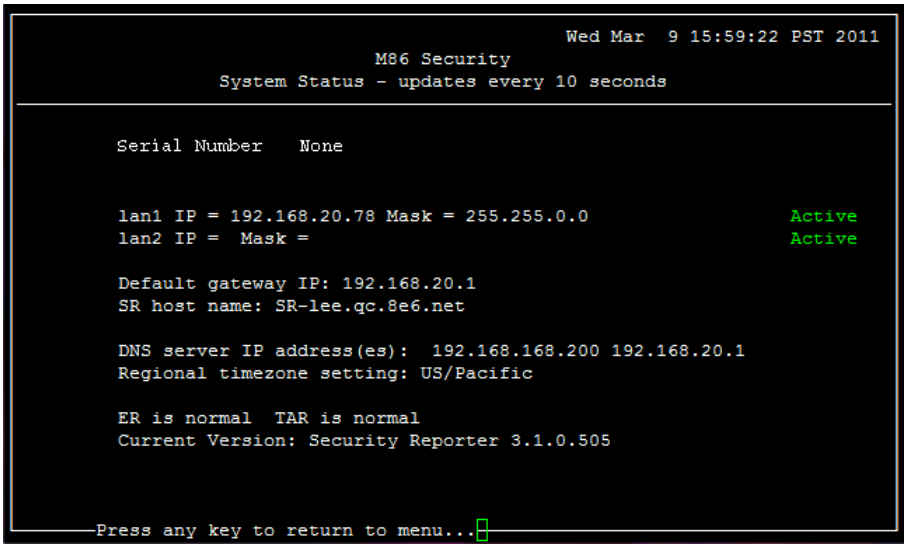
A. From the Quick Start menu, press **D** to go to the Reset admin GUI account confirmation screen that displays the following message:

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

***WARNING**: This option resets the global administrator's Single Sign-On password to 'reporter1!' and will unlock all IP addresses currently locked.*

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

System Status screen



The System Status screen contains the following information:

- **Serial Number** (applicable only to SR Appliances)
- **lan1 IP** address and netmask specified in screen 3, and current status ("Active" or "Inactive")
- **lan2 IP** address and netmask specified in screen 4, and current status ("Active" or "Inactive")
- **Default gateway IP** address specified in screen 5 (Configure default gateway)
- **SR host name** specified in screen 7 (Configure host name)
- **DNS server IP address(es)** specified in screen 6 (Configure DNS servers)
- **Regional timezone setting** specified in screen 8 (Time Zone regional setting)
- current status of ER (System Configuration) and TAR (real time reporting) applications
- **Current Version** of software installed

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

Log Off

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

Proceed to Step 2: Connect Peripheral Devices to the Host.

Step 2: Connect Peripheral Devices to the Host

Now that your SR network parameters are set, you can physically connect peripheral devices—i.e. Fibre Channel Connected Storage Device and/or Tap device—to the host appliance.

Storage Device Setup (for Attached Storage Units)

If you have a NAS (Fibre Channel Connected Storage Device or “SAN”) that will be used with the SR, you will need to connect it to the host appliance at this point.

Bandwidth Management

If you choose to install an Ethernet Tap for bandwidth monitoring, you will need to connect it to the host appliance at this point. Refer to Appendix A and Appendix B at the end of this document for instructions on how to configure Bandwidth Monitoring and how to connect an Ethernet Tap unit to the host appliance.

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

Step 3: Access the SR and its Applications Online

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

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

Access the SR via its LAN 1 IP Address

A. Launch an Internet supported browser:

- Firefox 6.0
- Internet Explorer 8.0
- Safari 5.1
- Google Chrome 13.0

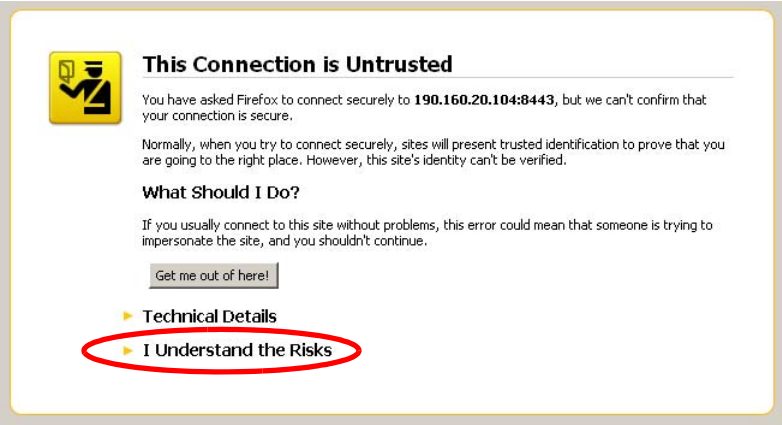
B. In the address field, type in the LAN 1 IP address you assigned to the SR during the Quick Start Setup Procedures. Be sure to use “https” and port **:8443** for a secure connection, appended by “/SR/”. For example, if the SR were assigned an IP address of 10.10.10.10, you would enter **https://10.10.10.10:8443/SR/**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

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

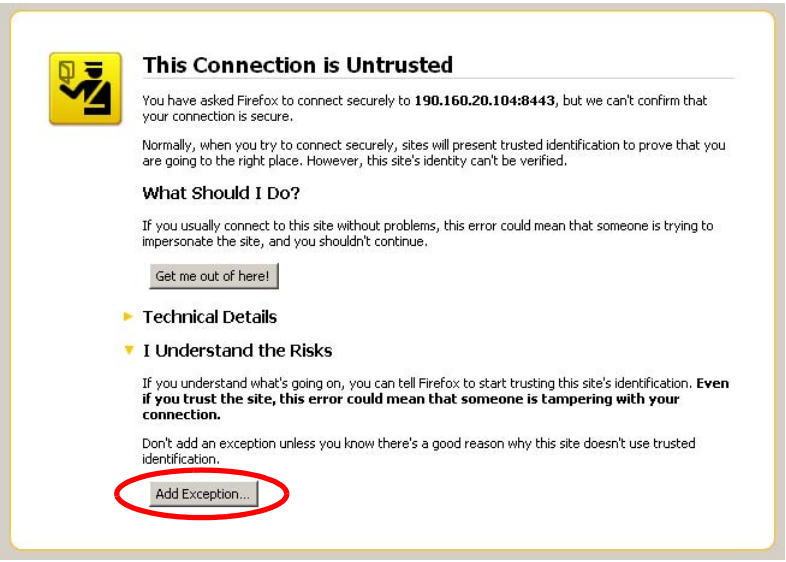
- If using Firefox, proceed to Accept the Security Certificate in Firefox.
- If using IE, proceed to Temporarily Accept the Security Certificate in IE.
- If using Safari, proceed to Accept the Security Certificate in Safari.
- If using Google Chrome, proceed to Accept the Security Certificate in Chrome.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

Accept the Security Certificate in Firefox

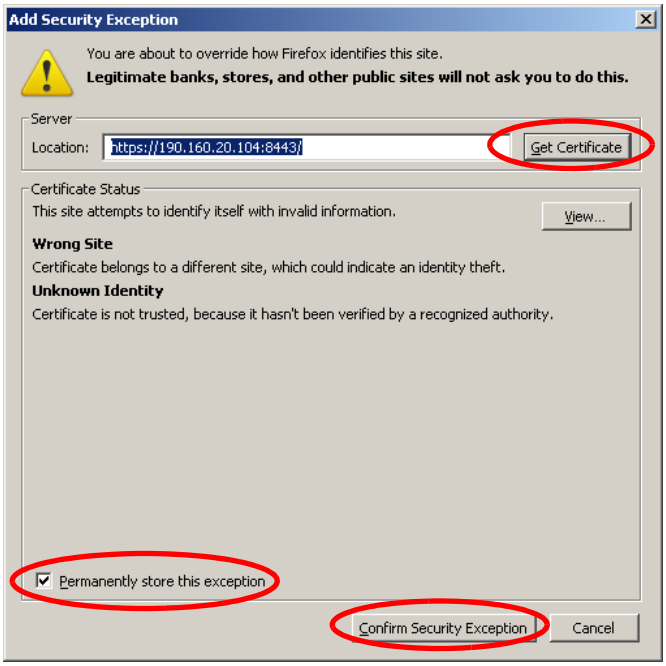
A. If using a Firefox browser, in the page "This Connection is Untrusted," click the option **I Understand the Risks**:



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



Clicking Add Exception opens the Add Security Exception window:



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

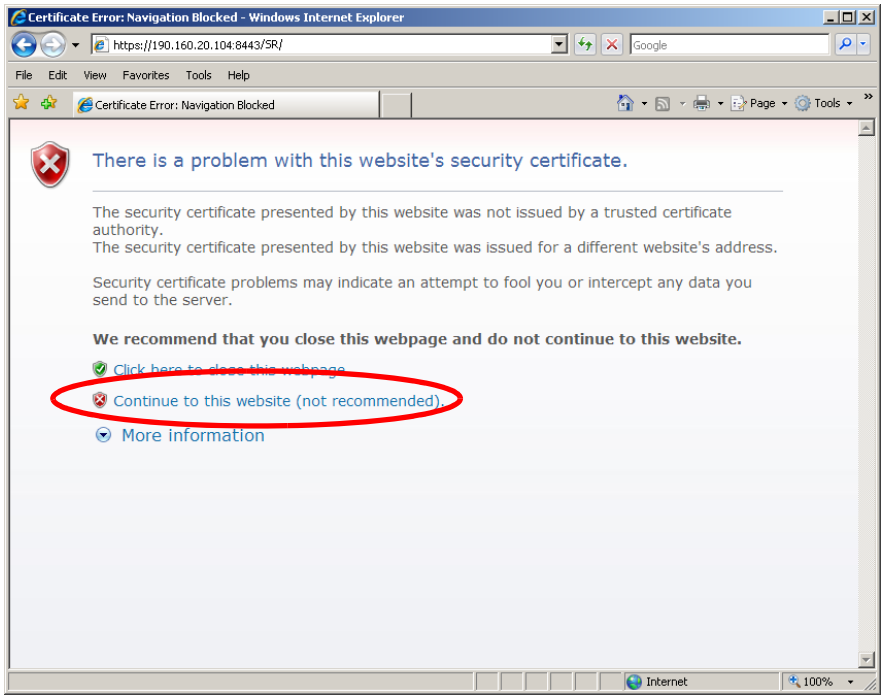
D. With the checkbox **Permanently store this exception** selected, click **Confirm Security Exception** to open the Security Reporter login window:

Proceed to Accept the End User License Agreement.

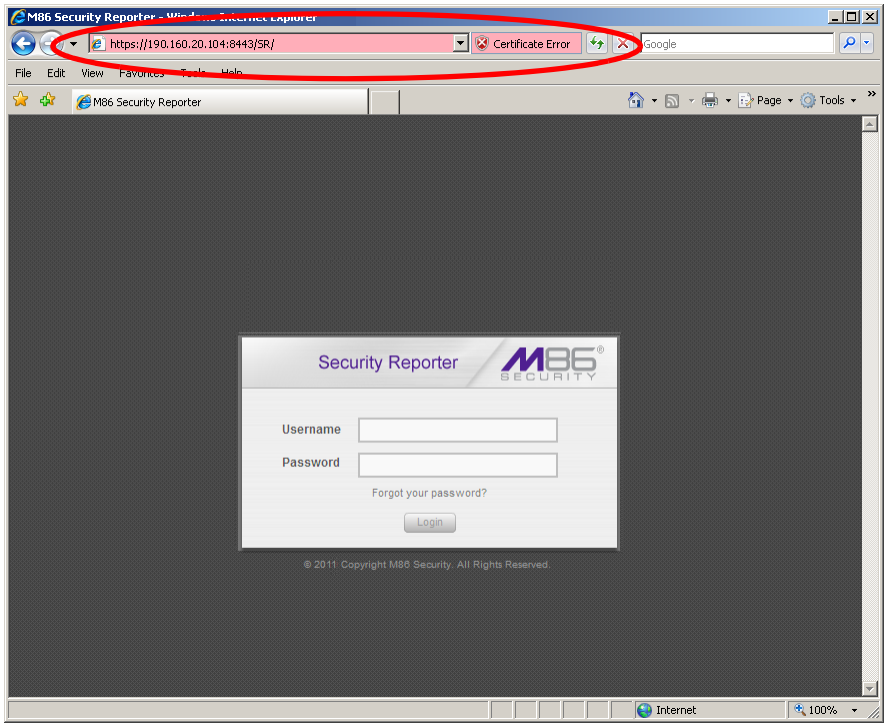
***NOTE**: On a newly installed unit, reports will remain inaccessible until logs are transferred to the SR and the database is built.*

Temporarily Accept the Security Certificate in IE

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



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



Proceed to Accept the End User License Agreement.

Accept the Security Certificate in Safari

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

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

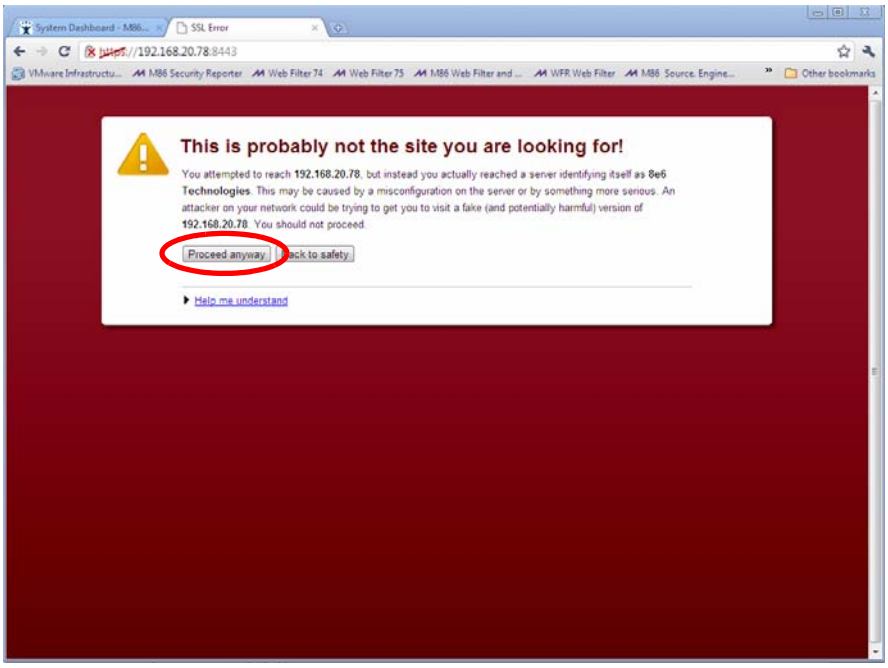
B. Click the "Always trust..." checkbox and then click **Continue**:

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

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

Accept the Security Certificate in Chrome

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



Clicking this button launches the Security Reporter login window:

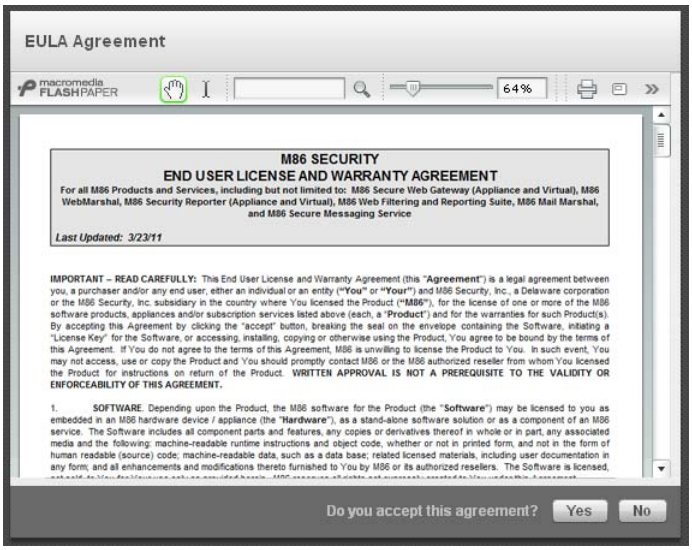
***NOTE**: The Security Certificate must be accepted each time a new browser is launched.*

B. Proceed to Accept the End User License Agreement.

Accept the End User License Agreement

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

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



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

Proceed to Log in to the Security Reporter Wizard.

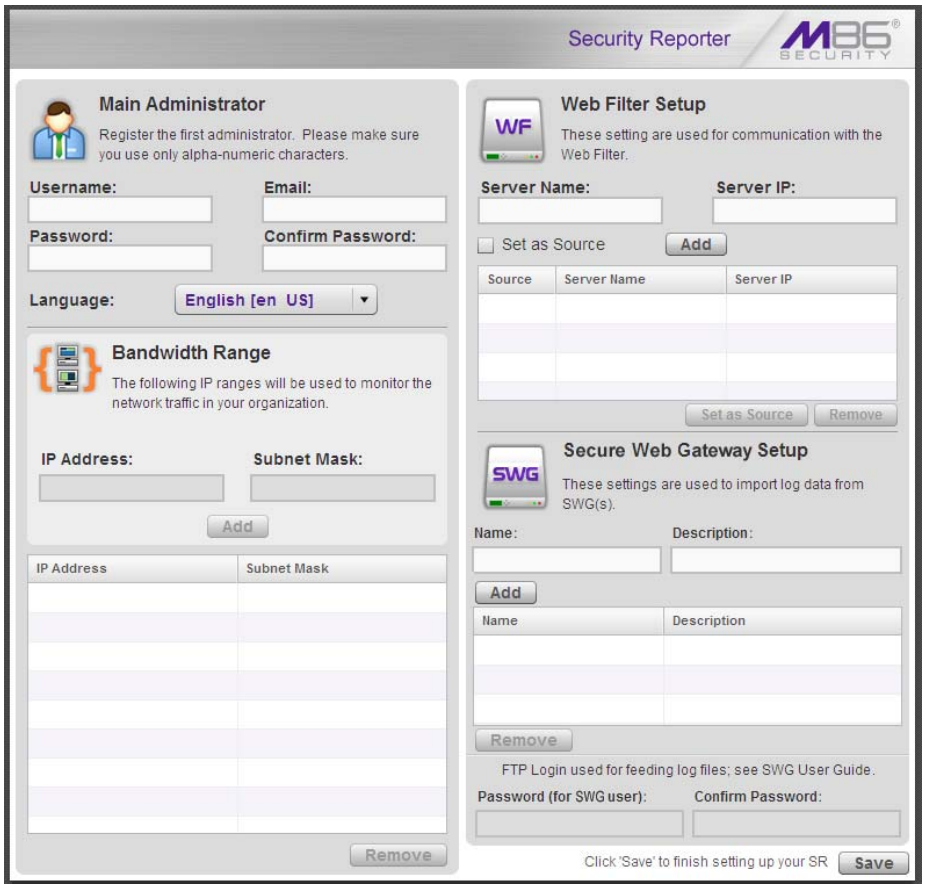
Log in to the Security Reporter Wizard

A. In the **Username** field of the Login window, type in the username specified in the Configure setup wizard user screen of the Quick Start Setup Procedures:

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

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

Use the SR Wizard to Specify Application Settings



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

- Bandwidth Range and Web Filter Setup sections, if using one or more Web Filters with this SR.

- Secure Web Gateway Setup section, if using one or more SWG policy servers with this SR.

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

Enter Main Administrator Criteria

A. Enter the **Username** the global administrator will use when logging into the Security Reporter. The global administrator has the highest level of permissions in all user applications in SR.

