M86 Security Reporter

USER GUIDE

Software Version: 3.1.0
Document Version: 04.01.11

M86 SECURITY REPORTER USER GUIDE

Version 1.01, published April 1, 2011

Printed in the United States of America

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.

The latest version of this document can be obtained from http://www.m86security.com/support/sr/documentation.asp

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.3.1-UG_v1.01-1104

CONTENTS

INTRODUCTORY SECTION

Security Reporter

The Security Reporter (SR) from M86 Security consists of the best in breed of M86 Professional Edition reporting software consolidated into one application, 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 SWG policy servers.

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

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

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

About this User Guide

The Security Reporter User Guide primarily addresses the network administrator designated to configure and manage the Security Reporter application on the network. This administrator is referred to as the “global administrator” throughout this user guide. In part, this user guide also addresses administrators who manage user groups on the network. These administrators are referred to as “group administrators” throughout this user guide. Additional information is provided for administrators of networks that use the SR with M86’s Web Filter or M86’s Secure Web Gateway (SWG) to obtain logs from these appliances for generating productivity reports and real time or security reports.

***NOTE**: See the M86 Web Filter User Guide at **http://www.m86security.com/support/wf/documentation.asp** for information on the Web Filter. See the M86 Secure Web Gateway User Guide at **http://www.m86security.com/support/Secure-Web-Gateway/Documentation.asp** for information on the SWG.*

This User Guide is organized into the following sections:

- **Introductory Section** - This section introduces the SR product, explains how to access and use the SR and this user guide, and provides information on how to contact M86 Security technical support.
- **System Configuration Section** - This section pertains to information on configuring and maintaining the administrator console of the SR application.
- **Report Manager Administration Section** - This section pertains to configuring and maintaining the administration side of the SR’s Report Manager application.
- **Productivity Reports Section** - Refer to this section for reporting information if using log feeds from a Web Filter and/or Secure Web Gateway to generate productivity reports.

- **Real Time Reports Section** - Refer to this section for real time report configuration and usage, if using a Web Filter appliance with the SR.
- **Security Reports Section** - Refer to this section for security report configuration and usage, if using a Secure Web Gateway appliance with the SR.
- **Appendices** - Appendix A of this section explains how to disable pop-up blocking software. Appendix B provides information on how to perform hardware maintenance and troubleshoot RAID on the SR chassis. Appendix C explains how to use the SR in the evaluation mode, and how to switch to the registered mode. Appendix D provides details on setting up and using the System Tray feature for real time gauge alerts. Appendix E features a glossary of technical terminology used in this user guide.
- **Index** - This section includes an index of subjects and the first page numbers where they appear in this user guide.

How to Use this User Guide

Conventions

The following icons are used throughout this user guide:

***NOTE**: The “note” icon is followed by italicized text providing additional information about the current topic.*

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

***WARNING**: The “warning” icon is followed by italicized text cautioning you about making entries in the application, executing certain processes or procedures, or the outcome of specified actions.*

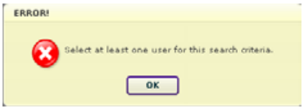
***IMPORTANT**: The "important" icon is followed by italicized text informing you about important information or procedures to follow to ensure maximum uptime on the SR application.*

Terminology

The following terms are used throughout this user guide. Sample images (not to scale) are included for each item.

- **accordion** - one of at least two or more like objects, stacked on top of each other in a frame or panel, that expands to fill a frame or collapses closed when clicked.

- **alert box** - a pop-up box that informs you about information pertaining to the execution of an action.



ERROR!

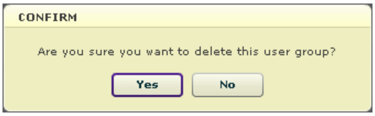
Select at least one user for this search criteria.

- **arrow** - a triangular-shaped object or button that displays in a window or on a screen. When displayed as a non-stationary object, the arrow points to the item that was selected in a list. When displayed as a button, the arrow is static. By clicking on this button, depending on the direction of the arrow, the previous item or the next item in a list displays or is selected.

- **button** - an object in a dialog box, alert box, window, or panel that can be clicked with your mouse to execute a command.

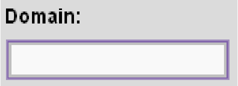
- **checkbox** - a small square in a dialog box, window, or panel used for indicating whether or not you wish to select an option. This object allows you to toggle between two choices. By clicking in this box, a check mark or an “X” is placed, indicating that you selected the option. When this box is not checked, the option is not selected.

- **dialog box -** a box that opens in response to a command made in a window or panel, and requires your input. You must choose an option by clicking a button (such as “Yes” or “No”, or “Next” or “Cancel”) to execute your command. As dictated by this box, you also might need to make one or more entries or selections prior to clicking a button.

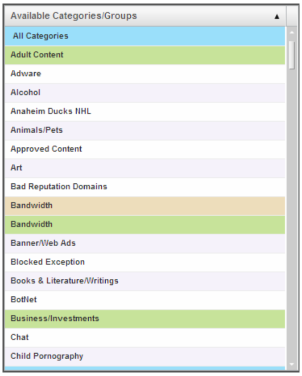

CONFIRM

Are you sure you want to delete this user group?

- **field -** an area in a dialog box, window, or panel that either accommodates your data entry, or displays pertinent information. A text box is a type of field.


Domain:

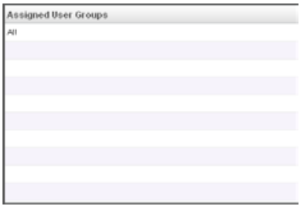
- **frame -** a boxed-in area in a dialog box, window, or panel that includes a group of objects such as fields, text boxes, list boxes, buttons, radio buttons, checkboxes, accordions, tables, tabs, and/or tables. Objects within a frame belong to a specific function or group. A frame often is labeled to indicate its function or purpose.


Available Categories/Groups

All Categories
Adult Content
Adware
Alcohol
Anaheim Ducks NHL
Animals/Pets
Approved Content
Art
Bad Reputation Domains
Bandwidth
Bandwidth
Banner/Web Ads
Blocked Exception
Books & Literature/Writings
BotNet
Business/Investments
Chat
Child Pornography

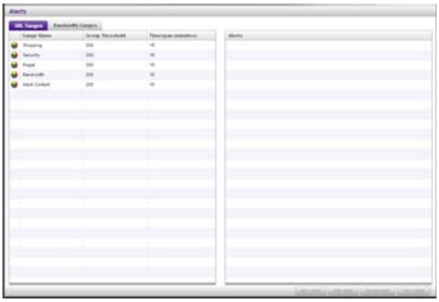
- **icon -** a small image in a dialog box, window, or screen that can be clicked. This object can be a button or an executable file.

- **list box -** an area in a dialog box, window, or panel that accommodates and/or displays entries of items that can be added or removed.


Assigned User Groups

All

- **panel** - the central portion of a screen that is replaced by a different view when clicking a pertinent link or button.



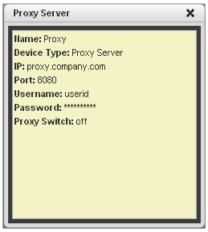
Alerts

URL Gauges | Bandwidth Gauges

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

Alerts

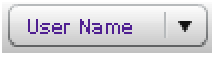
- **pop-up box** or **pop-up window** - a box or window that opens after you click a button in a dialog box, window, or panel. This box or window may display information, or may require you to make one or more entries. Unlike a dialog box, you do not need to choose between options.



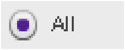
Proxy Server ✕

Name: Proxy
Device Type: Proxy Server
IP: proxy.company.com
Port: 8080
Username: userid
Password: *********
Proxy Switch: off

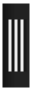
- **pull-down menu** - a field in a dialog box, window, or panel that contains a down arrow to the right. When you click the arrow, a menu of items displays from which you make a selection.



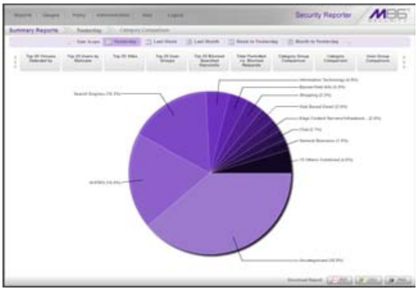
- **radio button** - a small, circular object in a dialog box, window, or screen used for selecting an option. This object allows you to toggle between two choices. By clicking a radio button, a dot is placed in the circle, indicating that you selected the option. When the circle is empty, the option is not selected.



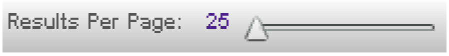
- **re-size button** - positioned between two frames, this button enlarges a frame or makes the frame narrower when clicked and dragged in a specific direction.



- **screen** - a main object of an application that displays across your monitor. A screen can contain panels, windows, frames, fields, tables, text boxes, list boxes, icons, buttons, and radio buttons.

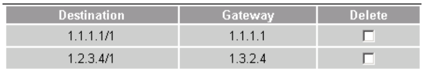


- **slider** - a small, triangular-shaped object—positioned on a line—that when clicked and dragged to the left or right decreases or increases the number of records displayed in the grid to which it pertains.


Results Per Page: 25

- **tab** - one of at least two objects positioned beside one another that display content specified to its label when clicked. A tab can display anywhere in a panel, usually above a frame.

- **table** - an area in a window or screen that contains items previously entered or selected.

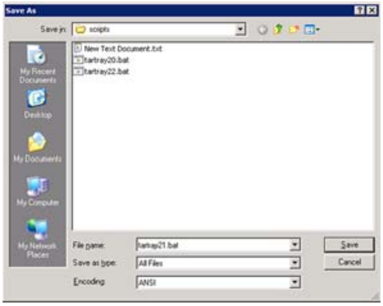


Destination	Gateway	Delete
1.1.1.1/1	1.1.1.1	□
1.2.3.4/1	1.3.2.4	□

- **text box** - an area in a dialog box, window, or screen that accommodates your data entry. A text box is a type of field. (See “field”.)

- **thumbnail** - a small image in a window or on a screen that when clicked displays the same image enlarged within a window or on the screen.

- **window** - can contain frames, fields, text boxes, list boxes, icons, buttons, and radio buttons. Types of windows include ones from the system such as the Save As window, pop-up windows, or login windows.



Save As

Save in: scripts

New Text Document.txt
tartray20.bat
tartray22.bat

File name: tartray21.bat
Save as type: All Files
Encoding: ANSI

Overview

The Security Reporter is comprised of System Configuration administrator console and Report Manager application.

Using System Configuration screens, the global administrator configures the SR to function on the network.

Using the Report Manager, the global administrator sets up group administrator accounts and grants these users access to designated sections in the Report Manager—and to the System Configuration console, as applicable—for managing and reporting on end user Internet and/or network activity.

Components and Environment

Components

Hardware

- High performance server equipped with RAID
- Two or four high-capacity hard drives
- Optional: One or more attached “NAS” storage devices (e.g. Ethernet connected, SCSI/Fibre Channel connected “SAN”)

***NOTE**: RAID is not used on an SR running as a virtual machine. The number of hard drives specified above is not applicable.*

Software

- Linux OS
- Administrator Graphical User Interface (GUI) console utilized by an authorized administrator to configure and maintain the SR application
- MySQL database

Environment

Network Requirements

- Power connection protected by an Uninterruptible Power Supply (UPS)
- HTTPS connection to M86 Security's software update server
- SR must be be fully configured, and the Structured Query Language (SQL) server must be installed on the network and connected to the Web access logging device(s) (e.g. Web Filter and/or Secure Web Gateway)
- High speed access to the SR server by authorized client workstations
- Ports 8443 and 8843 must be available for the SR user interface to use

Administrator Workstation Requirements

System requirements for the administrator include the following:

- Windows XP, Vista, or 7 operating system running:
  - Internet Explorer (IE) 7.0 or 8.0
  - Firefox 3.6
  - Google Chrome 9.0
- Macintosh OS X Version 10.5 or 10.6 running:
  - Safari 4.0
  - Firefox 3.6
  - Google Chrome 9.0
- JavaScript enabled
- Pop-up blocking software, if installed, must be disabled

- Session cookies from the SR server must be allowed in order for the System Configuration console to function properly

NOTE*: Information about disabling pop-up blocking software can be found in Appendix A: Disable Pop-up Blocking Software.*

End User Workstation Requirements

System requirements for the end user include the following:

- Windows XP, Vista, or 7 operating system running:
  - Internet Explorer (IE) 7.0 or 8.0
  - Firefox 3.6
  - Google Chrome 9.0
- Macintosh OS X Version 10.5 or 10.6 running:
  - Safari 4.0
  - Firefox 3.6
  - Google Chrome 9.0
- JavaScript enabled
- Pop-up blocking software, if installed, must be disabled

Getting Started

Initial Setup

To initially set up your M86 Security Reporter (SR), the administrator installing the unit should follow the instructions in the SR Appliance Installation Guide packaged with your SR appliance, or the SR Virtual Installation Guide—the latter if the SR image will be installed on an appliance in your network and running as a virtual machine. The Installation Guide explains how to perform the initial configuration of the SR so that it can be accessed via an IP address or host name on your network, and communicate with the Web access logging device(s) (Web Filter and/or Secure Web Gateway) to receive logs of end user Internet/network activity.

NOTE*: If you do not have the Installation Guide, contact M86 Security immediately to have a copy sent to you.*

WARNING*: In order to prevent data from being lost or corrupted while the SR is running, the server should be connected to a UPS or other battery backup system. Once you turn on the SR server,* ***DO NOT*** *interrupt the initial boot-up process. This process may take from five to 10 minutes per drive. If the process is interrupted, damage to key files may occur.*

Procedures for Logging In, Out

Log In

After the SR is set up on the network, the designated global administrator of the server should be able to access the unit via its URL on the Internet, using the username and password registered during the wizard hardware installation procedures.

NOTES*: A maximum of eight users can use the SR user interface simultaneously. However, for optimum results, M86 Security recommends no more than four users generate reports at the same time.*

If your browser is set to display in English, Simplified Chinese or Traditional Chinese, the SR user interface will display that language setting by default. However, this language selection can be changed for your user account as described in Chapter 1: Group, Profile Management of the Report Manager Administration Section.

1. Launch an Internet browser window supported by the SR.
2. In the address line of the browser window, type in “https://” and the SR server’s IP address or host name, a colon “**:**” and port number “8443” for a secure network connection, appended by “/SR/”.

   For example, if your IP address is 210.10.131.34, type in **https://210.10.131.34:8443/SR/**. Using a host name example, if the host name is logo.com, type in **https://logo.com:8443/SR/**.

   With a secure connection, the first time you attempt to access the SR’s user interface in your browser you will be prompted to accept the security certificate. In order to accept the security certificate for your browser, follow the instructions at: ***http://www.m86security.com/software/8e6/docs/ig/misc/sec-cert-sr3.1.pdf***

3. Click **Go** to open login window of the SR user interface:

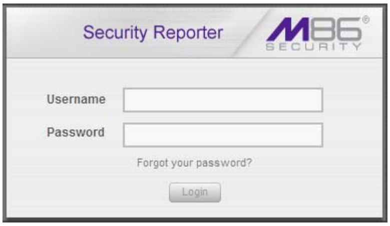


Fig. 1:1-1 Security Reporter login window

4. In the **Username** field, type in your username (the default username is ***admin***). Logging in as the global administrator for the first time, enter the username registered during the wizard hardware installation procedures. If you are logging in as a group administrator, enter the username set up for you by the global administrator.

TIP*: In any box or screen in the application, press the Tab key on your keyboard to move to the next field. To return to a previous field, press Shift-Tab.*

5. In the **Password** field, type in your password (the default password is ***testpass***). Logging in as the global administrator for the first time, enter the password registered during the wizard hardware installation procedures. If you are logging in as a group administrator, enter the password set up for you by the global administrator.

TIPS*: M86 Security recommends administrators who access this application for the first time should change their account password. Administrator usernames and passwords are modified in Report Manager: Administration > Admin Profiles.*

If you forgot your password, clicking the Forgot your password? link lets you reset your password (see Forgot Your Password in this sub-section).

6. Click **Login** to display the Summary Reports panel of the Report Manager user interface (if you have permissions to view this panel—see Fig. 1:1-2 for a sample panel), or the Drill Down Report Wizard Summary Report panel of the Report Manager user interface (if you do not have permission to view the Summary Report panel—see Fig. 1:1-3 for a sample panel):

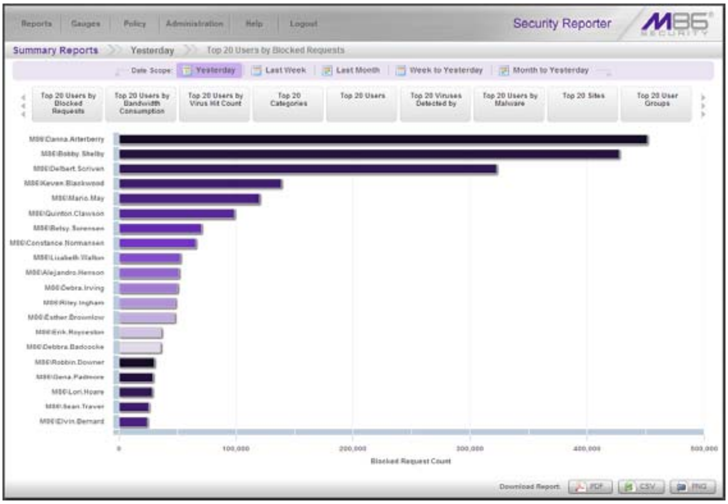
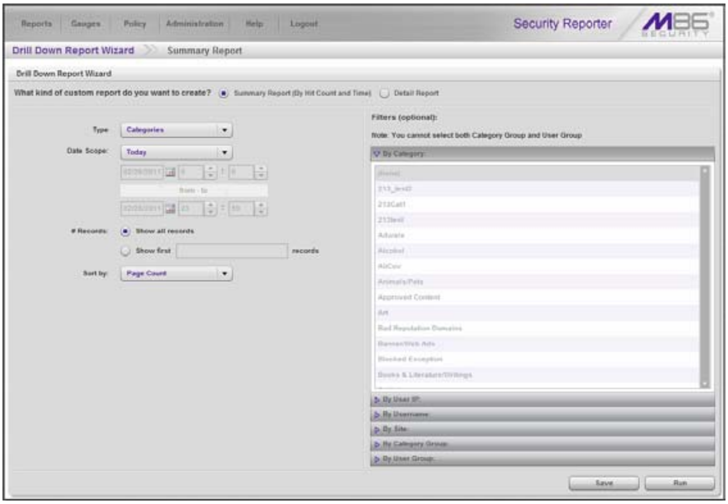


Fig. 1:1-2 Top 20 Users by Blocked Requests Summary Report

***NOTES**: On a newly installed unit, SR reporting data is inaccessible and will not display in the dashboard until the SR server is configured, a filter (Web Filter or SWG) is added to the device registry (via Reporter Manager: Administration > Device Registry), logs are transferred to the SR, and the database is built—the latter process could take about 24 hours. If a software update was recently applied on an existing server, it could take several hours before data is available.*

If the Block Request Count feature (set via System Configuration: Database > Optional Features) is disabled, the Top 20 Categories Summary Report displays instead of Top 20 Users by Blocked Requests.



Drill Down Report Wizard

What kind of custom report do you want to create? ● Summary Report (By Hit Count and Time) ○ Detail Report

Type: Categories

Date Scope: Today

Records: ● Show all records

○ Show first records

Sort by: Page Count

Filters (optional):

Note: You cannot select both Category Group and User Group

By Category:

- (none)
- 213_level2
- 213Cat1
- 213test
- Adware
- Alcohol
- AltCov
- Animals/Pets
- Approved Content
- Art
- Bad Reputation Domains
- Banner/Web Ads
- Blocked Exception
- Books & Literature/Writings

By User IP:

By Username:

By Site:

By Category Group:

By User Group:

Fig. 1:1-3 Drill Down Report Wizard Summary Report

Re-login

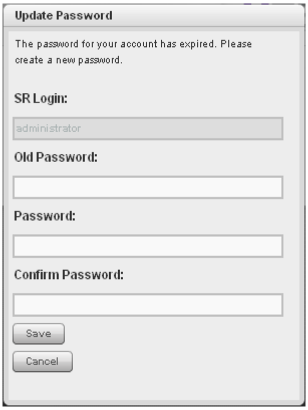
Each session is timed so that it remains active as long as there is activity in the user interface within an eight hour period. You need to log into the application again after an eight hour period of inactivity, or in the event that the SR server was restarted.

If your session in the application is timed out, when you click a button, thumbnail, or menu item in the Report Manager, an alert box opens with the message: “Session Timed out!” In the System Configuration administrator console, the following message displays: “Your session has ended, please login.”

To log in again, click **OK** to close the alert box; this action displays the Security Reporter login window where you will need to log in again.

Expired Passwords

If your password has been set by the global administrator to expire after a specified number of days (System Configuration: Database > Optional Features), upon clicking the **Login** button, the Update Password pop-up window opens:



The password for your account has expired. Please create a new password.

SR Login: administrator

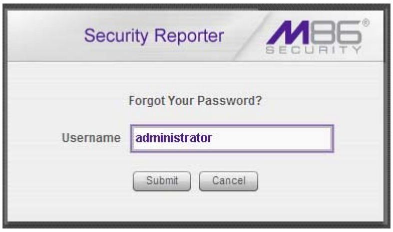
Fig. 1:1-4 Update Password window

1. Beneath your username displayed in the **SR Login** field, enter your **Old Password**.
2. In the **Password** and **Confirm Password** fields, enter eight to 20 characters for the new password, including at least one alpha character, one numeric character, and one special character. The password is case sensitive.
3. Click **Save** to close the pop-up window.
4. In the Security Reporter login window (see Fig. 1:1-1), enter your **Username** and new **Password**, and then click **Login** to access the user interface.

Forgot Your Password

If you forgot your password, you can reset it on demand.

1. Click the **Forgot your password?** link in the login window (see Fig. 1:1-1) to open the Forgot Your Password? window:



Username: administrator

Fig. 1:1-5 Forgot Your Password window

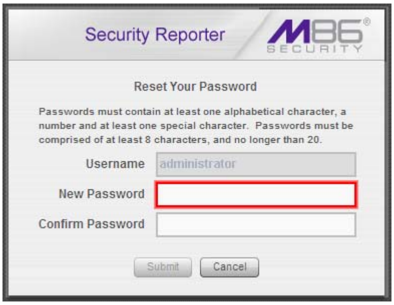
***TIP**: At any point during the password reset process, if you wish to cancel this request, click **Cancel** to cancel this request and display the original login window.*

2. Enter your **Username** and then click **Submit** to open an alert pop-up box informing you that "An email has been sent with instructions to reset your password."

3. Click **OK** to close the alert pop-up box and then check your email account (set up for your profile in Report Manager: Administration > Admin Profiles) for the "Security Reporter password reset" message.

***NOTE**: The action of clicking "OK" displays the original login window.*

4. Click the link in the email message to launch the Reset Your Password login window; the Username field displays your username greyed-out:


Security Reporter

Reset Your Password

Passwords must contain at least one alphabetical character, a number and at least one special character. Passwords must be comprised of at least 8 characters, and no longer than 20.

Username: administrator

New Password:

Confirm Password:

Fig. 1:1-6 Reset Your Password window

5. Enter a password comprised of eight to 20 characters (using at least one alpha, one numeric, and one symbol character) In the **New Password** and **Confirm Password** fields.

6. Click **Submit** to access the Security Reporter user interface.

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 host name 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.

User Interface Navigation

Once you have logged into the Report Manager, use the navigation toolbar at the top of the screen to navigate to the section of the user interface you wish to use.

This toolbar provides a menu link to access the System Configuration administrator console (if permissions are granted by the global administrator). If an M86 Web Filter is set up to send logs to this SR, a link to Web Filter is also available via a menu link.

Clicking “Security Reporter” or the M86 Security logo in the banner accesses the M86 Security Web site.

***NOTE**: See Appendix C: Evaluation Mode for information about using the Security Reporter in evaluation mode and/or converting the application to registered mode.*

Links in the Report Manager Navigation Toolbar

The navigation toolbar at the top of the Report Manager screen consists of the following links and menu topics for configuring and using the Report Manager:

- **Reports** - mouse over this link to open the Reports menu. Global and group administrators can click any Report menu item to view or generate a report, or schedule a report to run.
- **Gauges** (available for Web Filter) - mouse over this link to view menu options for setting and managing URL and bandwidth gauges, and end user Internet activity.
- **Policy** (available for Web Filter) - mouse over this link to view menu options for setting and maintaining policies used for triggering warnings when gauges approach their upper threshold limits.
- **Administration** - mouse over this link to view menu options for setting and maintaining administrator profiles

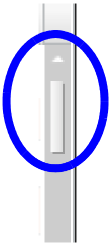
and groups, maintaining the Report Manager, and managing the SR.

- **Help** - mouse over this link to view menu options for assisting you in configuring this SR:
  - **Online Help** - Clicking this link accesses the Web page at M86Security.com containing links to the latest documentation in the .pdf format for this application
  - **About...** - Clicking this link opens a pop-up window containing information about the current software Version, and hardware Serial number if this SR is running on an M86 SR appliance. This criteria can be copied and pasted into an email or online form to be submitted to M86 Security for troubleshooting purposes. Click "Close" to close the pop-up window.
- **Logout** - click this link to log out of the SR (see Log Out for details on log out procedures).

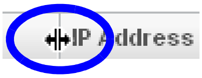
Navigation Tips and Conventions

The following tips and list of conventions will help you navigate the Report Manager user interface:

- **Move a pop-up window** - Click the toolbar of a pop-up window and simultaneously move your mouse to relocate the pop-up window to another area in the current browser window.
- **Scroll up and down, and across a list** - If available, use the scrollbar to the right or along the bottom of a frame or list box to view an entire list.

  An extensive list can be viewed in its entirety by clicking the Previous and Next buttons.
- **Tab to the next field** - Press the Tab key on your keyboard to advance to the next field in a panel.



- **Expand, contract a column -** Columns can be expanded or contracted by first mousing over the divider in the column header to display the arrow and double line characters (<-II->). A column is then expanded or contracted by left-clicking the mouse and dragging the column bar to the right or left.
- **Browser back button, refresh button -** Clicking either the back button in the browser window or the refresh button in your browser will refresh the SR user interface and log you out of the application.
- **Select multiple items in specified windows -** In specified panels, when moving several items from one list box to another, or when deleting several items, the Ctrl and Shift keys can be used to expedite this task.
    - **Ctrl Key -** To select multiple items from a list box, click each item while pressing the Ctrl key on your keyboard.
    - **Shift Key -** To select a block of consecutive items from a list box, click the first item, and then press the Shift key on your keyboard while clicking the last item.

  Once the group of items is selected, click the appropriate button to perform the action on the items.
- **Sort records by another column header -** Records can often be sorted by a different column header by clicking the header for that column. This action sorts the records that display in descending order by that column. Clicking the same column header again sorts the records in ascending order by that column.

  ⓘ •**View tooltip information -** To view information about any object that has a circled “i” icon beside it, mouse over the icon to display tooltips that explain how to use that button or field.

Wildcard Searches

1. When performing a search with wildcard(s), enter text in the following format: **%X%**, **%X**, or **X%** (in which “X” represents a partial or complete user IP address, username, site URL, or other specified search query item).

   Examples:

   - User IP: **%200.10.100.51%**, **%100**, or **192.168.%**
   - Username: **%jsmith%**, **%t**, or **%qa**
   - Site: **%yahoo%**, **%z**, or **cnn%**
2. Click the designated button to perform the wildcard search.
3. Make your selection from records returned by the search.

Links in the System Configuration Navigation Toolbar

The navigation toolbar at the top of the System Configuration screen consists of the following menu topics and selections for configuring and using the SR:

- **Network** - select a menu item to access its corresponding page used for creating and maintaining network configuration settings on the SR server.
- **Server** - select a menu item to access its corresponding page used for managing the SR server’s hardware and software.
- **Database** - select a menu item to access its corresponding page used for maintaining the SR database and Report Manager.
- **Help** - click this link to launch a separate browser window or tab displaying the page containing links to the latest user guides (in the .pdf format) for this application.
- **Logout** - click this link to log out of the SR (see Log Out for details on log out procedures).

Log Out

To log out of the SR, click the **Logout** button in the navigation toolbar; this action re-displays the login window.

Click the “X” in the upper right corner of the logout window or tab to close the window/tab.

Exiting the SR application will log you out of the user interface, but will not log you out of the SR server, nor turn off the server.

⚠ ***WARNING****: If you need to turn off the SR server, follow the shut down procedures outlined in the Shut Down screen sub-section under the Server Menu section in Chapter 2 of the System Configuration Section of this User Guide. Failure to properly shut down the server can result in data being lost or corrupted.*

Technical Support / Product Warranties

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

SYSTEM CONFIGURATION SECTION

Introduction

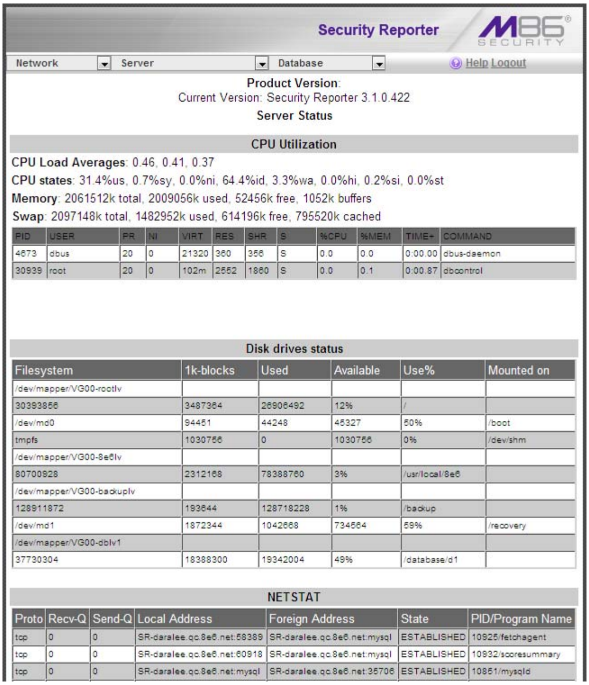
This section of the user guide provides instructions to the global administrator on configuring and managing the SR server.

The authorized administrator of the SR server is responsible for integrating the server into the existing network, configuring and maintaining the server. To attain this objective, the administrator performs the following tasks:

- executes Installation procedures defined in the Installation Guide booklet
- provides a suitable environment for the server, including:
  - high speed, HTTPS link to the current logging device
  - power connection protected by an Uninterruptible Power Supply (UPS)
  - high speed access to the server by authorized client workstations
- sets up administrators for receiving automatic alerts
- updates the server with software updates supplied by M86 Security
- analyzes server statistics
- utilizes diagnostics for monitoring the server status to ensure optimum functioning of the server
- establishes and implements backup and restoration procedures for the server

Chapter 1: Access System Configuration

If your account profile is set up with privileges to access the System Configuration administrator console, its user interface is accessible by navigating in the Report Manager to **Administration > System Configuration**:



Product Version:
Current Version: Security Reporter 3.1.0.422

Server Status

CPU Utilization

CPU Load Averages: 0.46, 0.41, 0.37
CPU states: 31.4%us, 0.7%sy, 0.0%ni, 64.4%id, 3.3%wa, 0.0%hi, 0.2%si, 0.0%st
Memory: 2061512k total, 2009056k used, 52456k free, 1052k buffers
Swap: 2097148k total, 1482952k used, 614196k free, 795520k cached

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
4673	dbus	20	0	21320	360	356	S	0.0	0.0	0:00.00	dbus-daemon
30939	root	20	0	102m	2552	1860	S	0.0	0.1	0:00.87	dbcontrol

Disk drives status

Filesystem	1k-blocks	Used	Available	Use%	Mounted on
/dev/mapper/VG00-rootlv					
30393856	3487364	26906492	12%	/	
/dev/md0	94451	44248	45327	50%	/boot
tmpfs	1030756	0	1030756	0%	/dev/shm
/dev/mapper/VG00-8e6lv					
80700928	2312168	78388760	3%	/usr/local/8e6	
/dev/mapper/VG00-backuplv					
128911872	193644	128718228	1%	/backup	
/dev/md1	1872344	1042668	734564	59%	/recovery
/dev/mapper/VG00-dblv1					
37730304	18388300	19342004	49%	/database/d1	

NETSTAT

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program Name
tcp	0	0	SR-daralee.qc.8e6.net:58389	SR-daralee.qc.8e6.net:mysql	ESTABLISHED	10925/fetchagent
tcp	0	0	SR-daralee.qc.8e6.net:60918	SR-daralee.qc.8e6.net:mysql	ESTABLISHED	10932/scoresummary
tcp	0	0	SR-daralee.qc.8e6.net:mysql	SR-daralee.qc.8e6.net:35706	ESTABLISHED	10851/mysqld

Fig. 2:1-1 Server Status screen

The System Configuration user interface launches in a separate window/tab (using port 8843) and displays the Server Status screen showing the current status of the SR.

***NOTES**: See Server Status screen in the Server section of this user guide for information about this screen.*

If using this product in the evaluation mode the SR Status pop-up window opens when accessing this screen. Please see Appendix C: Evaluation Mode for information about the evaluation mode.

Chapter 2: Configuring the Server

The System Configuration administrator console is comprised of Network, Server, and Database menu screens for configuring the SR server and maintaining the Report Manager.

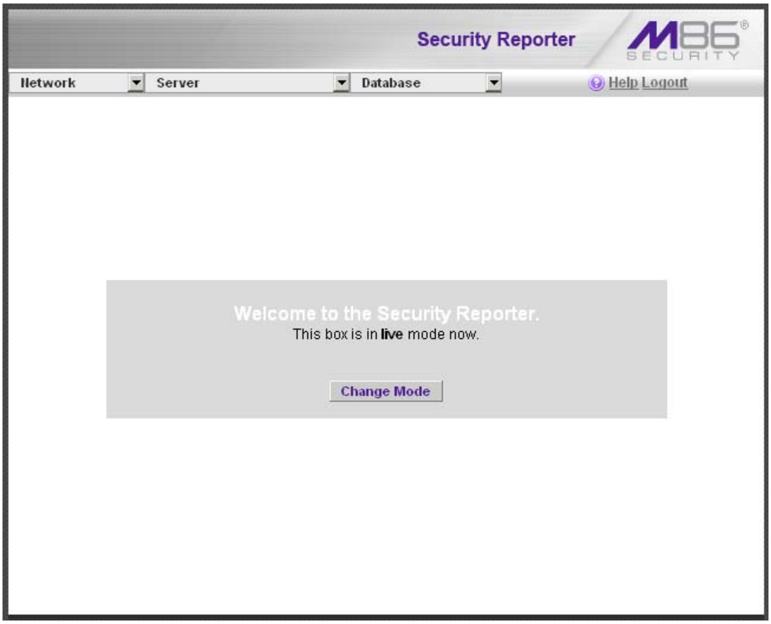
***TIP**: When making a complete configuration in the System Configuration administrator console, M86 Security recommends you navigate from left to right (Network to Server to Database) in choosing your menu options.*

Network Menu

The Network pull-down menu includes options for setting up and maintaining components to be used on the server's network. These options are: Box Mode (for Web Filter), Lockouts, Network Setting, Routing Table, Regional Setting, Diagnostics, and SNMP.

Box Mode screen

If using a Web Filter with this SR, the Box Mode screen displays when the Box Mode option is selected from the Network menu. The box mode indicates whether the server box is functioning in the “live” mode, or in the “archive” mode. When the box mode displays on the screen, you can view the current mode set for the server, and can change this setting, if necessary.



This box is in **live** mode now.

Fig. 2:2-1 Box Mode screen

Live Mode

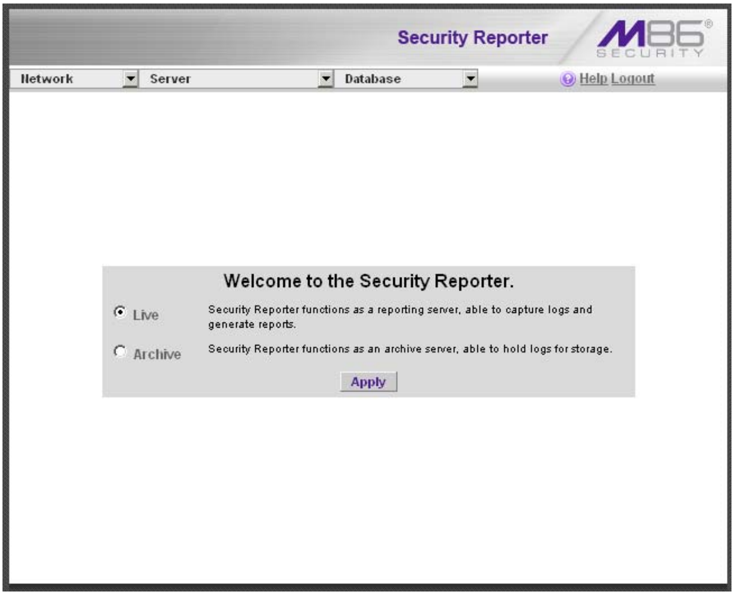
Once your server is configured and the server is set in the “live” mode, it will receive and process real time data from the Web access logging device (Web Filter). The Report Manager can then be used to capture data and create views.

Archive Mode

In the “archive” mode, the server solely functions as a receptacle in which historical, archived files are placed. In this mode, “old” files placed on the server can be viewed using the Report Manager.

Change the Box Mode

1. Click the **Change Mode** button to display the two server box mode options on the screen:



Welcome to the Security Reporter.

● Live Security Reporter functions as a reporting server, able to capture logs and generate reports.

○ Archive Security Reporter functions as an archive server, able to hold logs for storage.

Apply

Fig. 2:2-2 Change Box Mode

2. Click the radio button corresponding to **Live** or **Archive** to specify the mode in which the server should function:
   - choose **Live** if you wish the server to function in the “live” mode, receiving and processing real time data from the Web access logging device (Web Filter).

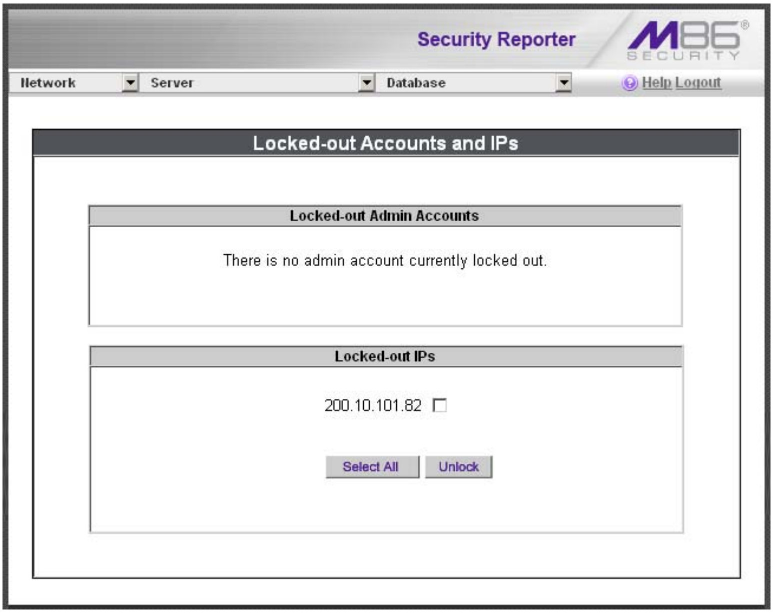
- choose **Archive** if you wish the server to function in the “archive” mode, solely as a receptacle for historical, archived files.

3. Click **Apply** to confirm your selection. The mode you specify will immediately be in effect.

***NOTE**: After applying the box mode setting, you must restart the server by selecting the **Restart Hardware** option on the Shut Down screen. (See the Shut Down sub-section under the Server menu section in this chapter.)*

Locked-out Accounts and IPs screen

The Locked-out Accounts and IPs screen displays when the Lockouts option is selected from the Network menu. This screen is used for unlocking accounts or IP addresses of administrators currently locked out of the SR user interface.



There is no admin account currently locked out.

200.10.101.82 □

Fig. 2:2-3 Locked-out Accounts and IPs screen

***NOTE**: An account or IP address becomes locked if the Password Security Options feature is enabled in the Optional Features screen (see Optional Features screen in this chapter), and a user is unable to log into the SR user interface due to an expired password, or having met the specified number of failed password attempts within the designated timespan.*

View Locked Accounts, IP addresses

The frames in this screen display the following messages if there are no users currently locked out:

- **Locked-out Admin Accounts** - There is no administrator account currently locked out.
- **Locked-out IPs** - There is no IP currently locked out.

If there are any locked accounts/IP addresses in a frame, each locked username/IP address displays on a separate line followed by a checkbox. The Select All and Unlock buttons display at the bottom of the frame.

Unlock Accounts, IP addresses

To unlock an account/IP address in a frame:

1. Click the checkbox corresponding to the username/IP address.

***TIP**: To unlock all accounts/IPs in a frame, click **Select All** to populate all checkboxes in the frame with check marks.*

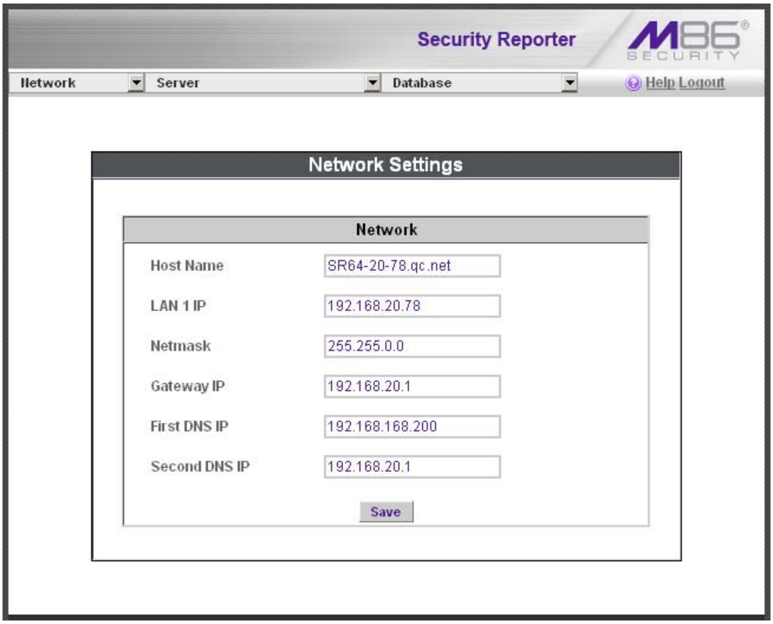
2. Click **Unlock** to unlock the specified accounts/IPs, and to display the message screen showing one of the following pertinent messages for each unlocked account/IP:
   - Admin account: ‘xxx’ has been successfully unlocked.
   - IP: ‘x.x.x.x’ has been successfully unlocked.

***NOTE**: In the text above, ‘xxx’ and ‘x.x.x.x’ represents the unlocked username/IP address.*

3. Click **OK** to return to the Locked-out Accounts and IPs screen that no longer shows the accounts/IPs that have been unlocked.

Network Settings screen

The Network Settings screen displays when the Network Setting option is selected from the Network menu. This screen is used for setting up IP addresses so the server can communicate with your system.



Network Settings

Network

Host Name: SR64-20-78.qc.net

LAN 1 IP: 192.168.20.78

Netmask: 255.255.0.0

Gateway IP: 192.168.20.1

First DNS IP: 192.168.168.200

Second DNS IP: 192.168.20.1

Fig. 2:2-4 Network Settings screen

Set up/Edit IP Addresses

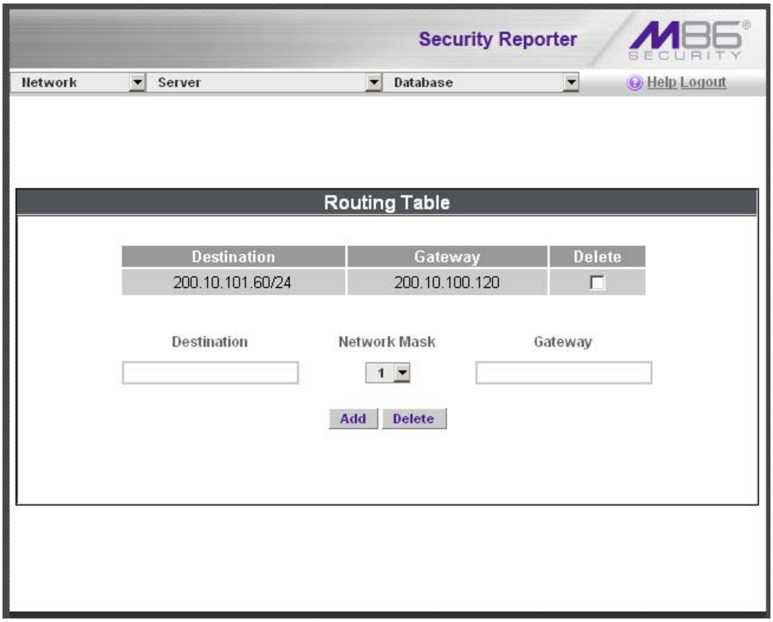
TIP*: In order for the server to effectively communicate with your system, be sure all fields contain accurate information before saving your settings.*

1. Enter or edit an IP address in each appropriate field:
   - In the **Host Name** field, enter the address or URL that will be used for accessing the System Configuration administrator console. This entry should include the full, qualified domain name, and the “host” name for the box (i.e. reporter.myserver.com).
   - In the **LAN 1 IP** field, enter the IP address of the SR server on your Local Area Network (LAN 1).
   - In the **Netmask** field, enter the netmask that will define the traffic designated for the LAN.
   - In the **Gateway IP** field, enter the IP address for the default router that will be the main gateway for the entire network segment.
   - In the **First DNS IP** field, enter the IP address of the primary Domain Name System (name server). The server will use this IP address to identify other IP addresses on the system, including its own IP address.
   - In the **Second DNS IP** field, enter the IP address of the fallback DNS.
2. Be sure each IP address is correct, and then click **Save**.

NOTE*: After appropriate entries have been made in these fields and saved, you must restart the server to activate the IPs. To restart the server, select the* ***Restart Hardware*** *option on the Shut Down screen. (See the Shut Down sub-section under the Server menu section in this chapter.)*

Routing Table screen

The Routing Table screen displays when the Routing Table option is selected from the Network menu. This screen is used for viewing, building, and maintaining a list of routers—network destination and gateway IP addresses—the server will use for communicating with other segments of the network. You will only need to set up a routing table if your local network is interconnected with another network.



Routing Table

Destination	Gateway	Delete
200.10.101.60/24	200.10.100.120	□

Destination

Network Mask 1

Gateway

Fig. 2:2-5 Routing Table screen

View a List of Routers

Each router that was configured in the routing table displays as a separate row in the table. The IP address and subnet mask to receive data packets display in the Destination column, and the IP address of the portal that will transfer data packets to and from the Internet displays in the Gateway column.

Add a Router

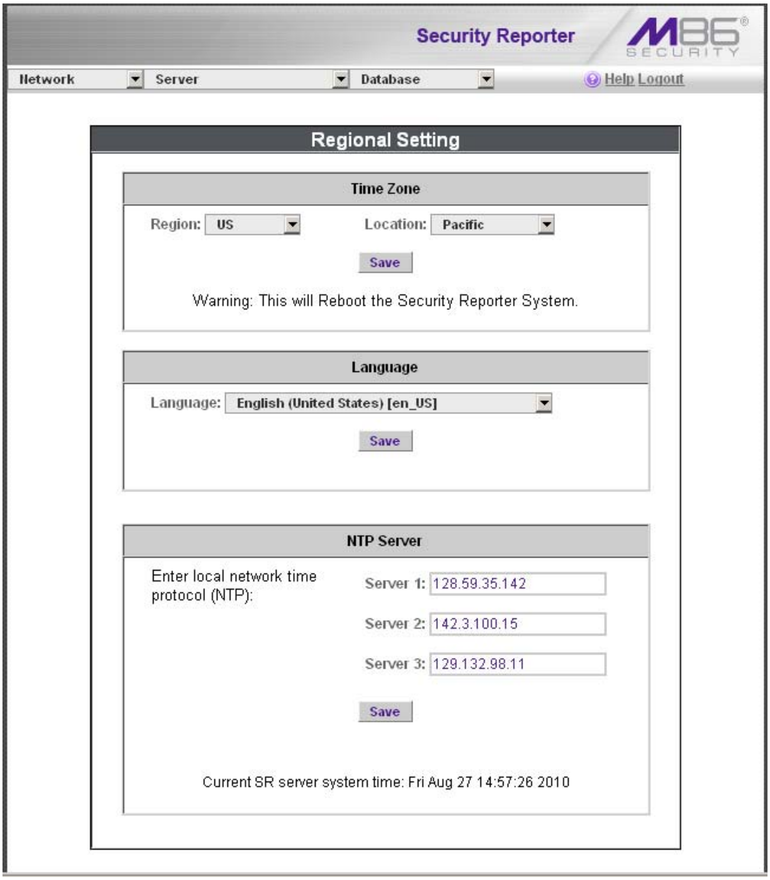
1. In the **Destination** field, enter the IP address of the network to which data packets will be forwarded.
2. At the **Network Mask** pull-down menu, specify the number (1-32) of the subnet mask that will be used for grouping IP addresses on the same local network.
3. In the **Gateway** field, enter the IP address of the portal to which data packets will be transferred to and from the Internet.
4. Click the **Add** button to include your entry in the table. If you have another router to add, follow steps 1-4.
5. Click the **Back** button on the confirmation screen to return to the Routing Table screen.

Delete a Router

1. Click in the **Delete** checkbox of the row corresponding to the router you wish to remove from the routing table.
2. Click the **Delete** button.
3. Click the **Back** button on the confirmation screen to return to the Routing Table screen.

Regional Setting screen

The Regional Setting screen displays when the Regional Setting option is selected from the Network menu. This screen is used for specifying the time zone and network time to be used by the server when generating reports via the Report Manager, and setting the language set type to be displayed in the application, if necessary.



Regional Setting

Time Zone

Region: US   Location: Pacific

Warning: This will Reboot the Security Reporter System.

Language

Language: English (United States) [en_US]

NTP Server

Enter local network time protocol (NTP):

Server 1: 128.59.35.142

Server 2: 142.3.100.15

Server 3: 129.132.98.11

Current SR server system time: Fri Aug 27 14:57:26 2010

Fig. 2:2-6 Regional Setting screen

Specify the Time Zone

1. At the **Region** pull-down menu, select your country from the available choices.
2. At the **Location** pull-down menu, select the time zone for the specified region.
3. Click **Save** to apply your settings, and to restart the Web Client Server.

⚠ ***WARNING**: The time zone set for the SR should be the same one set for each Web access logging device to be used by the SR. These "like" settings ensure consistency when tracking the logging times of all users on the network.*

Specify the Language Set

1. If necessary, select a language set from the **Language** pull-down menu to specify that you wish to display that text in the console.
2. Click **Save** to apply your settings.

Specify Network Time Protocol Servers

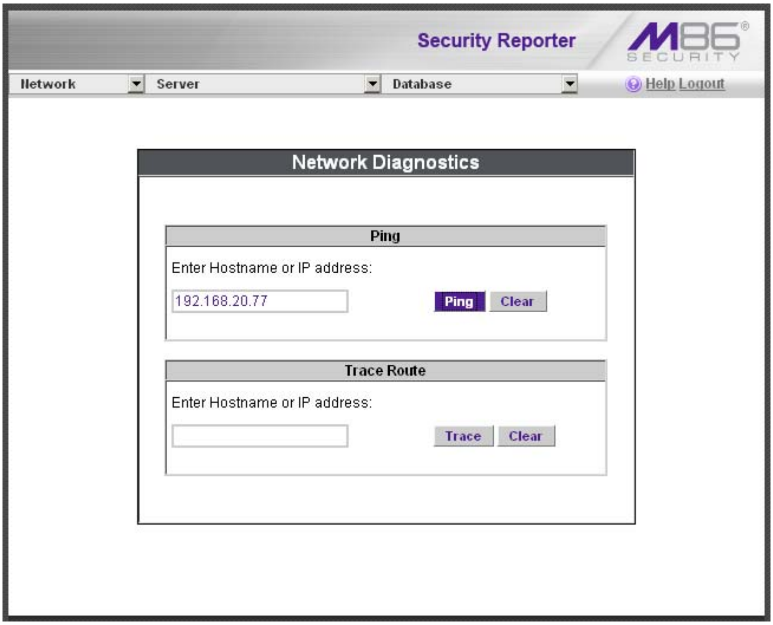
IP addresses of servers running Network Time Protocol (NTP) software are entered in the Server fields, and the Current SR server system time (day, date, HH:MM:SS time format, and year) displays below. NTP is a time synchronization system for computer clocks throughout the Internet. Your SR server will use the actual time from clocks at the IP addresses you've specified.

For the Enter local network time protocol (NTP) server fields, by default, the following IP addresses display in these three fields: 128.59.35.142, 142.3.100.15, and 129.132.98.11. If you wish to use different NTP servers, follow these steps:

1. Enter or edit an IP address in each appropriate field:
   - In the **Server 1** field, enter the IP address of the primary NTP server to be used for clock settings on your server.
   - In the **Server 2** field, enter the IP address of the secondary NTP server. The time from this server will be used by your server if the IP address for the primary server fails to be accessed by your server.
   - In the **Server 3** field, enter the IP address of the tertiary NTP server. The time from this server will be used by your server if the IP addresses for the primary and secondary servers fail to be accessed by your server.
2. Click the **Save** button to save your entries.

Network Diagnostics screen

The Network Diagnostics screen displays when the Diagnostics option is selected from the Network menu. This screen is used to help you identify and resolve problems with your network configuration, using the ping and trace route utility tools.



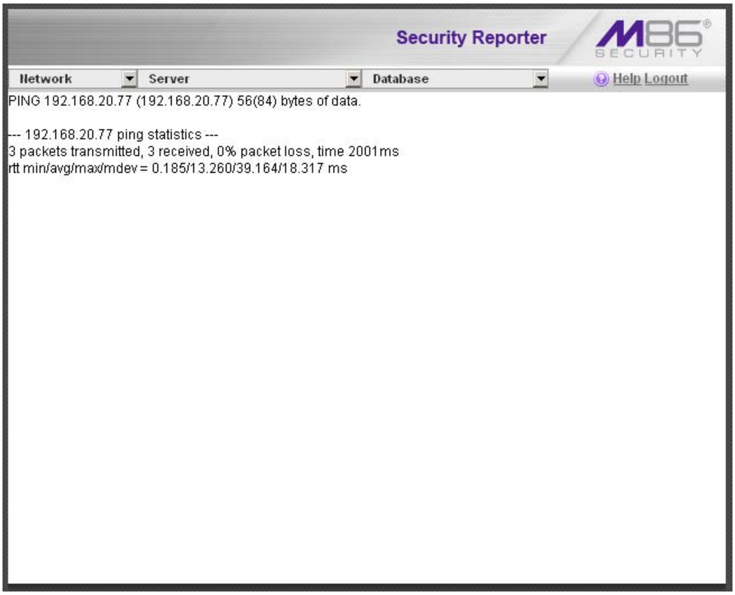
192.168.20.77

Fig. 2:2-7 Network Diagnostics screen, Ping entry

Ping

The ping utility is used for verifying whether the server can communicate with a machine at a given IP address within the network, and the speed of the network connection.

1. In the Ping frame, enter the IP address or host name of the specific Internet address to be contacted (pinged).
2. Click the **Ping** button to display the results found by the server, as shown on the sample screen:



```
PING 192.168.20.77 (192.168.20.77) 56(84) bytes of data.

--- 192.168.20.77 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 0.185/13.260/39.164/18.317 ms
```

Fig. 2:2-8 Ping results

As indicated by the results for the sample entry, the server at 192.168.20.78 was able to communicate with the machine at the IP address 192.168.20.77. The statistics show that three (3) data packets were transmitted by the server, and three (3) packets were received by the designated machine, for a total of zero (0) percent packet loss.

***TIP**: If the machine cannot be contacted, be sure the ping feature on that machine is turned on.*

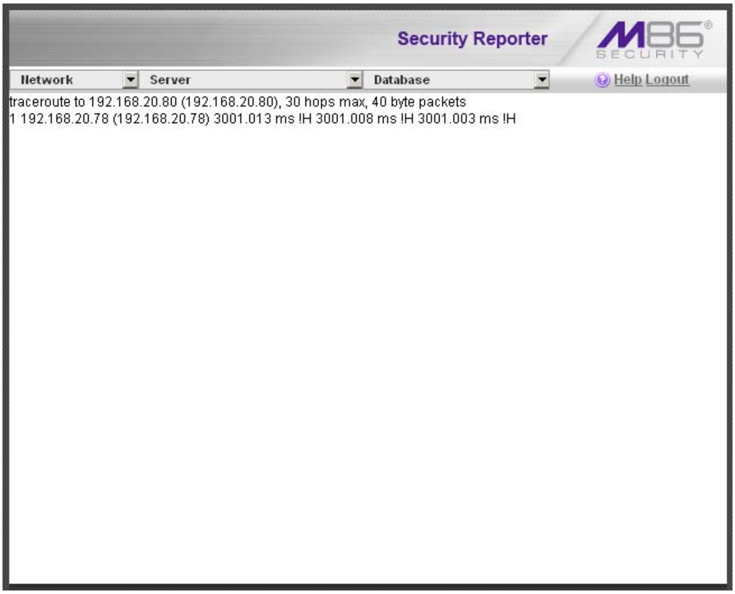
***NOTE**: To ping another IP address, click the Back button in your browser window, then click the Clear button in the Ping frame, and follow the procedures documented in this sub-section.*

Trace Route

If the ping utility was not able to help you diagnose the problem with your network configuration, you should use the trace route utility. This diagnostic tool records each “hop” (trip from one router to another) the data packet made, identifying the IP addresses of gateway computers where the packet stopped en route to its final destination, and the length of time of each hop.

***NOTE**: The trace route utility can be used after your routing table has been set up. To set up a routing table, see the Routing Table screen sub-section under the Network menu in this chapter.*

1. In the Trace Route frame, enter the IP address or host name of the specific Internet address to be validated.
2. Click the **Trace** button to display the results found by the server, as shown on the sample screen:



```
traceroute to 192.168.20.80 (192.168.20.80), 30 hops max, 40 byte packets
1 192.168.20.78 (192.168.20.78) 3001.013 ms !H 3001.008 ms !H 3001.003 ms !H
```

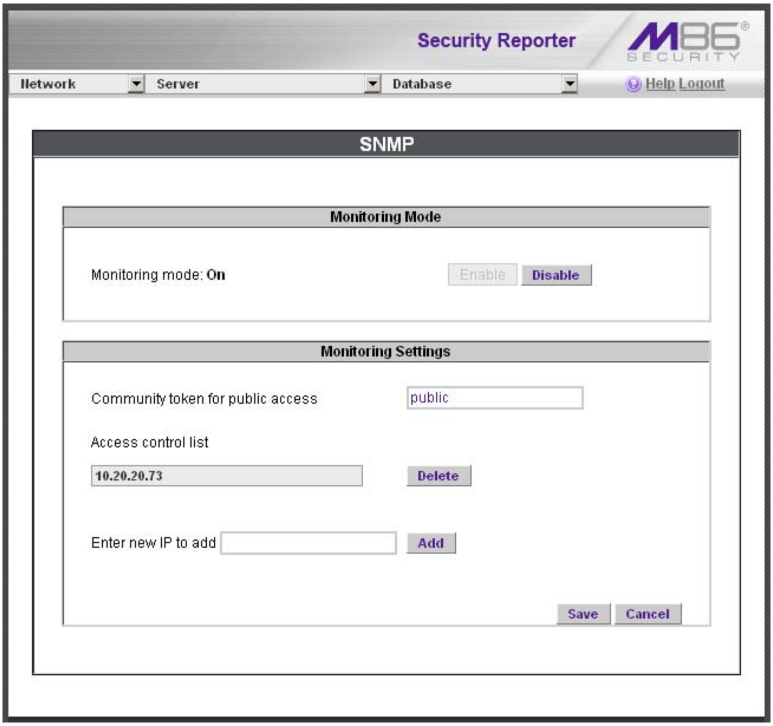
Fig. 2:2-9 Trace Route results

As indicated by the results for the sample entry, the packet made 30 hops. For each line in the report, the hop number displays, followed by the IP address or host name; the IP address in parentheses; and the maximum, minimum, and average response time in milliseconds.

TIP*: To “trace” another IP address, click the Back button in your browser window, then click the Clear button in the Trace Route frame, and follow the procedures documented in this sub-section.*

SNMP screen

The SNMP screen displays when the SNMP option is selected from the Network menu. This feature lets the global administrator use a third party Simple Network Management Protocol (SNMP) product for monitoring and managing the working status of the SR's Internet reporting on a network.



Monitoring mode: On

Community token for public access: public

Access control list: 10.20.20.73

Fig. 2:2-10 SNMP screen

The following aspects of the SR are monitored by SNMP: data traffic sent/received by a NIC, CPU load average at a given time interval, amount of free disk space for each disk partition, time elapse since the SR was last rebooted, and the amount of memory currently in usage.

Enable SNMP

The **Monitoring mode** is “Off” by default. To enable SNMP, click **Enable** in the Monitoring Mode frame. As a result, all elements in this window become activated.

Set up Community Token for Public Access

Enter the password to be used as the **Community token for public access**. This is the password that the management console would use when requesting access.

Create, Build the Access Control List

1. In the **Enter new IP to add** field, enter the IP address of an interface from/to which the SNMP should receive/ send data.
2. Click **Add** to include the entry in the Access control list box.

   Repeat steps 1 and 2 for each IP address to be included in the list.
3. After all entries are made, click **Save**.

Maintain the Access Control List

1. To remove one or more IP addresses from the list, select each IP address from the Access control list, using the **Ctrl** key for multiple selections.
2. Click **Delete**.
3. Click **Save**.

Server Menu

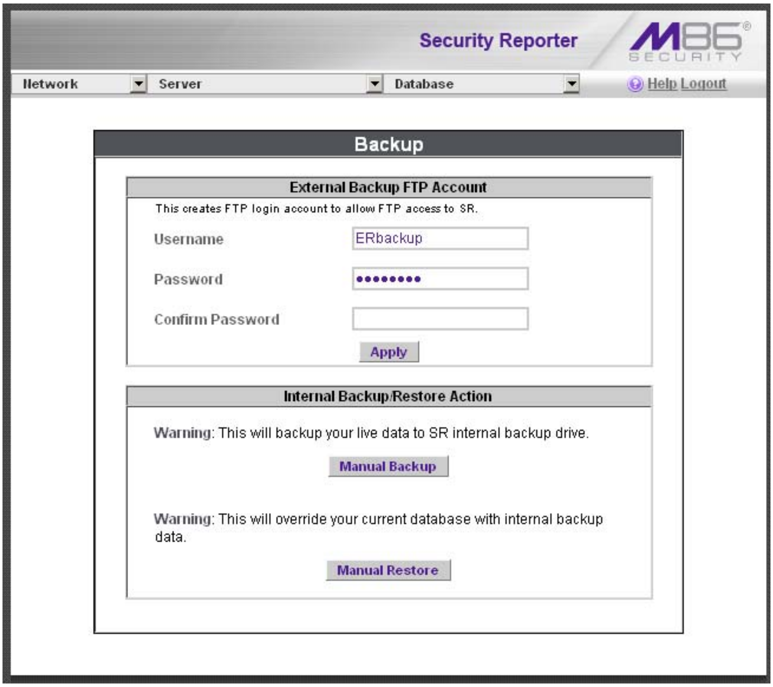
The Server pull-down menu includes options for setting up processes for maintaining the server. These options are: Backup, Self-Monitoring, SMTP Server Setting, Server Status, Secure Access, Software Update, Software Update Setting, Shut Down, Report Manager, and Hardware Failure Detection.

***NOTE**: If running the SR as a virtual machine, the Backup screen is not available, and the Hardware Failure Detection screen displays a message indicating the server is not a RAID server.*

Backup screen

The Backup screen displays when the Backup option is selected from the Server menu. This screen is used for setting up the password for the remote server's FTP account, for executing an immediate backup on the SR, and for performing a restoration to the database from the previous backup run.

***NOTE**: The Backup screen is not available if running the SR as a virtual machine.*



Backup

External Backup FTP Account

This creates FTP login account to allow FTP access to SR.

Username: ERbackup

Password: ●●●●●●●●●

Confirm Password:

Internal Backup/Restore Action

Warning: This will backup your live data to SR internal backup drive.

Warning: This will override your current database with internal backup data.

Fig. 2:2-11 Backup screen

Backup and Recovery Procedures

❗ ***IMPORTANT**: M86 Security recommends establishing backup and recovery procedures when you first begin using the SR. Please follow the advice in this section to ensure your SR is properly maintained in the event that data is lost and back up procedures need to be performed to recover data.*

Although automatic backups to a local SR hard drive are scheduled weekly by default, it is important that the SR administrator implements a backup policy to ensure data integrity and continuity in the event of any possible failure scenario. This policy should include frequent, remote backups, such that raw logs and SR database files are available for restoration without relying on the SR’s hard drives.

In general, recovery plans involve (i) restoring the most recent backup of the database, and (ii) restoring raw logs to fill in the gap between the most recent backup of the database, and the current date and time.

Some scenarios and action plans to consider include the following:

- **The SR database becomes corrupted** - Correct the root problem. Restore the database from the most recent SR backup, and reprocess raw logs up to the current date and time.
- **The data drive fails** - Replace the data drive. Restore the database from the SR backup drive, and reprocess raw logs up to the current date and time.
- **The backup drive fails** - Replace the backup drive, and perform a manual backup.
- **Both data and backup drives are damaged** - Restore the database from the most recent remote backup, and reprocess raw logs up to the current date and time.

As you can see, it is critical that raw logs are available to bridge the gap between the last database backup and the present time, and more frequent backups (local and remote) result in less “catch-up” time required for reprocessing raw logs.

Set up/Edit External Backup FTP Password

In order to back up the SR’s database to a remote server, an FTP account must be established for the remote server.

***NOTE**: In the External Backup FTP Account frame, the login name that will be used to access the remote server displays in the Username field. This field cannot be edited.*

1. In the **Password** field, enter up to eight characters for the password. The entry in this field is alphanumeric and case sensitive.
2. In the **Confirm Password** field, re-enter the password in the exact format used in the Password field.
3. Click the **Apply** button to save your entries. The updated Account ID will be activated after two minutes.

Execute a Manual Backup

In addition to performing on demand backups in preparation for a disaster recovery, you may wish to execute a manual backup under the following circumstances:

- **Power outage** - If there is a power outage at your facility and your system uses a backup battery, you might want to back up data before the battery fails.
- **Rolling blackout** - If your facility is subjected to rolling blackouts, and a blackout is scheduled during the time of your daily backup, you should back up your data before the blackout period, when the SR will be down.
- **Expiration about to occur** - If a data expiration is about to occur, you might want to back up your data before

losing the oldest data on the SR, prior to the daily backup process.

***WARNING**: If corrupted data is detected on the SR, do not backup your data, as you may back up and eventually restore a corrupted database.*

When performing a manual backup, the SR's database is immediately saved to the internal backup drive. From the remote server, the backup database can be retrieved via FTP, and then stored off site.

***TIP**: M86 Security recommends executing an on demand backup during the lightest period of system usage, so the server will perform at maximum capacity.*

1. Click the **Manual Backup** button in the Internal Backup/ Restore Action frame to specify that you wish to back up live data to the SR's internal backup drive.
2. On the Confirm Backup/Restore screen, click the **Yes** button to back up the database tables and indexes.

***WARNING**: M86 Security recommends that you do not perform other functions on the SR until the backup is complete. The time it will take to complete the backup depends on the size of all tables being saved.*

Perform a Remote Backup

After executing the manual backup, a remote backup can be performed on your remote server.

***NOTE**: Before beginning this FTP process, be sure you have enough space on the remote server for storing backup data. The required space can be upwards of 200 gigabytes.*

1. Log in to your FTP account.
2. Use FTP to download the SR's backup database to the remote server. When you are in the DAILY, WEEKLY, or MONTHLY sub-directory, be sure to get all the *.gz data files to include in your backup. You can then go to the

archive directory to get all the raw logs to include in your backup.

3. Store this backup data in a safe place off the remote server. If this backup database needs to be restored, it can be uploaded to the SR via FTP. (See Perform a Restoration to the SR Server.)

Perform a Restoration to the SR Server

There are two parts in performing a restoration of data to your SR. Part one requires data to be loaded on the remote server and then FTPed to the SR. Part two requires the FTPed data to be restored on the SR.

***NOTE**: Before restoring backup data to the SR, be sure you have enough space on the SR. Data that is restored to the SR will automatically include indexes.*

Perform these steps on the remote server:

1. Load the *.gz file backup data on your remote server.
2. Log in to your FTP account.
3. FTP the backup data to the SR's internal backup drive in the appropriate sub-directory: DAILY, WEEKLY, or MONTHLY.

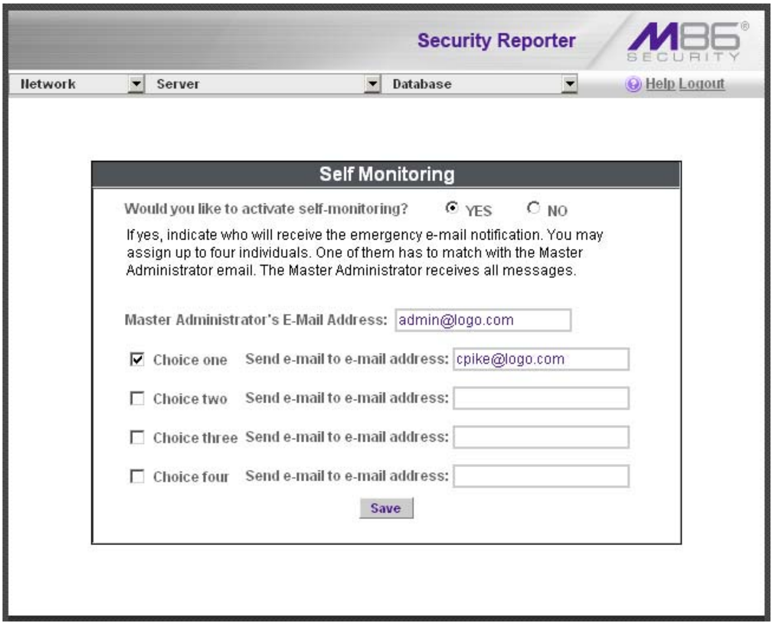
On the SR Server's Backup screen:

1. Click the **Manual Restore** button in the Internal Backup/ Restore Action frame to specify that you wish to over-write data on the live SR with data from the previous, internal backup run.
2. On the Confirm Backup/Restore screen, click the **Yes** button to restore database tables and indexes to the SR.

***NOTE**: The amount of time it will take to restore data to the SR depends on the combined size of all database tables being restored. M86 Security recommends that you do not perform other functions on the SR until the restoration is complete.*

Self Monitoring screen

The Self Monitoring screen displays when the Self-Monitoring option is selected from the Server menu. This screen is used for setting up and maintaining e-mail addresses of contacts who will receive automated notifications if problems occur with the network. Possible alerts include situations in which a daemon stops running, software fails to run, corrupted files are detected, or a power outage occurs.



Self Monitoring

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

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

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

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

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

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

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

Fig. 2:2-12 Self Monitoring screen

As the administrator of the server, you have the option to either activate or deactivate this feature. When the self-monitoring feature is activated, an automated e-mail message is dispatched to designated recipients if the server identifies a failed process during its hourly check for new data.

View a List of Contact E-Mail Addresses

If this feature is currently activated, the e-mail address of the Master Administrator displays on this screen, along with any other contacts set up as Choice one - four.

Set up and Activate Self-Monitoring

1. Click the radio button corresponding to **YES**.
2. Enter the **Master Administrator's E-Mail Address**.
3. In the **Send e-mail to e-mail address** fields, enter at least one e-mail address of a person authorized to receive automated notifications. This can be the same address entered in the previous field. Entries in the three remaining fields are optional.
4. If e-mail addresses were entered in any of the four optional e-mail address fields, click in the **Choice one - Choice four** checkboxes corresponding to the e-mail address(es).
5. Click the **Save** button to activate self-monitoring.

Remove Recipient from E-mail Notification List

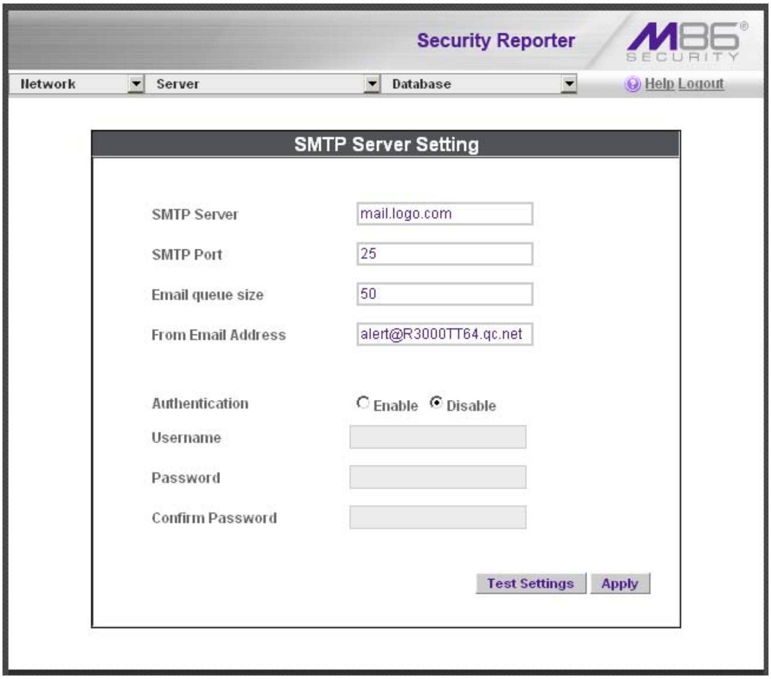
1. To stop sending emergency notifications to an e-mail address set up in the list, remove the check mark from the checkbox corresponding to the appropriate e-mail address.
2. Click the **Save** button to remove the recipient's name from the e-mail list. The Master Administrator and any remaining e-mail addresses in the list will continue receiving notifications.

Deactivate Self-Monitoring

1. Click the radio button corresponding to **NO**.
2. Click the **Save** button to deactivate self-monitoring.

SMTP Server Setting screen

The SMTP Server Setting screen is used for entering settings for the Simple Mail Transfer Protocol that will be used for sending email alert messages to specified administrators.



SMTP Server Setting

SMTP Server: mail.logo.com

SMTP Port: 25

Email queue size: 50

From Email Address: alert@R3000TT64.qc.net

Authentication ○ Enable ● Disable

Username

Password

Confirm Password

Fig. 2:2-13 SMTP Server Setting screen

Enter, Edit SMTP Server Settings

1. Enter the **SMTP Server** name, for example: **mail.logo.com**.
2. By default, the **SMTP Port** number used for sending email is *25*. This should be changed if the sending mail connection fails.
3. By default, the **Email queue size** is *50*. This can be changed to specify the maximum number of requests

that can be placed into the queue awaiting an available outbound connection.

4. In the **From Email Address** field, enter the email address of the server that will be sending alert email messages to designated administrators.
5. By default, **Authentication** is disabled. Click “Enable” if a username and password are required for logging into the SMTP server. This action activates the fields below.