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

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

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

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

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

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

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

Enter Bandwidth Range

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

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

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

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

Enter Web Filter Setup Criteria

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

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

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

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

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

For SWGs: Go to Secure Web Gateway Setup

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

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

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

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

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

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

Save settings

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

Step 4: Generate SSL Certificate

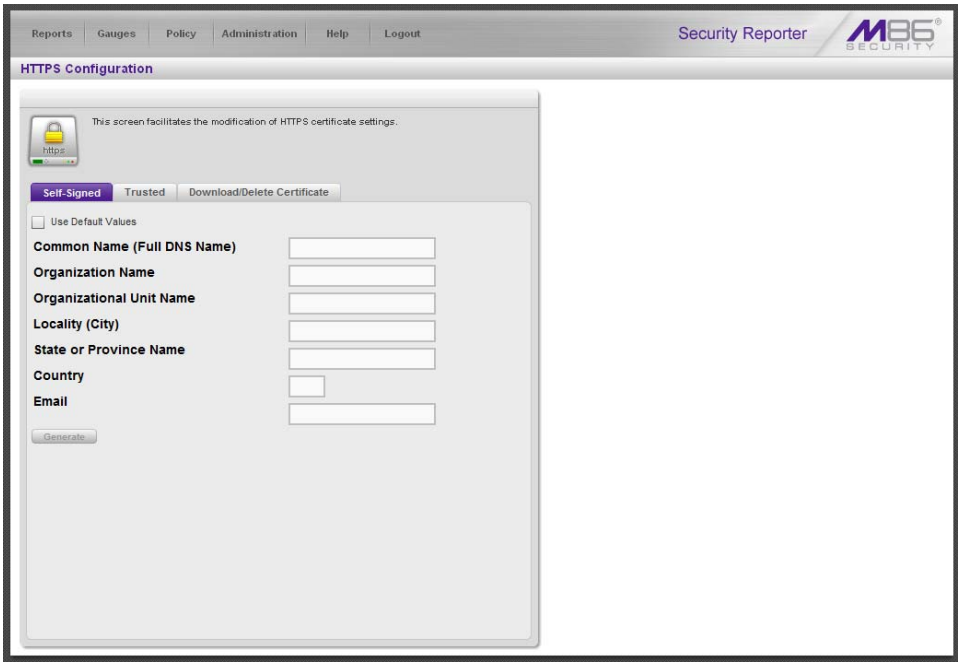
Generate a Self-Signed Certficate for the SR

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

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

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

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



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

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

D. Do the following:

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

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

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

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

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

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

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

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

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

IE Security Certificate Installation Procedures

Accept the Security Certificate in IE

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

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

Windows XP or Vista with IE 8

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

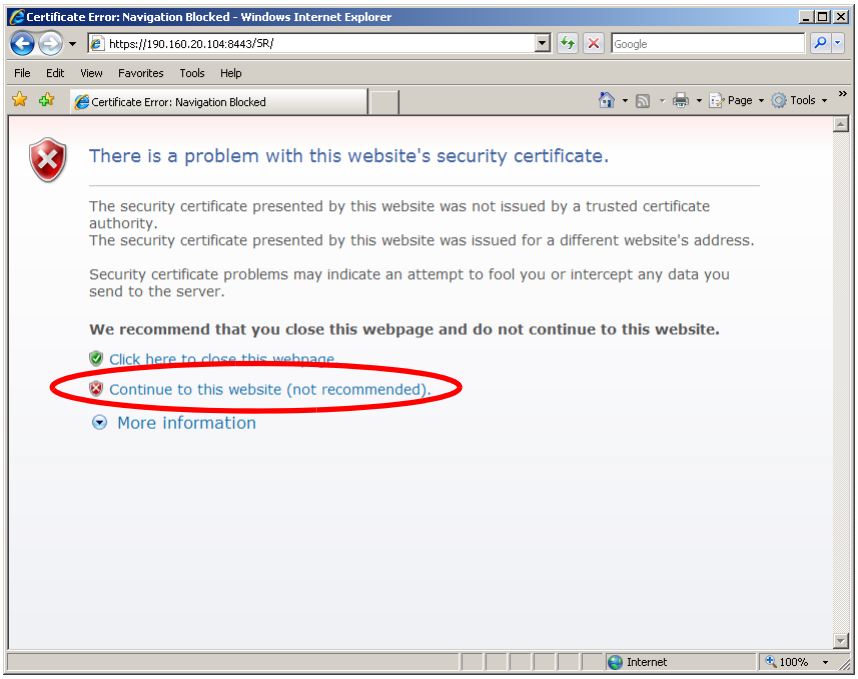


Figure A1: Windows XP, IE 8

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

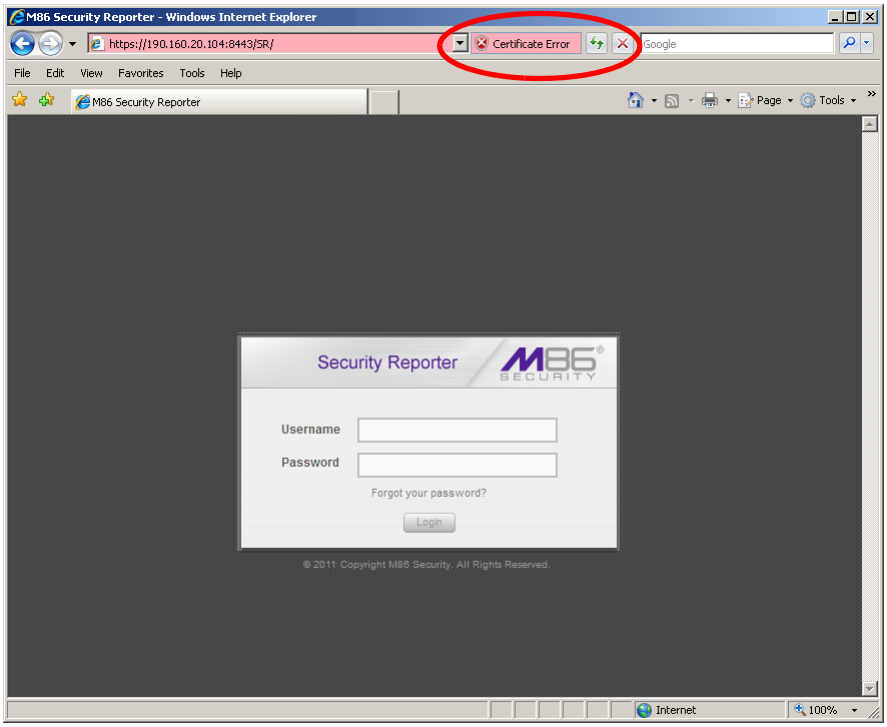


Figure A2: Windows XP, IE 8

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

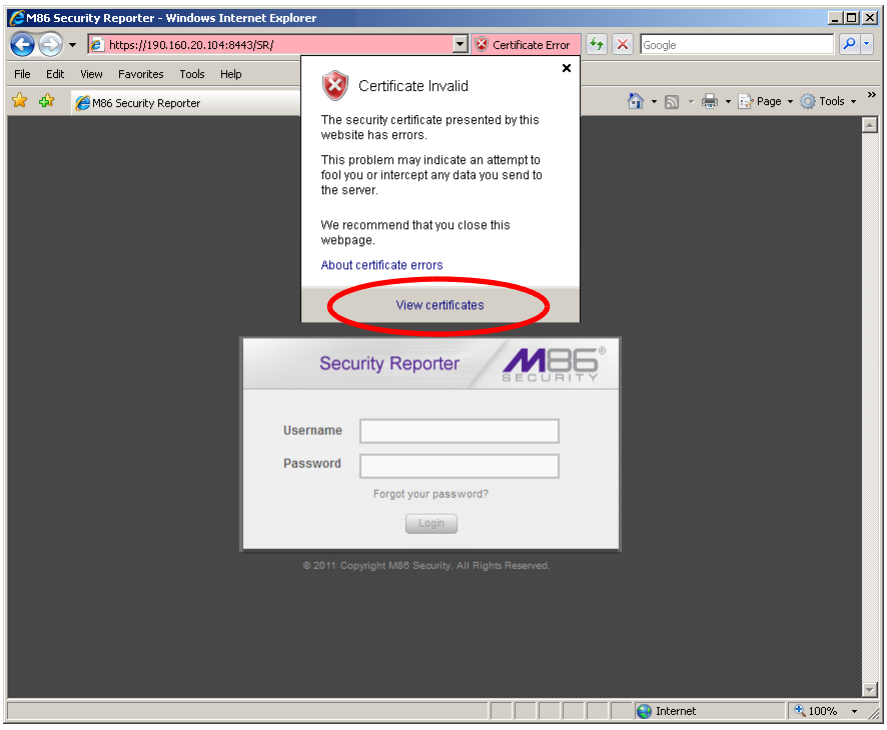


Figure B: Windows XP, IE 8

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

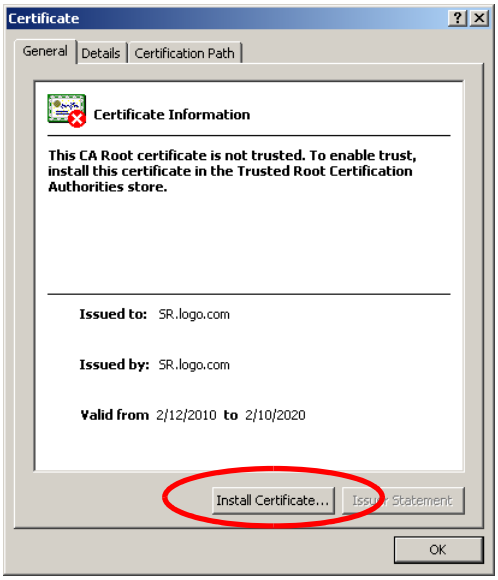


Figure C: Windows XP, IE 8

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

Figure D: Windows XP, IE 8

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

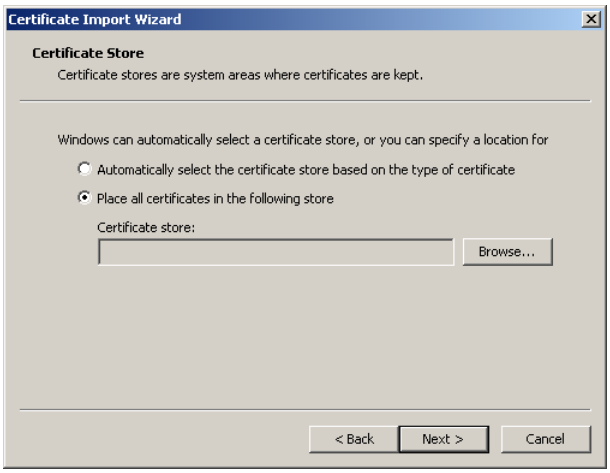


Figure E: Windows XP, IE 8

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

Figure F: Windows XP, IE 8

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

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

Figure H: Windows XP, IE 8

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

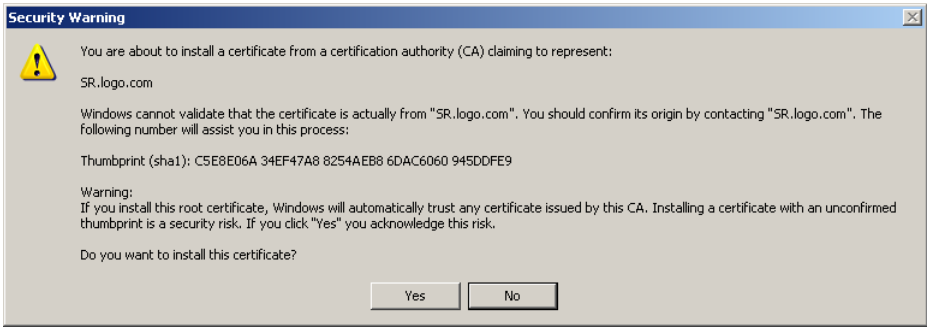


Figure I: Windows XP, IE 8

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

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

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

Windows 7 with IE 8

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

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

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

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

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

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

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

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

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

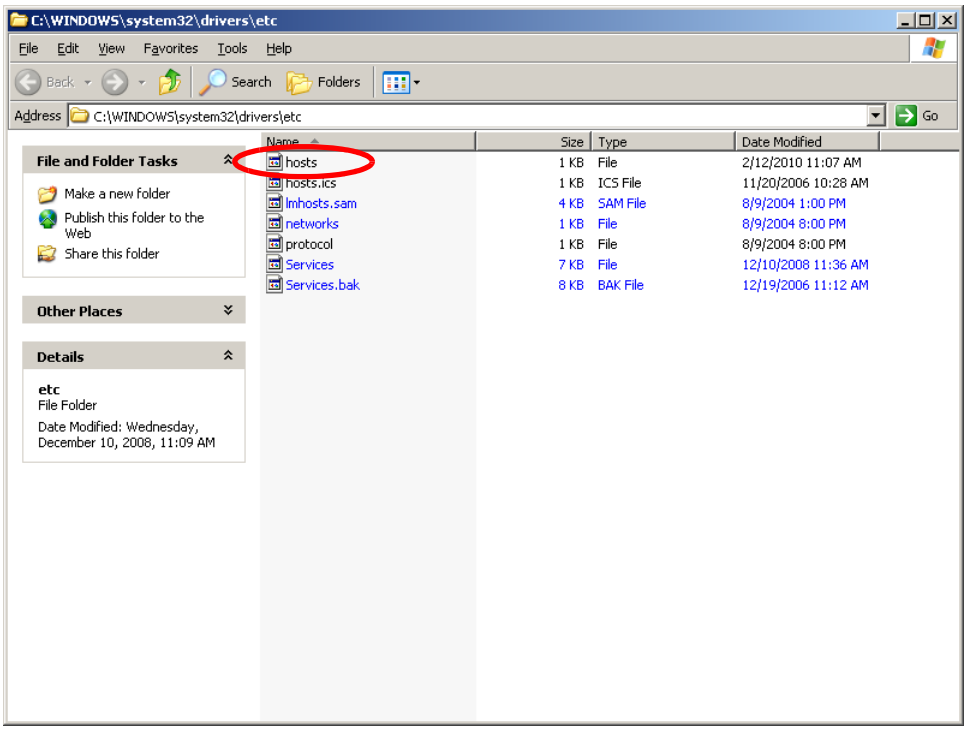
I. Select the Security tab, click **Trusted sites**, and then click **Sites** to open the Trusted sites pop-up box.

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

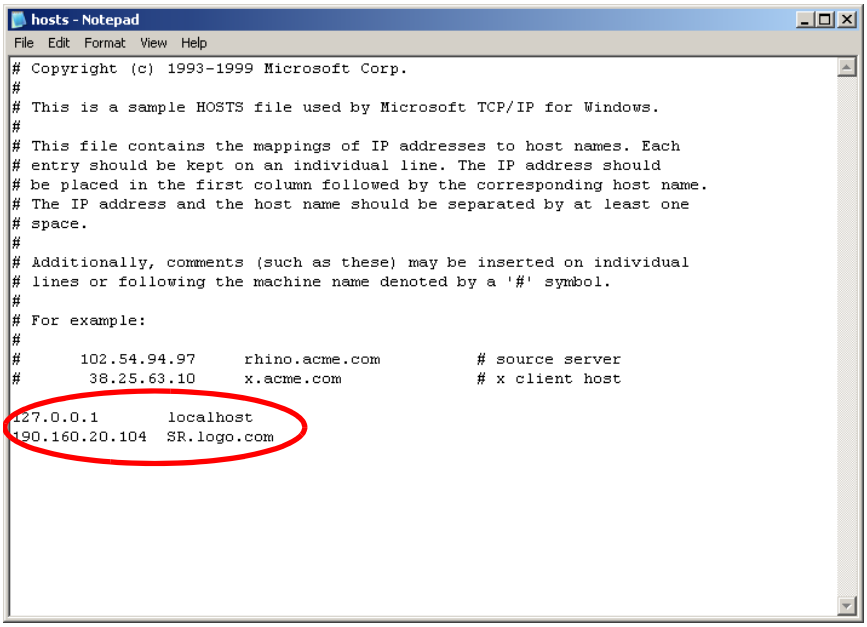
Now that the security certificate is installed, you will need to map the SR's IP address to its hostname. Proceed to Map the SR's IP Address to the Server's Hostname.

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

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

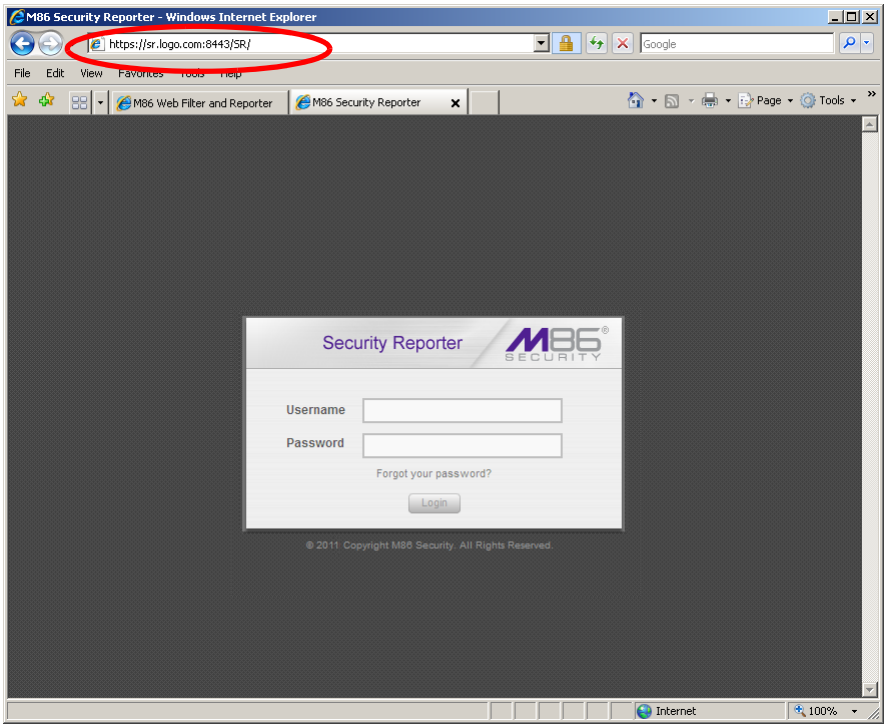


B. Double-click "hosts" to open a window asking which program you wish to use to open the file. Double-click "Notepad" or "TextPad" to launch the hosts file using that selected program:



C. Enter a line in the hosts file with the SR's IP address and its hostname—the latter entered during the Configure host name screen of the Quick Start Setup Procedures—and then save and close the file.

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

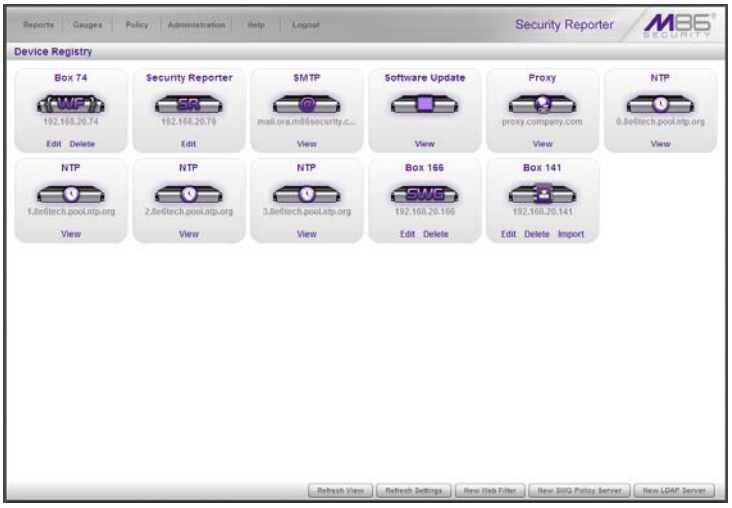


Proceed to Step 5: Add Web Filter, SWG to Device Registry.

Step 5: Add Web Filter, SWG to Device Registry

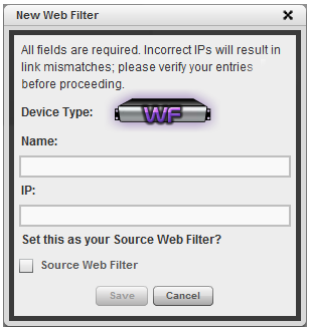
Before you begin configuring the Web Filter and/or SWG to send logs to the SR, you will need to add the Web Filter/SWG in the SR's Device Registry panel if the device(s) was/were not added during the SR Wizard installation process in Step 3.

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



Add a Web Filter Device

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



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

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

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

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

Add an SWG Device

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

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

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

C. Enter the **Password** this SR will use for communicating with this SWG and any other SWG subsequently added to the device registry. Make this same entry again in the **Confirm Password** field.