   Make the following entries:

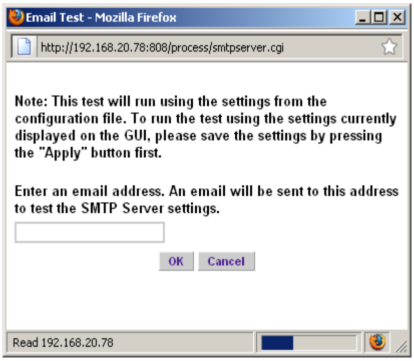
   a. Enter the **Username**.

   b. Enter the **Password** and make the same entry in the **Confirm Password** field.
6. Click **Apply** to apply your settings.

Verify SMTP Settings

To verify that email messages can be sent to a specified address:

1. Click **Test Settings** to open the pop-up box:



Email Test - Mozilla Firefox

http://192.168.20.78:808/process/smtpserver.cgi

Note: This test will run using the settings from the configuration file. To run the test using the settings currently displayed on the GUI, please save the settings by pressing the "Apply" button first.

Enter an email address. An email will be sent to this address to test the SMTP Server settings.

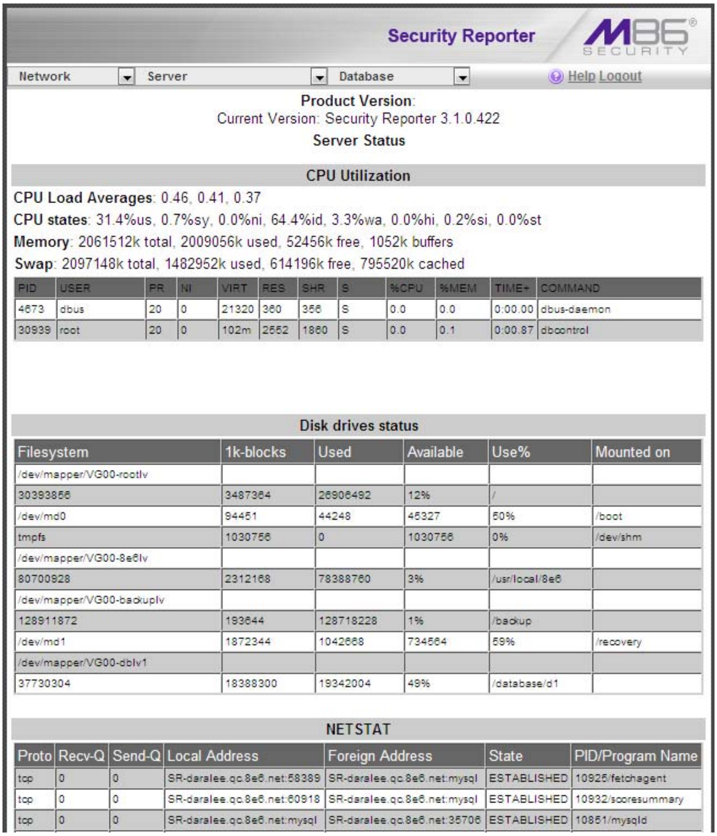
Fig. 2:2-14 SMTP Email Test box

2. Enter the email address in the pop-up box.

3. Click **OK** to close the pop-up box and to process your request. If all SMTP settings are accepted, the test email should be received at the specified address.

Server Status screen

The Server Status screen displays when the Server Status option is selected from the Server menu. This screen, which automatically refreshes itself every 10 seconds, displays the statuses of processes currently running on the server, and provides information on the amount of space and memory used by each process.



Product Version:
Current Version: Security Reporter 3.1.0.422

Server Status

CPU Utilization

CPU Load Averages: 0.46, 0.41, 0.37

CPU states: 31.4%us, 0.7%sy, 0.0%ni, 64.4%id, 3.3%wa, 0.0%hi, 0.2%si, 0.0%st

Memory: 2061512k total, 2009056k used, 52456k free, 1052k buffers

Swap: 2097148k total, 1482952k used, 614196k free, 795520k cached

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
4673	dbus	20	0	21320	360	356	S	0.0	0.0	0:00.00	dbus-daemon
30939	root	20	0	102m	2552	1860	S	0.0	0.1	0:00.87	dbcontrol

Disk drives status

Filesystem	1k-blocks	Used	Available	Use%	Mounted on
/dev/mapper/VG00-rootlv					
30393856	3487364	26906492	12%	/	
/dev/md0	94451	44248	45327	50%	/boot
tmpfs	1030756	0	1030756	0%	/dev/shm
/dev/mapper/VG00-8e6lv					
80700928	2312168	78388760	3%	/usr/local/8e6	
/dev/mapper/VG00-backuplv					
128911872	193644	128718228	1%	/backup	
/dev/md1	1872344	1042668	734564	59%	/recovery
/dev/mapper/VG00-dblv1					
37730304	18388300	19342004	49%	/database/d1	

NETSTAT

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program Name
tcp	0	0	SR-daralee.qc.8e6.net:58389	SR-daralee.qc.8e6.net:mysql	ESTABLISHED	10925/fetchagent
tcp	0	0	SR-daralee.qc.8e6.net:60918	SR-daralee.qc.8e6.net:mysql	ESTABLISHED	10932/scoresummary
tcp	0	0	SR-daralee.qc.8e6.net:mysql	SR-daralee.qc.8e6.net:35706	ESTABLISHED	10851/mysqld

Fig. 2:2-15 Server Status screen

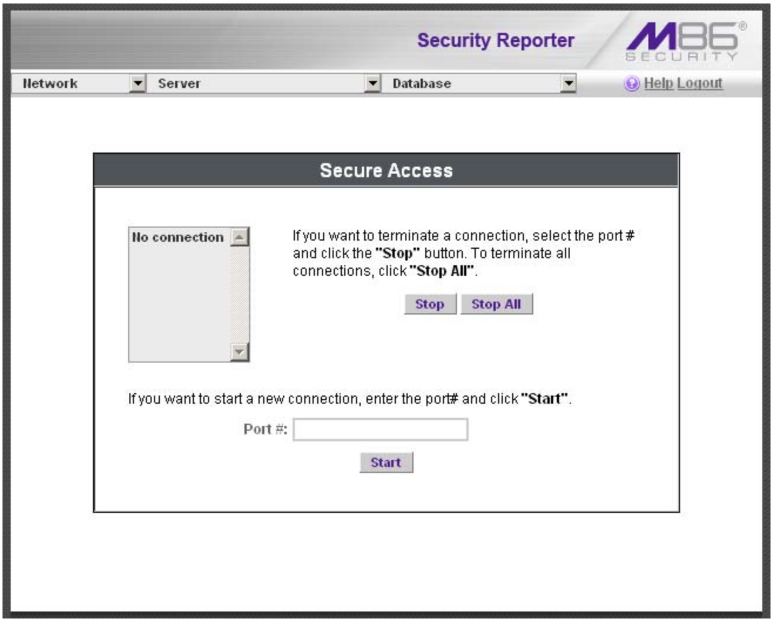
View the Status of the SR Server

The Product Version number of the software displays at the top of the screen, along with the date that software version was implemented. Status information displays in the following sections of this screen:

- CPU Utilization - includes CPU process data and information on the status of the top command
- Disk drives status - provides data on the status of each drive of the operating system
- NETSTAT - displays the status of a local IP address

Secure Access screen

The Secure Access screen displays when the Secure Access option is selected from the Server menu. This screen is primarily used by M86 Security technical support representatives to perform maintenance on your server, if your system is behind a firewall that denies access to your server.



If you want to terminate a connection, select the port # and click the **"Stop"** button. To terminate all connections, click **"Stop All"**.

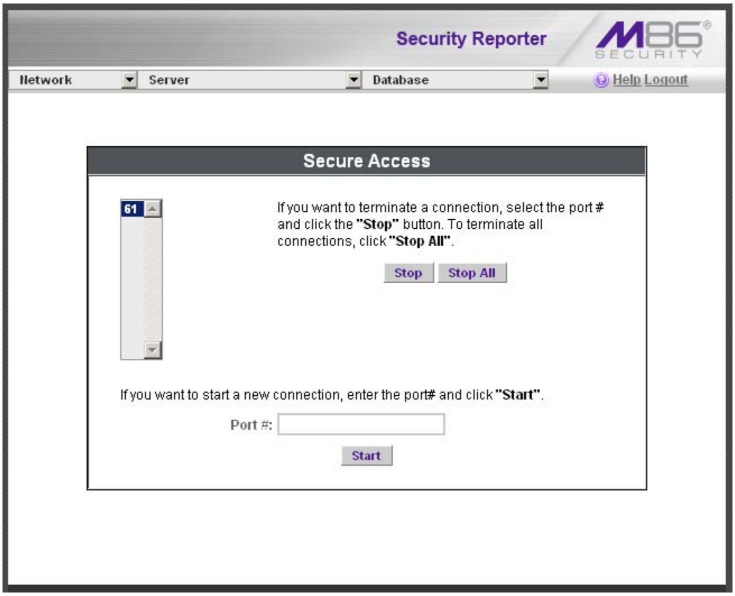
If you want to start a new connection, enter the port# and click **"Start"**.

Fig. 2:2-16 Secure Access screen

Activate a Port to Access the SR Server

1. After the administrator at the customer’s site authorizes you to use a designated port to access their server, enter that number at the **Port #** field.

2. Click the **Start** button to activate the port. This action enters the port number in the list box above, replacing the text: “No connection”.



Secure Access

If you want to terminate a connection, select the port # and click the **"Stop"** button. To terminate all connections, click **"Stop All"**.

If you want to start a new connection, enter the port# and click **"Start"**.

Port #:

Fig. 2:2-17 Port entries

Terminate a Port Connection

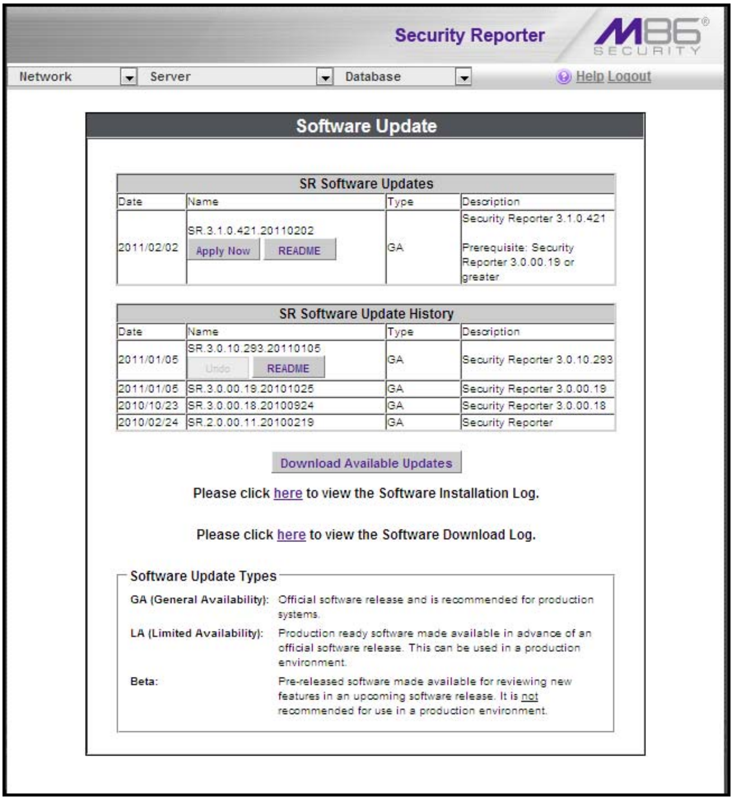
1. After maintenance has been performed on the customer’s server, select the active port number from the list box by clicking on it.
2. Click the **Stop** button to terminate the port connection. This action removes the port number from the list box.

Terminate All Port Connections

If more than one port is currently active on the customer’s server and you need to terminate all port connections, click the **Stop All** button. This action removes all port numbers from the list box.

Software Update screen

The Software Update screen displays when the Software Update option is selected from the Server menu. This screen is used for updating the SR with software updates supplied by M86 Security, verifying the download and/or installation of software updates on the SR, and viewing a list of software updates currently available and/or previously installed on the SR. This screen is also used for accepting LA/Beta software downloads, if choosing to download Limited Availability (LA) and/or Beta updates for previewing software features to be included in the General Availability (GA) release to be distributed to all SRs.



Software Update

SR Software Updates

Date	Name	Type	Description
2011/02/02	SR.3.1.0.421.20110202 Apply Now README	GA	Security Reporter 3.1.0.421 Prerequisite: Security Reporter 3.0.00.19 or greater

SR Software Update History

Date	Name	Type	Description
2011/01/05	SR.3.0.10.293.20110105 Undo README	GA	Security Reporter 3.0.10.293
2011/01/05	SR.3.0.00.19.20101025	GA	Security Reporter 3.0.00.19
2010/10/23	SR.3.0.00.18.20100924	GA	Security Reporter 3.0.00.18
2010/02/24	SR.2.0.00.11.20100219	GA	Security Reporter

Please click here to view the Software Installation Log.

Please click here to view the Software Download Log.

Software Update Types

GA (General Availability): Official software release and is recommended for production systems.

LA (Limited Availability): Production ready software made available in advance of an official software release. This can be used in a production environment.

Beta: Pre-released software made available for reviewing new features in an upcoming software release. It is not recommended for use in a production environment.

Fig. 2:2-18 Software Update screen

***NOTE**: Definitions for Software Update Types (GA, LA, and Beta) are provided in the frame at the bottom of this screen. General Availability (GA) software updates are supplied to all current SR units. Limited Availability (LA) and/or Beta software updates are available to SR units that have the feature to download LA and/or Beta software updates enabled, as described in this sub-section and the Software Update Setting screen sub-section.*

View Software Update Criteria

View Installed Software Updates

Information about software updates previously installed on the server displays in the SR Software Update History frame. For each installed software update, the following displays: Date installed (YYYY/MM/DD); software update Name; Type of update (GA, LA, or Beta), and Description.

View Available Software Updates

***NOTE**: The SR Software Updates frame displays only if there is at least one software update available to install.*

Any software update available for installation on the SR server displays in the SR Software Updates frame. The following information is included for each software update: Date the software update was made available (YYYY/MM/DD); software update Name; Type of update (GA, LA, or Beta), and Description (software version number and Prerequisite software version for installing the software update).

The Apply Now and README buttons display beneath the software update Name. (See Install a Software Update for information about these buttons.)

Install a Software Update

***WARNING**: All software updates must be installed in order from oldest to newest.*

***NOTE**: Be sure to terminate all reports that are currently running or are scheduled to run before applying a software update, and that port 8084 is open on your network.*

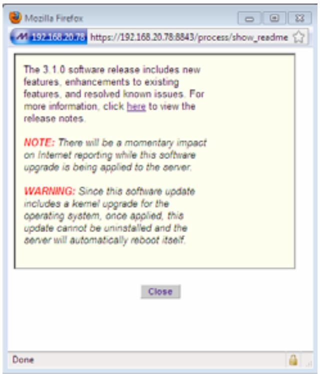
General Software Installation Procedures

The steps in this sub-section pertain to the installation of General Availability software updates, and the application of LA/Beta software updates following the initial LA/Beta software download acceptance procedures (described in First Time LA/Beta Software Install Procedures).

In the SR Software Updates frame (see Fig. 2:2-18), two buttons are available: README and Apply Now.

README:

1. Click **README** to open a pop-up box containing information about the software release:



The 3.1.0 software release includes new features, enhancements to existing features, and resolved known issues. For more information, click here to view the release notes.

NOTE: *There will be a momentary impact on Internet reporting while this software upgrade is being applied to the server.*

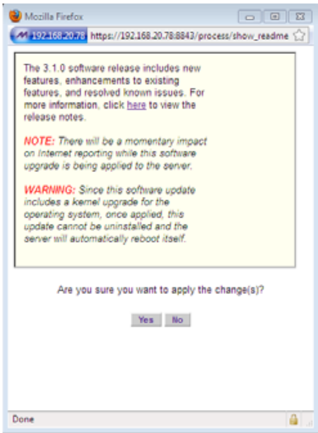
WARNING: *Since this software update includes a kernel upgrade for the operating system, once applied, this update cannot be uninstalled and the server will automatically reboot itself.*

Fig. 2:2-19 Readme box

2. After reading the contents of the software release, click **Close** to close the pop-up box.

Apply Now:

1. Click **Apply Now** to open a dialog box containing information about the software release:



The 3.1.0 software release includes new features, enhancements to existing features, and resolved known issues. For more information, click here to view the release notes.

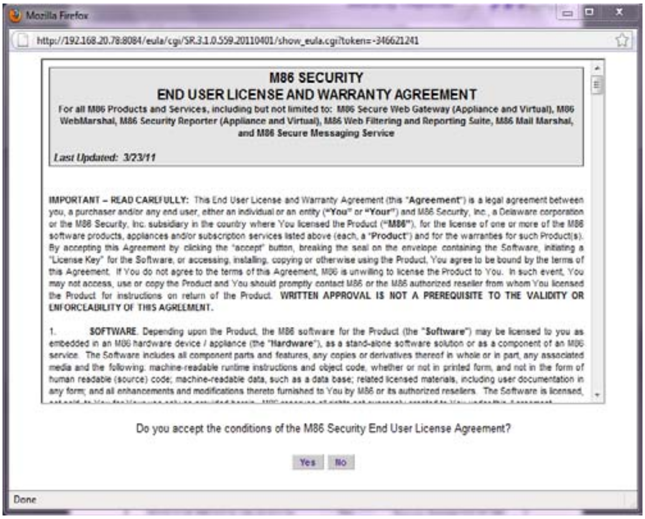
NOTE: There will be a momentary impact on Internet reporting while this software upgrade is being applied to the server.

WARNING: Since this software update includes a kernel upgrade for the operating system, once applied, this update cannot be uninstalled and the server will automatically reboot itself.

Are you sure you want to apply the change(s)?

Fig. 2:2-20 Software update dialog box

2. Click **Yes** to open the EULA dialog box:


Mozilla Firefox
http://192.168.20.78:8084/eula/cgi/SR.3.1.0.559.20110401/show_eula.cgi?token=-346621241

M86 SECURITY
END USER LICENSE AND WARRANTY AGREEMENT
For all M86 Products and Services, including but not limited to: M86 Secure Web Gateway (Appliance and Virtual), M86 WebMarshal, M86 Security Reporter (Appliance and Virtual), M86 Web Filtering and Reporting Suite, M86 Mail Marshal, and M86 Secure Messaging Service

Last Updated: 3/23/11

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

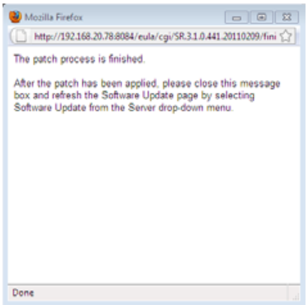
1. **SOFTWARE**. Depending upon the Product, the M86 software for the Product (the "**Software**") may be licensed to you as embedded in an M86 hardware device / appliance (the "**Hardware**"), as a stand-alone software solution or as a component of an M86 service. The Software includes all component parts and features, any copies or derivatives thereof in whole or in part, any associated media and the following: machine-readable runtime instructions and object code, whether or not in printed form, and not in the form of human readable (source) code; machine-readable data, such as a data base; related licensed materials, including user documentation in any form; and all enhancements and modifications thereto furnished to You by M86 or its authorized resellers. The Software is licensed,

Do you accept the conditions of the M86 Security End User License Agreement?

Fig. 2:2-21 EULA dialog box

3. After reading the contents of the End User License Agreement, click **Yes** if you agree to its terms. This action closes the EULA dialog box and begins the software update application process, launching a pop-up box showing the progress of the software installation.

   A successful software installation displays a completion message with notification that the Software Update screen needs to be refreshed via **Server > Software Update** in order to display the latest software update in the SR Software Update History frame:



Mozilla Firefox
http://192.168.20.78:8084/eula/cgi/SR.3.1.0.441.20110209/fini

The patch process is finished.

After the patch has been applied, please close this message box and refresh the Software Update page by selecting Software Update from the Server drop-down menu.

Fig. 2:2-22 Software installation progress box

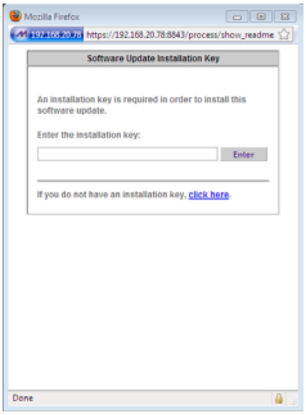
***NOTE**: After installing the software update, if a message displays that informs you to reboot the server, you should select the **Restart Software** option on the Shut Down screen.*

First Time LA/Beta Software Install Procedures

The steps in this sub-section pertain to the first acceptance and installation of Limited Availability or Beta software updates.

1. In the SR Software Updates frame (see Fig. 2:2-18), two buttons are available for the LA/Beta software update: README and Apply Now.

   Click **Apply Now** to open the Software Update Installation Key pop-up box:



Software Update Installation Key

An installation key is required in order to install this software update.

Enter the installation key:

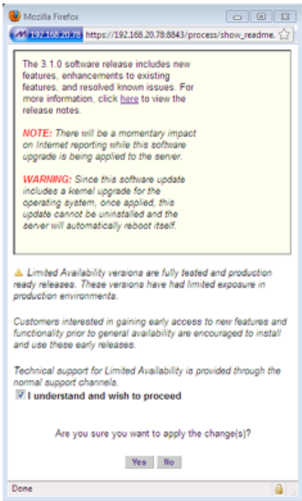
If you do not have an installation key, click here.

Fig. 2:2-23 Software Update Installation Key box

2. If you have an installation key for receiving LA or Beta software updates, go to the **Enter the installation key** field and type in that key.

NOTE*: If you do not have an installation key, click the link "****click here****" to go to the M86 Security Web site where you will need to log in and request an installation key.*

3. Click **Enter** to launch the applicable dialog box for accepting the software update type (see Fig. 2:2-24 for LA and Fig. 2:2-25 for Beta):



The 3.1.0 software release includes new features, enhancements to existing features, and resolved known issues. For more information, click here to view the release notes.

NOTE: There will be a momentary impact on Internet reporting while this software upgrade is being applied to the server.

WARNING: Since this software update includes a kernel upgrade for the operating system, once applied, this update cannot be uninstalled and the server will automatically reboot itself.

Limited Availability versions are fully tested and production ready releases. These versions have had limited exposure in production environments.

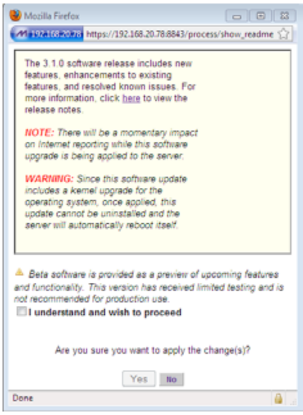
Customers interested in gaining early access to new features and functionality prior to general availability are encouraged to install and use these early releases.

Technical support for Limited Availability is provided through the normal support channels.

☑ **I understand and wish to proceed**

Are you sure you want to apply the change(s)?

Fig. 2:2-24 LA software acceptance box



The 3.1.0 software release includes new features, enhancements to existing features, and resolved known issues. For more information, click here to view the release notes.

NOTE: There will be a momentary impact on Internet reporting while this software upgrade is being applied to the server.

WARNING: Since this software update includes a kernel upgrade for the operating system, once applied, this update cannot be uninstalled and the server will automatically reboot itself.

Beta software is provided as a preview of upcoming features and functionality. This version has received limited testing and is not recommended for production use.

□ **I understand and wish to proceed**

Are you sure you want to apply the change(s)?

Fig. 2:2-25 Beta software acceptance box

4. Read the description for the software type to be installed (LA or Beta), and then click the checkbox corresponding to “I understand and wish to proceed”.
5. Click **Yes** to close the software acceptance dialog box and to open the End User License Agreement dialog (see Fig. 2:2-21).

6. Once you have read the contents of the End User License Agreement, click **Yes** if you agree to its terms. This action closes the EULA dialog box and begins the software update application process, launching a pop-up box showing the progress of the software installation.

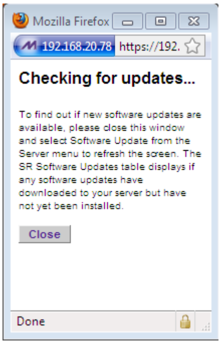
   A successful software installation displays a completion message with notification that the Software Update screen needs to be refreshed via **Server > Software Update** in order to display the latest software update in the SR Software Update History frame.

Uninstall the Most Recently Applied Update

In the SR Software Update History frame, the most recently applied software update can be unapplied by clicking **Undo**. This action removes the software update from the server.

Download Available Updates

1. Click **Download Available Updates** beneath the SR Software Update History frame to check for the latest software updates, and to launch a pop-up box explaining that any new software downloads will display in the SR Software Updates frame by refreshing the current screen:



Checking for updates...

To find out if new software updates are available, please close this window and select Software Update from the Server menu to refresh the screen. The SR Software Updates table displays if any software updates have downloaded to your server but have not yet been installed.

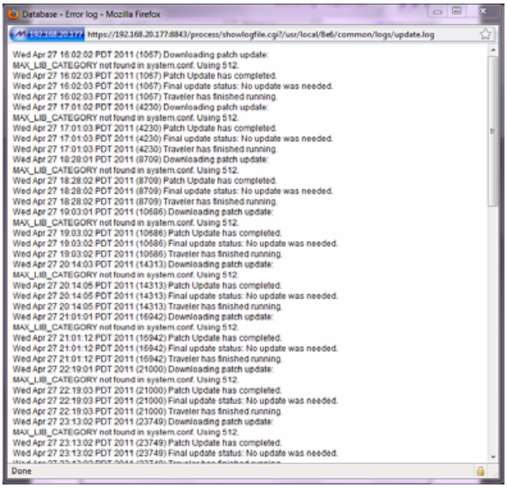
Fig. 2:2-26 Download Updates box

2. Click **Close** to close the pop-up box.

3. Refresh the screen by going to the Server menu and re-selecting Software Updates to see if there are new available software updates in the SR Software Updates frame.

View Software Download Log

1. To determine whether software updates are being downloaded to the SR, click the Software Download Log link named "**here**" to open the pop-up window that shows criteria on the latest software download attempts:


Database - Error log - Mozilla Firefox
192.168.20.177 https://192.168.20.177:8843/process/showlogfile.cgi?/usr/local/8e6/common/logs/update.log
Done

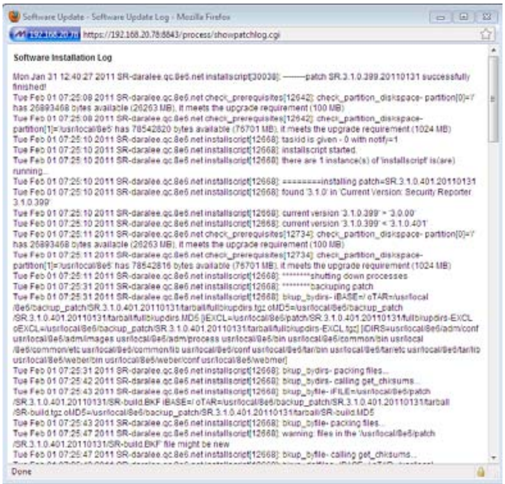
```
Wed Apr 27 16:02:02 PDT 2011 (1067) Downloading patch update:
MAX_LIB_CATEGORY not found in system.conf. Using 512.
Wed Apr 27 16:02:03 PDT 2011 (1067) Patch Update has completed.
Wed Apr 27 16:02:03 PDT 2011 (1067) Final update status: No update was needed.
Wed Apr 27 16:02:03 PDT 2011 (1067) Traveler has finished running.
Wed Apr 27 17:01:02 PDT 2011 (4230) Downloading patch update:
MAX_LIB_CATEGORY not found in system.conf. Using 512.
Wed Apr 27 17:01:03 PDT 2011 (4230) Patch Update has completed.
Wed Apr 27 17:01:03 PDT 2011 (4230) Final update status: No update was needed.
Wed Apr 27 17:01:03 PDT 2011 (4230) Traveler has finished running.
Wed Apr 27 18:28:01 PDT 2011 (8709) Downloading patch update:
MAX_LIB_CATEGORY not found in system.conf. Using 512.
Wed Apr 27 18:28:02 PDT 2011 (8709) Patch Update has completed.
Wed Apr 27 18:28:02 PDT 2011 (8709) Final update status: No update was needed.
Wed Apr 27 18:28:02 PDT 2011 (8709) Traveler has finished running.
Wed Apr 27 19:03:01 PDT 2011 (10686) Downloading patch update:
MAX_LIB_CATEGORY not found in system.conf. Using 512.
Wed Apr 27 19:03:02 PDT 2011 (10686) Patch Update has completed.
Wed Apr 27 19:03:02 PDT 2011 (10686) Final update status: No update was needed.
Wed Apr 27 19:03:02 PDT 2011 (10686) Traveler has finished running.
Wed Apr 27 20:14:03 PDT 2011 (14313) Downloading patch update:
MAX_LIB_CATEGORY not found in system.conf. Using 512.
Wed Apr 27 20:14:05 PDT 2011 (14313) Patch Update has completed.
Wed Apr 27 20:14:05 PDT 2011 (14313) Final update status: No update was needed.
Wed Apr 27 20:14:05 PDT 2011 (14313) Traveler has finished running.
Wed Apr 27 21:01:01 PDT 2011 (16942) Downloading patch update:
MAX_LIB_CATEGORY not found in system.conf. Using 512.
Wed Apr 27 21:01:12 PDT 2011 (16942) Patch Update has completed.
Wed Apr 27 21:01:12 PDT 2011 (16942) Final update status: No update was needed.
Wed Apr 27 21:01:12 PDT 2011 (16942) Traveler has finished running.
Wed Apr 27 22:19:01 PDT 2011 (21000) Downloading patch update:
MAX_LIB_CATEGORY not found in system.conf. Using 512.
Wed Apr 27 22:19:03 PDT 2011 (21000) Patch Update has completed.
Wed Apr 27 22:19:03 PDT 2011 (21000) Final update status: No update was needed.
Wed Apr 27 22:19:03 PDT 2011 (21000) Traveler has finished running.
Wed Apr 27 23:13:02 PDT 2011 (23749) Downloading patch update:
MAX_LIB_CATEGORY not found in system.conf. Using 512.
Wed Apr 27 23:13:02 PDT 2011 (23749) Patch Update has completed.
Wed Apr 27 23:13:02 PDT 2011 (23749) Final update status: No update was needed.
```

Fig. 2:2-27 Software Update Log window

2. Click **Close** to close the pop-up window.

View Software Installation Log

1. To determine whether the latest software update has been successfully applied to this SR, click the Software Installation Log link named "**here**" to open the Software Installation Log pop-up window that shows information about the latest software installation procedures performed on the SR:


Software Update - Software Update Log - Mozilla Firefox
192.168.20.78 https://192.168.20.78:8843/process/showpatchlog.cgi
Done

Software Installation Log

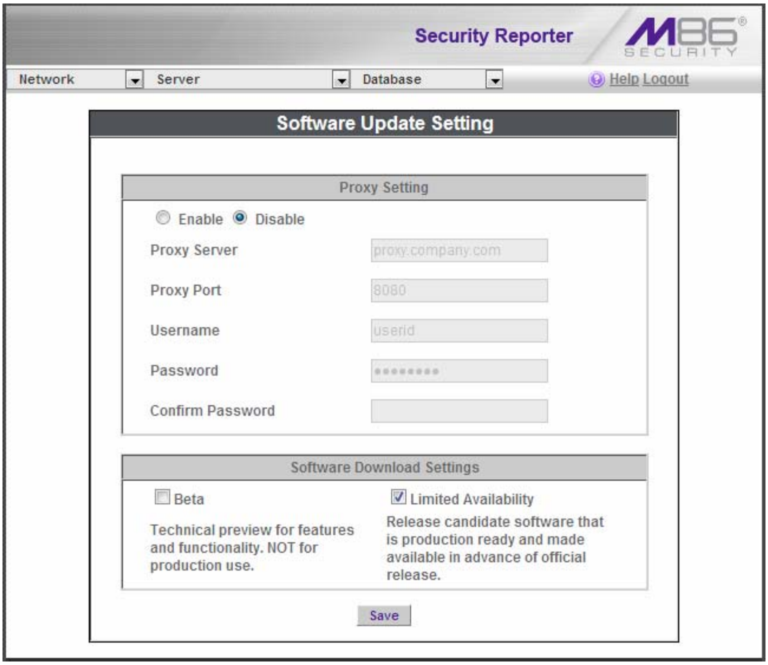
```
Mon Jan 31 12:40:27 2011 SR-daralee.qc.8e6.net installscript[30038]: ———patch SR.3.1.0.399.20110131 successfully
finished!
Tue Feb 01 07:25:08 2011 SR-daralee.qc.8e6.net check_prerequisites[12642]: check_partition_diskspace- partition[0]='/'
has 26893468 bytes available (26263 MB). It meets the upgrade requirement (100 MB)
Tue Feb 01 07:25:08 2011 SR-daralee.qc.8e6.net check_prerequisites[12642]: check_partition_diskspace-
partition[1]='/usr/local/8e6' has 78542820 bytes available (76701 MB). It meets the upgrade requirement (1024 MB)
Tue Feb 01 07:25:10 2011 SR-daralee.qc.8e6.net installscript[12668]: taskid is given - 0 with notify=1
Tue Feb 01 07:25:10 2011 SR-daralee.qc.8e6.net installscript[12668]: installscript started.
Tue Feb 01 07:25:10 2011 SR-daralee.qc.8e6.net installscript[12668]: there are 1 instance(s) of 'installscript' is(are)
running...
Tue Feb 01 07:25:10 2011 SR-daralee.qc.8e6.net installscript[12668]: ========installing patch=SR.3.1.0.401.20110131
Tue Feb 01 07:25:10 2011 SR-daralee.qc.8e6.net installscript[12668]: found '3.1.0' in 'Current Version: Security Reporter
3.1.0.399'
Tue Feb 01 07:25:10 2011 SR-daralee.qc.8e6.net installscript[12668]: current version '3.1.0.399' > '3.0.00'
Tue Feb 01 07:25:10 2011 SR-daralee.qc.8e6.net installscript[12668]: current version '3.1.0.399' < '3.1.0.401'
Tue Feb 01 07:25:11 2011 SR-daralee.qc.8e6.net check_prerequisites[12734]: check_partition_diskspace- partition[0]='/'
has 26893468 bytes available (26263 MB). It meets the upgrade requirement (100 MB)
Tue Feb 01 07:25:11 2011 SR-daralee.qc.8e6.net check_prerequisites[12734]: check_partition_diskspace-
partition[1]='/usr/local/8e6' has 78542816 bytes available (76701 MB). It meets the upgrade requirement (1024 MB)
Tue Feb 01 07:25:11 2011 SR-daralee.qc.8e6.net installscript[12668]: ********shutting down processes
Tue Feb 01 07:25:31 2011 SR-daralee.qc.8e6.net installscript[12668]: ********backuping patch
Tue Feb 01 07:25:31 2011 SR-daralee.qc.8e6.net installscript[12668]: bkup_bydirs- iBASE=/ oTAR=/usr/local
/8e6/backup_patch/SR.3.1.0.401.20110131/tarball/fullbkupdirs.tgz oMD5=/usr/local/8e6/backup_patch
/SR.3.1.0.401.20110131/tarball/fullbkupdirs.MD5 [iEXCL=/usr/local/8e6/patch/SR.3.1.0.401.20110131/fullbkupdirs-EXCL
oEXCL=/usr/local/8e6/backup_patch/SR.3.1.0.401.20110131/tarball/fullbkupdirs-EXCL.tgz] [iDIRS=usr/local/8e6/adm/conf
usr/local/8e6/adm/images usr/local/8e6/adm/process usr/local/8e6/bin usr/local/8e6/common/bin usr/local
/8e6/common/etc usr/local/8e6/common/lib usr/local/8e6/conf usr/local/8e6/tar/bin usr/local/8e6/tar/etc usr/local/8e6/tar/lib
usr/local/8e6/weber/bin usr/local/8e6/weber/conf usr/local/8e6/webmer]
Tue Feb 01 07:25:31 2011 SR-daralee.qc.8e6.net installscript[12668]: bkup_bydirs- packing files...
Tue Feb 01 07:25:42 2011 SR-daralee.qc.8e6.net installscript[12668]: bkup_bydirs- calling get_chksums...
Tue Feb 01 07:25:43 2011 SR-daralee.qc.8e6.net installscript[12668]: bkup_byfile- iFILE=/usr/local/8e6/patch
/SR.3.1.0.401.20110131/SR-build.BKF iBASE=/ oTAR=/usr/local/8e6/backup_patch/SR.3.1.0.401.20110131/tarball
/SR-build.tgz oMD5=/usr/local/8e6/backup_patch/SR.3.1.0.401.20110131/tarball/SR-build.MD5
Tue Feb 01 07:25:43 2011 SR-daralee.qc.8e6.net installscript[12668]: bkup_byfile- packing files...
Tue Feb 01 07:25:47 2011 SR-daralee.qc.8e6.net installscript[12668]: warning: files in the '/usr/local/8e6/patch
/SR.3.1.0.401.20110131/SR-build.BKF' file might be new
Tue Feb 01 07:25:47 2011 SR-daralee.qc.8e6.net installscript[12668]: bkup_byfile- calling get_chksums...
```

Fig. 2:2-28 Software Installation Log window

2. After viewing the contents of this window, click **Close** to close this window.

Software Update Setting screen

The Software Update Setting screen displays when the Software Update Setting option is selected from the Server menu. This screen is used for configuring the SR to receive software updates.



Software Update Setting

Proxy Setting

○ Enable ● Disable

Proxy Server	proxy.company.com
Proxy Port	8080
Username	userid
Password	••••••••
Confirm Password	

Software Download Settings

□ Beta

Technical preview for features and functionality. NOT for production use.

☑ Limited Availability

Release candidate software that is production ready and made available in advance of official release.

Fig. 2:2-29 Software Update Setting screen

Specify Proxy Settings

1. In the Proxy Setting frame, by default “Disable” is selected. Click “Enable” if the server is in a proxy server environment.
2. In the **Proxy Server** field, enter the host name of the proxy server.
3. In the **Proxy Port** field, enter the port number of the proxy server.
4. In the **Username** field, enter the username for the proxy account.
5. Enter the same password in the **Password** and **Confirm Password** fields.

TIP*: When you are finished making edits to this screen, click* ***Save*** *to save your settings.*

Download LA, Beta Software Updates

The Software Download Settings frame is used for specifying whether or not this SR will receive Limited Availability (LA) and/or Beta software updates that provide previews of software features currently being tested prior to the General Availability software release.

Enable LA Software Downloads

By default, the “Limited Availability” checkbox is enabled, indicating this SR will receive software updates recommended for use in a production environment only. With this feature enabled, the latest LA software update will automatically download and be available via the SR Software Updates table in the Software Update screen.

If this SR does not have the “Limited Availability” checkbox enabled, click the “Limited Availability” checkbox.

Enable Beta Software Downloads

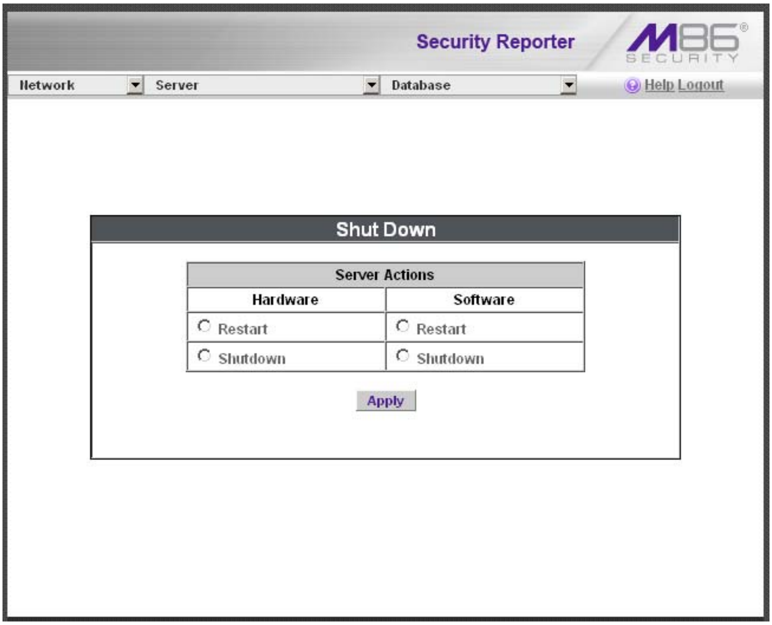
Click the “Beta” checkbox to enable this SR to receive Beta software updates on an SR used in a non-production environment.

Save Settings

Click **Save** to save your settings.

Shut Down screen

The Shut Down screen displays when the Shut Down option is selected from the Server menu. This screen is used to restart or shut down the server's software or hardware.



Server Actions	
Hardware	Software
○ Restart	○ Restart
○ Shutdown	○ Shutdown

Fig. 2:2-30 Shut Down screen

Server Action Selections

- **Restart the Server's Hardware -** The Restart Hardware option should be selected if the server needs to be rebooted—for example, when applying certain hardware configurations. You will need to use this option if the box mode has been changed or after an IP address has been entered in the Network Settings screen. During the Hardware Restart process, files normally FTPed to the server are routed to a problem directory in the logging device.

  When the server is running again, these files are FTPed to the server.

- **Shut Down the Server’s Hardware** - The Shutdown Hardware option should only be selected if the server’s hardware must be completely shut down—for example, if the server will be physically relocated. When this option is selected, the server shuts off, and files normally FTPed to the server will be routed to a problem directory in the logging device. When the server is rebooted, these files will be FTPed to the server.
- **Restart the Server’s Software** - The Restart Software option should be selected if daemons fail to run and/or the database needs to be started again. When this option is selected, the MySQL database is rebooted.
- **Shut Down the Server’s Software** - The Shutdown Software option should be selected if the MySQL database needs to be shut off and no files FTPed to the server.

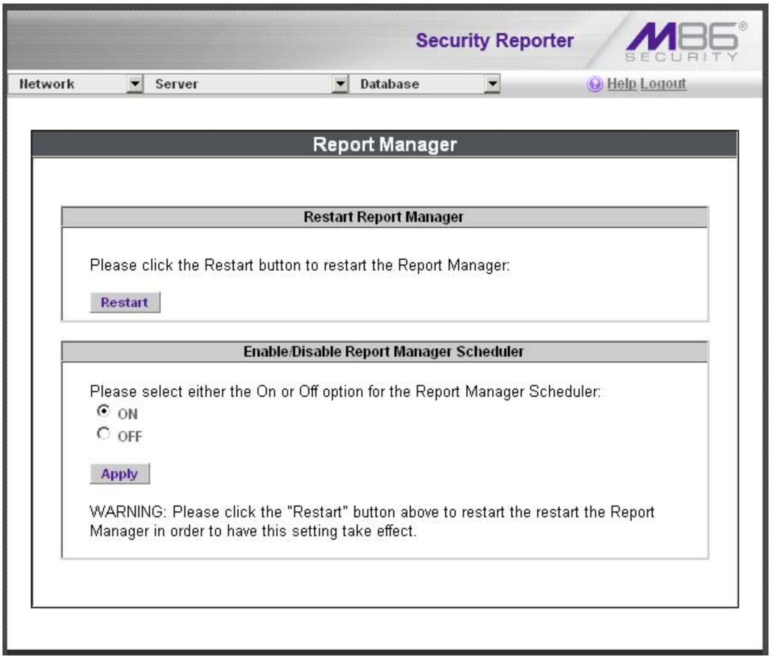
Perform a Server Action

1. Click the radio button corresponding to the Server Action you wish to execute.
2. Click the **Apply** button to display the warning screen.
3. To proceed with your selection, click the **RESTART** or **SHUTDOWN** button on the warning screen. To change your selection, select the Shutdown from the Server menu again to return to the Shut Down screen.

***NOTE**: When the Restart Software option is selected, the server will take five to 10 minutes to reboot. After this time, you can go to another screen or log off.*

Report Manager screen

The Report Manager screen displays when the Report Manager option is selected from the Server menu. This screen is used for enabling specified features on the reporting side of the application.



Please click the Restart button to restart the Report Manager:

Please select either the On or Off option for the Report Manager Scheduler:

● ON
○ OFF

WARNING: Please click the "Restart" button above to restart the restart the Report Manager in order to have this setting take effect.

Fig. 2:2-31 Report Manager screen

Restart the Report Manager

1. In the Restart Report Manager frame, click **Restart** to restart the Report Manager application.

   As a result of this action, a screen displays with the following message: “The Report Manager will restart in a few minutes.”

2. Click **OK** to return to the Report Manager screen.

Enable/Disable the Report Manager Scheduler

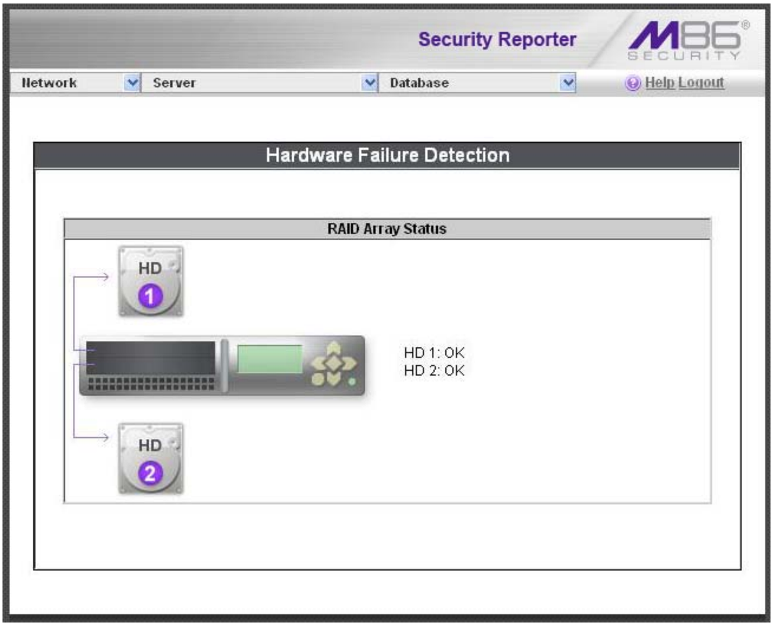
1. In the Enable/Disable Report Manager Scheduler frame, click the appropriate radio button to specify whether or not to automatically run scheduled reports:
   - "ON" - Choose this option to let the Report Manager automatically run scheduled reports.
   - "OFF" - Choose this option if you do not want the Report Manager to run scheduled reports.
2. Click **Apply**.
3. Click **Restart** to restart the Report Manager application.

Hardware Failure Detection screen

The Hardware Failure Detection screen displays when the Hardware Failure Detection option is selected from the Server menu. This screen is used for showing the status of each drive on the RAID server.

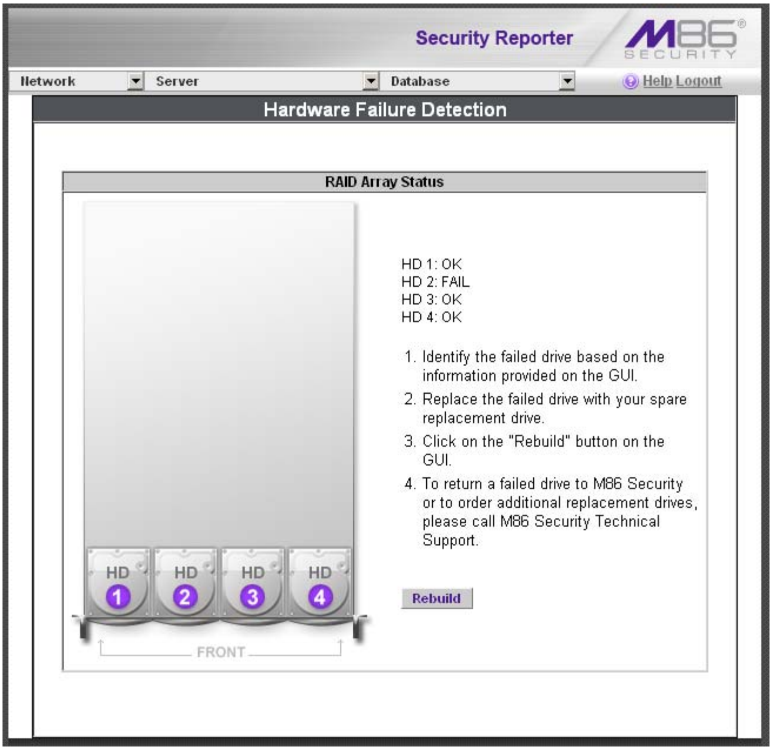
***NOTES**: This screen displays the image for the type of SR appliance used: 300 series Equus model with two hard drives (see Fig. 2:2-32); 500 and 700 series Equus model with four hard drives (see Fig. 2:2-33); or 700 series IBM model with an eight hard drive capacity, but using only four hard drives to run SR, with one spare hard drive in the event of a drive failure (see Fig. 2:2-34).*

If running the SR as a virtual machine, this screen displays the following message only: “Hardware Failure Detection is unavailable since this is not a RAID server.”



HD 1: OK
HD 2: OK

Fig. 2:2-32 Hardware Failure Detection screen, 300 model



Hardware Failure Detection

RAID Array Status

HD 1: OK
HD 2: FAIL
HD 3: OK
HD 4: OK

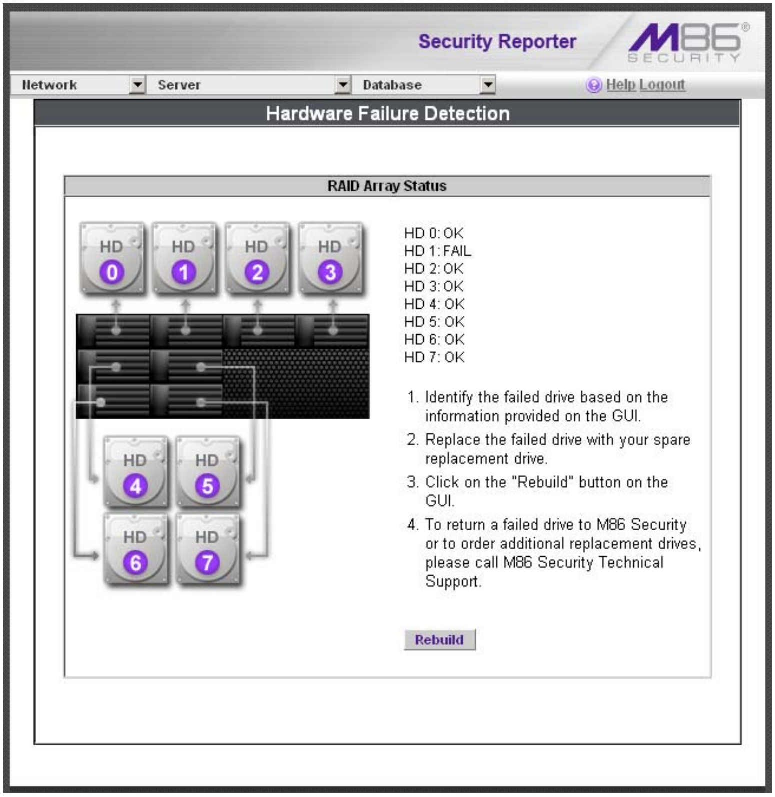
1. Identify the failed drive based on the information provided on the GUI.
2. Replace the failed drive with your spare replacement drive.
3. Click on the "Rebuild" button on the GUI.
4. To return a failed drive to M86 Security or to order additional replacement drives, please call M86 Security Technical Support.

Fig. 2:2-33 Hardware Failure Detection screen, 500, 700, 730 model

View the Status of the Hard Drives

The current RAID Array Status displays for all hard drives:

- HD 1 and HD 2 for 300 series Equus models
- HD 1 through HD 4 for 500 and 700 series Equus models
- HD 0 through HD 7 for 700 series IBM models (the diagram includes eight hard drives, even though the appliance only uses HD 0 through HD 3 for running SR, with HD 4 used as a backup drive in the event of a hard drive failure).



HD 0: OK
HD 1: FAIL
HD 2: OK
HD 3: OK
HD 4: OK
HD 5: OK
HD 6: OK
HD 7: OK

1. Identify the failed drive based on the information provided on the GUI.
2. Replace the failed drive with your spare replacement drive.
3. Click on the "Rebuild" button on the GUI.
4. To return a failed drive to M86 Security or to order additional replacement drives, please call M86 Security Technical Support.

Fig. 2:2-34 Hardware Failure Detection screen, 705 or 735 IBM model

If all hard drives are functioning without failure, the text “OK” displays for each corresponding drive number listed at the right of the screen, and no other text displays.

If any of the hard drives has failed, the message “FAIL” displays for the corresponding drive number listed at the right of the screen, and instructions for replacing the hard drive display below:

1. Identify the failed drive based on the information provided on the GUI.
2. Replace the failed drive with your spare replacement drive.

3. Click on the “Rebuild” button on the GUI.
4. To return a failed drive to M86 or to order additional replacement drives, please call M86 Technical Support.

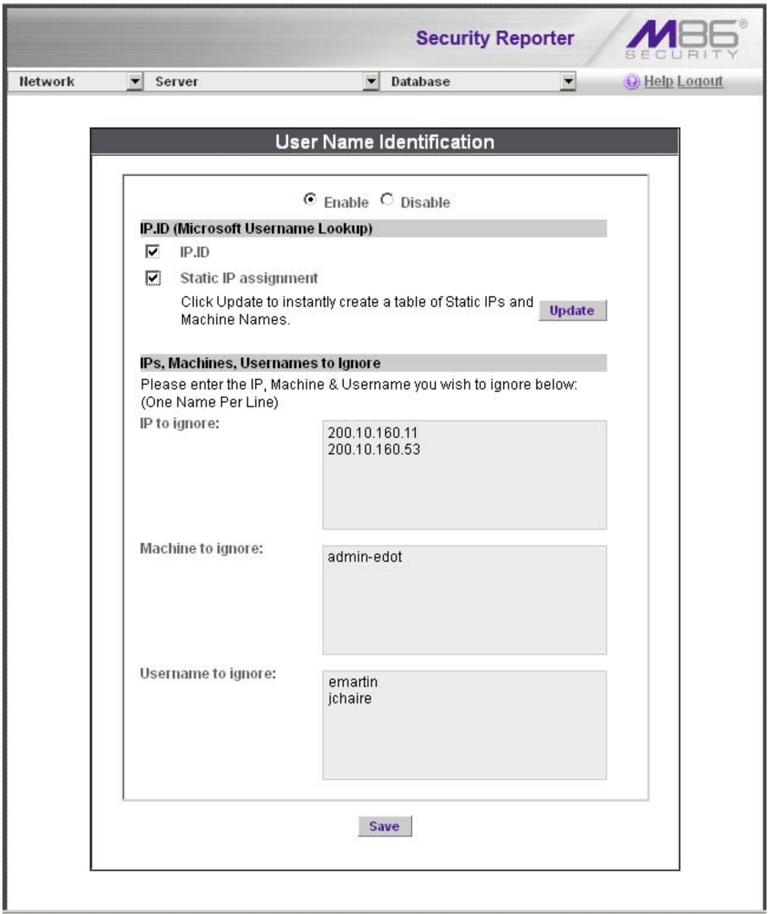
***NOTE**: For information on troubleshooting RAID, refer to Appendix B: RAID and Hardware Maintenance.*

Database Menu

The Database pull-down menu includes options for configuring the database. These options are: IP.ID (for Web Filter), Elapsed Time, Page Definition, Tools, Expiration, Optional Features, and User Group Import (for Web Filter).

User Name Identification screen

If using a Web Filter with this SR, the User Name Identification screen displays when the IP.ID option is selected from the Database menu. This screen is used for configuring the server to identify users based on the IP addresses of their machines, their usernames, and/or their machine names. Information set up on this screen is used by the Report Manager when logging a user’s Internet activity.



User Name Identification

● Enable ○ Disable

IP.ID (Microsoft Username Lookup)

☑ IP.ID

☑ Static IP assignment

Click Update to instantly create a table of Static IPs and Machine Names. Update

IPs, Machines, Usernames to Ignore

Please enter the IP, Machine & Username you wish to ignore below: (One Name Per Line)

IP to ignore:
200.10.160.11
200.10.160.53

Machine to ignore:
admin-edot

Username to ignore:
emartin
jchaire

Save

Fig. 2:2-35 User Name Identification screen with IP.ID activated

As the administrator of the server, you have the option to either enable or disable this feature for logging users' activities by usernames, machine names, and/or IP addresses of machines.

Warnings

⚠ *The SR will generate NetBIOS requests outside the network if IP.ID is activated **and** if no segment settings have been specified in the configuration of the Web access logging device—causing it to log external traffic. To resolve this issue, the Web access logging device should be modified to log activity only within the network. If a firewall is used, it should be set up to prevent logging NetBIOS requests outside the network.*

***NOTE**: Depending on the type of Web access logging device you are using, there may not be a configuration parameter for segment settings.*

⚠ *Be sure the time zone specified for the SR is the same for each Web access logging device the SR uses. Failure in executing this setup will cause inconsistencies when users' logging times are reported, especially if IP.ID is activated. If multiple Web access logging devices are used, be sure to identify the subnets assigned to each of these devices, as users cannot be tracked solely by IP address.*

⚠ *If using IP.ID, note that user login times are established for set periods of 15 minutes, and if more than one user logs onto the same machine during that time period, the activity on that machine will be identified with the first user who logged onto that machine. For example, the first user logs on a machine for three minutes and then logs off. The second user logs on the same machine for 11 minutes and then logs off. The first user logs back on that machine for 16 minutes. All 30 minutes are logged as the first user's activity.*

View the User Name Identification screen

If user name identification is enabled, specified IP.ID criteria displays, and IP, Machine, and Username frames will be populated if entries were previously made in them.

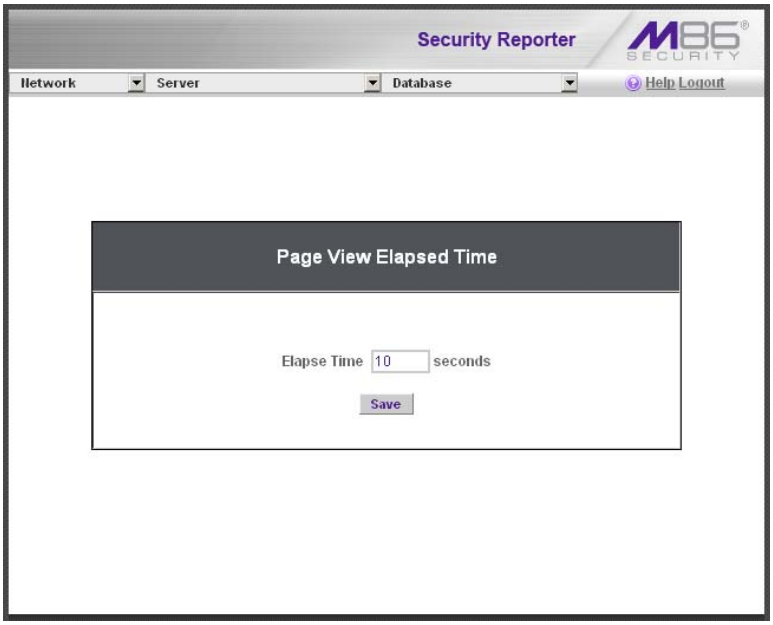
***NOTE**: If this feature is disabled, checkboxes in the IP.ID (Microsoft Username Lookup) section display greyed-out.*

Configure the Server to Log User Activity

1. In the area above the IP.ID (Microsoft Username Lookup) section of the screen, click the radio button corresponding to **Enable**. This action opens an alert box informing you that if usernames are enabled, these usernames will overwrite those that are being imported from the shadow log.
2. Click **OK** to close the alert box, and to activate the IP.ID and Static IP assignment checkboxes.
3. in the IP.ID (Microsoft Username Lookup) section of the screen, select one or both of the following options by clicking in the designated checkbox(es):
    - **IP.ID** - this option logs a user's activity by username (login ID).
    - **Static IP assignment** - this option logs a user's activity by the IP address of the machine used. When selecting this option, the Update button becomes activated.
        a. Click the **Update** button to automatically generate a table of static IP addresses and machine names. After this table is created, the message screen displays to confirm the successful execution of this task.
        b. Click the **Back** button to return to the User Name Identification screen.

Page View Elapsed Time screen

The Page View Elapsed Time screen displays when the Elapsed Time option is selected from the Database menu. This screen is used for establishing the value—amount of time—that will be used when tracking the length of a user's stay at a given Web site, and the number of times the user accesses that site.



Elapse Time 10 seconds

Fig. 2:2-36 Page View Elapsed Time screen

Establish the Unit of Elapsed Time for Page Views

1. In the **Elapse Time** field, enter the number of seconds that will be used as the value when tracking a user's visit to a Web site.

2. Click the **Save** button.

Elapsed Time Rules

Each time a user on the network accesses a Web site, this activity is logged as one or more visit(s) to that site. The amount of time a user spends on that site and the number of times he/she accesses that site is tracked according to the following rules:

- A user will be logged as having visited a Web site one time if the amount of time spent on any pages at that site is equivalent to the value entered at the Elapse Time field, or less than that value.

  For example, if the value entered at the Elapse Time field is 10 seconds, and if the user is at a site between one to 10 seconds—on the same page or on any other page within the same site—the user's activity will be tracked as one visit to that Web site.

- Each time the user exceeds the value entered at the Elapse Time field, the user will be tracked as having visited the site an additional time.

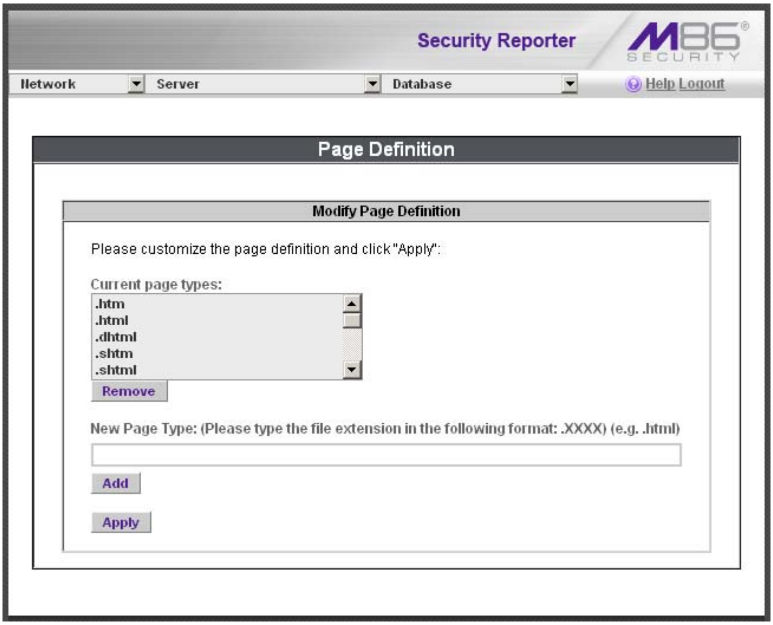
  For example, if the value entered at the Elapse Time field is 10 seconds and the user remains at a Web site for 12 seconds, two visits to that site will be logged for him/her.

- Each session at a Web site is tracked as one or more visit(s), depending on the duration of the session. A session is defined as a user's activity at a site that begins when the user accesses the site and ends when the user exits the site.

  For example, if the value entered at the Elapse Time field is 10 seconds and the user spends five seconds on a Web site, then exits, then returns to the same site for another 15 seconds, the user will have two sessions or three visits to that site logged for him/her (5 seconds = 1 visit, 15 seconds = 2 visits, for a total of 3 visits).

Page Definition screen

The Page Definition screen displays when the Page Definition option is selected from the Database menu. This screen is used for specifying the types of pages to be included in the detail report for Page searches.



Please customize the page definition and click "Apply":

Current page types:

.htm
.html
.dhtml
.shtm
.shtml

New Page Type: (Please type the file extension in the following format: .XXXX) (e.g. .html)

Fig. 2:2-37 Page Definition screen

View the Current Page Types

The Current page types list box contains the extensions of page types to be included in the detail report.

Remove a Page Type

To remove a page type from the detail report:

1. Select the page extension from the Current page types list box.
2. Click **Remove**.
3. Click **Apply**.

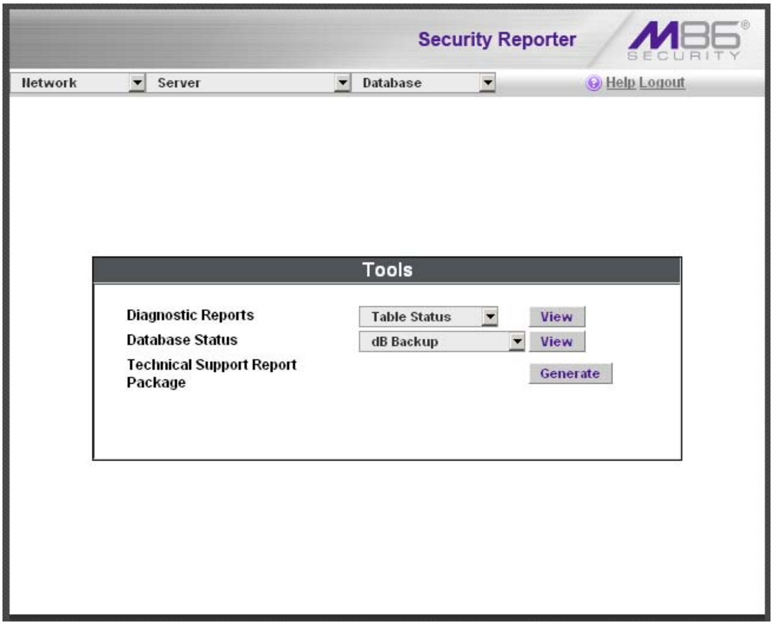
Add a Page Type

To add a page type in the detail report:

1. Enter the **New Page Type** extension.
2. Click **Add** to include the extension in the Current page types list box.
3. Click **Apply**.

Tools screen

The Tools screen displays when the Tools option is selected from the Database menu. This screen is used for viewing reports and logs to help you troubleshoot problems with the Report Manager application.



Diagnostic Reports: Table Status [View]
Database Status: dB Backup [View]
Technical Support Report Package [Generate]

Fig. 2:2-38 Tools screen

The following options are available on this screen:

- View Diagnostic Reports
- View Database Status Logs
- Technical Support Report Package

View Diagnostic Reports

1. Choose a report from the pull-down menu (Table Status, Process List, Full Process List, Tables, or Daily Summary).
2. Click the **View** button to view the selected diagnostic report in a pop-up window:
    - **Table Status** - This report contains a list of Client table names, and columns of statistics on each table, such as type, size, number of rows, and time created and updated.
    - **Process List** - This report shows a list of current SQL queries in the database, in an abbreviated format.
    - **Full Process List** - This report shows a list of current SQL queries in the database, in the full format that includes all columns of data.
    - **Tables** - This report contains a list of the names of tables currently in the database.
    - **Daily Summary** - This report shows the date range of summary tables currently in the database.
3. Click the “X” in the upper right corner of the pop-up window to close the window.

View Database Status Logs

1. Choose a database status log from the pull-down menu.
2. Click the **View** button to view the selected database status log in a pop-up window:
    - **db Active** (for Web Filter) - This log indicates when client tables were last updated with hits_objects and hits_pages.
    - **db Backup** - This log provides information about the MySQL backup/restore operation.

- **db Control** (for Web Filter) - This log shows a list of actions performed by the SR process when processing log files.
- **db Identify** (for Web Filter) - This log provides information about the server's action of obtaining user/ machine names from name log files and populating the database with these names.
- **db Logloader** (for Web Filter) - This log provides information about log file parsing and the number of valid and invalid records that are processed.
- **db Nbtlookup** (for Web Filter) - This log provides a list of user/machine IP addresses from the NetBIOS lookup.
- **db Split** (for Web Filter) - This log contains information pertaining to the formation of the hits_objects/ hits_pages tables.
- **db Staticip** (for Web Filter) - This log provides information about settings on the server for the static IP assignment option.
- **db Summary** - This log shows a summarization of activities from the dbsummary database tool.
- **db Support** (for Web Filter) - This log includes a list of temporary tables that were created for the formation of the hits tables.
- **db Tool** - This log shows information about system checks performed on disk usage, free memory, unprocessed files, and daemons.
- **db Traffic** - This log provides information about the daily traffic table.
- **Error Entry - Web Filter** (for Web Filter) - This log displays a list of Web Filter query errors.
- **File Watch Log** (for Web Filter) - This log shows a list of records that were imported from one machine to another.

- **MYSQL Log** - This log provides information pertaining to the MySQL server.
- **Partitioner Log** - This displays results of server partitioning for database expiration.
- **Software Installation Log** - This log gives information about the most recently applied software update.
- **Software Download Log** - This log gives information about recent software updates that have downloaded to this SR.
- **Vsimporter** (for SWG) - This log displays results of SWG archive log importation.

3. Click the “X” in the upper right corner of the pop-up window to close the window.

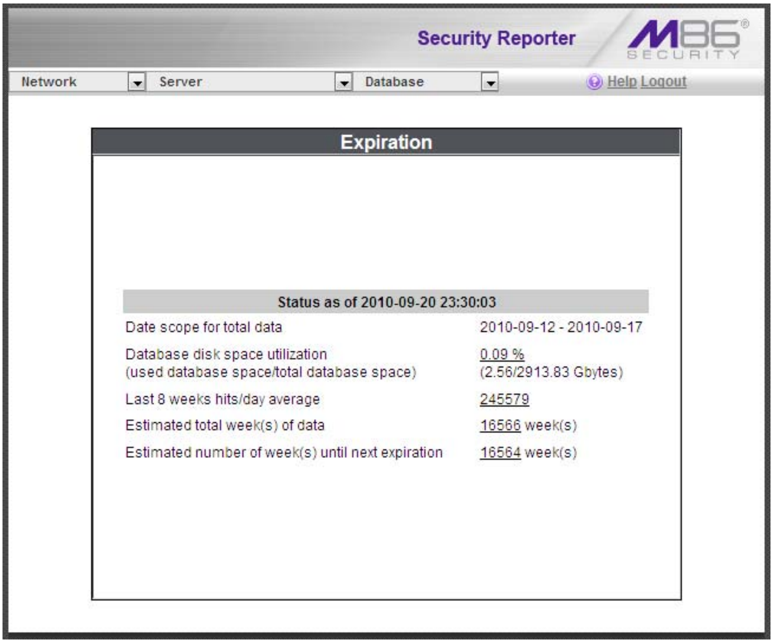
Generate Technical Support Report Package

When troubleshooting the SR unit with M86 Security Technical Support, a diagnostic report can be generated and submitted to M86 Security for further analysis. This report contains files with information about the ‘health’ of the unit.

1. At the **Techncal Support Report Package** field, click **Generate** to begin generating the report package.
2. After the package has generated, the “Successfully generated tech support log” pop-up window opens with the message: “Please download the file to email to M86 tech support.” Click **Download** to download the .tgz package to your machine.
3. Email the package to M86 Technical Support as instructed by your M86 technical support representative.

Expiration screen

The Expiration screen displays when the Expiration option is selected from the Database menu. This screen shows statistics on the amount of data currently stored on the SR, and provides an estimated date when that data will expire.



Status as of 2010-09-20 23:30:03

Date scope for total data	2010-09-12 - 2010-09-17
Database disk space utilization (used database space/total database space)	0.09 % (2.56/2913.83 Gbytes)
Last 8 weeks hits/day average	245579
Estimated total week(s) of data	16566 week(s)
Estimated number of week(s) until next expiration	16564 week(s)

Fig. 2:2-39 Expiration screen

***NOTES**: Though the database is backed up automatically each week, under certain circumstances you may need to perform a manual backup to the internal backup drive, and then save this data off site. (See the Server Menu: Backup screen section for information on establishing backup procedures, and backing up and restoring data on the SR.)*

See the Server Information panel in the Report Manager Administration Section for more information about expired data. See also Appendix C: Evaluation Mode for information about using the SR in the evaluation mode.

Expiration Rules

The server calculates the maximum number of weeks of data it can store, based on the storage capacity of the hard drive and the average number of end user hits per day within the last eight weeks.

Each night at 11:30 p.m., the server checks to see if it will soon be running out of storage capacity—by finding the week with the highest end user hit activity and assuming this may be the trend for future end user activity—then determines whether it will have enough storage space for the current week and the following week.

If the server anticipates it may run out of allocated data storage space by the next week, the oldest week’s data (Sunday through Saturday period) stored on the server is expired—i.e. deleted from the database.

Once data expires, it cannot be recovered.

⚠ ***WARNING**: Storage capacity maintenance is performed each evening between 11:30 p.m. and midnight. During this period, the database will be locked.*

View Data Storage Statistics

In the Status section of this screen, the date and time of the last database expiration check displays in the Status bar. The date displays in the YYYY-MM-DD format, and the time displays in military time (01-24 hours) using the HH:MM:SS time format.

***NOTE**: The Status date and time does not display if the server is newly installed or has been reset to factory default settings. (See Reset to Factory Defaults panel in Chapter 2 of the Report Manager Administration Section for information about resetting the server to factory default settings.)*

The following data that displays is current as of the most recent database expiration check:

- **Date scope for total data** - the first line in this field displays the range of weeks of data stored on the server, represented in the YYYY-MM-DD - YYYY-MM-DD format.

***NOTE**: If the server has not yet expired any data, the first date and time in the range is represented by “0” (zeroes).*

- **Database disk space utilization** - the percentage of space currently being used on the hard drive for data storage.
- **(used database space/total database space)** - the amount of space in Gigabytes currently being used on the hard drive for data storage, and the total amount of space in Gigabytes (Gbytes) on the hard drive allocated to database storage.
- **Last 8 weeks hits/day average** - the average number of end user hits per day, based on the last eight weeks of data stored on the server.

***NOTE**: If the server has not yet expired any data, a “0” (zero) displays in this field.*

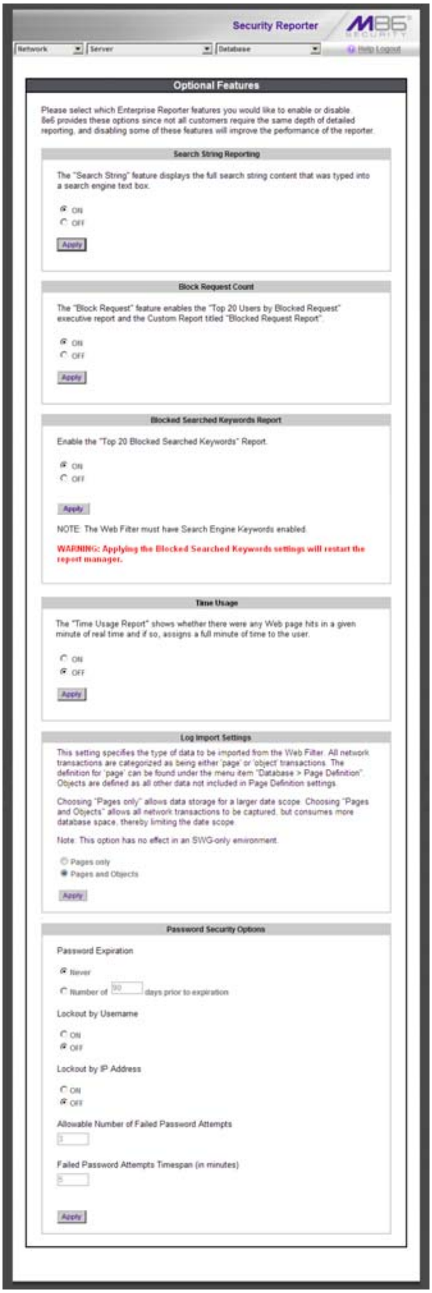
- **Estimated total week(s) of data** - the estimated number of weeks of data the server will store. This number is affected by end user hits/day and the storage capacity of the server.
- **Estimated number of week(s) until next expiration** - the estimated number of weeks from this week that data on the server will expire, based on the hits/day and storage capacity of the server.

***NOTE**: See Appendix C: Evaluation Mode for information about viewing the Expiration screen in the evaluation mode.*

Optional Features screen

The Optional Features screen displays when Optional Features is selected from the Database menu. This screen is used for specifying the following types of reports and report elements to be available in the Report Manager: Search String Reporting, Block Request Count, Blocked Searched Keywords, Time Usage, and Log Import Settings. This screen also is used for configuring password security rules to affect users who access the SR user interface (see Fig. 2-2:40).

***NOTE**: Optional features can be enabled or disabled at any time.*



Optional Features

Please select which Enterprise Reporter features you would like to enable or disable. 8e6 provides these options since not all customers require the same depth of detailed reporting, and disabling some of these features will improve the performance of the reporter.

Search String Reporting

The "Search String" feature displays the full search string content that was typed into a search engine text box.

● ON
○ OFF

Apply

Block Request Count

The "Block Request" feature enables the "Top 20 Users by Blocked Request" executive report and the Custom Report titled "Blocked Request Report".

● ON
○ OFF

Apply

Blocked Searched Keywords Report

Enable the "Top 20 Blocked Searched Keywords" Report.

● ON
○ OFF

Apply

NOTE: The Web Filter must have Search Engine Keywords enabled.

WARNING: Applying the Blocked Searched Keywords settings will restart the report manager.

Time Usage

The "Time Usage Report" shows whether there were any Web page hits in a given minute of real time and if so, assigns a full minute of time to the user.

○ ON
● OFF

Apply

Log Import Settings

This setting specifies the type of data to be imported from the Web Filter. All network transactions are categorized as being either 'page' or 'object' transactions. The definition for 'page' can be found under the menu item "Database > Page Definition". Objects are defined as all other data not included in Page Definition settings.

Choosing "Pages only" allows data storage for a larger date scope. Choosing "Pages and Objects" allows all network transactions to be captured, but consumes more database space, thereby limiting the date scope.

Note: This option has no effect in an SWG-only environment.

○ Pages only
● Pages and Objects

Apply

Password Security Options

Password Expiration

● Never
○ Number of 90 days prior to expiration

Lockout by Username

○ ON
● OFF

Lockout by IP Address

○ ON
● OFF

Allowable Number of Failed Password Attempts

3

Failed Password Attempts Timespan (in minutes)

5

Apply

Fig. 2:2-40 Optional Features screen

Enable Search String Reporting

If Search String Reporting is enabled, detail drill down reports display the full search string content typed into a search engine text box for search sites such as Google, Bing, Yahoo!, MSN, AOL, Ask.com, YouTube.com, and MySpace.com.

1. Click the radio button corresponding to “ON” to let search string entries display in drill down reports.
2. Click **Apply** to apply your setting.

Enable Block Request Count

If Block Request Count is enabled, the Top 20 Users by Blocked Requests Summary Report can be generated by the administrator.

1. Click the radio button corresponding to “ON” to make the Top 20 Users by Blocked Request report selection available in an administrator’s Summary Reports menu.
2. Click **Apply** to apply your setting.

***NOTE**: Since Summary Reports are processed each night, any changes made to settings today will not effective until the following day.*

Enable Blocked Searched Keywords

If Blocked Seached Keywords is enabled, the Top 20 Blocked Searched Keywords Summary Report can be generated by the administrator.

1. Click the radio button corresponding to “ON” to make the Top 20 Users by Blocked Request report selection available in an administrator’s Summary Reports menu.
2. Click **Apply** to apply your setting.

⚠ ***WARNING**: Applying this setting restarts the Report Manager.*

***NOTE**: Since Summary Reports are processed each night, any changes made to settings today will not effective until the following day.*

Enable Time Usage reports

If Time Usage Report is enabled, Time Usage reports can be generated by the administrator. These reports use the time usage algorithm to calculate the amount of time an end user spent accessing a given page or object—disregarding the number of seconds from each hit and counting each unique minute of Web time as one minute. Using this algorithm, an end user could never have more than 24 hours of Web time within a given 24-hour period.

1. Click the radio button corresponding to “ON” to make the Time Usage Report selection available in an administrator’s Custom Reports menu.
2. Click **Apply** to apply your setting.

***NOTE**: Since Time Usage reports are processed each night, any changes made to settings today will not effective until the following day.*

Enable Page and/or Object Count

If using a Web Filter, in the Log Import Settings frame, indicate whether drill down, Time Usage reports, and scheduled custom reports will include Web page hits only, or both Web page and object hits. Objects include images, graphics, multimedia items, and text item object files.

***WARNING**: If “Pages only” is selected, **all** records of objects accessed by end users will be lost for the time period in which this option was enabled. Even if there were objects accessed by end users during that time period, zeroes (“0”) will display for object activity in generated reports.*

1. Select one of two radio buttons to specify the type of hits to be included in drill down, Time Usage reports, and scheduled custom reports:

- "Pages only" - Choose this option to include *only* Web page hits in reports.
- "Pages and Objects" - Choose this option to include *both* Web page and object hits in reports.

2. Click **Apply** to apply your setting.

Enable, Configure Password Security Option

In the Password Security Options frame, passwords for accessing the SR user interface can be set to expire after a specified number of days, and/or lock out the user from accessing the SR after a specified number of failed password entry attempts within a defined interval of time.

***NOTE**: User accounts can be manually unlocked via System Configuration: Network > Lockouts > Locked-out Accounts and IPs (see Locked-out Accounts and IPs screen in this chapter).*

1. Enable any of the following options:
   - At the **Password Expiration** field, click the radio button corresponding to either password expiration option:
     - **Never** - Choose this option if passwords will be set to never expire.
     - **Number of 'x' days prior to expiration** - Choose this option if password will be set to expire after 'x' number of days (in which 'x' represents the number of days the password will be valid).

***NOTES**: The maximum number of days that can be entered is 365.*

If a user's password has expired, when he/she enters his/her Username and Password in the login screen and clicks Login, he/she will be prompted to re-enter his/her Username and enter a new password in the Password and Confirm Password fields.

- At the **Lockout by Username** field, click the radio button corresponding to either of the following options:
  - **ON** - Choose this option to lock out the user by username if the incorrect password is entered—for the number of times specified in the Allowable Number of Failed Password Attempts field—within the interval defined in the Failed Password Attempts Timespan (in minutes) field.
  - **OFF** - Choose this option if the user will not be locked out by username after entering the incorrect password.
- At the **Lockout by IP Address** field, click the radio button corresponding to either of the following options:
  - **ON** - Choose this option to lock out the user by IP address if the incorrect password is entered—for the number of times specified in the Allowable Number of Failed Password Attempts field—within the interval defined in the Failed Password Attempts Timespan (in minutes) field.
  - **OFF** - Choose this option if the user will not be locked out by IP address after entering the incorrect password.
- **Allowable Number of Failed Password Attempts** - With the Lockout by Username and/or Lockout by IP Address option(s) enabled, enter the number of times a user can enter an incorrect password during the interval defined in the Failed Password Attempts Timespan (in minutes) field before being locked out of the SR user interface.

***NOTE**: The maximum number of failed attempts that can be entered is 10.*

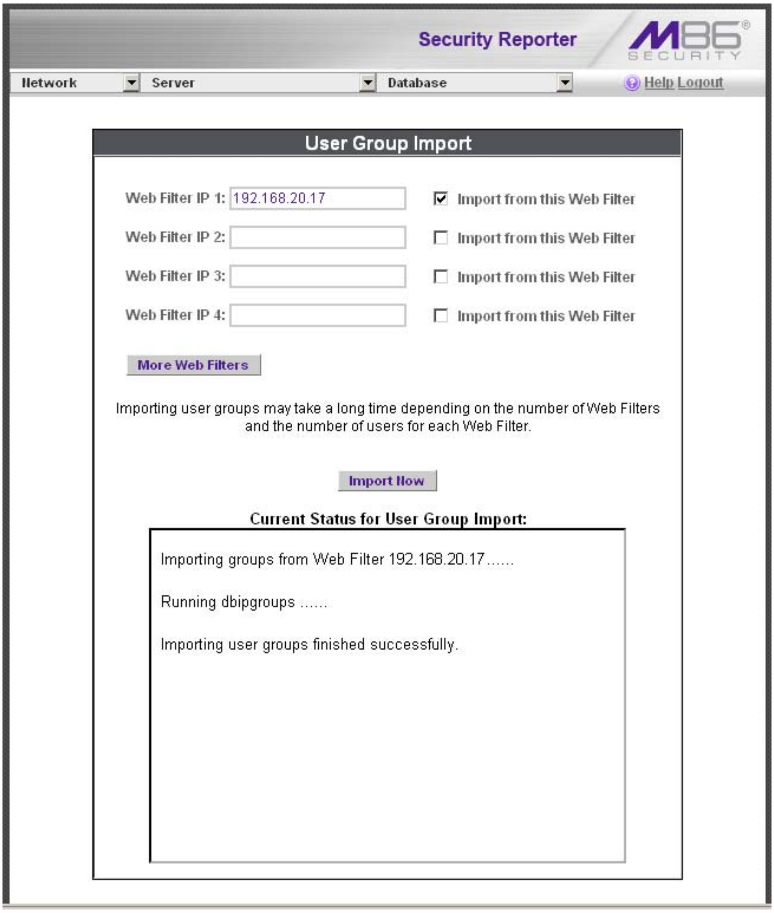
- **Failed Password Attempts Timespan (in minutes)** - With the Lockout by Username and/or Lockout by IP Address option(s) enabled, enter the number of minutes that defines the interval in which a user can enter an incorrect password—as specified in the Allowable Number of Failed Password Attempts field—before being locked out of the SR application.

***NOTE**: The maximum number of minutes that can be entered is 1440.*

2. Click **Apply** to apply your settings.

User Group Import screen

If using a Web Filter with this SR, the User Group Import screen displays when the User Group Import option is selected from the Database menu. This screen is used for specifying Web Filter servers to send LDAP user group membership information to this SR, for performing a user group import on demand, and for viewing on demand user group import criteria.



Web Filter IP 1: 192.168.20.17 ☑ Import from this Web Filter

Web Filter IP 2: ☐ Import from this Web Filter

Web Filter IP 3: ☐ Import from this Web Filter

Web Filter IP 4: ☐ Import from this Web Filter

Importing user groups may take a long time depending on the number of Web Filters and the number of users for each Web Filter.

Current Status for User Group Import:

```
Importing groups from Web Filter 192.168.20.17......

Running dbipgroups ......

Importing user groups finished successfully.
```

Fig. 2:2-41 User Group Import screen

Import User Groups

NOTE*: Web Filter IP fields are populated by default if one or more Web Filter servers are connected to this SR.*

1. Specify the **Web Filter IP** address of each Web Filter to send LDAP user group membership data to this SR.
2. Click the checkbox corresponding to “Import from this Web Filter”.

NOTE*: If additional Web Filter servers need to be specified, click* ***More Web Filters*** *to display the next four sets of entry fields.*

3. After specifying all Web Filter servers from which to import user group data, click **Import Now** to begin the data importation process. The status of this process displays in the Current Status for User Group Import box that opens at the bottom of this screen when the Import Now button is clicked.

NOTE*: User groups will be imported in the exact format defined on the Web Filter.*

REPORT MANAGER ADMINISTRATION SECTION

Introduction

This section of the user guide provides instructions to the global administrator on configuring and managing the administration portion of the Report Manager for use with a Web Filter and/or SWG appliance, and to the group administrator on using the SR application to manage end user Internet and network activity.

***NOTES**: If using a Web Filter, the Report Manager displays all menu selections: Reports, Gauges, Policy, Administration, Help, and Logout. If using an SWG, the Report Manager does not include the Gauges and Policy menu selections.*

Before configuring the Report Manager, the global administrator must fully configure the SR server via the System Configuration administrator console (as described in the previous section of this user guide), and the Structured Query Language (SQL) server must be installed on the network and connected to the Web access logging device(s).

The Report Manager’s Administration menu consists of the following options described in these chapters:

- Chapter 1: Group, Profile Management - This chapter explains how to set up user groups whose Internet activity will be monitored by group administrators; how to set up permissions so that an administrator in your group will only be able to access areas of the SR console that you specify; and how to set up a group administrator account.
- Chapter 2: Database Management - This chapter explains how to configure the server to use a secure network connection; view a list of user profiles (if using a Web Filter); view administrator activity; manage the

profiles of devices connected to the server; maintain Report Manager processes; analyze data storage on the server; and remove all profiles and configuration settings in the Report Manager.

- Chapter 3: Report Configuration - This chapter explains how to create and manage Custom Category Groups used for monitoring end user Internet activity, and configure general report settings.

Chapter 1: Group, Profile Management

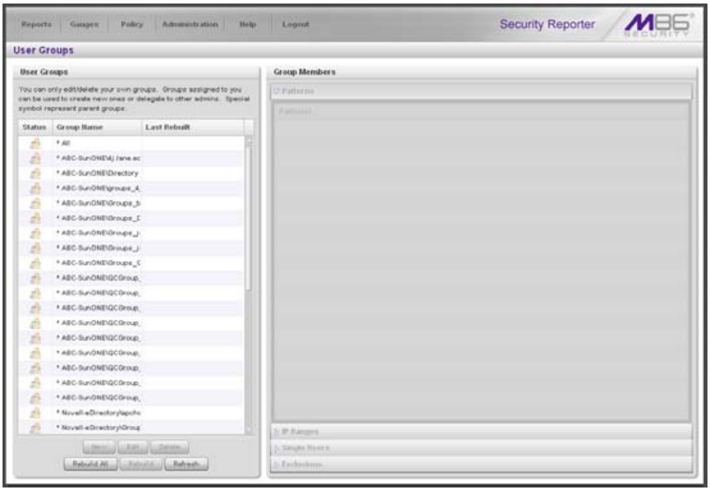
The following panels from the Administration menu of the Report Manager are described in this chapter: User Groups, Admin Groups, and Admin Profiles.

User Groups panel

On a new SR, the global administrator should first set up user groups—whose Internet activity will be monitored by group administrators.

A group administrator should set up user groups once he/she is given an account by the global administrator with permissions to access User Groups, as detailed in the next chapters in this section.

1. In the navigation toolbar, mouse over the Administration menu link to display topics available to you.
2. Click **User Groups** to display the User Groups panel, which is comprised of the User Groups frame to the left and its Group Members target frame to the right:



You can only edit/delete your own groups. Groups assigned to you can be used to create new ones or delegate to other admins. Special symbol represent parent groups.

Status	Group Name	Last Rebuilt
	* All	
	* ABC-SunONE\j.lane.ac	
	* ABC-SunONE\Directory	
	* ABC-SunONE\groups_A	
	* ABC-SunONE\Groups_b	
	* ABC-SunONE\Groups_E	
	* ABC-SunONE\Groups_j	
	* ABC-SunONE\Groups_j	
	* ABC-SunONE\Groups_C	
	* ABC-SunONE\GCGroup_	
	* ABC-SunONE\GCGroup_	
	* ABC-SunONE\GCGroup_	
	* ABC-SunONE\GCGroup_	
	* ABC-SunONE\GCGroup_	
	* ABC-SunONE\GCGroup_	
	* ABC-SunONE\GCGroup_	
	* ABC-SunONE\GCGroup_	
	* ABC-SunONE\GCGroup_	
	* Novell-eDirectory\apchs	
	* Novell-eDirectory\Group	

Fig. 3:1-1 User Groups panel

Names of user groups previously added by the administrator display in black text in the User Groups frame. Imported user groups display preceded by an up arrow. For the global administrator, “All” displays as the first record in the list by default.

NOTE*: A global administrator will see all user groups, and a group administrator will only see user groups assigned to him/her.*

From this panel you can view information about an existing user group, or click a button to add a user group, modify or delete an existing user group, rebuild a user group on demand, or refresh the display of the current list.

NOTES*: This version of SR will import user groups from a source Web Filter or SWG using IP group authentication or the following LDAP server types:*

- *Active Directory*
- *Novell eDirectory*
- *Sun One*
- *Open Directory*

If using a Web Filter:

- *Active Directory Mixed Mode and Active Directory Native Mode are supported.*
- *Open LDAP usernames will be included in user profiles only if those users generate network traffic.*

View User Group Information

For each group in the User Groups frame, the following information displays: Status icon, Group Name, and the date the user group was Last Rebuilt on demand (YYYY-MM-DD HH:SS)—if the latter is applicable.

***NOTE**: User groups are automatically rebuilt daily.*

User group status key

- The user groups icon indicates the group has been updated and is ready to be rebuilt.

- The lock icon indicates the user group is currently being rebuilt.

- The user groups icon with an exclamation point indicates the user group cannot be rebuilt on demand.

View a list of members in a user group

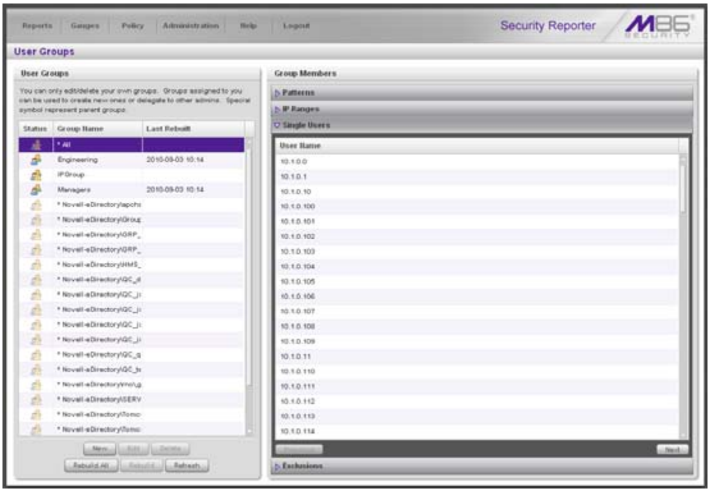
To view a list of members that belong to an existing user group:

1. Select the user group from the User Groups frame by clicking its Group Name to highlight that record. Based on this selection, the Group Members frame to the right becomes activated along with the following buttons in the section below, based on the status of the user group:
   - If the selected user group is ready to be rebuilt, this action activates all buttons (New, Edit, Delete, Rebuild, Rebuild All, Refresh).
   - If the selected user group was not imported and cannot be rebuilt on demand, this action activates the New, Edit, Delete, Rebuild All, and Refresh buttons.
   - If the selected user group was imported and cannot be rebuilt on demand, this action activates the New, Rebuild All, and Refresh buttons only.

***NOTE**: A user group name preceded by an asterisk (*) indicates that user group is a parent group.*

2. Click an accordion in the Group Members frame to open it and view pertinent information:

   - Patterns accordion - view patterns previously set up for that user group.
   - IP Ranges accordion - view Starting IP and Ending IP ranges previously added for that user group.
   - Single Users accordion - view a list of User Names and IP Addresses for individual users previously selected from the Available Users list for that user group.
   - Exclusions accordion - view a list of User Names and IP Addresses for individual users previously selected from the Available Users list to be excluded from that user group.



You can only edit/delete your own groups. Groups assigned to you can be used to create new ones or delegate to other admins. Special symbol represent parent groups.

Status	Group Name	Last Rebuilt
	* All	
	Engineering	2010-09-03 10:14
	IPGroup	
	Managers	2010-09-03 10:14
	* Novell-eDirectory\apchs	
	* Novell-eDirectory\Grou	
	* Novell-eDirectory\GRP_	
	* Novell-eDirectory\GRP_	
	* Novell-eDirectory\HMS_	
	* Novell-eDirectory\QC_d	
	* Novell-eDirectory\QC_ji	
	* Novell-eDirectory\QC_ji	
	* Novell-eDirectory\QC_ji	
	* Novell-eDirectory\QC_ji	
	* Novell-eDirectory\QC_g	
	* Novell-eDirectory\QC_ts	
	* Novell-eDirectory\mo\g	
	* Novell-eDirectory\SERV	
	* Novell-eDirectory\Tomc	
	* Novell-eDirectory\Tomc	

User Name
10.1.0.0
10.1.0.1
10.1.0.10
10.1.0.100
10.1.0.101
10.1.0.102
10.1.0.103
10.1.0.104
10.1.0.105
10.1.0.106
10.1.0.107
10.1.0.108
10.1.0.109
10.1.0.11
10.1.0.110
10.1.0.111
10.1.0.112
10.1.0.113
10.1.0.114

Fig. 3:1-2 View user group information, Single Users accordion

***NOTE**: If using the LDAP user authentication method, user names display in the User Name column. If using IP groups, IP addresses of user machines display instead of user names.*

Add a User Group

To add a new user group:

1. From the User Groups list, select an existing user group to be used as the base group for creating the new user group.
2. Click **New** to display the New User Group panel:

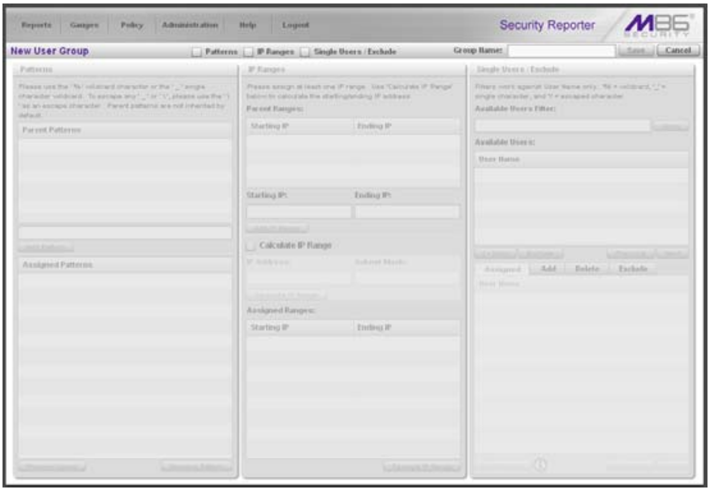


Fig. 3:1-3 New User Group panel

At the top of this panel are the Patterns, IP Ranges, Single Users/Exclude checkboxes, Group Name field, and Save and Cancel buttons. Greyed-out frames corresponding to the checkboxes display below. The only checkboxes that are activated are the ones pertinent to the selected user group.

3. Enter at least three characters for the **Group Name** to be used for the new user group; this action activates the Save button.
4. Click the checkbox(es) to activate the pertinent corresponding frame(s) below: **Patterns**, **IP Ranges**, **Single Users/Exclude**.

***TIP**: At any time before saving the new user group, if you need to cancel the entry of the new user group, click the Cancel button to return to the main User Groups panel.*

5. After making entries in the pertinent frames—as described in the following sub-sections—click **Save** to save your edits, and to redisplay the User Groups panel where the user group you added now displays in the User Groups frame.

Patterns frame

When creating a user group, the Patterns frame is used for adding one or more patterns in order to narrow the list of users to be included in the new group. A pattern consists of a wildcard, or a wildcard plus one or more alphanumeric characters.

Add a new pattern

To add a pattern to the new user group:

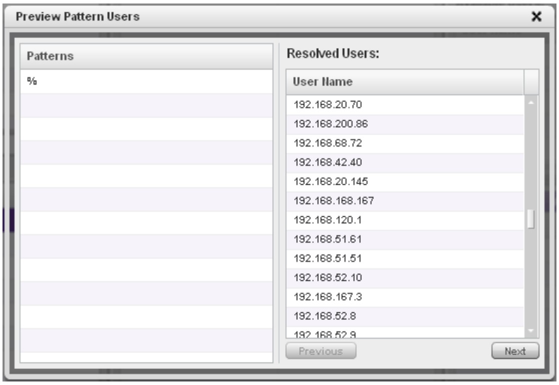
1. Do one of the following:
   - To add a pattern included in the base group, select the pattern from the Parent Patterns box to display that pattern in the field below.
   - To add a new pattern, enter the pattern in the field beneath the Parent Patterns box. For example: Enter *200.10.100.3%* to include all IP addresses with ”200.10.100.3” as part of the IP address.
2. Click **Add Pattern** to include the pattern in the Assigned Patterns list box below.

***TIP**: Follow steps 1 and 2 above to include additional patterns for the new user group.*

View users resolved by the pattern

To view a list of users resolved by the pattern you added:

1. Select the pattern from the Assigned Patterns list box.
2. Click **Preview Users** to open the Preview Pattern Users pop-up window that shows the Patterns frame to the left and the Resolved Users frame to the right:



Patterns
%

User Name
192.168.20.70
192.168.200.86
192.168.68.72
192.168.42.40
192.168.20.145
192.168.168.167
192.168.120.1
192.168.51.61
192.168.51.51
192.168.52.10
192.168.167.3
192.168.52.8
192.168.52.9

Fig. 3:1-4 Add user group Patterns, Preview Pattern Users

The Patterns frame displays the pattern you added to the Assigned Patterns list box. The Resolved Users frame includes a list of each user resolved by the pattern, including that user's User Name for LDAP authentication or IP address for IP group authentication.

3. Click the “X” in the upper right corner to close this pop-up window.

Remove a pattern

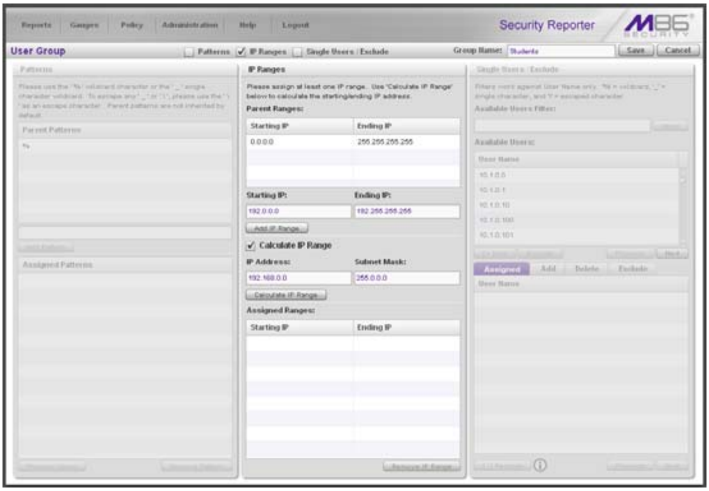
To remove a pattern in the Assigned Patterns list box:

1. In the Patterns frame, select the pattern from the Assigned Patterns list box to highlight it.
2. Click **Remove Pattern** to remove that pattern from the list box.

IP Ranges frame

When creating a user group, the IP Ranges frame is used for specifying IP ranges to be used by the new group. The top portion of this frame includes a box with Parent Ranges. Beneath this section are fields for entering a Starting IP and Ending IP range. Beneath those fields is a section in which you can Calculate an IP Range by entering a single IP Address and Subnet Mask. At the bottom of this frame is the Assigned Ranges list box that includes any IP ranges that have been added.

NOTE: *If using IP group authentication, parent ranges do not display in this frame unless an IP range was originally set up for this user group's parent user group. To set up the first parent user group to include an IP range, "All" user groups must be used as the base group.*



□ Patterns ☑ IP Ranges □ Single Users / Exclude

Group Name: Students

IP Ranges

Please assign at least one IP range. Use 'Calculate IP Range' below to calculate the starting/ending IP address.

Parent Ranges:

Starting IP	Ending IP
0.0.0.0	255.255.255.255

Starting IP: 192.0.0.0 Ending IP: 192.255.255.255

☑ Calculate IP Range

IP Address: 192.168.0.0 Subnet Mask: 255.0.0.0

Assigned Ranges:

Starting IP	Ending IP

Available Users:

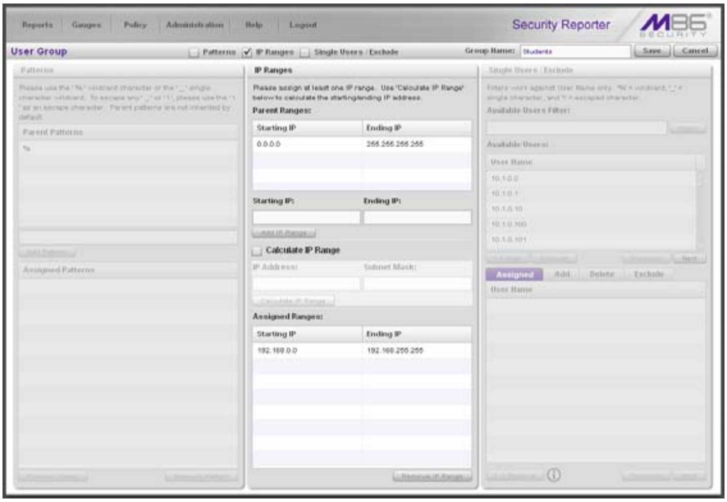
User Name
10.1.0.0
10.1.0.1
10.1.0.10
10.1.0.100
10.1.0.101

Fig. 3:1-5 Add user group, IP Ranges frame

Specify an IP range

To add an IP address range:

1. Do one of the following:
   - To make a selection from Parent Ranges, click the row in the Parent Ranges box to highlight and select that row, and also to add that Starting IP and Ending IP range in the Starting IP and Ending IP fields below. If necessary, edits can be made to these fields.
   - To add an IP address range without selecting from the Parent Ranges frame:
     a. Enter the **Starting IP** address.
     b. Enter the **Ending IP** address.
   - To calculate an IP address range:
     a. Click the **Calculate IP Range** checkbox to activate the IP Address and Subnet Mask fields below.
     b. Enter the **IP Address**.
     c. Enter the **Netmask** which activates the Calculate Range button.
     d. Click **Calculate IP Range** to display the Starting IP and Ending IP in the fields above.
2. Click **Add IP Range** to include that IP range in the Assigned Ranges list box below:



Group Name: Students

IP Ranges

Please assign at least one IP range. Use 'Calculate IP Range' below to calculate the starting/ending IP address.

Parent Ranges:

Starting IP	Ending IP
0.0.0.0	255.255.255.255

Starting IP: Ending IP:

□ Calculate IP Range

IP Address: Subnet Mask:

Assigned Ranges:

Starting IP	Ending IP
192.168.0.0	192.168.255.255

User Name
10.1.0.0
10.1.0.1
10.1.0.10
10.1.0.100
10.1.0.101

Fig. 3:1-6 Add user group, IP range added

Remove an IP address range

To remove an IP address range from the Assigned Ranges list box:

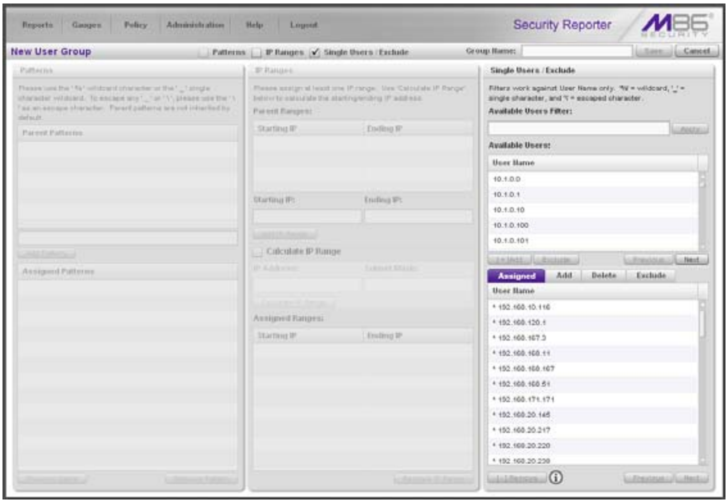
1. Click the row to highlight and select it; this action activates the Remove IP Range button below.
2. Click **Remove IP Range** to remove the IP address range from the list box.

Single Users/Exclude frame

When creating a user group, the Single Users/Exclude frame is used for adding one or more users to the group. This frame includes the Available Users Filter to be used with the Available Users box that is populated with individual users from the base user group. For each record in the list, the User Name or IP address displays. The list box below includes the target Assigned, Add, Delete, and Exclude tabs. The Add tab displays by default and the Assigned tab displays greyed-out until the user group is saved.

NOTES: *Only users previously selected from the base user group will be included in the Available Users list.*

*A user name preceded by an asterisk (*) indicates an auto-assigned user that can only be removed by adjusting the pattern or IP range for that user's group.*



Filters work against User Name only. '%' = wildcard, '_' = single character, and '\' = escaped character.

User Name
10.1.0.0
10.1.0.1
10.1.0.10
10.1.0.100
10.1.0.101

User Name
* 192.168.10.116
* 192.168.120.1
* 192.168.167.3
* 192.168.168.11
* 192.168.168.167
* 192.168.168.51
* 192.168.171.171
* 192.168.20.145
* 192.168.20.217
* 192.168.20.220
* 192.168.20.230

Fig. 3:1-7 Add user group, Single Users frame

Add one or more individual users

To add users to the Assigned Users list, make your selections from the Available Users list. If the Available Users list is long, you can reduce the number of results that display in this list by using the Available Users Filter.

Use the filter to narrow Available Users results

To use the **Available Users Filter**:

1. Enter filter terms to narrow the selection of Available Users. For example: Type in *150%* to only display results matching an IP address that begins with “150”.
2. Click **Apply** to display filtered results in the Available Users box.

Select users to add to the Assigned Users list

To make selections from the Available Users box:

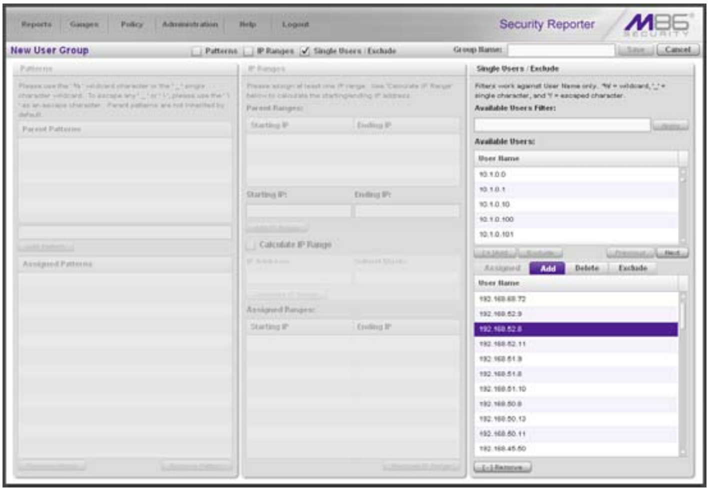
1. Select one or more IPs from the list to highlight the record(s).
2. Click **[+] Add** to include the selected user(s) in the Add tab.

***NOTE**: Users added to the Add tab will still be listed in the Available Users list. After saving the entries in the New User Group panel, the users added to the Add tab display in the Assigned tab.*

Remove users from the Add tab

To remove users from this user group:

1. Select the user(s) from the Add tab; this action activates the [-] Remove button:



Filters work against User Name only. '%' = wildcard, '_' = single character, and '\' = escaped character.

Available Users:

User Name
10.1.0.0
10.1.0.1
10.1.0.10
10.1.0.100
10.1.0.101

Add:

User Name
192.168.68.72
192.168.52.9
192.168.52.8
192.168.52.11
192.168.51.9
192.168.51.8
192.168.51.10
192.168.50.8
192.168.50.13
192.168.50.11
192.168.45.50

Fig. 3:1-8 Add user group, remove user from Add tab

2. Click **[-] Remove** to remove the user(s) from the Add tab.

Edit a User Group

***NOTE**: Global and group administrators can only edit user groups they have created, and cannot edit their base groups or imported user groups.*

To edit a user group:

1. From the main User Groups panel, select the user group from the list in the User Groups frame.
2. Click **Edit** to display the User Group panel showing activated frames—i.e. if the Patterns frame had settings made in it, that frame is activated; if the Single Users frame was the only frame with settings made in it, that frame is activated. Any frame without settings made in it displays greyed-out.
3. Make any of these edits:
    - To make entries in a frame that is not yet activated, click the available checkbox to activate that frame: **Patterns**, **IP Ranges**, **Single Users/Exclude**.
    - Make any of these edits in a frame:
        - Patterns frame - add or remove a pattern.
        - IP Ranges frame - add or remove an IP address range.
        - Single Users/Exclude frame - add or remove one or more users.

***NOTE**: When editing the Single Users/Exclude frame, users who are added display in the Add tab, and users who are removed display in the Delete tab.*

- If necessary, edit the name of the user group in the **Group Name** field.

4. Click **Save** to save your edits and to return to the User Groups panel.

Rebuild the User Group

After editing the user group, the user group profile should be rebuilt.

1. In the User Groups panel, select the user group to be rebuilt.
2. Click **Rebuild** to initiate the rebuild process for that user group.
3. After a few minutes, click the **Refresh** button to refresh the display in the panel. Note that the Last Rebuilt column for user group you rebuilt now displays the date and time of the rebuild.

Delete a User Group

***NOTES**: A user group can only be deleted by the administrator who added it. A base group cannot be deleted.*

To delete a user group:

1. In the User Groups panel, select the user group from the User Groups list.
2. Click **Delete** to open the Confirm dialog box with the message: "Are you sure you want to delete this user group?"

***WARNING**: If the user group to be deleted has been delegated to an administrator, that user group will be removed from that administrator’s User Groups list as well as your User Groups list.*

***TIP**: Click No to close the dialog box and to return to the User Groups panel.*

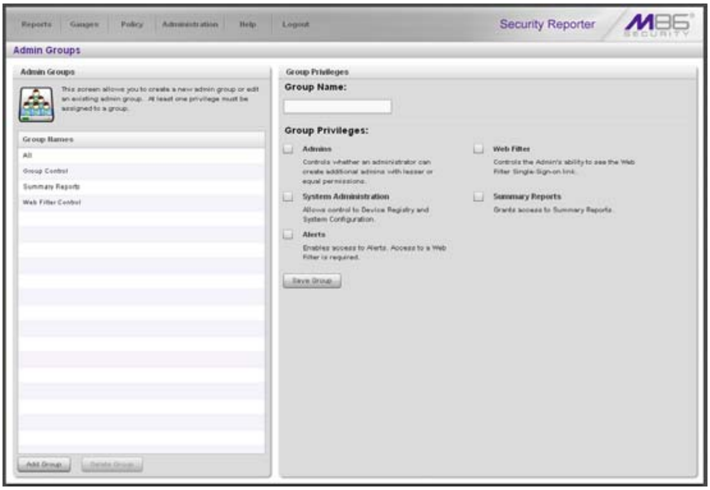
3. Click **Yes** to close the dialog box, and to remove the user group from the User Groups list.

Admin Groups panel

Once you have set up user groups, you are ready to create a set of management permissions (administrator group or admin group), so that a group administrator you set up will only be able to access areas of the SR console that you specify.

This function is available to a group administrator only if permissions were granted by the administrator who set up his/her account, as detailed in this chapter.

In the navigation toolbar, mouse over the Administration menu link and select **Admin Groups** to open the Admin Groups panel, comprised of the Admin Groups frame to the left and the Group Privileges frame to the right:



This screen allows you to create a new admin group or edit an existing admin group. At least one privilege must be assigned to a group.

Group Names
All
Group Control
Summary Reports
Web Filter Control

Group Name:

Group Privileges:

□ **Admins**
Controls whether an administrator can create additional admins with lesser or equal permissions.

□ **System Administration**
Allows control to Device Registry and System Configuration.

□ **Alerts**
Enables access to Alerts. Access to a Web Filter is required.

□ **Web Filter**
Controls the Admin's ability to see the Web Filter Single-Sign-on link.

□ **Summary Reports**
Grants access to Summary Reports.

Fig. 3:1-9 Admin Groups panel

***NOTES**: Any administrator groups previously set up display in the Group Names list box in the Admin Groups frame. If using an SWG, the Alerts and Web Filter options are greyed-out.*

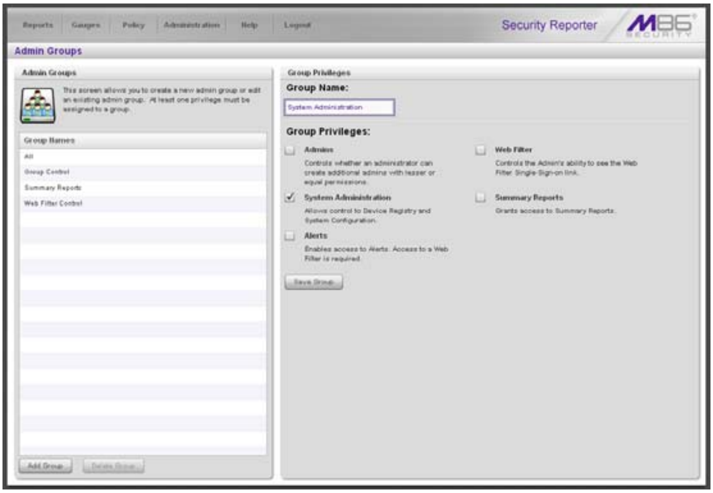
In this panel, you can add an administrator group, view information for an existing administrator group, and modify or delete that group, as necessary.

Add a Group

1. At the bottom of the Admin Groups frame, Click **Add Group**.
2. At the top of the Group Privileges frame, type in up to 32 characters for the **Group Name**.

***TIP**: You may want to name the group for the type of permissions to be assigned. This will distinguish the name from other names, such as those set up for user groups.*

3. In the Group Privileges section, click the appropriate checkbox(es) to specify the type of access the administrator group will be granted on the SR console or its related devices:



This screen allows you to create a new admin group or edit an existing admin group. At least one privilege must be assigned to a group.

All
Group Control
Summary Reports
Web Filter Control

Group Name: System Administration

Group Privileges:

□ Admins
Controls whether an administrator can create additional admins with lesser or equal permissions.

☑ System Administration
Allows control to Device Registry and System Configuration.

□ Alerts
Enables access to Alerts. Access to a Web Filter is required.

□ Web Filter
Controls the Admin's ability to see the Web Filter Single-Sign-on link.

□ Summary Reports
Grants access to Summary Reports.

Fig. 3:1-10 Add a new Group

- **Admins** - This privilege lets the administrator create another administrator account with equal or lesser privileges as that administrator.
- **System Administration** - This privilege gives the administrator access to the Device Registry and System Configuration administrator console.

- **Alerts** - This privilege for Web Filter users lets the administrator manage alerts that indicate if URL or bandwidth gauges (driven by end user Internet/ network activity) are close to—or have reached—their established upper thresholds.
- **Web Filter** - This privilege for Web Filter users gives the administrator access to the Web Filter via a link in the Administration menu.
- **Summary Reports** - This privilege lets the administrator access Summary Reports from the Report menu.

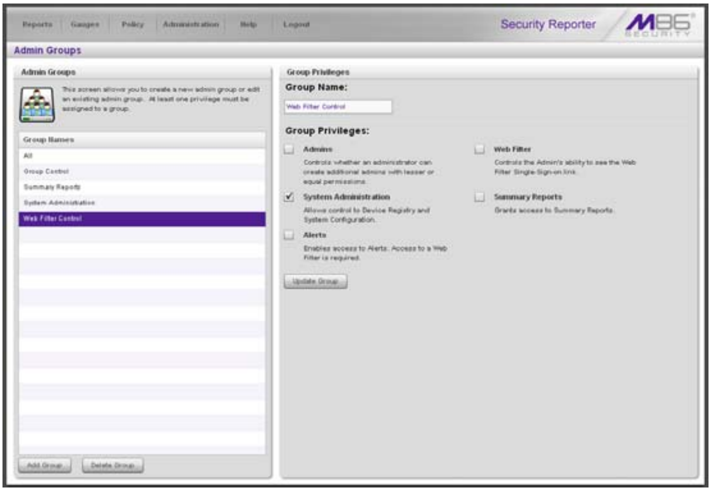
***TIP**: To remove a checkmark from any active checkbox containing a checkmark, click the checkbox.*

4. Click **Save Group** to save your entries and to add the new administrator group name in the Group Names list box.

View, Edit an Admin Group's Permissions

View Admin Group settings

In the Admin Groups frame, click the name of the administrator group to highlight the group name, activate all buttons, and to populate the Group Privileges frame with previously-saved settings:



This screen allows you to create a new admin group or edit an existing admin group. At least one privilege must be assigned to a group.

Group Name: Web Filter Control

Group Privileges:

□ Admins
Controls whether an administrator can create additional admins with lesser or equal permissions.

☑ System Administration
Allows control to Device Registry and System Configuration.

□ Alerts
Enables access to Alerts. Access to a Web Filter is required.

□ Web Filter
Controls the Admin's ability to see the Web Filter Single-Sign-on link.

□ Summary Reports
Grants access to Summary Reports.

Fig. 3:1-11 Admin Groups group selections

With the Group Privileges frame populated, you can now make edits as described in the following sub-section.

Edit Admin Group settings

1. In the Group Privileges frame, perform any of the following actions:
   - Modify the **Group Name**
   - Add functions to be monitored by the administrator group
   - Remove functions to be monitored by the administrator group
2. Click **Update Group** to save your settings and to clear all selections in the Group Privileges frame.

Delete an Administrator Group

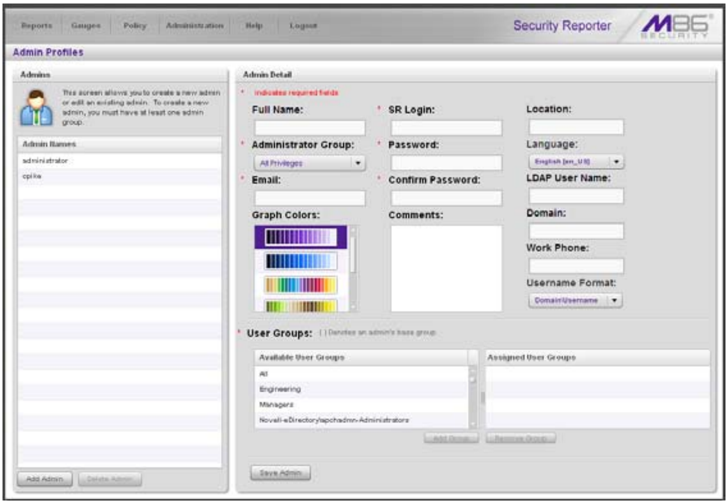
1. In the Group Names list box, click the name of the administrator group to highlight the group name, activate all buttons, and to populate the Group Privileges frame with previously-saved settings.
2. Click **Delete Group** to open the Confirm dialog box with the message: “Are you sure you want to delete this admin group?”
3. Click **Yes** to close the dialog box and to remove the administrator group from the Group Names list box.

***NOTE**: Clicking Cancel closes the dialog box without removing the administrator group.*

Admin Profiles panel

After permission sets have been created, profiles of group administrators can be set up to monitor user groups.

In the navigation toolbar, mouse over the Administration menu link and select **Admin Profiles** to display the Admin Profiles panel:



This screen allows you to create a new admin or edit an existing admin. To create a new admin, you must have at least one admin group.

Admin Names: administrator, cpike

* indicates required fields

Administrator Group: All Privileges

Language: English (en_US)

Username Format: Domain\Username

User Groups: ( ) Denotes an admin's base group

Available User Groups: All, Engineering, Managers, Novell-eDirectory/apchadmin-Administrators

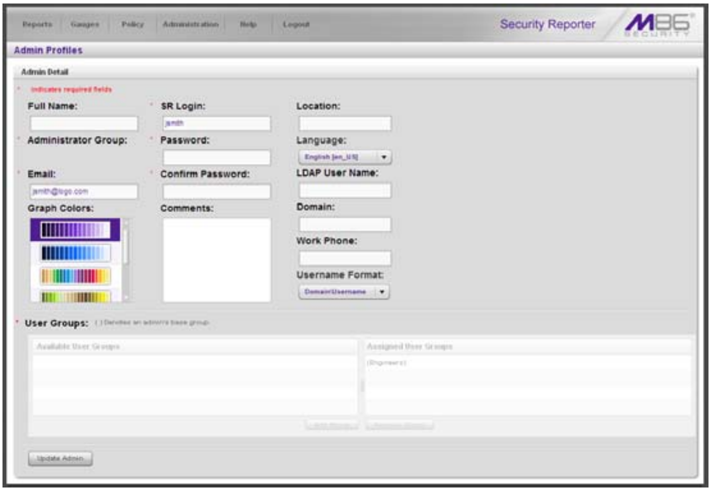
Fig. 3:1-12 Admin Profiles panel, global administrator view

If logged in as the global administrator, or as a group administrator with privileges to create other administrator profiles, at the left side of this panel, the Admin Names list box in the Admins frame displays SR Login IDs of administrator accounts previously set up in this panel (see Fig. 3:2-4).

***NOTE**: In addition to seeing account IDs set up and saved by the administrator in this panel, a global administrator will also see the SR Login ID established during the wizard hardware installation process.*

At the right side of this panel is the Admin Detail panel, used for adding a group administrator profile, viewing an existing administrator's account information, and modifying or deleting a group administrator profile, as necessary.

If logged in as a group administrator without privileges to create other administrator profiles, only the Admin Detail panel displays, as in the sample screen below:



* indicates required fields

Full Name:

* Administrator Group:

* Email: jsmith@logo.com

Graph Colors:

* SR Login: jsmith

* Password:

* Confirm Password:

Comments:

Location:

Language: English [en_US]

LDAP User Name:

Domain:

Work Phone:

Username Format: Domain\Username

* User Groups: ( ) Denotes an admin's base group

Available User Groups

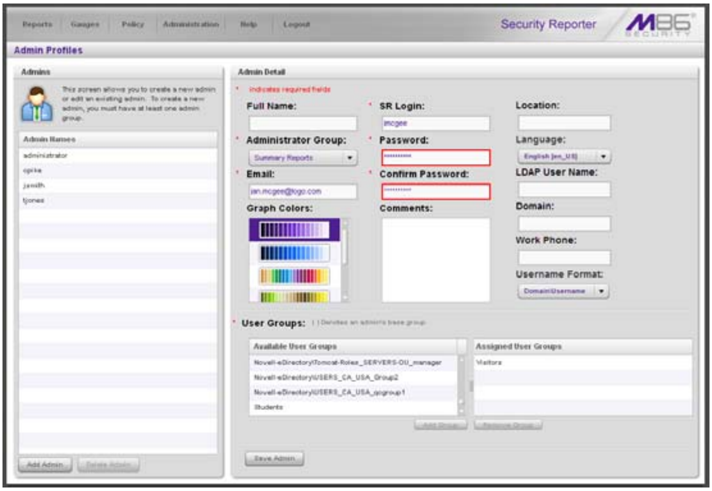
Assigned User Groups: (Engineers)

Fig. 3:1-13 Admin Profiles panel, group administrator view

Add an Administrator Profile

1. If privileges are granted for you to create a group administrator profile, at the bottom of the Admins frame, click **Add Admin** to clear and reset the Admin Detail frame.

2. In the Admin Detail frame, make the following entries or selections as appropriate:



This screen allows you to create a new admin or edit an existing admin. To create a new admin, you must have at least one admin group.

Admin Names: administrator, cpike, jsmith, tjones

* indicates required fields

Full Name:

* SR Login: jmcgee

Location:

* Administrator Group: Summary Reports

* Password: **********

Language: English [en_US]

* Email: jan.mcgee@logo.com

* Confirm Password: **********

LDAP User Name:

Graph Colors:

Comments:

Domain:

Work Phone:

Username Format: Domain\Username

* User Groups: [ ] Denotes an admin's base group

Available User Groups	Assigned User Groups
Novell-eDirectory\Tomcat-Roles_SERVERS-OU_manager	Visitors
Novell-eDirectory\USERS_CA_USA_Group2	
Novell-eDirectory\USERS_CA_USA_qagroup1	
Students	

Fig. 3:1-14 New administrator information entered but not yet saved

- Optional: Type in the group administrator's **Full Name**.
- Select the **Administrator Group** (previously set up in the Admins Group panel) from the available choices in the pull-down menu.
- Type in the group administrator's **Email** address.
- Optional: Select another report color scheme from the available **Graph Colors** choices.
- Type in the **SR Login** ID the group administrator will use to access the SR user interface. This entry will display in the Admin Names list when the record is saved.

- Type in the **Password** the group administrator will use in conjunction with the SR Login ID, and enter that same password again in the **Confirm Password** field. These entries display as asterisks for security purposes.
- Optional: Type in any **Comments** to be associated with the group administrator's account.
- Optional: Type in identifying information about the group administrator's physical office **Location**.
- Optional: If necessary, select the language from the **Language** menu (English, Simplified Chinese, Traditional Chinese).

NOTE*: If English, Simplified Chinese or Traditional Chinese is set to display in your browser, the SR user interface will display that language setting by default.*

- Optional: If the administrator has an Active Directory LDAP account, user name, and domain, type in the alphanumeric group administrator's **LDAP User Name** exactly as set up on the Active Directory domain in which he/she is registered.
- Optional: If an entry was made in the LDAP User Name field, type in the exact characters for the LDAP Active Directory **Domain** name in which the group administrator is registered.

NOTE*: If the group administrator will be using the System Tray feature—that triggers an alert in his/her System Tray if an end user's Internet usage has reached the upper threshold established for a gauge's alert—the LDAP User Name and Domain entered in these fields should be the same as the login ID and password the group administrator uses to authenticate on his/her workstation. (See Real Time Reports Section: Alerts, Lockout Management and Appendix D: System Tray Alerts: Setup, Usage for details on setting up and using the System Tray feature.)*

- Optional: Type in the group administrator’s **Work Phone** number, without entering special characters such as parentheses ( ), a hyphen (-), a period (.), or a left slash (/).
- Optional: If necessary, specify the **Username Format** used on the LDAP server by making a selection from the available choices—Domain\Username, Username\Domain, Username, Domain.

3. In the User Groups section, select the user group(s) to be monitored by the group administrator:
    - In the Available User Groups list box, click the user group(s) to highlight your selection(s), and to activate the Add Group button.
    - Click **Add Group** to include the user group(s) in the Assigned User Groups list box.

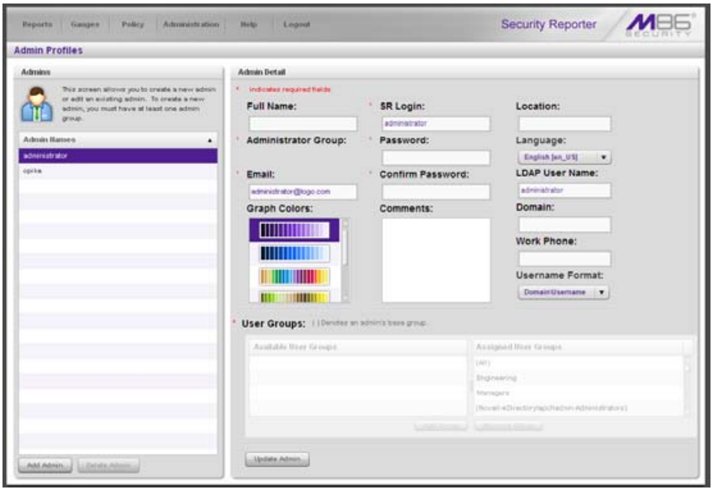
***TIP**: To remove any user group from the Assigned User Groups list box, select the user group(s), and then click Remove Group to remove the user group(s).*

4. After selecting each user group to be assigned to the group administrator, click **Save Admin** to add the SR Login ID for the new administrator to the Admin Names list box.

View, Edit Admin Detail

View Admin Details

For an account with permissions to create other administrator profiles, in the Admin Names list box, select the administrator's SR Login ID to populate that user's profile information in the Admin Detail frame:



This screen allows you to create a new admin or edit an existing admin. To create a new admin, you must have at least one admin group.

Admin Names: administrator, cpike

* indicates required fields

Full Name:
* SR Login: administrator
Location:
* Administrator Group:
* Password:
Language: English [en_US]
* Email: administrator@logo.com
* Confirm Password:
LDAP User Name: administrator
Graph Colors:
Comments:
Domain:
Work Phone:
Username Format: Domain\Username

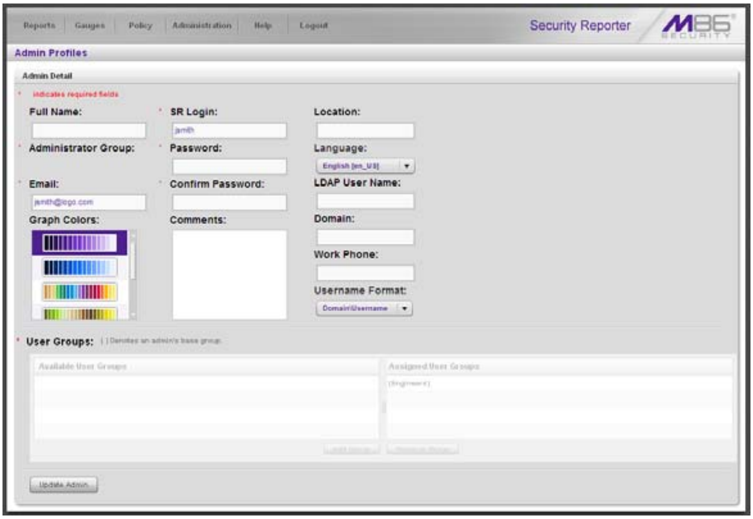
* User Groups: [ ] Denotes an admin's base group

Available User Groups:
Assigned User Groups: (All), Engineering, Managers, [Novell-eDirectory\apichadon-Administrators]

Fig. 3:1-15 Admin Names selection

***NOTE**: Administrator accounts with permissions to create other user profiles display at minimum the Email address, Graph Colors selection, SR Login ID, Language selection, LDAP User Name, Username Format selection, and all user groups greyed-out in the Assigned User Groups list box.*

For an account without permission to create other user profiles, the Admin Detail frame displays at minimum the Email address, Graph Colors selection, SR Login ID, Language selection, Username Format selection, and Assigned User Groups selection(s) greyed-out:



Full Name:

Administrator Group:

SR Login: jsmith

Password:

Confirm Password:

Email: jsmith@logo.com

Location:

Language: English (en_US)

Username Format: Domain\Username

Assigned User Groups: (Engineering)

Fig. 3:1-16 Admin Detail frame

Edit Account Info

1. In the populated Admin Detail frame:
   - The following information can be updated: Email address, Graph Colors, SR Login ID, Password and Confirm Password entries, Language selection, and Username Format selection.
   - The following information can be added, modified, or deleted: Full Name, Comments, Location information, and LDAP User Name or Domain name—the latter two fields are available if using LDAP—and Work Phone number.
   - An administrator account with permissions to create other user accounts also has the ability to modify the Administrator Group selection, and User Groups selections for user accounts he/she set up.
2. After making any modifications, click **Update Admin** to save your edits.

***NOTE**: If the administrator whose password was changed is currently logged into SR, he/she will need to log out and log back in again using the new password.*

Delete Admin

Only an administrator with privileges to create another user profile can delete a user profile he/she created.

***NOTE**: The global administrator account established during the wizard hardware installation process can be modified but cannot be deleted.*

1. In the Admin Names list box, select the group administrator's SR Login ID.
2. Click **Delete Admin** to open the Confirm dialog box with the message: "Are you sure you want to delete this admin?"

***TIP**: Clicking Cancel closes the dialog box without removing the group administrator profile.*

3. Click **Yes** to close the dialog box and to remove the administrator's SR Login ID from the list.

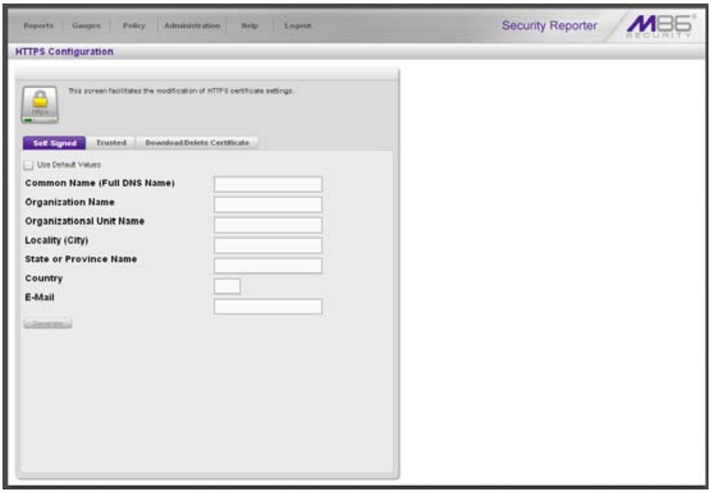
Chapter 2: Database Management

The following panels from the Administration menu of the Report Manager are described in this chapter: HTTPS Configuration, User Profiles (not available for SWG), Activity View, Device Registry, Database Processes List, Server Information, and Reset to Factory Defaults.

HTTPS Configuration panel

The global administrator uses the HTTPS Configuration panel to generate a Secured Sockets Layer (SSL) self-signed certificate or a trusted SSL certificate for administrator workstations so that the SR will be recognized as a valid server with which they can communicate.

In the navigation toolbar, mouse over the Administration menu link and select **HTTPS Configuration** to open the HTTPS Configuration panel, comprised of Self-Signed, Trusted, and Download/Delete Certificate tabs used for creating, uploading, downloading, and/or deleting self-signed or third party SSL certificates:



This screen facilitates the modification of HTTPS certificate settings.

□ Use Default Values

Common Name (Full DNS Name)	
Organization Name	
Organizational Unit Name	
Locality (City)	
State or Province Name	
Country	
E-Mail	

Fig. 3:2-1 HTTPS Configuration panel, Self-Signed tab

Generate a Self-Signed Certificate for the SR

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.*

1. 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)** - Host name 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. **E-Mail** - Your email address.
2. Click **Create** to generate the SSL certificate to be stored on the SR, and to restart the Report Manager. Hereafter, 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.

***NOTES**: Once the SSL certificate has been created, the Generate button displays greyed-out. Although the Security Reporter login window may re-display right away, the service will take a few minutes before it starts up again.*

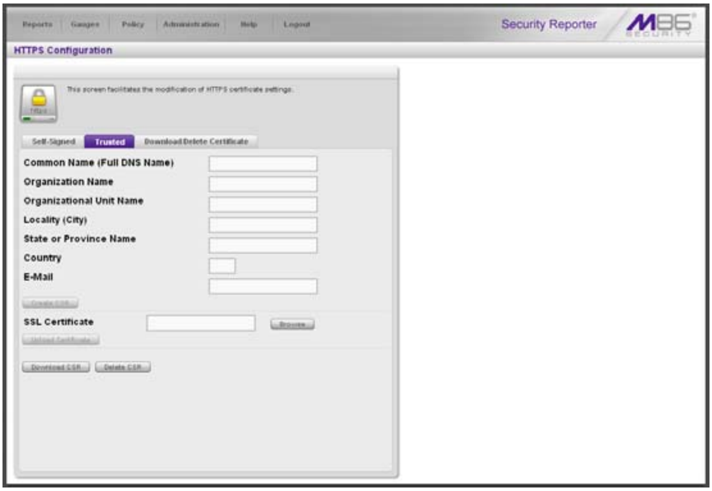
Create, Upload a Third Party Certificate

On the Trusted tab, you create a Certificate Signing Request for the SR's digital identity certificate, download, save or delete a CSR, and upload a trusted SSL certificate.

Step A: Create a CSR

***WARNING**: Generating the CSR 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.*

1. Click the Trusted tab:



This screen facilitates the modification of HTTPS certificate settings.

Fig. 3:2-2 HTTPS Configuration panel, Trusted tab

2. Make entries in these fields:

   a. **Common Name (Full DNS Name)** - Host name of the SR 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. **E-Mail** - Your email address.

3. Click **Create CSR** to generate the Certificate Signing Request and to restart the Report Manager.

NOTE*: Once the CSR has been created, the Create CSR button displays greyed-out and the Browse, Save CSR, and Delete CSR buttons become activated.*

Step B: Download the CSR, Submit to Agency

1. In the Trusted tab, click **Download CSR** to download the CSR you created to your machine.

   When the CSR is downloaded to your machine, the Download CSR button toggles to Save CSR.

2. Click **Save CSR** to save the CSR to your machine.

TIP*: Click* ***Delete CSR*** *to remove the CSR you created on your machine.*

3. Submit the CSR to a trusted third party agency authorized to sign SSL certificates.

Step C: Upload the Signed SSL Certificate to SR

When the SSL certificate is emailed back to you with the authorized signature, do the following:

1. Launch Notepad on your machine.
2. Copy and paste the contents of the certificate into Notepad in the following order:

   a. SSL certificate

   b. Intermediate certificate(s)—this step is not required if you have a Single Root SSL Certificate

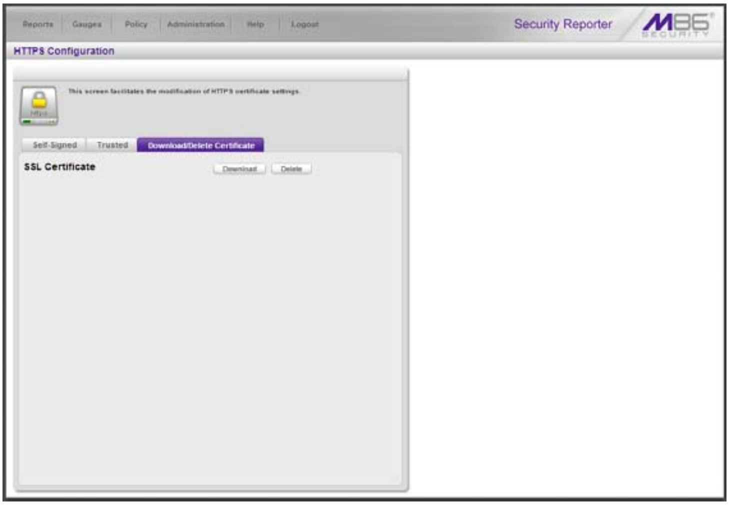
   c. Root certificate
3. Save the contents of the Notepad file with a .cer extension.
4. In the Trusted tab, go to the **SSL certificate** field and click **Browse** to find the .cer file you just saved.
5. Click **Upload** to load the certificate on the SR.

NOTE*: Do not click this button until performing the actions in the following steps.*

TIP*: Click* ***Cancel*** *in the dialog box to cancel the procedure.*

Download, Delete a Third Party Certificate

If a trusted certificate was generated and uploaded to the SR, the Download/Delete Certificate tab shows the Download and Delete buttons enabled:



This screen facilitates the modification of HTTPS certificate settings.

Fig. 3:2-3 HTTPS Configuration panel, Trusted tab

Download the SSL Certificate

To download the SR's third party SSL certificate to your workstation, go to the Download/Delete Certificate tab and click **Download** to download the certificate to your machine.

The certificate can now be distributed to group administrator workstations.

Delete the SSL Certificate

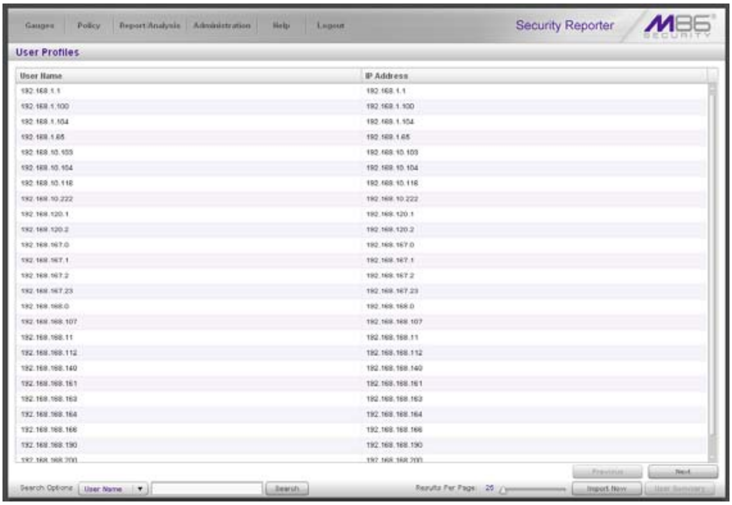
To delete the third party certificate from the SR, go to the Download/Delete Certificate tab and click **Delete** to remove the certificate from the SR.

User Profiles panel

If using a Web Filter, the User Profiles panel lets you view the list of users that is created when the SR first communicates with the source Web Filter. This list is used for verifying that the list of active end users on the source Web Filter matches the list of end users on the SR application. If there are any discrepancies, synchronization can be forced between the two servers (see Device Registry panel in this chapter).

***NOTE**: The User Profiles panel is available to a group administrator only if permissions were granted by the administrator who set up his/her account.*

In the navigation toolbar, mouse over the Administration menu link and select **User Profiles** to open the User Profiles panel:



User Profiles

User Name	IP Address
192.168.1.1	192.168.1.1
192.168.1.100	192.168.1.100
192.168.1.104	192.168.1.104
192.168.1.65	192.168.1.65
192.168.10.103	192.168.10.103
192.168.10.104	192.168.10.104
192.168.10.116	192.168.10.116
192.168.10.222	192.168.10.222
192.168.120.1	192.168.120.1
192.168.120.2	192.168.120.2
192.168.167.0	192.168.167.0
192.168.167.1	192.168.167.1
192.168.167.2	192.168.167.2
192.168.167.23	192.168.167.23
192.168.168.0	192.168.168.0
192.168.168.107	192.168.168.107
192.168.168.11	192.168.168.11
192.168.168.112	192.168.168.112
192.168.168.140	192.168.168.140
192.168.168.161	192.168.168.161
192.168.168.163	192.168.168.163
192.168.168.164	192.168.168.164
192.168.168.166	192.168.168.166
192.168.168.190	192.168.168.190
192.168.168.200	192.168.168.200

Search Options: User Name ▼

Results Per Page: 25

Fig. 3:2-4 User Profiles panel

By default, this panel is comprised of rows of end user records, sorted in ascending order by User Name (IP address). For each user name in the list, the corresponding end user IP Address displays.

At the bottom left of the panel is the Search Options menu that lets you search for a specific user by User Name or IP Address. At the bottom right of the panel is the User Summary button takes you to the User Summary panel for the selected user.

Search the User Database

1. Specify search criteria by making a selection from the **Search Options** pull-down menu:
   - **User Name** - This selection performs a search by an end user’s user name.
   - **IP Address** - This selection performs a search by an end user’s IP address.
2. Make an entry in the blank field to the right:
   - If User Name was selected, enter a user name
   - If IP Address was selected, enter an IP address.
3. Click **Search** to display a record that matches your criteria.

***TIPS**: After performing a search, if you wish to re-display all end users records in the list again—or import new users and new user groups from the LDAP server—click **Import Now**.*

To display more end user records at a time than the default 25 user records, move the slider to the right and specify the maximum number of records to display in the list: 50, 75, 100, 125, 150, 175, 200, 225, 250.

View End User Activity

1. To drill down and view additional information about an end user’s activity, select the user’s record to highlight it.
2. Click **User Summary** to open the User Summary panel, and perform any of the actions described for this panel in the Real Time Reports Section.

Activity View panel

The Activity View panel is used for viewing the most recent administrative activity performed on the SR.

In the navigation toolbar, mouse over the Administration menu link and select **Activity View** to display the Activity View panel:

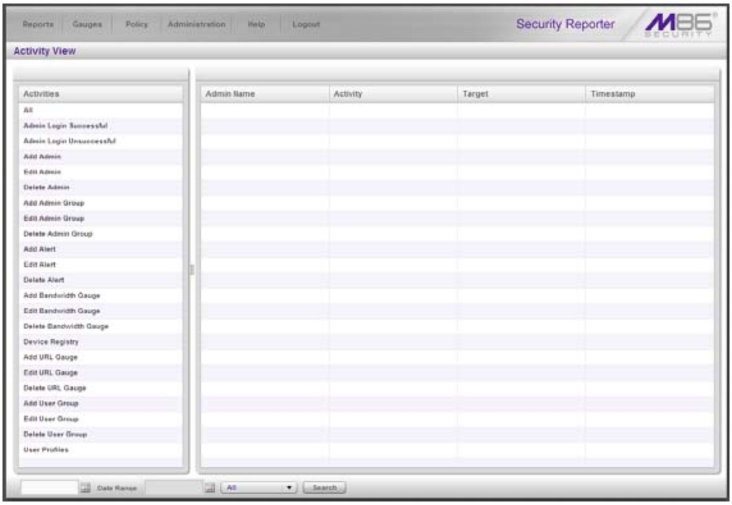


Fig. 3:2-5 Activity View panel

The Activities frame displays to the left and the empty target frame displays to the right. Below these frames is the Date Range field, the administrator user names menu, and Search button.

Perform a Search on a Specified Activity

To perform a search on a specified activity:

1. Select the type of Activity from available choices in the list: All, Admin Login Successful, Admin Login Unsuccessful, Add Admin, Edit Admin, Delete Admin, Add Admin Group, Edit Admin Group, Delete Admin Group,

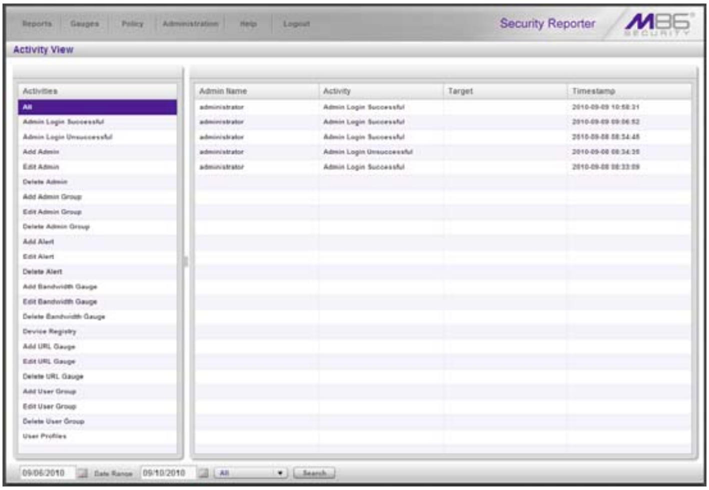
Add Alert, Edit Alert, Delete Alert, Add Bandwidth Gauge, Edit Bandwidth Gauge, Delete Bandwidth Gauge, Device Registry, Add URL Gauge, Edit URL Gauge, Delete URL Gauge, Add User Group, Edit User Group, Delete User Group, User Profiles.

***NOTE**: The Activities list will only display activity types performed on SR within the past 30 days.*

2. In the **Date Range** field, click the 📅 calendar icon on the left to open the larger calendar for the current month, with today’s date highlighted.

***TIP**: To view the calendar for the previous month, click the left arrow. To view the calendar for the next month, click the right arrow.*

3. Click the starting date to select it and to close the calendar pop-up window. This action populates the field to the left of the calendar icon with the selected date.
4. Click the 📅 calendar icon on the right to open the larger calendar for the current month, with today’s date highlighted.
5. Click the ending date to select it and to close the calendar pop-up window. This action populates the field to the left of the calendar icon with the selected date.
6. To view the activity of a specified administrator, select the user name from the pull-down menu.
7. Click **Search** to display the specified records for the selected dates in the results list:



Activities

- All
- Admin Login Successful
- Admin Login Unsuccessful
- Add Admin
- Edit Admin
- Delete Admin
- Add Admin Group
- Edit Admin Group
- Delete Admin Group
- Add Alert
- Edit Alert
- Delete Alert
- Add Bandwidth Gauge
- Edit Bandwidth Gauge
- Delete Bandwidth Gauge
- Device Registry
- Add URL Gauge
- Edit URL Gauge
- Delete URL Gauge
- Add User Group
- Edit User Group
- Delete User Group
- User Profiles

Admin Name	Activity	Target	Timestamp
administrator	Admin Login Successful		2010-09-09 10:58:31
administrator	Admin Login Successful		2010-09-09 09:06:52
administrator	Admin Login Successful		2010-09-08 08:54:48
administrator	Admin Login Unsuccessful		2010-09-08 08:34:35
administrator	Admin Login Successful		2010-09-08 08:33:09

09/06/2010 Date Range 09/10/2010 All

Fig. 3:2-6 Activity View results

Search results

When populated with rows of records, the results list includes data in the following columns: Admin Name (entry from the Admin Name field in the login window); Activity; Target (administrator group name or group administrator name, if applicable), and Timestamp (using the YYYY-MM-DD HH:MM:SS format).