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

Step 6: Set up Web Filter, SWG Log Transfers

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

Web Filter Setup

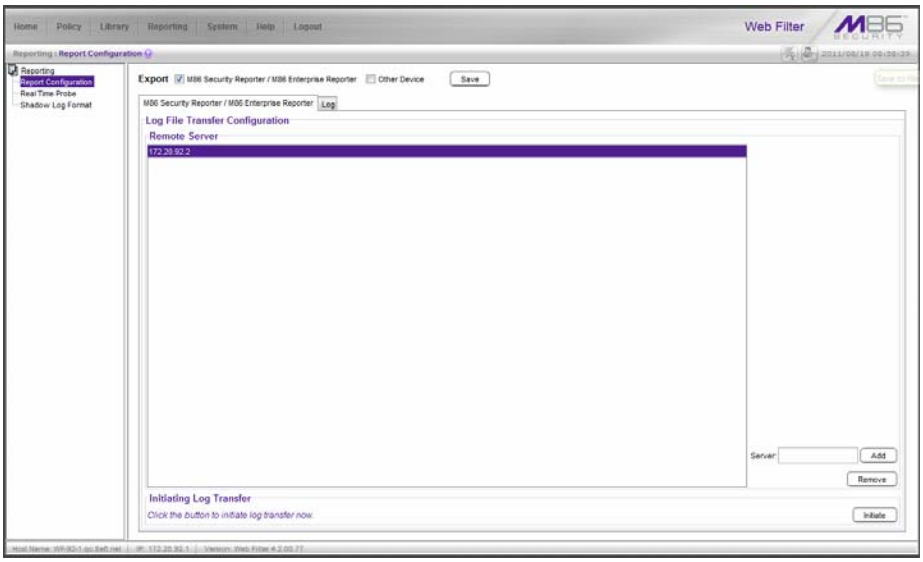
Web Filter Configuration

A. Access the user interface of the Web Filter.

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

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

D. Select **M86 Security Reporter / M86 Enterprise Reporter** to display the M86 Security Reporter / M86 Enterprise Reporter tab:



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

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

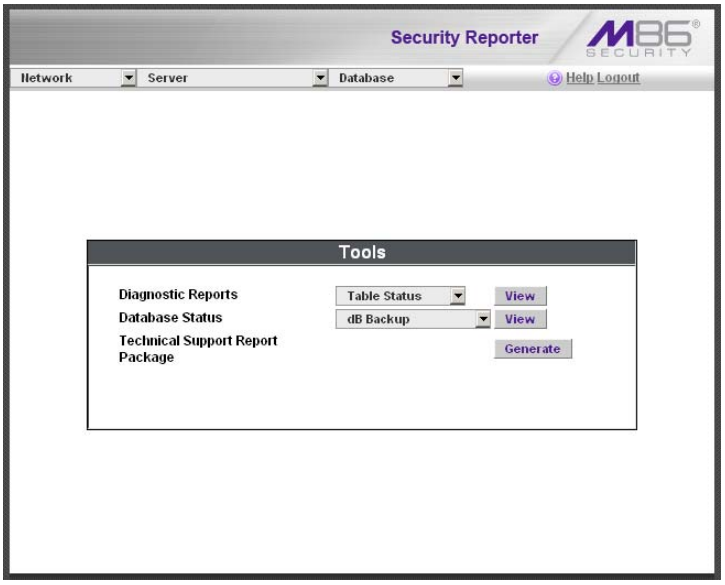
***NOTE**: It is recommended you wait for 1 - 2 hours after the initial installation so sufficient data is available for viewing.*

Web Filter Log Transfer Verification

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

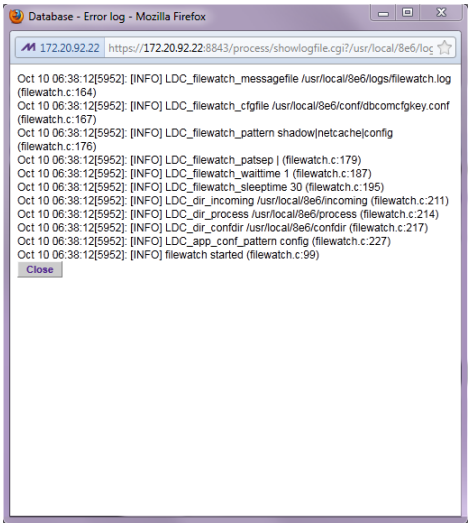
A. Access the System Configuration administrator console.

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



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

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

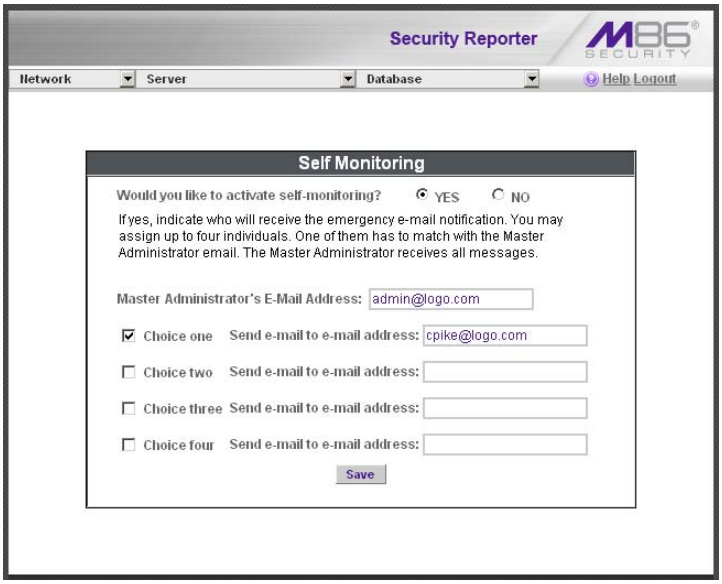


The transfer is working if you see an entry that includes the date and time for incoming shadow logs. The transfer should occur every hour. Once you see an entry, reporting information will be available one hour after the timestamp of the import listing.

Set Self-Monitoring

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

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



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

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

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

F. Click **Save**.

SWG Setup

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

SWG Configuration for Software Version 10.0

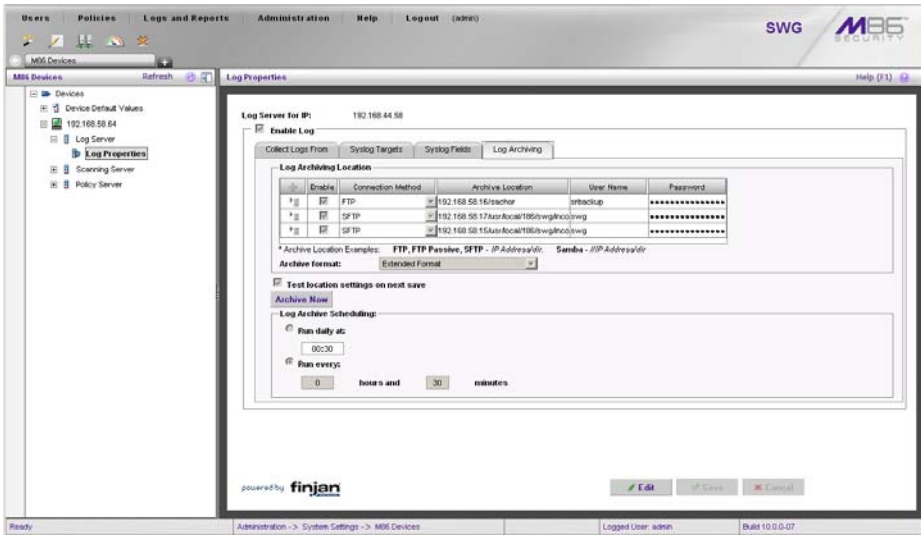
Configure SWG to Send Logs to the SR

A. Access the SWG user interface.

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

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

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



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

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

- **Connection Method**: Select "SFTP" from the pull-down menu.
- **Archive Location**: Type in the IP address of this SR appended by a slash character (/) and the word 'incoming'. For example: ***200.260.10.56/ incoming*** for an SR with that IP address.
- **User Name**: Type in the SWG's Username from the Device Registry, which is ***swg*** (in lower case characters).
- **Password**: Type in the password you entered for the SWG in the Device Registry.

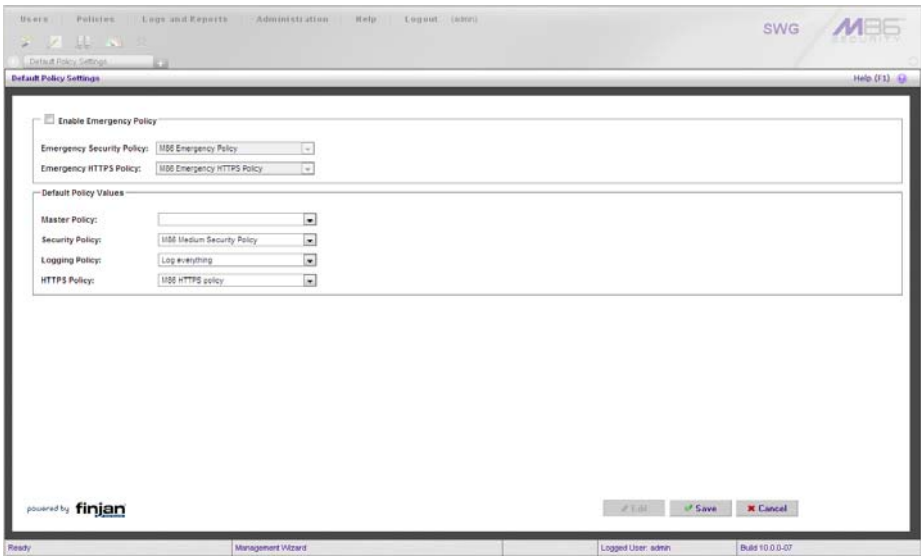
***NOTE**: Be sure "Extended Format" is selected for Archive format, and Log Archive Scheduling specifies the correct interval you wish to use for sending logs from the SWG to the SR.*

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

Policy Settings

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

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



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

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

SWG Configuration for Software Version 9.2.5

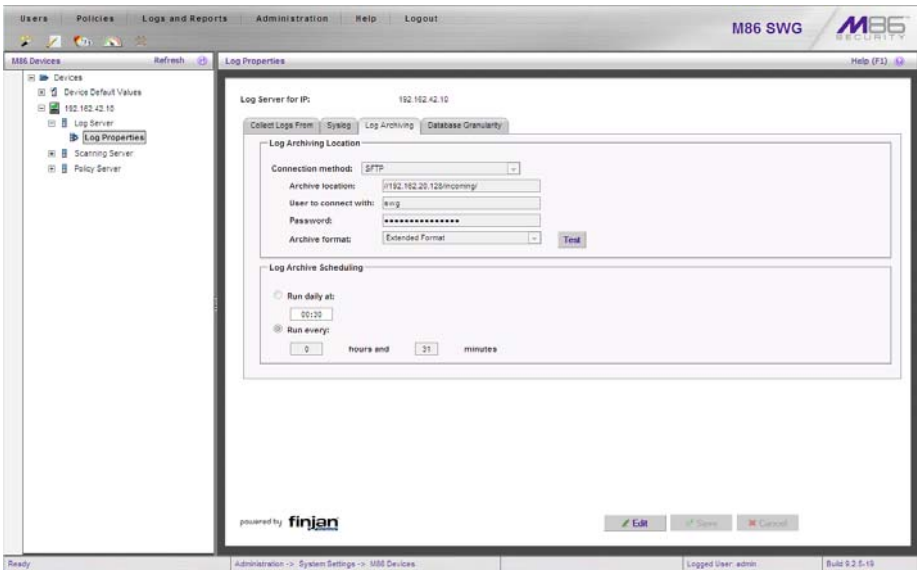
Configure SWG to Send Logs to the SR

A. Access the SWG user interface.

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

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

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



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

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

- **Connection Method**: "SFTP" is selected from the pull-down menu.
- **Archive Location**: The IP address of this SR is preceded by double slash characters (//) and followed by a single slash character (/), the word 'incoming', and another single slash character. For example: ***//200.260.10.56/incoming/*** for an SR with that IP address.
- **Password**: The password you entered for the SWG in the Device Registry.
- **Archive Format**: "Extended" is selected from the pull-down menu.

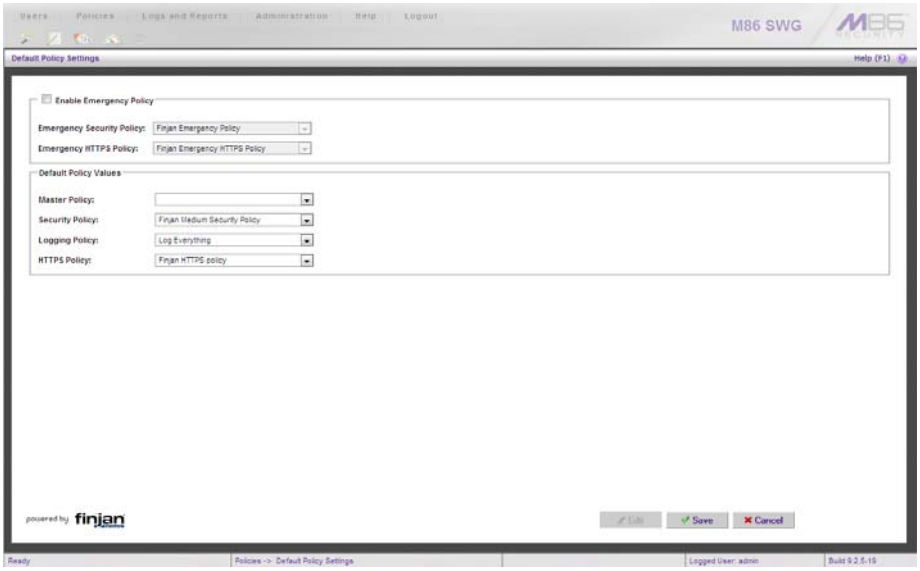
***NOTE**: Be sure Log Archive Scheduling specifies the correct interval you wish to use for sending logs from the SWG to the SR.*

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

Policy Settings

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

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



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

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

Single Sign-On Access, Default Username/Password

Single Sign-On Access

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

Default Usernames and Passwords

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

Application	Username	Password
Security Reporter	admin	testpass
Web Filter	admin	user3

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

CONCLUSION

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

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

For real time and security reports, the next step is to set up user groups or administrator groups. For real time reports, you will set up and configure gauges thereafter.

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

***NOTE**: If you cannot view reports, or if your specific environment is not covered in the Security Reporter User Guide, contact an M86 Security solutions engineer or technical support representative.*

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

BEST REPORTING PRACTICES

This Best Reporting Practices section is provided to help you get started using the Report Manager user interface. The main areas of focus in this section are productivity reporting, security reporting, and real time reporting.

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

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

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

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

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

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

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

Productivity Reports Usage Scenarios

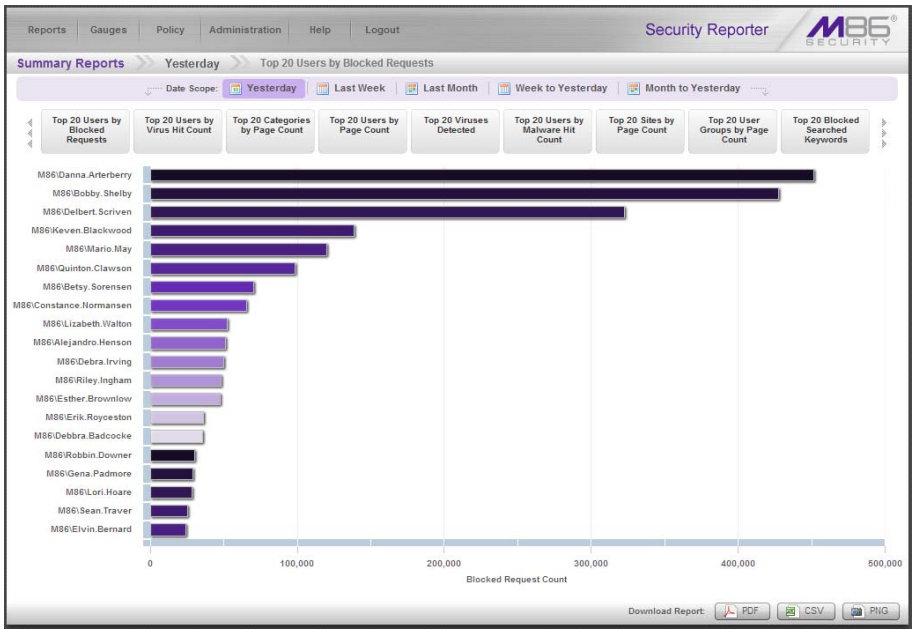
This collection of productivity reporting scenarios is designed to help you use the Report Manager to create typical snapshots of end user Internet activity. Each scenario is followed by setup information. Please consult the “How to” section in the index of the Security Reporter User Guide for pages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

I. Summary Report and Drill Down Report exercise

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

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

From the navigation menu, select **Reports > Summary Reports** to display yesterday’s “Top 20 Users by Blocked Requests” Summary Report containing pre-generated data. Since the data has already been captured from the previous day, the report loads quickly in your browser:



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

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

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

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

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

Step B: Further investigate using a Summary Drill Down Report

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

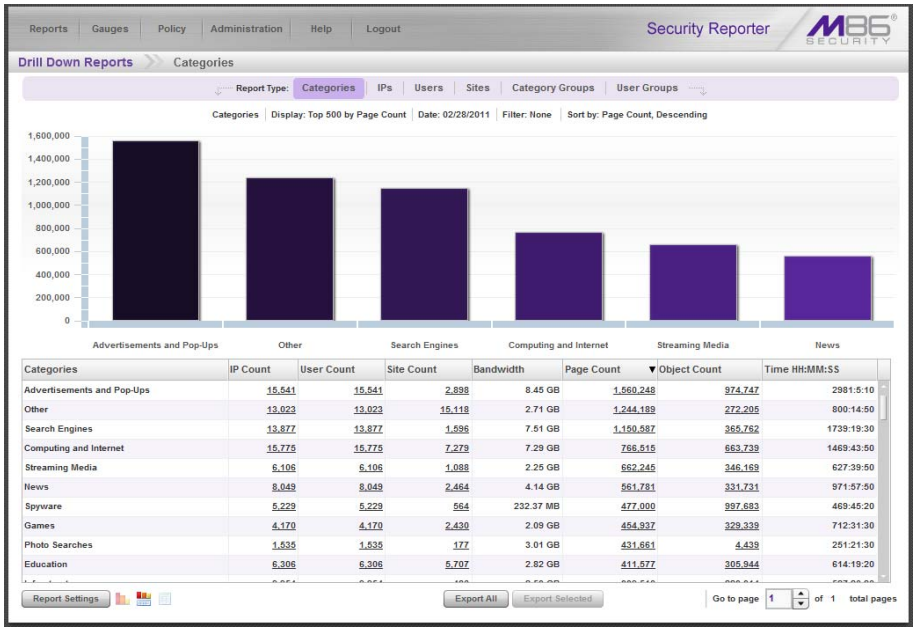
From the navigation menu, go to **Reports > Drill Down Reports > Categories** to display the generated Summary Drill Down Report view, ranking categories in order by the most visited.

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

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

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

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



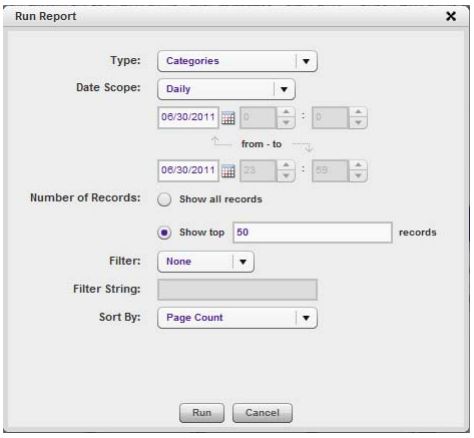
Note that the drill down report view has been generated for today's activity by default.

To continue this investigation using data from yesterday's Summary Report, you must create a new report from this current report view by first changing the date scope.

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

Step C: Create a new report using yesterday's date scope

1. At the bottom of the Summary Drill Down Report view, navigate to **Report Settings > Run** to open the Run Report pop-up window:



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

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

Step D: Create a report grouped by two report types

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

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

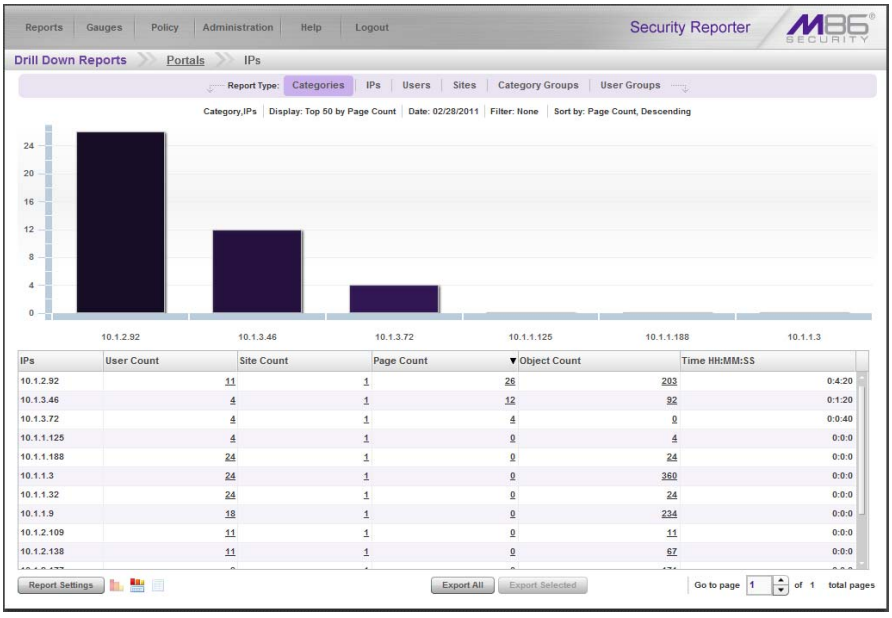
2. Now, to find out who is visiting sites in this category, you will need to identify the user(s).

   Since there are two sets of criteria you need for this exercise, you must drill down into the selected category and also specify that you wish to view user IP addresses, thereby creating a report view grouped by two report types.

   Note the Count columns to the right of the Categories column, each with clickable links.