The information that displays in these columns differs depending on the type of search performed, and if an administrator name was selected from the drop-down menu.

The Target field displays information only as applicable for any of the following actions executed by the administrator (Admin Name), such as:

- administrator name for Add/Edit/Delete Admin
- group name for Add/Edit/Delete Admin Group
- alert name for Add/Edit/Delete Alert
- gauge name for Add/Edit/Delete URL/Bandwidth Gauge.

Device Registry panel

The Device Registry panel is used for viewing information about devices connected to the SR, synchronizing the SR with user groups and libraries from the source Web Filter, editing M86 appliance criteria, and adding/deleting a Web Filter, SWG, or LDAP server to/from the registry.

This function is available to a group administrator only if permissions were granted by the administrator who set up his/her account, as detailed in Admins Group panel in Chapter 1.

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

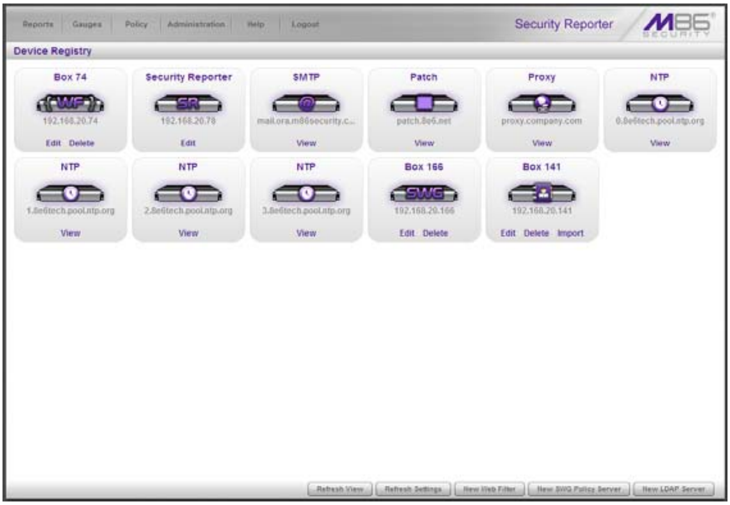


Fig. 3:2-7 Device Registry

This panel is comprised of icons representing devices set up to communicate with the SR. All device icons include at least one link describing the action(s) that can be performed on that device: View, Edit, Delete.

At the bottom of the panel the following buttons display:

- **Refresh View** - Click this button if any icon representing a device does not properly display in the user interface.
- **Refresh Settings** (displays only if using a Web Filter) - Click this button to synchronize Web Filter library Categories, and/or User Groups.
- **New Web Filter** - Click this button to add a Web Filter to the device registry.
- **New SWG Policy Server** - Click this button to add an SWG policy server to the device registry.
- **New LDAP Server** (enabled only if an SWG has been added to the device registry) - Click this button to add an LDAP server to the device registry.

***NOTE**: A Web Filter or SWG policy server must be added to the device registry in order for the SR to generate reports. If a Web Filter or SWG policy server was not specified during the wizard installation process, please add this device now.*

Removing/adding Web Filter, SWG devices

Please note the following conditions that occur if removing a Web Filter and/or SWG device, and/or adding another device of either of these types:

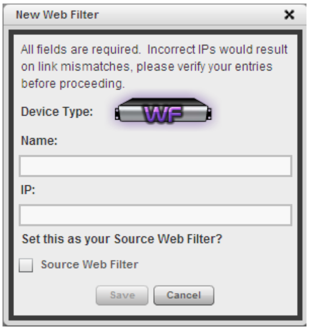
Device(s) listed in registry	Change(s) made to registry	Result
SWG	Remove SWG	All data for Time Usage Reports, Summary Reports, Summary Drill Down Reports and Detail Drill Down Reports will be purged.
SWG	Retain SWG and add Web Filter	All data for Time Usage Reports, Summary Reports, Summary Drill Down Reports and Detail Drill Down Reports will be purged.
SWG and Web Filter	Retain Web Filter only	Web Filter productivity data will be retained, SWG and security report data will be purged.
Web Filter	Remove Web Filter	All data for Time Usage Reports, Summary Reports, Summary Drill Down Reports and Detail Drill Down Reports will be purged.
Web Filter	Retain Web Filter and add SWG	No data will be purged.
Web Filter and SWG	Retain SWG only	All data for Time Usage Reports, Summary Reports, Summary Drill Down Reports and Detail Drill Down Reports will be purged.

⚠ ***WARNING**: For any scenario specified above that would result in data being purged from the Security Reporter, M86 recommends backing up and saving current SR data off the server before adding or removing the designated device from the device registry. If this is an SR server with RAID, please refer to the Backup screen sub-section from Chapter 2 of the System Configuration Section of this User Guide for information about backing up data.*

Web Filter Device Maintenance

Add a Web Filter to the device registry

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



New Web Filter ✕

All fields are required. Incorrect IPs would result on link mismatches, please verify your entries before proceeding.

Device Type:

Name:

IP:

Set this as your Source Web Filter?

□ Source Web Filter

Fig. 3:2-8 New Web Filter pop-up window

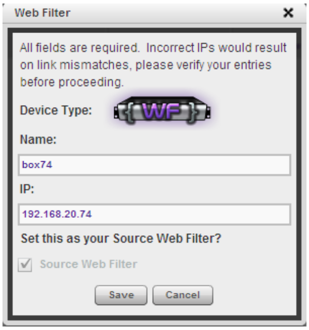
2. Type in the server **Name**.
3. Type in the **IP** address of the server.
4. If this Web Filter will be the source server, click the **Source Web Filter** checkbox.

***TIP**: Click **Cancel** to close this pop-up window.*

5. 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.

View, edit Web Filter device criteria

1. Go to the Web Filter server icon in the Device Registry panel and click **Edit** to open the Web Filter pop-up window:



Web Filter

All fields are required. Incorrect IPs would result on link mismatches, please verify your entries before proceeding.

Device Type: WF

Name:

box74

IP:

192.168.20.74

Set this as your Source Web Filter?

☑ Source Web Filter

Fig. 3:2-9 Web Filter pop-up window

The Device Type (WF) displays and cannot be edited.

2. Edit any of the following:
   - **Name** - Name of the application.
   - **IP** - IP address of the server.
   - **Source Web Filter** - If this checkbox is not populated and the Web Filter will now be the source Web Filter, click in the checkbox to place a check mark here.

***TIP**: Click **Cancel** to close this pop-up window.*

3. Click **Save** to save your edits and to close the pop-up window.

Delete a Web Filter from the device registry

1. Go to the Web Filter server icon in the Device Registry panel and click **Delete** to open the CONFIRM dialog box with the message: “Are you sure you want to delete this device?”

***NOTE**: Click **No** to close the dialog box.*

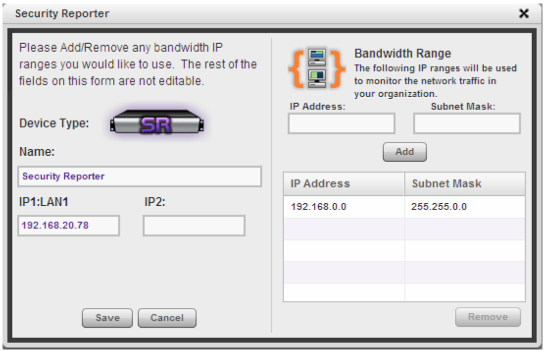
2. Click **Yes** to delete the Web Filter device from the registry, and to remove the Web Filter server icon from the Device Registry panel.

***TIPS**: If the current source Web Filter needs to be replaced, please use the edit function to specify a different Web Filter as the source server before deleting the Web Filter currently designated as the source server. A source Web Filter cannot be deleted until all target Web Filters have been removed.*

Security Reporter Maintenance

View SR device criteria

Go to the SR server icon in the Device Registry panel and click **Edit** to open the Security Reporter pop-up window:



Security Reporter

Please Add/Remove any bandwidth IP ranges you would like to use. The rest of the fields on this form are not editable.

Device Type: SR

Name: Security Reporter

IP1:LAN1: 192.168.20.78

IP2:

Bandwidth Range

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

IP Address:

Subnet Mask:

IP Address	Subnet Mask
192.168.0.0	255.255.0.0

Fig. 3:2-10 Security Reporter pop-up window

The following displays at the left side of this window: Device Type (SR), Name of the application (Security Reporter), and IP1:LAN1 and IP2 address(es), if entered during—or subsequently to—the wizard hardware installation process.

The following displays at the right side of this window: Bandwidth Range IP Address and Subnet Mask fields, and buttons for adding or removing a range of IP addresses the SR application will monitor for network traffic.

***NOTE**: Bandwidth Range criteria is only required if a Web Filter will be used with this SR.*

If an IP Address and Subnet Mask were previously entered in this window, that information displays in the list box.

Add, remove a bandwidth range

1. Do the following in the Bandwidth Range section:
   - To add a bandwidth IP address range:
     a. Type in the **IP Address**.
     b. Type in the **Subnet Mask**.
     c. Click **Add** to add the bandwidth IP range in the list box.
   - To remove a bandwidth IP address range:
     a. Select the IP address range from the list box; this action activates the Remove button.
     b. Click **Remove** to remove the IP address range.

***TIP**: Click **Cancel** to close the pop-up window without saving your entries.*

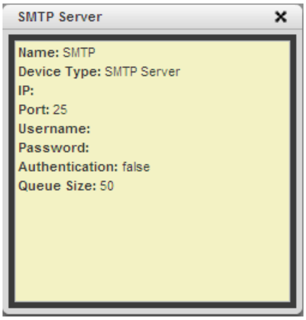
2. After making all modifications in this window, click **Save** to save your edits and to close the pop-up window.

View Other Device Criteria

View only actions are permitted in the Device Registry panel for the following devices: SMTP, Patch Server, NTP Server, and Proxy Server.

View SMTP device criteria

1. Go to the image of the SMTP server in the Device Registry panel and click **View** to open the SMTP Server pop-up window:



SMTP Server

Name: SMTP
Device Type: SMTP Server
IP:
Port: 25
Username:
Password:
Authentication: false
Queue Size: 50

Fig. 3:2-11 SMTP window

The following information displays: Name of server, Device Type (SMTP), IP address, Port number (if applicable), Username (if applicable), Password (if applicable), Authentication ("true" or "false"), Queue Size.

2. Click the “X” in the upper right corner to close this pop-up window.

View Patch Server device criteria

1. Go to the image of the Patch Server in the Device Registry panel and click **View** to open the Patch Server pop-up window. The following information displays: Name of server, Device Type (Patch Server), IP address, Username (if applicable), Password (if applicable, asterisks display), HTTPS ("on" or "off"), Transfer Mode ("active" or "passive").
2. Click **Close** to close this pop-up window.

View Proxy Server device criteria

1. Go to the image of the Proxy Server in the Device Registry panel and click **View** to open the Proxy Server pop-up window. The following information displays: Name of server (Proxy Server), Device Type (Proxy Server), IP address, Port number, Username (if applicable), Password (if applicable, asterisks display), Proxy Switch ("on" or "off").

2. Click **Close** to close this pop-up window.

View NTP Server device criteria

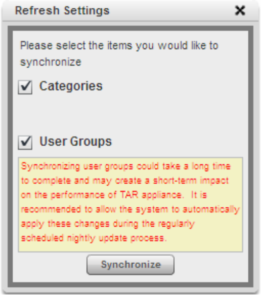
1. Go to the image of the NTP Server in the Device Registry panel and click **View** to open the NTP Server pop-up window. The following information displays: Name of server (NTP Server), Device Type (NTP Server), IP address.

2. Click **Close** to close this pop-up window.

Refresh Settings

If using a Web Filter, a forced synchronization should be performed on the SR unit if any of the source Web Filter's related devices listed in the device registry are updated.

1. Click **Refresh Settings** to open the Refresh Settings pop-up window:



Refresh Settings ✕

Please select the items you would like to synchronize

☑ Categories

☑ User Groups

Synchronizing user groups could take a long time to complete and may create a short-term impact on the performance of TAR appliance. It is recommended to allow the system to automatically apply these changes during the regularly scheduled nightly update process.

Fig. 3:2-12 Refresh Settings

2. Check the checkbox(es) pertaining to information to be synchronized between the Web Filter and SR devices, and to activate the Synchronize button:

   - **Categories** - Make this selection to synchronize M86 supplied library category updates and custom library categories from the source Web Filter to the SR.

- **User Groups** - Make this selection to synchronize LDAP user group information on the source Web Filter to the SR.

TIP: *Click the "X" in the upper right corner of this pop-up window to close it.*

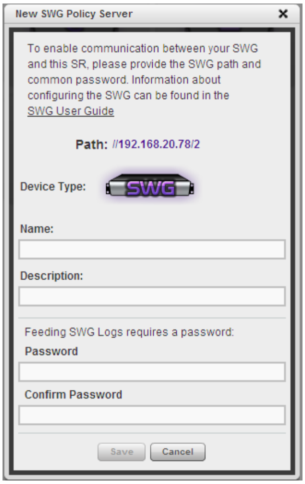
WARNING: *The User Groups synchronization process may be lengthy and thus may create an impact on the SR's performance.*

3. Click **Synchronize** to close the pop-up window and to begin the synchronization process.

SWG Policy Server Device Maintenance

Add the first Policy Server to the device registry

1. If an SWG Policy Server will be used with this SR and was not added during the SR Wizard installation process—nor subsequently added to this device registry—click **New SWG Policy Server** at the bottom of the Device Registry panel to open the New SWG Policy Server pop-up window:


New SWG Policy Server

To enable communication between your SWG and this SR, please provide the SWG path and common password. Information about configuring the SWG can be found in the SWG User Guide

Path: //192.168.20.78/2

Device Type: SWG

Name:

Description:

Feeding SWG Logs requires a password:

Password

Confirm Password

Fig. 3:2-13 Add New SWG Policy Server

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

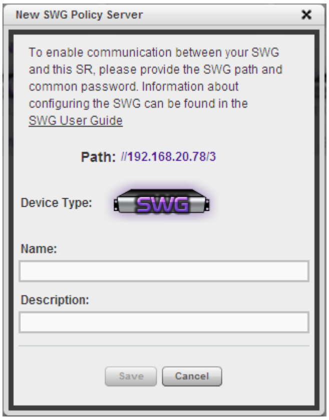
2. Enter a **Name** for the device and/or a **Description** for the device.
3. Enter the **Password** this SR will use for communicating with this SWG and any other SWG subsequently added to the device registry. Make this same entry again in the **Confirm Password** field.

TIP*: Click* ***Cancel*** *to close this pop-up window.*

4. 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.

Add another Policy Server to the device registry

1. If adding an additional SWG Policy Server to the device registry, click **New SWG Policy Server** at the bottom of the Device Registry panel to open the New SWG Policy Server pop-up window:



New SWG Policy Server ✕

To enable communication between your SWG and this SR, please provide the SWG path and common password. Information about configuring the SWG can be found in the SWG User Guide

Path: //192.168.20.78/3

Device Type: SWG

Name:

Description:

Save Cancel

Fig. 3:2-14 Add another New SWG Policy Server

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

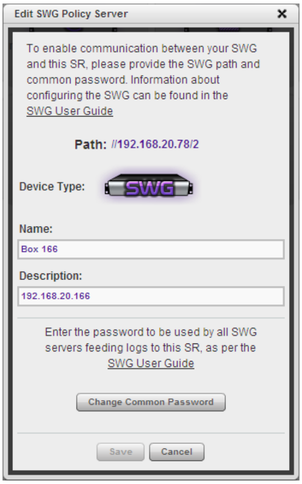
2. Enter a **Name** for the device and/or a **Description** for the device.

*TIP: Click **Cancel** to close this pop-up window.*

3. 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.

Edit Policy Server criteria, change password

1. Go to the SWG server icon in the Device Registry panel and click **Edit** to open the Edit SWG Policy Server pop-up window:



Edit SWG Policy Server

To enable communication between your SWG and this SR, please provide the SWG path and common password. Information about configuring the SWG can be found in the SWG User Guide

Path: //192.168.20.78/2

Device Type: SWG

Name: Box 166

Description: 192.168.20.166

Enter the password to be used by all SWG servers feeding logs to this SR, as per the SWG User Guide

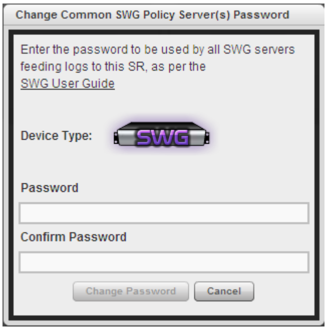
Fig. 3:2-15 Edit SWG Policy Server pop-up window

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

2. The following actions can be performed in this window:
   - Make entries or edits in the following fields:
     - **Name** - Name for the device.
     - **Description** - Description of the device.

*TIP: Click **Cancel** to close this pop-up window.*

- Click **Change Common Password** to open the Change SWG Policy Server(s) Password pop-up window:



Change Common SWG Policy Server(s) Password

Enter the password to be used by all SWG servers feeding logs to this SR, as per the SWG User Guide

Device Type: SWG

Password

Confirm Password

Fig. 3:2-16 Change Common Password pop-up window

a) Enter the **Password** this SR will use for accessing any SWG server entered in this device registry. The password must be comprised of eight to 20 characters, and include at least one alpha, numeric, and special character.

b) Enter the same password again in the **Confirm Password** field; this action activates the Change Password button.

***TIP**: Click **Cancel** to close this pop-up window.*

c) Click **Change Password** to save your entries, close this pop-up window, and return to the Edit SWG Policy Server pop-up window.

3. Click **Save** to save your edits and to close the pop-up window.

Delete a Policy Server from the device registry

1. Go to the SWG server icon in the Device Registry panel and click **Delete** to open the CONFIRM dialog box with the message: "Are you sure you want to delete this device?"

***NOTE**: Click **No** to close the dialog box.*

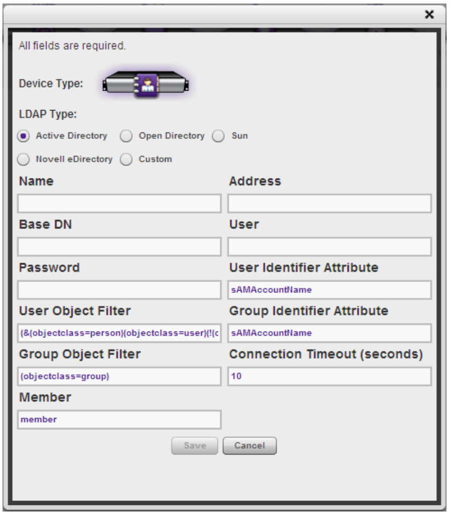
2. Click **Yes** to delete the SWG device from the registry, and to remove the SWG server icon from the Device Registry panel.

LDAP Server Device Management

If using an SWG, any LDAP server used with the SWG should be added to the device registry.

Add an LDAP Server to the device registry

1. At the bottom of the Device Registry panel, click **New LDAP Server** to open the LDAP server pop-up window:



All fields are required.

Device Type:

LDAP Type:

● Active Directory ○ Open Directory ○ Sun

○ Novell eDirectory ○ Custom

Name

Address

Base DN

User

Password

User Identifier Attribute: sAMAccountName

User Object Filter: (&(objectclass=person)(objectclass=user)(!(c

Group Identifier Attribute: sAMAccountName

Group Object Filter: (objectclass=group)

Connection Timeout (seconds): 10

Member: member

Fig. 3:2-17 Add LDAP server

The Device Type image displays.

2. Make entries in the following fields:
   - **LDAP Type**: Active Directory, Open Directory, Sun, Novell eDirectory, Custom
   - **Name** - Label assigned to the LDAP server
   - **Base DN** - Root of the LDAP database to be queried using the LDAP syntax, e.g. *DC=domain,DC=com*, or *o=server-org*. The entry in this field is case sensitive.
   - **Password** - LDAP server password
   - **User Object Filter** - Identify user objects, if necessary
   - **Group Object Filter** - Identify group objects, if necessary
   - **Member** - Specify membership attributes, if necessary
   - **Address** - LDAP server IP address
   - **User** - Enter the authorized user's full LDAP Distinguished Name. For example, enter the entire string in a format such as:

     cn=Administrator,cn=Users,dc=qa,dc=local

     or

     cn=admin,o=logo-org
   - **User Identifier Attribute** - Specify attributes used for identifying a user, if necessary
   - **Group Identifier Attribute** - Specify attributes used for identifying a group, if necessary
   - **Connection Timeout (seconds)** - Default is 10 seconds for connecting to the LDAP server

TIP: *Click* ***Cancel*** *to close this pop-up window.*

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

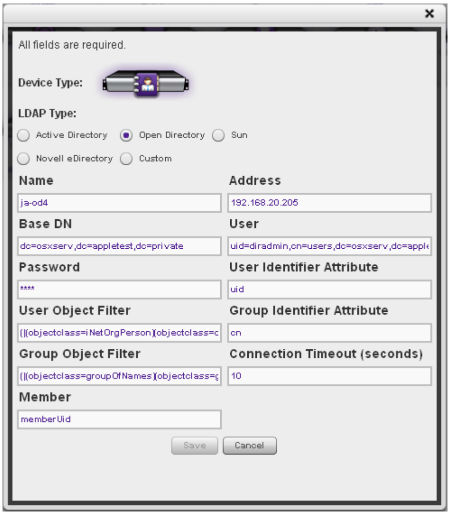
Import LDAP Group profiles

1. Go to the LDAP server icon in the Device Registry panel and click **Import** to begin importing group profiles from the LDAP server.
2. After the alert box opens to specify whether or not the LDAP group importation process was successful, click **OK** to close the pop-up box.

***TIP**: If the importation process failed, make edits in the LDAP server pop-up window and run the import process again.*

View, edit LDAP Server device criteria

1. Go to the LDAP server icon in the Device Registry panel and click **Edit** to open the pop-up window:



All fields are required.

Device Type:

LDAP Type:

○ Active Directory ● Open Directory ○ Sun

○ Novell eDirectory ○ Custom

Name ja-od4	Address 192.168.20.205
Base DN dc=osxserv,dc=appletest,dc=private	User uid=diradmin,cn=users,dc=osxserv,dc=apple
Password ****	User Identifier Attribute uid
User Object Filter (|(objectclass=iNetOrgPerson)(objectclass=c	Group Identifier Attribute cn
Group Object Filter (|(objectclass=groupOfNames)(objectclass=g	Connection Timeout (seconds) 10
Member memberUid	

Fig. 3:2-18 LDAP Server pop-up window

The Device Type image for the LDAP server displays, along with entries previously made and saved in this window.

2. Edit any of the fields in this pop-up window.

***TIP**: Click **Cancel** to close this pop-up window.*

3. Click **Save** to save your edits and to close the pop-up window.

Delete an LDAP Server from the device registry

1. Go to the LDAP server icon in the Device Registry panel and click **Delete** to open the CONFIRM dialog box with the message: “Are you sure you want to delete this device?”

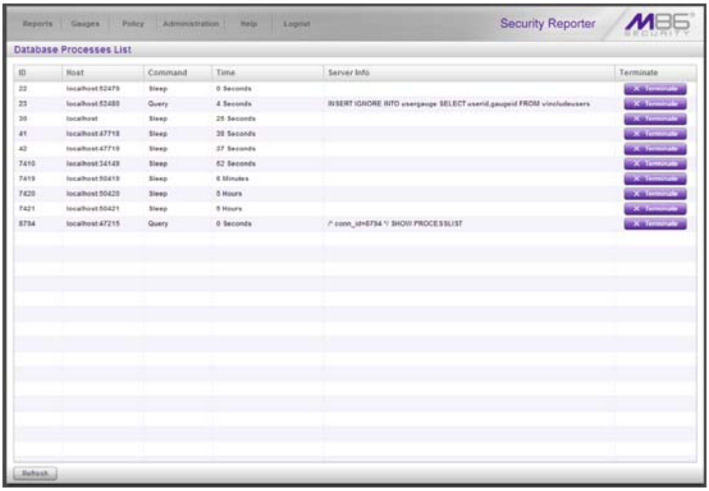
***NOTE**: Click **No** to close the dialog box.*

2. Click **Yes** to delete the LDAP server device from the registry, and to remove the LDAP server icon from the Device Registry panel.

Database Processes List panel

The global administrator uses the Database Process List panel to view a list of processes currently running on the SR or to halt a process that is currently running.

In the navigation toolbar, mouse over the Administration menu link and select **Database Processes List** to display the Database Processes List panel:



Database Processes List

ID	Host	Command	Time	Server Info	Terminate
22	localhost:52479	Sleep	0 Seconds		X Terminate
23	localhost:52480	Query	4 Seconds	INSERT IGNORE INTO usergauge SELECT userid,gaugeid FROM vincludeusers	X Terminate
30	localhost	Sleep	25 Seconds		X Terminate
41	localhost:47718	Sleep	38 Seconds		X Terminate
42	localhost:47719	Sleep	37 Seconds		X Terminate
7410	localhost:34149	Sleep	62 Seconds		X Terminate
7419	localhost:50419	Sleep	6 Minutes		X Terminate
7420	localhost:50420	Sleep	5 Hours		X Terminate
7421	localhost:50421	Sleep	5 Hours		X Terminate
8794	localhost:47215	Query	0 Seconds	/* conn_id=8794 */ SHOW PROCESSLIST	X Terminate

Fig. 3:2-19 Database Processes List window

View Details on a Process

Each row in the list includes the following information: process identification number (ID) on the MySQL server; Host name or IP address of the server, and port connected to the database; the state of the last Command issued by the user (“Query” or “Sleep”); the amount of Time in seconds the process has remained in its current state, and SQL statement for a process currently running (Server Info). At the end of each row is the Terminate option.

***TIP**: Click the **Refresh** button to refresh the list of records.*

Terminate a Process

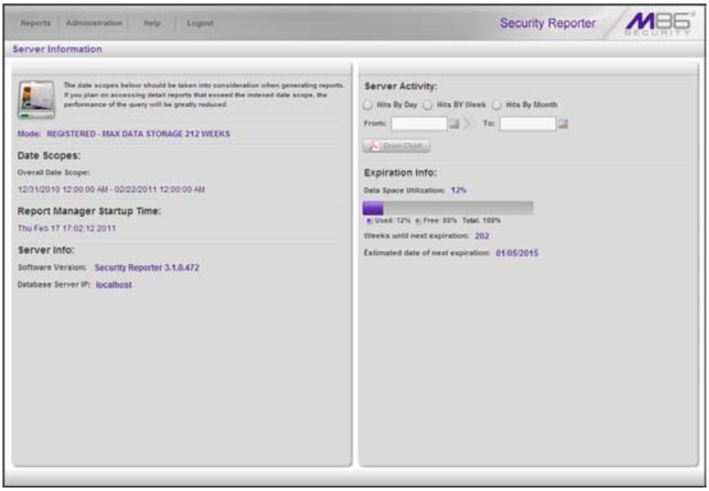
Select the process to be terminated and click **Terminate**.

***WARNING**: Be sure that you do not terminate the wrong process.*

Server Information panel

The global administrator uses the Server Information panel to obtain details about data storage on the SR Server, the time the Report Manager was last restarted, and the SR Server's IP address and current software version number.

In the navigation toolbar, mouse over the Administration menu link and select **Server Information** to display the Server Information panel:



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

Mode: REGISTERED - MAX DATA STORAGE 212 WEEKS

Date Scopes:

Overall Date Scope:

12/31/2010 12:00:00 AM - 02/22/2011 12:00:00 AM

Report Manager Startup Time:

Thu Feb 17 17:02:12 2011

Server Info:

Software Version: Security Reporter 3.1.0.472

Database Server IP: localhost

Server Activity:

From: To:

Expiration Info:

Data Space Utilization: 12%

Used: 12% Free: 88% Total: 100%

Weeks until next expiration: 202

Estimated date of next expiration: 01/05/2015

Fig. 3:2-20 Server Information panel

The panel is comprised of six sections: Mode (this section does not display for an SR in evaluation mode), Date Scopes, Report Manager Startup Time, Server Info, Server Activity, and Expiration Info.

***NOTE**: If the SR server is newly installed, server statistics will be available after they are initially correlated for the server, immediately after midnight. If this problem persists, please contact your system administrator.*

Mode

Registered Mode and Evaluation Mode

The Mode section displays information about an SR in registered mode: “REGISTERED” followed by the maximum number of weeks of data storage (“MAX DATA STORAGE ‘X’ WEEKS”—in which ‘X’ represents the number of weeks).

Registered mode pertains to an SR server that has been activated online and registered by M86 Security. An SR in registered mode will store as much data as allocated for data storage on its hard drive—and on its attached storage device, if applicable to the hardware model of the SR server. When the SR is close to reaching its maximum capacity of data storage—as determined by the SR when making its routine 30-minute check of available storage space—the oldest week of data (from Sunday through Saturday) is dropped from the database.

Evaluation mode is used during the evaluation period of an SR, a maximum of three weeks by default. Since data is expired from the server in full weekly increments from Sunday through Saturday, if a newly installed SR is up and running on any day of the week after a Sunday (i.e. on a Monday through a Saturday), the evaluation period would be less than three weeks. For example, if the SR was installed on Wednesday, January 5, 2011, the evaluation period would run from that day until Saturday, January 22, 2011.

NOTES*: See the Expiration screen in the System Configuration Section for more information about data expiration. See also Appendix C: Evaluation Mode for information about using the SR in the evaluation mode.*

Date Scopes

The Date Scopes section displays the Overall Date Scope of data stored on the SR. This date scope includes the range for the period of stored data, using the MM/DD/YYYY HH:MM:SS AM/PM format.

Report Manager Startup Time

The Report Manager Startup Time section contains the following information pertaining to the last time the Report Manager was restarted: Day of the week and month name abbreviation, day, military time (HH:MM:SS), and year (YYYY).

NOTE*: This information is useful for troubleshooting manually generated reports. If your reports are not displaying, it may be that the Report Manager has restarted and terminated the report generation process.*

Server Info

The Server Info section contains the following SR server information: **Software Version** number and **Database Server IP** address—or the label “localhost” that designates the SR as the host server for the Report Manager.

Server Activity

In the Server Activity section, specify the type of chart you wish to generate that provides details on the number of hits within a designated time period. A “hit” is any page and/or object an end user accesses as the result of entering a URL in his/her browser window.

1. Specify the time period for the chart you wish to draw by doing the following:

   a. Click the radio button corresponding to **Hits By Day**, **Hits By Week**, or **Hits By Month**.

   b. At the **From** and **To** fields, make a selection for the date range using the calendar icons:

   - Click the 📅 calendar icon to open the larger calendar for the current month, with today’s date highlighted.

__TIP__: To view the calendar for the previous month, click the left arrow. To view the calendar for the next month, click the right arrow.

   - Click the date to select it and to close the calendar pop-up window. This action populates the field to the left of the calendar icon with the selected date.

2. Click the **Draw Chart** button to open a window that displays the chart of your selection in the PDF file format.

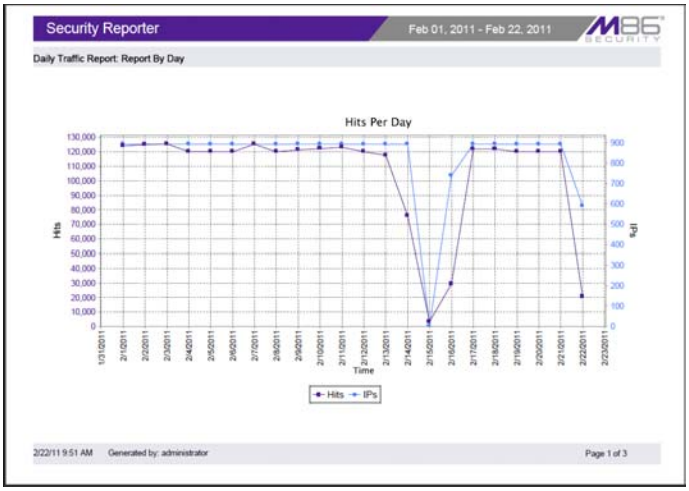
   The header section includes the title of the chart and date range. The footer section includes the date and time the chart was generated (shown in the MM/DD/YYYY HH:MM AM/PM format), the login ID of the person who generated the chart (Generated by) and the Page number and page range.

   The chart image includes a graph illustrating the general Number of Hits (in purple) and Number of IPs that generated those hits (in blue) for each unit of Time in the specified period.

Rows of report details indicate the time measurement (Day, Week, or Month), the exact Number of Hits corresponding to each unit of time, and the Total Records.

Depending on the time frame specified, this chart may be several pages in length.

- **Hits Per Day** - If you selected Hits By Day, days within the date range are plotted on the graph, grouped into equal time intervals. The summary shows the Number of Hits (in purple) and Number of IPs (in blue) for a specified Day (MM/DD/YYYY).



Security Reporter

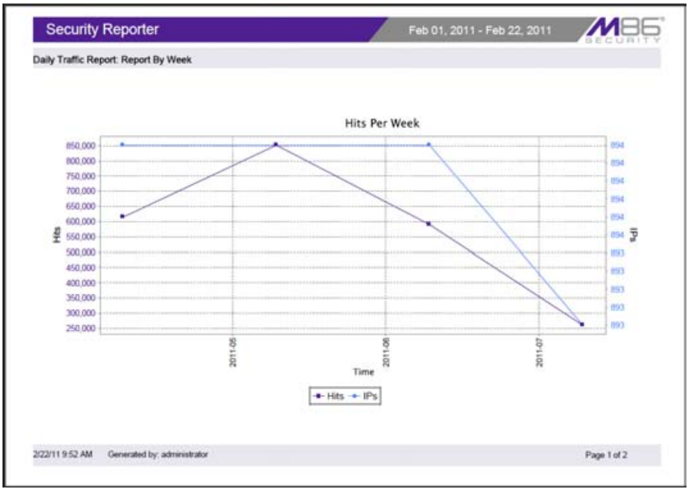
Feb 01, 2011 - Feb 22, 2011

Daily Traffic Report: Report By Day

2/22/11 9:51 AM Generated by: administrator Page 1 of 3

Fig. 3:2-21 Hits Per Day chart

- **Hits Per Week** - If you selected Hits By Week, each week within the date range is plotted on the graph. The summary shows the general Number of Hits (in purple) and Number of IPs that generated those hits (in blue) for a specified Week (YYYY-WW). Weeks are numbered 01-52. For example, 2011-05 indicates the fifth week in the year 2011—or the first week of February 2011, which included days 1-5.



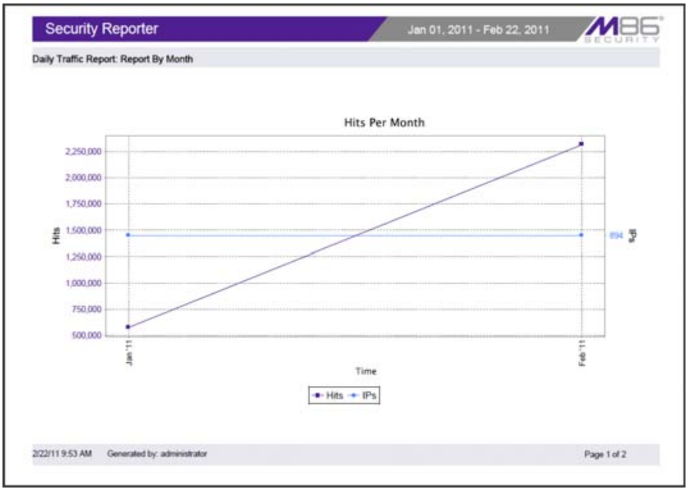
Security Reporter   Feb 01, 2011 - Feb 22, 2011

Daily Traffic Report: Report By Week

2/22/11 9:52 AM   Generated by: administrator   Page 1 of 2

Fig. 3:2-22 Hits Per Week chart

- **Hits Per Month -** If you selected Hits By Month, each month within the date range is plotted on the graph. The summary shows the general Number of Hits (in purple) and Number of IPs that generated those hits (in blue) for a specified Month (Month ’YY). Month names are abbreviated.



Security Reporter   Jan 01, 2011 - Feb 22, 2011

Daily Traffic Report: Report By Month

2/22/11 9:53 AM   Generated by: administrator   Page 1 of 2

Fig. 3:2-23 Hits Per Month chart

3. You now have the option to do any of the following:

   - print the chart - click the print 🖶 icon to open the Print dialog box, and proceed with standard print procedures.

   - save the chart - click the save 💾 icon to open the Save a Copy dialog box, and proceed with standard save procedures.
   - close the chart window - click the “X” in the upper right corner to close the chart window.
   - generate a new chart - make new entries in the Server Information panel.

Expiration Info

In the Expiration Info section, the following data displays:

- **Data Space Utilization** - The percentage of database storage space currently being used on the SR. Beneath this line is a colored bar depicting the percentage of data "Used" (purple) and "Free" (grey). A key displays beneath the colored bar to indicate the percentage of data both "Used" and "Free", and "Total" data percentage.
- **Weeks until next expiration** - The number of weeks from this week that data on the SR will expire.

***NOTE**: If using the SR in evaluation mode, the text "(IF REGISTERED)" is included in the label to indicate the number of weeks of data that would be stored on the SR if the server was activated and running in registered mode. (See Registered Mode and Evaluation Mode in this sub-section.)*

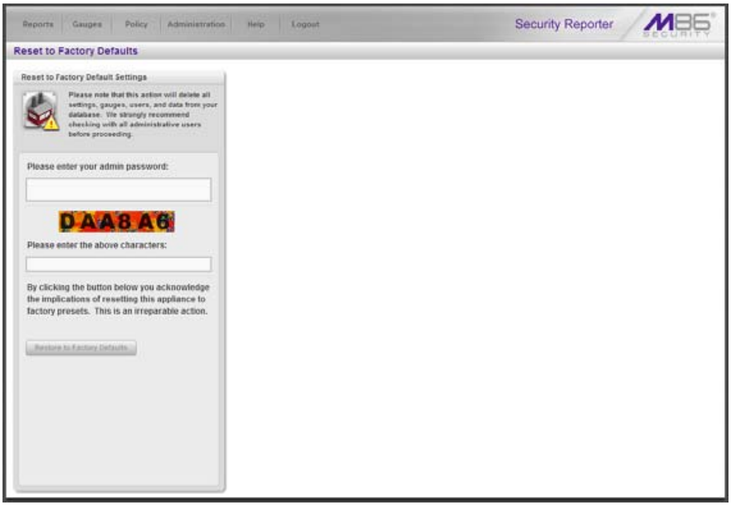
- **Estimated date of next expiration** - the date scheduled for the next automatic database expiration (MM/DD/YYYY format).

***NOTE**: If using the SR in evaluation mode, the text "(IF REGISTERED)" is included in the label to indicate the number of weeks of data that would be stored on the SR if the server was activated and running in registered mode. (See Registered Mode and Evaluation Mode in this sub-section.)*

Reset to Factory Defaults panel

The global administrator uses the Reset to Factory Defaults panel, if necessary, to restore the SR to default settings for the current software update level of the application.

In the navigation toolbar, mouse over the Administration menu link and select **Reset to Factory Defaults** to display the Reset to Factory Defaults panel:



Reset to Factory Defaults

Reset to Factory Default Settings

Please note that this action will delete all settings, gauges, users, and data from your database. We strongly recommend checking with all administrative users before proceeding.

Please enter your admin password:

DAA8A6

Please enter the above characters:

By clicking the button below you acknowledge the implications of resetting this appliance to factory presets. This is an irreparable action.

Fig. 3:2-24 Reset to Factory Defaults panel

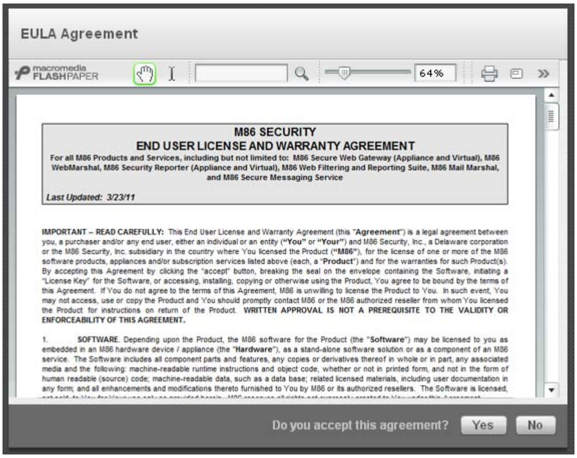
WARNING: *When using this option, all settings made to the SR—including administrator, group, and real time gauge configuration settings and alerts—will be purged and cannot be restored. The SR will also be set to evaluation mode.*

Reset to Factory Default Settings frame

1. In the Reset to Factory Default Settings panel, **Please enter your admin password** that was created during the SR wizard hardware installation process.

2. Beneath the security characters, **Please enter the above characters**.

3. Click **Restore to Factory Defaults** to reset the SR application and to display the SR's End User License Agreement window:



EULA Agreement

M86 SECURITY
END USER LICENSE AND WARRANTY AGREEMENT
For all M86 Products and Services, including but not limited to: M86 Secure Web Gateway (Appliance and Virtual), M86 WebMarshal, M86 Security Reporter (Appliance and Virtual), M86 Web Filtering and Reporting Suite, M86 Mail Marshal, and M86 Secure Messaging Service

Last Updated: 3/23/11

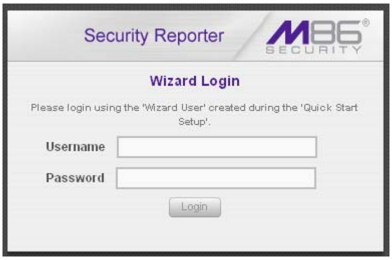
IMPORTANT – READ CAREFULLY: This End User License and Warranty Agreement (this "**Agreement**") is a legal agreement between you, a purchaser and/or any end user, either an individual or an entity (**"You"** or **"Your"**) and M86 Security, Inc., a Delaware corporation or the M86 Security, Inc. subsidiary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

1. **SOFTWARE**. Depending upon the Product, the M86 software for the Product (the "**Software**") may be licensed to you as embedded in an M86 hardware device / appliance (the "**Hardware**"), as a stand-alone software solution or as a component of an M86 service. The Software includes all component parts and features, any copies or derivatives thereof in whole or in part, any associated media and the following: machine-readable runtime instructions and object code, whether or not in printed form, and not in the form of human readable (source) code; machine-readable data, such as a data base; related licensed materials, including user documentation in any form; and all enhancements and modifications thereto furnished to You by M86 or its authorized resellers. The Software is licensed,

Do you accept this agreement?

Fig. 3:2-25 End User License Agreement

4. After reading the contents of the EULA, click **Yes** to accept it and to go to the Wizard Login window:



Wizard Login

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

Username

Password

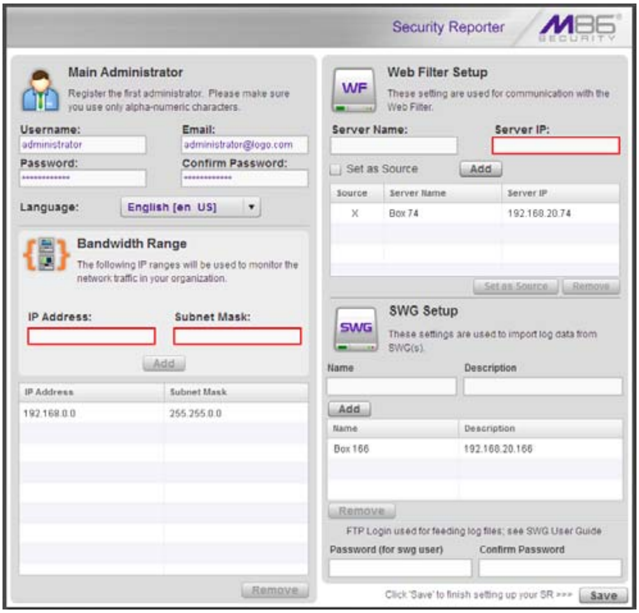
Fig. 3:2-26 Wizard Login window

Wizard panel

1. In the Wizard Login window, type in the **Username** created during the wizard hardware installation process.

2. Type in the **Password** created for the Username during the wizard hardware installation process.

3. Click **Login** to display the wizard panel:



Main Administrator

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

Username: administrator

Email: administrator@logo.com

Password: ************

Confirm Password: ************

Language: English [en US]

Bandwidth Range

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

IP Address:

Subnet Mask:

IP Address	Subnet Mask
192.168.0.0	255.255.0.0

Web Filter Setup

These setting are used for communication with the Web Filter.

Server Name:

Server IP:

□ Set as Source

Source	Server Name	Server IP
X	Box 74	192.168.20.74

SWG Setup

These settings are used to import log data from SWG(s).

Name

Description

Name	Description
Box 166	192.168.20.166

FTP Login used for feeding log files; see SWG User Guide

Password (for swg user)

Confirm Password

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

Fig. 3:2-27 Wizard panel

Main Administrator

1. In the Main Administrator section, type in the following information: **Username**, **Email** address, **Password**, **Confirm Password**.

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

2. 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.*

***TIP**: The Language setting field is also available in the Admin Profiles panel, accessible to each administrator and sub-administrator. See Admin Profiles panel in Chapter 1 of this Section for information about making Language setting changes.*

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

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, as described in the Device Registry panel sub-section of this chapter.*

1. In the Bandwidth Range section, type in the **IP Address** and **Subnet Mask**, and then click **Add** to include the bandwidth IP address range in the list box below.

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

2. In the Web Filter Setup section type in the **Server Name** and **Server IP** address, indicate if this Web Filter will be **Set as Source**, and then click **Add** to include the server criteria in the list box below.

***TIPS**: To add another Web Filter, follow the instructions in step 6 above. To remove a Web Filter from the list box, select it and then click **Remove**. To make a Web Filter the Source server—if no Web Filter in the list has yet been specified as the Source server, or if the IP address of the Source server has changed—select the Web Filter from the list box and then click **Set as Source**.*

SWG Setup

***NOTE**: SWG 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, as described in the Device Registry panel sub-section of this chapter.*

1. In the SWG Setup section, type in the **Name** and/or **Description** for the SWG, and then 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**.*

2. 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, as explained in the SWG's Management Console Reference Guide.*

Save Entries

Click **Save** to save your entries and to go to the SR login window:

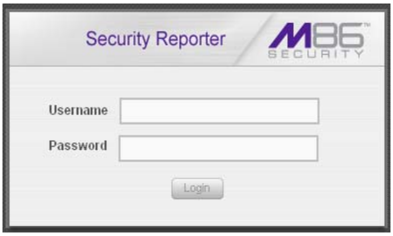


Fig. 3:2-28 SR Login window

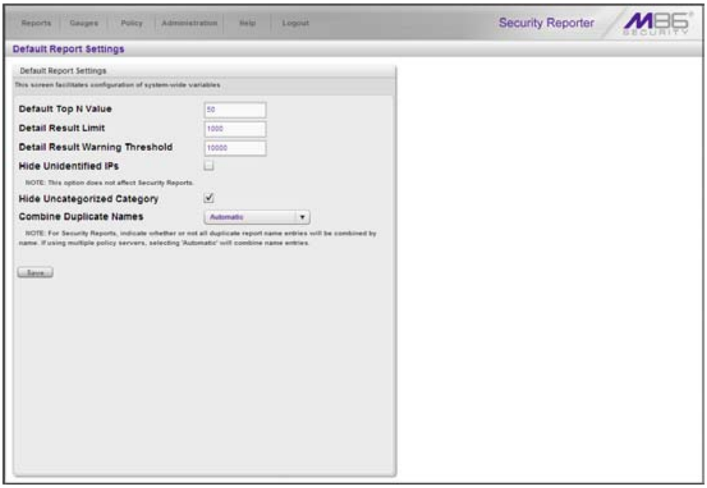
Chapter 3: Report Configuration

The following panels from the Administration menu of the Report Manager are described in this chapter: Default Report Settings, and Custom Category Groups.

Default Report Settings panel

The global administrator uses the Default Report Settings panel for specifying various settings to be used in reports.

In the navigation toolbar, mouse over the Administration menu link and select **Default Report Settings** to display the Default Report Settings panel:



Default Report Settings

This screen facilitates configuration of system-wide variables

Default Top N Value: 50

Detail Result Limit: 1000

Detail Result Warning Threshold: 10000

Hide Unidentified IPs □

NOTE: This option does not affect Security Reports.

Hide Uncategorized Category ☑

Combine Duplicate Names: Automatic

NOTE: For Security Reports, indicate whether or not all duplicate report name entries will be combined by name. If using multiple policy servers, selecting 'Automatic' will combine name entries.

Fig. 3:3-1 Default Report Settings panel

Set New Defaults

1. Enter the **Default Top N Value** of records that will be generated for summary reports. The default is “50” records.
2. Enter the maximum number of records that will be included in a detail report’s **Detail Result Limit**. If the number of records from a query exceeds the limit established in this field, the overflow will be included in the next set of records. The default is “1000” records per set.
3. Enter the maximum number of records that can be returned by a detail report query before triggering the **Detail Result Warning Threshold** message. This warning message indicates that the number of records exceeds the number specified in this field. The default is “10000” records.
4. By default, the **Hide Unidentified IPs** checkbox is de-selected. This feature for Web Filters only indicates that activity on machines not assigned to specific users will be included in reports.

   If you wish to exclude activity from machines not assigned to specific users, click in the checkbox to enter a check mark.
5. If using a Web Filter with this SR being configured, the **Hide Uncategorized Category** checkbox displays and is selected by default. This indicates that uncategorized sites will not be displayed or counted in drill down reports.

   If you wish to include uncategorized sites in drill down reports, click in the checkbox to remove the check mark.
6. If using one or more SWG policy servers with this SR being configured, make a selection from the **Combine Duplicate Names** pull-down menu:

- Automatic - This default selection indicates that duplicate name entries found in SWG log feeds will be combined under one record entry in the generated security report, whether from one SWG or multiple policy servers.
- Force combination - This selection indicates that duplicate name entries from log feeds of all SWGs collectively will be combined under one record entry in the generated report.
- Do not combine names - This selection indicates that duplicate name entries from log feeds of all SWGs collectively will remain as separate record entries in the generated report.

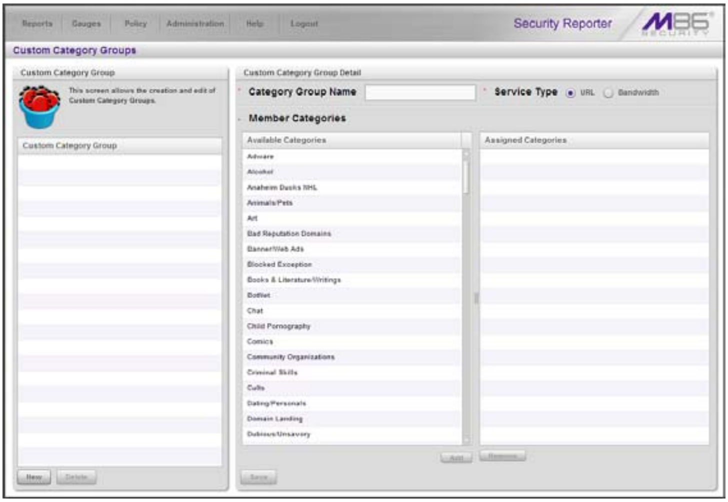
***TIP**: Click Cancel to exit without saving your entries.*

7. Click the **Save** button to save your settings in the Default Report Settings panel.

Custom Category Groups panel

The Custom Category Groups option is used for defining a customized group of filter categories or ports, if you wish to run reports only using certain filter categories or ports.

In the navigation toolbar, mouse over the Administration menu link and select **Custom Category Groups** to display the Custom Category Groups panel:



This screen allows the creation and edit of Custom Category Groups.

Custom Category Group

* Category Group Name

* Service Type ● URL ○ Bandwidth

Member Categories

Available Categories

Adware
Alcohol
Anaheim Ducks NHL
Animals/Pets
Art
Bad Reputation Domains
Banner/Web Ads
Blocked Exception
Books & Literature/Writings
BotNet
Chat
Child Pornography
Comics
Community Organizations
Criminal Skills
Cults
Dating/Personals
Domain Landing
Dubious/Unsavory

Assigned Categories

Fig. 3:3-2 Custom Category Groups panel

The Custom Category Groups panel is comprised of two frames used for setting up and maintaining category groups: Custom Category Group, and Custom Category Group Detail.

Add a Custom Category Group

1. At the bottom of the Custom Category Group frame, click **Add**.
2. In the Custom Category Group Detail frame, type in the **Category Group Name**.
3. Specify the **Service Type** to use: “URL” or “Bandwidth”.
4. Include the following **Member Categories** based on the Service Type selection:
   - URL - Select Available Categories from the list and click **Add >** to move the selection(s) to the Assigned Categories list box.
   - Bandwidth - In the **Port Number** field, type in a specific value in the pre-populated field, and/or use the up/ down arrow buttons to increment/decrement the current value by one, and then click **Add Port >** to move the selection to the Assigned Ports list box.

***NOTE**: At least one library category/protocol/port must be selected when creating a gauge. The maximum number of library categories/ports that can be selected/added is 15.*

***TIP**: To remove one or more library categories or ports from the Assigned Categories/Ports list box, make your selection(s), and then click Remove to remove the selection(s).*

5. Click **Save** to save your settings and to include the name of the group you added in the Custom Category Group list.

Modify a Custom Category Group

1. Select the Custom Category Group name from the list box by clicking on your choice to highlight it.
2. Make your edits:
   - To modify the Custom Category Group name, edit the **Category Group Name** in the Custom Category Group Detail frame.
   - To update the assigned selections in the list box, select the item to select it, and then click **Remove** to remove it.
3. Click **Update** to save your modification(s).

Delete a Category Group

1. Select the Custom Category Group name from the list box by clicking on your choice to highlight it.
2. Click **Delete** to remove the Custom Category Group name from the list box.

PRODUCTIVITY REPORTS SECTION

Introduction

This section of the user guide provides instructions to administrators on how to utilize the Report Manager to generate productivity report views and interpret results, whether using a Web Filter and/or SWG appliance.

Reports unique to environments that only use a Web Filter are addressed in the Real Time Reports Section. Reports unique to environments that only use an SWG are addressed in the Security Reports Section.

For Web Filter and SWG environments, the Reports menu consists of the following options described in these chapters:

- Chapter 1: A High Level Overview - This chapter shows you how to view productivity report data in the Dashboard, canned Summary Reports, and Sample Reports that provide a high level overview of end user Internet and network activity.
- Chapter 2: Drill Down Reports - This chapter provides instructions on using tools to generate summary and detail Drill Down Reports that give you more information on specific end user activity.
- Chapter 3: Customize, Maintain Reports - This chapter tells you how to generate customized reports using the Report Wizard, maintain Saved Reports for ongoing usage, and set up a Report Schedule for running reports on a regular basis.
- Chapter 4: Specialized Reports - This chapter informs you of three specialized types of reports you can generate: Executive Internet Usage Summary Reports, Blocked Request Reports, and Time Usage Reports.

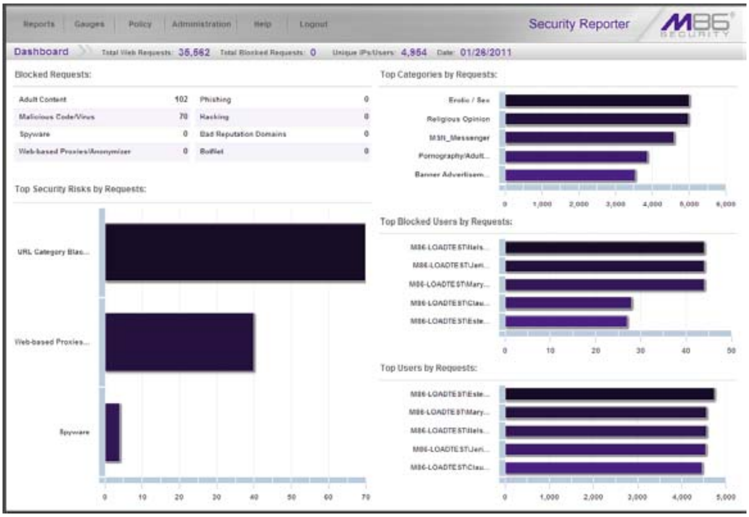
Chapter 1: A High Level Overview

The following productivity reporting topics from the Reports menu of the Report Manager are described in this chapter: Dashboard, Summary Reports, and Sample Reports. These tools give you a high level overview of how end users are currently using the Internet and network resources.

Dashboard

The Dashboard provides statistics and bar charts depicting the top end user requests in various productivity report categories.

The Dashboard displays by selecting **Reports > Dashboard** in the navigation toolbar:



Dashboard Total Web Requests: 35,562 Total Blocked Requests: 0 Unique IPs/Users: 4,954 Date: 01/28/2011

Blocked Requests:

Adult Content	102	Phishing	0
Malicious Code/Virus	70	Hacking	0
Spyware	0	Bad Reputation Domains	0
Web-based Proxies/Anonymizer	0	BotNet	0

Fig. 4:1-1 Dashboard panel

***NOTE**: If using both a Web Filter and an SWG, only Web Filter log results display.*

At the top of the panel, the following information displays for the current period: Total Web Requests, Total Blocked

Requests, Unique IPs/Users, and Date (MM/DD/YYYY format).

The following information displays in the center of the panel:

- **Blocked Requests** - Top eight blocked library categories requested by end users, and the corresponding number of end user requests.
- **Top Categories by Requests** - Top five requested library categories and a bar chart depicting the number of end user requests.
- **Top Security Risks by Requests** - Top five requested Security group library categories and a bar chart depicting the number of end user requests.
- **Top Blocked Users by Requests** - Top five end users with blocked library category requests and a bar chart depicting the number of these end user requests.
- **Top Users by Requests** - Top five end users with library category requests and a bar chart depicting the number of these end user requests.

TIP*: Mouse over each bar in the bar graph to view the name of graph entry and number of requests for that entry.*

Once you have a high level overview of end user productivity report activity on the network, you can use productivity reports to obtain more information about specific end user trends and activity.

Summary Reports

Summary Reports are "canned" productivity reports that use pre-generated data to display bar charts or pie charts of end user Internet/network activity for a specified report type within a designated period of time prior to today.

Summary Reports are available to group administrators assigned the privilege to access the **Reports > Summary Reports** menu selection. By default, yesterday's report view showing the Top 20 Users by Blocked Request displays in the panel:

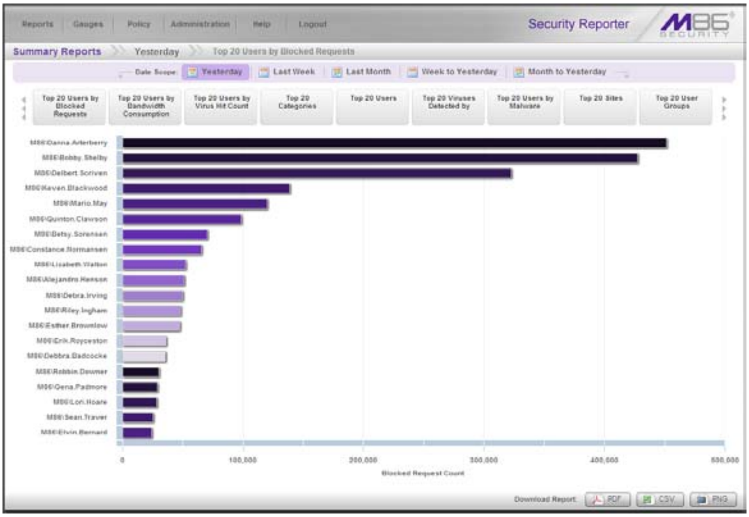


Fig. 4:1-2 Yesterday's Top 20 Users by Blocked Requests Report

***NOTES**: On a newly installed SR unit, the panel will not show any thumbnail images or bar chart report. If there was no activity for a given report type, the message "No Data to display." displays in the panel.*

If the Blocked Requests Report feature is disabled in System Configuration > Database > Optional Features > Blocked Request Count frame, yesterday's Top 20 Categories report view displays by default instead.

***TIPS**: Click the left arrows or right arrows at the edges of the dashboard to display thumbnail images that are currently hidden. Click the tab for the specified time period (Yesterday, Last Week, Last Month, Week to Yesterday, Month to Yesterday) to change the Date Scope. Mouse over each bar in the bar graph to view the name of graph entry and number of requests for that entry.*

Summary Report types

Available Summary Reports are as follows by clicking the thumbnail for the corresponding report type:

- **Top 20 Users by Blocked Requests** - Bar chart report depicting each top end user's total Page Count for Blocked and Warn Blocked requests. If using a Web Filter only, this report is available if the Block Request Count feature is enabled in the Optional Features screen in the System Configuration administrator console.
- **Top 20 Users by Bandwidth Consumption** (for SWG only environments) - Bar chart depicting each top end user's total Mega Bytes for bandwidth requests.

***NOTE**: The thumbnail for this report will not display in any environment with a Web Filter.*

- **Top 20 Users by Virus Hit Count** (for SWG) - Bar chart report depicting each top end user's total Virus Count (both Blocked and Permitted) detected by the anti-virus engine.
- **Top 20 Categories** - Bar chart report depicting the total Page Count in the top requested filtering library categories.
- **Top 20 Users** - Bar chart report depicting each top end user's total Page Count.
- **Top 20 Viruses Detected by** (for SWG) - Bar chart report depicting the top viruses and Virus Count detected by the anti-virus engine.

- **Top 20 Users by Malware** - Bar chart report depicting each top end user’s total “Blocked” and “Permitted” Hit Count from the following categories in the Security, Internet Productivity, and Internet Communication (Instant Messaging) category groups: BotNet, Malicious Code/Virus, Bad Reputation Domains, Spyware, Adware, and IRC.

***NOTE**: For SWG users, results that display in the Top 20 Users by Malware report reflect library contents mapped to the M86 Supplied Categories.*

- **Top 20 Sites** - Bar chart report depicting the total Page Count for the most popular sites accessed by end users.
- **Top 20 User Groups** - Bar chart report depicting the total Page Count for the top scoring user groups.
- **Top 20 Blocked Searched Keywords** - Bar chart report depicting the total blocked keyword requests Page Count. For Web Filter users, this report is only available if the Block Searched Keywords Report feature is enabled in the Optional Features screen in the System Configuration administrator console.
- **Total Permitted vs. Blocked Requests** - Pie chart report depicting the total Page Count for all filtering categories Permitted to pass and all filtering categories set up to be Blocked.
- **Category Group Comparison** - Pie chart report depicting the total Page Count in each top scoring filtering category group.
- **Category Comparison** - Pie chart report depicting the total Page Count in each top scoring filtering category.
- **User Group Comparison** - Pie chart report depicting the total Page Count in each top scoring user group.

Modify the Summary Report view

The report view displays either a bar chart or pie chart graph based on the selected report type.

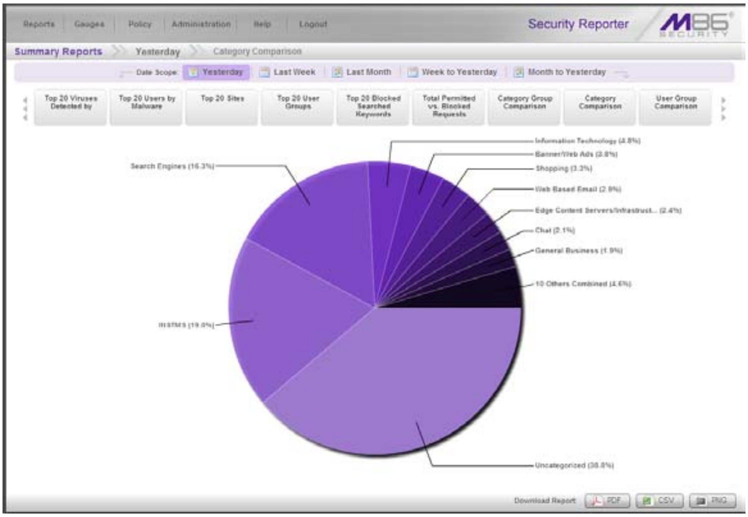


Fig. 4:1-3 Yesterday’s Category Comparison Report

Use any the following tools to modify the report view:

- **Date Scope** - Click one of these tabs at the top of the panel to display data for another period: Yesterday (default), Last Week, Last Month, Week to Yesterday, or Month to Yesterday
- Report type thumbnails - Click one of the report type thumbnails beneath the Date Scope to display that report view.

***TIP**: Click the left arrows or right arrows at the edges of the dashboard to display thumbnail images that are currently hidden.*

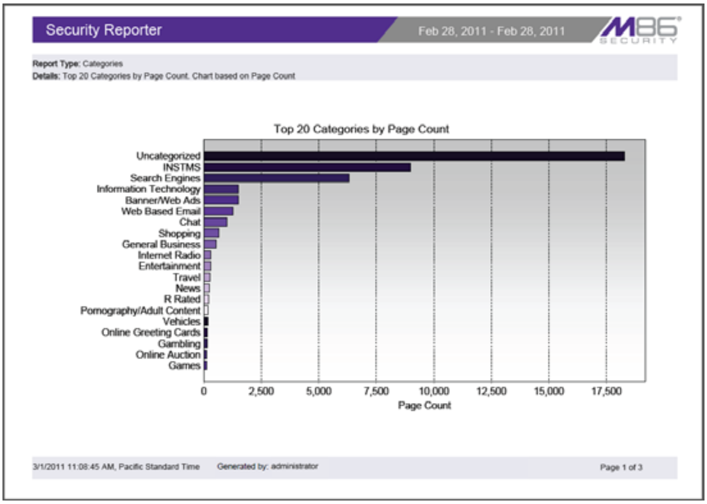
Download, Export a Summary Report

At the bottom of the report view, click a **Download Report** option for PDF, CSV, or PNG to generate a report in the specified file format (.pdf, .csv, or .png).

PDF format

Download the report in the PDF format

Clicking the **PDF** button opens a separate browser window containing the Summary Report in the .pdf format:



Security Reporter

Feb 28, 2011 - Feb 28, 2011

Report Type: Categories
Details: Top 20 Categories by Page Count. Chart based on Page Count

3/1/2011 11:08:45 AM, Pacific Standard Time Generated by: administrator Page 1 of 3

Fig. 4:1-4 Sample Summary Report in the PDF format

The header of the generated report includes the date range, Report Type, and Details criteria.

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

The body of the first page of the report includes the following information:

- Bar chart - Name of category, username, username path, URL or site IP address, user group name, or blocked user request, and corresponding bar graph. Beneath the bar graph are count indicators and a label describing the type of Count used in the report.
- Pie chart - Color-coded pie graph showing a maximum of 15 categories or user groups. Any categories or user groups with page counts totalling less than one percent are grouped together under the “Others Combined” label.

The body of the pages following the first page of the bar or pie chart report includes the following information:

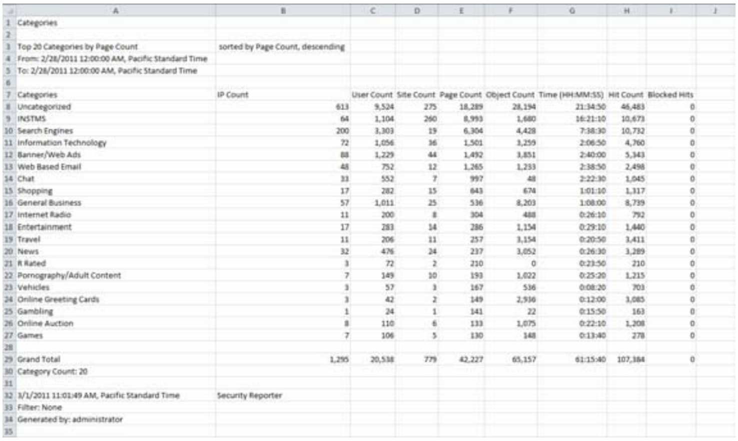
- Top 20 Users by Blocked Request report - User NAME and corresponding BLOCKED REQUEST COUNT—which includes Blocked and Warn Blocked requests. Total Records and Total Number of Blocked Requests for this Date Scope display at the end of the report.
- Top 20 Blocked Searched Keywords report - Blocked Keywords and corresponding Blocked Count. A Grand Total of Blocked Count displays at the end of the report.
- All other reports - Count columns and corresponding totals for all reports. Grand Total and Count display at the end of the report.

The report can be exported by printing it or saving it to your machine.

CSV format

Download the report in the CSV format

Clicking the **CSV** button opens a separate browser window containing the Summary Report in the .csv format:



	A	B	C	D	E	F	G	H	I	J
1	Categories									
2										
3	Top 20 Categories by Page Count	sorted by Page Count, descending								
4	From: 2/28/2011 12:00:00 AM, Pacific Standard Time									
5	To: 2/28/2011 12:00:00 AM, Pacific Standard Time									
6										
7	Categories	IP Count	User Count	Site Count	Page Count	Object Count	Time (HH:MM:SS)	Hit Count	Blocked Hits	
8	Uncategorized	613	9,524	275	18,289	28,194	21:34:50	46,483	0	
9	INSTMS	64	1,104	260	8,993	1,680	16:21:10	10,673	0	
10	Search Engines	200	3,303	19	6,304	4,428	7:38:30	10,732	0	
11	Information Technology	72	1,056	36	1,501	3,259	2:06:50	4,760	0	
12	Banner/Web Ads	88	1,229	44	1,492	3,851	2:40:00	5,343	0	
13	Web Based Email	48	752	12	1,265	1,233	2:38:50	2,498	0	
14	Chat	33	552	7	997	48	2:22:30	1,045	0	
15	Shopping	17	282	15	643	674	1:01:10	1,317	0	
16	General Business	57	1,011	25	536	8,203	1:08:00	8,739	0	
17	Internet Radio	11	200	8	304	488	0:26:10	792	0	
18	Entertainment	17	283	14	286	1,154	0:29:10	1,440	0	
19	Travel	11	206	11	257	3,154	0:20:50	3,411	0	
20	News	32	476	24	237	3,052	0:26:30	3,289	0	
21	R Rated	3	72	2	210	0	0:23:50	210	0	
22	Pornography/Adult Content	7	149	10	193	1,022	0:25:20	1,215	0	
23	Vehicles	3	57	3	167	536	0:08:20	703	0	
24	Online Greeting Cards	3	42	2	149	2,936	0:12:00	3,085	0	
25	Gambling	1	24	1	141	22	0:15:50	163	0	
26	Online Auction	8	110	6	133	1,075	0:22:10	1,208	0	
27	Games	7	106	5	130	148	0:13:40	278	0	
28										
29	Grand Total	1,295	20,538	779	42,227	65,157	61:15:40	107,384	0	
30	Category Count: 20									
31										
32	3/1/2011 11:01:49 AM, Pacific Standard Time	Security Reporter								
33	Filter: None									
34	Generated by: administrator									
35										

Fig. 4:1-5 Sample Summary Report in the CSV format

The header of the generated report includes the Report Type, report description, sort criteria, From/To date and time range (MM/D/YYYY HH:MM:SS AM/PM format), and time zone for the reporting period and location.

The body of the report includes a row containing column labels, followed by rows of user data with values corresponding to each column.

The Grand Total and Counts display after the last row of user data.

The footer of the report includes the date, time, and time zone in which the report was generated (MM/D/YYYY HH:MM:SS AM/PM, time zone code), product name, Filter specifications, and the login ID of the user who generated the report (Generated by).

The report can be exported by printing it or saving it to your machine.

PNG format

Download the report in the PNG format

Clicking the **PNG** button opens a separate browser window containing the Summary Report in the .png format:

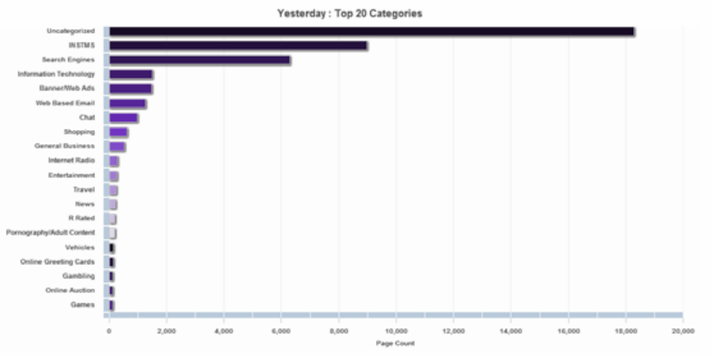


Fig. 4:1-6 Sample Summary Report in the PNG format

The generated report includes the report title followed by a graphical chart image:

- Bar chart - Name of category, username, username path, URL or site IP address, user group name, or blocked user request, and corresponding bar graph. Beneath the bar graph are count indicators and a label describing the type of Count used in the report.
- Pie chart - color-coded pie graph showing a maximum of 15 categories or user groups. Any categories or user groups with page counts totalling less than one percent are grouped together under the “Others Combined” label.

The report can be exported by printing it or saving it to your machine.

Sample Reports

Sample Reports are productivity reports in the PDF format that contain today's data for a specified reporting topic. These types of reports are accessible by navigating to **Reports > Sample Reports** and clicking one of the thumbnails in the panel:

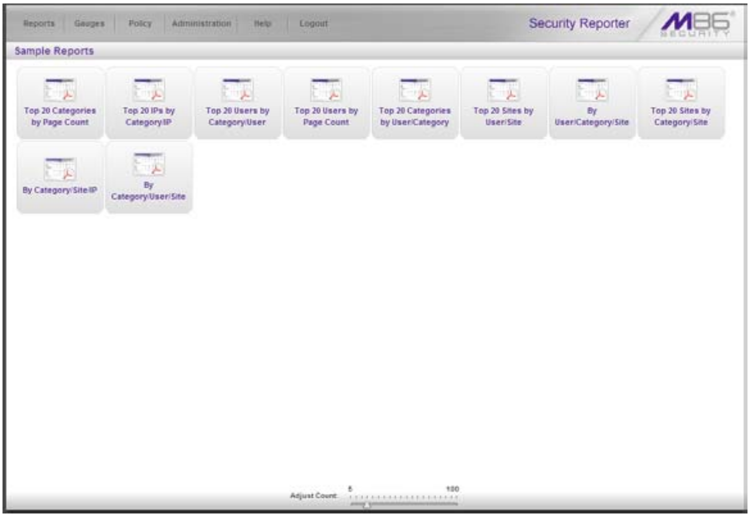

Reports
Gauges
Policy
Administration
Help
Logout
Security Reporter
M86 SECURITY
Sample Reports
Top 20 Categories by Page Count
Top 20 IPs by Category/IP
Top 20 Users by Category/User
Top 20 Users by Page Count
Top 20 Categories by User/Category
Top 20 Sites by User/Site
By User/Category/Site
Top 20 Sites by Category/Site
By Category/Site/IP
By Category/User/Site
Adjust Count:
5
100

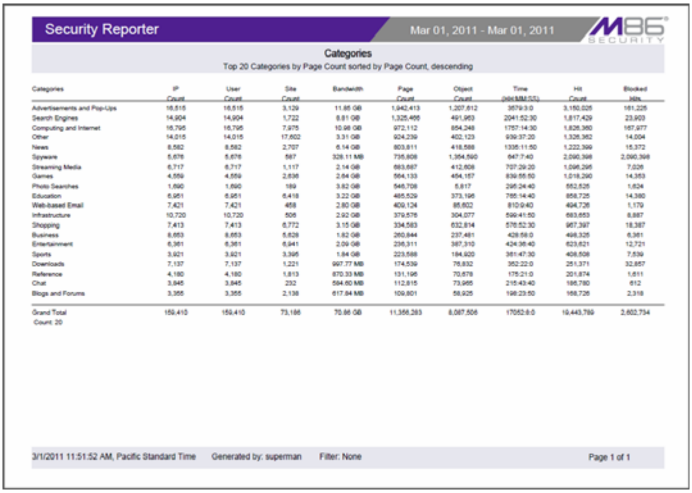
Fig. 4:1-7 Sample Reports

Sample Report types

Available Sample Report types are as follows:

- **Top 20 Categories by Page Count -** Top library categories end users accessed
- **Top 20 IPs by Category/IP** - Top end user IP addresses in each library category
- **Top 20 Users by Category/User -** Top usernames in each library category
- **Top 20 Users by Page Count -** Top end users who accessed library categories
- **Top 20 Categories by User/Category** - Top library categories each end user accessed
- **Top 20 Sites by User/Site -** Top sites each end user accessed
- **By User/Category/Site -** For each end user, the sites he/she visited in each library category
- **Top 20 Sites by Category/Site -** Top sites end users accessed in each library category
- **By Category/Site/IP -** For each library category, the sites end users accessed, and IP address of each end user
- **By Category/User/Site** - For each library category, the end users with activity in that library category, and the sites each end user accessed

View, Export a Sample Report



Security Reporter

Mar 01, 2011 - Mar 01, 2011

Categories

Top 20 Categories by Page Count sorted by Page Count, descending

Categories	IP Count	User Count	Site Count	Bandwidth	Page Count	Object Count	Time (HH:MM:SS)	Hit Count	Blocked Hits
Advertisements and Pop-Ups	16,515	16,515	3,129	11.85 GB	1,942,413	1,207,612	3679:3:0	3,150,026	161,226
Search Engines	14,904	14,904	1,722	8.81 GB	1,325,466	491,963	2041:52:30	1,817,429	23,903
Computing and Internet	16,795	16,795	7,975	10.98 GB	972,112	654,248	1757:14:30	1,826,360	167,977
Other	14,015	14,015	17,602	3.31 GB	924,239	402,123	939:37:20	1,326,362	14,004
News	8,582	8,582	2,707	6.14 GB	803,811	418,588	1336:11:50	1,222,399	15,372
Spyware	5,676	5,676	587	328.11 MB	735,808	1,354,590	647:7:40	2,090,398	2,090,398
Streaming Media	6,717	6,717	1,117	2.14 GB	683,687	412,608	707:29:20	1,096,295	7,026
Games	4,559	4,559	2,636	2.64 GB	564,133	454,157	839:55:50	1,018,290	14,353
Photo Searches	1,690	1,690	189	3.82 GB	546,708	5,817	295:24:40	552,525	1,624
Education	6,951	6,951	6,418	3.22 GB	485,529	373,196	785:14:40	858,725	14,380
Web-based Email	7,421	7,421	458	2.80 GB	409,124	85,602	810:9:40	494,726	1,179
Infrastructure	10,720	10,720	506	2.92 GB	379,576	304,077	599:41:50	683,653	8,887
Shopping	7,413	7,413	6,772	3.15 GB	334,583	632,814	576:52:30	967,397	18,387
Business	8,653	8,653	5,626	1.82 GB	260,844	237,481	428:58:0	498,325	6,361
Entertainment	6,361	6,361	6,941	2.09 GB	236,311	387,310	424:36:40	623,621	12,721
Sports	3,921	3,921	3,396	1.84 GB	223,588	184,920	361:47:30	408,508	7,539
Downloads	7,137	7,137	1,221	997.77 MB	174,539	76,832	352:22:0	251,371	32,857
Reference	4,180	4,180	1,813	870.33 MB	131,196	70,678	175:21:0	201,874	1,611
Chat	3,846	3,846	232	584.60 MB	112,815	73,965	215:43:40	186,780	612
Blogs and Forums	3,355	3,355	2,136	617.84 MB	109,801	58,925	198:23:50	168,726	2,318
Grand Total Count: 20	159,410	159,410	73,186	70.86 GB	11,358,283	8,087,506	17052:8:0	19,443,789	2,602,734

3/1/2011 11:51:52 AM, Pacific Standard Time   Generated by: superman   Filter: None   Page 1 of 1

Fig. 4:1-8 Sample Categories report

View Sample Report contents

The report header contains the following information: “Security Reporter” and date range for today’s date; report name; description for that report type, including the sort order and **Page Count, descending**

The body of the report contains rows of records and is comprised of one or more sections.

For each record, end user statistics display in columns such as: Category Count, IP Count, Site Count, Bandwidth (GB or MB amounts display for SWG only), Page Count, Object Count, Time (HH:MM:SS), Hit Count, and Blocked Hits.

Total counts display at the end of each section.

The Grand Total and total Count for all sections display at the end of the report.

The footer on each page contains the following information: today’s date (M/D/YYYY), time (HH:MM:SS AM/PM), and time zone in which the report was generated; **Generated by**: manager’s login ID; **Filter: None**; **Page** number and page range.

Export the Sample Report

PDF file window

1. From the open PDF file window, the Sample Report can be exported in some of the following ways:
   - print the report - click the print 🖨 icon to open the Print dialog box, and proceed with standard print procedures.
   - save the report - navigate to **File > Save a Copy** to open the Save a Copy dialog box, and proceed with standard save procedures.
2. Click the “X” in the upper right corner of the PDF file window to close it.

PDF opened in browser tab

1. From the open PDF in the browser window tab, the Sample Report can be exported in some of the following ways:
   - print the report - navigate to the **Print** selection to open the Print dialog box, and proceed with standard print procedures.
   - save the report - navigate to the **Save (Page) As...** selection to open the Save As window, and proceed with standard save procedures.
2. Click the “X” in the upper right corner of the tab to close it.

Chapter 2: Drill Down Reports

This chapter provides information about generating drill down productivity reports that let you query the database to access more detailed information about end user Internet activity.

The two basic productivity reports administrators can generate with customizations are the summary drill down report and the detail drill down report. Report views for these reports are executed via **Reports > Drill Down Reports** from the Report Manager user interface:

- **Categories** - Includes data in each filter category that was set up for monitoring user activity.
- **IPs** - Includes Internet activity by user IP address.
- **Users** - Includes Internet activity by username.
- **Sites** - Includes activity on Web sites users accessed.
- **Category Groups** - Includes activity by Category Groups.
- **User Groups** - Includes activity by User Groups.

NOTE*: The Report Wizard feature for drill down reports is discussed in detail in Chapter 3: Customize, Maintain Reports.*

Once you have generated a drill down report view, you can customize your view, save the view, export the view, and/or schedule the report to run at a designated time.

NOTE*: Before you begin generating report views for these reports, we recommend that you review this chapter in order to become familiar with the organization of these report views, and how report view tools and components are used in creating summary drill down reports and detail drill down reports customized to your specifications.*

Generate a Drill Down Report

To generate a drill down productivity report:

1. Choose one of the following topics from the **Reports > Drill Down Reports** menu for the type of summary drill down report you wish to view: Categories, IPs, Users, Sites, Category Groups, User Groups.

***NOTES**: As the report is generating, the "Processing..." message displays. After the report has finished being generated, if no records are available an alert box opens displaying the message "No records returned!"*

2. Once the generated summary drill down report has loaded in the panel, use the tools in the panel to create the desired drill down view.

***NOTE**: A detail drill down report view is generated by clicking a link in the Page Count or Object Count column corresponding to a specific record displayed in the current summary drill down report view.*

3. The drill down view can be exported, saved, modified and re-run, and/or scheduled to run at a specified time.

Summary Drill Down Report View

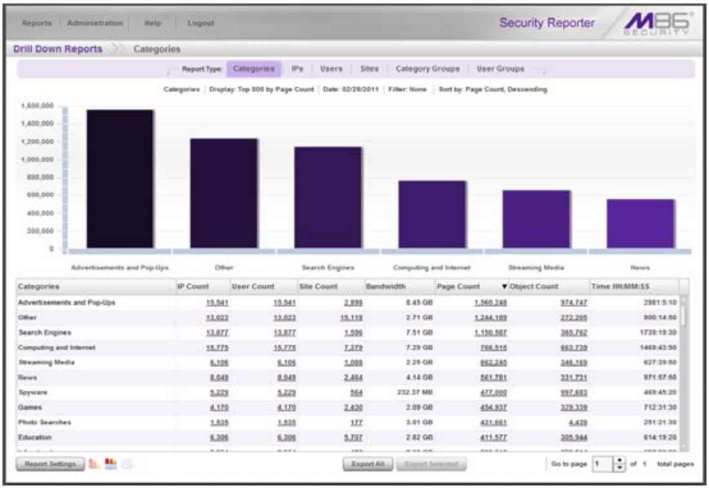
The summary drill down productivity report view provides a snapshot of end user activity for a specified report type and defined date of activity recorded by the SR.

For each report type, by default the top portion of the report view includes tabs for all productivity Report Types (Categories, IPs, Users, Sites, Category Groups, and User Groups). The following information displays beneath this row of tabs: report type, Display criteria, Date, Filter criteria, and Sort by criteria. Beneath this row, a bar chart depicts the first six records for the current report type.

***NOTE**: Mousing 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.



Categories | Display: Top 500 by Page Count | Date: 02/28/2011 | Filter: None | Sort by: Page Count, Descending

Categories	IP Count	User Count	Site Count	Bandwidth	Page Count ▼	Object Count	Time HH:MM:SS
Advertisements and Pop-Ups	15,541	15,541	2,898	8.45 GB	1,560,248	974,747	2981:5:10
Other	13,023	13,023	15,118	2.71 GB	1,244,189	272,205	800:14:50
Search Engines	13,877	13,877	1,596	7.51 GB	1,150,587	365,762	1739:19:30
Computing and Internet	15,775	15,775	7,279	7.29 GB	766,515	663,739	1469:43:50
Streaming Media	6,106	6,106	1,088	2.25 GB	662,245	346,169	627:39:50
News	8,049	8,049	2,464	4.14 GB	561,781	331,721	971:57:50
Spyware	5,229	5,229	564	232.37 MB	477,000	997,683	469:45:20
Games	4,170	4,170	2,420	2.09 GB	454,937	329,339	712:31:30
Photo Searches	1,535	1,535	177	3.01 GB	431,661	4,429	251:21:30
Education	6,306	6,306	5,707	2.82 GB	411,577	305,944	614:19:20

Go to page 1 of 1 total pages

Fig. 4:2-1 Default Summary Drill Down Report view

***TIP**: To refresh the current report view, select **Reports > Drill Down Reports** and choose the report type again.*

Summary Report View Tools and Tips

Report Type tabs

Report Type tabs let you generate another summary drill down report view by clicking that tab (Categories, IPs, Users, Sites, Category Groups, or User Groups).

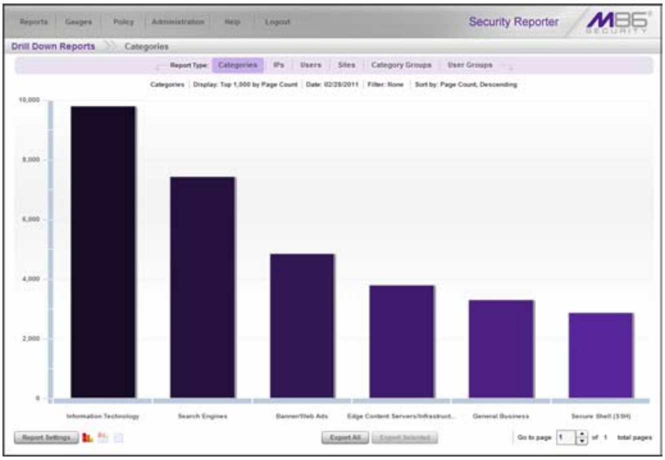
Summary Drill Down Report Settings menu

Mouse over **Report Settings** to display a menu of reporting options: Run, Save, Limit Detail Result (see Report View Navigation and Usage).

Report view option icons

Click the following report view icon to change the report view display:

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

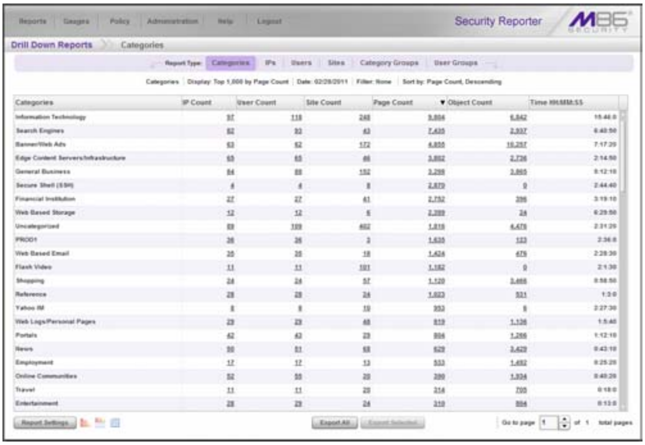


Categories | Display: Top 1,000 by Page Count | Date: 02/28/2011 | Filter: None | Sort by: Page Count, Descending

Fig. 4:2-2 Sample top six bars view

- Click this icon to display the top six bars and table of records (see Fig. 4:2-1).

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



Categories | Display: Top 1,000 by Page Count | Date: 02/28/2011 | Filter: None | Sort by: Page Count, Descending

Categories	IP Count	User Count	Site Count	Page Count ▼	Object Count	Time HH:MM:SS
Information Technology	97	118	248	9,804	6,842	15:46:0
Search Engines	82	93	43	7,435	2,937	6:40:50
Banner/Web Ads	63	62	172	4,855	16,257	7:17:20
Edge Content Servers/Infrastructure	65	65	46	3,802	2,736	2:14:50
General Business	84	88	152	3,298	3,865	8:12:10
Secure Shell (SSH)	4	4	8	2,879	0	2:44:40
Financial Institution	27	27	41	2,752	396	3:19:10
Web Based Storage	12	12	6	2,289	24	6:29:50
Uncategorized	89	109	402	1,819	4,478	2:31:20
PROD1	36	36	3	1,635	123	2:36:0
Web Based Email	35	35	18	1,424	476	2:28:30
Flash Video	11	11	101	1,182	0	2:1:30
Shopping	24	24	57	1,120	3,466	0:58:50
Reference	28	28	24	1,023	531	1:3:0
Yahoo IM	8	8	19	953	8	2:27:30
Web Logs/Personal Pages	29	29	48	819	1,136	1:5:40
Portals	42	43	29	804	1,266	1:12:10
News	50	51	68	629	3,429	0:43:10
Employment	17	17	13	553	1,492	0:25:20
Online Communities	52	55	20	390	1,934	0:40:20
Travel	11	11	20	214	705	0:18:0
Entertainment	28	29	24	310	894	0:13:0

Fig. 4:2-3 Sample records only view

Count columns and links

Count columns (Category Count, IP Count, User Count, Site Count, Page Count, Object Count) display after the column containing the record name. Clicking a specific link in a record's Count column gives more in-depth analysis on a given record displayed in the current view. Clicking a link in the Page Count or Object Count column generates a detail drill down report view.

- **Category Count -** Displays the number of categories a user has visited, or the number of categories included within a given site. It is possible for a site to be listed in more than one category, so even if a user has visited only one site, this column may count the user's visit in two or three categories.

- **IP Count** - Displays the number of sites or categories visited by the IP address for a user's machines.
- **User Count** - Displays the number of individuals who have visited a specific site or category.
- **Site Count** - Displays the number of sites a user has visited, or the number of sites in a category. This figure is based on the root name of the site. For example, if a user visits www.espn.com, www.msn.com, and www.fox-sports.com, that user will have visited three pages. If that same user additionally visits www.espn.com/scores, the total number of sites visited would still count as three—and not as four—because the latter page is on the original ESPN site that was already counted.
- **Page Count** - displays the total number of pages visited. A user may visit only one site, but visit 20 pages on that site. If a user visits a page with pop-up ads, these items would add to the page count. If a page has banner ads that link to other pages, these items also would factor into the page count. In categories that use a lot of pop-up ads—porn, gambling, and other related sites—the page count usually exceeds the number of objects per page.

  By clicking the link in this column, the detail report view displays data for all pages accessed, including hyperlinks to those pages.
- **Object Count** - displays the number of objects on a Web page. All images, graphics, multimedia items, and text items count as objects. The number of objects on a page is generally higher than the number of pages a user visits.

  However, if an advertisement or banner ad (an object on the page) is actually a page from another site, this item would not be classified as an object but as a page, since it comes from a different server.

By clicking the link in this column, the detail report view displays data for all objects accessed, including hyperlinks to those objects.

***NOTE**: If “Pages only” was specified in the Log Import Settings frame of the Optional Features screen in the System Configuration user interface, **all** records of objects accessed by end users will be lost for the time period in which this option was enabled. Even if there were objects accessed by end users during that time period, zeroes (“0”) will display in the Object Count column in the report. See the Optional Features sub-section of the System Configuration Section for information about Log Import Settings frame options.*

Bandwidth and Time columns

In a summary drill down report view, the Bandwidth and Time columns provide additional information about a record.

- **Bandwidth** - Displays the amount of bandwidth in GB or MB used for each record, if using an SWG only with this SR.

***NOTE**: The Bandwidth column does not display if a Web Filter is used with this SR—with or without an SWG.*

- **Time HH:MM:SS** - Displays the amount of time a user spent at a given site. Each page detected by a user’s machine adds to the count. If a browser window is opened to a certain page and left there for an extended time period, and that page is refreshed by either the user or a banner ad, the counter starts again and continues as long as Web activity is detected. If that Web page contains an active banner ad that refreshes the page every 10 to 30 seconds, a user could show an incredibly high page count and many minutes, even though only one page was opened by that user.

Column sorting tips

To sort summary report view records in ascending/ descending order by a specified column, click that column's header: Category Count, IP Count, User Count, Site Count, Bandwidth (for SWG only environments), Page Count, Object Count, or Time HH:MM:SS.

Click the same column header again to sort records for that column in the reverse order.

Click another column header to sort records by that specified column.

Summary Drill Down Record exportation

In a summary drill down report view, all records are selected for exportation by default. Clicking **Export All** opens the Export pop-up window in which you specify criteria for the report to be generated and distributed (see Export a Productivity Report).

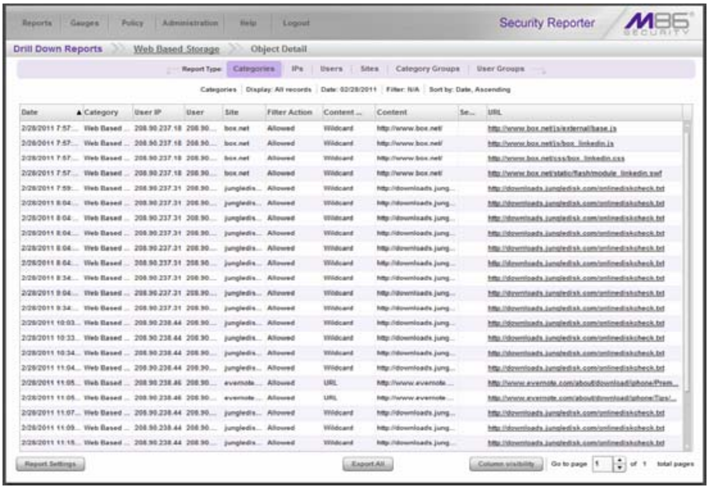
To select only specific records to export, click the first column of selected record rows in the table, and then click **Export Selected** to open the Export pop-up window (see Export a Productivity Report).

Other navigation tips

See Report View Navigation and Usage for information about navigating the current report view using breadcrumb trails and the **Go to page 'x' of 'x' total pages** field.

Detail Drill Down Report View

The detail drill down productivity report view provides information on pages or objects accessed by end users within a specific time period and is horizontally organized into a similar format as the summary drill down report view:



Categories | Display: All records | Date: 02/28/2011 | Filter: N/A | Sort by: Date, Ascending

Date	▲ Category	User IP	User	Site	Filter Action	Content ...	Content	Se...	URL
2/28/2011 7:57:...	Web Based ...	208.90.237.18	208.90....	box.net	Allowed	Wildcard	http://www.box.net/		http://www.box.net/js/external/base.js
2/28/2011 7:57:...	Web Based ...	208.90.237.18	208.90....	box.net	Allowed	Wildcard	http://www.box.net/		http://www.box.net/js/box_linkedin.js
2/28/2011 7:57:...	Web Based ...	208.90.237.18	208.90....	box.net	Allowed	Wildcard	http://www.box.net/		http://www.box.net/css/box_linkedin.css
2/28/2011 7:57:...	Web Based ...	208.90.237.18	208.90....	box.net	Allowed	Wildcard	http://www.box.net/		http://www.box.net/static/flash/module_linkedin.swf
2/28/2011 7:59:...	Web Based ...	208.90.237.31	208.90....	jungledis...	Allowed	Wildcard	http://downloads.jung...		http://downloads.jungledisk.com/onlinediskcheck.txt
2/28/2011 8:04:...	Web Based ...	208.90.237.31	208.90....	jungledis...	Allowed	Wildcard	http://downloads.jung...		http://downloads.jungledisk.com/onlinediskcheck.txt
2/28/2011 8:04:...	Web Based ...	208.90.237.31	208.90....	jungledis...	Allowed	Wildcard	http://downloads.jung...		http://downloads.jungledisk.com/onlinediskcheck.txt
2/28/2011 8:04:...	Web Based ...	208.90.237.31	208.90....	jungledis...	Allowed	Wildcard	http://downloads.jung...		http://downloads.jungledisk.com/onlinediskcheck.txt
2/28/2011 8:04:...	Web Based ...	208.90.237.31	208.90....	jungledis...	Allowed	Wildcard	http://downloads.jung...		http://downloads.jungledisk.com/onlinediskcheck.txt
2/28/2011 8:04:...	Web Based ...	208.90.237.31	208.90....	jungledis...	Allowed	Wildcard	http://downloads.jung...		http://downloads.jungledisk.com/onlinediskcheck.txt
2/28/2011 8:34:...	Web Based ...	208.90.237.31	208.90....	jungledis...	Allowed	Wildcard	http://downloads.jung...		http://downloads.jungledisk.com/onlinediskcheck.txt
2/28/2011 9:04:...	Web Based ...	208.90.237.31	208.90....	jungledis...	Allowed	Wildcard	http://downloads.jung...		http://downloads.jungledisk.com/onlinediskcheck.txt
2/28/2011 9:34:...	Web Based ...	208.90.237.31	208.90....	jungledis...	Allowed	Wildcard	http://downloads.jung...		http://downloads.jungledisk.com/onlinediskcheck.txt
2/28/2011 10:03...	Web Based ...	208.90.238.44	208.90....	jungledis...	Allowed	Wildcard	http://downloads.jung...		http://downloads.jungledisk.com/onlinediskcheck.txt
2/28/2011 10:33...	Web Based ...	208.90.238.44	208.90....	jungledis...	Allowed	Wildcard	http://downloads.jung...		http://downloads.jungledisk.com/onlinediskcheck.txt
2/28/2011 10:34...	Web Based ...	208.90.238.44	208.90....	jungledis...	Allowed	Wildcard	http://downloads.jung...		http://downloads.jungledisk.com/onlinediskcheck.txt
2/28/2011 11:04...	Web Based ...	208.90.238.44	208.90....	jungledis...	Allowed	Wildcard	http://downloads.jung...		http://downloads.jungledisk.com/onlinediskcheck.txt
2/28/2011 11:05...	Web Based ...	208.90.238.46	208.90....	evernote....	Allowed	URL	http://www.evernote....		http://www.evernote.com/about/download/iphone/Prem...
2/28/2011 11:05...	Web Based ...	208.90.238.46	208.90....	evernote....	Allowed	URL	http://www.evernote....		http://www.evernote.com/about/download/iphone/Tips/...
2/28/2011 11:07...	Web Based ...	208.90.238.44	208.90....	jungledis...	Allowed	Wildcard	http://downloads.jung...		http://downloads.jungledisk.com/onlinediskcheck.txt
2/28/2011 11:09...	Web Based ...	208.90.238.44	208.90....	jungledis...	Allowed	Wildcard	http://downloads.jung...		http://downloads.jungledisk.com/onlinediskcheck.txt
2/28/2011 11:15...	Web Based ...	208.90.238.44	208.90....	jungledis...	Allowed	Wildcard	http://downloads.jung...		http://downloads.jungledisk.com/onlinediskcheck.txt

Fig. 4:2-4 Detail Drill Down Report view

As in the summary drill down report view, the top portion of the detail drill down report view includes tabs for all productivity Report Types, followed by a row of criteria about the report view contents.

By default, the following columns display for each record in the table: Date, Category, User IP, User name, Site, Filter Action, and URL—as well as Content Type, Content criteria, and Search String for environments with a Web Filter. Any of these columns can be hidden by unchecking the corresponding title in the Column visibility checkbox.

The bottom portion of the report view panel includes tools for modifying the current report view, exporting, and/or saving the report.

Detail Report View Tools and Tips

Report Type tabs

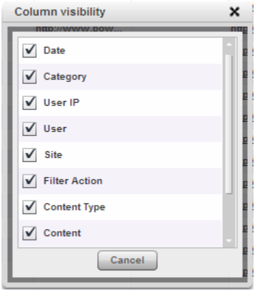
Report Type tabs let you generate a summary drill down report view by clicking that tab (Categories, IPs, Users, Sites, Category Groups, or User Groups).

Detail Drill Down Report Settings menu

Mouse over **Report Settings** to display a menu of reporting options: Run, Save (see Report View Navigation and Usage).

Page/Object Detail columns

By default all Page/Object Detail column(s) display. Any of these columns can be hidden from view by clicking the **Column visibility** button at the bottom of the panel to open the Column visibility pop-up window, and de-selecting the checkbox corresponding to that column:



Column visibility ✕

☑ Date
☑ Category
☑ User IP
☑ User
☑ Site
☑ Filter Action
☑ Content Type
☑ Content

Cancel

***TIP**: After making your modifications, click **Close** to close the Column visibility pop-up window.*

- **Date** - Displays the date in the M/D/YYYY H:M:S AM/PM format
- **Category** - Displays the category name (e.g. “Alcohol”).

- **User IP** - Displays the IP address of the user’s machine (e.g. “200.10.101.80”).
- **User** - Displays any of the following information: username, user IP address, or the path and username (e.g. “logo\admin\jsmith”).
- **Site** - Displays the URL the user attempted to access (e.g. “coors.com”).
- **Filter Action** - Displays the type of filter action used by the Web Filter in creating the record: "Allowed", "Blocked", "Warn Blocked" (for the first warning page that displayed for the end user), "Warn Allowed" (for any subsequent warning page that displayed for the end user), “Quota Blocked” (if a quota blocked the end user), "X-Strike", or "N/A" if the filter action was unclassified at the time the log file was created.
- **Content Type** (for Web Filter only environments) - Displays the method used by the Web Filter in creating the record: “Search KW” (Search Engine Keyword), “URL KW” (URL Keyword), “URL”, “Wildcard”, “Https High” (HTTPS Filtering Level set at High), “X-strike” (X Strikes Blocking), “Pattern” (Proxy Pattern Blocking), “File Type”, “Https Medium” (HTTPS Filtering Level set at Medium), or “N/A” if the content was unclassified at the time the log file was created.
- **Content** (for Web Filter only environments) - Displays criteria used for determining the categorization of the record, or “N/A” if unclassified.
- **Search String** (for Web Filter only environments) - Displays the full search string the end user typed into a search engine text box in search sites such as Google, Bing, Yahoo!, MSN, AOL, Ask.com, YouTube.com, and MySpace.com—if the Search Engine Reporting option is enabled in the Optional Features screen of the System Configuration administrator console user interface.

***NOTE**: Refer to the Optional Features screen sub-section of the System Configuration Section for information about the Search String feature.*

- **URL** - Displays the link for the page/object accessed by the end user.

Column sorting tips

To sort detail report view records in ascending/descending order by a specified column, click that column's header: Date, Category, User IP, User name, Site, Filter Action, Content Type, Content criteria, Search String, or URL.

***NOTE**: Content Type, Content, and Search String columns only display in environments using a Web Filter.*

Click the same column header again to sort records for that column in the reverse order.

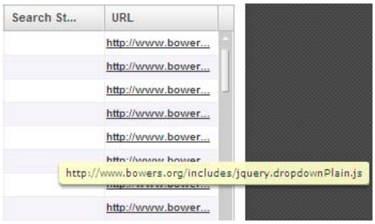
Click another column header to sort records by that specified column.

Page/Object viewing tip

Click the URL for a specified record to view the page or object currently indexed in the SR's memory.

Truncated data viewing tip

To view the entire text that displays truncated in a detail report view column, mouse over the column to view the entire string of data in the column for a given record:



Search St...	URL
	http://www.bower...
	http://www.bower...
	http://www.bower...
	http://www.bower...
	http://www.bower...
	http://www.bower
	[illegible]
	http://www.bower...

http://www.bowers.org/includes/jquery.dropdownPlain.js

Detail Drill Down Record exportation

In a detail drill down report view, all records are selected for exportation by default. Clicking **Export All** opens the Export pop-up window in which you specify criteria for the report to be generated and distributed (see Export a Productivity Report).

Other navigation tips

See Report Navigation and Usage for information about navigating the current report view using breadcrumb trails and the **Go to page ‘x’ of ‘x’ total pages** field.

Report View Navigation and Usage

Understanding how to use report view tools is paramount to generating a report containing relevant content, since the usage of these tools determines the results of your query.

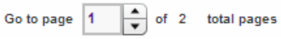
As you will learn from the rest of this chapter, report view tools along with report view components help you create the desired report view. This report view can then be exported, saved, and/or scheduled to run at a specified time.

Navigation Tips

Report view breadcrumb trail links

When generating a report view and modifying that report view to create another report view, a trail of breadcrumb links remain in the row beneath the navigation toolbar. Clicking a specified level in the trail link returns you to that prior report view.

Page navigation

At the bottom right of the panel, the **Go to page** field displays: 

Go to page 1 of 2 total pages

If more than one page of records displays for the total pages returned, enter a page number within that range to navigate to that page of records, or use the up/down arrow(s) to specify the page you want displayed.

Usage Tools

The bottom panel contains objects that let you customize, export, and/or save the current report view using pop-up boxes and/or panels accessible via the Report Settings menu and the Export button(s).

***NOTES**: Information on using the fields in these pop-up boxes or panels can be found in the Report View Components sub-section. Information on using the Export and Export All pop-up boxes can be found in the Export a Productivity Report sub-section, and information about Column visibility can be found in Detail Report View Tools and Tips.*

Report Settings menu options

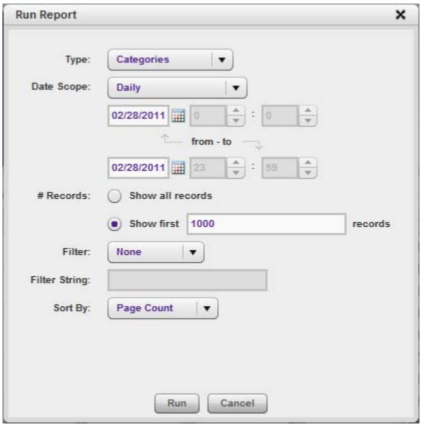
Mouse over the Report Settings object at the bottom left of the panel to open its menu containing the following selections:

- **Run** - Clicking this selection opens the Run Report pop-up box that lets you choose different criteria to display in the report view.
- **Save** - Clicking this selection opens the Save Report pop-up box that lets you modify the current report view and save it, and/or email the report or schedule it to run at a specified time.
- **Limit Detail Result** (available in summary drill down report menus) - Clicking this selection in a summary drill down report opens the Limit Detail Result pop-up box that lets you specify the default number of records to include in the report view for detail drill down reports.

Modify a report via the Run option

The Run option lets you modify the current report view by changing any of the following: Date Scope, maximum number of Records to be included other than the number entered in Default Report Settings, or sort column.

***NOTE**: For summary drill down reports, if specifying a Sort By the first column, summary results must be limited to the top count for another designated column.*


Run Report

Type: Categories

Date Scope: Daily

02/28/2011 0 : 0

from - to

02/28/2011 23 : 59

Records: ○ Show all records

● Show first 1000 records

Filter: None

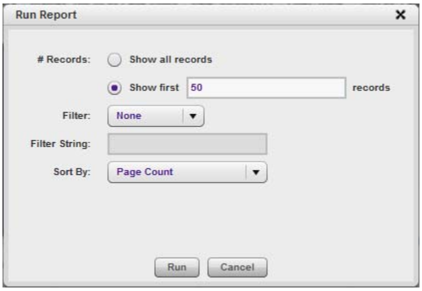
Filter String:

Sort By: Page Count

Fig. 4:2-5 Summary drill down Run Report pop-up box

Selection of a different report Type or execution of a search for specific text can also be performed for summary drill down reports.

If the summary drill down report view is currently grouped by more than one report type, choosing the Run option opens a Run Report pop-up box that does not include the Type and Date Scope selections:



# Records: ○ Show all records

● Show first 50 records

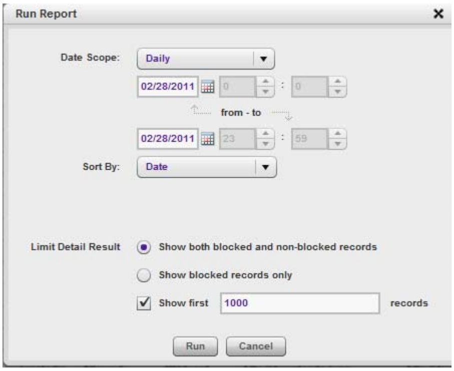
Filter: None

Filter String:

Sort By: Page Count

Fig. 4:2-6 Run Report pop-up box for multi-report group selection

For detail drill down reports, you have the additional option to specify whether blocked records or all returned records—both blocked and non-blocked—will display.



Date Scope: Daily

02/28/2011 0 : 0

02/28/2011 23 : 59

Sort By: Date

Limit Detail Result ● Show both blocked and non-blocked records

○ Show blocked records only

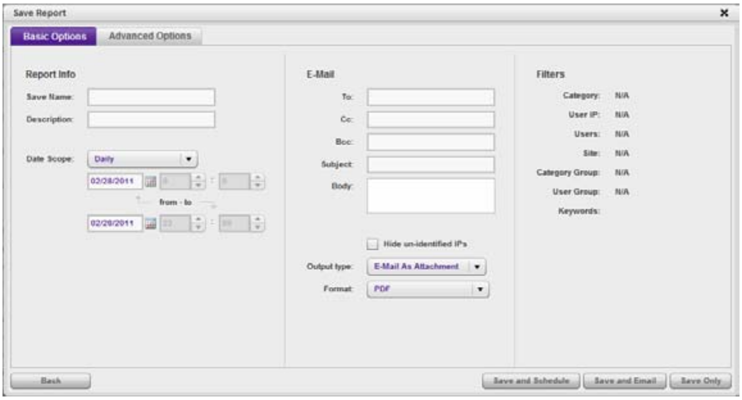
☑ Show first 1000 records

Fig. 4:2-7 Detail drill down Run Report pop-up box

***NOTE**: After all modifications are made, click **Run** to generate the new report view and to close the pop-up box.*

Save report option

The Save option lets you save the current report view so a report using these customizations can be run again later at a designated time. Basic Options requirements include a report Save Name, Description, Date Scope, Email and Output type and Format criteria, and whether unidentified IPs should be included.



Report Info

Save Name:

Description:

Date Scope: Daily

02/28/2011

from - to

02/28/2011

E-Mail

To:

Cc:

Bcc:

Subject:

Body:

□ Hide un-identified IP's

Output type: E-Mail As Attachment

Format: PDF

Filters

Category: N/A

User IP: N/A

Users: N/A

Site: N/A

Category Group: N/A

User Group: N/A

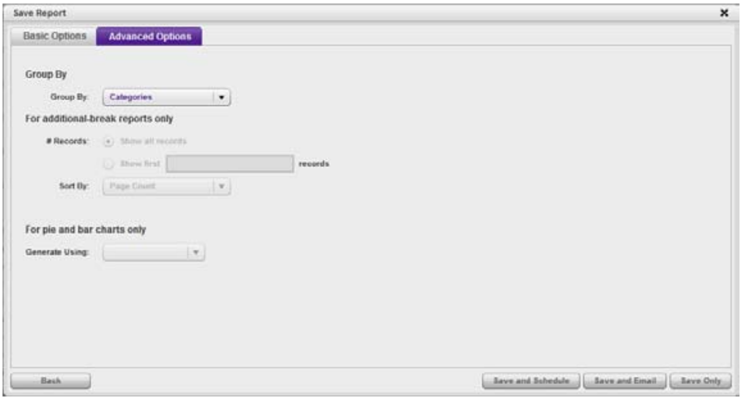
Keywords:

Fig. 4:2-8 Save Report pop-up window for summary reports

***TIP**: The Copy (Ctrl+C) and Paste (Ctrl+V) functions can be used in the fields in the Save Report pop-up window. Clicking **Back** closes the pop-up window.*

The Advanced Options tab lets you specify additional criteria for the report.

For a summary drill down report, Advanced Options include Group By, additional-break type, and pie and bar chart criteria.



Group By

Group By: Categories

For additional-break reports only

Records: ● Show all records

○ Show first records

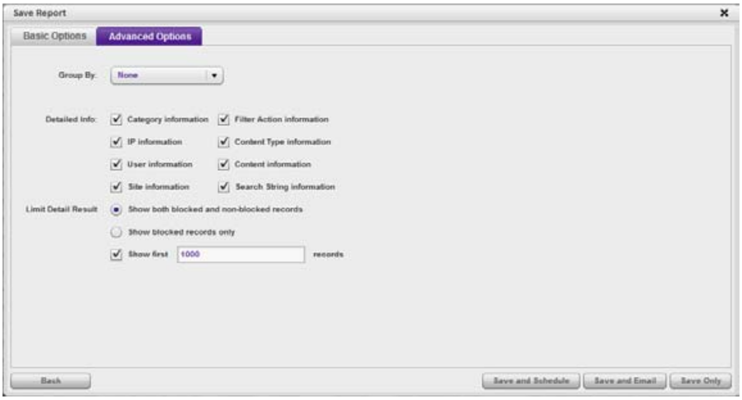
Sort By: Page Count

For pie and bar charts only

Generate Using:

Fig. 4:2-9 Save Report, Advanced Options tab for summary reports

For a detail drill down report, Advanced Options include Group By, column selection, and record type criteria.



Group By: None

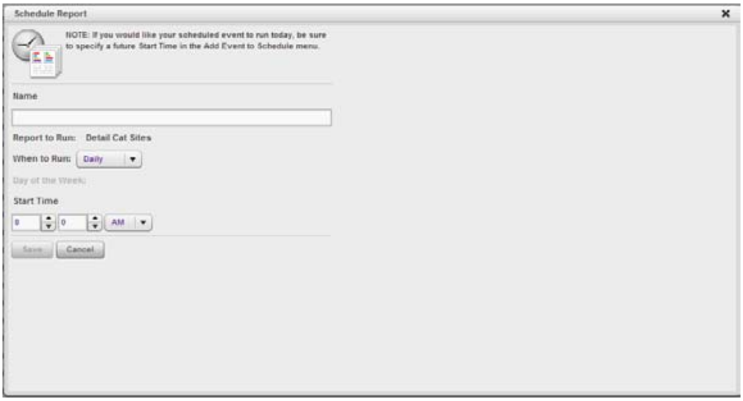
Detailed Info: ☑ Category information ☑ Filter Action information
☑ IP information ☑ Content Type information
☑ User information ☑ Content information
☑ Site information ☑ Search String information

Limit Detail Result ● Show both blocked and non-blocked records
○ Show blocked records only
☑ Show first 1000 records

Fig. 4:2-10 Save Report, Advanced Options tab for detail reports

After all modifications are made, click one of the save option buttons:

- **Save and Schedule** to open the Schedule Report pop-up window where a schedule can be set up for running the report:



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

Name

Report to Run: Detail Cat Sites

When to Run: Daily

Day of the Week:

Start Time

0 0 AM

Fig. 4:2-11 Save Report, Schedule Report option

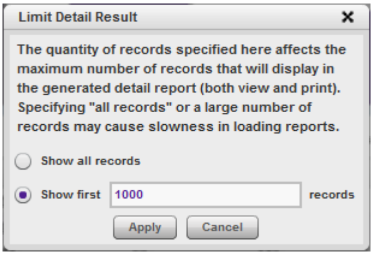
- **Save and Email** to save the report in the specified format and then email it to the designated email address(es).

- **Save Only** to save the report.

NOTE: *See Report Wizard and Report Schedule in Chapter 3 for information about using these report options.*

Limit Detail Result option

The Limit Detail Result option lets you specify the maximum number of records to be included in a detail drill down report view, instead of the default number entered in Default Report Settings.



Limit Detail Result ✕

The quantity of records specified here affects the maximum number of records that will display in the generated detail report (both view and print). Specifying "all records" or a large number of records may cause slowness in loading reports.

○ Show all records

● Show first 1000 records

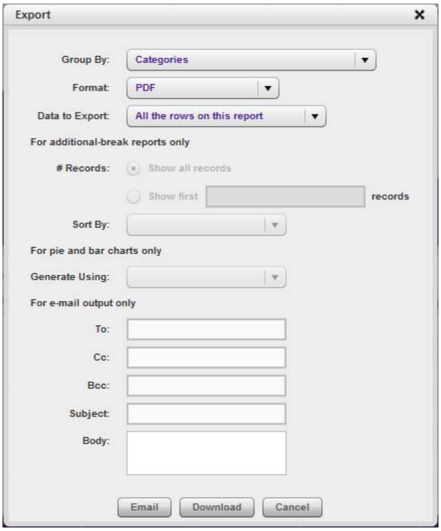
Fig. 4:2-12 Limit Detail Result pop-up box

NOTE: *After all modifications are made, click* ***Apply*** *to save your settings and to close the pop-up box. If generating a detail drill down report, the number of records specified in this box will display in the Run Report and Export pop-up boxes and in the generated report view.*

Export records option

The Export All or Export Selected option lets you Email or Download the current report view in the specified Group By and output Format.

For summary drill down reports, if specifying a drill down Group By selection, indicate the records to be exported, and the Count column to be used for sorting these records.



Export

Group By: Categories

Format: PDF

Data to Export: All the rows on this report

For additional-break reports only

Records: ● Show all records

○ Show first records

Sort By:

For pie and bar charts only

Generate Using:

For e-mail output only

To:

Cc:

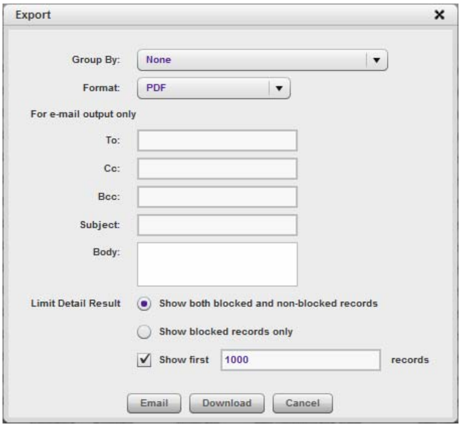
Bcc:

Subject:

Body:

Fig. 4:2-13 Summary drill down Export pop-up box

For detail drill down reports, you have the option to specify the quantity of records, and whether blocked records or all returned records—both blocked and non-blocked—will be included.



Export ✕

Group By: None ▼

Format: PDF ▼

For e-mail output only

To:

Cc:

Bcc:

Subject:

Body:

Limit Detail Result ● Show both blocked and non-blocked records

○ Show blocked records only

☑ Show first 1000 records

Fig. 4:2-14 Detail drill down Export pop-up box

***NOTES**: After all modifications are made, click **Email** to dispatch the report to the email recipient, or click **Download** to launch a separate browser window or tab containing the generated report in the specified format.*

- *See Export a Productivity Report in this chapter for information about using the Email option to email a report.*
- *See View and Print Options in this chapter for information about using the View option to view and print a generated report, and for sample reports.*

Report View Components

Report Fields and Usage

The following fields are used in the summary and detail drill down productivity Report Wizard, Save Report, and/or summary or detail report views and pop-up boxes linked to report views.

Type field

The Type field is used for specifying the report type for the summary report to be generated.

At the **Type** field, make a selection from the pull-down menu for one of the following report types:

- **Categories** - This option performs a query on filter categories accessed by end users.
- **IPs** - This option performs a query on Internet activity by end user IP address.
- **Users** - This option performs a query on end user Internet activity by username.
- **Sites** - This option performs a query on Web sites visited by end users.
- **Category Groups** - This option performs a query on end user Internet activity in Category Groups and Custom Category Groups, the latter which are set up using the Custom Category Groups option from the Administration menu.
- **User Groups** - This option performs a query on Internet activity of User Groups. User Groups are set up using the User Groups option from the Administration menu.

Date Scope and date fields

The Date Scope field is used for specifying the period of time to be included in the generated report view. Reports can be run for any data saved in the SR's memory.

At the **Date Scope** field, make a selection from the pull-down menu for the time frame you wish to use in your query (depending on the scope selected, the from and to date fields are used in conjunction with this field):

- **Today** - This option generates the report view for today only, if logs from the Web access logging device have been received and processed.
- **Month to Date** - This option generates the report view for the range of days that includes the first day of the current month through today.
- **Monthly** - Selecting this option activates the **from** and **to** date fields where you specify the date range using the calendar icons.
- **Year to Date** - This option generates the report view for the range of days that includes the first day of the current year through today.
- **Daily** - Selecting this option activates the **from** and **to** date fields where you specify the date range using the calendar icons. The generated report view includes data for the specified days only, if the data for these days are stored on the SR.
- **Yesterday** - This option generates the report view for yesterday only.
- **Month to Yesterday** - This option generates the report view for the range of days that includes the first day of the current month through yesterday.

- **Year to Yesterday** - This option generates the report view for the range of days that includes the first day of the current year through yesterday.
- **Last Week** - This option generates the report view for all days in the past week, beginning with Sunday and ending with Saturday.
- **Last Weekend** - This option generates the report view for the past Saturday and Sunday.
- **Current Week** - This option generates the report view for today and all previous days in the current week, beginning with Sunday and ending with Saturday.
- **Last Month** - This option generates the report view for all days within the past month.

For detail reports, the following fields are additionally available:

- **Part of Today** - This option generates the report view for today within a specified time range. Make a selection for the hour (1-24) and minutes (0-59).
- **Part of Yesterday** - This option generates the report view for yesterday, within a specified time range. Make a selection for the hour (1-24) and minutes (0-59).
- **Part of Specific Day** - This option generates the report view for the date specified via the calendar icon. In the time fields, make a selection for the hour (1-24) and minutes (0-59).
- **User Defined** - This option generates the report view for the specified time range within the specified date range. In the **from** and **to** fields, use the calendar icons to make selections for the date range. In the time fields, specify the hour (1-24) and minute (0-59) time ranges.

# Records fields

The # Records fields are used for specifying the number of records from the query you wish to include in the summary drill down report view, and how these records will be sorted.

In the **# Records** field, indicate whether the report view should “Show all records” or “Show first ‘x’ records”. If the latter selection is made, the value that displays in this field may have come from the Default Report Settings panel and can be modified.

***NOTE**: The Default Top N Value entry is modified in the Default Report Settings panel, accessible via the Administration menu. See the Default Report Settings panel sub-section in Chapter 3: Report Configuration from the Report Manager Administration Section for information about the Default Top N Value.*

Filter and Filter String fields

The filter fields are used for narrowing results that display in the current summary drill down report view.

At the **Filter** field, make a selection from the pull-down menu for the filter term to be used: “None”, “Contains”, “Starts with”, “Ends with”.

The **Filter String** field displays greyed-out if “None” was selected at the Filter field. If any other selection was made at that field, enter text in this field corresponding to the type of filter term to be used.

Sort By fields

The sort fields are used for specifying the report view column by which the generated report will be sorted.

For summary drill down reports, at the **Sort By** field, make a selection from the pull-down menu for one of the available sort options: “Category Count”, “IP Count”, “User Count”, “Site Count”, “Page Count”, “Object Count”, “Time”, “Hit

Count”, “Bandwidth”—the latter available for an SWG only environment.

For detail drill down reports, at the **Sort By** field, make a selection from the pull-down menu for one of the available sort options: "Date", "Category", "User IP", "User", "Site", "Filter Action", "Content Type", "Content", "Search String", "URL".

NOTE*: In an SWG only environment, the Content Type, Content, and Search String options are not applicable.*

Limit Detail Results fields

Limit Detail Results fields are used for specifying the maximum number of records to be included in the detail report view.

Select the appropriate radio button:

- **Show all records** - Click this radio button to include all records returned by the report query.
- **Show first** ‘x’ **records** - Click this radio button to only include the first set of records returned by the report query, and make an entry to specify the maximum number of records in that set.
- **Show both blocked and non-blocked records** - Click this radio button to include records for URLs that were blocked, as well as those that were not blocked.
- **Show blocked records only** - Click this radio button to only include records for URLs that were blocked.

Group By field

The Group By field is used for indicating the manner in which records will display for the current report view when exported.

Choose from the available report selections at the **Group By** pull-down menu. Based on the current report view displayed, the selections in this menu might include the main report type such as “Sites”, double-combination report types such as “Users/Sites”, triple-combination report types such as “User/Category/IPs”, or pie or bar charts.

Format field

The Format field is used for specifying the manner in which text from the report view will be outputted.

At the **Format** pull-down menu, choose the format for the report: “MS-DOS Text”, “PDF”, “Rich Text Format”, “HTML”, “Comma-Delimited Text”, “Excel (Chinese)”, “Excel (English)”.

Data to Export field

The Data to Export field is used for specifying which records will be exported when the generated summary drill down report is emailed or viewed.

At the **Data to Export** field pull-down menu, specify the amount of data to be exported: “All the rows on this report”, “Only rows on this page”, or “Only selected rows on this page”.

For additional-break reports only

The # Records and Sort By fields are used when exporting multi-combination summary drill down reports and are deactivated by default.

Records field

The # Records field is used for specifying the number of records that will display for the selected sort option. By default, this field displays greyed-out and becomes activated when a different Group By option is selected.

In the activated **# Records** field, indicate whether to “Show all records” or “Show first ‘x’ records”.

Sort By field

The Sort By field is used for specifying the report view column by which the generated report will be sorted.

For summary drill down reports, at the **Sort By** field, make a selection from the pull-down menu for one of the available sort options: “Category Count”, “IP Count”, “User Count”, “Site Count”, “Page Count”, “Object Count”, “Time”, “Hit Count”, “Bandwidth”—the latter option available in an SWG only environment.

For pie and bar charts only

Generate Using field

The Generate Using field is used when exporting a drill down Categories, Category Group, or User Group pie chart or bar chart report, and determines by which column the report will be sorted. By default, the field displays greyed-out and becomes activated when a pie or bar chart report is selected from the Group By pull-down menu.

At the activated **Generate Using** field, make a selection from the pull-down menu for the sort option to be used: “Category Count”, IP Count”, “User Count”, “Site Count”, “Page Count”, “Object Count”, “Time”, “Hit Count”, “Bandwidth”—the latter option available in an SWG only environment.

Output type field

The Output type field is used for specifying how the generated report will be sent to the recipient(s).

At the **Output type** field, choose either “E-Mail As Attachment”, or “E-Mail As Link”.

Hide un-Identified IPs checkbox

The Hide un-Identified IPs checkbox is used for specifying whether or not IP addresses of workstations that are not assigned to a designated end user will be included in reports. This checkbox is deselected by default if the checkbox by this same name was de-selected in the Default Report Settings panel.

***NOTE**: The Default Report Settings panel is accessible via the Administration menu. See the Default Report Settings panel subsection in Chapter 3 of the Report Manager Administration Section for more information about the Hide Unidentified IPs option.*

To change the selection in this field, click the **Hide un-identified IPs** checkbox to remove—or add—a check mark in the checkbox. By entering a check mark in this checkbox, activity on machines not assigned to specific end users will not be included in report views. Changing this selection will not affect the setting previously saved in the Default Report Settings panel.

E-Mail / For e-mail output only fields

E-Mail fields are used for entering email criteria pertinent to the report to be sent to the designated addressee(s).

Specify the following in the **E-Mail** or **For E-Mail output only** fields:

- **To** - Enter the email address of each intended report recipient, separating each address by a comma (,) and a space.
- **Subject** - Type in a brief description about the report.
- **Cc** (optional) - Enter the email address of each intended recipient of a carbon copy of this message, separating each address by a comma (,) and a space.
- **Bcc** (optional) - Enter the email address of each intended recipient of a blind carbon copy of this message, separating each address by a comma (,) and a space.
- **Body** - Type in text pertaining to the report.

Detailed Info fields

Detailed Info fields are used for specifying which columns of data will be excluded from detail drill down reports.

In the **Detailed Info** fields, by default all checkboxes corresponding to detail drill down report columns are selected. Click the checkbox corresponding to any of the following options to remove the check marks and thereby exclude those columns of information from displaying in the report:

- **Category information -** Click this checkbox to exclude the column that displays the library category name.
- **IP information -** Click this checkbox to exclude the column that displays the end user IP address.
- **User information -** Click this checkbox to exclude the column that displays the username.
- **Site information -** Click this checkbox to exclude the column that displays the IP addresses or URLs of sites.
- **Filter Action information -** Click this checkbox to exclude the column that displays the type of filter action used by the Web Filter in creating the record: "Allowed", "Blocked", "Warn Blocked" (for the first warning page that displayed for the end user), "Warn Allowed" (for any subsequent warning page that displayed for the end user), “Quota Blocked” (if a quota blocked the end user), "X-Strike", or "N/A" if the filter action was unclassified at the time the log file was created.
- **Content Type information** (for Web Filters) - Click this checkbox to exclude the column that displays the method used by the Web Filter in creating the record: “Search KW” (Search Engine Keyword), “URL KW” (URL Keyword), “URL”, “Wildcard”, “Https High” (HTTPS Filtering Level set at High), “X-strike” (X Strikes Blocking), “Pattern” (Proxy Pattern Blocking), or “N/A” if

the content was unclassified at the time the log file was created.

- **Content information** (for Web Filters) - Click this checkbox to exclude the column that displays criteria used for determining the categorization of the record, or “N/A” if unclassified.
- **Search String information** (for Web Filters) - Click this checkbox to exclude the column that displays the full search string the end user typed into a search engine text box. This column displays pertinent information only if the Search Engine Reporting option is enabled in the Optional Features screen of the System Configuration administrator console user interface.

***NOTE**: Refer to the Optional Features screen sub-section of the System Configuration Section for information about the Search String feature.*

Export a Productivity Report

The email option for exporting drill down reports lets you electronically send the report in the specified file format to designated personnel.

⚠ ***WARNING****: If using a spam filter on your mail server, email messages or attachments might not be delivered if these messages contain keywords that are set up to be blocked. Consult with the administrator of the mail server for work around solutions between the spam filter and mail server.*

1. In the Export pop-up box, enter the following information:
   - **To** field - Type in the email address of each intended report recipient, separating each address by a comma (,) and a space.
   - **Subject** field (optional) - Type in a brief description about the report.
   - **Cc** field (optional) - Type in the email address of each intended recipient of a carbon copy of this message, separating each address by a comma (,) and a space.
   - **Bcc** field (optional) - Type in the email address of each intended recipient of a blind carbon copy of this message, separating each address by a comma (,) and a space.
   - **Body** field (optional) - Type in text pertaining to the report.
2. Click **Email** to send the report to the designated recipient(s).

⚠ ***WARNING****: Large reports might not be sent due to email size restrictions on your mail server. The maximum size of an email message is often two or three MB. Please consult your mail server administrator for more information about email size restrictions.*

View and Print Options

The view and print options for exporting drill down reports let you view/print the report in the specified file format. The view option lets you make any necessary adjustments to your report file settings prior to printing the report. To print the report, you must have a printer configured for your workstation.

In the Export pop-up box, click the **Download** button to generate and download the report in the specified file format.

NOTE*: Reports generated in the format for MS-DOS Text, Comma-Delimited Text, or Excel (Chinese or English) will display a single row of text for each record. Reports generated in all other formats (PDF, Rich Text Format, HTML) will display any lengthy string of text wrapped around below.*

View and Print Tools

In the browser window containing the report, the tools available via the toolbar let you perform some of the following actions on the open report file:

File:

- **Save** (Ctrl+S) or **Save (Page) As -** Save the report file to your local drive.
- **Print** (Ctrl+P) **-** Open the Print dialog box where specifications can be made before printing the report file, such as changing the orientation of the printed page by selecting **Portrait** (vertical) or **Landscape** (horizontal).

Edit:

- **Select All** - Hghlight the entire text (Ctrl+A), and then Copy (Ctrl+C) and Paste (Ctrl+V) this text in an open file
- Perform a search for text > **Find -** Search for specific text in the file (Ctrl+F)

Sample Report File Formats

The following report file formats are available for emailing and viewing drill down reports: MS-DOS Text, PDF, Rich Text Format, HTML, Comma-Delimited Text, Excel (Chinese), Excel (English).

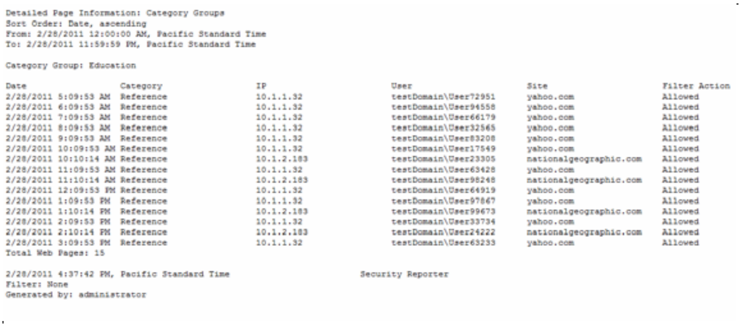
***NOTES**: M86 Security recommends using the PDF and HTML file formats over other file format selections—in particular for detail reports—since these files display and print in a format that is easiest to read. Lengthy text in PDF, HTML, and Rich Text Format files wraps around within the column so all text is captured without displaying truncated.*

Comma-Delimited Text and Excel report columns may display with truncated text, but an entire column can be viewed by manipulating the column width in the generated report file. These reports can then be printed at a smaller percentage than normal size in order to accommodate all text.

For MS-DOS Text reports, text may display truncated—in particular for lengthy usernames and URLs in detail reports—but an entire column can be viewed by scrolling to the right. Since there is no way to manipulate text in the generated report file, the printed report may display with truncated text. However, the maximum amount of text can be captured by printing the report in the landscape format.

MS-DOS Text

This is a sample of the Category Groups report in the MS-DOS Text format, saved with a .txt file extension:

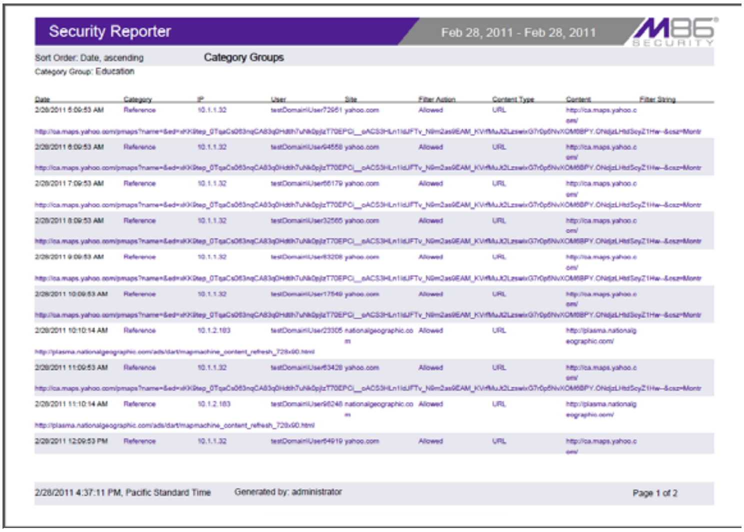


```
Detailed Page Information: Category Groups
Sort Order: Date, ascending
From: 2/28/2011 12:00:00 AM, Pacific Standard Time
To: 2/28/2011 11:59:59 PM, Pacific Standard Time

Category Group: Education

Date                  Category                 IP                       User                   Site                     Filter Action
2/28/2011 5:09:53 AM  Reference                10.1.1.32                testDomain\User72951   yahoo.com                Allowed
2/28/2011 6:09:53 AM  Reference                10.1.1.32                testDomain\User94558   yahoo.com                Allowed
2/28/2011 7:09:53 AM  Reference                10.1.1.32                testDomain\User66179   yahoo.com                Allowed
2/28/2011 8:09:53 AM  Reference                10.1.1.32                testDomain\User32565   yahoo.com                Allowed
2/28/2011 9:09:53 AM  Reference                10.1.1.32                testDomain\User83208   yahoo.com                Allowed
2/28/2011 10:09:53 AM Reference                10.1.1.32                testDomain\User17549   yahoo.com                Allowed
2/28/2011 10:10:14 AM Reference                10.1.2.183               testDomain\User23305   nationalgeographic.com   Allowed
2/28/2011 11:09:53 AM Reference                10.1.1.32                testDomain\User63428   yahoo.com                Allowed
2/28/2011 11:10:14 AM Reference                10.1.2.183               testDomain\User98248   nationalgeographic.com   Allowed
2/28/2011 12:09:53 PM Reference                10.1.1.32                testDomain\User64919   yahoo.com                Allowed
2/28/2011 1:09:53 PM  Reference                10.1.1.32                testDomain\User97867   yahoo.com                Allowed
2/28/2011 1:10:14 PM  Reference                10.1.2.183               testDomain\User99673   nationalgeographic.com   Allowed
2/28/2011 2:09:53 PM  Reference                10.1.1.32                testDomain\User33734   yahoo.com                Allowed
2/28/2011 2:10:14 PM  Reference                10.1.2.183               testDomain\User24222   nationalgeographic.com   Allowed
2/28/2011 3:09:53 PM  Reference                10.1.1.32                testDomain\User63233   yahoo.com                Allowed
Total Web Pages: 15

2/28/2011 4:37:42 PM, Pacific Standard Time                      Security Reporter
Filter: None
Generated by: administrator
```

Fig. 4:2-15 Category Groups report, MS-DOS Text file format

PDF

This is a sample of the Category Groups report in the PDF format, saved with a .pdf file extension:



Security Reporter

Feb 28, 2011 - Feb 28, 2011

Sort Order: Date, ascending

Category Groups

Category Group: Education

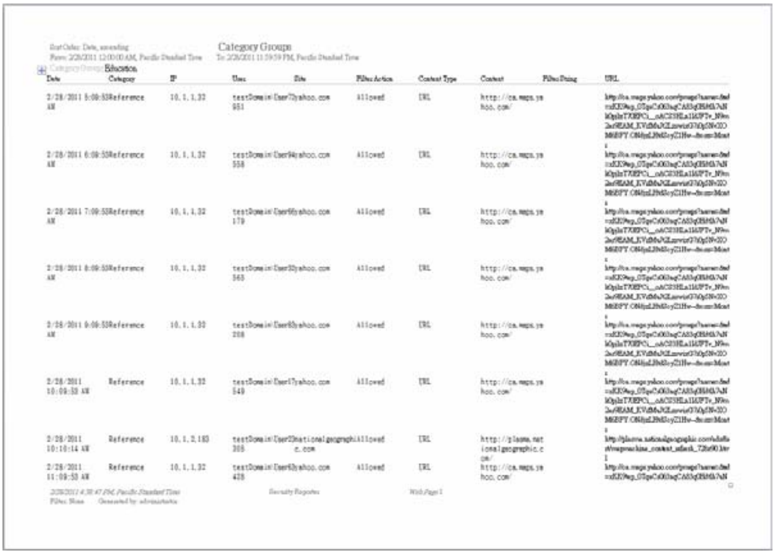
Date	Category	IP	User	Site	Filter Action	Content Type	Content	Filter String
2/28/2011 5:09:53 AM	Reference	10.1.1.32	testDomain\User72951	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/	
http://ca.maps.yahoo.com/pmaps?name=&ed=xKK9tep_0TqaCs063nqCA83qDHdth7uNk0pjlzT70EPCi__oACS3HLn1IdJFTv_N9m2as9EAM_KVrfMuJt2LzswixG7r0p6NvXOM6BPY.ONdjzLHtdScyZ1Hw--&csz=Montr								
2/28/2011 6:09:53 AM	Reference	10.1.1.32	testDomain\User94558	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/	
http://ca.maps.yahoo.com/pmaps?name=&ed=xKK9tep_0TqaCs063nqCA83qDHdth7uNk0pjlzT70EPCi__oACS3HLn1IdJFTv_N9m2as9EAM_KVrfMuJt2LzswixG7r0p6NvXOM6BPY.ONdjzLHtdScyZ1Hw--&csz=Montr								
2/28/2011 7:09:53 AM	Reference	10.1.1.32	testDomain\User66179	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/	
http://ca.maps.yahoo.com/pmaps?name=&ed=xKK9tep_0TqaCs063nqCA83qDHdth7uNk0pjlzT70EPCi__oACS3HLn1IdJFTv_N9m2as9EAM_KVrfMuJt2LzswixG7r0p6NvXOM6BPY.ONdjzLHtdScyZ1Hw--&csz=Montr								
2/28/2011 8:09:53 AM	Reference	10.1.1.32	testDomain\User32565	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/	
http://ca.maps.yahoo.com/pmaps?name=&ed=xKK9tep_0TqaCs063nqCA83qDHdth7uNk0pjlzT70EPCi__oACS3HLn1IdJFTv_N9m2as9EAM_KVrfMuJt2LzswixG7r0p6NvXOM6BPY.ONdjzLHtdScyZ1Hw--&csz=Montr								
2/28/2011 9:09:53 AM	Reference	10.1.1.32	testDomain\User83208	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/	
http://ca.maps.yahoo.com/pmaps?name=&ed=xKK9tep_0TqaCs063nqCA83qDHdth7uNk0pjlzT70EPCi__oACS3HLn1IdJFTv_N9m2as9EAM_KVrfMuJt2LzswixG7r0p6NvXOM6BPY.ONdjzLHtdScyZ1Hw--&csz=Montr								
2/28/2011 10:09:53 AM	Reference	10.1.1.32	testDomain\User17549	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/	
http://ca.maps.yahoo.com/pmaps?name=&ed=xKK9tep_0TqaCs063nqCA83qDHdth7uNk0pjlzT70EPCi__oACS3HLn1IdJFTv_N9m2as9EAM_KVrfMuJt2LzswixG7r0p6NvXOM6BPY.ONdjzLHtdScyZ1Hw--&csz=Montr								
2/28/2011 10:10:14 AM	Reference	10.1.2.183	testDomain\User23305	nationalgeographic.com	Allowed	URL	http://plasma.nationalgeographic.com/	
http://plasma.nationalgeographic.com/ads/dart/mapmachine_content_refresh_728x90.html								
2/28/2011 11:09:53 AM	Reference	10.1.1.32	testDomain\User63428	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/	
http://ca.maps.yahoo.com/pmaps?name=&ed=xKK9tep_0TqaCs063nqCA83qDHdth7uNk0pjlzT70EPCi__oACS3HLn1IdJFTv_N9m2as9EAM_KVrfMuJt2LzswixG7r0p6NvXOM6BPY.ONdjzLHtdScyZ1Hw--&csz=Montr								
2/28/2011 11:10:14 AM	Reference	10.1.2.183	testDomain\User98248	nationalgeographic.com	Allowed	URL	http://plasma.nationalgeographic.com/	
http://plasma.nationalgeographic.com/ads/dart/mapmachine_content_refresh_728x90.html								
2/28/2011 12:09:53 PM	Reference	10.1.1.32	testDomain\User64919	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/	

2/28/2011 4:37:11 PM, Pacific Standard Time   Generated by: administrator   Page 1 of 2

Fig. 4:2-16 Category Groups report, PDF format

Rich Text Format

This is a sample of the Category Groups report in the Rich Text file Format, saved with a .rtf file extension:



Sort Order: Date, ascending

Category Groups

From: 2/28/2011 12:00:00 AM, Pacific Standard Time To: 2/28/2011 11:59:59 PM, Pacific Standard Time

Category Groups: Education

Date	Category	IP	User	Site	Filter Action	Content Type	Content	Filter Rating	URL
2/28/2011 5:09:53 AM	Reference	10.1.1.32	testDomain\User7951	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/pmaps?name=[illegible]
2/28/2011 6:09:53 AM	Reference	10.1.1.32	testDomain\User94558	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/pmaps?name=[illegible]
2/28/2011 7:09:53 AM	Reference	10.1.1.32	testDomain\User66179	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/pmaps?name=[illegible]
2/28/2011 8:09:53 AM	Reference	10.1.1.32	testDomain\User33565	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/pmaps?name=[illegible]
2/28/2011 9:09:53 AM	Reference	10.1.1.32	testDomain\User83208	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/pmaps?name=[illegible]
2/28/2011 10:09:53 AM	Reference	10.1.1.32	testDomain\User17549	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/pmaps?name=[illegible]
2/28/2011 10:10:14 AM	Reference	10.1.2.183	testDomain\User23305	nationalgeographic.com	Allowed	URL	http://plasma.nationalgeographic.com/		http://plasma.nationalgeographic.com/[illegible]
2/28/2011 11:09:53 AM	Reference	10.1.1.32	testDomain\User63428	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/pmaps?name=[illegible]

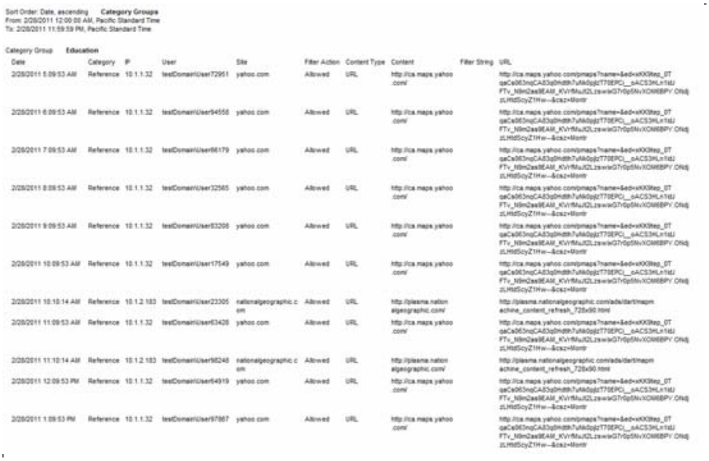
2/28/2011 4:38:47 PM, Pacific Standard Time Security Reporter Web Page 1

Filter: None Generated by: administrator

Fig. 4:2-17 Category Groups report, RTF format

HTML

This is a sample of the Category Groups report in the HTML format, saved with a .html file extension:



Sort Order: Date, ascending   **Category Groups**
From: 2/28/2011 12:00:00 AM, Pacific Standard Time
To: 2/28/2011 11:59:59 PM, Pacific Standard Time

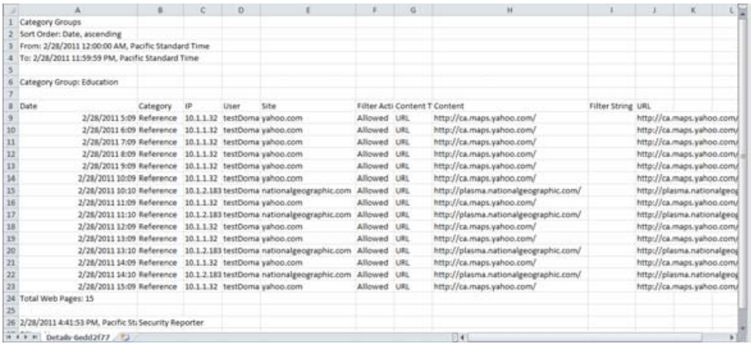
Category Group   **Education**

Date	Category	IP	User	Site	Filter Action	Content Type	Content	Filter String	URL
2/28/2011 5:09:53 AM	Reference	10.1.1.32	testDomain\User72951	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/pmaps?name=&ed=xKK9tep_0TqaCa063nqCA83q0Hd8h7uNk0pjzT70EPCi__oACS3HLn1tdJFTv_N9m2aa9EAM_KVYfMuJt2LzswleG7r0p5NvXOM6BPY.ONdjzLHtdScyZ1Hw--&csz=Montr
2/28/2011 6:09:53 AM	Reference	10.1.1.32	testDomain\User94558	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/pmaps?name=&ed=xKK9tep_0TqaCa063nqCA83q0Hd8h7uNk0pjzT70EPCi__oACS3HLn1tdJFTv_N9m2aa9EAM_KVYfMuJt2LzswleG7r0p5NvXOM6BPY.ONdjzLHtdScyZ1Hw--&csz=Montr
2/28/2011 7:09:53 AM	Reference	10.1.1.32	testDomain\User66179	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/pmaps?name=&ed=xKK9tep_0TqaCa063nqCA83q0Hd8h7uNk0pjzT70EPCi__oACS3HLn1tdJFTv_N9m2aa9EAM_KVYfMuJt2LzswleG7r0p5NvXOM6BPY.ONdjzLHtdScyZ1Hw--&csz=Montr
2/28/2011 8:09:53 AM	Reference	10.1.1.32	testDomain\User32585	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/pmaps?name=&ed=xKK9tep_0TqaCa063nqCA83q0Hd8h7uNk0pjzT70EPCi__oACS3HLn1tdJFTv_N9m2aa9EAM_KVYfMuJt2LzswleG7r0p5NvXOM6BPY.ONdjzLHtdScyZ1Hw--&csz=Montr
2/28/2011 9:09:53 AM	Reference	10.1.1.32	testDomain\User53206	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/pmaps?name=&ed=xKK9tep_0TqaCa063nqCA83q0Hd8h7uNk0pjzT70EPCi__oACS3HLn1tdJFTv_N9m2aa9EAM_KVYfMuJt2LzswleG7r0p5NvXOM6BPY.ONdjzLHtdScyZ1Hw--&csz=Montr
2/28/2011 10:09:53 AM	Reference	10.1.1.32	testDomain\User17549	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/pmaps?name=&ed=xKK9tep_0TqaCa063nqCA83q0Hd8h7uNk0pjzT70EPCi__oACS3HLn1tdJFTv_N9m2aa9EAM_KVYfMuJt2LzswleG7r0p5NvXOM6BPY.ONdjzLHtdScyZ1Hw--&csz=Montr
2/28/2011 10:10:14 AM	Reference	10.1.2.183	testDomain\User22305	nationalgeographic.com	Allowed	URL	http://plasma.nationalgeographic.com/		http://plasma.nationalgeographic.com/ads/dart/mapmachine_content_refresh_728x90.html
2/28/2011 11:09:53 AM	Reference	10.1.1.32	testDomain\User63426	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/pmaps?name=&ed=xKK9tep_0TqaCa063nqCA83q0Hd8h7uNk0pjzT70EPCi__oACS3HLn1tdJFTv_N9m2aa9EAM_KVYfMuJt2LzswleG7r0p5NvXOM6BPY.ONdjzLHtdScyZ1Hw--&csz=Montr
2/28/2011 11:10:14 AM	Reference	10.1.2.183	testDomain\User98248	nationalgeographic.com	Allowed	URL	http://plasma.nationalgeographic.com/		http://plasma.nationalgeographic.com/ads/dart/mapmachine_content_refresh_728x90.html
2/28/2011 12:09:53 PM	Reference	10.1.1.32	testDomain\User64919	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/pmaps?name=&ed=xKK9tep_0TqaCa063nqCA83q0Hd8h7uNk0pjzT70EPCi__oACS3HLn1tdJFTv_N9m2aa9EAM_KVYfMuJt2LzswleG7r0p5NvXOM6BPY.ONdjzLHtdScyZ1Hw--&csz=Montr
2/28/2011 1:09:53 PM	Reference	10.1.1.32	testDomain\User97867	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/pmaps?name=&ed=xKK9tep_0TqaCa063nqCA83q0Hd8h7uNk0pjzT70EPCi__oACS3HLn1tdJFTv_N9m2aa9EAM_KVYfMuJt2LzswleG7r0p5NvXOM6BPY.ONdjzLHtdScyZ1Hw--&csz=Montr

Fig. 4:2-18 Category Groups report, HTML file format

Comma-Delimited Text

This is a sample of the Category Groups report in the Comma-Delimited Text format, saved with a .csv file extension:

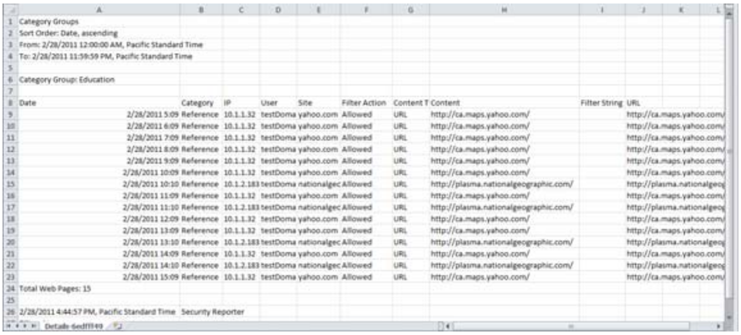


	A	B	C	D	E	F	G	H	I	J	K	L
1	Category Groups											
2	Sort Order: Date, ascending											
3	From: 2/28/2011 12:00:00 AM, Pacific Standard Time											
4	To: 2/28/2011 11:59:59 PM, Pacific Standard Time											
5												
6	Category Group: Education											
7												
8	Date	Category	IP	User	Site	Filter Acti	Content T	Content	Filter String	URL		
9	2/28/2011 5:09	Reference	10.1.1.32	testDoma	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/		
10	2/28/2011 6:09	Reference	10.1.1.32	testDoma	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/		
11	2/28/2011 7:09	Reference	10.1.1.32	testDoma	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/		
12	2/28/2011 8:09	Reference	10.1.1.32	testDoma	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/		
13	2/28/2011 9:09	Reference	10.1.1.32	testDoma	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/		
14	2/28/2011 10:09	Reference	10.1.1.32	testDoma	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/		
15	2/28/2011 10:10	Reference	10.1.2.183	testDoma	nationalgeographic.com	Allowed	URL	http://plasma.nationalgeographic.com/		http://plasma.nationalgeo		
16	2/28/2011 11:09	Reference	10.1.1.32	testDoma	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/		
17	2/28/2011 11:10	Reference	10.1.2.183	testDoma	nationalgeographic.com	Allowed	URL	http://plasma.nationalgeographic.com/		http://plasma.nationalgeo		
18	2/28/2011 12:09	Reference	10.1.1.32	testDoma	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/		
19	2/28/2011 13:09	Reference	10.1.1.32	testDoma	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/		
20	2/28/2011 13:10	Reference	10.1.2.183	testDoma	nationalgeographic.com	Allowed	URL	http://plasma.nationalgeographic.com/		http://plasma.nationalgeo		
21	2/28/2011 14:09	Reference	10.1.1.32	testDoma	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/		
22	2/28/2011 14:10	Reference	10.1.2.183	testDoma	nationalgeographic.com	Allowed	URL	http://plasma.nationalgeographic.com/		http://plasma.nationalgeo		
23	2/28/2011 15:09	Reference	10.1.1.32	testDoma	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/		
24	Total Web Pages: 15											
25												
26	2/28/2011 4:41:53 PM, Pacific St	Security Reporter										

Fig. 4:2-19 Category Groups report, Comma-Delimited Text file

Excel (English)

This is a sample of the Category Groups report in the Excel (English) format, saved with a .xls file extension:



	A	B	C	D	E	F	G	H	I	J	K	L
1	Category Groups											
2	Sort Order: Date, ascending											
3	From: 2/28/2011 12:00:00 AM, Pacific Standard Time											
4	To: 2/28/2011 11:59:59 PM, Pacific Standard Time											
5												
6	Category Group: Education											
7												
8	Date	Category	IP	User	Site	Filter Action	Content T	Content	Filter String	URL		
9	2/28/2011 5:09	Reference	10.1.1.32	testDoma	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/		
10	2/28/2011 6:09	Reference	10.1.1.32	testDoma	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/		
11	2/28/2011 7:09	Reference	10.1.1.32	testDoma	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/		
12	2/28/2011 8:09	Reference	10.1.1.32	testDoma	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/		
13	2/28/2011 9:09	Reference	10.1.1.32	testDoma	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/		
14	2/28/2011 10:09	Reference	10.1.1.32	testDoma	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/		
15	2/28/2011 10:10	Reference	10.1.2.183	testDoma	nationalgec	Allowed	URL	http://plasma.nationalgeographic.com/		http://plasma.nationalgeog		
16	2/28/2011 11:09	Reference	10.1.1.32	testDoma	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/		
17	2/28/2011 11:10	Reference	10.1.2.183	testDoma	nationalgec	Allowed	URL	http://plasma.nationalgeographic.com/		http://plasma.nationalgeog		
18	2/28/2011 12:09	Reference	10.1.1.32	testDoma	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/		
19	2/28/2011 13:09	Reference	10.1.1.32	testDoma	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/		
20	2/28/2011 13:10	Reference	10.1.2.183	testDoma	nationalgec	Allowed	URL	http://plasma.nationalgeographic.com/		http://plasma.nationalgeog		
21	2/28/2011 14:09	Reference	10.1.1.32	testDoma	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/		
22	2/28/2011 14:10	Reference	10.1.2.183	testDoma	nationalgec	Allowed	URL	http://plasma.nationalgeographic.com/		http://plasma.nationalgeog		
23	2/28/2011 15:09	Reference	10.1.1.32	testDoma	yahoo.com	Allowed	URL	http://ca.maps.yahoo.com/		http://ca.maps.yahoo.com/		
24	Total Web Pages: 15											
25												
26	2/28/2011 4:44:57 PM, Pacific Standard Time	Security Reporter										

Fig. 4:2-20 Category Groups report, Excel (English) file format

***NOTES**: The Excel (English) option supports up to 65,000 rows of exported data. If exporting more than 65,000 rows of data, M86 Security recommends using another format.*

The Excel (Chinese) option supports up to 10,000 rows of exported data. If exporting more than 10,000 rows of data, M86 Security recommends using the PDF format option.