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

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



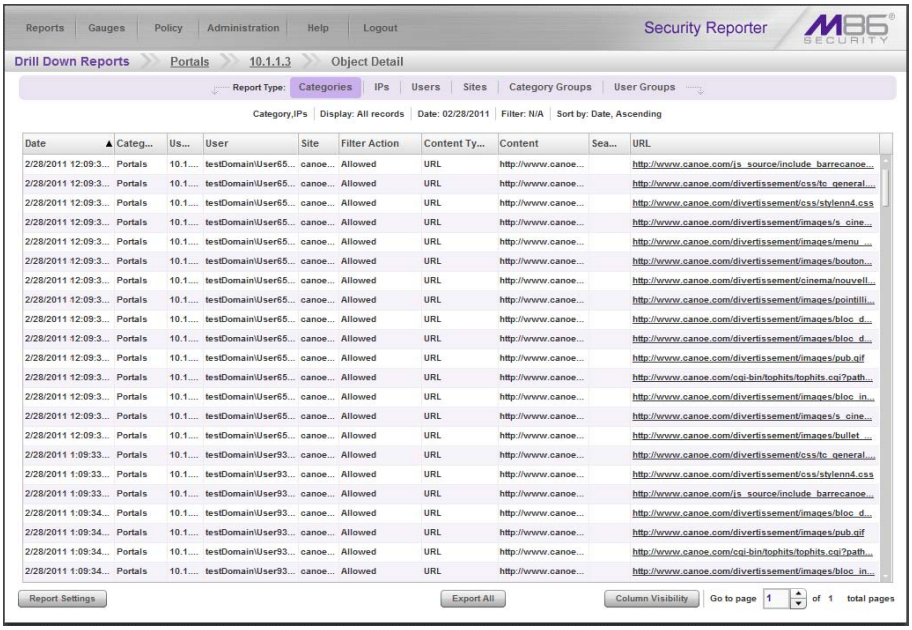
After executing the last command, note that user IP addresses now display in the first column of the report view instead of categories.

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

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

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

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



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

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

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

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

---

You have now learned how to access Summary Reports and to use Drill Down Reports to conduct an investigation. You have also learned how to change the date scope of a Drill Down Report to create a new report, generate a report view grouped by two report types, and drill down into the current summary report view to create a detail report view.

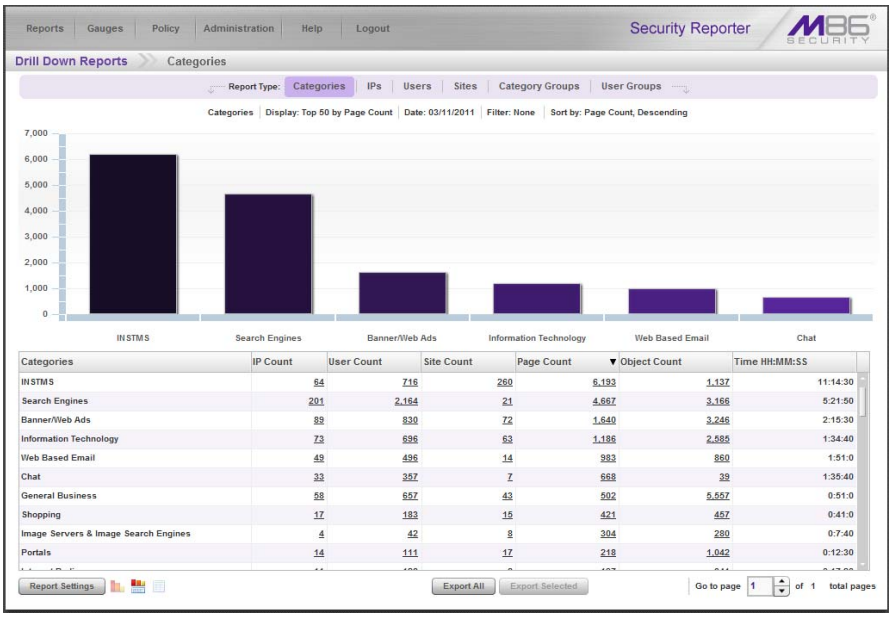
These tools and other tools can be used separately or combined to create many different types of reports to fulfill different purposes.

II. 'Group By' Report and Export Report exercise

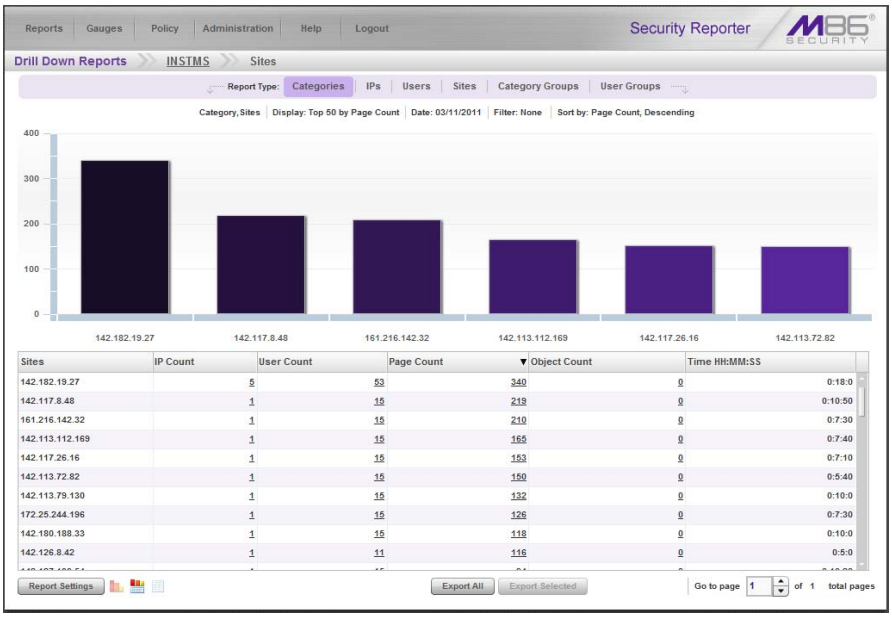
In this exercise you will learn how to display only the top 10 records of a summary drill down 'group by' report view, export that report view in the PDF output format, and then view the results of the generated PDF file.

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

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



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



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

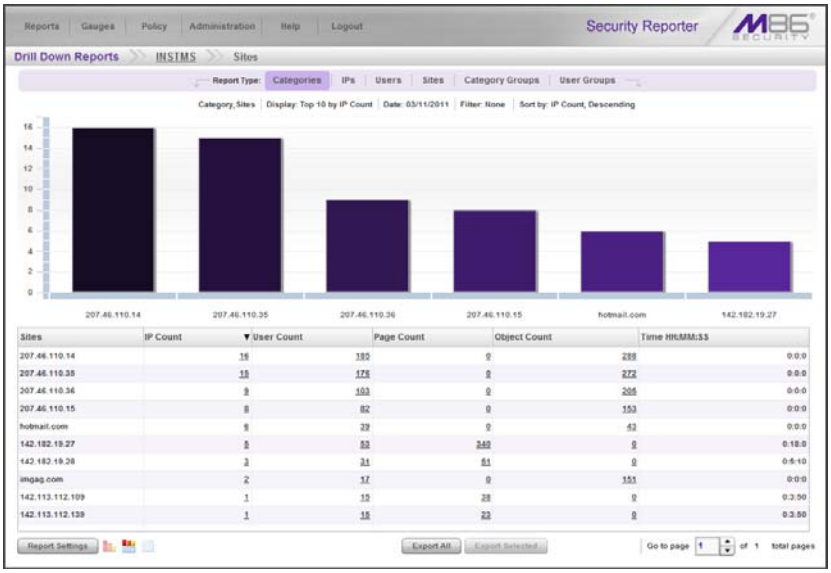
In the Security Reporter User Guide index, see:
• How to: generate a Drill Down Report
• How to: use count columns and links

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

1. Now, to only display the top 10 sites users visited in that category, navigate to **Report Settings > Run** to open the Run Report pop-up window in which you make customizations to display in the current report view:

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

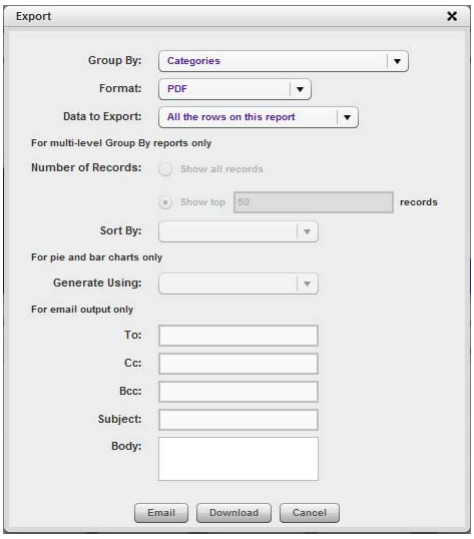
2. At the **Number of Records** field, select "Show top" and and type in ***10*** records.
3. Select **Sort By** "IP Count".
4. Click **Run** to close the pop-up window and to display the report view showing only the top 10 site records for the selected category:



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

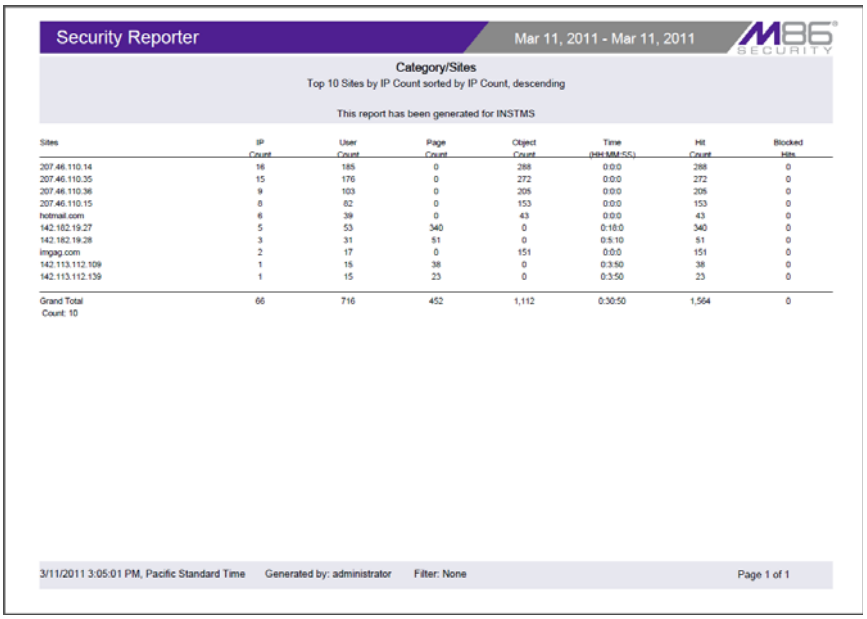
Step C: Export the report view in the PDF output format

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



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

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



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

***NOTE**: Notice that the report is sorted by IP Count, the selection made in the Run Report pop-up window.*

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

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

See also:
• How to: export a detail report
• How to: email a productivity report

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

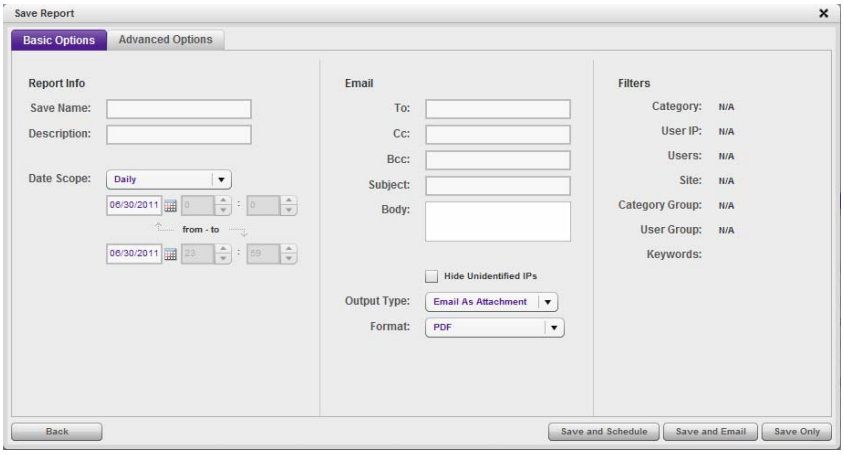
Variations of this exercise can be performed to generate and export countless reports using criteria of your specifications.

III. Save and schedule a report exercise

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

Step A. Save a report

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



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

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

3. Choose the **Save and Schedule** option from the "save" options at the bottom of the window. The three "save" options are as follows:
   - **Save and Schedule** - this option lets you save criteria from the current report view and then set up a schedule to run the report using that criteria.
   - **Save and Email** - this option lets you save criteria from the current report view and then email the report in the specified output format.
   - **Save Only** - this option lets you save criteria from the current report view.

***NOTE**: Saved reports can be edited at any time. These reports are accessed by going to Reports > Saved Reports, and then choosing the report from the **Reports list**.*

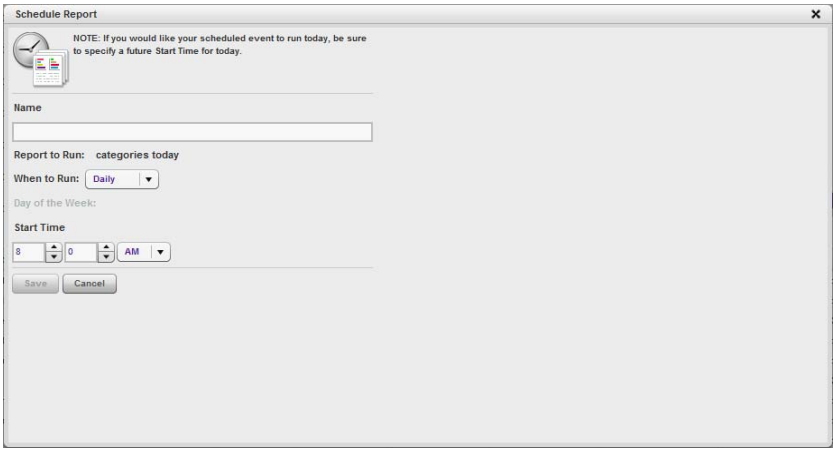
In the Security Reporter User Guide index, see:
• How to: save a productivity report

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

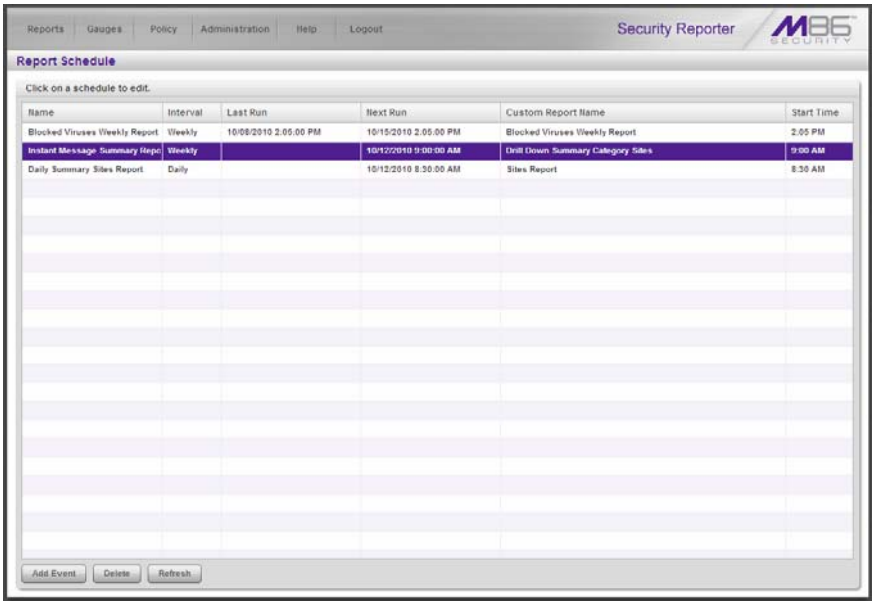
Step B. Schedule a recurring time for the report to run

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



3. In the Schedule Report 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 with the message confirming the event was successfully added.
5. Click **OK** to close the alert box and to display the Report Schedule panel with the event added to the schedule:



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

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

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

IV. Create a Custom Category Group and generate reports

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

Step A: Create a Custom Category Group

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

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

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

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

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

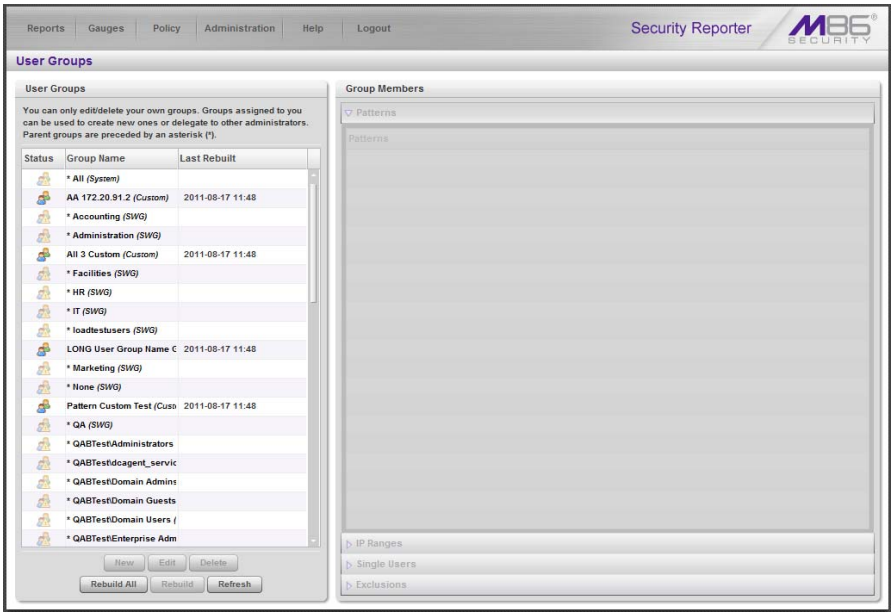
V. Create a custom User Group and generate reports

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

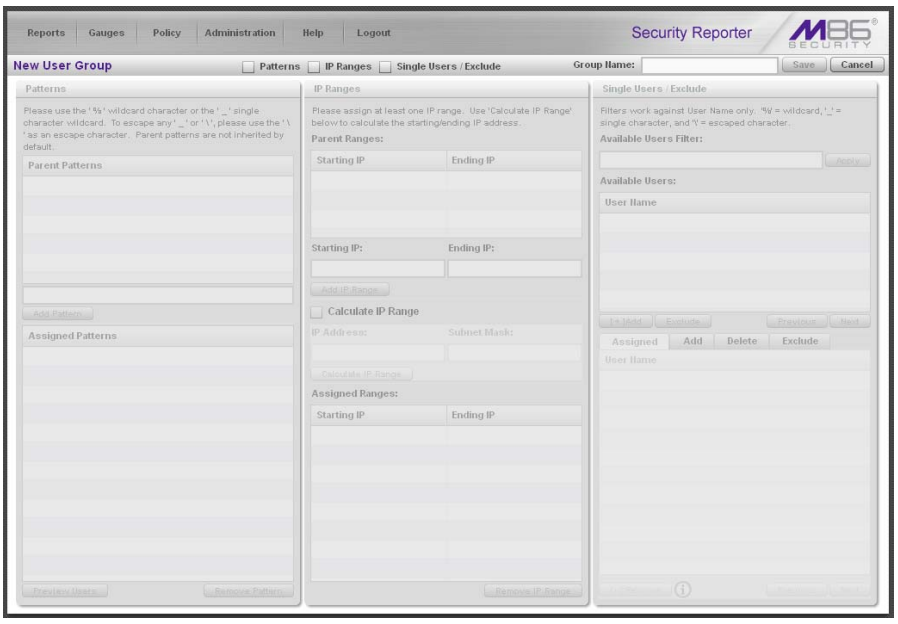
***NOTE**: In order to generate reports for a custom user group, the user group must be created a day in advance, since the list of users is updated each day automatically based on group definitions and latest usage data.*

Step A: Create a custom User Group

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



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



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

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

Step B: Generate a report for a custom User Group

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

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

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

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

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

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

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

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

Security Reports Usage Scenarios

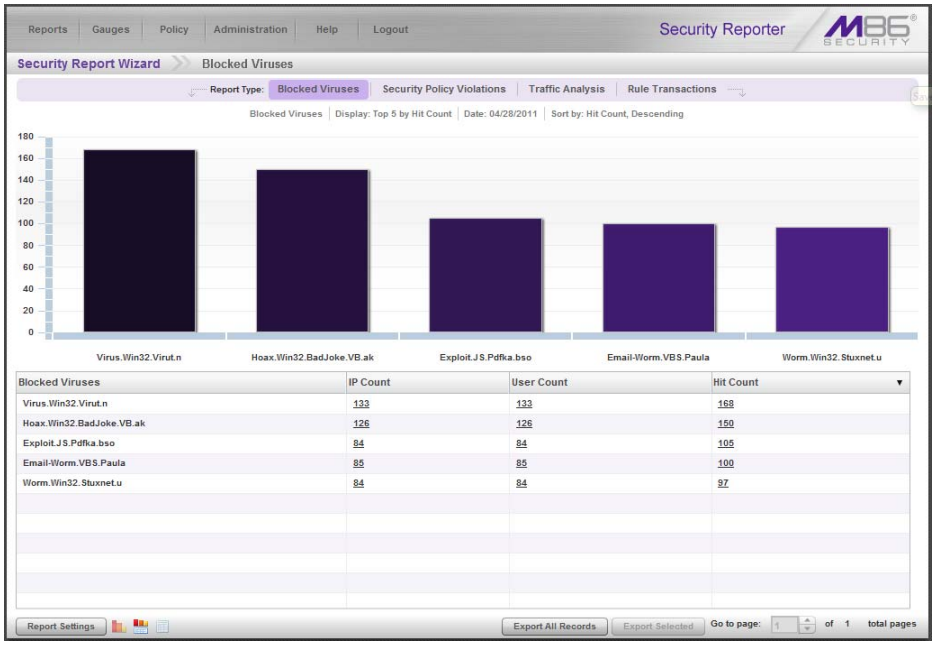
This collection of reporting scenarios is tailored towards familiarizing you with tools for generating, exporting, saving, and scheduling security reports. Each scenario is followed by user interface access information. Please consult the "How to" section in the index of the Security Reporter User Guide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

I. Explore the four basic Security Reports types

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

Step A: Navigate to the Blocked Viruses report

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



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

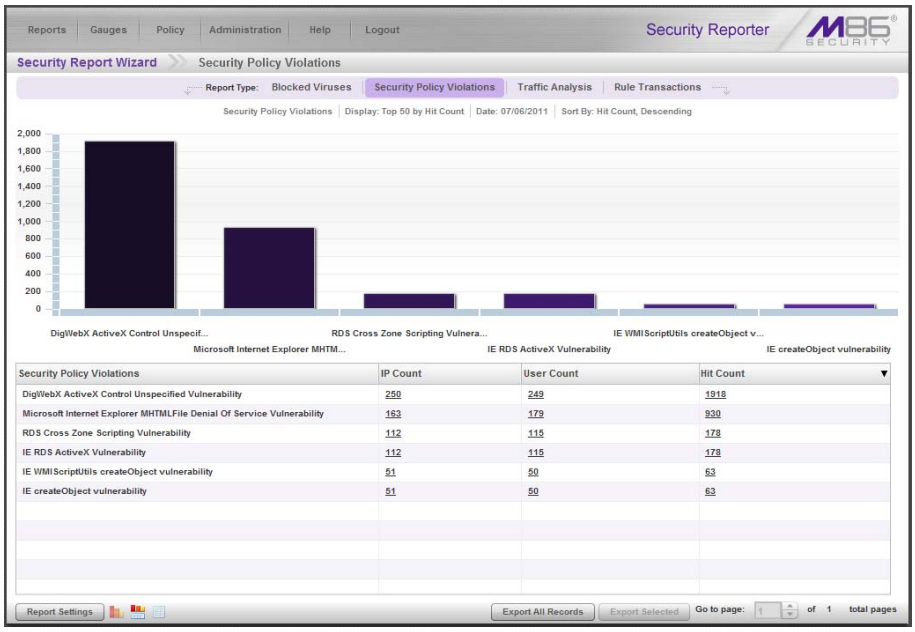
Note the tabs for the four Report Types at the top of the panel. By default, the bar chart beneath these tabs depicts the first six records for the current report type.

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

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

Step B: Navigate to the Security Policy Violations report

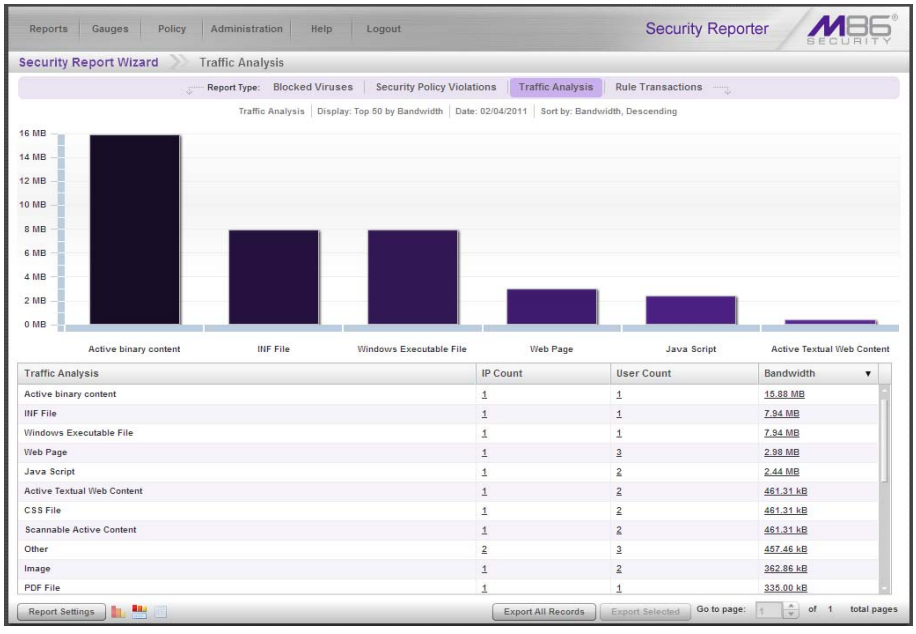
Click the **Security Policy Violations** tab to display the the Security Policy Violations report view:



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

Step C: Navigate to the Traffic Analysis report

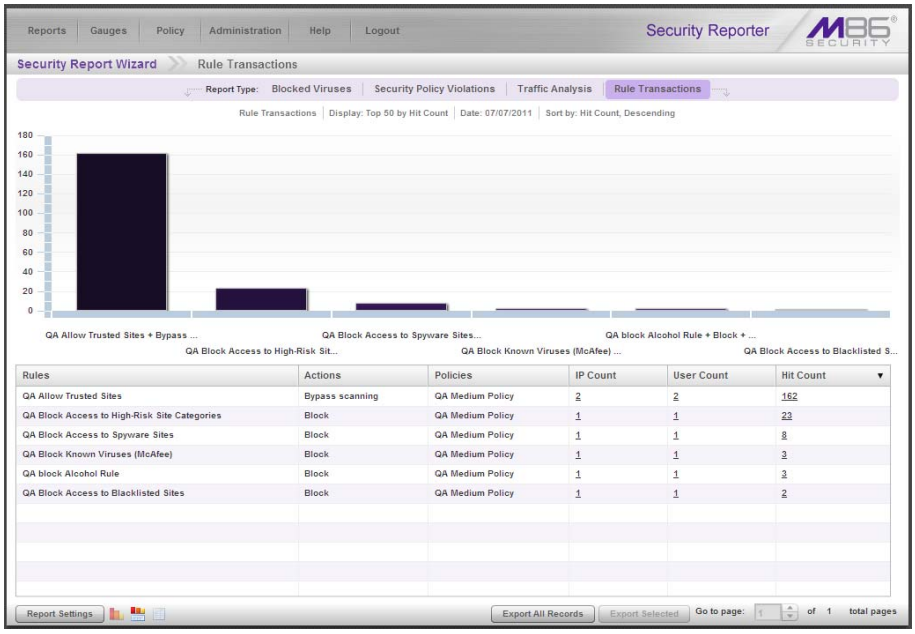
Click the **Traffic Analysis** tab to display the Traffic Analysis report view:



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

Step D: Navigate to the Rule Transactions report

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

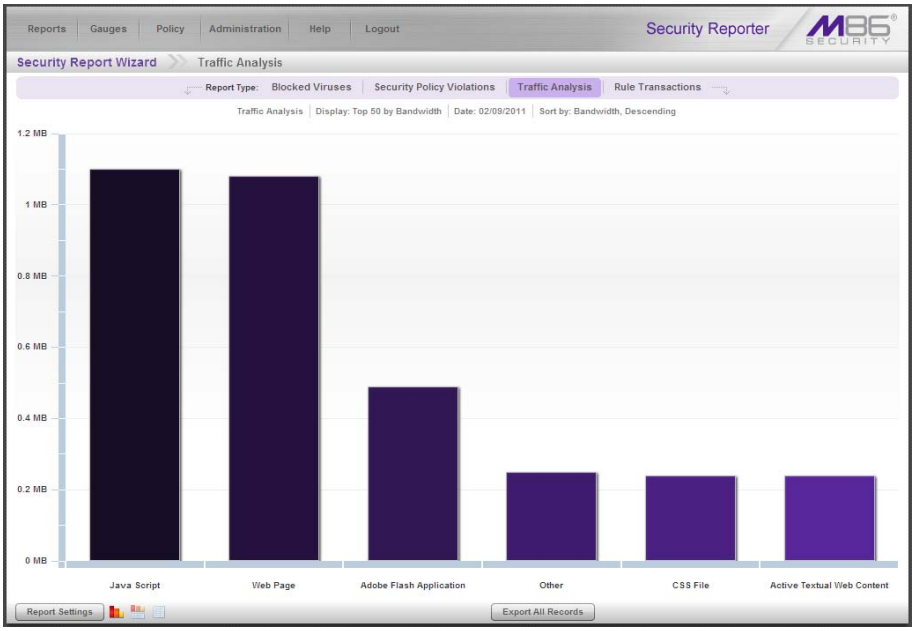


This report includes each instance in which an end user triggered a threshold in an SWG Security Policy.

Step E: Modify the current report view

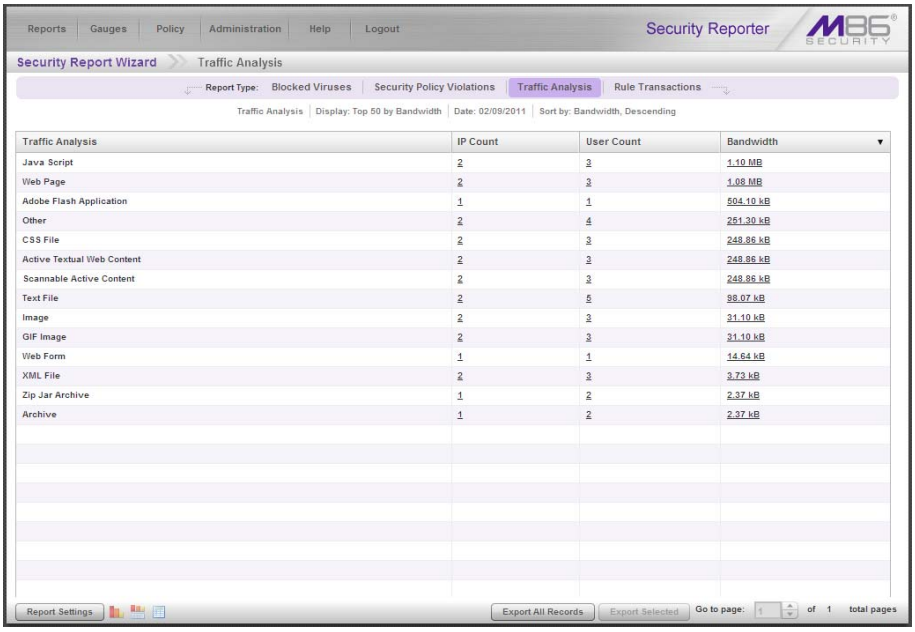
Now that you have viewed the four basic report types, you will learn how to modify the current report view. With a security report view displayed, go to the icons at the bottom left of the panel and do the following:

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



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

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



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

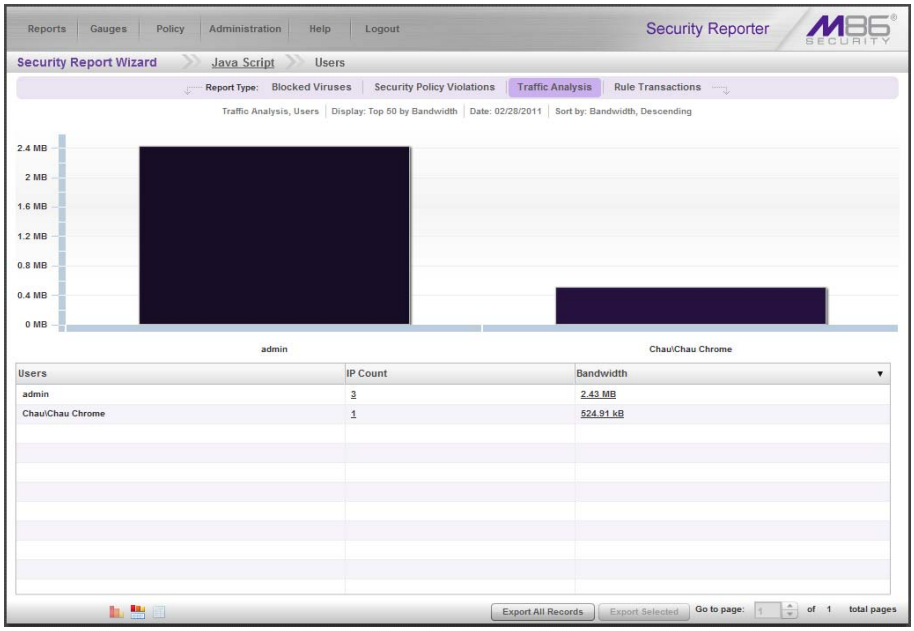
II. Create a drill down Security Report view

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

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

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

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



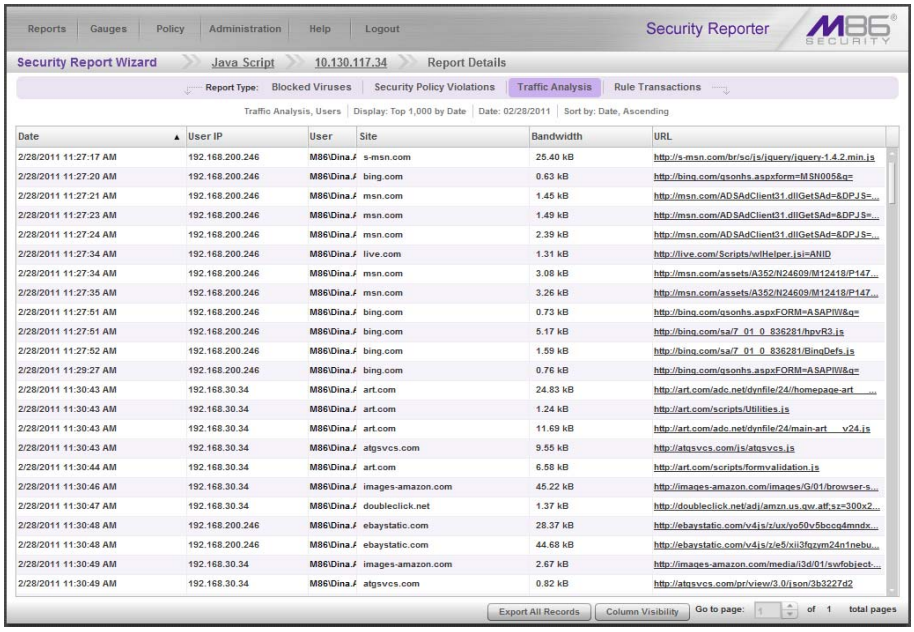
Note that this report view looks similar to a basic security report view, with the following exceptions:

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

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

Exercise B: Create a detail report view

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



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

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

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

---

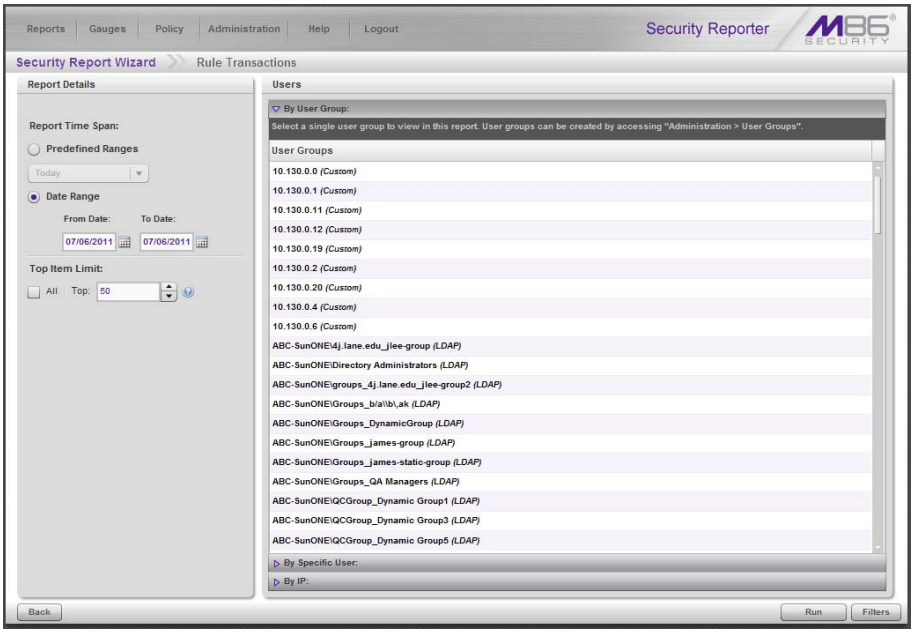
In the Security Reporter User Guide index, see:
• How to: drill down into a Security Report
• How to: use Security Report tools

III. Create a customized Security Report

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

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

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



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

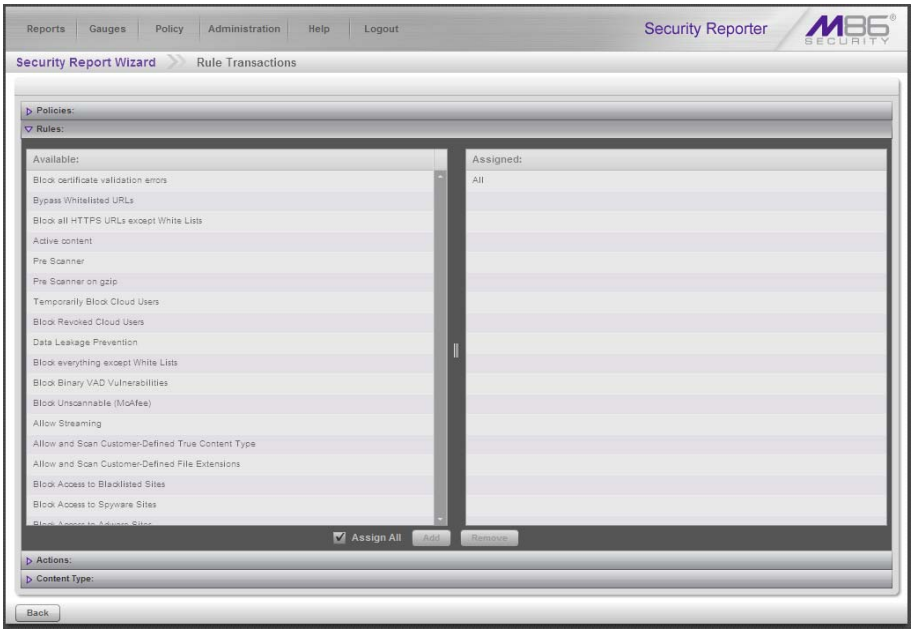
***NOTE**: Choosing "All" records may take a long time for the report to generate, depending on the number of records to be included.*

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

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

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

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

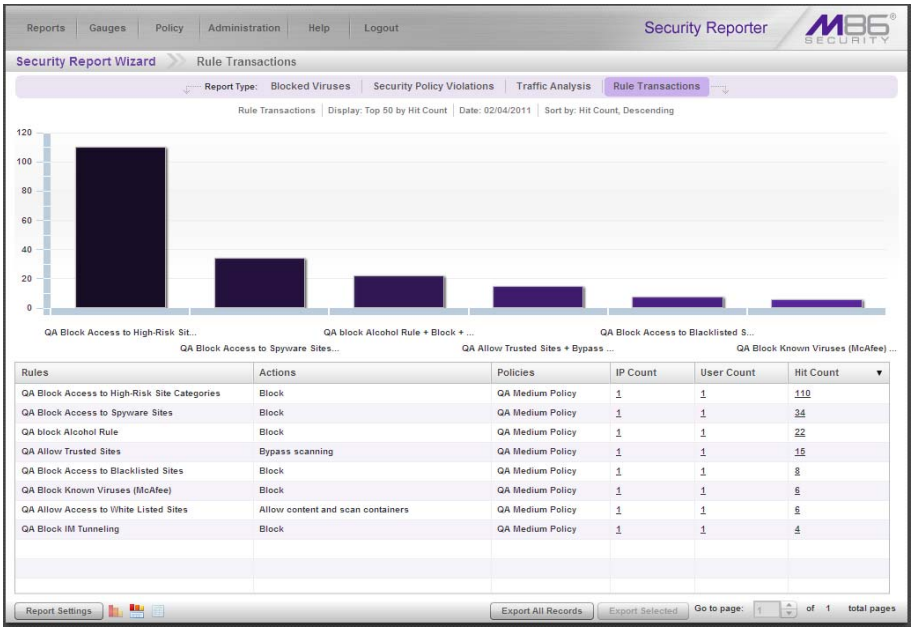


b. Choose a filter type from an available accordion (Policies, Rules, Action, Content Type) and indicate criteria to use in the filter:

- Select one or more records from the Available list box and click **Add** to move the record(s) to the Assigned list box.
- Click the "Assign All" checkbox to select all records and grey-out the panel.