The number of rows that can be exported varies with each file format.

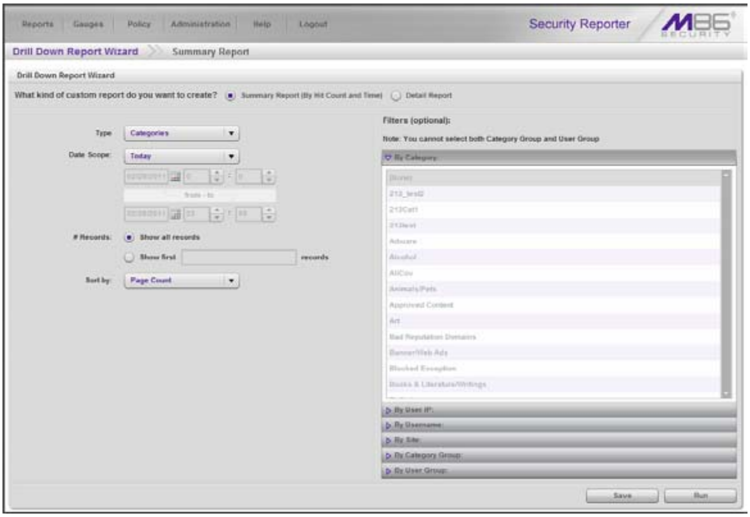
Chapter 3: Customize, Maintain Reports

The following report topics from the Reports menu of the Report Manager are described in this chapter: Report Wizard, Saved Reports, and Report Schedule.

Report Wizard

Report Wizard lets you generate a customized drill down report, querying the database for hits, pages, or objects viewed by end users.

In the navigation toolbar, mouse over the Reports menu link and navigate to **Drill Down Reports > Report Wizard** to display the drill down Report Wizard panel:



Drill Down Report Wizard

What kind of custom report do you want to create? ● Summary Report (By Hit Count and Time) ○ Detail Report

Type: Categories

Date Scope: Today

from - to

Records: ● Show all records ○ Show first records

Sort by: Page Count

Filters (optional):

Note: You cannot select both Category Group and User Group

By Category:

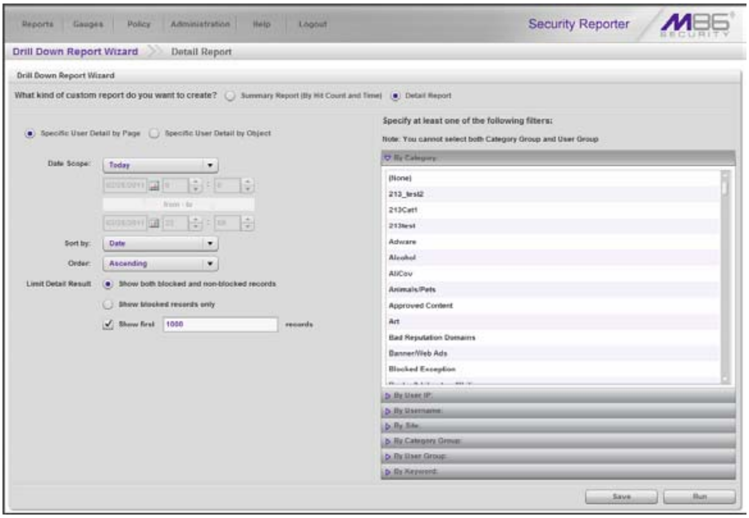
Fig. 4:3-1 Report Wizard panel for summary reports

Step A: Select the Report Option

Select one of two available custom drill down report options:

- **Summary Report (By Hit Count and Time) -** This report provides a synopsis of specified end user Internet activity by hit count and time for a designated period.
- **Detail Report -** This report provides information about end user Web page or Web object access for a specified time period.

The fields that display in this panel depend upon whether a summary report or a detail report is selected.



Drill Down Report Wizard

What kind of custom report do you want to create? ○ Summary Report (By Hit Count and Time) ● Detail Report

● Specific User Detail by Page ○ Specific User Detail by Object

Date Scope: Today

from - to

Sort by: Date

Order: Ascending

Limit Detail Result: ● Show both blocked and non-blocked records

○ Show blocked records only

☑ Show first 1000 records

Specify at least one of the following filters:

Note: You cannot select both Category Group and User Group

Fig. 4:3-2 Report Wizard panel for detail reports

Step B: Specify the Report Type

Summary report

Make a choice for the **Type** of report to be generated: “Categories”, “IPs”, “Users”, “Sites”, “Category Groups”, “User Groups”.

To narrow your results, use the appropriate **Filters (optional)** accordions to the right, described in Step C.

Detail report

1. Choose the type of detail report to use in the query:
   - **Specific User Detail by Page -** Includes viewed page results
   - **Specific User Detail by Object** - Includes viewed object results
2. **Specify at least one of the following filters** in the accordions at right to narrow your search, described in Step C.

Step C: Specify Filters

This step is optional for summary drill down reports, but required for detail drill down reports.

- **By Category -** If selecting this filter, choose the category to filter your report query results.

TIP*: To de-select a Category choose “(None)” from the list.*

- **By User IP** - If selecting this filter, enter the end user IP address for filtering your results—using the ‘%’ wildcard to return multiple IP addresses—and then click **Search** to display query results in the list box below.

TIP*: Click* ***Reset*** *to remove the IP address(es) from the list box.*

- **By Username** - If selecting this filter, enter the end user name to filter your results—using the '%' wildcard to return multiple usernames—and then click **Search** to display query results in the list box below.

  For a detail drill down report, select the username and click the right arrow (>) to move the username into the Added user names list box. Additional searches can be performed to include other usernames in the list box.

***TIP**: For a summary drill down report, click **Reset** to remove the username from the list box. For a detail drill down report, use the left arrow (<) to remove the username from the list box.*

***NOTE**: If more than one username is entered, the following message displays at the bottom of this panel: 'NOTE: This report is very processor and time intensive and may take several minutes to complete.' The report must now be saved and run at a later time.*

- **By Site** - If selecting this filter, enter the site name to filter your results—using the '%' wildcard to return multiple site names—and then click **Search** to display query results in the list box below.

***TIP**: Click **Reset** to remove the site(s) from the list box.*

- **By Category Group** - If selecting this filter, choose the Category Group to filter your report query results.

***TIP**: To de-select a Category Group, choose "(None)" from the list.*

- **By User Group** - If selecting this filter, choose the User Group to filter your report query results.

***TIP**: To de-select a User Group, choose "(None)" from the list.*

- **By Keyword** - This selection is available for detail drill down reports only. If selecting this filter, enter a keyword from three to 255 characters to filter your results, and then click **Add** to include your keyword term in the list box below. More than one keyword can be included in the list box.

***TIP**: To remove a keyword, select the keyword from the list box and click **Remove**.*

***NOTE**: If a keyword is entered, the following message displays at the bottom of this panel: 'NOTE: This report is very processor and time intensive and may take several minutes to complete.' The report must now be saved and run at a later time.*

Step D: Specify Other Report Components

Specify criteria for the remaining components to be used in the report:

- **Date Scope -** Choose the date scope to be included in the results.

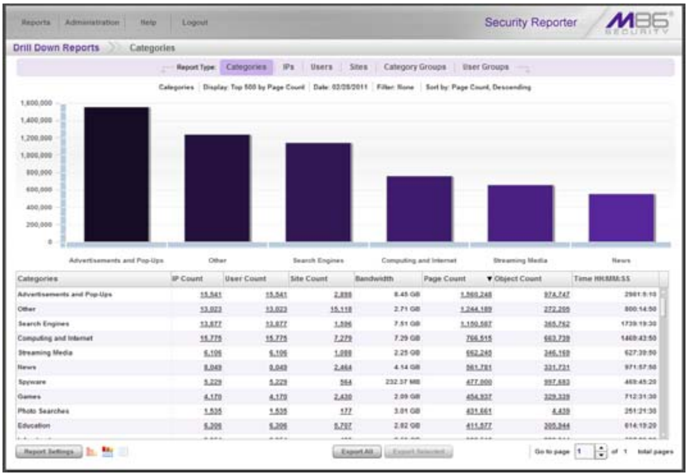
***NOTE**: For detail reports, if more than one username or if any keyword is entered in this panel, the following Date Scope choices are the only choices available: "Yesterday" (default), "Previous 7 Days", selections for Previous 6, 5, 4, 3, or 2 Days, and "Daily".*

- **# Records -** For a summary drill down report, specify the number of records to be returned in the results.
- **Sort by** - Select column by which the results will be sorted and displayed in the report.
- **Order** - For a detail drill down report, indicate whether results will be sorted in "Ascending" or "Descending" order.
- **Limit Detail Result** - For a detail drill down report, specify the number of records to be returned in the results, and if these records will only include records of blocked end user queries, or also records of non-blocked end user queries.

Step E: Specify when to Generate the Report

Indicate the next step in the wizard by selecting one of two choices that specify when the report will be generated:

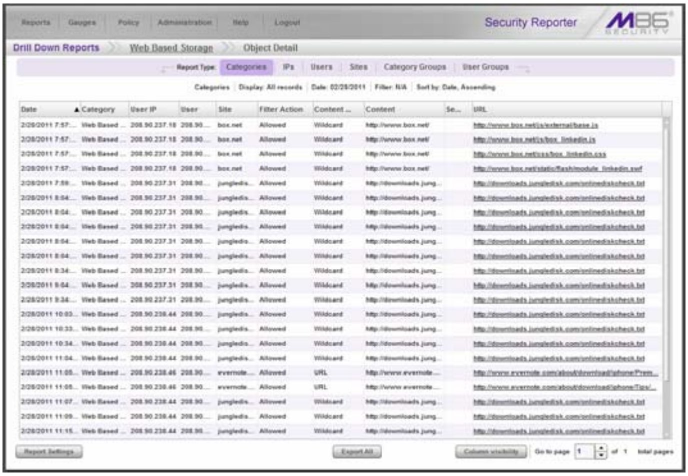
- **Run** - Click this button to generate and view the drill down report now in the specified report view format.



Categories | Display: Top 500 by Page Count | Date: 02/28/2011 | Filter: None | Sort by: Page Count, Descending

Categories	IP Count	User Count	Site Count	Bandwidth	Page Count ▼	Object Count	Time HH:MM:SS
Advertisements and Pop-Ups	15,541	15,541	2,898	8.45 GB	1,560,248	974,747	2981:5:10
Other	13,023	13,023	15,118	2.71 GB	1,244,189	272,205	800:14:50
Search Engines	13,877	13,877	1,596	7.51 GB	1,150,587	365,762	1739:19:30
Computing and Internet	15,775	15,775	7,279	7.29 GB	766,515	663,739	1469:43:50
Streaming Media	6,105	6,105	1,089	2.25 GB	662,245	346,169	627:39:50
News	8,049	8,049	2,464	4.14 GB	561,781	331,721	971:57:50
Spyware	5,229	5,229	564	232.37 MB	477,000	997,683	469:45:20
Games	4,170	4,170	2,430	2.09 GB	454,937	329,339	712:31:30
Photo Searches	1,535	1,535	177	3.01 GB	431,661	4,439	251:21:30
Education	6,206	6,206	5,707	2.82 GB	411,577	305,944	614:19:20

Fig. 4:3-3 Summary drill down report



Categories | Display: All records | Date: 02/28/2011 | Filter: N/A | Sort by: Date, Ascending

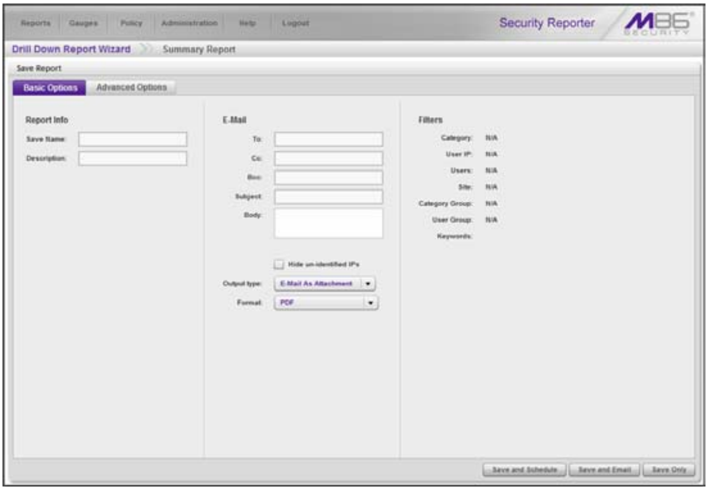
Date ▲	Category	User IP	User	Site	Filter Action	Content ...	Content	Se...	URL
2/28/2011 7:57:...	Web Based ...	208.90.237.18	208.90....	box.net	Allowed	Wildcard	http://www.box.net/		http://www.box.net/js/external/base.js
2/28/2011 7:57:...	Web Based ...	208.90.237.18	208.90....	box.net	Allowed	Wildcard	http://www.box.net/		http://www.box.net/js/box_linkedin.js
2/28/2011 7:57:...	Web Based ...	208.90.237.18	208.90....	box.net	Allowed	Wildcard	http://www.box.net/		http://www.box.net/css/box_linkedin.css
2/28/2011 7:57:...	Web Based ...	208.90.237.18	208.90....	box.net	Allowed	Wildcard	http://www.box.net/		http://www.box.net/static/flash/module_linkedin.swf
2/28/2011 7:59:...	Web Based ...	208.90.237.31	208.90....	jungledis...	Allowed	Wildcard	http://downloads.jung...		http://downloads.jungledisk.com/onlinediskcheck.txt
2/28/2011 8:04:...	Web Based ...	208.90.237.31	208.90....	jungledis...	Allowed	Wildcard	http://downloads.jung...		http://downloads.jungledisk.com/onlinediskcheck.txt
2/28/2011 8:04:...	Web Based ...	208.90.237.31	208.90....	jungledis...	Allowed	Wildcard	http://downloads.jung...		http://downloads.jungledisk.com/onlinediskcheck.txt
2/28/2011 8:04:...	Web Based ...	208.90.237.31	208.90....	jungledis...	Allowed	Wildcard	http://downloads.jung...		http://downloads.jungledisk.com/onlinediskcheck.txt
2/28/2011 8:04:...	Web Based ...	208.90.237.31	208.90....	jungledis...	Allowed	Wildcard	http://downloads.jung...		http://downloads.jungledisk.com/onlinediskcheck.txt
2/28/2011 8:04:...	Web Based ...	208.90.237.31	208.90....	jungledis...	Allowed	Wildcard	http://downloads.jung...		http://downloads.jungledisk.com/onlinediskcheck.txt
2/28/2011 8:34:...	Web Based ...	208.90.237.31	208.90....	jungledis...	Allowed	Wildcard	http://downloads.jung...		http://downloads.jungledisk.com/onlinediskcheck.txt
2/28/2011 9:04:...	Web Based ...	208.90.237.31	208.90....	jungledis...	Allowed	Wildcard	http://downloads.jung...		http://downloads.jungledisk.com/onlinediskcheck.txt
2/28/2011 9:34:...	Web Based ...	208.90.237.31	208.90....	jungledis...	Allowed	Wildcard	http://downloads.jung...		http://downloads.jungledisk.com/onlinediskcheck.txt
2/28/2011 10:03...	Web Based ...	208.90.238.44	208.90....	jungledis...	Allowed	Wildcard	http://downloads.jung...		http://downloads.jungledisk.com/onlinediskcheck.txt
2/28/2011 10:33...	Web Based ...	208.90.238.44	208.90....	jungledis...	Allowed	Wildcard	http://downloads.jung...		http://downloads.jungledisk.com/onlinediskcheck.txt
2/28/2011 10:34...	Web Based ...	208.90.238.44	208.90....	jungledis...	Allowed	Wildcard	http://downloads.jung...		http://downloads.jungledisk.com/onlinediskcheck.txt
2/28/2011 11:04...	Web Based ...	208.90.238.44	208.90....	jungledis...	Allowed	Wildcard	http://downloads.jung...		http://downloads.jungledisk.com/onlinediskcheck.txt
2/28/2011 11:05...	Web Based ...	208.90.238.46	208.90....	evernote....	Allowed	URL	http://www.evernote....		http://www.evernote.com/about/download/iphone/Prem...
2/28/2011 11:05...	Web Based ...	208.90.238.46	208.90....	evernote....	Allowed	URL	http://www.evernote....		http://www.evernote.com/about/download/iphone/Tips/...
2/28/2011 11:07...	Web Based ...	208.90.238.44	208.90....	jungledis...	Allowed	Wildcard	http://downloads.jung...		http://downloads.jungledisk.com/onlinediskcheck.txt
2/28/2011 11:09...	Web Based ...	208.90.238.44	208.90....	jungledis...	Allowed	Wildcard	http://downloads.jung...		http://downloads.jungledisk.com/onlinediskcheck.txt
2/28/2011 11:15...	Web Based ...	208.90.238.44	208.90....	jungledis...	Allowed	Wildcard	http://downloads.jung...		http://downloads.jungledisk.com/onlinediskcheck.txt

Fig. 4:3-4 Detail by page drill down report

- **Save** - Click this button to go to the Save Report panel where you save your report criteria now but generate your report later (see Step F and Saved Reports).

Step F: Save Report panel

1. Click the **Save** button to display the Basic Options tab of the Report Wizard > Save Report panel:



Output type: E-Mail As Attachment

Format: PDF

Category: N/A

User IP: N/A

Users: N/A

Site: N/A

Category Group: N/A

User Group: N/A

Keywords:

Fig. 4:3-5 Report Wizard's Save Report panel Basic Options tab

This panel is similar in design to the Save Report pop-up window that displays when saving a drill down report (see Chapter 2: Drill Down Reports). However, the Date Scope does not display in this panel.

2. In the **Save Name** field, enter a name for the report. This name will display in the Reports > Saved Reports list box.

TIP: *The Copy (Ctrl+C) and Paste (Ctrl+V) functions can be used in the fields in this screen.*

3. In the **Description** field, enter the report description.
4. Specify **E-Mail** criteria:

- **To** and **Subject**, and optional fields for Body, Cc, and Bcc.
- **Hide un-identified IPs** checkbox is de-selected by default if the “Hide Unidentified IPs” checkbox is de-selected in the Default Report Settings panel.

***NOTE**: The Default Report Settings panel is accessible via Administration > Default Report Settings. See the Default Report Settings sub-section in Chapter 3 of the Report Manager Administration Section for more information about the Hide Unidentified IPs option.*

- **Output type** - Choose either “E-Mail As Attachment”, or “E-Mail As Link”.
- **Format** - Choose from available output format selections in the pull-down menu.

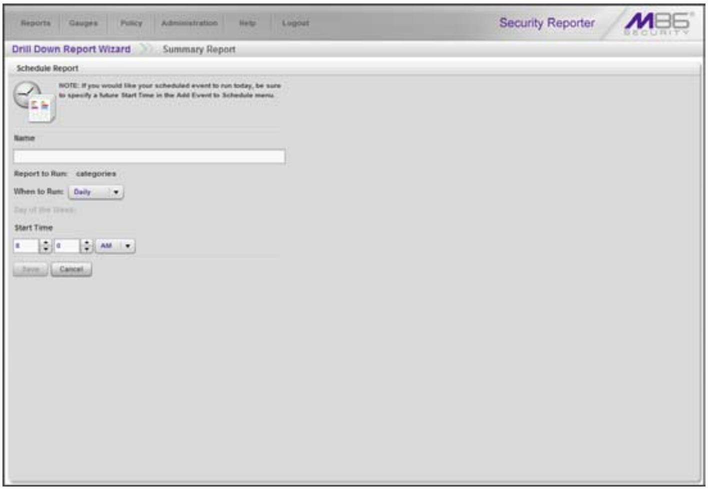
***NOTE**: Any selected filter options display to the right.*

5. Click the Advanced Options tab for additional options:

    - **Group By** - Available selections are based on the type of report specified.
    - For summary drill down reports:
        - at the **For additional-break reports only** field, if a selection was made in the Group By field, specify the top count option to be used in the **# Records** and **Sort By** fields.
        - at the **For pie and bar charts only** section, the activated **Generate using** field lets you select the count column sort option.
    - For detail drill down reports, specify any of the following options:
        - **Detailed Info** - Uncheck any checkbox corresponding to a column that should not be included in the report.
        - **Limit Detail Result** - Indicate the maximum number of records to be included in the report, and

whether these records will only include blocked end user queries, or also records of non-blocked end user queries.

6. Specify the next—or final—step in the wizard by selecting one of three choices:
   - **Save and Schedule** - Click this button to save your entries and to go to the Schedule Report panel where you set up a schedule for running the drill down report:



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

Name

Report to Run: categories

When to Run: Daily

Day of the Week:

Start Time

8 0 AM

Fig. 4:3-6 Report Wizard’s Schedule Report panel

a. Enter a **Name** for the event.

b. Select the **Report to Run** from the list.

c. 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).

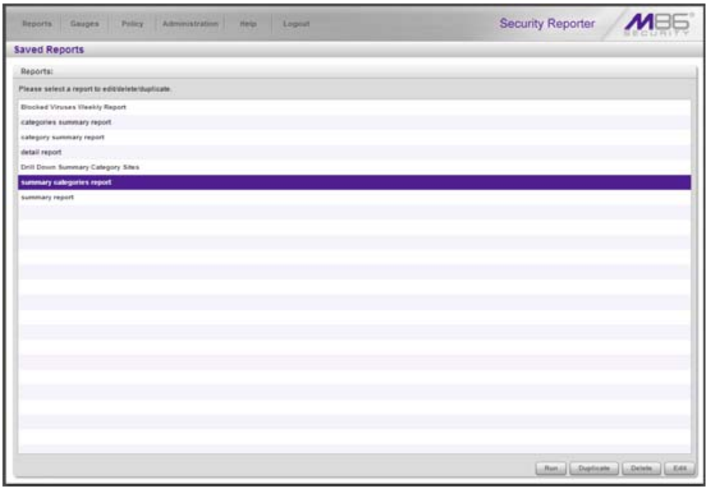
d. Select the **Start Time** for the report: 1 - 12 for the hour, 0 - 59 for the minutes, and AM or PM.

***NOTE**: The default Start Time is 8:00 AM. If you wish to run a report today and this time has already passed, be sure to select a future time.*

e. Click **Save** to save your report schedule settings and to go to the Report Schedule panel where the report is now included in the list (see Fig. 4:3-13).

***TIP**: Click **Cancel** to save the report and to return to the Report Wizard panel without scheduling a time for running the report.*

- **Save and Email** - Click this button to save your entries and to email the generated report to the designated recipient(s). After the report is emailed, the Saved Reports panel displays if you need to run this report again or another report.



Please select a report to edit/delete/duplicate.

Blocked Viruses Weekly Report
categories summary report
category summary report
detail report
Drill Down Summary Category Sites
summary categories report
summary report

Fig. 4:3-7 Saved Reports panel

***NOTE**: If more than one username or if any keyword was entered in the Report Wizard for a detail report, the Save and Email button is greyed-out.*

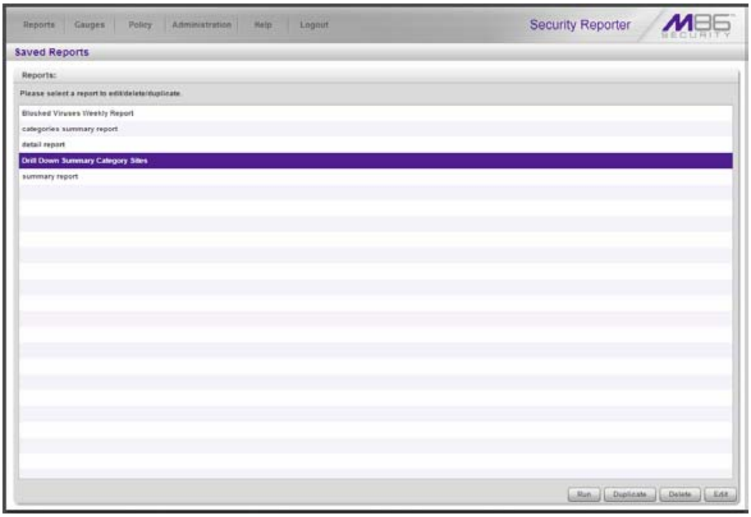
- **Save Only** - Click this button to save your entries and to go to the Saved Reports panel where you can delete, edit, or run this report or another report.

***NOTE**: See Report Schedule and Saved Reports in this chapter for information on using these options.*

Saved Reports

The Saved Reports option lets you view, copy, or edit data in a report you created, run a report, or delete a report.

In the navigation toolbar, mouse over the Reports menu link and select **Saved Reports** to display the Saved Reports panel that displays any drill down reports or security reports you saved:



Saved Reports

Reports:

Please select a report to edit/delete/duplicate

Blocked Viruses Weekly Report
categories summary report
detail report
Drill Down Summary Category Sites
summary report

Fig. 4:3-8 Saved Reports panel

To perform any action in this panel, select the report name from the list to activate the buttons at the bottom right corner.

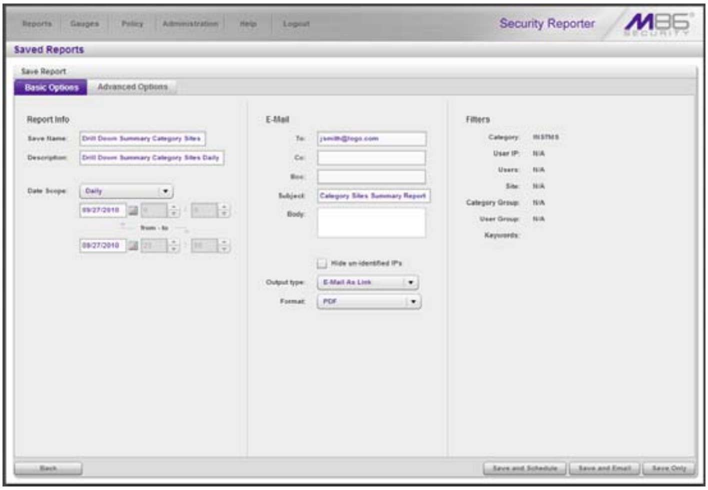
***TIP**: On the Save Report panel discussed in this sub-section, click **Back** to return to the Saved Reports panel without saving your edits or performing any other action.*

***NOTES**: Refer to Report View Components in Chapter 2: Drill Down Reports for information on using the fields in the Save Report panel discussed on the following pages in this sub-section. Refer to the Security Reports Section for information on security reports.*

Edit a Report

Edit a Drill Down Report

1. To edit a drill down report, click **Edit** to display the Save Report panel where you edit report settings for a saved report:



Save Name: Drill Down Summary Category Sites
Description: Drill Down Summary Category Sites Daily
Date Scope: Daily
09/27/2010
09/27/2010
To: jsmith@logo.com
Cc:
Bcc:
Subject: Category Sites Summary Report
Body:
□ Hide un-identified IP's
Output type: E-Mail As Link
Format: PDF
Category: INSTMS
User IP: N/A
Users: N/A
Site: N/A
Category Group: N/A
User Group: N/A
Keywords:

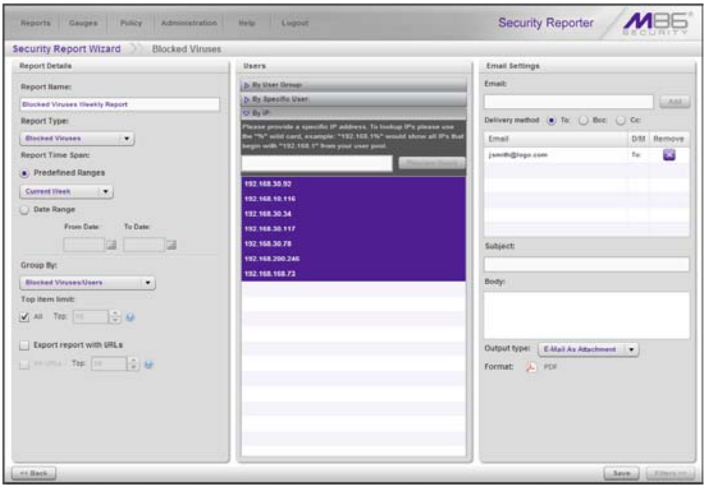
Fig. 4:3-9 Save Report, edit summary drill down report

***TIP**: The Copy (Ctrl+C) and Paste (Ctrl+V) functions can be used in the fields in the Save Report panel.*

2. After making your selections and entries on the Basic Options tab and Advanced Options tab (as described in Save Report panel in this chapter, and for the Save button option in Chapter 2), click **Save Only**.

Edit a Security Report

1. To edit a security report, click **Edit** to display the Security Report Wizard panel where you edit report settings for a saved report:



Report Name: Blocked Viruses Weekly Report

Report Type: Blocked Viruses

Report Time Span:
● Predefined Ranges: Current Week
○ Date Range — From Date: To Date:

Group By: Blocked Viruses/Users

Top item limit: ☑ All Top:

□ Export report with URLs

Please provide a specific IP address. To lookup IP's please use the "%" wild card, example: "192.168.1%" would show all IP's that begin with "192.168.1" from your user pool.

192.168.30.92
192.168.10.116
192.168.30.34
192.168.30.117
192.168.30.78
192.168.200.246
192.168.168.73

Email:

Delivery method ● To: ○ Bcc: ○ Cc:

Email	D/M	Remove
jsmith@logo.com	To:	☒

Subject:

Body:

Output type: E-Mail As Attachment

Format: PDF

Fig. 4:3-10 Save Report, edit Security Report

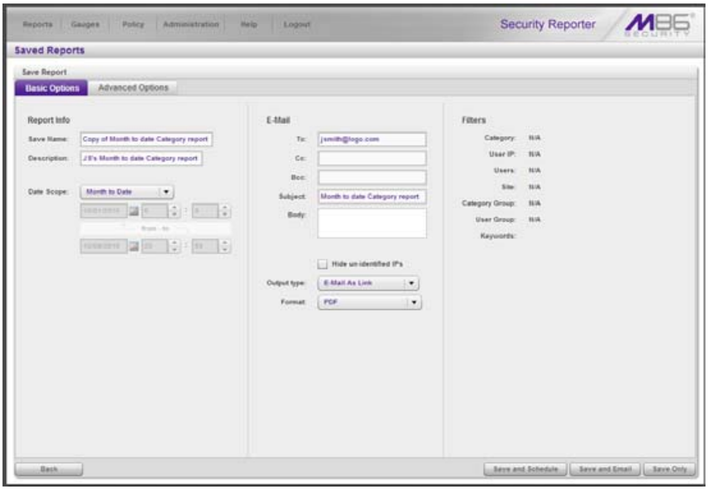
***TIP**: The Copy (Ctrl+C) and Paste (Ctrl+V) functions can be used in the fields in this panel.*

2. After making your selections and entries in the Report Details, Users, and Email Settings frames—and Filters panel, if available for use—(as described in Chapter 2: Security Report Wizard from the Security Reports Section), click **Save**.

Copy a Saved Report

The copy feature is a great time saver, letting you use settings from a saved drill down report.

1. In the Saved Reports panel, select the report from the list.
2. Click **Duplicate** to display the panel for the specified report:
   - Save Report panel for a drill down report:



Report Info

Save Name: Copy of Month to date Category report

Description: JB's Month to date Category report

Date Scope: Month to Date

E-Mail

To: jsmith@logo.com

Cc:

Bcc:

Subject: Month to date Category report

Body:

☐ Hide un-identified IP's

Output type: E-Mail As Link

Format: PDF

Filters

Category: N/A

User IP: N/A

Users: N/A

Site: N/A

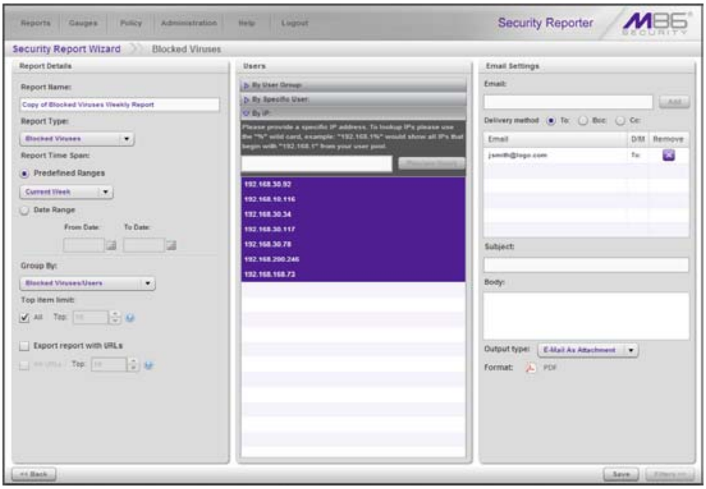
Category Group: N/A

User Group: N/A

Keywords:

Fig. 4:3-11 Save Report, duplicate report

- Security Report Wizard panel for a security report:



Report Details

Report Name: Copy of Blocked Viruses Weekly Report

Report Type: Blocked Viruses

Report Time Span:

● Predefined Ranges: Current Week

○ Date Range — From Date: To Date:

Group By: Blocked Viruses/Users

Top item limit: ☑ All Top:

□ Export report with URLs

□ All URLs Top:

Users

By User Group:

By Specific User:

By IP:

Please provide a specific IP address. To lookup IPs please use the "%" wild card, example: "192.168.1%" would show all IPs that begin with "192.168.1" from your user pool.

192.168.30.92
192.168.10.116
192.168.30.34
192.168.30.117
192.168.30.78
192.168.200.246
192.168.168.73

Email Settings

Email:

Delivery method ● To: ○ Bcc: ○ Cc:

Email	D/M	Remove
jsmith@logo.com	To:	☒

Subject:

Body:

Output type: E-Mail As Attachment

Format: PDF

Fig. 4:3-12 Security Report Wizard, duplicate report

***NOTE**: The Report Name field displays the text "Copy of 'X'", in which 'X' represents the report name of the report being copied. Edit this text if you wish to modify this report name.*

3. After making your selections and entries in the panel:
   - Click **Save Only** in the Save Report panel.
   - Click **Save** in the Security Report Wizard panel.

Run a Saved Report

1. In the Saved Reports panel (see Fig. 4:3-8), select the report from the list.
2. Click **Run** to generate the report view and email the report to the specified recipient(s).

Delete a Report

To remove the report from choices available in the Report Name list, and the list in the Report Schedule panel:

1. In the Saved Reports panel (see Fig. 4:3-8), select the report from the list.
2. Click **Delete** to open the Confirmation dialog box with the message: “Are you sure you wish to delete the report? Event schedules associated will also be deleted.”
3. Click **Yes** to close the dialog box and delete the report.

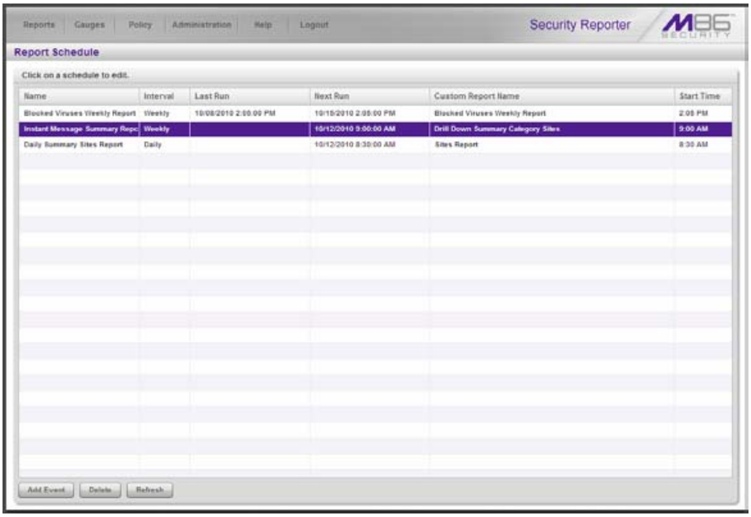
TIP*: Click* ***No*** *to close the dialog box without deleting the report.*

NOTE*: If a report is scheduled to run via the Report Schedule option, deleting the report removes it from the Report Schedule list.*

Report Schedule

The Report Schedule option is used for maintaining a schedule for generating a customized drill down or security report.

In the navigation toolbar, mouse over the Reports menu link and select **Report Schedule** to display the Report Schedule panel:



Report Schedule

Click on a schedule to edit.

Name	Interval	Last Run	Next Run	Custom Report Name	Start Time
Blocked Viruses Weekly Report	Weekly	10/08/2010 2:00:00 PM	10/15/2010 2:05:00 PM	Blocked Viruses Weekly Report	2:05 PM
Instant Message Summary Repc	Weekly		10/12/2010 9:00:00 AM	Drill Down Summary Category Sites	9:00 AM
Daily Summary Sites Report	Daily		10/12/2010 8:30:00 AM	Sites Report	8:30 AM

Fig. 4:3-13 Report Schedule panel

In the Report Schedule panel, 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 (H:MM AM/PM) for the report to run.

NOTES*: Records in this panel may include drill down reports and security reports. Security reports are scheduled to run via the Schedule Settings option in the Security Report Wizard (see the Security Reports Section for more information about the Security Report Wizard).*

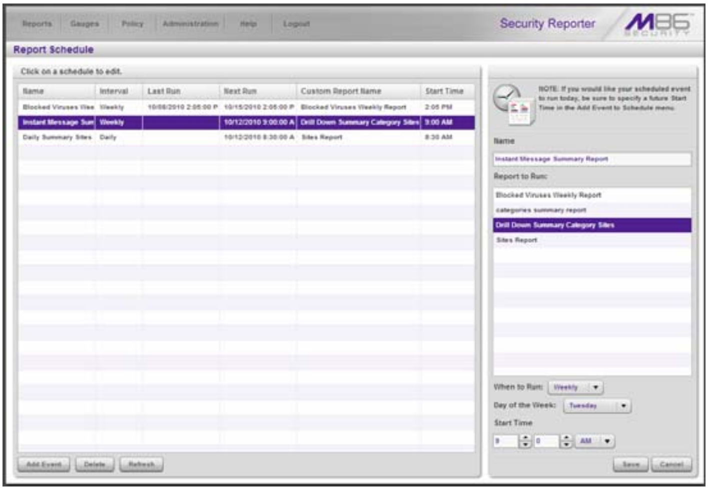
Click the **Refresh** button to refresh the list of records and to scroll to the top of the list.

***NOTE**: Refer to these sub-sections for information about the following topics:*

- *To save drill down reports, see the Saved Reports sub-section and the Save Report panel from the Report Wizard sub-section in this chapter, and the Save button sub-section in Chapter 2: Drill Down Reports.*
- *To save security reports, see the Security Reports Section—Save a Security Report in Chapter 1, and Chapter 2: Security Report Wizard.*
- *To enable or disable the Report Manager to run scheduled reports, see the Report Manager screen sub-section of the System Configuration Section in this User Guide.*

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 the report schedule details frame to the right of the table of report records:



Report Schedule

Click on a schedule to edit.

Name	Interval	Last Run	Next Run	Custom Report Name	Start Time
Blocked Viruses Wee	Weekly	10/08/2010 2:05:00 P	10/15/2010 2:05:00 P	Blocked Viruses Weekly Report	2:05 PM
Instant Message Sum	Weekly		10/12/2010 9:00:00 A	Drill Down Summary Category Sites	9:00 AM
Daily Summary Sites	Daily		10/12/2010 8:30:00 A	Sites Report	8:30 AM

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

Name: Instant Message Summary Report

Report to Run:
Blocked Viruses Weekly Report
categories summary report
Drill Down Summary Category Sites
Sites Report

When to Run: Weekly

Day of the Week: Tuesday

Start Time: 9 0 AM

Fig. 4:3-14 View report schedule details

The following information displays in this frame: 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.*

Edit a Scheduled Report Run Event

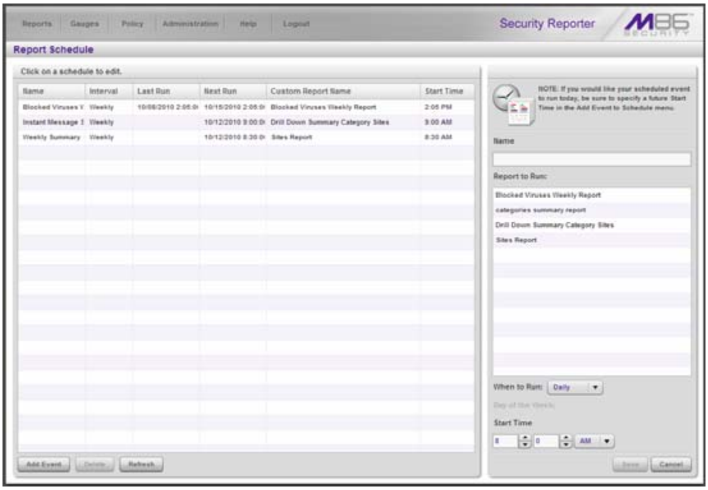
1. To edit criteria for a report scheduled to run, do the following in the report schedule details frame:
   - change the **Name** of the report
   - make different selections as necessary from the pull-down menus for **Report to Run**, **When to Run**, and/or **Day of the Week** or **Day of the Month**
   - change the **Start Time** for running the report

TIP*: Click* ***Cancel*** *if you wish to return to the Report Schedule panel without saving your edits.*

2. Click **Save** to display the updated criteria in the Report Schedule panel.

Add a Report Run Event to the Schedule

1. In the Report Schedule panel, click **Add Event** to display the report schedule details frame to the right side of the panel:



Report Schedule

Click on a schedule to edit.

Name	Interval	Last Run	Next Run	Custom Report Name	Start Time
Blocked Viruses V	Weekly	10/08/2010 2:05:0	10/15/2010 2:05:0	Blocked Viruses Weekly Report	2:05 PM
Instant Message 1	Weekly		10/12/2010 9:00:0	Drill Down Summary Category Sites	9:00 AM
Weekly Summary	Weekly		10/12/2010 8:30:0	Sites Report	8:30 AM

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

Name

Report to Run:

Blocked Viruses Weekly Report
categories summary report
Drill Down Summary Category Sites
Sites Report

When to Run: Daily

Day of the Week:

Start Time

8 : 0 AM

Fig. 4:3-15 Add an event to the schedule

2. Enter a **Name** for the report run event you are scheduling.
3. Select the **Report to Run** from the list.
4. 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).
5. Select the **Start Time** for the report: 1 - 12 for the hour, 0 - 59 for the minutes, and AM or PM.

***NOTE**: The default Start Time is 8:00 AM. If you wish to run a report today and this time has already passed, be sure to select a future time.*

***TIP**: Click **Cancel** to return to the Report Schedule panel without saving your edits.*

6. Click **Save** to add the scheduled event to the list of reports to run.

Delete a Scheduled Report Run Event

1. In the Report Schedule panel, select the report record from the list and click the **Delete**; this action opens a dialog box with the message: “Are you sure you want to delete this event?”
2. Click **Yes** to close the dialog box and remove the record from the list.

***TIP**: Click **Cancel** to return to the Report Schedule panel without deleting the record from the list of reports scheduled to run.*

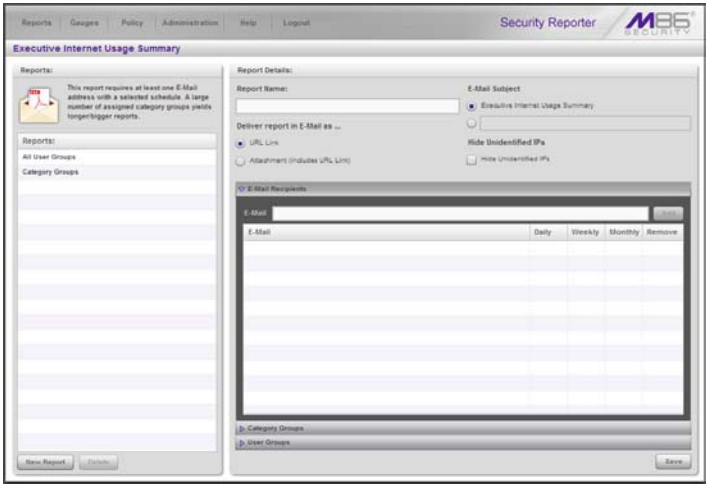
Chapter 4: Specialized Reports

The following types of productivity reports from the Reports menu of the Report Manager are described in this chapter: Executive Internet Usage Summary Reports, Blocked Request Reports, and Time Usage Reports.

Executive Internet Usage Summary

The Executive Internet Usage Summary option is used for specifying email addresses of users authorized to receive daily, weekly, and/or monthly bar and line chart productivity reports showing activity in library category groups or user groups of your choice.

In the navigation toolbar, mouse over the Reports menu link and select **Executive Internet Usage Summary** to display the Executive Internet Usage Summary panel:



This report requires at least one E-Mail address with a selected schedule. A large number of assigned category groups yields longer/bigger reports.

E-Mail Subject: ● Executive Internet Usage Summary ○

Deliver report in E-Mail as ...: ● URL Link ○ Attachment (includes URL Link)

Hide Unidentified IPs: □ Hide Unidentified IPs

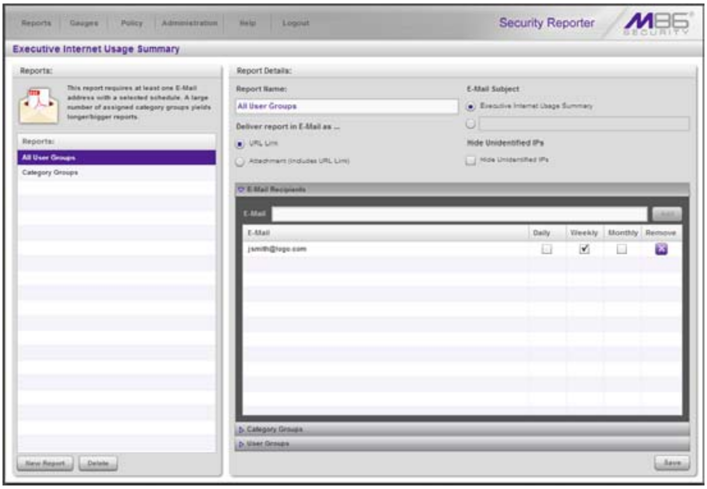
E-Mail	Daily	Weekly	Monthly	Remove

Fig. 4:4-1 Executive Internet Usage Summary panel

This panel contains the Reports frame listing saved report names, and the Report Details frame used for configuring reports.

View, Edit Report Settings

1. In the Reports frame, select the report name to display report setting criteria in the Report Details frame.



Executive Internet Usage Summary

Reports:

This report requires at least one E-Mail address with a selected schedule. A large number of assigned category groups yields longer/bigger reports.

Reports:
All User Groups
Category Groups

Report Details:

Report Name: All User Groups

Deliver report in E-Mail as ...
● URL Link
○ Attachment (includes URL Link)

E-Mail Subject
● Executive Internet Usage Summary
○

Hide Unidentified IPs
□ Hide Unidentified IPs

▽ E-Mail Recipients

E-Mail

E-Mail	Daily	Weekly	Monthly	Remove
jsmith@logo.com	□	☑	□	☒

▷ Category Groups
▷ User Groups

Fig. 4:4-2 Executive Internet Usage Summary report details

The following information displays and can be viewed and edited: Report Name, E-Mail Subject criteria, Deliver report in E-Mail as... selection, Hide Unidentified IPs choice, E-Mail Recipients list and report delivery schedule, and Category Groups and/or User Groups selection(s).

2. Click **Save** to update any modifications made to these report settings.

Add a New Report

1. At the bottom of the Reports frame, click **New Report** to clear the panel.

2. At the top of the Report Details frame, enter the **Report Name** to be used.

3. In the **Deliver report in E-Mail as...** section, by default the “URL Link” option is selected, indicating the email will only include a URL link to the report.

   To specify that both a URL link to the report and an attachment of the report will be included in the email, choose the “Attachment (includes URL Link)” option.

4. In the **E-Mail Subject** section, by default the “Executive Internet Usage Summary” option is selected, indicating the subject line to be used in the email.

   To create a custom subject line for the email, select the radio button to the left of the blank field below, and make an entry in the text box for the subject line to be used in the email.

5. In the **Hide Unidentified IPs** section, by default the **Hide Unidentified IPs** checkbox is de-selected. This indicates that activity on machines not assigned to specific users will be included in reports.

   If you wish to exclude activity from machines not assigned to specific users, click in the checkbox to enter a check mark.

***NOTE**: If enabling this feature, the generated report will only hide hit counts for IP addresses in sections of the report labeled “Users.” IP hit counts **will be included** for all other sections of the report, such as those labeled “Categories”, “Category Groups”, etc.*

6. In the E-Mail Recipients accordion, specify the user(s) to receive the report and the frequency of delivery.

a. Click in the empty field and type in the **E-Mail** address.

b. Click **Add** to clear the field and to add the email address in the list box below.

c. By default, checkmarks populate the frequency checkboxes: **Daily**, **Weekly**, **Monthly**. This indicates reports will be emailed to the recipient at the specified intervals.

To change these settings, click the checkbox to remove the selection.

Follow the steps above to add additional recipients.

***TIP**: To remove a recipient from the list of users authorized to receive reports, click the 'X' in the **Remove** column.*

7. Click to open the Category Groups and/or User Groups accordion(s) and specify groups for inclusion in the report:

   - In the Category Groups accordion, select the category group(s) from the Available M86 Category Groups and Custom Category Groups, and then click **Add Category Group** to move the selection(s) to the Selected list box.

     By default, the following categories are included in the Selected list box: Adult Content, Security, and Illegal/ Questionable.

***TIPS**: Multiple category groups can be selected by clicking each category group while pressing the Ctrl key on your keyboard. Blocks of category groups can be selected by clicking the first category group, and then pressing the Shift key on your keyboard while clicking the last category group.*

*To remove a category group from the Selected list box, select the category group and then click **Remove Category Group**.*

   - In the User Groups accordion, select the user group(s) from the Available User Groups, and then click **Add User Group** to move the selection(s) to the Selected list box.

***TIPS**: Multiple user groups can be selected by clicking each user group while pressing the Ctrl key on your keyboard. Blocks of user groups can be selected by clicking the first user group, and then pressing the Shift key on your keyboard while clicking the last user group.*

*To remove a user group from the Selected list box, select the user group and then click **Remove User Group**.*

8. Click **Save** to save all settings made in this panel and to include the new report in the Reports list box.

Sample Executive Internet Usage report

The recipient of the Executive internet Usage Summary report receives an email containing a link to the report, and a .pdf attachment of the report, if specified (if the size of the .pdf file is within the limits).

Links are available for the following time frame:

- Daily reports (14 days)
- Weekly reports (30 days)
- Monthly reports (90 days)

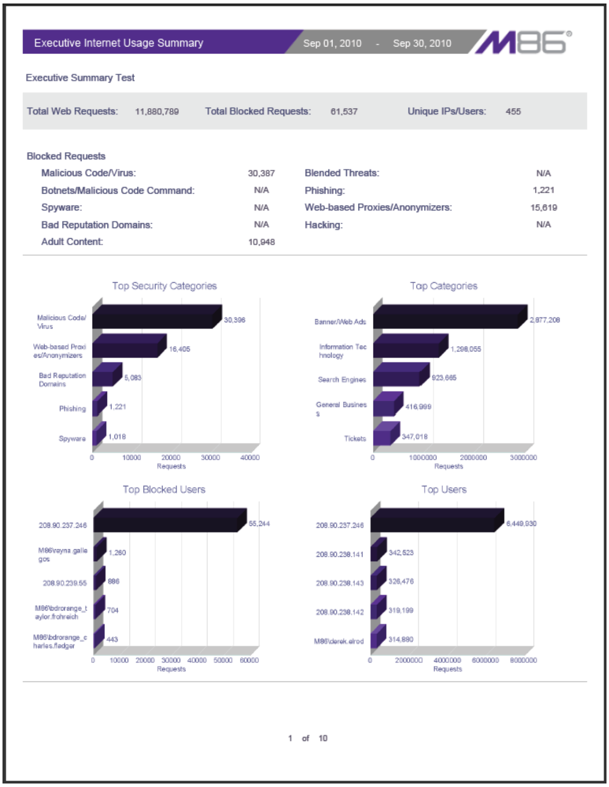
The header of the generated report includes the title and date range. The footer includes the page number and page range.

The first page includes statistics for the following: Total Web Requests, Total Blocked Requests, Unique IPs/Users.

Total Blocked Requests are given for the following library categories: Malicious Code/Virus, Botnets/Malicious Code Command, Spyware, Bad Reputation Domains, Adult Content, Blended Threats, Phishing, Web-based Proxies/ Anonymizers, Hacking.

***NOTE**: Blended Threats is not currently used and displays “N/A.”*

Bar charts for Top Security Risks (library categories), Top Categories, Top Blocked Users, and Top Users show the top five categories/users and their corresponding total Requests.



Executive Internet Usage Summary   Sep 01, 2010 - Sep 30, 2010

Executive Summary Test

Total Web Requests: 11,880,789   Total Blocked Requests: 61,537   Unique IPs/Users: 455

Blocked Requests

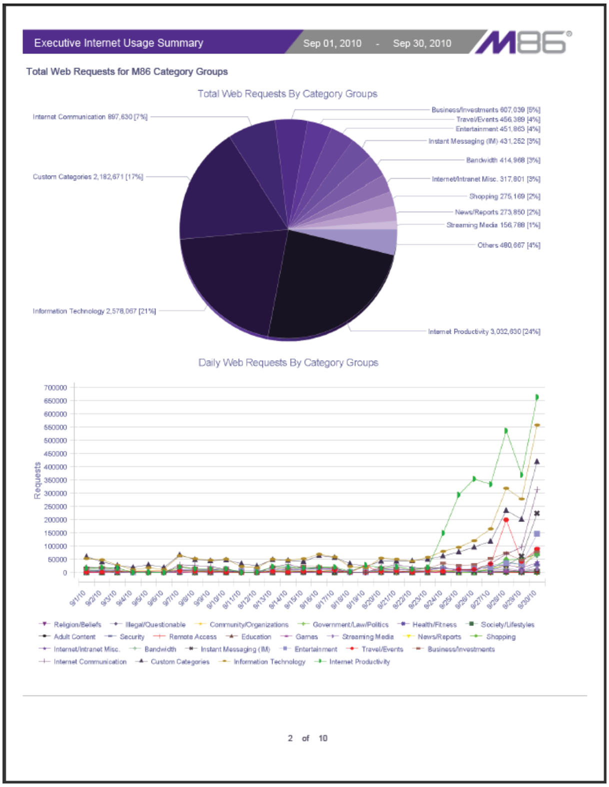
Malicious Code/Virus:	30,387	Blended Threats:	N/A
Botnets/Malicious Code Command:	N/A	Phishing:	1,221
Spyware:	N/A	Web-based Proxies/Anonymizers:	15,619
Bad Reputation Domains:	N/A	Hacking:	N/A
Adult Content:	10,948		

1 of 10

Fig. 4:4-3 Executive Internet Usage Summary monthly report, page 1

The second page includes a pie chart depicting Total Web Requests for M86 Category Groups. Each category group in the chart is represented by a pie slice and shows the number of requests and overall percentage for that pie slice.

For Weekly and Monthly reports, the bottom half of the second page includes a line chart for Daily Web Requests by Category Groups. Each category group in the chart is represented by a colored symbol that can be identified by the key at the bottom of the page. The range of Requests is shown to the left of the chart, and the days (M/D/YY) are shown beneath the chart.



Executive Internet Usage Summary Sep 01, 2010 - Sep 30, 2010

Total Web Requests for M86 Category Groups

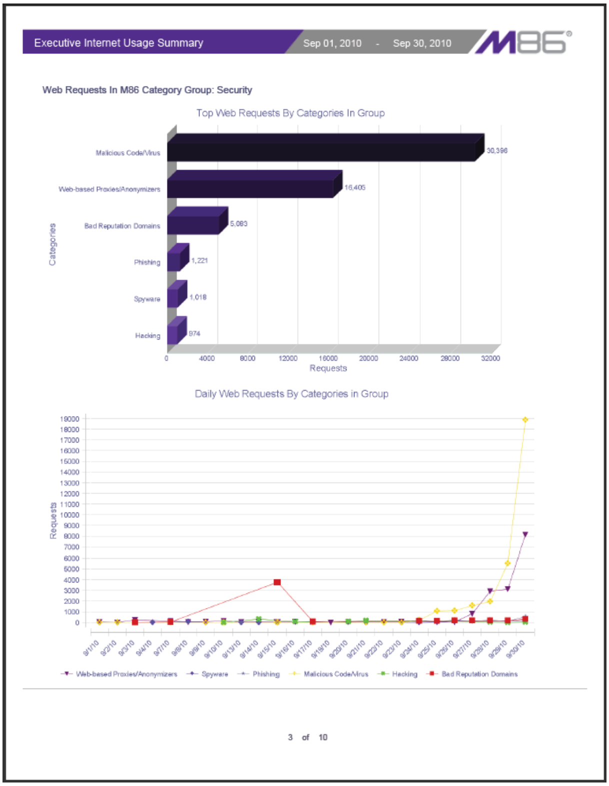
2 of 10

Fig. 4:4-4 Executive Internet Usage Summary monthly report, page 2

The third page includes a bar chart depicting Top Web Requests By Categories In Group 'X', in which 'X' represents the name of the category group. The top 15 affected library categories in the group are named in the Categories list to the left, and each library category is represented in the chart by a bar and corresponding number of requests. The range of Requests is shown beneath the chart.

For Weekly and Monthly reports, the bottom half of the third page includes a line chart for Top Daily Web Requests by

Categories in Group. Each library category in the chart is represented by a colored symbol that can be identified by the key at the bottom of the page. The range of Requests is shown to the left of the chart, and the days (M/D/YY) are shown beneath the chart.



Executive Internet Usage Summary Sep 01, 2010 - Sep 30, 2010

Web Requests In M86 Category Group: Security

Top Web Requests By Categories In Group

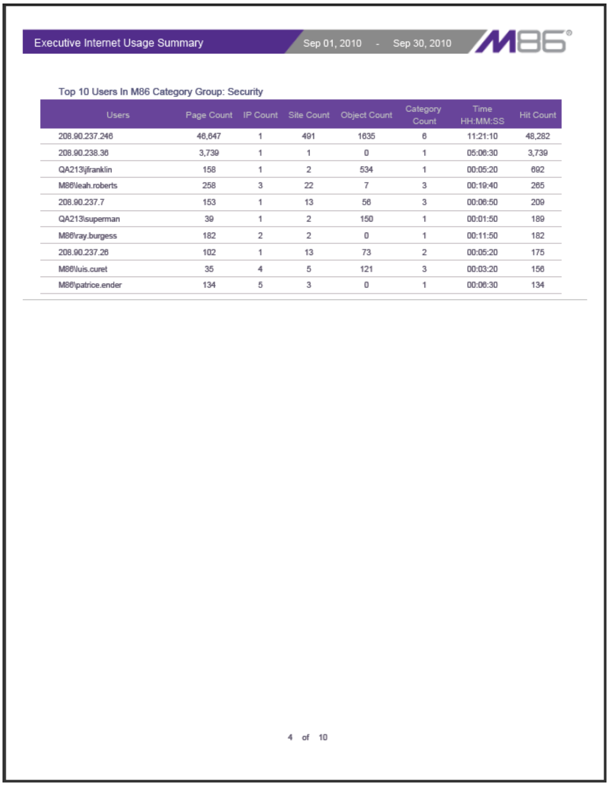
Daily Web Requests By Categories in Group

3 of 10

Fig. 4:4-5 Executive Internet Usage Summary monthly report, page 3

For Daily reports, the bottom half of the third page includes a chart showing the Top 10 Users In Category Group ‘X’, in which ‘X’ represents the name of the category group. The top 10 Users are listed in this chart, along with each user’s corresponding Page Count, IP Count, Site Count, Category Count, Time HH:MM:SS, and Hit Count.

For Weekly and Monthly reports, the fourth page includes the Top 10 Users In Category Group ‘X’ chart:



Executive Internet Usage Summary Sep 01, 2010 - Sep 30, 2010

Top 10 Users In M86 Category Group: Security

Users	Page Count	IP Count	Site Count	Object Count	Category Count	Time HH:MM:SS	Hit Count
208.90.237.246	46,647	1	491	1635	6	11:21:10	48,282
208.90.238.36	3,739	1	1	0	1	05:06:30	3,739
QA213\jfranklin	158	1	2	534	1	00:05:20	692
M86\leah.roberts	258	3	22	7	3	00:19:40	265
208.90.237.7	153	1	13	56	3	00:06:50	209
QA213\superman	39	1	2	150	1	00:01:50	189
M86\ray.burgess	182	2	2	0	1	00:11:50	182
208.90.237.26	102	1	13	73	2	00:05:20	175
M86\luis.curet	35	4	5	121	3	00:03:20	156
M86\patrice.ender	134	5	3	0	1	00:06:30	134

4 of 10

Fig. 4:4-6 Executive Internet Usage Summary monthly report, page 4

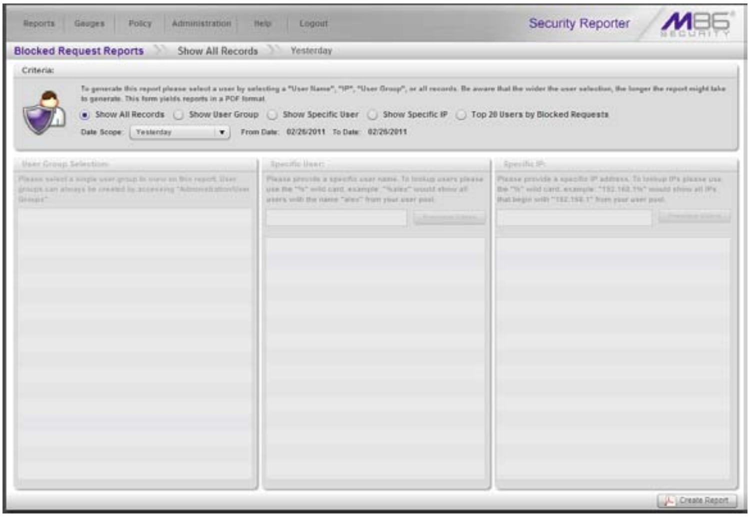
The balance of the report is comprised of statistics for each of the remaining category groups, represented by report page 3, and page 4 for Weekly and Monthly reports.

Blocked Request Reports

The Blocked Request Reports option is used for obtaining results of blocked URLs end users attempted to access within a specified time period.

***NOTE**: If using a Web Filter only, the Blocked Request Reports option does not display if the Block Request Count feature is disabled in the System Configuration administrator console. Refer to the Optional Features screen sub-section of the System Configuration Section of this user guide for information about enabling or disabling the Block Request Count feature.*

In the navigation toolbar, mouse over the Reports menu link and select **Blocked Request Reports** to display the Blocked Request Reports panel:



To generate this report please select a user by selecting a "User Name", "IP", "User Group", or all records. Be aware that the wider the user selection, the longer the report might take to generate. This form yields reports in a PDF format.

● Show All Records ○ Show User Group ○ Show Specific User ○ Show Specific IP ○ Top 20 Users by Blocked Requests

Date Scope: Yesterday ▾ From Date: 02/26/2011 To Date: 02/26/2011

Please select a single user group to view on this report. User groups can always be created by accessing "Administration/User Groups"

Please provide a specific user name. To lookup users please use the "%" wild card. example: "%ales" would show all users with the name "ales" from your user pool.

Please provide a specific IP address. To lookup IPs please use the "%" wild card. example: "192.168.1%" would show all IPs that begin with "192.168.1" from your user pool.

Fig. 4:4-7 Blocked Request Reports panel

Generate a Blocked Request Report

To generate a Blocked Request Report:

1. In the Criteria frame, specify the type of report to be generated by clicking the radio button corresponding to that option, and—if necessary—making entries/selections in pertinent fields:

   - **Show All Records -** If choosing this option, the Date Scope field displays "Yesterday" and yesterday's date.
   - **Show User Group -** If choosing this option, select the user group from the User Group Selection list box below. The Date Scope field displays "Yesterday" and yesterday's date.
   - **Show Specific User -** If choosing this option, enter the username—or a portion of the username with the '%' wildcard—in the Specific User frame, and then click **Preview Users** to display results in the list box below. Select the user, and then make a selection from the **Date Scope** field to display the date range for that time period: Yesterday, Last Week, Last Month, Week to Yesterday, Month to Yesterday.
   - **Show Specific IP -** If choosing this option, enter the IP address—or a portion of the IP address with the '%' wildcard—in the Specific IP frame, and then click **Preview Users** to display results in the list box below. Select the user IP address, and then make a selection from the **Date Scope** field to display the date range for that time period: Yesterday, Last Week, Last Month, Week to Yesterday, Month to Yesterday.
   - **Top 20 Users by Blocked Requests -** If choosing this option, make a selection from the **Date Scope** field to display the date range for that time period: Yesterday, Last Week, Last Month, Week to Yesterday, Month to Yesterday.

2. Click **Create Report** to generate the report view in the PDF format.

   As with other reports exported in the PDF format, this report can be saved and/or printed.

NOTES*: If there is no data available—or if data is available for only a partial number of days within the date scope range—a message displays indicating that no records are available.*

If a new user group with existing usernames or IP addresses was added, data for that user group will not be available for viewing on the current day. Data for the following viewing options are available according to this schedule:

- *Yesterday, Week to Yesterday, and Month to Yesterday - available by the next day*
- *Last Week - available by the next Sunday*
- *Last Month - available by the first of next month.*

If a new user group with new users was added, by the next day only the “Yesterday” viewing option will contain data available for viewing. All other viewing options will not be available until the full length of time indicated by the viewing option has transpired.

View the Blocked Request Report

The header of the generated Blocked Request Report includes the date range, Report Type, and criteria Details.

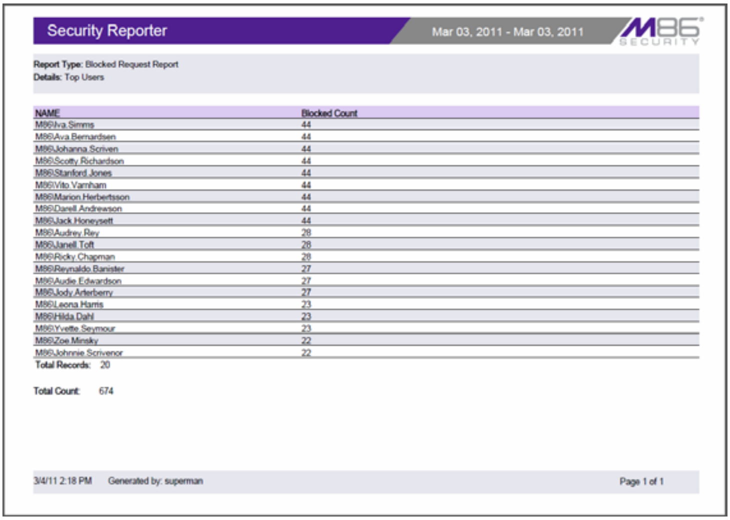
'RESULTS FOR: the date' displays above the NAME column header if the report criteria is other than "Top 20 Users by Blocked Requests".

In the body of the report, rows of records display beneath the following column headers: end user NAME, IP address (if the report criteria is other than "Top 20 Users by Blocked Requests"), and Blocked Count quantity.

If the report was generated for any criteria other than "Top 20 Users by Blocked Requests", the Total for Day count displays beneath each section.

The footer of the report includes the Date and Time the report was generated, and Page number.

The Total Count for all blocked requests displays at the end of the report.



Report Type: Blocked Request Report
Details: Top Users

NAME	Blocked Count
M86\Iva.Simms	44
M86\Ava.Bernardsen	44
M86\Johanna.Scriven	44
M86\Scotty.Richardson	44
M86\Stanford.Jones	44
M86\Vito.Varnham	44
M86\Marion.Herbertsson	44
M86\Darell.Andrewson	44
M86\Jack.Honeysett	44
M86\Audrey.Rey	28
M86\Janell.Toft	28
M86\Ricky.Chapman	28
M86\Reynaldo.Banister	27
M86\Audie.Edwardson	27
M86\Jody.Arterberry	27
M86\Leona.Harris	23
M86\Hilda.Dahl	23
M86\Yvette.Seymour	23
M86\Zoe.Minsky	22
M86\Johnnie.Scrivenor	22

Total Records: 20

Total Count: 674

3/4/11 2:18 PM Generated by: superman Page 1 of 1

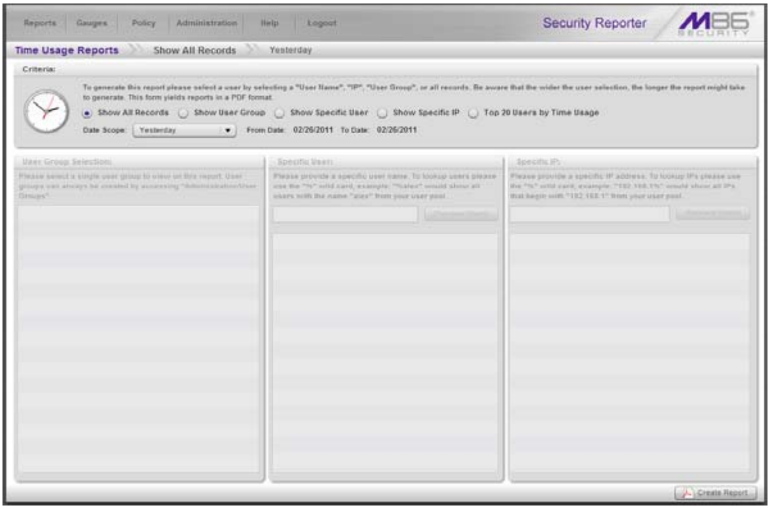
Fig. 4:4-8 Blocked Request Report for Top 20 Users

Time Usage Reports

The Time Usage Reports option is used for obtaining end user Internet usage activity for a specified time period, based on the Time Usage algorithm. This algorithm calculates the amount of time an end user spent accessing a given page or object, disregarding the number of seconds per hit, and counting each unique minute of Web time as one minute. Using this algorithm, an end user could never have more than 24 hours of Web time within a given 24-hour period.