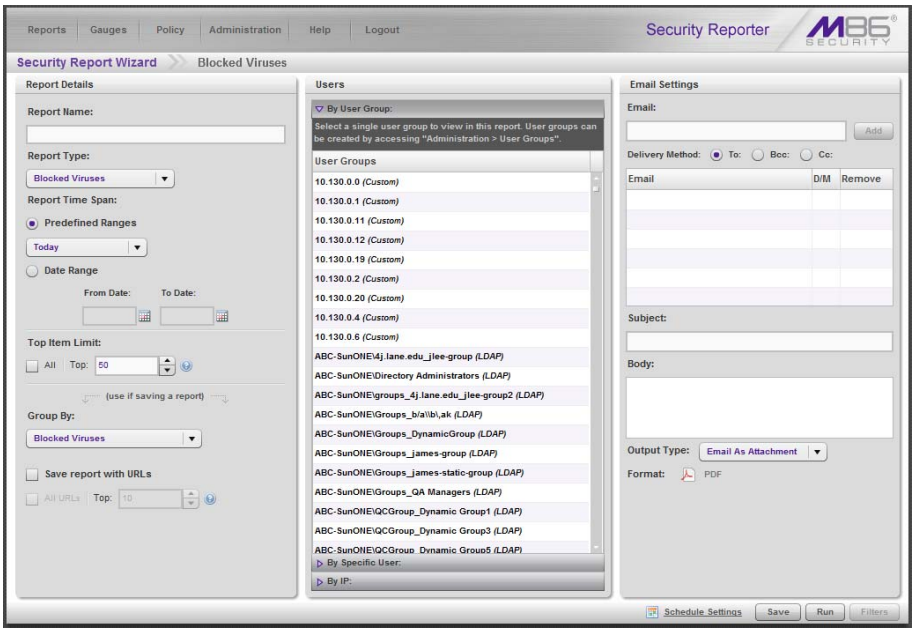
c. Click **Back** to return to the Security Report Wizard panel.

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



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

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



2. In Report Details, choose the **Report Type** from the pull-down menu (“Blocked Viruses”, “Security Policy Violations”, “Traffic Analysis”, “Rule Transactions”); by default “Blocked Viruses” displays.

3. Specify the **Report Time Span** by choosing one of two options:

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

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

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

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

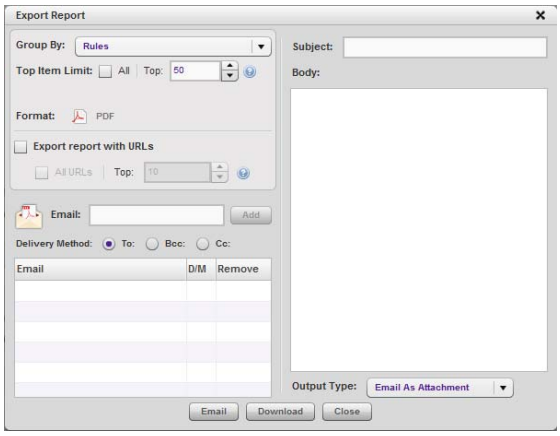
In the Security Reporter User Guide index, see:
• How to: run a Security Report

IV. Export a Security Report

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

Step A: Specify records to include in the report

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



Export Report pop-up window, Export All Records option

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

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

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

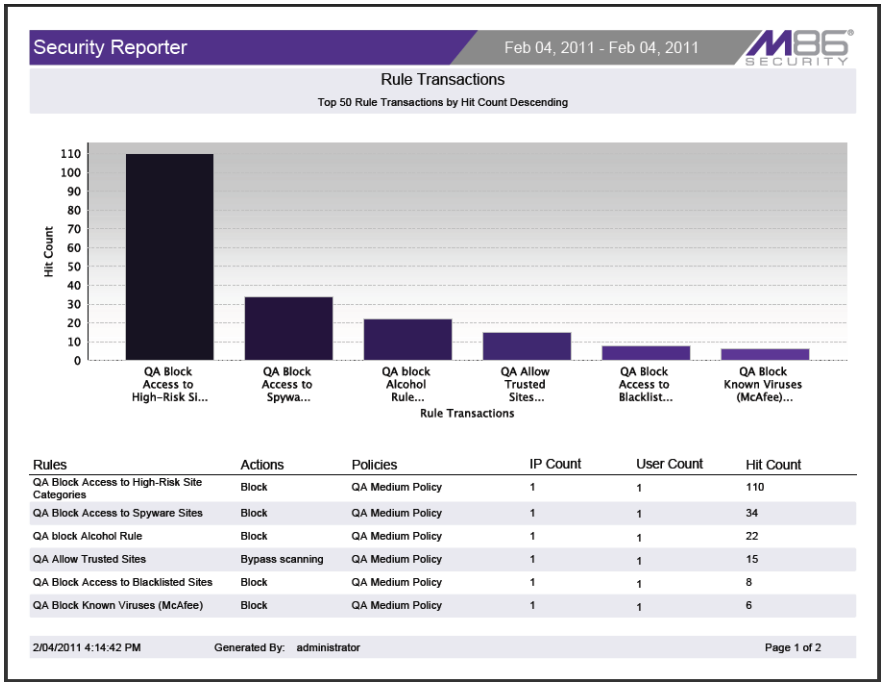
   - If the Export Selected option was selected, "All" is greyed-out. Specify the **Top** number of items to be included in the exported report.
3. By default, **Export report with URLs** is de-selected. Click this checkbox to select this option, and then specify the number of URLs to export:
   - **All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

Step C: Download the report

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

Step D: View the exported Security Report

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

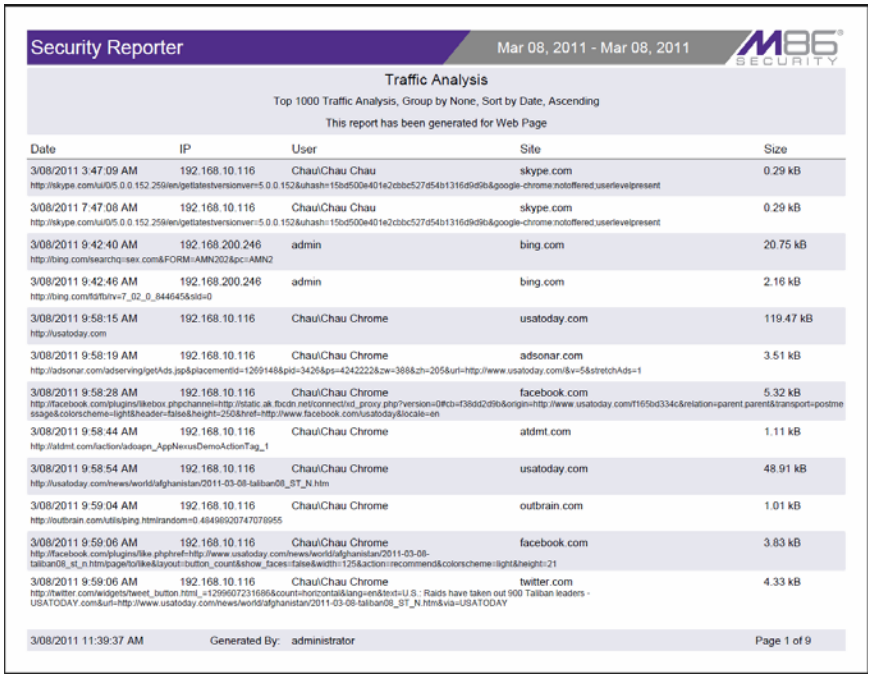


The header of the generated report includes the date range, report type, and report criteria, and report description.

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

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

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



Security Reporter — Mar 08, 2011 - Mar 08, 2011

Traffic Analysis

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

This report has been generated for Web Page

Date	IP	User	Site	Size
3/08/2011 3:47:09 AM	192.168.10.116	Chau\Chau Chau	skype.com	0.29 kB
http://skype.com/ui/0/5.0.0.152.259/en/getlatestversionver=5.0.0.152&uhash=15bd500e401e2cbbc527d54b1316d9d9b&google-chrome:notoffered;userlevelpresent				
3/08/2011 7:47:08 AM	192.168.10.116	Chau\Chau Chau	skype.com	0.29 kB
http://skype.com/ui/0/5.0.0.152.259/en/getlatestversionver=5.0.0.152&uhash=15bd500e401e2cbbc527d54b1316d9d9b&google-chrome:notoffered;userlevelpresent				
3/08/2011 9:42:40 AM	192.168.200.246	admin	bing.com	20.75 kB
http://bing.com/search?q=sex.com&FORM=AMN202&pc=AMN2				
3/08/2011 9:42:46 AM	192.168.200.246	admin	bing.com	2.16 kB
http://bing.com/fd/ftb/rv=7_02_0_844645&sid=0				
3/08/2011 9:58:15 AM	192.168.10.116	Chau\Chau Chrome	usatoday.com	119.47 kB
http://usatoday.com				
3/08/2011 9:58:19 AM	192.168.10.116	Chau\Chau Chrome	adsonar.com	3.51 kB
http://adsonar.com/adserving/getAds.jsp&placementId=1269148&pid=3426&ps=4242222&zw=368&zh=205&url=http://www.usatoday.com/&v=5&stretchAds=1				
3/08/2011 9:58:28 AM	192.168.10.116	Chau\Chau Chrome	facebook.com	5.32 kB
http://facebook.com/plugins/likebox.php?channel=http://static.ak.fbcdn.net/connect/xd_proxy.php?version=0#cb=f38dd2d9b&origin=http://www.usatoday.com/f165bd334c&relation=parent.parent&transport=postmessage&colorscheme=light&header=false&height=250&href=http://www.facebook.com/usatoday&locale=en				
3/08/2011 9:58:44 AM	192.168.10.116	Chau\Chau Chrome	atdmt.com	1.11 kB
http://atdmt.com/iaction/adoapn_AppNexusDemoActionTag_1				
3/08/2011 9:58:54 AM	192.168.10.116	Chau\Chau Chrome	usatoday.com	48.91 kB
http://usatoday.com/news/world/afghanistan/2011-03-08-taliban08_ST_N.htm				
3/08/2011 9:59:04 AM	192.168.10.116	Chau\Chau Chrome	outbrain.com	1.01 kB
http://outbrain.com/utils/ping.html#random=0.48498920747078955				
3/08/2011 9:59:06 AM	192.168.10.116	Chau\Chau Chrome	facebook.com	3.83 kB
http://facebook.com/plugins/like.php#href=http://www.usatoday.com/news/world/afghanistan/2011-03-08-taliban08_st_n.htm/page/to/like&layout=button_count&show_faces=false&width=125&action=recommend&colorscheme=light&height=21				
3/08/2011 9:59:06 AM	192.168.10.116	Chau\Chau Chrome	twitter.com	4.33 kB
http://twitter.com/widgets/tweet_button.html_=1299607231686&count=horizontal&lang=en&text=U.S.: Raids have taken out 900 Taliban leaders - USATODAY.com&url=http://www.usatoday.com/news/world/afghanistan/2011-03-08-taliban08_ST_N.htm&via=USATODAY				

3/08/2011 11:39:37 AM Generated By: administrator Page 1 of 9

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

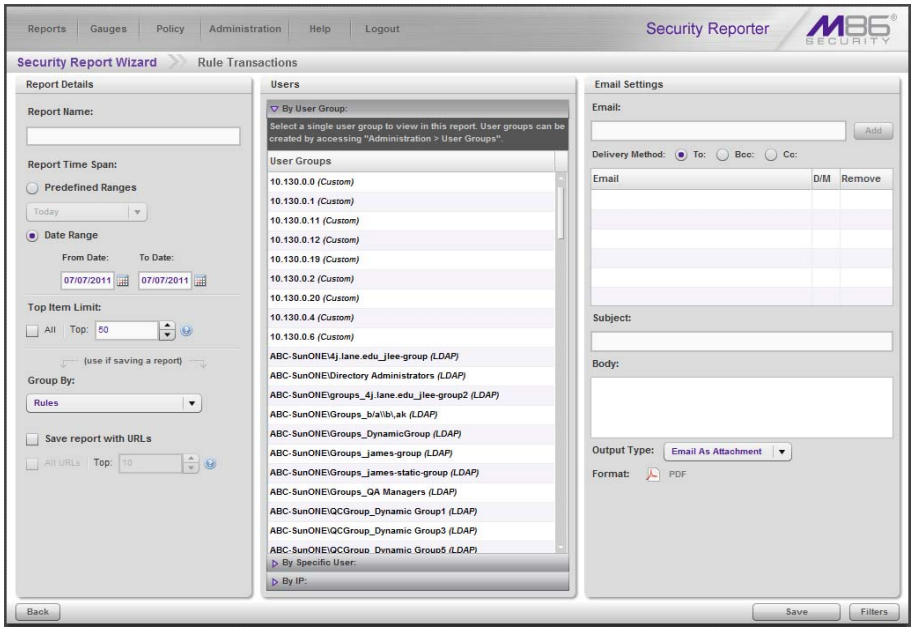
In the Security Reporter User Guide index, see:
• How to: export a Security Report

V. Save a Security Report

A security report can be saved only by using the “Report Settings” Save option.

Step A: Select Report Settings, Save option

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



Step B: Specify criteria in Report Details

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

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

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

Step C: Select the users or group in Users

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

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

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

1. Click **Filters** at the bottom right of the panel to display the filter results panel.
2. Choose a filter type from an available accordion (Policies, Rules, Action, Content Type) and indicate criteria to use in the filter:
   - Select one or more records from the Available list box and click **Add** to move the record(s) to the Assigned list box.
   - Click the "Assign All" checkbox to select all records and grey-out the panel.
3. Click **Back** to return to the Security Report Wizard panel.

Step D: Populate Email Settings

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

Step E: Save the report

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

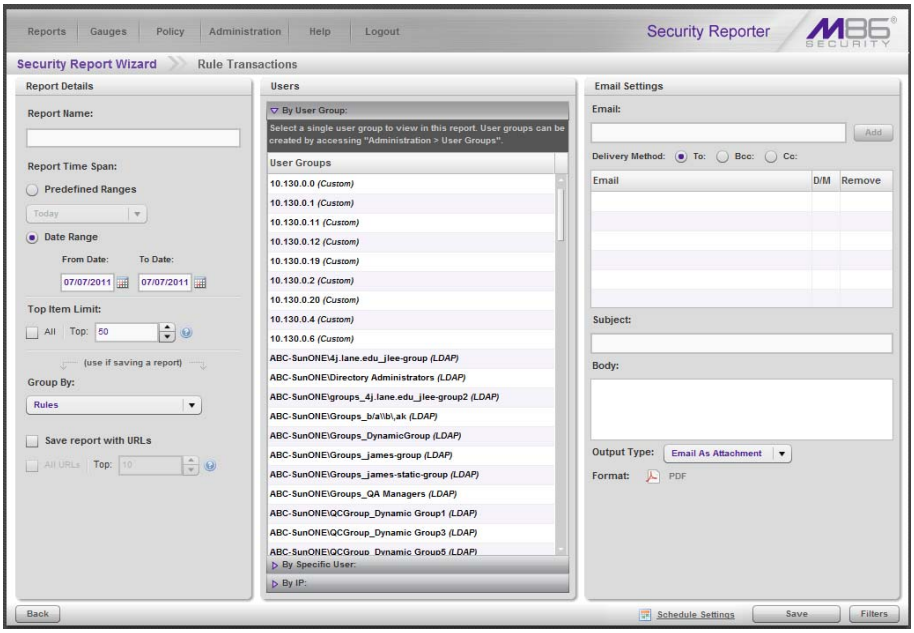
In the Security Reporter User Guide index, see:
• How to: save a Security Report

VI. Schedule a Security Report to run

A security report is scheduled to run using either the Report Settings Schedule method or the Security Report Wizard. Using the former method saves several steps, since the panel will be pre-populated with data from the current report view.

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

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



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

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

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

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

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

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

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

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

      - Select one or more records from the Available list box and click **Add** to move the record(s) to the Assigned list box.
      - Click the "Assign All" checkbox to select all records and grey-out the panel.

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

8. In the Email Settings:

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

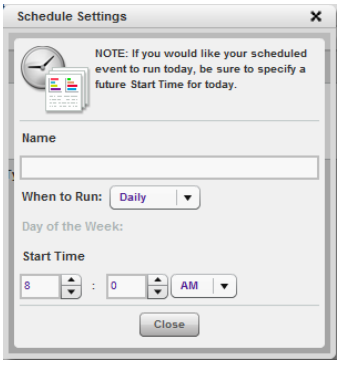
   b. Specify the **Delivery Method** for the email address: "To" (default), "Bcc", or "Cc".

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

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

   e. Specify the **Output Type** for the email: "Email As Attachment" or "Email As Link".

9. Go to the lower right corner of the panel and click **Schedule Settings** to open the Schedule Settings pop-up window:



   a. Enter a **Name** for the report run event you are scheduling.

   b. Select the frequency **When to Run** from the pull-down menu (Daily, Weekly, or Monthly).

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

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

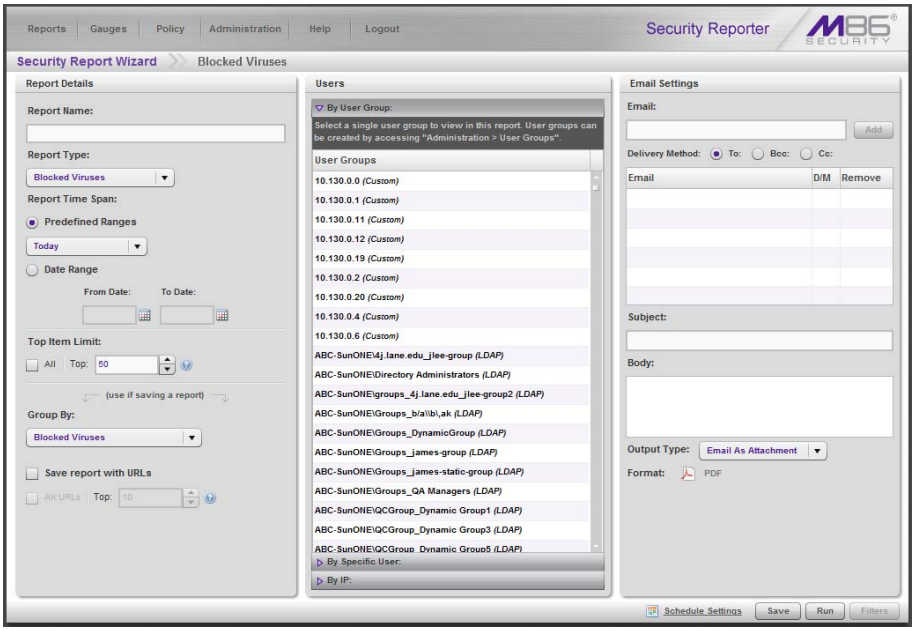
c. Select the **Start Time** for the report: 1 - 12 for the hour, 0 - 59 for the minutes, and AM or PM.

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

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

Exercise B: Use the Wizard to create and schedule reports

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



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

3. Choose the **Report Type** from the pull-down menu (“Blocked Viruses”, “Security Policy Violations”, “Traffic Analysis”, “Rule Transactions”); by default “Blocked Viruses” displays.

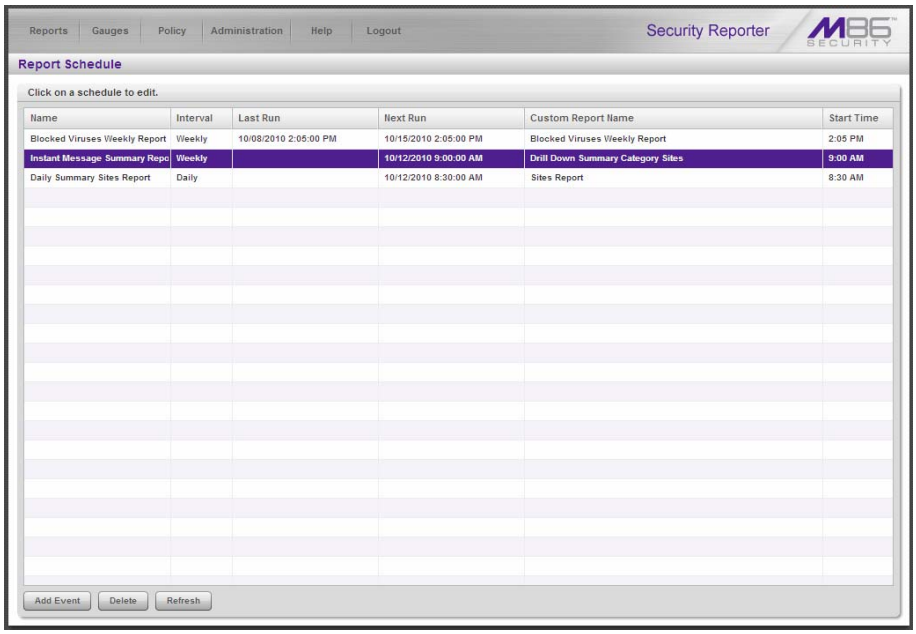
4. Specify the **Report Time Span** by choosing one of two options:

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

5. Follow steps 4 - 10 for Exercise A in this section to complete the remainder of this exercise.

Access the Report Schedule panel

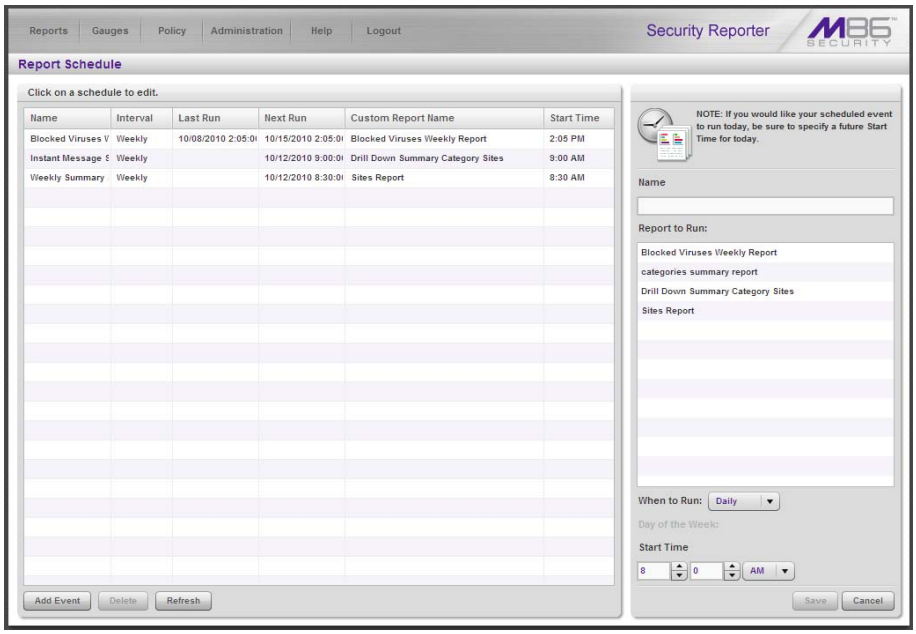
To access the Report Schedule panel that includes all productivity and security reports scheduled to run, navigate to **Reports > Report Schedule**:



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

View Details for a Scheduled Report Run Event

To view additional information on a scheduled report run event, select the record from the list to display report schedule details to the right of the table of report records:



The following information displays: Name assigned to the scheduled event; selected Report to Run; interval When to Run the report; Day of the Week the report will run if the report is a daily report, or Day of the Month the report will run if the report is a monthly report, and Start Time to run.

***TIP**: To remove a report from the Report to Run list, go to the Saved Reports panel and delete that report from the list.*

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

---

Real Time Reports Usage Scenarios

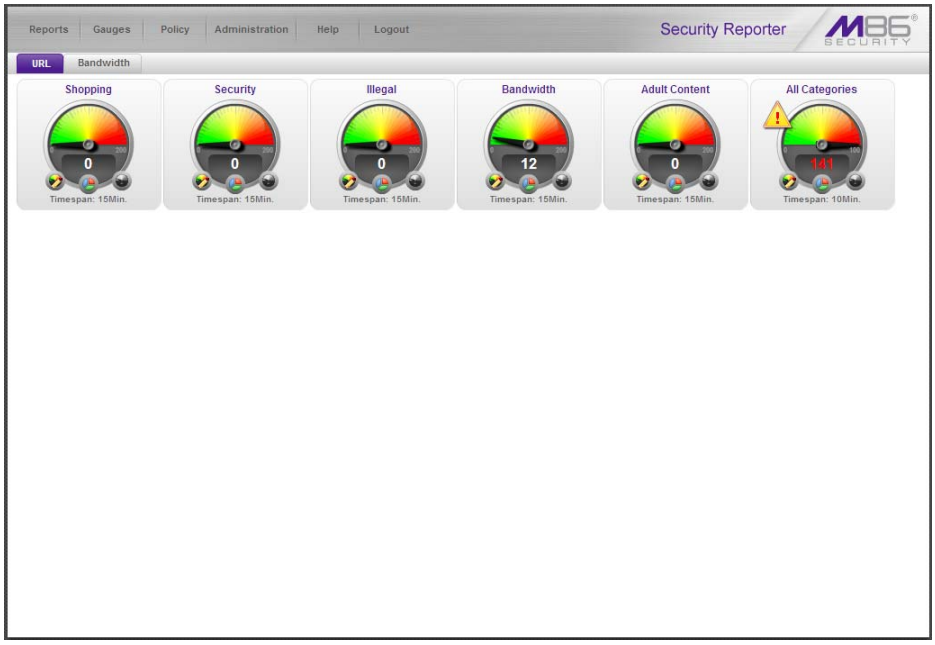
This collection of setup and usage scenarios is designed to help you understand and use basic tools in the console for enforcing your Internet usage policy. Each scenario is followed by console setup information. Please consult the “How to” section in the index of the Security Reporter User Guide for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

I. Screen navigation exercise

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

Step A: Navigate panels in the Gauges section

The URL Gauges Dashboard displays by default when you select Gauges in the navigation toolbar:



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

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

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

- **Dashboard** - view current gauge activity

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

Step B: Navigate panels in the Policy section

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

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

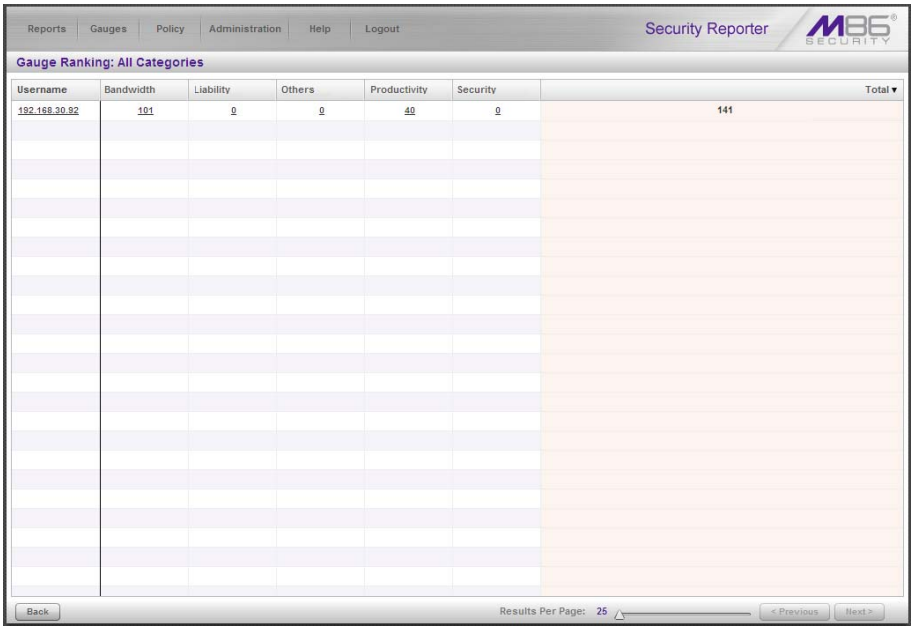
In the Security Reporter User Guide index, see:
• How to: use Gauges and Policy menu selections

II. Drill down into a gauge exercise

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

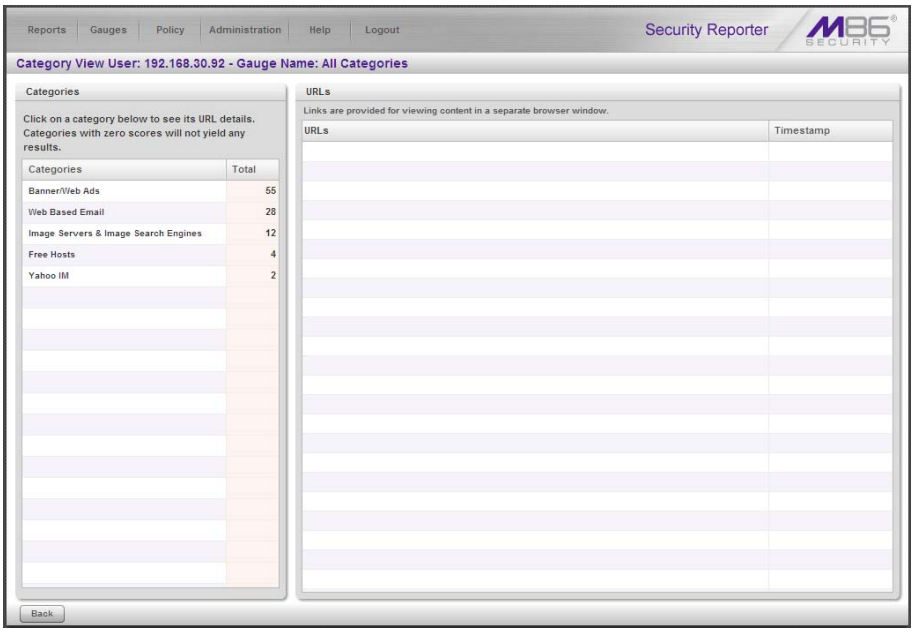
Step A: Select the gauge with the highest score

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



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

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



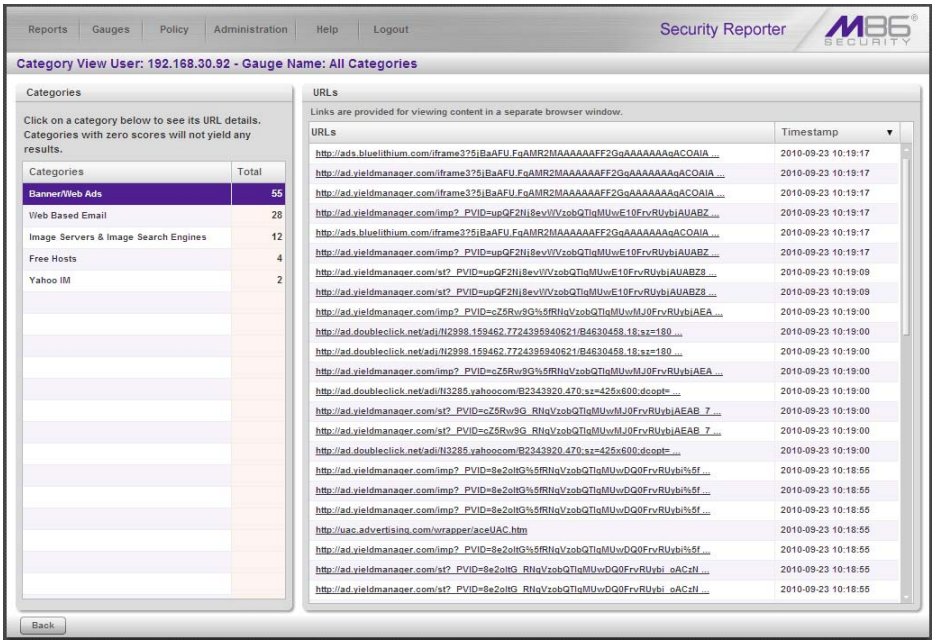
Note the left side of this panel is populated with rows of records for Categories affected by the selected end user.

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

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

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

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



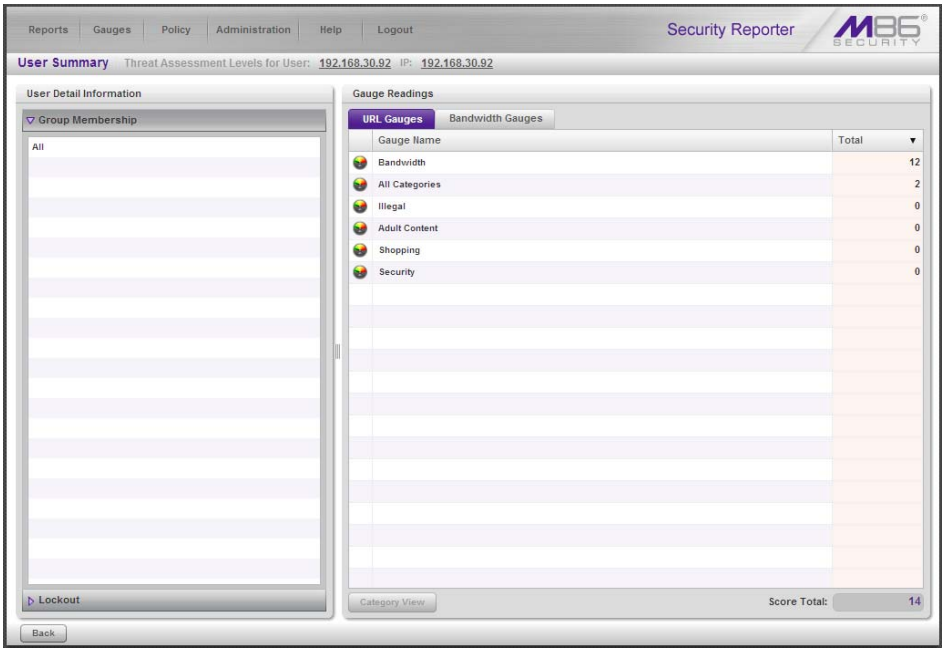
2. Choose a URL you wish to view, and then click it to open a separate browser window accessing that URL.

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

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

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

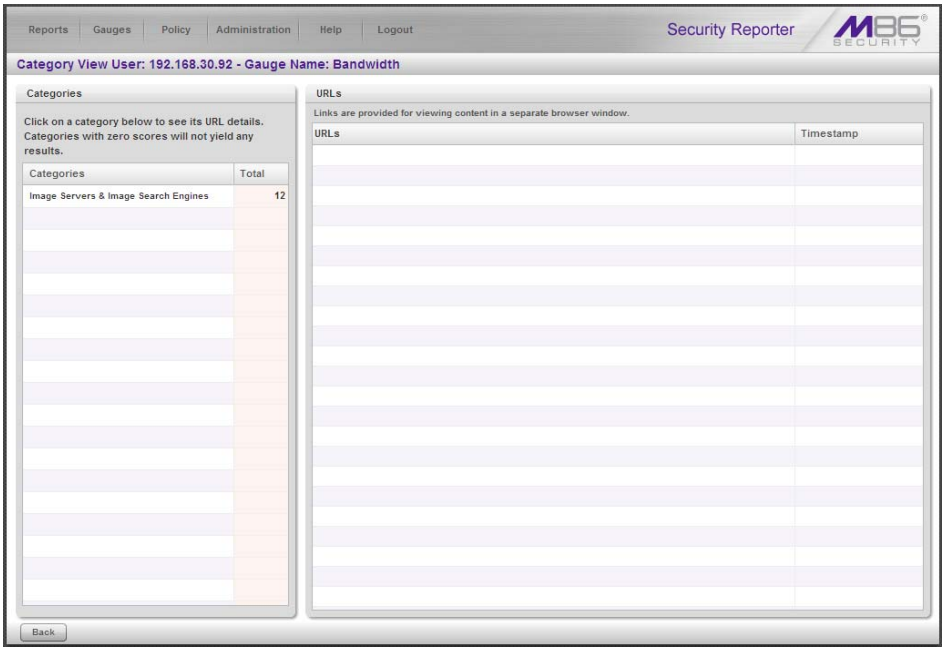
1. To find out which other gauges the same user is currently affecting, return to the Gauge Ranking table by going to the lower left corner of the Category View User panel and clicking the **Back** button. In the Username column, click that user's link to display the User Summary panel for that user:



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

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

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



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

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

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

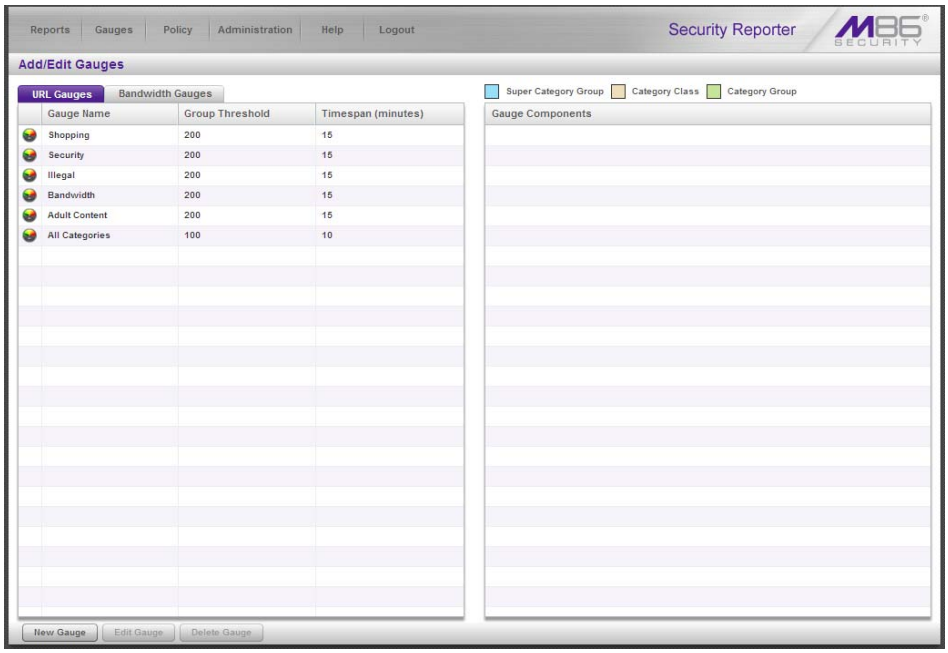
When you become accustomed to using the gauges on a regular basis to conduct these types of investigations, you will eventually want to explore other tools in the interface to restrict or lock out offending users from accessing certain library categories.

III. Create a gauge exercise

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

Step A: Access the Add/Edit Gauges panel

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



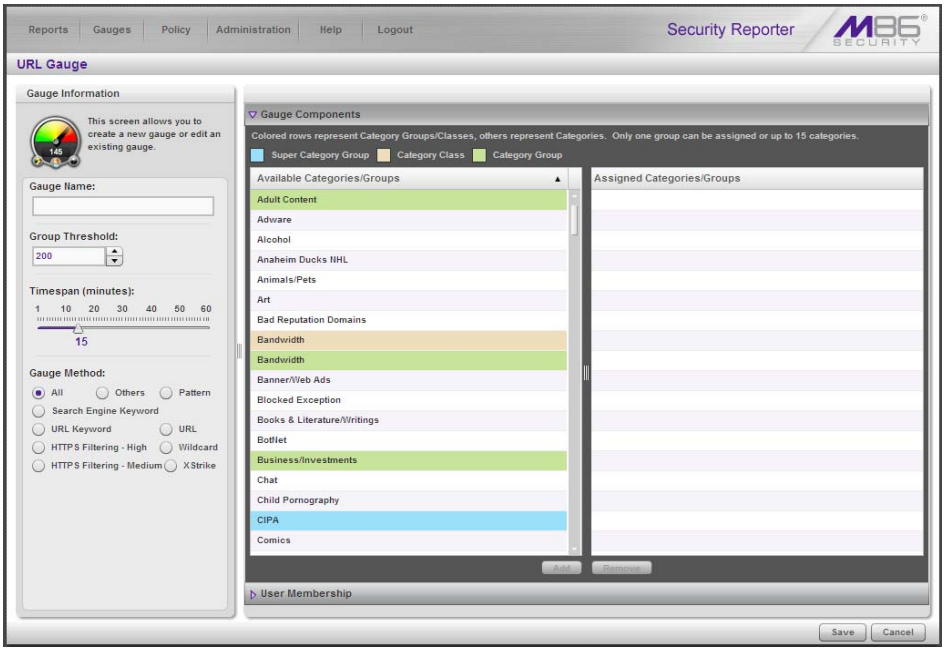
Note that this panel contains the current Gauge Name list at the left side.