NOTE*: The Time Usage Reports option does not display if the Time Usage feature is disabled in the System Configuration administrator console. Refer to the Optional Features screen sub-section of the System Configuration Section of this user guide for information about enabling or disabling the Time Usage feature.*

In the navigation toolbar, mouse over the Reports menu link and select **Time Usage Reports** to display the Time Usage Reports panel:



To generate this report please select a user by selecting a "User Name", "IP", "User Group", or all records. Be aware that the wider the user selection, the longer the report might take to generate. This form yields reports in a PDF format.

● Show All Records ○ Show User Group ○ Show Specific User ○ Show Specific IP ○ Top 20 Users by Time Usage

Date Scope: Yesterday ▾ From Date: 02/26/2011 To Date: 02/26/2011

User Group Selection:

Please select a single user group to view on this report. User groups can always be created by accessing "Administration/User Groups".

Specific User:

Please provide a specific user name. To lookup users please use the "%" wild card, example: "%ales" would show all users with the name "ales" from your user pool.

Specific IP:

Please provide a specific IP address. To lookup IPs please use the "%" wild card, example: "192.168.1%" would show all IPs that begin with "192.168.1" from your user pool.

Fig. 4:4-9 Time Usage Reports panel

Generate a Time Usage Report

To generate a Time Usage report:

1. In the Criteria frame, specify the type of report to be generated by clicking the radio button corresponding to that option, and—if necessary—making entries/selections in pertinent fields:

   - **Show All Records** - If choosing this option, the Date Scope field displays "Yesterday" and yesterday's date.
   - **Show User Group** - If choosing this option, select the user group from the User Group Selection list box below. The Date Scope field displays "Yesterday" and yesterday's date.
   - **Show Specific User** - If choosing this option, enter the username—or a portion of the username with the '%' wildcard—in the Specific User frame, and then click **Preview Users** to display results in the list box below. Select the user, and then make a selection from the **Date Scope** field to display the date range for that time period: Yesterday, Last Week, Last Month, Week to Yesterday, Month to Yesterday.
   - **Show Specific IP** - If choosing this option, enter the IP address—or a portion of the IP address with the '%' wildcard—in the Specific IP frame, and then click **Preview Users** to display results in the list box below. Select the user IP address, and then make a selection from the **Date Scope** field to display the date range for that time period: Yesterday, Last Week, Last Month, Week to Yesterday, Month to Yesterday.
   - **Top 20 Users by Time Usage** - If choosing this option, make a selection from the **Date Scope** field to display the date range for that time period: Yesterday, Last Week, Last Month, Week to Yesterday, Month to Yesterday.

2. Click **Create Report** to generate the report view in the PDF format.

   As with other reports exported in the PDF format, this report can be saved and/or printed.

NOTES*: If there is no data available—or if data is available for only a partial number of days within the date scope range—a message displays indicating that no records are available.*

If a new user group with existing usernames or IP addresses was added, data for that user group will not be available for viewing on the current day. Data for the following viewing options are available according to this schedule:

- *Yesterday, Week to Yesterday, and Month to Yesterday - available by the next day*
- *Last Week - available by the next Sunday*
- *Last Month - available by the first of next month.*

If a new user group with new users was added, by the next day only the "Yesterday" viewing option will contain data available for viewing. All other viewing options will not be available until the full length of time indicated by the viewing option has transpired.

View the Time Usage Report

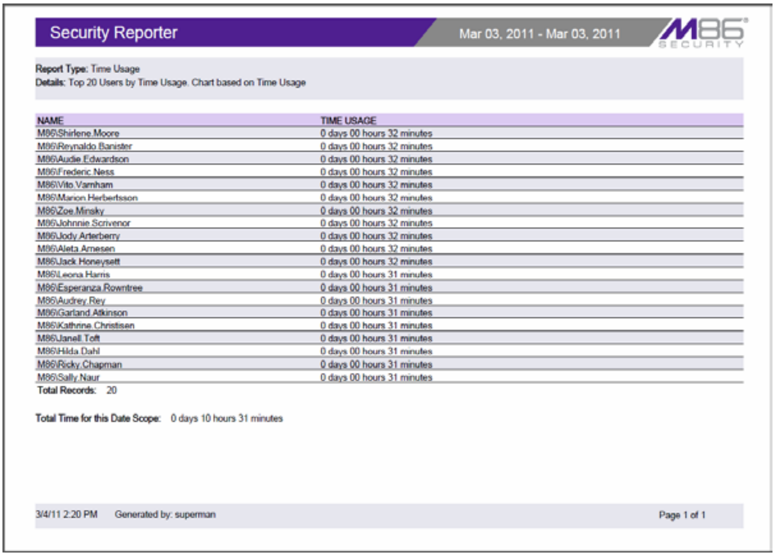
The header of the generated Time Usage report includes the date range, Report Type, and Details criteria.

The body of the report includes the end user NAME, TIME USAGE time totals in days, hours, and minutes, and any other relative criteria, such as username path or IP address.

The Total Records displays at the end of each section.

The footer of the report includes the Date and Time the report was generated, and Page number.

The Total Time for this Date Scope in days, hours, and minutes displays at the end of the report.



Security Reporter

Mar 03, 2011 - Mar 03, 2011

Report Type: Time Usage
Details: Top 20 Users by Time Usage. Chart based on Time Usage

NAME	TIME USAGE
M86\Shirlene.Moore	0 days 00 hours 32 minutes
M86\Reynaldo.Banister	0 days 00 hours 32 minutes
M86\Audie.Edwardson	0 days 00 hours 32 minutes
M86\Frederic.Ness	0 days 00 hours 32 minutes
M86\Vito.Varnham	0 days 00 hours 32 minutes
M86\Marion.Herbertsson	0 days 00 hours 32 minutes
M86\Zoe.Minsky	0 days 00 hours 32 minutes
M86\Johnnie.Scrivenor	0 days 00 hours 32 minutes
M86\Jody.Arterberry	0 days 00 hours 32 minutes
M86\Aleta.Arnesen	0 days 00 hours 32 minutes
M86\Jack.Honeysett	0 days 00 hours 32 minutes
M86\Leona.Harris	0 days 00 hours 31 minutes
M86\Esperanza.Rowntree	0 days 00 hours 31 minutes
M86\Audrey.Rey	0 days 00 hours 31 minutes
M86\Garland.Atkinson	0 days 00 hours 31 minutes
M86\Kathrine.Christisen	0 days 00 hours 31 minutes
M86\Janell.Toft	0 days 00 hours 31 minutes
M86\Hilda.Dahl	0 days 00 hours 31 minutes
M86\Ricky.Chapman	0 days 00 hours 31 minutes
M86\Sally.Naur	0 days 00 hours 31 minutes

Total Records: 20

Total Time for this Date Scope: 0 days 10 hours 31 minutes

3/4/11 2:20 PM Generated by: superman Page 1 of 1

Fig. 4:4-10 Sample Time Usage Report for Top 20 Users

Time Usage algorithm

For each end user included in the report, the number of seconds from the log is dropped, and each unique minute within a given hour counts as one minute.

In the following example, the end user shows a total of seven minutes of Time Usage:

```
12:00:01    www.m86security.com
12:00:10    www.abc.com
12:01:00    www.m86security.com
12:02:04    www.whitepages.com
12:05:58    www.yellowpages.com
12:05:58    www.yellowpages.com/714.jsp
12:05:59    www.yellowpages.com/phone_number.gif
12:07:03    www.google.com
12:07:33    www.yahoo.com
12:08:23    www.news.com
12:08:30    www.usatoday.com
12:08:59    www.usatoday.com/usa.gif
12:09:00    www.usatoday.com/ca.gif
12:09:01    www.yahoo.com
12:09:02    http://200.100.10.65:88
12:09:03    www.abc.com
12:09:04    www.nbc.com
```

The total for this end user is based on a nine-minute time span that includes 17 entries in the log, and seven unique minute entries: 00, 01, 02, 05, 07, 08, and 09.

REAL TIME REPORTS SECTION

Introduction

This section of the user guide provides instructions to administrators on how to utilize data from Web Filter logs for monitoring end user Internet and network activity in real time.

- Chapter 1: Gauge Components - This chapter describes the types of gauges, the components of a gauge, how to read a gauge, and how to perform shortcuts using gauges.
- Chapter 2: Custom Gauge Setup, Usage - This chapter explains how gauges are configured and monitored.
- Chapter 3: Alerts, Lockout Management - This chapter explains how alerts are set up and used, and how to manage end user lockouts.
- Chapter 4: Analyze Usage Trends - This chapter explains how trend charts are used for assessing end user Internet/network activity.
- Chapter 5: Identify Users, Categories - This chapter explains how to perform a custom search on Internet/ network usage by a specified user, or for a specified category or category group.

Chapter 1: Gauge Components

Types of Gauges

There are two types of gauges that are used for monitoring user activity on the network: URL gauges and bandwidth gauges.

Either gauge type is referred to as a “gauge group” if it is comprised of a group of library categories or protocol(s)/port numbers.

URL gauges

A URL gauge is comprised of library categories and monitors a targeted user group’s access of URLs in a specified library category.

When clicking **Gauges** in the navigation toolbar, the URL gauges Dashboard panel displays showing overall activity in URL gauges:

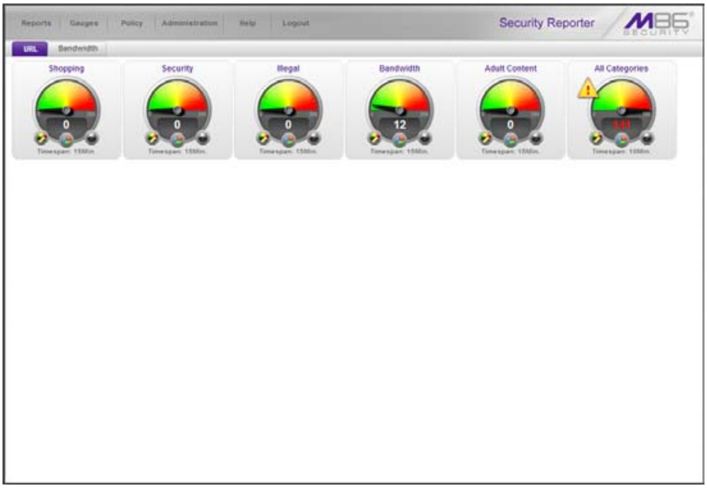


Fig. 5:1-1 URL gauges Dashboard

Bandwidth gauges

A bandwidth gauge is comprised of protocols/port numbers and monitors a targeted user group’s inbound/outbound network traffic generated for specified protocols/port numbers.

With the URL gauges Dashboard displayed, click the Bandwidth tab—located beside the URL tab—to display the Bandwidth gauges Dashboard panel showing overall activity in bandwidth gauges:

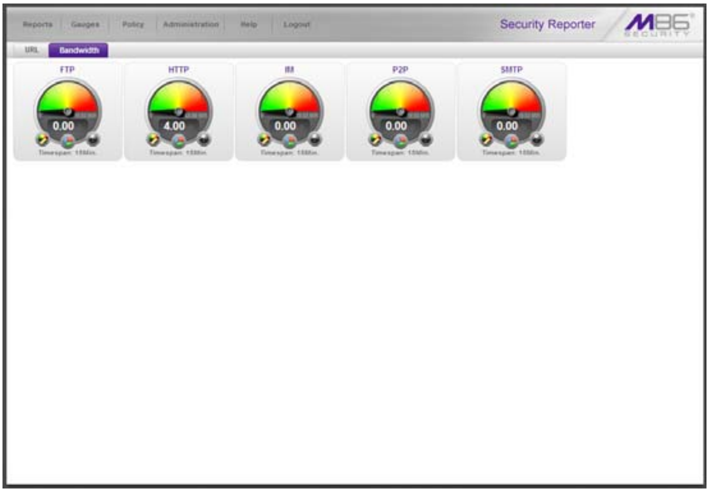


Fig. 5:1-2 Bandwidth gauges Dashboard

Anatomy of a Gauge

Understanding the anatomy of a gauge will help you better configure and maintain gauges to monitor network threats.

The illustration below depicts a URL gauge and a bandwidth gauge and some of their components:

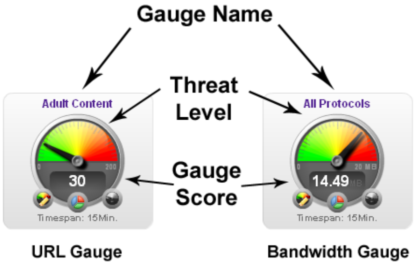


Fig. 5:1-3 URL and bandwidth gauge anatomy

Gauge Name: The name of the gauge displays above the gauge icon.

Timespan: The Timespan for the gauge's activity displays beneath the gauge icon.

Threat Level: The top portion of the gauge is comprised of three colored sections, one in which the gauge's dial is positioned: green (safe) section, yellow (warning) section, or red (network threat) section. This position of the dial represents the current threat level for the gauge.

Gauge Score: The bottom portion of the gauge contains a numerical score, based on the Timespan, activity of end users assigned to the gauge, and type of gauge:

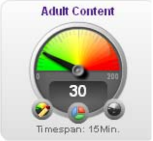
- URL gauge - score includes the total number of end user hits (page count plus blocked object count) for all library categories the gauge monitors.
- Bandwidth gauge - score includes the total number of bytes (kB, MB, GB) of inbound/outbound end user traffic for all protocols/ports the gauge monitors.

How to Read a Gauge

Gauges become active when end users access URLs/ports included in that gauge. Activity is depicted by the position of the dial within one of three sections in the gauge—green, yellow, or red—and by the gauge's score.

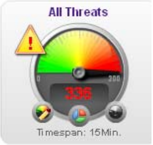
The score will always reflect activity from the most recent past number of specified minutes set up in the Timespan, unless gauge settings were manually changed and saved, at which point the gauge is reset.

If the threat for a gauge is currently low or medium, the score displays in white text.



The image to the right shows a URL gauge with its score displayed in white text and the dial positioned in the green section of the gauge, indicating there is no immediate threat for the library categories in this gauge group.

If the threat level for a gauge is high (exceeding 66 percent of the ceiling established for a gauge), the score displays in red text with a flashing yellow triangle containing a red exclamation point. However, if the score drops below 66 percent within the Timespan set up for the gauge, the text changes from red to solid white again.



The image to the right shows a URL gauge that has exceeded its threshold limit. The source of the threat can be investigated by drilling down into the gauge. It may be that one or more library categories within the gauge currently have a high score, and that one or more end users are responsible for this threat.

For bandwidth gauges, if the total byte score reaches the threshold limit, the score displays in red text and the triangle flashes.

Bandwidth Gauge Components

Incoming/outgoing bandwidth gauges include the following gauges and ports (TCP and/or UDP) to monitor:

- **HTTP** - Hyper Text Transfer Protocol gauge monitors the protocol used for transferring files via the World Wide Web or an intranet.

  This protocol gauge is comprised of gauges for monitoring the following ports by default:

  - **80** - HTTP TCP port used for transferring and listening
  - **443** - HTTPS TCP/UDP port used for encrypted transmission over TLS/SSL
  - **8080** - HTTP Alternate (http-alt) TCP port used under the following conditions: when running a second Web server on the same machine (the other is using port 80), as a Web proxy and caching server, or when running a Web server as a non-root user. This port is used for Tomcat.
- **FTP** - File Transfer Protocol gauge monitors the protocol used for transferring files from one computer to another on the Internet or an intranet.

  This protocol gauge is comprised of gauges for monitoring the following ports by default:

  - **20** - FTP TCP/UDP data port for file transfer
  - **21** - FTP TCP/UDP control (command) port for file transfer
- **SMTP** - Simple Mail Transfer Protocol gauge monitors the protocol used for transferring email messages from one server to another.

  This protocol gauge is comprised of gauges for monitoring the following ports by default:

  - **25** - SMTP TCP/UDP port used for email routing between mail server email messages
  - **110** - POP3 (Post Office Protocol version 3) TCP port used for sending/retrieving email messages
- **P2P** - Peer-to-Peer gauge monitors the protocol used for communication between computing devices—desktops, servers, and other smart devices—that are linked directly to each other.

  This protocol gauge is comprised of gauges for monitoring the following ports by default:

  - **1214** - TCP/UDP port for Kazaa, Morpheous, Grokster, etc.
  - **4662** - TCP/UDP port for eMule, eDonkey, etc.
  - **4665** - TCP/UDP port for eDonkey 2000
  - **6346** - TCP/UDP port for Gnutella file sharing (FrostWire, LimeWire, BearShare, etc.)
  - **6347** - TCP/UDP port for Gnutella
  - **6699** - UDP port for Napster
  - **6881** - TCP/UDP port for BitTorrent
- **IM** - Instant Messaging gauge monitors the protocol used for direct connections between workstations either locally or across the Internet.

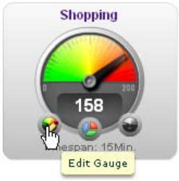
  This protocol gauge is comprised of gauges for monitoring the following ports by default:

  - **1863** - TCP/UDP port for MSN Messenger
  - **5050** - TCP/UDP port for Yahoo! Messenger
  - **5190** - TCP/UDP port for ICQ and AOL Instant Messenger (AIM)
  - **5222** - TCP/UDP port for Google Talk, XMPP/Jabber client connection

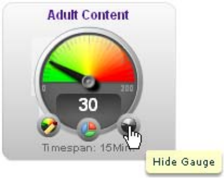
Gauge Usage Shortcuts

The following shortcut actions can be performed in the gauges dashboard:

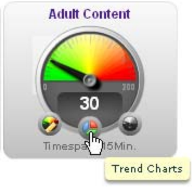
- **View Gauge Ranking** - Clicking a gauge or right-clicking a gauge and selecting this topic from the menu displays the Gauge Ranking panel. The table in this panel contains a list of library categories/protocols/ports that comprise the gauge, along with the list of current users driving the gauge's score. (See View End User Gauge Activity in Chapter 2.)



•**Edit Gauge** - Clicking the left icon at the bottom of a gauge—or right-clicking a gauge and then selecting this menu topic—displays the panel that lets you edit the gauge's components. This is a shortcut to use instead of going to the Add/Edit Gauges panel, selecting the gauge, and then clicking Edit Gauge. (See Modify a Gauge in Chapter 2.)



•**Hide Gauge** - Clicking the right icon at the bottom of a gauge—or right-clicking a gauge and then selecting this menu topic—lets you remove the gauge from the dashboard. This is a shortcut to use instead of going to Dashboard Settings, selecting the gauge from the list, and then clicking the Hide Gauge icon. (See Hide, Disable, Delete, Rearrange Gauges in Chapter 2.)



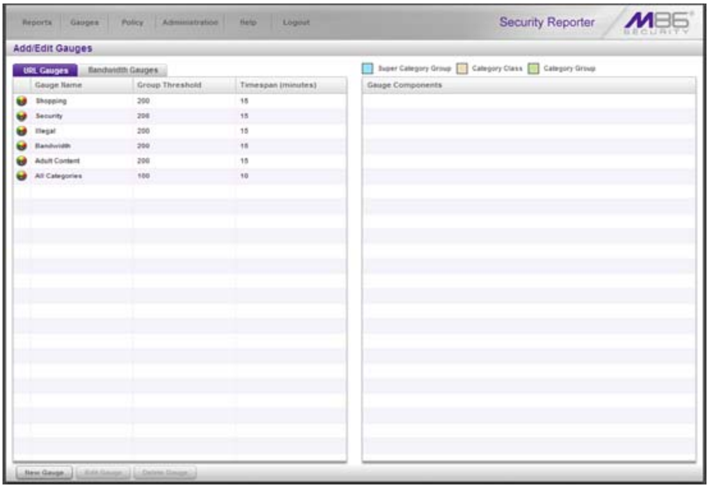
•**Trend Charts** - Clicking the middle icon at the bottom of a gauge—or right-clicking a gauge and then selecting this menu topic—displays a Trend Chart for this particular gauge that lets you analyze the gauge's activity. (See View Trend Charts in Chapter 4.)

- **Disable Gauge** - Right-clicking a gauge and then selecting this menu topic lets you disable a gauge. This is a shortcut to use instead of going to Dashboard Settings, selecting the gauge from the list, and then clicking the Disable Gauge icon. (See Hide, Disable, Delete, Rearrange Gauges in Chapter 2.)
- **Delete Gauge** - Right-clicking a gauge and then selecting this menu topic lets you delete a gauge. This is a shortcut to use instead of going to Dashboard Settings, selecting the gauge from the list, and then clicking the Delete Gauge icon. (See Hide, Disable, Delete, Rearrange Gauges in Chapter 2.)

Chapter 2: Custom Gauge Setup, Usage

Once an account for the group administrator is set up, he/ she can begin setting up gauges for monitoring end users' Internet activity.

1. In the navigation toolbar, mouse over the the Gauges menu link and select **Add/Edit Gauges** to open the Add/ Edit Gauges panel:



Gauge Name	Group Threshold	Timespan (minutes)
Shopping	200	15
Security	200	15
Illegal	200	15
Bandwidth	200	15
Adult Content	200	15
All Categories	100	10

Fig. 5:2-1 Add/Edit Gauges panel

By default, a frame containing the URL Gauges and Bandwidth Gauges tabs displays to the left, and the empty, target Gauge Components frame displays to the right.

2. Do the following to view the contents in the tab to be used:

   - Click **URL Gauges** if this tab currently does not display. By default, this tab includes the following list of Gauge Names: Shopping, Security, Illegal, Bandwidth, Adult Content.

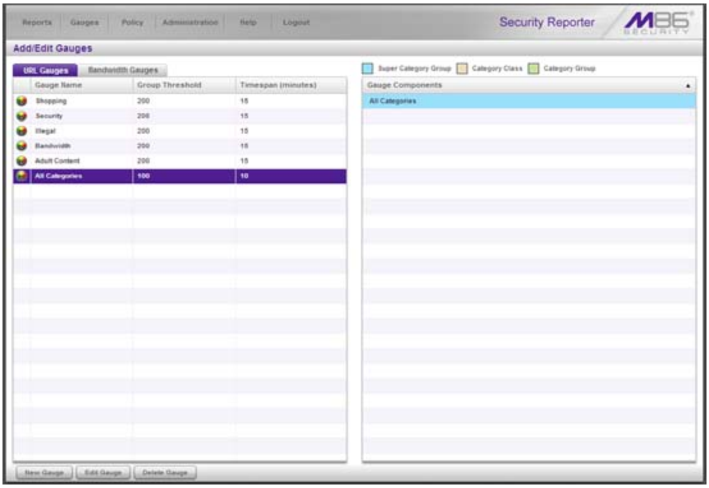
For each Gauge Name in this list, the following information displays: Group Threshold (*200*), Timespan (minutes)—*15* by default.

- Click **Bandwidth Gauges** to view the contents of this tab. By default, this tab includes the following list of Gauge Names: FTP, HTTP, IM, P2P, SMTP.

  For each Gauge Name in this list, the following information displays: Group Threshold (*20 MB*), Timespan (minutes)—*15* by default.

***NOTE**: Up to five bandwidth gauges can be used at a time. If a different bandwidth gauge is needed, one of the default bandwidth gauges must be deleted before a new bandwidth gauge can be added.*

3. Select a Gauge Name to display a list of its library categories/protocols/ports in the Gauge Components frame:



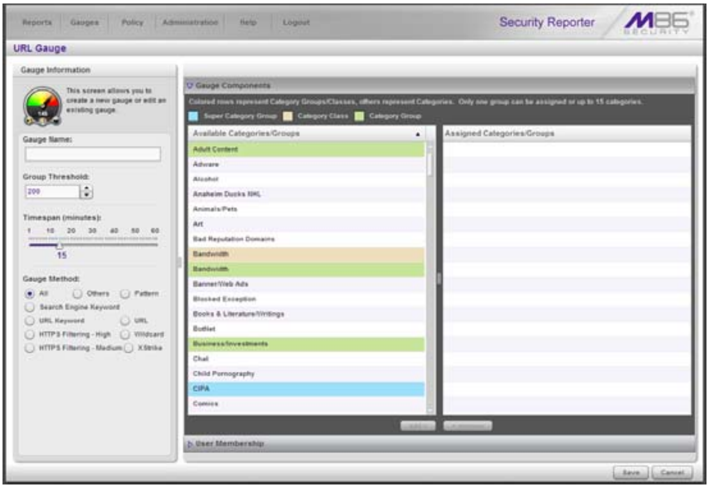
Gauge Name	Group Threshold	Timespan (minutes)
Shopping	200	15
Security	200	15
Illegal	200	15
Bandwidth	200	15
Adult Content	200	15
All Categories	100	10

Gauge Components
All Categories

Fig. 5:2-2 Gauge Components frame populated

Add a Gauge

In the Add/Edit Gauge panel, click **New Gauge** to display URL Gauge panel:



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

Gauge Name:

Group Threshold: 200

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

Gauge Method:
● All ○ Others ○ Pattern
○ Search Engine Keyword
○ URL Keyword ○ URL
○ HTTPS Filtering - High ○ Wildcard
○ HTTPS Filtering - Medium ○ X Strike

Colored rows represent Category Groups/Classes, others represent Categories. Only one group can be assigned or up to 15 categories.

🟦 Super Category Group 🟨 Category Class 🟩 Category Group

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

Fig. 5:2-3 *Add a new gauge*

This panel includes the Gauge Information frame to the left and accordions for Gauge Components and User Membership to the right.

When adding a new gauge, do the following:

- Name the gauge, and specify group threshold limits, timespan values, and the method(s) to be used by the gauge (see Specify Gauge Information).
- Select the library categories/protocols/ports for the gauge to monitor (see Define Gauge Components).
- Assign user groups whose end users' Internet/network activity will be monitored by the gauge (see Assign User Groups).

Specify Gauge Information

In the Gauge Information frame:

1. Type in at least two characters for the **Gauge Name** using upper and/or lowercase alphanumeric characters, and spaces, if desired.
2. Specify the **Group Threshold** ceiling of gauge activity. The default and recommended value is ***200*** for a URL gauge and ***20 MB*** for a bandwidth gauge. This ceiling can be adjusted after using SR for awhile and evaluating activity levels at your organization.

   To modify information in this field, type a specific value in the pre-populated field, and/or use the up/down arrow buttons to increment/decrement the current byte value by one. Make a selection from the pull-down menu if you need to change the byte unit (kB, MB, GB).
3. Use the slider tool to specify the **Timespan (minutes)** for tracking gauge activity (1 - 60 minutes). The default and recommended value is ***15*** minutes. The timespan will always keep pace with the current time period, so that if a timespan of 15 minutes is specified, the gauge will always reflect the most recent end user activity from the past 15 minutes.
4. If necessary, specify a different **Gauge Method** to be used for tracking gauge activity:
   - For a URL gauge - **All** (default), **Others** (all gauge methods, not including Keywords or URLs), **Pattern**, **Search Engine Keyword**, **URL Keyword**, **URL**, **HTTPS Filtering - High**, **HTTPS Filtering - Medium**, **Wildcard**, **XStrike**.
   - For a bandwidth gauge - **Inbound, Outbound**, **Both** (default).

***NOTE**: If the selected gauge method is "Search Engine Keyword" or "URL Keyword", Filter Options for end user profiles on the source Web Filter used with this SR must have "Search Engine Keyword Filter Control" or "URL Keyword Filter Control" enabled.*

Define Gauge Components

Next, specify which library categories/protocols/ports the gauge will use for monitoring end user activity.

***NOTE**: At least one library category/protocol/port must be selected when creating a gauge. The maximum number of library categories/ports that can be selected/added is 15.*

1. From the Available Categories/Groups list in the Gauge Components accordion, select an available Category Group/Class or library categories/ports the end user should not access.

   For bandwidth gauges, to modify criteria in the **Port Number** field, type a specific value in the pre-populated field, and/or use the up/down arrow buttons to increment/ decrement the current value by one.

***NOTES**: For the global administrator, Available Categories/ Groups include All Categories and CIPA selections for URL gauges, and All Protocols and Common Protocols selections for bandwidth gauges, if these selections are not currently in use by another gauge. Common Protocols include: FTP, HTTP, IM, P2P, and SMTP.*

Even though a group administrator does not have the Common Protocols bandwidth selection available when creating a gauge, this Super Category Group is available to him/her via the User Summary Panel. Thus, he/she will have the ability to lock out all users (assigned to him/her) who are currently using FTP, HTTP, IM, P2P and SMTP protocols. (See Monitor, Restrict End User Activity.)

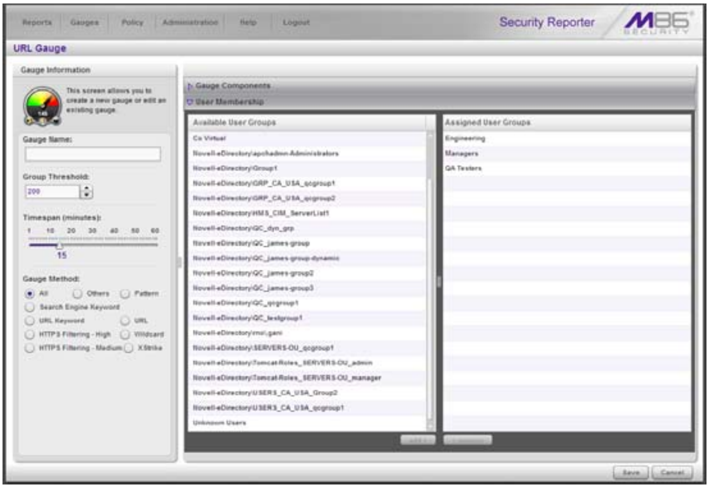
2. Click **add >** (for URL gauges) or **add port >** (for bandwidth gauges) to move the selection(s) to the Assigned Categories/Groups list box.

***TIP**: To remove one or more library categories from the Assigned Categories/Groups list box, make your selection(s), and then click <remove to move the selection(s) back to the Available Categories/Groups list.*

Assign user groups

To assign user groups to be monitored by the gauge:

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



Gauge Name:

Group Threshold: 200

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

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

Available User Groups	Assigned User Groups
Ca Virtual	Engineering
Novell-eDirectory/apchadmin Administrators	Managers
Novell-eDirectory/Group1	QA Testers
Novell-eDirectory/GRP_CA_USA_qcgroup1	
Novell-eDirectory/GRP_CA_USA_qcgroup2	
Novell-eDirectory/HMS_CIM_ServerList1	
Novell-eDirectory/QC_dyn_grp	
Novell-eDirectory/QC_james-group	
Novell-eDirectory/QC_james-group-dynamic	
Novell-eDirectory/QC_james-group2	
Novell-eDirectory/QC_james-group3	
Novell-eDirectory/QC_qcgroup1	
Novell-eDirectory/QC_testgroup1	
Novell-eDirectory/rnol.gani	
Novell-eDirectory/SERVERS-OU_qcgroup1	
Novell-eDirectory/Tomcat-Roles_SERVERS-OU_admin	
Novell-eDirectory/Tomcat-Roles_SERVERS-OU_manager	
Novell-eDirectory/USERS_CA_USA_Group2	
Novell-eDirectory/USERS_CA_USA_qcgroup1	
Unknown Users	

Fig. 5:2-4 User Membership accordion opened

***NOTE**: The base group displays in the Assigned list box by default but can be removed. This group consists of all end users whose network activities are set up to be monitored by the designated group administrator.*

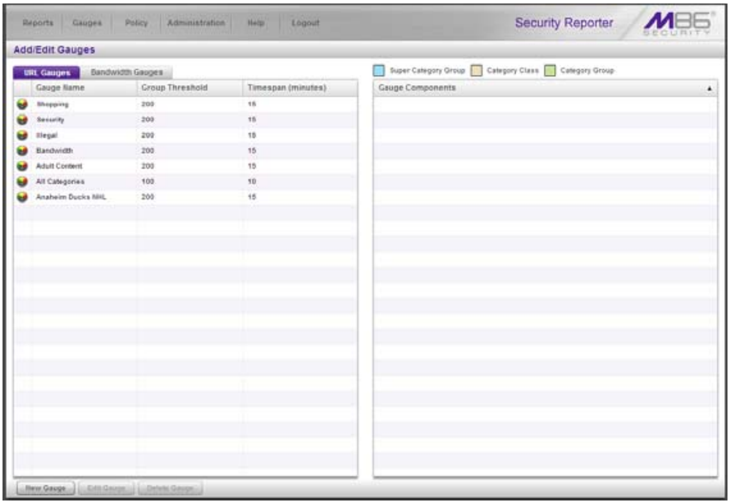
2. From the Available User Groups list, select the user group to highlight it.

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

***TIP**: To remove a user group from the Assigned User Groups list box, click the user group to highlight it, and then click < remove to move the group back to the Available User Groups list.*

Save gauge settings

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



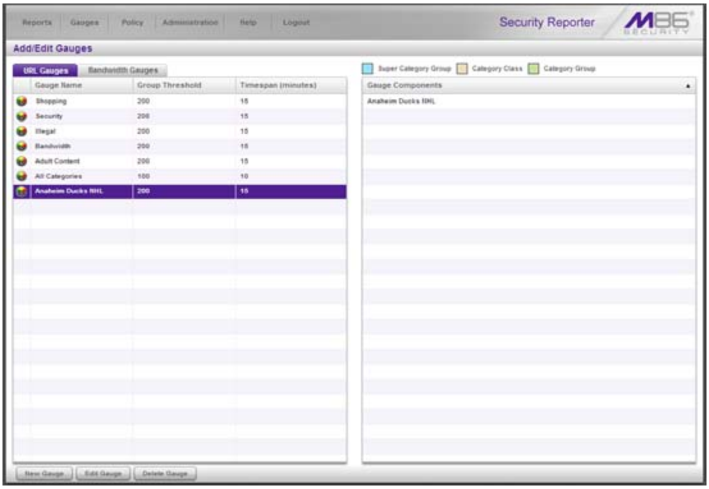
	Gauge Name	Group Threshold	Timespan (minutes)
●	Shopping	200	15
●	Security	200	15
●	Illegal	200	15
●	Bandwidth	200	15
●	Adult Content	200	15
●	All Categories	100	10
●	Anaheim Ducks NHL	200	15

Fig. 5:2-5 New gauge added

Modify a Gauge

Edit gauge settings

1. In the Add/Edit Gauge panel, click the URL Gauges or Bandwidth Gauges tab.
2. Select the gauge from the list to activate all buttons below and populate the Gauge Components frame to the right:

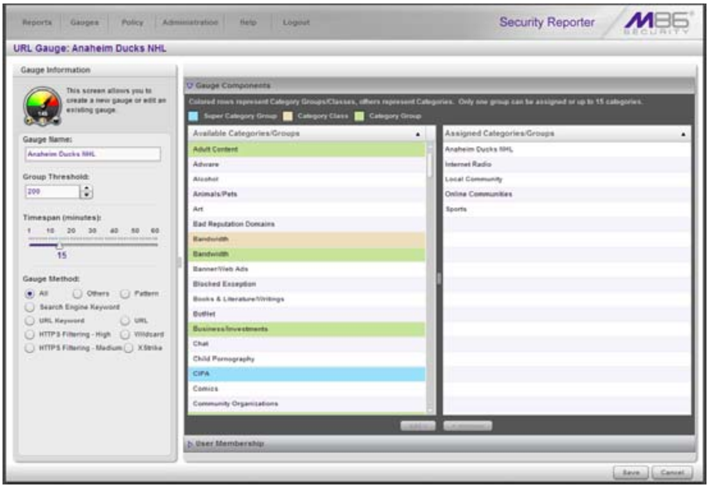


Gauge Name	Group Threshold	Timespan (minutes)
Shopping	200	15
Security	200	15
Illegal	200	15
Bandwidth	200	15
Adult Content	200	15
All Categories	100	10
Anaheim Ducks NHL	200	15

Gauge Components
Anaheim Ducks NHL

Fig. 5:2-6 Select the gauge to be edited

3. Click **Edit Gauge** to display the URL Gauge or Bandwidth Gauge panel showing the Gauge Information frame to the left and the Gauge Components frame to the right, populated with settings previously saved for the gauge:



URL Gauge: Anaheim Ducks NHL

Gauge Information

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

Gauge Name: Anaheim Ducks NHL

Group Threshold: 200

Timespan (minutes): 15

Gauge Method:

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

Gauge Components

Colored rows represent Category Groups/Classes, others represent Categories. Only one group can be assigned or up to 15 categories.

🟦 Super Category Group 🟨 Category Class 🟩 Category Group

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

Assigned Categories/Groups:
Anaheim Ducks NHL
Internet Radio
Local Community
Online Communities
Sports

User Membership

Fig. 5:2-7 Edit gauge settings

TIP*: This panel is also accessible from the gauges dashboard by clicking the Edit Gauge icon at the bottom left of the gauge.*

4. Edit any of the following criteria, as necessary:
   - Gauge Information - Gauge Name, Group Threshold, Timespan in minutes, Gauge Method (see Specify Gauge Information).
   - Gauge Components (see Define Gauge Components).
   - User Membership (see Assign user groups).
5. Click **Save** to save your edits and return to the Add/Edit Gauges panel.

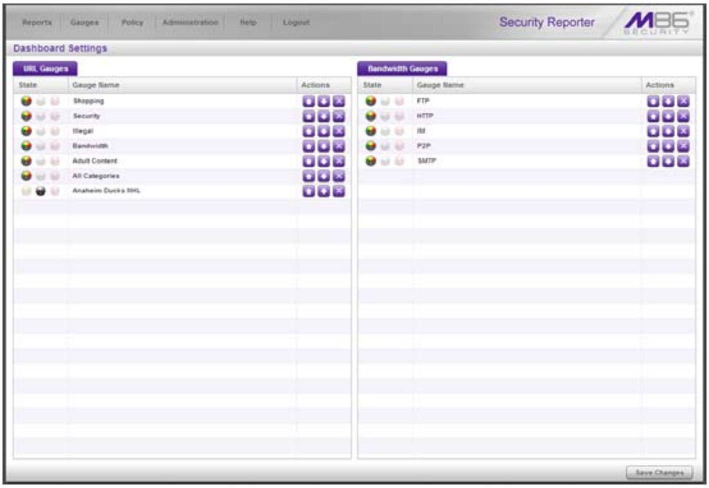
Hide, Disable, Delete, Rearrange Gauges

If you want to view certain gauges in the dashboard, options are available to hide, disable, or delete a specified gauge. You can also manipulate the order in which gauges display in the dashboard.

TIP*: In addition to the instructions provided in this sub-section, gauges can be hidden, disabled, and deleted from the gauges dashboard by right-clicking the gauge to display its menu, and then choosing the appropriate topic. See Gauge Usage Shortcuts in Chapter 1.*

NOTE*: If the global administrator hides or disables a gauge, this will not affect the dashboard view for a group administrator who has been assigned to monitor this gauge.*

1. In the navigation toolbar, mouse over the Gauges menu link and select **Dashboard Settings** to display the Dashboard Settings panel:



Dashboard Settings

URL Gauges

State	Gauge Name	Actions
● ○ ○	Shopping	↑ ↓ ✕
● ○ ○	Security	↑ ↓ ✕
● ○ ○	Illegal	↑ ↓ ✕
● ○ ○	Bandwidth	↑ ↓ ✕
● ○ ○	Adult Content	↑ ↓ ✕
● ○ ○	All Categories	↑ ↓ ✕
○ ● ○	Anaheim Ducks NHL	↑ ↓ ✕

Bandwidth Gauges

State	Gauge Name	Actions
● ○ ○	FTP	↑ ↓ ✕
● ○ ○	HTTP	↑ ↓ ✕
● ○ ○	IM	↑ ↓ ✕
● ○ ○	P2P	↑ ↓ ✕
● ○ ○	SMTP	↑ ↓ ✕

Fig. 5:2-8 Dashboard Settings panel

This panel shows the URL Gauges tab to the left and the Bandwidth Gauges tab to the right. In each of these tabs, a list of gauges displays with the following information:

- State - A gauge icon displays in one of three columns to indicate the current status of the gauge, with the other two columns greyed-out:

  (visible) - This icon in the first column indicates the gauge displays in the dashboard.

  (hidden) - This icon in the second column indicates the gauge does not display in the dashboard.

  (disabled) - This icon in the third column indicates the gauge does not display in the dashboard. This gauge most likely has not been deleted because it will be used on a later occasion.

***NOTE**: Statistics for gauges that are hidden or disabled will not be included in trend reports.*

- Gauge Name - The name given to the gauge.
- Actions - Icons display for performing any one of the following actions on the gauge as necessary: Move the gauge up or down in the current list in order to change the position in which that gauge displays the dashboard, or delete the gauge.

2. After making all necessary Dashboard Settings modifications—hide, disable, show, rearrange, or delete a gauge—defined in the following sub-sections, click **Save Changes** to save your edits.

Hide a gauge

To hide a gauge from displaying in the dashboard:

1. Select the gauge in the URL Gauges or Bandwidth Gauges tab.
2. In the State column, click the icon in the second column (Hide Gauge) to change the gauge’s status to “hidden.”

Disable a gauge

To disable a gauge:

1. Select the gauge in the URL Gauges or Bandwidth Gauges tab.
2. In the State column, click the icon in the third column (Disable Gauge) to change the gauge’s status to “disabled.”

Show a gauge

To re-display a gauge in the dashboard again:

1. Select the gauge in the URL Gauges or Bandwidth Gauges tab.
2. In the State column, click the icon in the first column (show Gauge) to change the gauge’s status to “show.”

Rearrange the gauge display in the dashboard

To rearrange the order in which gauges display in the dashboard:

1. Select the gauge in the URL Gauges or Bandwidth Gauges tab.
2. In the Actions column, perform any of the following actions:

- Click the “up” arrow icon in the first column to move the Gauge Name up one row in this tab, and one position forward in the dashboard.
- Click the “down” arrow icon in the second column to move the Gauge Name down one row in this tab, and one position backward in the dashboard.

***TIP**: These actions can be performed multiple times in order to move the gauge to the desired position in the dashboard.*

Delete a gauge

To delete a gauge:

1. Select the gauge in the URL Gauges or Bandwidth Gauges tab.
2. In the Actions column, click the “X” icon in the far right column to open the Confirm dialogue box with the message: “Deleting this gauge will remove all alerts that are associated with this gauge. Are you sure you want to delete this gauge?”

***NOTE**: Deleting a gauge also deletes any associated alerts set up for that gauge.*

***TIP**: Clicking Cancel closes the dialog box without removing the gauge.*

3. Click **Yes** to close the dialog box and to remove both the Gauge Name from the tab and the gauge from the dashboard.

View End User Gauge Activity

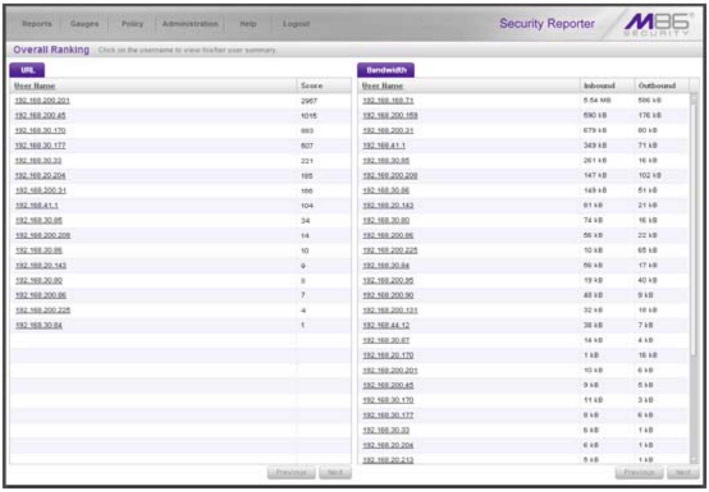
There are two types of gauge activity you will want to view and monitor:

- Overall Ranking - Use this option for a snapshot of end user activity for all gauges, ranked in order by the highest to lowest end user score.
- Gauge Ranking - Use this option for a snapshot of a specific gauge's end user activity, ranked in order by the highest to lowest end user score.

Either option lets you drill down and view information on a specific end user's activity, and lets you lock out the end user, if necessary.

View Overall Ranking

1. In the navigation toolbar, mouse over the Gauges menu link and select **Overall Ranking** to open the Overall Ranking panel:



Overall Ranking Click on the username to view his/her user summary.

User Name	Score
192.168.200.201	2967
192.168.200.45	1015
192.168.20.170	883
192.168.30.177	607
192.168.30.33	221
192.168.20.204	185
192.168.200.31	166
192.168.41.1	104
192.168.30.85	34
192.168.200.208	14
192.168.30.86	10
192.168.20.143	9
192.168.30.80	8
192.168.200.86	7
192.168.200.225	4
192.168.30.84	1

User Name	Inbound	Outbound
192.168.168.71	5.54 MB	586 kB
192.168.200.169	690 kB	176 kB
192.168.200.31	679 kB	80 kB
192.168.41.1	349 kB	71 kB
192.168.30.85	261 kB	16 kB
192.168.200.208	147 kB	102 kB
192.168.30.86	149 kB	51 kB
192.168.20.143	81 kB	21 kB
192.168.30.80	74 kB	16 kB
192.168.200.86	56 kB	22 kB
192.168.200.225	10 kB	65 kB
192.168.30.84	86 kB	17 kB
192.168.200.95	19 kB	40 kB
192.168.200.90	48 kB	9 kB
192.168.200.131	32 kB	18 kB
192.168.44.12	38 kB	7 kB
192.168.30.87	14 kB	4 kB
192.168.20.170	1 kB	16 kB
192.168.200.201	10 kB	6 kB
192.168.200.45	9 kB	5 kB
192.168.30.170	11 kB	3 kB
192.168.30.177	9 kB	6 kB
192.168.30.33	6 kB	1 kB
192.168.20.204	6 kB	1 kB
192.168.20.213	5 kB	1 kB

Fig. 5:2-9 Overall Ranking panel

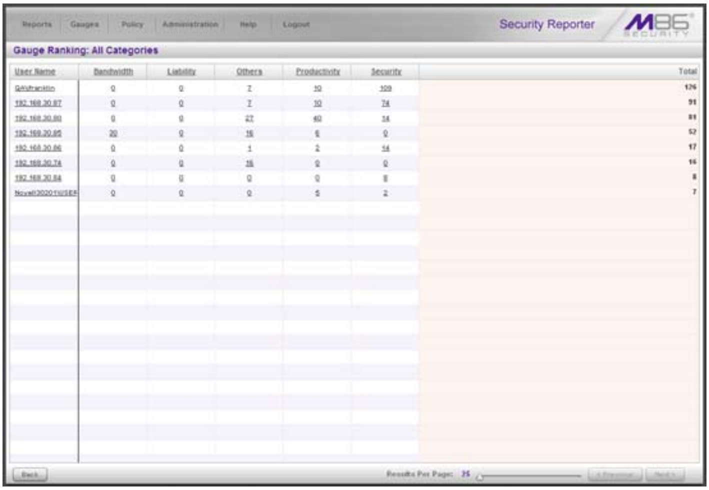
The URL frame displays to the left and the Bandwidth frame displays to the right, containing the User Name (or IP address) and Score for each user currently affecting one or more gauges.

In the URL tab, this Score includes the number of hits the user made in library categories. In the Bandwidth tab, this score includes the end user's byte total for Inbound/Outbound protocols/ports.

2. To drill down and view additional information about an end user's activity, click the **User Name** in the appropriate tab to access the User Summary panel (see Monitor, Restrict End User Activity).
3. In the User Summary panel, you can view URLs visited by the end user and lock out that user from accessing designated areas of the Internet/network.

View a Gauge Ranking table

1. In the gauges dashboard, click a gauge to open the Gauge Ranking panel:



Gauge Ranking: All Categories

User Name	Bandwidth	Liability	Others	Productivity	Security	Total
GAVfranklin	0	0	7	10	109	126
192.168.20.87	0	0	7	10	74	91
192.168.20.80	0	0	27	40	14	81
192.168.20.85	30	0	16	6	0	52
192.168.20.86	0	0	1	2	14	17
192.168.20.74	0	0	16	0	0	16
192.168.20.84	0	0	0	0	8	8
Novell\20201\USE	0	0	0	5	2	7

Fig. 5:2-10 Gauge Ranking table

***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.*

This panel includes rows of records for each end user who is affecting the gauge. For each record in the list, the following information displays: User Name (or IP address), gauge name and end user score, and the end user’s Total score for all gauges he/she affected. End users are ranked in descending order by their Total score.

2. Perform one of two drill-down actions from here:

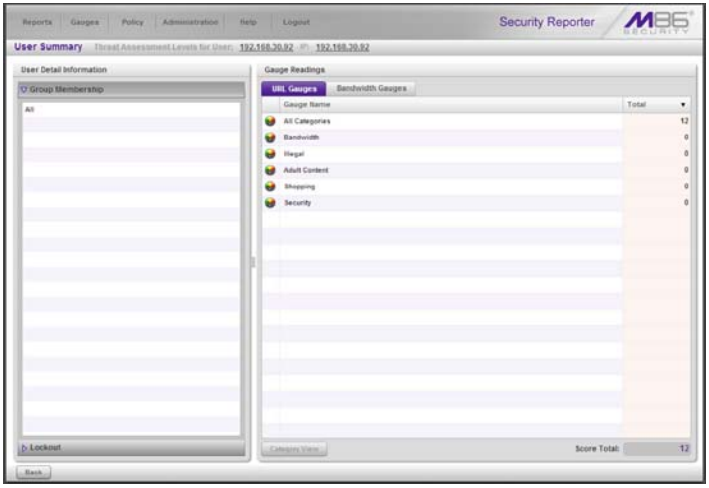
   - Access the User Summary panel by clicking the **User Name** (see Monitor, Restrict End User Activity: View User Summary data). In the User Summary panel, you can view URLs visited by the end user and lock out that user from accessing designated areas of the Internet/network.
   - Access the Category View User panel by clicking a user’s score for a gauge (see Monitor, Restrict End User Activity: Access the Category View User panel). In the Category View User panel, you view current details for the gauge.

Monitor, Restrict End User Activity

View User Summary data

The User Summary panel contains the following frames:

- User Detail Information frame to the left that includes the Group Membership and Lockout accordions. The Group Membership accordion is expanded by default and displays a list of groups in which the end user belongs.
- Gauge Readings frame to the right that includes the URL Gauges and Bandwidth Gauges tabs, each showing the Gauge Name and end user's Total score for each gauge in the dashboard.



User Summary Threat Assessment Levels for User: 192.168.20.92 IP: 192.168.20.92

User Detail Information

▽ Group Membership

All

▷ Lockout

Gauge Readings

URL Gauges | Bandwidth Gauges

Gauge Name	Total ▼
All Categories	12
Bandwidth	0
Illegal	0
Adult Content	0
Shopping	0
Security	0

Score Total: 12

Fig. 5:2-11 User Summary panel

In this panel you can perform the following actions:

- Access the Category View User panel to see which of the gauge's library categories/ports the end user accessed and the score (see Access the Category View User panel).

- Access the Lockout option to lock out the end user from specified Internet/network privileges (see Manually lock out an end user).

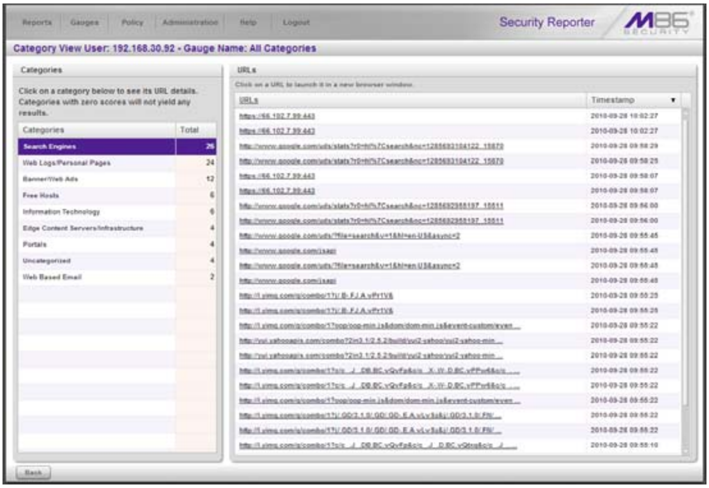
Access the Category View User panel

1. In the User Summary panel, make sure the appropriate tab (URL Gauges or Bandwidth Gauges) is selected, then click a Gauge Name with a score to activate the Category View button.
2. Click **Category View** to display the Category View User panel which includes criteria that is based on the type of gauges to be viewed (URL or bandwidth).

URL Gauges tab selection

For URL gauges, the Category View User panel displays the Categories frame to the left, showing a list of current library categories that were accesssed and the Total score of each category for that end user. The target URLs frame displays to the right.

1. Select a category from the list, which populates the URLs frame with URLs accessed by that end user for that category:



Category View User: 192.168.30.92 - Gauge Name: All Categories

Categories

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

Categories	Total
Search Engines	26
Web Logs/Personal Pages	24
Banner/Web Ads	12
Free Hosts	6
Information Technology	6
Edge Content Servers/Infrastructure	4
Portals	4
Uncategorized	4
Web Based Email	2

URLs

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

URLs	Timestamp ▼
https://66.102.7.99:443	2010-09-28 10:02:27
https://66.102.7.99:443	2010-09-28 10:02:27
http://www.google.com/uds/stats?r0=hl%7Csearch&nc=1285693104122_15670	2010-09-28 09:58:29
http://www.google.com/uds/stats?r0=hl%7Csearch&nc=1285693104122_15670	2010-09-28 09:58:25
https://66.102.7.99:443	2010-09-28 09:58:07
https://66.102.7.99:443	2010-09-28 09:58:07
http://www.google.com/uds/stats?r0=hl%7Csearch&nc=1285692968197_15611	2010-09-28 09:56:00
http://www.google.com/uds/stats?r0=hl%7Csearch&nc=1285692968197_15611	2010-09-28 09:56:00
http://www.google.com/uds/?file=search&v=1&hl=en-US&async=2	2010-09-28 09:55:45
http://www.google.com/jsapi	2010-09-28 09:55:48
http://www.google.com/uds/?file=search&v=1&hl=en-US&async=2	2010-09-28 09:55:45
http://www.google.com/jsapi	2010-09-28 09:55:48
http://l.yimg.com/g/combo/1?j/_B-FJ.A.vPr1V6	2010-09-28 09:55:25
http://l.yimg.com/g/combo/1?j/_B-FJ.A.vPr1V6	2010-09-28 09:55:25
http://l.yimg.com/g/combo/1?oop/oop-min.js&dom/dom-min.js&event-custom/even ...	2010-09-28 09:55:22
http://yui.yahooapis.com/combo?2in3.1/2.5.2/build/yui2-yahoo/yui2-yahoo-min ...	2010-09-28 09:55:22
http://yui.yahooapis.com/combo?2in3.1/2.5.2/build/yui2-yahoo/yui2-yahoo-min ...	2010-09-28 09:55:22
http://l.yimg.com/g/combo/1?c/c_J_D8.BC.vQvfa&c/c_X-W-D.BC.vPPw6&c/c_ ...	2010-09-28 09:55:22
http://l.yimg.com/g/combo/1?c/c_J_D8.BC.vQvfa&c/c_X-W-D.BC.vPPw6&c/c_ ...	2010-09-28 09:55:22
http://l.yimg.com/g/combo/1?oop/oop-min.js&dom/dom-min.js&event-custom/even ...	2010-09-28 09:55:22
http://l.yimg.com/g/combo/1?j/_GD/3.1.0/_GD/_GD-_E.A.vLv3a&j/_GD/3.1.0/_FN/ ...	2010-09-28 09:55:22
http://l.yimg.com/g/combo/1?j/_GD/3.1.0/_GD/_GD-_E.A.vLv3a&j/_GD/3.1.0/_FN/ ...	2010-09-28 09:55:22
http://l.yimg.com/g/combo/1?c/c_J_D8.BC.vQvfa&c/c_J_D.BC.vQtna&c/c_J ...	2010-09-28 09:55:10

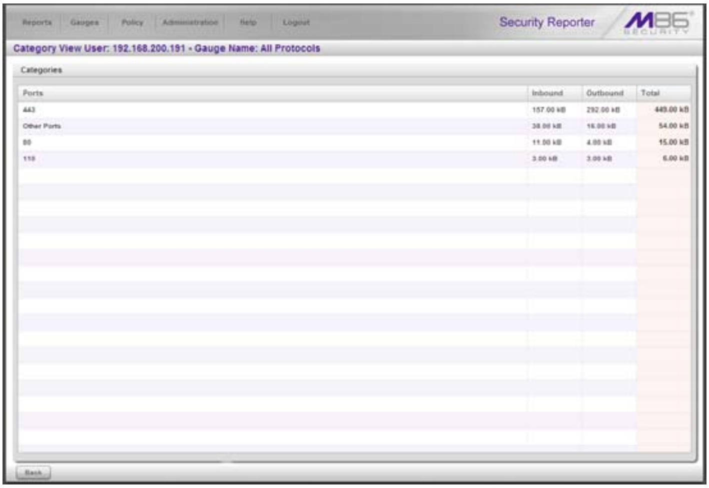
Fig. 5:2-12 Category View User panel for URL Gauges tab selection

For each URL included in the list, the Timestamp displays using military time in the YYYY-MM-DD HH:MM:SS format.

2. Click a URL from the list to open a separate browser window or tab displaying the contents of that URL.

Bandwidth Gauges tab selection

For Bandwidth gauges, the Category View User panel contains the Categories frame showing the Ports column and corresponding Inbound/Outbound bandwidth usage by the end user for that port, and the combined Total inbound and outbound bandwidth usage by the end user for that port:



Category View User: 192.168.200.191 - Gauge Name: All Protocols

Categories

Ports	Inbound	Outbound	Total
443	157.00 kB	292.00 kB	449.00 kB
Other Ports	38.00 kB	16.00 kB	54.00 kB
80	11.00 kB	4.00 kB	15.00 kB
110	3.00 kB	3.00 kB	6.00 kB

Fig. 5:2-13 Category View User panel for Bandwidth tab selection

Manually lock out an end user

1. In the User Summary panel, in the User Detail Information frame, click the Lockout accordion to open it:

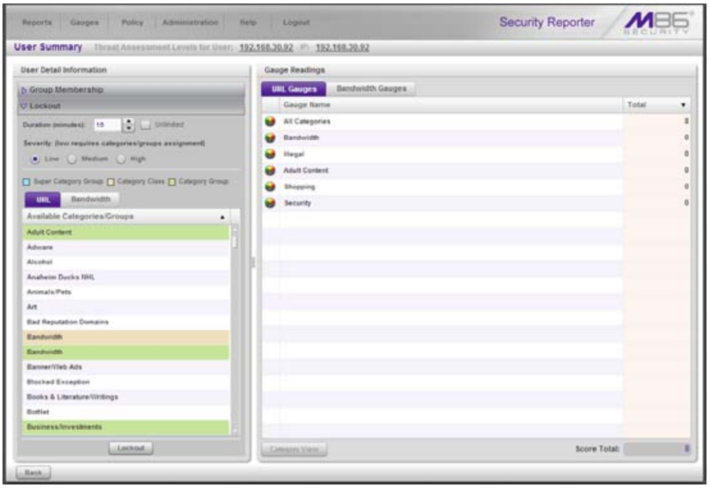


Fig. 5:2-14 User Summary panel, Lockout accordion expanded

2. Specify the **Duration** (minutes) of the lockout (the default is “15” minutes), or click the “Unlimited” checkbox.

***NOTES**: If “Unlimited” is selected, the end user remains locked out of the specified areas on the Internet/network until the administrator unlocks his/her workstation. To “unlock” the end user, go to the Gauges > Lockouts panel. For information on this feature, see Chapter 3: Alerts, Lockout Management.*

3. Specify the **Severity** of the lockout from the radio button choices:

   - **Low** - This selection lets you choose which library categories/ports the end user will not be able to access (see Low severity lockout).
   - **Medium** - This selection locks out the end user from access to the World Wide Web (see Medium and High severity lockout).

- **High** - This selection locks out the end user from all network access via a TCP connection (see Medium and High severity lockout).

4. After performing the additional steps based on the chosen lockout Severity level, click **Lockout** at the bottom of the frame to open the Info alert box with the message: “This user has been locked out.”

5. Click **OK** to close the alert box and to lock out the user from the designated library categories/ports for the specified duration of time.

Low severity lockout

If a “Low” Severity lockout was selected, the Available Categories/Groups box displays. Do the following:

- If using the URL tab, choose the library category/categories from the list. Up to 15 categories or one category group/class can be added.

- If using the Bandwidth tab, make a selection from the protocols in the list.

  You can also enter a port number in the **Port Number** field, or modify the value in that field by clicking the up/down arrows to increment/decrement the current value by one, and then click **add port >** to include the port number in the Assigned Categories/Groups frame. Up to 15 port numbers can be added.

***NOTE**: In the Available Categories/Groups box, a global administrator will not see the “All Categories” selection for URL gauges, nor see the “All Protocols” selection available for bandwidth gauges. In order to lock out end users using either of these selections, a “Medium” severity lockout should be used.*

Medium and High severity lockout

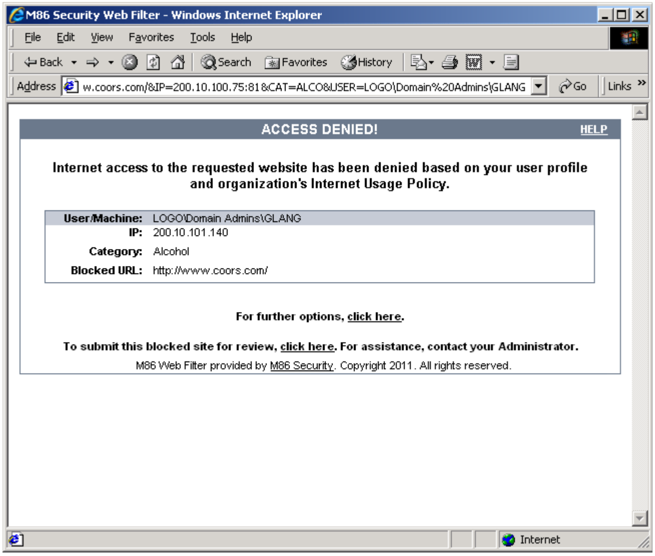
If a “Medium” or “High” Severity lockout was selected, the **Type** field displays. Click either “Medium” or “High” to select that lockout level.

End user workstation lockout

There are two different scenarios that can occur for end users when they are locked out, based on the severity of the lockout (low, medium, or high), and the gauge type (URL or bandwidth).

Low severity URL, medium URL/bandwidth lockout

In a low or medium severity URL lockout, or a medium severity bandwidth type lockout, when an end user attains the User Threshold established for a gauge, and that end user attempts to access a category/port or category group set up to be monitored by that gauge, the following lockout page displays for the end user.


M86 Security Web Filter - Windows Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address
Go
Links
Internet

w.coors.com/&IP=200.10.100.75:81&CAT=ALCO&USER=LOGO\Domain%20Admins\GLANG

ACCESS DENIED! HELP

Internet access to the requested website has been denied based on your user profile and organization's Internet Usage Policy.

User/Machine:	LOGO\Domain Admins\GLANG
IP:	200.10.101.140
Category:	Alcohol
Blocked URL:	http://www.coors.com/

For further options, click here.

To submit this blocked site for review, click here. For assistance, contact your Administrator.

M86 Web Filter provided by M86 Security. Copyright 2011. All rights reserved.

Fig. 5:2-15 Low, medium level URL, medium bandwidth lockout page

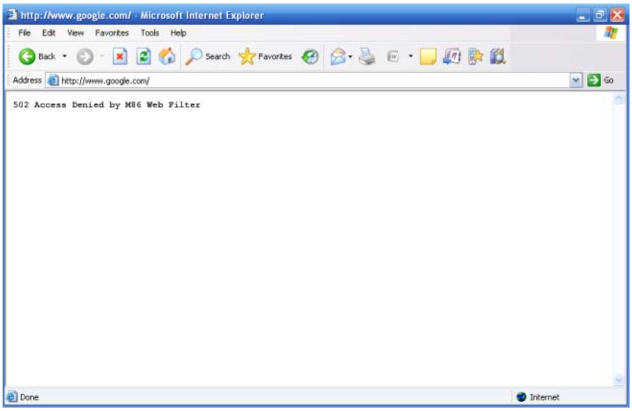
This page contains the following information: header “ACCESS DENIED!”, User/Machine name for an LDAP user (blank for an IP group user), user’s IP address, library Category in which the URL resides, and the Blocked URL the user attempted to access.

By default, the following standard links are included in the block page: HELP; M86 Security; For further options, click here; To submit this blocked site for review, click here.

***NOTE**: Please refer to the Global Administrator Section of the M86 Web Filter User Guide or M86 IR Web Filter User Guide for information about fields in the block page and how to use them.*

High severity URL, low/high bandwidth lockout

In a high severity URL lockout, or a low or high severity bandwidth type lockout, when an end user attains the User Threshold established for a gauge, and that end user attempts to access a URL for a threat category/port or category group set up to be monitored by that gauge, the following lockout page displays for the end user:



```
502 Access Denied by M86 Web Filter
```

Fig. 5:2-16 High level URL, low and high bandwidth lockout page

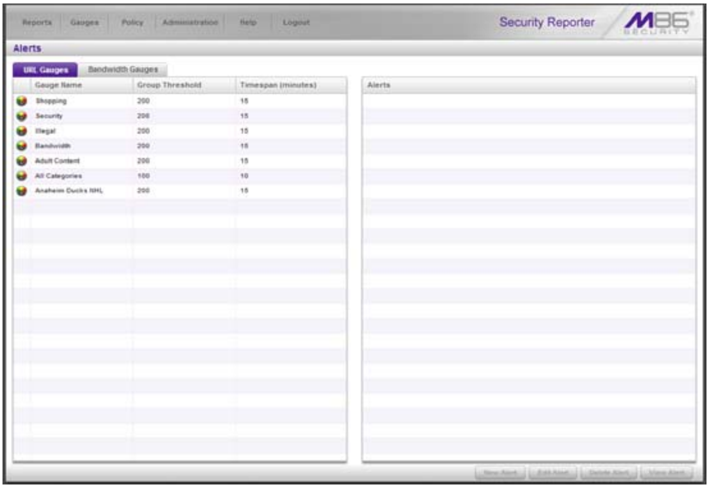
This page contains the following information: “502 Access Denied by M86 Web Filter”.

Chapter 3: Alerts, Lockout Management

After setting up gauges for monitoring end user Internet activity, notifications for Internet abuse should be set up in the form of policy alerts. These messages inform the administrator when an end user has triggered an alert for having reached the threshold limit established for a gauge. If the end user was locked out of Internet/network for an indefinite time period as a result of his/her Internet activity, the administrator can determine when to unlock that end user's workstation.

These functions are available to a group administrator only if permissions were granted by the administrator who set up his/her account.

1. In the navigation toolbar, mouse over the Policy menu link and select **Alerts** to open the Alerts panel:



Gauge Name	Group Threshold	Timespan (minutes)
Shopping	200	15
Security	200	15
Illegal	200	15
Bandwidth	200	15
Adult Content	200	15
All Categories	100	10
Anaheim Ducks NHL	200	15

Fig. 5:3-1 Alerts panel

This panel includes a frame to the left that contains the URL Gauges and Bandwidth Gauges tabs, and the empty, target Alerts frame to the right.

2. Do the following to view the contents in the tab to be used:

   - Click **URL Gauges** if this tab currently does not display. By default, this tab includes the following list of Gauge Names: Shopping, Security, Illegal, Bandwidth, Adult Content.

     For each Gauge Name in this list, the following information displays: Group Threshold (*200*), Timespan (minutes)—*15* by default.

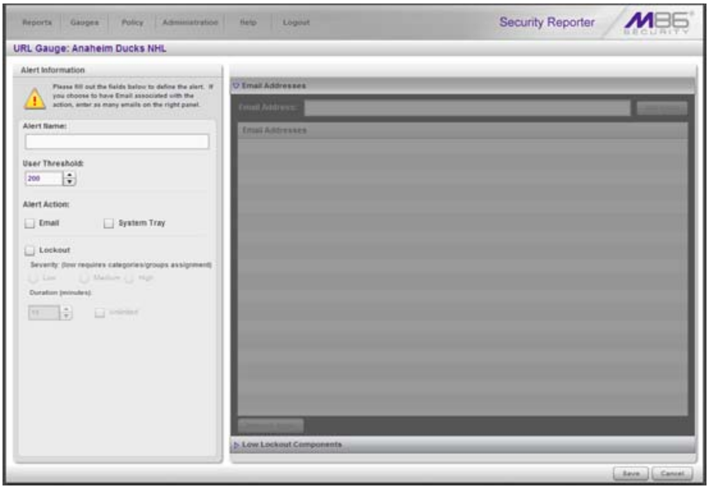
   - Click **Bandwidth Gauges** to view the contents of this tab. By default, this tab includes the following list of Gauge Names: FTP, HTTP, IM, P2P, SMTP.

     For each Gauge Name in this list, the following information displays: Group Threshold (*20 MB—64 MB for “HTTP”*), Timespan (minutes)—*15* by default.

Add an Alert

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

2. Click **New Alert** to open the panel for that gauge:



URL Gauge: Anaheim Ducks NHL

Alert Information

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

Alert Name:

User Threshold: 200

Alert Action:

□ Email □ System Tray

□ Lockout

Severity: (low requires categories/groups assignment)

○ Low ○ Medium ○ High

Duration (minutes):

□ Unlimited

Fig. 5:3-2 Add a new Alert

In this panel, the Alert Information frame displays to the left and the greyed-out target panel displays to the right containing the Email Addresses and Low Lockout Components accordions.

3. In the Alert Information frame, type in the **Alert Name** to be used for the alert that will be delivered to the group administrator.

4. Specify the **User Threshold** ceiling of gauge activity that will trigger the alert.

***NOTE**: An alert is triggered for any end user whose current score for a gauge matches the designated threshold limit. (See How to Read a Gauge in Chapter 1 for information on how scoring is defined.)*

5. In the Alert Action section, specify the mode(s) to use when an alert is triggered:

    - **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.

***NOTE**: The System Tray alert feature is only available for an administrator with an Active Directory LDAP account, user name, and domain, and is not available if using IP groups.*

6. After making all entries in this panel, click **Save** to save your entries and to activate your alert.

Email alert function

Configure email alerts

To set up the email alert function:

1. In the Alert Action section of the Alert Information frame, click the checkbox corresponding to **Email** to open the Email Addresses accordion in the target frame to the right.
2. Type in the **Email Address**.
3. Click **Add Email** to include the address in the Email Addresses list box.

    Follow steps 2 and 3 for each email address to be sent an alert.

TIP: *To remove an email address from the list box, select the email address and then click Remove Email. Click Submit to save your settings.*

Receive email alerts

If an alert is triggered, an email message is sent to the mailbox address(es) specified. This message includes the following information:

- Subject: Alert triggered by user (user name/IP address).
- Body of message: User (user name/IP address) has triggered the (Alert Name) alert with a threshold of ‘X’ (in which “X” represents the alert threshold) on the (gauge name) gauge.

  Beneath this information, the date and time (YYYY-MM-DD HH:MM:SS), and clickable URL display for each URL accessed by the user that triggered this alert.

System Tray alert function

If using LDAP with an Active Directory user name, account, and domain, to set up the feature for System Tray alerts, click the checkbox corresponding to **System Tray** and follow the instructions in Appendix D: System Tray Alerts: Setup, Usage.

NOTE: *In order to use this feature, the LDAP User Name and Domain set up in the administrator’s profile account must be the same ones he/she uses when logging into his/her workstation.*

Lockout function

To set up the lockout function:

1. Click the checkbox corresponding to **Lockout** to activate the Severity and Duration (minutes) fields.
2. Specify the **Severity** of the end users’ lockout:
   - **Low** - Choosing this option opens the Low Lockout Components accordion containing the Available Categories/Groups and Assigned Categories/Groups frames.

     Select the library category/categories or protocol(s) the end user should not access.

     For bandwidth gauges, to specify a port number the user should not access, type a specific value in the **Port Number** field, and/or use the up/down arrow buttons to increment/decrement the current value by one.

     Click **add >** (for URL gauges) or **add port >** (for bandwidth gauges) to move the selection(s) to the Assigned Categories/Groups list box.

***TIP**: To remove one or more library categories/ports from the Assigned Categories/Groups list box, make your selection(s), and then click <remove to move the selection(s) back to the Available Categories/Groups list.*

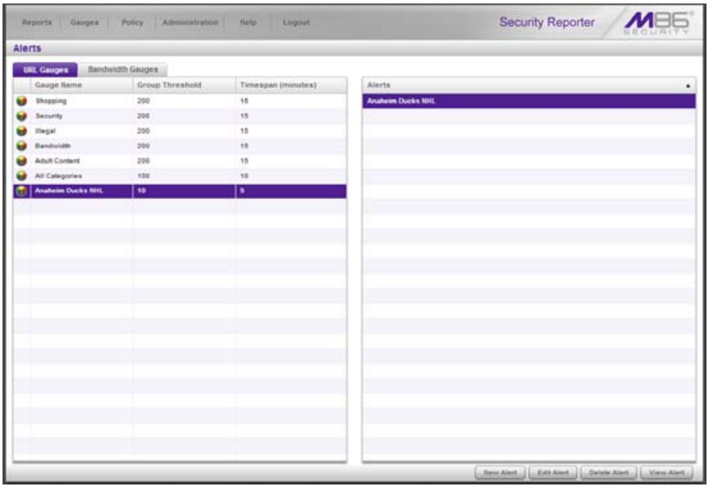
   - **Medium** - Choosing this option will lock out an end user from World Wide Web access if he/she reaches the threshold limit set up for the gauge.
   - **High** - Choosing this option will lock out an end user from network access via a TCP connection if he/she reaches the threshold limit set up for the gauge.
3. Specify the **Duration** (minutes) of the lockout (the default is “15” minutes), or click the “Unlimited” checkbox.