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

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

Step B: Add a URL Gauge

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



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

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

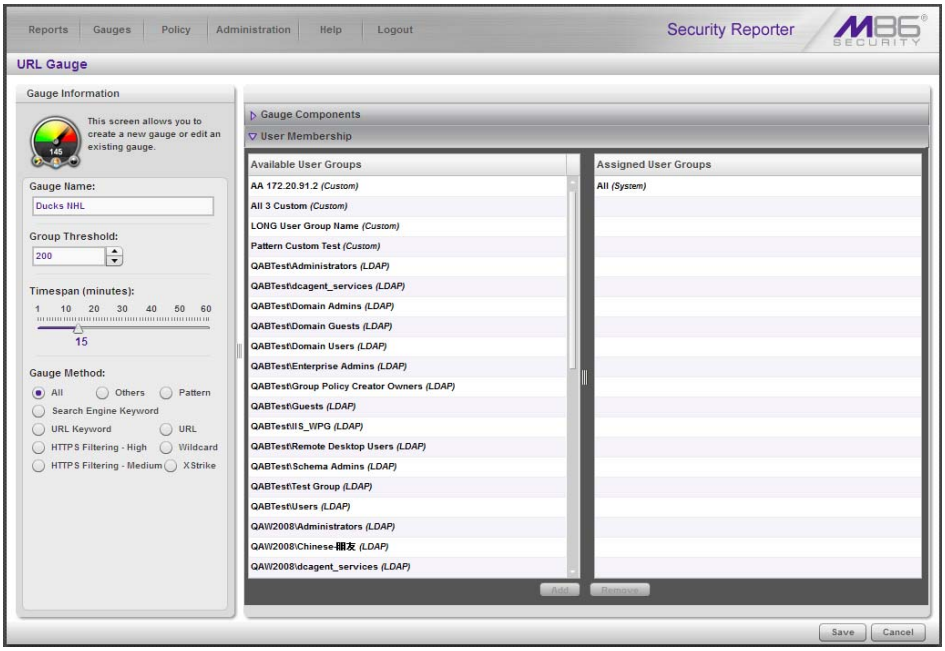
   b. **Group Threshold** for the ceiling of gauge activity. For this exercise we will use the default and recommended value, which is 200 for a URL gauge.

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

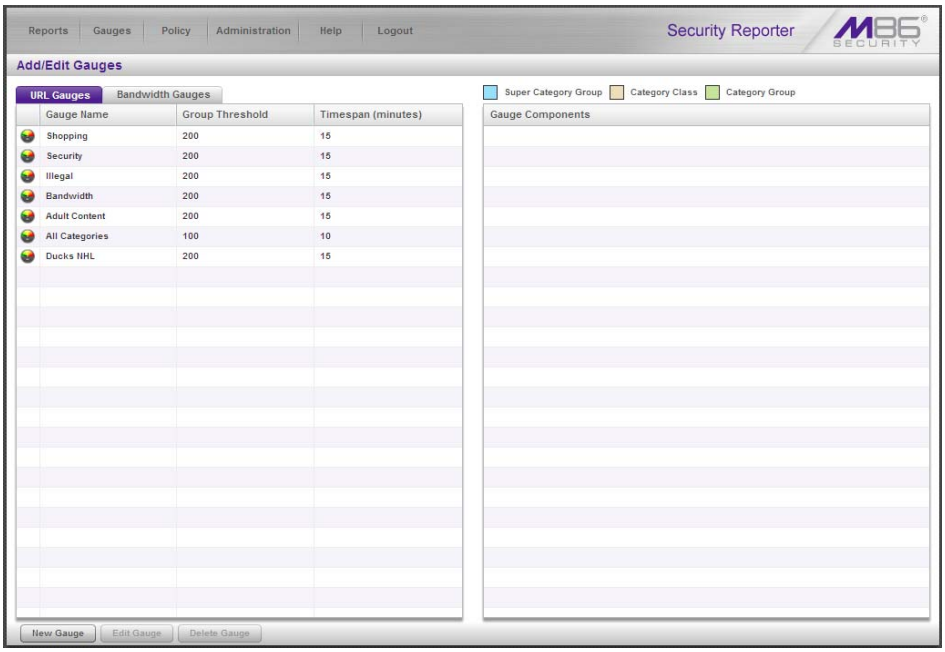
   d. **Gauge Method** to be used for tracking gauge activity. For this exercise we will use the default “All” gauge method, so you do not need to make any selection from the drop-down menu. The selected “All” method considers all methods users can use to access URLs in library categories included in the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

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

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



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



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

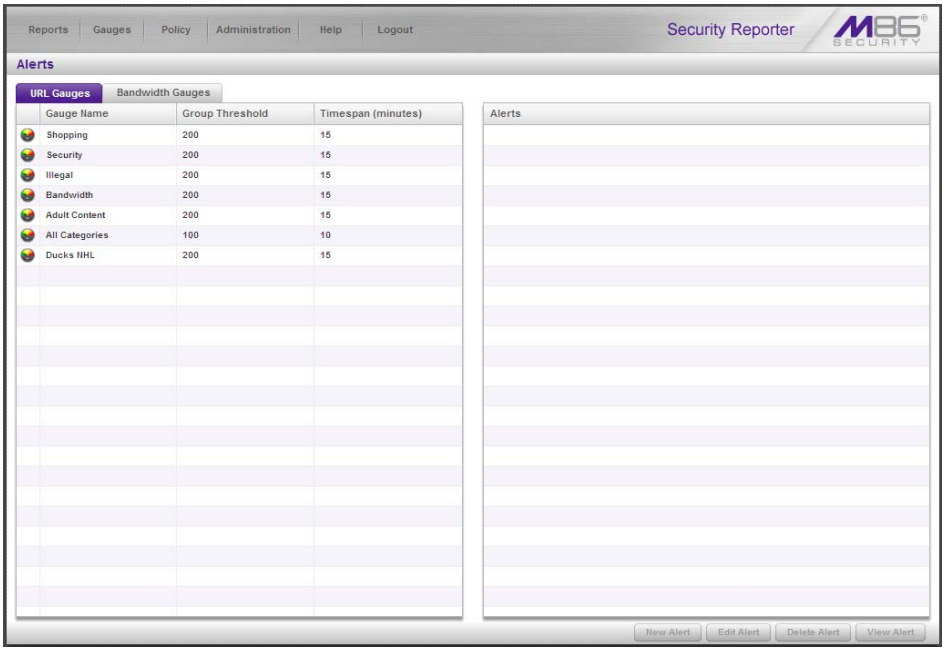
Now that you know the basics of creating a gauge, you will soon be able to create and use gauges to monitor various groups of users who frequent URLs in library categories you wish to restrict, and deal in real time with Internet usage issues that endanger your network and/or consume an excessive amount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

IV. Create an email alert exercise

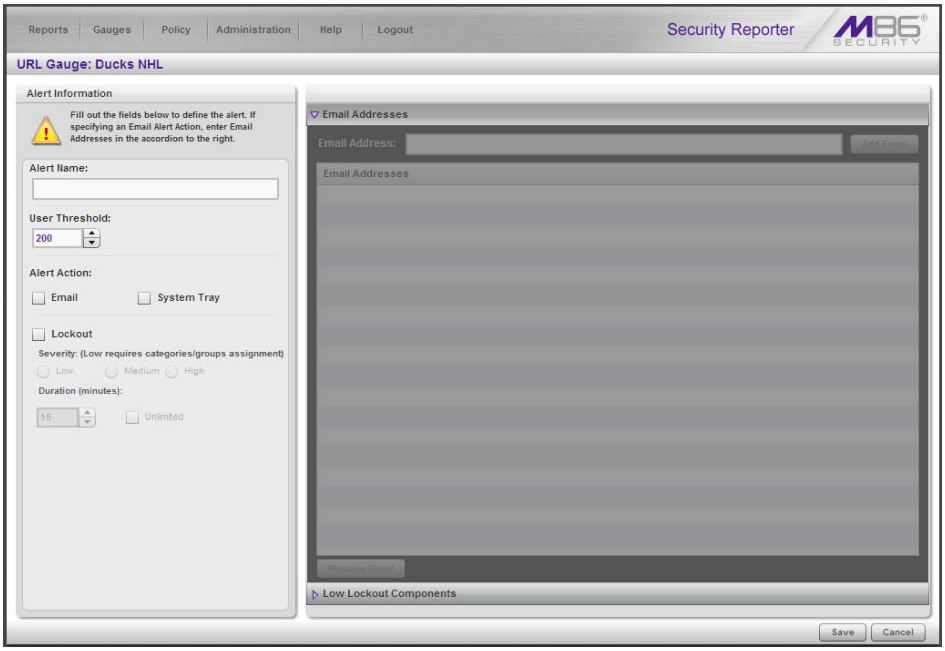
This exercise will teach you how to set up an email alert so you will be notified when a gauge reaches the high end of its established threshold.

Step A: Add a new alert

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



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



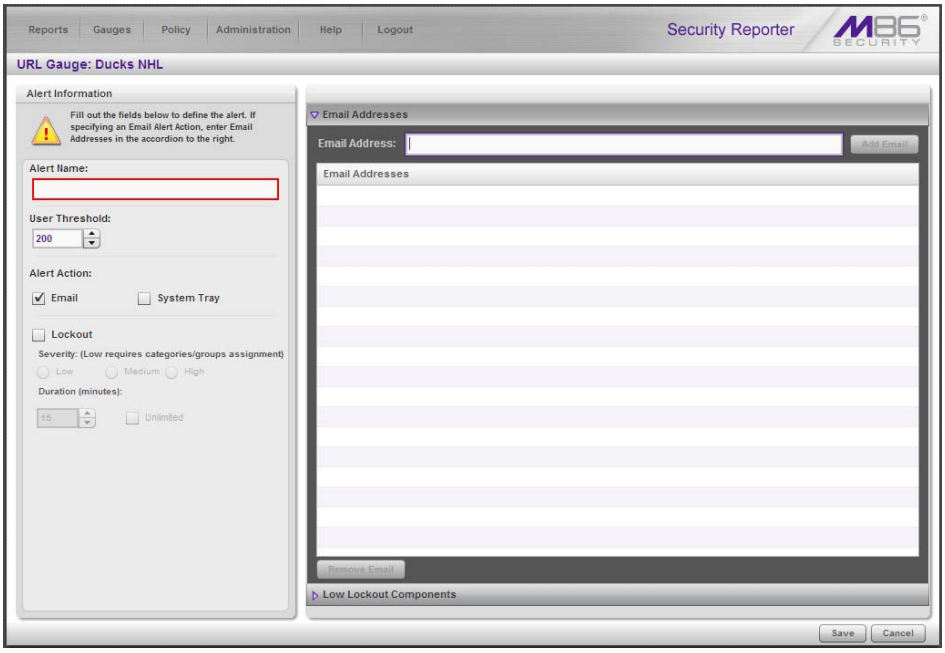
4. Type in the **Alert Name** to be used for the alert that will be delivered to the group administrator.
5. Specify the **User Threshold** ceiling of gauge activity that will trigger the alert. The default and recommended value is 200 for a URL gauge.
6. Specify the **Alert Action** method(s) to be used for alert notifications:
   - **Email** - An email alert notifies a group administrator via email if an end user has reached the threshold limit set up in a gauge alert.
   - **System Tray** - An SR Alert message notifies a group administrator via his/her workstation's System Tray if an end user has reached the threshold limit set up in a gauge alert.
   - **Lockout** - The Lockout function locks out an end user from Internet/network access if he/she reaches the threshold limit set up in a gauge alert.

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

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

Step B: Select Email Alert Action

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



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

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

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

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

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

Step C: Receiving an email alert

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

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

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

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

IMPORTANT INFORMATION ABOUT USING THE SR IN THE EVALUATION MODE

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

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

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

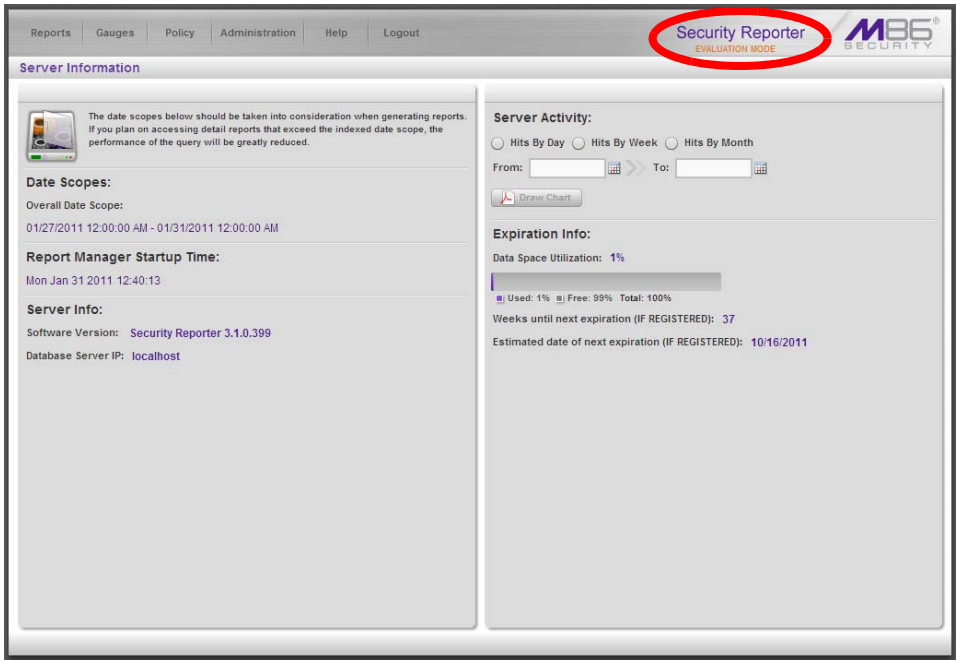
Report Manager

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

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

Server Information Panel

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

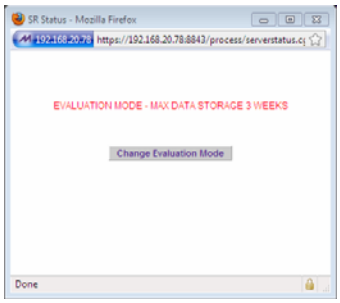


System Configuration

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

Evaluation Mode Pop-Up

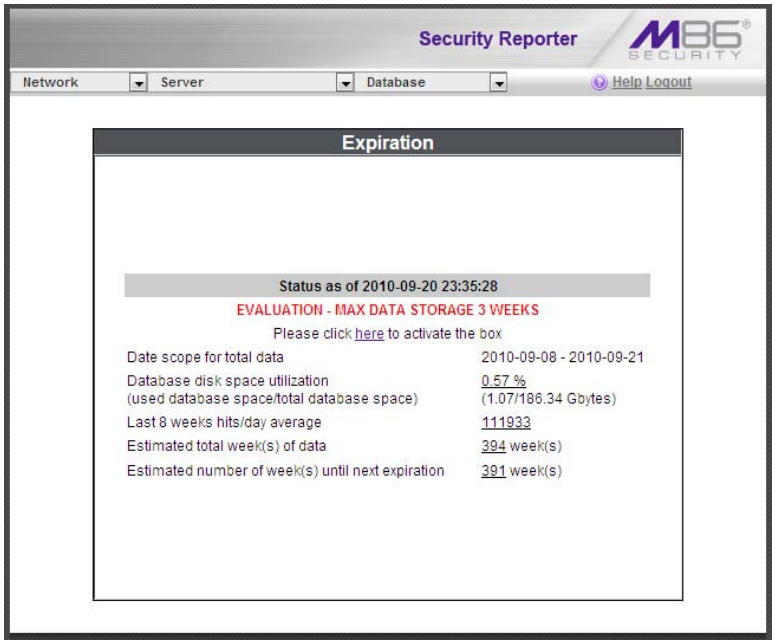
In evaluation mode, the SR Status pop-up box opens when accessing the System Configuration administrator console:



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

Expiration screen

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



APPENDIX A: BANDWIDTH MONITORING

Initial Setup on the ESXi Server

1. Plug in a network cable from the switch used for Bandwidth monitoring to an empty NIC on the ESXi server.
2. On the ESXi server, open the vSphere client and select the host machine.
3. Select the Configuration tab and choose **Add Networking...** to open the Add Network Wizard pop-up window. For each step, do the following:

   a. Connection Type: Select “Virtual Machine”, then click **Next >**.

   b. Network Access: Select “Create a virtual switch”—the virtual NIC should be automatically selected—then click **Next >**.

   c. Connection Settings: Enter the **Network Label**, then click **Next >**.

   d. Summary: Review the settings, then click **Finish** to close the Wizard window.
4. In the Configuration tab, choose **Properties...** for the Virtual Switch that will monitor Bandwidth traffic; this action opens the vSwitch Properties window. Do the following:

   a. In the Ports tab, select **vSwitch**, then click **Edit...** to open the second vSwitch Properties window.

   b. Select the Security tab, then set the **Promiscuous Mode** to “Accept”, and then click **OK** to close the Properties window.
5. Click **Close** to close the first vSwitch Properties window.

Steps to Set Up the VM to Use Bandwidth Monitoring

1. Open the vSphere client, then Login to the ESXi server.
2. Select the Virtual Machine to use for Bandwidth monitoring.
3. Select the Summary tab, then choose **Edit Settings** to open the Virtual Machine Properties window.
4. In the Hardware tab, select “Network adapter 2”.
5. In the Network Connection frame, for **Network Label** choose the network that was created for Bandwidth monitoring.
6. Click **OK** to close the Virtual Machine Properties window.

APPENDIX B: OPTIONAL ETHERNET TAP INSTALLATION

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

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

Preliminary Setup Procedures

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

Unpack the Ethernet Tap Unit from the Box

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

The NetOptics box should contain the following items:

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

Other Required Installation Items

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

- 1 standard CAT-5E cable

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

Install the Ethernet Tap Unit

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

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

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

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

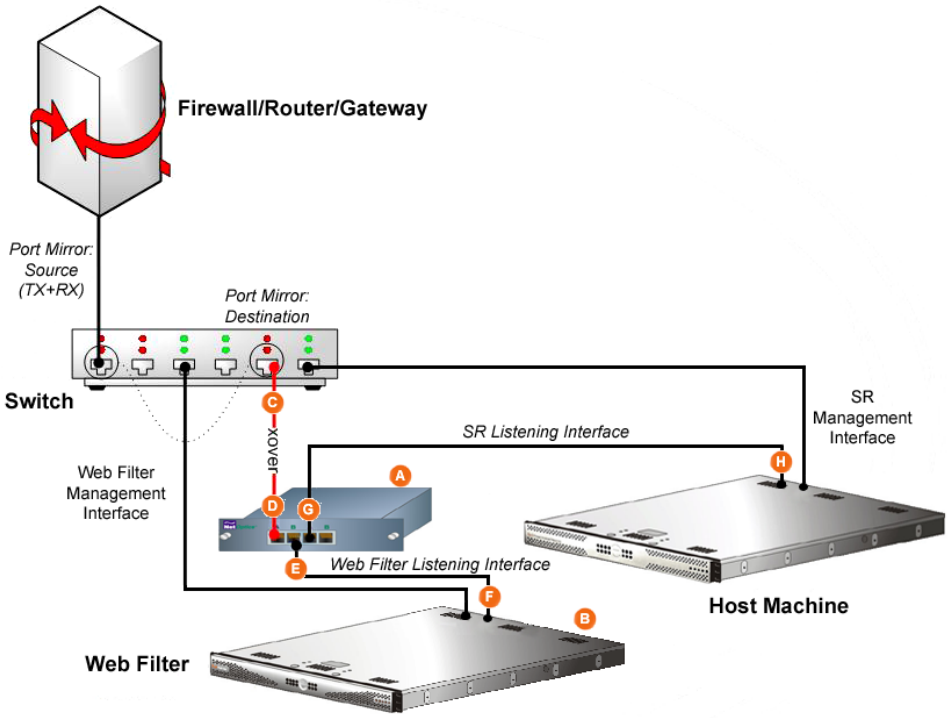


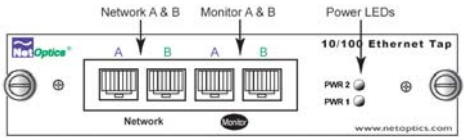
Diagram showing Ethernet Tap installation on the network

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

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

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

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



Ports in front panel of NetOptics 10/100BaseT Tap

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

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

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

H. Connect the other end of the second straight through cable to the host machine's listening interface.

Proceed to Step 3: Access the SR and its Applications Online.

INDEX

A

Access the Report Schedule panel *77*
Add to Report Schedule *54*

C

Change Quick Start password *10*
Create a customized Security Report *65*
Create a gauge *84*
Create an email alert *87*
Custom Category Group *55*
custom User Group *56*

D

Detail Drill Down Report *48*, *53*
double-break report *50*
Drill down into a gauge *80*

E

Evaluation Mode *91*
Export a Security Report *69*
Export report *50*, *52*

F

Fibre Channel *12*

G

group by report type *47*

I

Install Tap *94*

L

Login screen *7*

M

Modify report *51*

N

NAS *12*

P

ping the SR *13*

Q

Quick Start menu *7*

R

reboot *10*
report for a custom user group *58*
Reset Admin account *10*

S

Save a Security Report *71*
Save report *53*
Schedule a Security Report to run *74*
Security Report exportation *69*
Security Reports types *59*
Single Sign-On *10*, *41*
SR Wizard User *10*
Summary Drill Down Report *45*, *47*, *48*, *50*, *53*
Summary Reports *44*
SWG *13*

U

usernames and passwords *41*

W

Web Filter *13*
wizard
    installation procedures *41*

M86 Security Corporate Headquarters (USA):
8845 Irvine Center Drive, CA 92618 • Tel: 949.932.1000 or 888.786.7999
Fax: 949.932.1086