***NOTE**: If "Unlimited" is specified, the end user will remain locked out from Internet/network access until the group administrator unlocks his/her workstation using the Gauges > Lockouts panel.*

***TIP**: After making your selections, click **Save** to save your settings.*

View, Modify, Delete an Alert

1. In the Alerts panel, select the URL Gauges or Bandwidth Gauges tab.
2. Select the gauge for which an alert will be viewed and/or modified. This action populates the Alerts frame list box with any existing alerts created for that gauge.
3. Select the alert to be viewed or modified by clicking on it to highlight it; this action activates all buttons below the Alerts frame (Add Alert, Edit Alert, Delete Alert, View Alert):



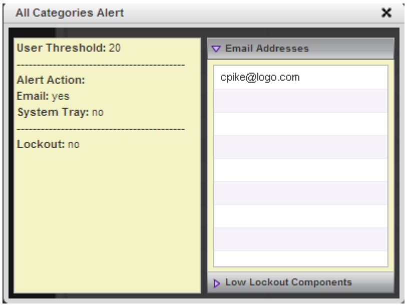
Gauge Name	Group Threshold	Timespan (minutes)
Shopping	200	15
Security	200	15
Illegal	200	15
Bandwidth	200	15
Adult Content	200	15
All Categories	100	10
Anaheim Ducks NHL	10	5

Alerts
Anaheim Ducks NHL

Fig. 5:3-3 Alert added

View alert settings

1. Beneath the Alerts frame, click **View Alert** to open the alert viewer pop-up window:



User Threshold: 20

Alert Action:
Email: yes
System Tray: no

Lockout: no

cpike@logo.com

Fig. 5:3-4 View an alert

The following information displays to the left of this window:

- User Threshold amount
- Alert Action criteria (yes/no): Email, System Tray
- Lockout (yes/no)

If a Lockout was set up for the alert, the following information displays below “Lockout”:

- Severity (Low, Medium, High)
- Duration (minutes)

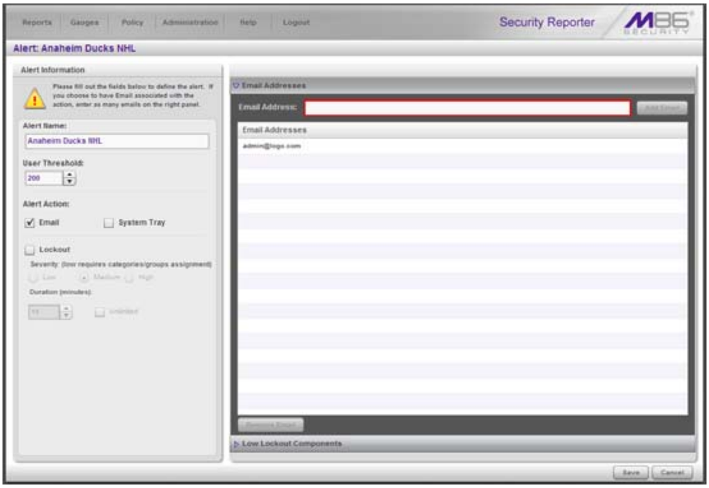
To the right of this window, the Email Addresses and Low Lockout Components accordions display. Click an accordion to expand it, and view the contents—if any—within that accordion.

***NOTE**: The System Tray alert feature is only available if using Active Directory LDAP, and is not available if using IP groups.*

2. Click the “X” in the upper right corner of the alert viewer pop-up window to close it.

Modify an alert

1. In the Alerts panel, click the URL Gauges or Bandwidth Gauges tab.
2. Select the gauge from the list to populate the Alerts frame with alerts for that gauge, and to activate all buttons beneath the frame.
3. Click **Edit Alert** to open the edit Alert panel:



Alert: Anaheim Ducks NHL

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

Alert Name: Anaheim Ducks NHL

User Threshold: 200

Alert Action:

☑ Email □ System Tray

□ Lockout

Severity: (low requires categories/groups assignment)

○ Low ● Medium ○ High

Duration (minutes): 15 □ Unlimited

Email Address:

Email Addresses

admin@logo.com

Fig. 5:3-5 Edit an alert

4. The following items can be edited:
   - Alert Name
   - User Threshold
   - Alert Action selections: Email, System Tray—the latter is only functional for Active Directory LDAP—and Lockout
   - Lockout Severity selection (Low, Medium, High)
   - Duration (minutes) selection
   - Email Addresses
   - Low Lockout Components

5. Click **Save** to save your edits, and to return to the main Alerts panel.

Delete an alert

1. In the Alerts panel, click the URL Gauges or Bandwidth Gauges tab.
2. Select the gauge from the list to populate the Alerts frame with alerts for that gauge, and to activate all buttons beneath the frame.
3. Click **Delete Alert** to open the Confirm dialog box with the message: “Are you sure you want to delete this alert?”

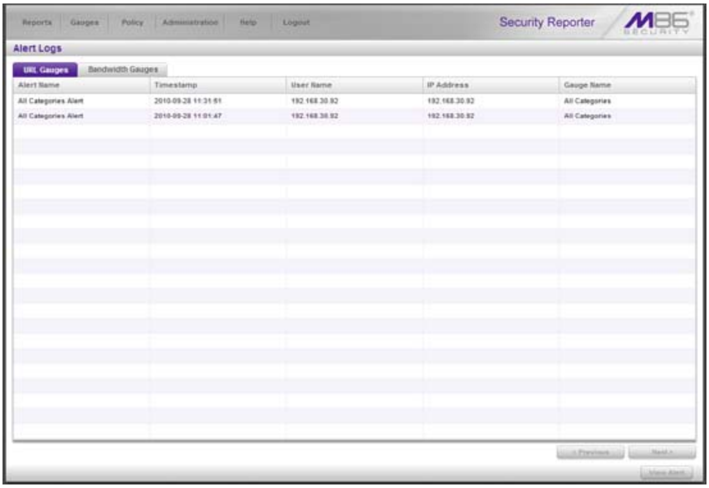
***NOTE**: Clicking No closes the dialog box without removing the alert, and returns you to the main Alerts panel.*

4. Click **Yes** to close the Confirm dialog box and to remove the alert from the list.

View the Alert Log

After alerts are sent to an administrator, a list of alert activity is available for viewing in the Alert Logs panel.

1. In the navigation toolbar, mouse over the Policy menu link and select **Alert Logs** to open the Alert Logs panel.
2. Select the URL Gauges or Bandwidth Gauges tab to display its contents:



Alert Logs

Alert Name	Timestamp	User Name	IP Address	Gauge Name
All Categories Alert	2010-09-28 11:31:51	192.168.30.92	192.168.30.92	All Categories
All Categories Alert	2010-09-28 11:01:47	192.168.30.92	192.168.30.92	All Categories

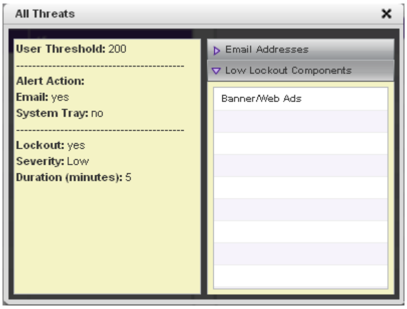
Fig. 5:3-6 Alert Logs panel

The alert log contains a list of alert records for the most recent 24-hour time period. Each record displays in a separate row. For each row in the list, the following information displays: Alert Name, Timestamp (using the YYYY-MM-DD HH:MM:SS military time format), User Name (or IP address), IP Address, Gauge Name.

***NOTE**: If an alert was deleted during the most recent 24-hour time period, any records associated with that alert will be removed from the alert log.*

3. To view details on an alert, select the alert record in the list to highlight it.

4. Click **View Alert** to open the alert viewer pop-up window:



User Threshold: 200

Alert Action:
Email: yes
System Tray: no

Lockout: yes
Severity: Low
Duration (minutes): 5

Fig. 5:3-7 View an alert

The following information displays to the left of this window:

- User Threshold amount
- Alert Action criteria (yes/no): Email, System Tray
- Lockout (yes/no)

If a Lockout was set up for the alert, the following information displays below “Lockout”:

- Severity (Low, Medium, High)
- Duration (minutes)

To the right of this window, the Email Addresses and Low Lockout Components accordions display. Click an accordion to expand it, and view the contents—if any—within that accordion.

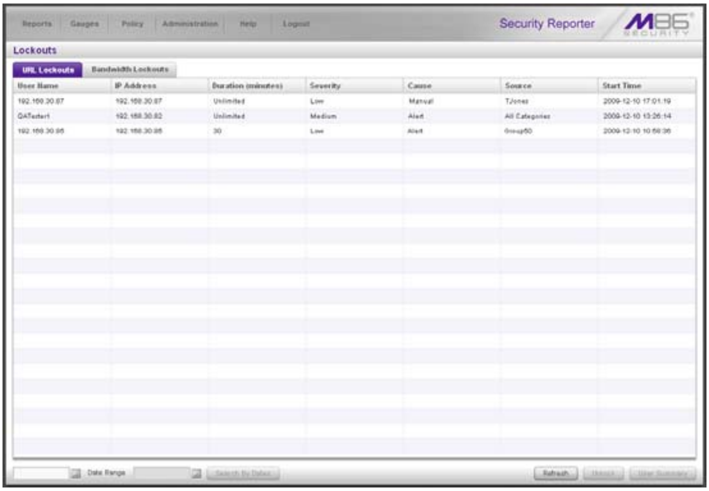
5. Click the “X” in the upper right corner of alert viewer pop-up window to close it.

Manage the Lockout List

An end user who is manually or automatically locked out for an “Unlimited” period of time—from accessing designated content on the Internet or using the network—can only have his/her workstation unlocked by an administrator.

To view the current lockout list:

1. In the navigation toolbar, mouse over the Gauges menu link and select **Lockouts** to open the Lockouts panel.
2. Select the URL Gauges or Bandwidth Gauges tab to display its contents:



User Name	IP Address	Duration (minutes)	Severity	Cause	Source	Start Time
192.168.30.87	192.168.30.87	Unlimited	Low	Manual	TJones	2009-12-10 17:01:19
QATester1	192.168.30.82	Unlimited	Medium	Alert	All Categories	2009-12-10 13:26:14
192.168.30.95	192.168.30.95	30	Low	Alert	Group50	2009-12-10 10:58:36

Fig. 5:3-8 View Lockouts

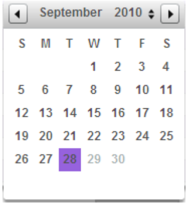
The lockout list contains records for all end users currently locked out of the Internet/network. Each end user’s record displays in a separate row. For each row in the list, the following information displays: User Name (or IP address); IP address; Duration (minutes); Severity of the lockout (Low, Medium, High); Cause of the lockout (Manual, Automatic); Source of the lockout (user name of the administrator who locked out the end user in a

Manual lockout, or name of the alert in an Automatic lockout); Start Time for the alert (using the YYYY-MM-DD HH:MM:SS format).

View a specified time period of lockouts

If the lockout list is populated with many records, using the Date Range feature will only show you records within the range of dates you specify.

1. At the **Date Range** field, click the ▦ calendar icon located to the right of the first date field; this action opens the larger calendar for the current month, with today's date highlighted:



S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

***TIP**: To view the calendar for the previous month, click the left arrow at the top left of the box. To view the calendar for the next month, click the right arrow at the top right of the box.*

2. Click the starting date to select it and to close the calendar pop-up window. This action populates the field with the selected date.

3. At the **Date Range** field, click the ▦ calendar icon located to the right of the second date field; this action opens the larger calendar for the current month, with today's date highlighted.

4. Click the ending date to select it and to close the calendar pop-up window. This action populates the field with the selected date.

5. Click **Search By Dates** to display records for only the selected dates.

TIP*: Click Refresh to clear all records returned by the search query, and to display the default records (all lockout records) in the panel.*

Unlock workstations

1. In the populated Lockouts panel, click each record to highlight it.
2. Click **Unlock** to unlock the end user(s) and to remove the record(s) from the list.

NOTE*: By unlocking an end user's workstation, all records in this list pertaining to that end user are removed from the list.*

Access User Summary details

1. To access details about an end user's online activity, first click the user's record to highlight it.
2. Next, click **User Summary** to display the User Summary panel where you can monitor that end user's online activity and lock him/her out of designated areas of the Internet/network. (See Monitor, Restrict End User Activity for details about using the User Summary panel.)

Chapter 4: Analyze Usage Trends

When analyzing end user Internet usage trends, trend charts help you configure gauges and alerts so you can focus on current traffic areas most affecting the network.

If more information is required in your analysis, the Web Filter application, Report Manager tools, and System Configuration administrator console should be consulted so you can generate customized reports to run for a time period of your specifications.

View Trend Charts

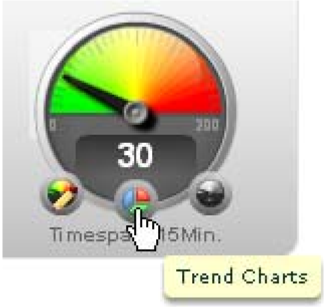
There are three basic types of trend charts that can be generated on demand to show total gauge score averages for a specified, limited time period:

- Pie trend chart for an individual URL or bandwidth gauge
- Pie trend chart for all collective URL or bandwidth gauges
- Line chart showing details for a pie chart

View activity for an individual gauge

To view activity for any individual URL or bandwidth gauge:

1. If the gauges dashboard does not currently display, choose **Dashboard** from the Gauges menu in the navigation toolbar.
2. Be sure the dashboard of your choice (URL or Bandwidth gauges) displays. If not, click the URL or Bandwidth button above the dashboard to display the dashboard of your choice.
3. Find the gauge for which the trend chart will be generated, and then click the Trend Charts icon at the bottom middle of that gauge:



This action of clicking the Trend Charts icon displays the Gauge Trend Chart panel:

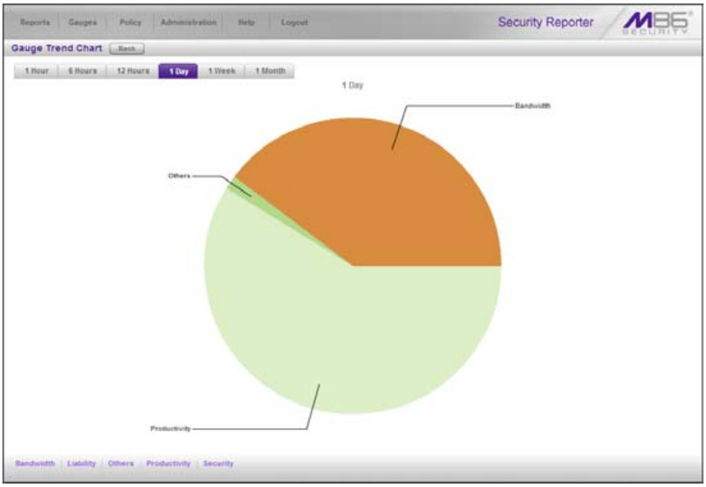


Fig. 5:4-1 Pie trend chart for an individual URL gauge

The pie trend chart that displays in the middle of this panel includes the following information:

- For a URL gauge - By default, each slice of the pie represents the percentage of end user hits in a library category during the last hour; the total for all categories in that gauge equaling 100 percent.
- For a Bandwidth gauge - By default, each slice of the pie represents the percentage of end user traffic for a port during the last hour; the total for all ports in that gauge equaling 100 percent.

The top and bottom sections of this panel contain tabs.

Information about all actions that can be performed in this panel appears in the Navigate a trend chart sub-section.

View overall URL or bandwidth gauge activity

1. In the navigation toolbar, mouse over the Reports menu link and select either the **URL Trend Charts** to display the URL Trend Charts panel, or select **Bandwidth Trend Charts** to display the BandWidth Trend Charts panel:

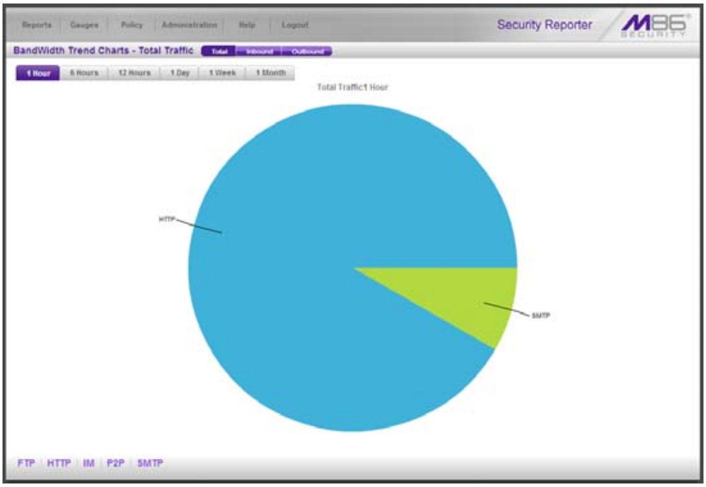


Fig. 5:4-2 Overall Bandwidth Trend Chart, Total Traffic

The pie trend chart that displays in the middle of this panel includes the following information:

- For URL gauges - By default, each slice of the pie represents that URL gauge’s percentage of end user scores during the last hour; the total for all URL gauges in the dashboard equaling 100 percent.
- For Bandwidth gauges - By default, each slice of the pie represents that bandwidth gauge’s percentage of end user traffic during the last hour; the total for all bandwidth gauges in the dashboard equaling 100 percent.

The top and bottom sections of this panel contains tabs. For the bandwidth trend chart, buttons display above this panel.

Information about all actions that can be performed in this panel appears in the Navigate a trend chart sub-section.

Navigate a trend chart

The following actions can be performed in this panel:

- View gauge activity for a different time period (1 Hour, 6 Hours, 12 Hours, 1 Day, 1 Week, 1 Month)
- Analyze gauge activity in a pie chart
- Analyze gauge activity in a line chart
- View Inbound, Outbound bandwidth gauge activity
- Print a trend chart from an IE browser window

View gauge activity for a different time period

To view a pie chart showing activity for a different time period of gauge activity, click the appropriate tab above the pie chart diagram:

- **1 Hour** - This selection displays the gauge URL/byte average score in 10 minute increments for the past 60-minute time period
- **6 Hours** - This selection displays the gauge URL/byte average score in 30 minute increments for the past six-hour time period
- **12 Hours** - This selection displays the gauge URL/byte average score in one hour increments for the past 12-hour time period
- **1 Day** - This selection displays the gauge URL/byte average score in one hour increments for the past 24-hour time period
- **1 Week** - This selection displays the gauge URL/byte average score in 12 hour increments for the past seven-day time period

- **1 Month -** This selection displays the gauge URL/byte average score in one-day increments for the past month’s time period

Once you’ve selected the time period you wish to view, you can analyze the activity for that gauge (see Analyze gauge activity in a pie chart), and drill down into a slice of the pie to view a line chart for that given time period (see Analyze gauge activity in a line chart).

Analyze gauge activity in a pie chart

Once a pie chart displays in the panel, its pieces can be analyzed by mousing over that slice of the pie chart.

The following information displays for that pie slice: gauge component name, percentage of that pie slice (based on a total of 100 percent for all pie slices), and total end user score for that pie slice.

That slice of the pie can be further analyzed by drilling down into it (see Analyze gauge activity in a line chart).

Analyze gauge activity in a line chart

1. To view a line chart showing activity for a slice of the pie chart, do either of the following:
   - Click that slice of the pie chart
   - Click the specified tab beneath the pie chart

   Either action displays the line Trend Chart:

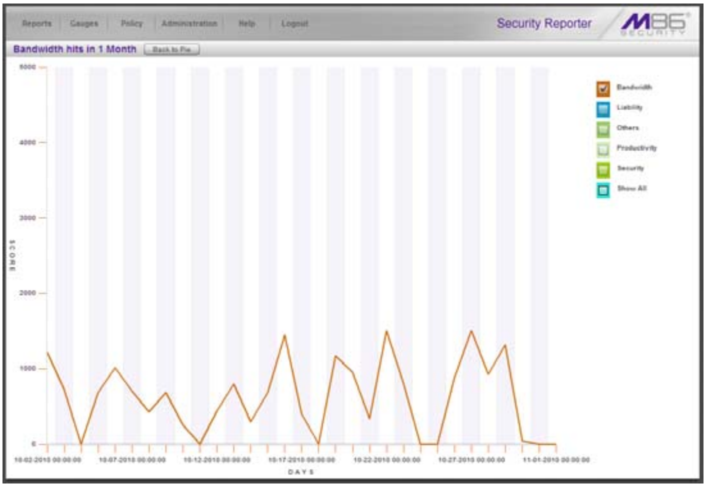


Fig. 5:4-3 Drill into a pie slice to display a line Trend Chart

By default, this chart contains the following information: linear depiction of the total end user SCORE in fixed time increments (using the MM-DD-YYYY HH:MM:SS format) for MINUTES or HOURS included in the specified time period for the gauge component, and the checkbox populated for the selected library category/protocol/port.

NOTE*: See View gauge activity for a different time period for a definition of MINUTES or HOURS included in the current chart.*

2. Perform any of the following actions in this chart:

- To include other gauge component activity in this line chart, click the checkboxes corresponding to the gauge names.

TIP*: Click a populated checkbox to remove the check mark and the line showing activity for that gauge.*

- To view information about a specific point in the line chart, mouse over that point in the chart:

If the chart includes more than one line, and more than one point is located in the area of the mouse pointer, a separate box appears for each point in that section of the chart.

Each box includes the following information: gauge component name, Score for that point, and Minutes or Hours for that fixed time increment (using the MM-DD-YYYY HH:MM:SS format).

- To return to the pie chart, click **Back to Pie** in the upper right portion of the panel.
- To print this trend chart, if using an IE browser, see Print a trend chart from an IE browser window.

View In/Outbound bandwidth gauge activity

By default, the total inbound and outbound bandwidth activity is included in the overall Bandwidth Trend Chart. To view only Inbound or Outbound activity, click the **Inbound** or **Outbound** button above the pie chart, to the right of the Total button.

Print a trend chart from an IE browser window

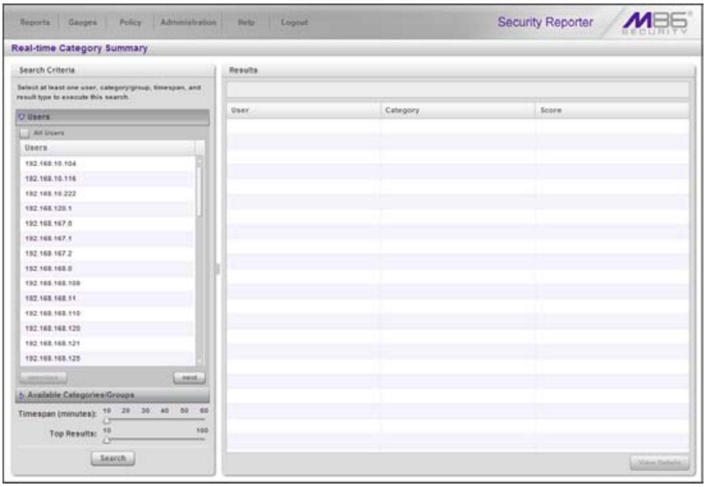
A trend chart can be printed from an IE browser window by using the browser window’s toolbar and going to **File > Print** and proceeding with the print commands.

Chapter 5: Identify Users, Categories

If there are certain end users who are generating excessive, unwanted traffic on the network, or if some library categories containing URLs against your organization's policies are persistently being frequented, you can target offending entities by performing a custom search to identify which users, URLs, and port are being accessed.

Perform a Custom Search

In the navigation toolbar, mouse over the Reports menu link and select **Real-time Category Summary** to display the Real-time Category Summary panel:



Select at least one user, category/group, timespan, and result type to execute this search.

Users
192.168.10.104
192.168.10.116
192.168.10.222
192.168.120.1
192.168.167.0
192.168.167.1
192.168.167.2
192.168.168.0
192.168.168.109
192.168.168.11
192.168.168.110
192.168.168.120
192.168.168.121
192.168.168.125

Fig. 5:5-1 Real-time Category Summary, Users accordion opened

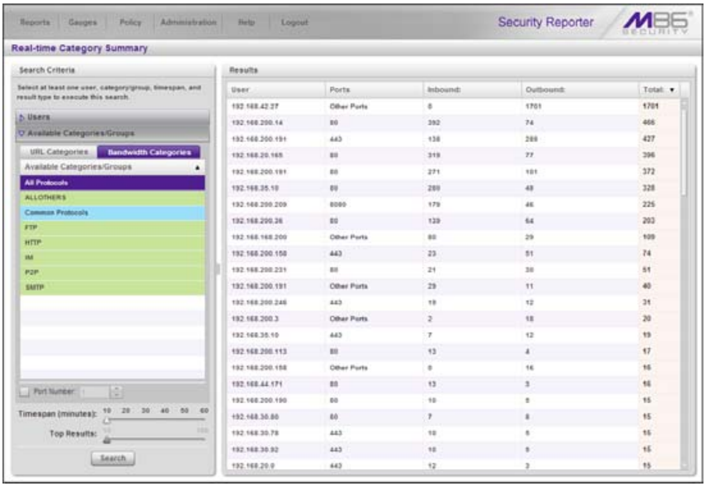
This panel displays the Search Criteria frame to the left with the open Users accordion and closed Available Categories/Groups accordion, Timespan and Top Results sliders, Search button; and to the right, the empty Results target frame.

Specify Search Criteria

1. In the **Users** accordion, do one of the following:
   - To identify users with the highest scores - Click the **All Users** checkbox to select all users in the list and to grey-out the list.
   - To identify the activities of a specific user - Select the user name/IP address from the list to highlight it.
2. Click the Available Categories/Groups accordion to open it.
3. Select either the **URL Categories** or **Bandwidth Categories** tab to display its list of library categories/protocols, and do either of the following:
   - To identify library categories or protocols with the highest scores - Select a category group or protocol that includes as many of categories/ports as possible.
   - To identify activities for a specific class/group - Select that class or group.

     For bandwidth gauges, to query activities for a specific port number, click the **Port Number** checkbox to activate the port field and to deactivate the listed bandwidth protocol selections. Type a specific value in the pre-populated field, and/or use the up/down arrow buttons to increment/decrement the current value by one.
4. Use the **Timespan (Minutes)** slider to specify the time period in which the threat(s)/group(s) were accessed: last 10, 20, 30, 40, 50, 60 minutes.
5. If a user selection other than “All Users” was specified in the Users accordion, the **Top Results** slide becomes activated and you can make a selection for the maximum number of records to return in the results for that user: top 10, 20, 30, 40, 50, 60, 70, 80, 90, 100 records.

6. Click **Search** to display records returned by the query in the Results frame at the right side of the panel:



Real-time Category Summary

Search Criteria

Select at least one user, category/group, timespan, and result type to execute this search.

□ Port Number:

Timespan (minutes):

Top Results:

Results

User	Ports	Inbound:	Outbound:	Total: ▾
192.168.42.27	Other Ports	0	1701	1701
192.168.200.14	80	392	74	466
192.168.200.191	443	138	289	427
192.168.20.165	80	319	77	396
192.168.200.181	80	271	101	372
192.168.35.10	80	280	48	328
192.168.200.209	8080	179	46	225
192.168.200.26	80	139	64	203
192.168.168.200	Other Ports	80	29	109
192.168.200.158	443	23	51	74
192.168.200.231	80	21	30	51
192.168.200.191	Other Ports	29	11	40
192.168.200.246	443	19	12	31
192.168.200.3	Other Ports	2	18	20
192.168.35.10	443	7	12	19
192.168.200.113	80	13	4	17
192.168.200.158	Other Ports	0	16	16
192.168.44.171	80	13	3	16
192.168.200.190	80	10	5	15
192.168.30.80	80	7	8	15
192.168.30.78	443	10	5	15
192.168.30.92	443	10	5	15
192.168.20.0	443	12	3	15

Fig. 5:5-2 Search results for Bandwidth Categories

For each record in the table, the following information displays:

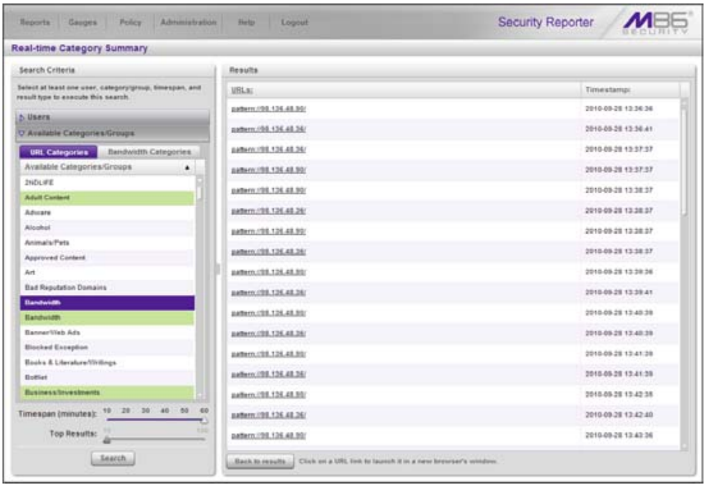
- For a URL search - User (user name/IP address), Category name, and the end user’s total Score for that record.
- For a bandwidth search - User (user name/IP address), Ports number, Inbound score, Outbound score, and the end user’s Total score for that record.

For a URL search, you can drill down even further by selecting a user’s record and then viewing the URLs that user accessed (see View URLs within the accessed category).

View URLs within the accessed category

In the Results frame, do the following to view a specific URL:

1. Click the User name/IP address to highlight that user's record and to activate the View Details button.
2. Click **View Details** to display a list of URLs and corresponding Timestamp (using the YYYY-MM-DD HH:MM:SS format) for each URL in the library category accessed by the end user within the specified time period:



Select at least one user, category/group, timespan, and result type to execute this search.

URLs:	Timestamp:
pattern://98.126.48.90/	2010-09-28 13:36:36
pattern://98.126.48.36/	2010-09-28 13:36:41
pattern://98.126.48.36/	2010-09-28 13:37:37
pattern://98.126.48.90/	2010-09-28 13:37:37
pattern://98.126.48.90/	2010-09-28 13:38:37
pattern://98.126.48.26/	2010-09-28 13:38:37
pattern://98.126.48.90/	2010-09-28 13:38:37
pattern://98.126.48.26/	2010-09-28 13:38:37
pattern://98.126.48.90/	2010-09-28 13:39:36
pattern://98.126.48.26/	2010-09-28 13:39:41
pattern://98.126.48.90/	2010-09-28 13:40:38
pattern://98.126.48.26/	2010-09-28 13:40:39
pattern://98.126.48.90/	2010-09-28 13:41:38
pattern://98.126.48.36/	2010-09-28 13:41:39
pattern://98.126.48.90/	2010-09-28 13:42:38
pattern://98.126.48.26/	2010-09-28 13:42:40
pattern://98.126.48.90/	2010-09-28 13:43:36

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

Fig. 5:5-3 List of URLs visited by the user

***TIP**: Click Back to results to return to the previous page where you can perform another query.*

You can now print the results displayed in this window if using an IE browser window, or access another selected URL.

SECURITY REPORTS SECTION

Introduction

This section of the user guide provides instructions to administrators on how to utilize data from SWG logs for monitoring end user Internet and network usage via security reports.

- Chapter 1: Security Reports - This chapter explains how to use the four basic security reports: Blocked Viruses, Security Policy Violations, Traffic Analysis, and Rule Transactions.
- Chapter 2: Security Report Wizard - This chapter explains how to use the Report Wizard to create your own customized security reports.

***NOTES**: If the SR is connected to an SWG running software version 9.2.X, reports may not be accurate since bypass transactions (e.g. streaming) are not logged for the SR to process.*

***WARNING**: To prevent requested security reports from being blocked by your email client, be sure to whitelist the SR's source email address in your email client. The source email address can be found in System Configuration > Server > SMTP Server Setting, in the "From Email Address" field.*

Chapter 1: Security Reports

Security Reports are accessible by navigating to **Reports > Security Reports** and selecting the report type from the menu:

- **Blocked Viruses** - This report displays details for each instance of each blocked virus detected from end user Internet/network activity:
- **Security Policy Violations** - This report provides information on each instance in which an end user breached a security policy.
- **Traffic Analysis** - This report shows activity for end user access of objects utilizing an excessive amount of network bandwidth.
- **Rule Transactions** - This report lists each instance in which an end user triggered a threshold in an SWG Security Policy.

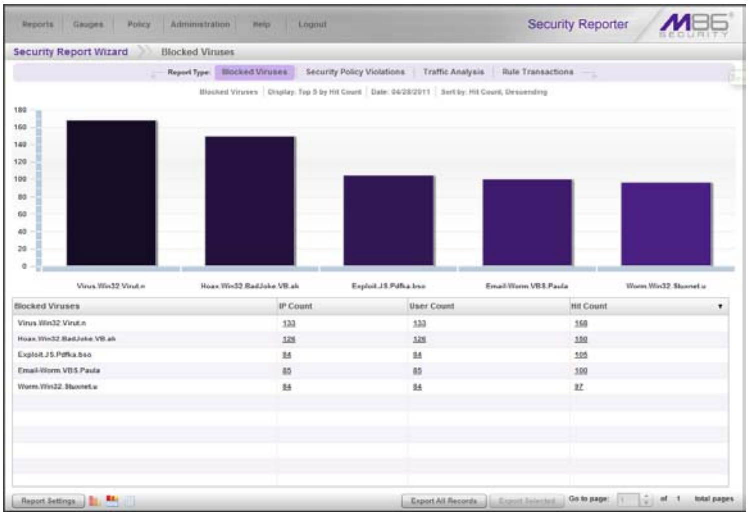
***NOTE**: Once you have generated one of the four basic security report views, you can use the Report Wizard to customize your view, save the view, export the view, and/or schedule the report to run at a designated time. The Report Wizard feature for security reports is discussed in detail in Chapter 2: Security Report Wizard.*

Security Report Format

For each report type, by default the top portion of the report view includes tabs for all security Report Types. The following information displays beneath this row of tabs: report type, Display criteria, Date (MM/DD/YYYY format), and Sort by criteria. Beneath this row, a bar chart depicts the first six records for the current report type.

***NOTE**: Mousing 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.*

Beneath the bar chart is a table containing rows of records. Columns of pertinent statistics display for each record (e.g. IP Count, User Count, etc.).



Blocked Viruses | Display: Top 5 by Hit Count | Date: 04/28/2011 | Sort by: Hit Count, Descending

Blocked Viruses	IP Count	User Count	Hit Count ▼
Virus.Win32.Virut.n	133	133	168
Hoax.Win32.BadJoke.VB.ah	126	126	150
Exploit.JS.Pdfka.bso	84	84	105
Email-Worm.VBS.Paula	85	85	100
Worm.Win32.Stuxnet.u	84	84	97

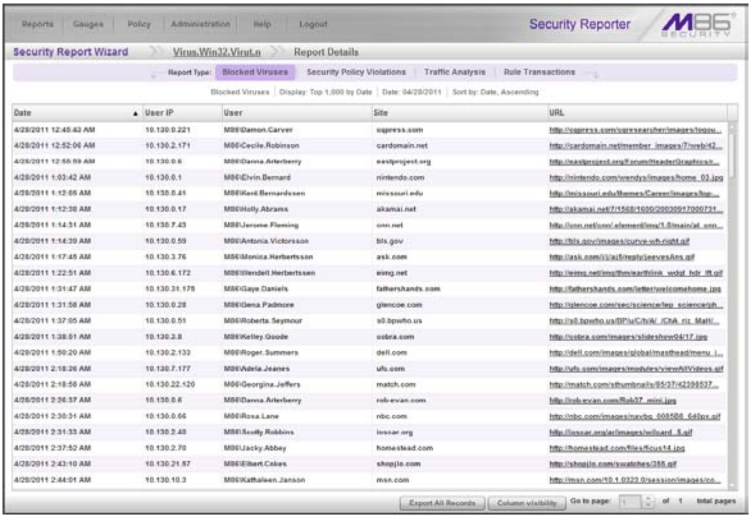
Go to page: 1 of 1 total pages

Fig. 6:1-1 Sample Blocked Viruses report view

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

Clicking an IP Count or User Count link in a column for a specific record displays additional information about that record in a similar report view format (as depicted in Fig. 6:1-1). However, this second or third level drill down report view cannot be re-run, saved, or scheduled to run at a designated time.

Clicking a link in the Hit Count or Bandwidth column generates a detail report view with only a table of records and not a bar chart, as shown in the sample report below:



Blocked Viruses | Display: Top 1,000 by Date | Date: 04/28/2011 | Sort by: Date, Ascending

Date ▲	User IP	User	Site	URL
4/28/2011 12:40:43 AM	10.130.0.221	M86\Damon.Carver	cqpress.com	http://cqpress.com/cqresearcher/images/logou...
4/28/2011 12:52:06 AM	10.130.2.171	M86\Cecile.Robinson	cardomain.net	http://cardomain.net/member_images/7/web/42...
4/28/2011 12:55:59 AM	10.130.0.6	M86\Danna.Arterberry	eastproject.org	http://eastproject.org/Forum/HeaderGraphics/r...
4/28/2011 1:03:42 AM	10.130.0.1	M86\Elvin.Bernard	nintendo.com	http://nintendo.com/wendys/images/home_03.jpg
4/28/2011 1:12:05 AM	10.130.0.41	M86\Kent.Bernardssen	missouri.edu	http://missouri.edu/themes/Career/images/top...
4/28/2011 1:12:38 AM	10.130.0.17	M86\Holly.Abrams	akamai.net	http://akamai.net/7/1560/1000/20030917000731...
4/28/2011 1:14:31 AM	10.130.7.43	M86\Jerome.Fleming	cnn.net	http://cnn.net/cnn/.element/img/1.0/main/at_cnn...
4/28/2011 1:14:39 AM	10.130.0.59	M86\Antonia.Victorsson	bls.gov	http://bls.gov/images/curve-wh-right.gif
4/28/2011 1:17:45 AM	10.130.3.76	M86\Monica.Herbertsson	ask.com	http://ask.com/i/j/ajf/reply/jeevesAns.gif
4/28/2011 1:22:51 AM	10.130.6.172	M86\Wendell.Herbertssen	eimg.net	http://eimg.net/img/thm/earthlink_wdgt_hdr_lft.gif
4/28/2011 1:31:47 AM	10.130.31.178	M86\Gaye.Daniels	fathershands.com	http://fathershands.com/letter/welcomehome.jpg
4/28/2011 1:31:58 AM	10.130.0.28	M86\Gena.Padmore	glencoe.com	http://glencoe.com/sec/science/ep_science/ph...
4/28/2011 1:37:05 AM	10.130.0.51	M86\Roberta.Seymour	s0.bpwho.us	http://s0.bpwho.us/BP/u/C/h/A/_/ChA_riz_Matt/...
4/28/2011 1:38:01 AM	10.130.2.8	M86\Kelley.Goode	cobra.com	http://cobra.com/images/slideshow04/17.jpg
4/28/2011 1:50:20 AM	10.130.2.133	M86\Roger.Summers	dell.com	http://dell.com/images/global/masthead/menu_i...
4/28/2011 2:18:26 AM	10.130.7.177	M86\Adela.Jeanes	ufo.com	http://ufo.com/images/modules/viewAllVideos.gif
4/28/2011 2:18:56 AM	10.130.22.120	M86\Georgina.Jeffers	match.com	http://match.com/sthumbnails/95/37/42398537...
4/28/2011 2:26:37 AM	10.130.0.6	M86\Danna.Arterberry	rob-evan.com	http://rob-evan.com/Rob37_mini.jpg
4/28/2011 2:30:31 AM	10.130.0.66	M86\Rosa.Lane	nbc.com	http://nbc.com/images/navbg_008500_640px.gif
4/28/2011 2:31:33 AM	10.130.2.40	M86\Scotty.Robbins	iowscar.org	http://iowscar.org/ar/images/wilboard_5.gif
4/28/2011 2:37:52 AM	10.130.2.70	M86\Jacky.Abbey	homestead.com	http://homestead.com/files/ficus14.jpg
4/28/2011 2:43:10 AM	10.130.21.87	M86\Elbert.Cokes	shopjlo.com	http://shopjlo.com/swatches/355.gif
4/28/2011 2:44:01 AM	10.130.10.3	M86\Kathaleen.Janson	msn.com	http://msn.com/10.1.0323.0/session/images/co...

Go to page: 1 of 1 total pages

Fig. 6:1-2 Blocked Viruses detail report view for Hit Count

The bottom portion of this panel only includes tools for hiding columns and exporting all records.

***TIP**: To refresh the report view displayed in the panel, select **Reports > Security Reports** and choose the report type again.*

Security Report Types

Blocked Viruses report view

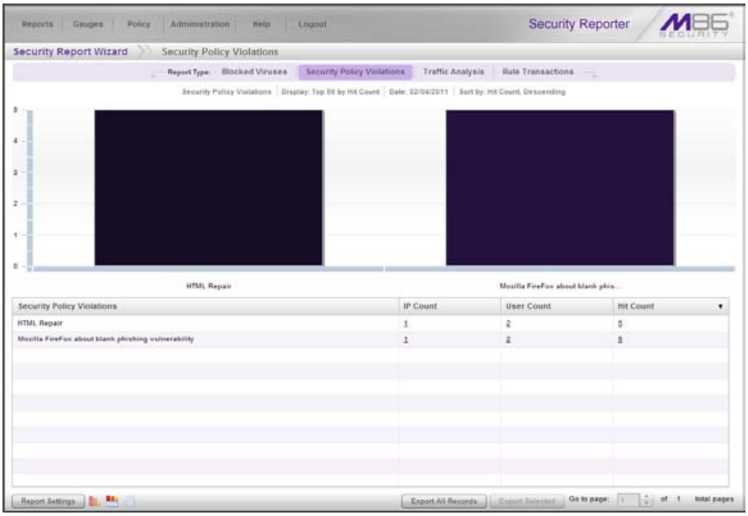
The Blocked Viruses report view is accessible via **Reports > Security Reports > Blocked Viruses** (see Fig. 6:1-1).

The following statistics display for each Blocked Virus record in the table: IP Count and User Count of end users who encountered the blocked virus, and the Hit Count for all instances of this blocked virus encounter.

Click a link in any of these columns to drill down into the specified record and create a new report view (see Drill Down into a Security Report).

Security Policy Violations report view

The Security Policy Violations report view is accessible via **Reports > Security Reports > Security Policy Violations**:



Security Policy Violations | Display: Top 50 by Hit Count | Date: 02/04/2011 | Sort by: Hit Count, Descending

Security Policy Violations	IP Count	User Count	Hit Count ▼
HTML Repair	1	2	5
Mozilla FireFox about blank phishing vulnerability	1	2	5

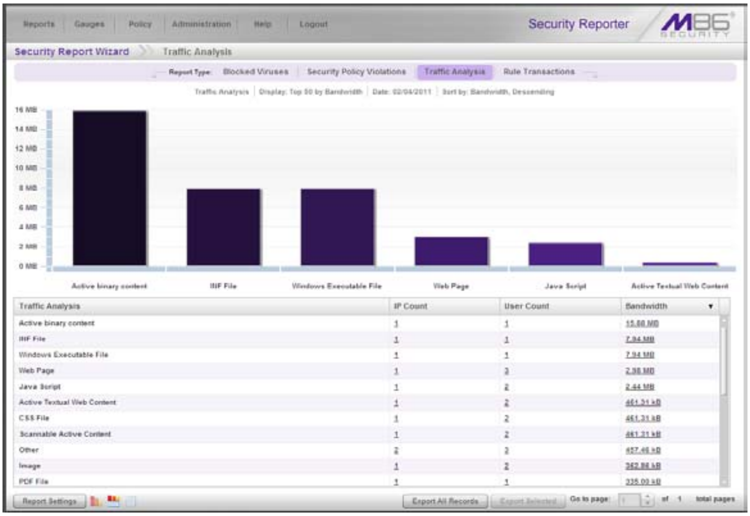
Fig. 6:1-3 Security Policy Violations report view

The following statistics display for each Security Policy Violation record in the table: IP Count, User Count, and Hit Count for end users who breached that security policy, and the Hit Count for all instances of this type of security breach.

Click a link in any of these columns to drill down into the specified record and create a new report view (see Drill Down into a Security Report).

Traffic Analysis report view

The Blocked Viruses report view is accessible via **Reports > Security Reports > Traffic Analysis**:



Traffic Analysis | Display: Top 50 by Bandwidth | Date: 02/04/2011 | Sort by: Bandwidth, Descending

Traffic Analysis	IP Count	User Count	Bandwidth ▼
Active binary content	1	1	15.60 MB
IIIF File	1	1	7.94 MB
Windows Executable File	1	1	7.94 MB
Web Page	1	3	2.98 MB
Java Script	1	2	2.44 MB
Active Textual Web Content	1	2	461.31 kB
CSS File	1	2	461.31 kB
Scannable Active Content	1	2	461.31 kB
Other	2	3	457.46 kB
Image	1	2	362.86 kB
PDF File	1	1	335.03 kB

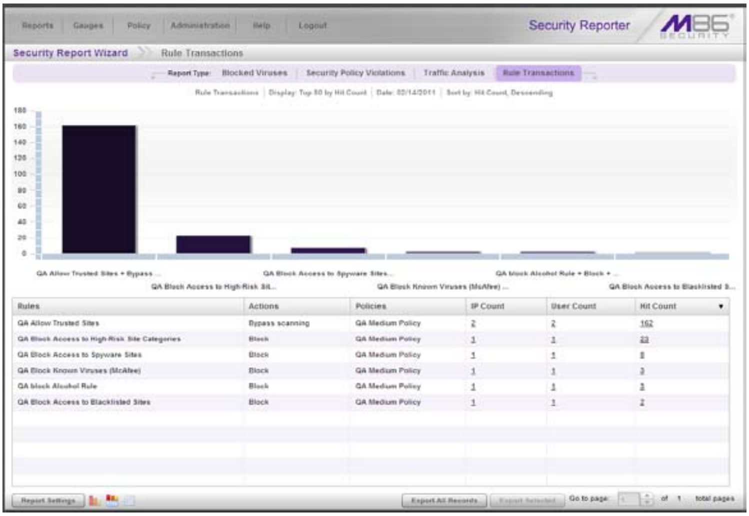
Fig. 6:1-4 Traffic Analysis report view

The following statistics display for each Traffic Analysis record in the table: IP Count and User Count of end users who accessed the high bandwidth usage object, and the Bandwidth used in all occurrences of accessing this object.

Click a link in any of these columns to drill down into the specified record and create a new report view (see Drill Down into a Security Report).

Rule Transactions report view

The Blocked Viruses report view is accessible via **Reports > Security Reports > Rule Transactions**:



Rule Transactions | Display: Top 50 by Hit Count | Date: 02/14/2011 | Sort by: Hit Count, Descending

Rules	Actions	Policies	IP Count	User Count	Hit Count ▼
QA Allow Trusted Sites	Bypass scanning	QA Medium Policy	2	2	162
QA Block Access to High-Risk Site Categories	Block	QA Medium Policy	1	1	23
QA Block Access to Spyware Sites	Block	QA Medium Policy	1	1	8
QA Block Known Viruses (McAfee)	Block	QA Medium Policy	1	1	3
QA block Alcohol Rule	Block	QA Medium Policy	1	1	3
QA Block Access to Blacklisted Sites	Block	QA Medium Policy	1	1	2

Go to page: 1 of 1 total pages

Fig. 6:1-5 Rule Transactions report view

The following statistics display for each Rule Transactions record in the table: In the Actions column, the action performed by the SWG regarding the rule applied to that transaction; in the Policies column, the policy from the SWG applied to that transaction; the IP Count and User Count of end users who triggered that rule, and the Hit Count of all user encounters for that record.

Click a link in any of the Count columns to drill down into the specified record and create a new report view (see Drill Down into a Security Report).

Drill Down into a Security Report

In the current report view, more details about a record can be obtained by drilling down into a column for that record.

For Blocked Viruses, Security Policy Violations, and Rules Transactions reports:

- Clicking an IP Count column link displays a report view with columns for IPs, User Count, and Hit Count.

  From this report view, clicking a User Count column link displays a report view with columns for Users and Hit Count.

***NOTE**: Clicking a Hit Count link displays a detail report view with columns for Date (M/D/YYYY H:MM:SS AM/PM format), User IP, User name path, Site name, and URL.*

- Clicking a User Count column link displays a report view with columns for Users, IP Count, and Hit Count.

  From this report view, clicking an IP Count column link displays a report view with columns for IPs and Hit Count.

For Traffic Analysis reports:

- Clicking an IP Count column link displays a report view with columns for IPs, User Count, and Bandwidth.

  From this report view, clicking a User Count column link displays a report view with columns for Users and Bandwidth.

***NOTE**: Clicking a Bandwidth link displays a detail report view with columns for Date (M/D/YYYY H:MM:SS AM/PM format), User IP, User name path, Site name, Bandwidth, and URL.*

- Clicking a User Count column link displays a report view with columns for Users, IP Count, and Bandwidth.

From this report view, clicking an IP Count column link displays a report view with columns for IPs and Bandwidth.

Security Report Tools

Security Report Type tabs

Report Type tabs (Blocked Viruses, Security Policy Violations, Traffic Analysis, and Rule Transactions) display at the top of the panel. Click one of these tabs to display the specified report view.

Report Settings menu

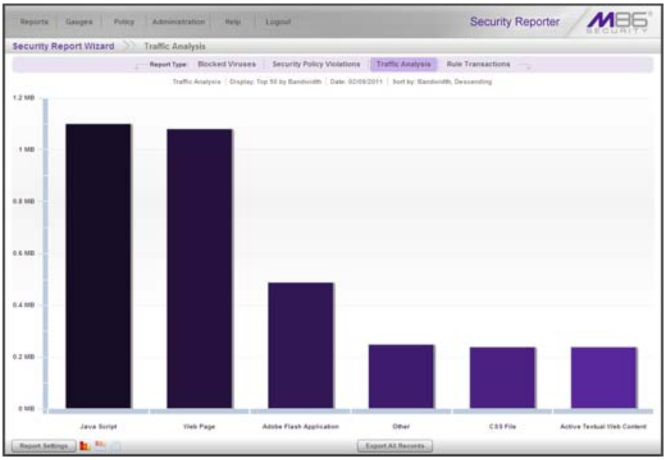
For basic Security Report types, mouse over **Report Settings** at the bottom of the panel to display a menu of reporting options: Run, Save, Schedule (see Report Settings Options).

NOTE*: The Report Settings menu is not available for second and third level report views.*

Report view icons

Click the following report view icon to change the report view display:

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

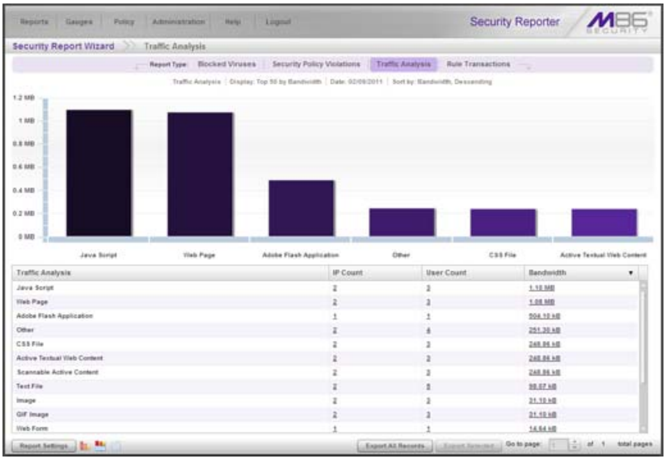


Traffic Analysis | Display: Top 50 by Bandwidth | Date: 02/09/2011 | Sort by: Bandwidth, Descending

Fig. 6:1-6 Sample top six bars view

Note that the graph only report view footer does not include the Export Selected button and page navigation field.

- Click this icon to display the top six bars and table of records:



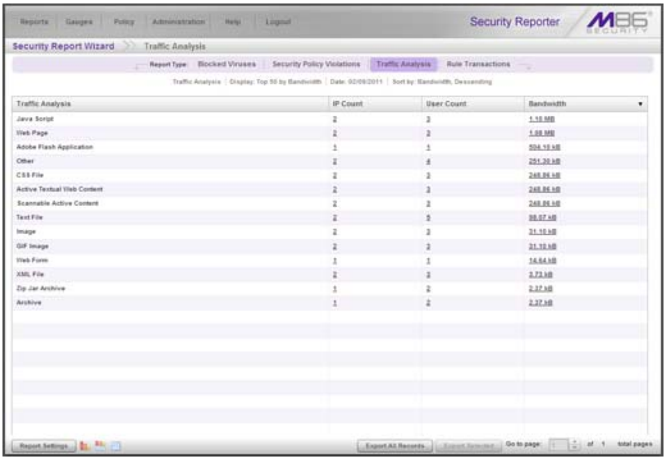
Traffic Analysis | Display: Top 50 by Bandwidth | Date: 02/09/2011 | Sort by: Bandwidth, Descending

Traffic Analysis	IP Count	User Count	Bandwidth ▼
Java Script	2	2	1.10 MB
Web Page	2	3	1.08 MB
Adobe Flash Application	1	1	504.10 kB
Other	2	4	251.30 kB
CSS File	2	3	248.86 kB
Active Textual Web Content	2	2	248.86 kB
Scannable Active Content	2	3	248.86 kB
Text File	2	5	98.07 kB
Image	2	3	31.10 kB
GIF Image	2	3	31.10 kB
Web Form	1	1	14.64 kB

Go to page: 1 of 1 total pages

Fig. 6:1-7 Sample top six bars and report records view (default view)

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



Traffic Analysis | Display: Top 50 by Bandwidth | Date: 02/09/2011 | Sort by: Bandwidth, Descending

Traffic Analysis	IP Count	User Count	Bandwidth
Java Script	2	3	1.15 MB
Web Page	2	2	1.08 MB
Adobe Flash Application	1	1	504.15 kB
Other	2	4	251.30 kB
CSS File	2	3	248.86 kB
Active Textual Web Content	2	3	248.86 kB
Scannable Active Content	2	2	248.86 kB
Text File	2	5	98.07 kB
Image	2	3	31.10 kB
GIF Image	2	2	31.10 kB
Web Form	1	1	14.64 kB
XML File	2	3	3.73 kB
Zip Jar Archive	1	2	2.27 kB
Archive	1	2	2.27 kB

Go to page: 1 of 1 total pages

Fig. 6:1-8 Sample records only view

Security Report Exportation

Click **Export All Records** to open the Export Report pop-up window in which you specify criteria for the report to be generated and distributed (see Export a Security Report).

After selecting one or more records in the table by clicking the first column to select records, click **Export Selected** to open the Export Report pop-up window (see Export a Security Report).

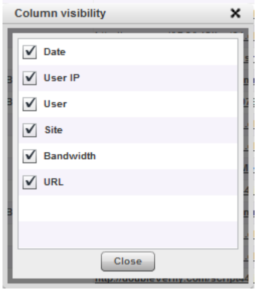
Navigating Pages of Records

At the bottom right of the panel, the **Go to page** field displays: Go to page 1 of 2 total pages

If more than one page of records displays for the total pages returned, enter a page number within that range to navigate to that page of records, or use the up/down arrow(s) to specify the page you want displayed.

Detail Report Column visibility

By default all report view column(s) display. For a detail report view created by drilling down into a Hit Count or Bandwidth column, you can hide a column by clicking the **Column visibility** button at the bottom of the panel to open the Column visibility pop-up window, and then de-selecting the checkbox corresponding to that column:


Column visibility ×

☑ Date
☑ User IP
☑ User
☑ Site
☑ Bandwidth
☑ URL

*TIP: After making your modifications, click **Close** to close the Column visibility pop-up window.*

- **Date** - Displays the date in the M/D/YYYY H:M:S AM/PM format
- **User IP** - Displays the IP address of the user’s machine (e.g. “200.10.101.80”).
- **User** - Displays any of the following information: username, user IP address, or the path and username (e.g. “logo\admin\jsmith”).
- **Site** - Displays the URL the user attempted to access (e.g. “coors.com”).
- **Bandwidth** (for Bandwidth detail results only) - Displays the amount of bandwidth (in MB or GB) used by the end user.
- **URL** - Displays the link for the item accessed by the end user.

Security Report Tips

Breadcrumb trail

When generating a report view and modifying that report view to create another report view, a trail of breadcrumb links remain in the row beneath the navigation toolbar. Clicking a specified level in the trail link returns you to that prior report view.

Column sorting tips

To sort report view records in ascending/descending order by a specified column, click that column's header: report type name, IP Count, User Count, Bandwidth, Hit Count, Rules, Actions, Policies, Date, User IP, User name, Site, or URL.

Click the same column header again to sort records for that column in the reverse order.

Click another column header to sort records by that specified column.

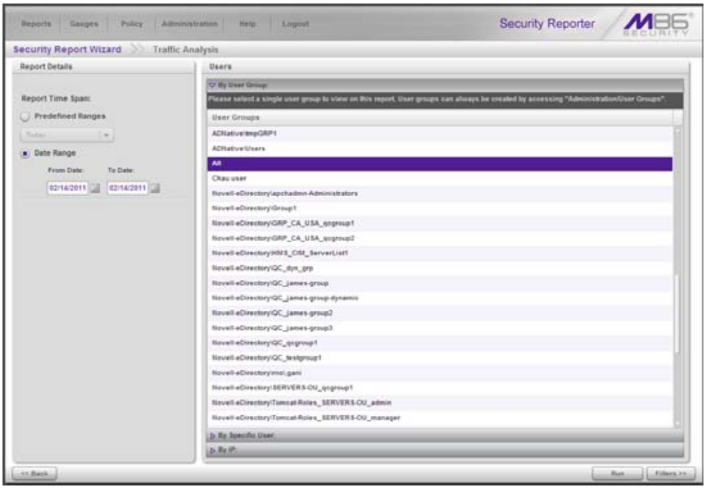
URL viewing tip

In a URL column, click the URL for a specified record to view the item currently indexed in the SR's memory.

Report Settings Options

Run a Security Report

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



Report Details

Report Time Span:

○ Predefined Ranges

Today

● Date Range

From Date: 02/14/2011

To Date: 02/14/2011

Users

By User Group

Please select a single user group to view on this report. User groups can always be created by accessing "Administration/User Groups".

User Groups

ADNative\tmpGRP1
ADNative\Users
All
Chau user
Novell-eDirectory\apchadmn-Administrators
Novell-eDirectory\Group1
Novell-eDirectory\GRP_CA_USA_qcgroup1
Novell-eDirectory\GRP_CA_USA_qcgroup2
Novell-eDirectory\HMS_CIM_ServerList1
Novell-eDirectory\QC_dyn_grp
Novell-eDirectory\QC_james-group
Novell-eDirectory\QC_james-group-dynamic
Novell-eDirectory\QC_james-group2
Novell-eDirectory\QC_james-group3
Novell-eDirectory\QC_qcgroup1
Novell-eDirectory\QC_testgroup1
Novell-eDirectory\mol_gani
Novell-eDirectory\SERVERS-OU_qcgroup1
Novell-eDirectory\Tomcat-Roles_SERVERS-OU_admin
Novell-eDirectory\Tomcat-Roles_SERVERS-OU_manager

By Specific User

By IP

Fig. 6:1-9 Report Settings Run option

2. In the Report Details frame, specify the **Report Time Span** by choosing one of two options:

   - **Predefined Ranges** - If selecting this option, make a choice 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** (default) - If selecting this option, use the calendar icons to set the date range.

TIP: *At the bottom left of the panel, click **<< Back** at any time to return to the previous Security Report panel.*

3. In the Users frame, 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:

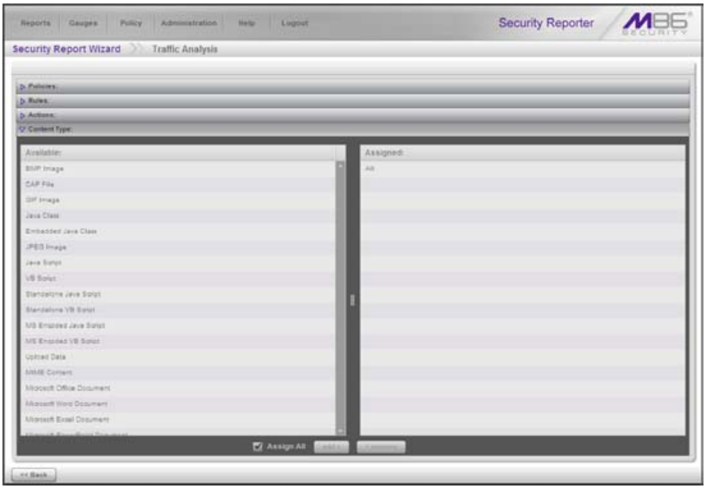


Fig. 6:1-10 Report Filters option

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.

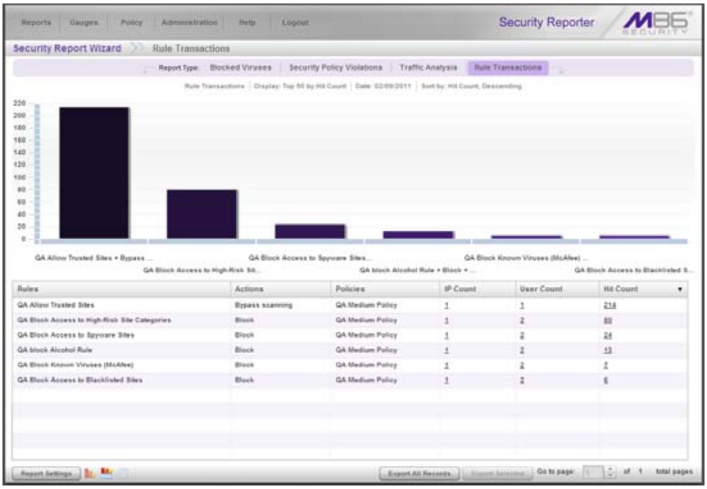
***TIPS**: Multiple records can be selected by clicking each record while pressing the Ctrl key on your keyboard. Blocks of records can be selected by clicking the first record, and then pressing the Shift key on your keyboard while clicking the last record.*

*To remove the record(s), select the record(s) from the Assigned list box and click **< remove**.*

- 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.

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



Rule Transactions | Display: Top 50 by Hit Count | Date: 02/09/2011 | Sort by: Hit Count, Descending

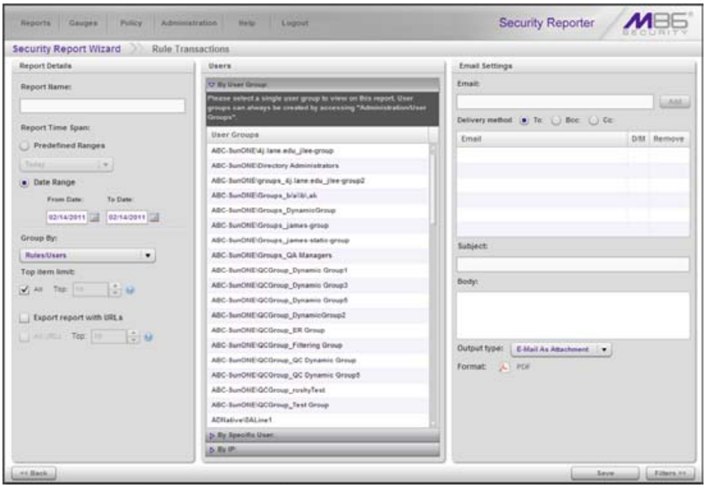
Rules	Actions	Policies	IP Count	User Count	Hit Count ▼
QA Allow Trusted Sites	Bypass scanning	QA Medium Policy	1	1	214
QA Block Access to High-Risk Site Categories	Block	QA Medium Policy	1	2	80
QA Block Access to Spyware Sites	Block	QA Medium Policy	1	2	24
QA block Alcohol Rule	Block	QA Medium Policy	1	2	13
QA Block Known Viruses (McAfee)	Block	QA Medium Policy	1	2	7
QA Block Access to Blacklisted Sites	Block	QA Medium Policy	1	2	6

Fig. 6:1-11 Generated Security Report view

The report can now be exported by selecting one of the export options (see Export a Security Report).

Save a Security Report

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


Reports
Gauges
Policy
Administration
Help
Logout
Security Reporter
M86 SECURITY
Security Report Wizard
Rule Transactions
Report Details
Report Name:
Report Time Span:
○ Predefined Ranges
Today
● Date Range
From Date:
To Date:
Group By:
Top item limit:
☑ All
Top:
□ Export report with URLs
□ All URLs
Top:
Users
By User Group
User Groups
ABC-SunONE\4j.lane.edu_jlee-group
ABC-SunONE\Directory Administrators
ABC-SunONE\groups_4j.lane.edu_jlee-group2
ABC-SunONE\Groups_b/a\b\ak
ABC-SunONE\Groups_DynamicGroup
ABC-SunONE\Groups_james-group
ABC-SunONE\Groups_james-static-group
ABC-SunONE\Groups_QA Managers
ABC-SunONE\QCGroup_Dynamic Group1
ABC-SunONE\QCGroup_Dynamic Group3
ABC-SunONE\QCGroup_Dynamic Group5
ABC-SunONE\QCGroup_DynamicGroup2
ABC-SunONE\QCGroup_ER Group
ABC-SunONE\QCGroup_Filtering Group
ABC-SunONE\QCGroup_QC Dynamic Group
ABC-SunONE\QCGroup_QC Dynamic Group5
ABC-SunONE\QCGroup_roshyTest
ABC-SunONE\QCGroup_Test Group
ADNative\SALine1
By Specific User:
By IP:
Email Settings
Email:
Add
Delivery method: ● To: ○ Bcc: ○ Cc:
Email
D/M
Remove
Subject:
Body:
Output type:
Format:
PDF
<< Back
Save
Filters >>

Please select a single user group to view on this report. User groups can always be created by accessing "Administration/User Groups".

From Date: 02/14/2011 To Date: 02/14/2011

Group By: Rules/Users

Output type: E-Mail As Attachment

Fig. 6:1-12 Report Settings Save option

2. In the Report Details frame:

   a. Type in the **Report Name**.

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

   - **Predefined Ranges** - If selecting this option, make a choice 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 selecting this default option, use the calendar icons to set the date range.

c. Specify the **Group By** report type selection from the available choices in the pull-down menu, if the report will be grouped by more than one report type.

d. Indicate the **Top item limit** to be included in the report; by default “All” is selected. To modify this selection, uncheck this box and specify the **Top** number of items.

e. 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

3. In the Users frame, 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 (see Fig. 6:1-10).

TIP: *At the bottom left of the panel, click* ***<< Back*** *at any time to return to the Security Report Wizard 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.

***TIPS**: Multiple records can be selected by clicking each record while pressing the Ctrl key on your keyboard. Blocks of records can be selected by clicking the first record, and then pressing the Shift key on your keyboard while clicking the last record. To remove the record(s), select the record(s) from the Assigned list box and click **< remove**.*

- 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.

4. In the Email Settings frame:

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".

***TIP**: To remove an email address, click the "**X**" in the **Remove** column of the list box.*

***NOTE**: Follow the above procedures for each email to be added.*

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

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

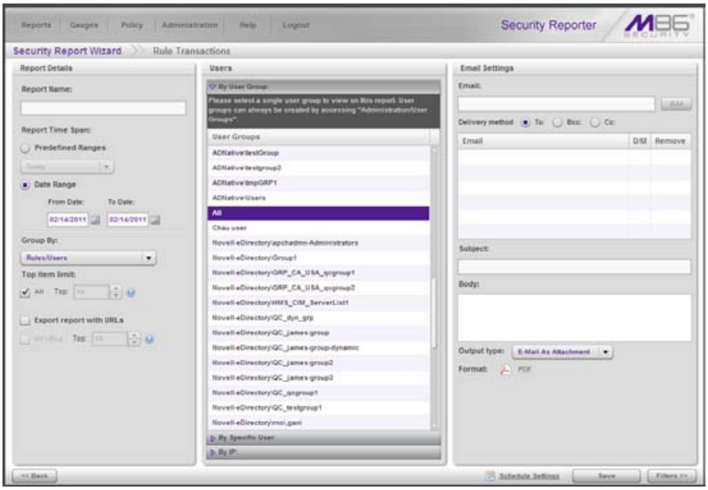
e. Specify the **Output type** to be used for the PDF report file in the email: "E-Mail As Attachment" or "E-Mail As Link".

***NOTE**: The report will be generated in the PDF Format and emailed to the address(es) provided.*

5. 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 (see Saved Reports in Chapter 3 of the Productivity Reports Section).

Schedule a Security Report to Run

1. In the security report view, click **Report Settings** and choose **Schedule** to display the Security Report Wizard panel for scheduling the report to run:



● Date Range
From Date: 02/14/2011 To Date: 02/14/2011
Group By: Rules/Users
Top item limit: ☑ All Top:
□ Export report with URLs

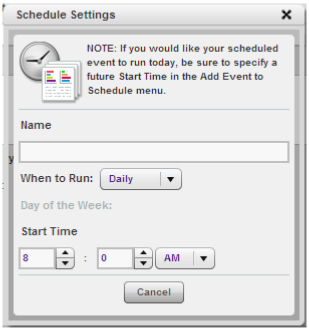
Please select a single user group to view on this report. User groups can always be created by accessing "Administration/User Groups".

ADNative\testGroup
ADNative\testgroup2
ADNative\tmpGRP1
ADNative\Users
All
Chau user
Novell-eDirectory\apchadmn-Administrators
Novell-eDirectory\Group1
Novell-eDirectory\GRP_CA_USA_qcgroup1
Novell-eDirectory\GRP_CA_USA_qcgroup2
Novell-eDirectory\HMS_CIM_ServerList1
Novell-eDirectory\QC_dyn_grp
Novell-eDirectory\QC_james-group
Novell-eDirectory\QC_james-group-dynamic
Novell-eDirectory\QC_james-group2
Novell-eDirectory\QC_james-group3
Novell-eDirectory\QC_qcgroup1
Novell-eDirectory\QC_testgroup1
Novell-eDirectory\rnoi_gani

Delivery method ● To: ○ Bcc: ○ Cc:
Output type: E-Mail As Attachment
Format: PDF

Fig. 6:1-13 Report Settings Schedule option

2. After specifying criteria for saving the report, go to the lower right corner of the panel and click **Schedule Settings** to open the Schedule Settings pop-up window:



Schedule Settings

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

Name

When to Run: Daily

Day of the Week:

Start Time

8 : 0 AM

Fig. 6:1-14 Schedule Settings

3. Enter a **Name** for the report run event you are scheduling.
4. 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).
5. Select the **Start Time** for the report: 1 - 12 for the hour, 0 - 59 for the minutes, and AM or PM.

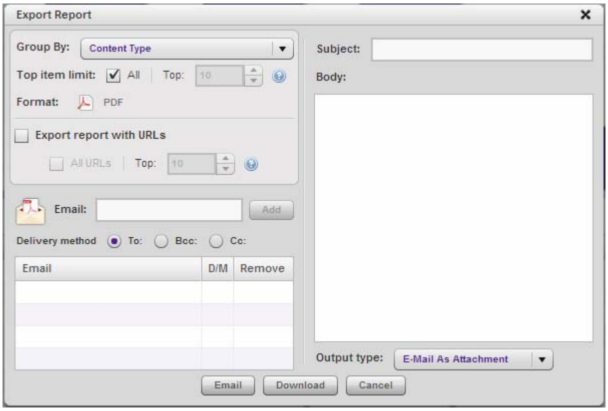
NOTE: *The default Start Time is 8:00 AM. If you wish to run a report today and this time has already passed, be sure to select a future time.*

TIP: *Click **Cancel** to close the pop-up window without saving a schedule.*

6. 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 (see Report Schedule in Chapter 3 of the Productivity Reports Section).

Export a Security Report

At the bottom of the security report view panel, click either **Export All Records** or **Export Selected** to open the Export Report pop-up window:


Export Report

Group By: Content Type

Top item limit: ☑ All Top: 10

Format: PDF

□ Export report with URLs

□ All URLs Top: 10

Email:

Delivery method ● To: ○ Bcc: ○ Cc:

Email	D/M	Remove

Subject:

Body:

Output type: E-Mail As Attachment

Fig. 6:1-15 Export Report pop-up window

***TIP**: Click **Cancel** to close the pop-up window without executing any of the export functions.*

1. Specify the **Group By** report type selection from the available choices in the pull-down menu.
2. If the Export Selected option was specified, the **Top item limit** for “All” is selected and greyed-out.

   If the Export All Records option was specified, the **Top item limit** for “All” is selected but can be changed. To modify this selection, uncheck this box and specify the **Top** number of items to be included in the exported report.
3. For the basic four Security Report types, 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

For Bandwidth or Hit Count detail drill down report views, the Export report with URLs checkbox displays selected and greyed-out.

For all other drill down report views, the Export report with URLs checkbox does not display.

4. To download the report in the PDF format without emailing it, click **Download**. To email the report, proceed to step 5.
5. If the report will be emailed instead of downloaded:

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”.

TIP: *To remove an email address, click the “**X**” in the **Remove** column of the list box.*

NOTE: *Follow the above procedures in step 5 for each email to be added.*

c. Enter the **Subject** for the email message.

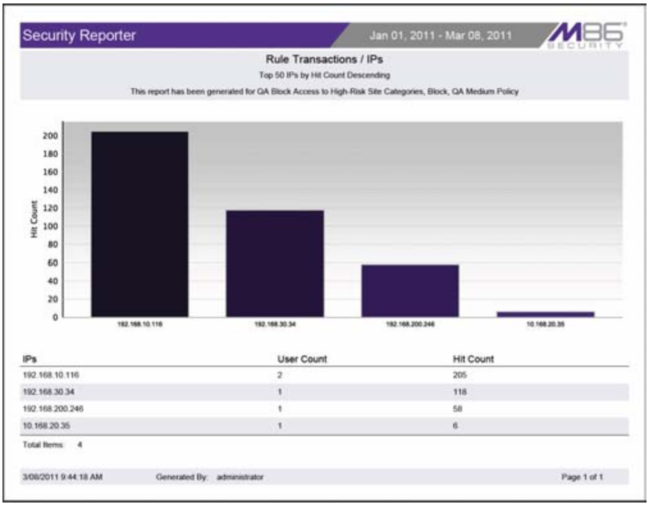
d. If you wish, enter text to be included in the **Body** of the message.

e. Specify the **Output type** to be used for the PDF report file in the email: “E-Mail As Attachment” or “E-Mail As Link”.

f. Click **Email Report** to send the report in the PDF format via email to the specified recipient(s).

Security Report Format

The generated Security Report PDF file includes the following information:



Security Reporter Jan 01, 2011 - Mar 08, 2011

Rule Transactions / IPs

Top 50 IPs by Hit Count Descending

This report has been generated for QA Block Access to High-Risk Site Categories, Block, QA Medium Policy

IPs	User Count	Hit Count
192.168.10.116	2	205
192.168.30.34	1	118
192.168.200.246	1	58
10.168.20.35	1	6

Total Items 4

3/08/2011 9:44:18 AM Generated By: administrator Page 1 of 1

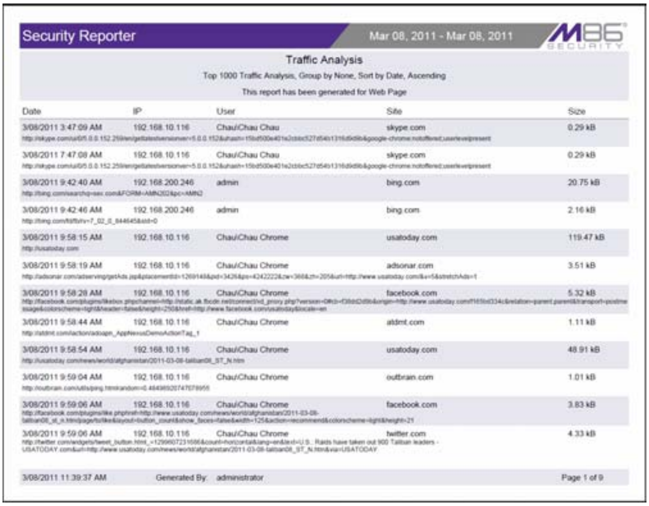
Fig. 6:1-16 Sample PDF for Rule Transactions report, page 1

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

The footer of the report includes the date and time the report was generated (M/D/YYYY, HH:MM 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 sample below:



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/getlatestversion?ver=5.0.0.152&uhash=1[illegible]&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/getlatestversion?ver=5.0.0.152&uhash=1[illegible]&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/fb/r?v=7_02_0_944645&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=[illegible]&origin=http://www.usatoday.com/[illegible]&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/action/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.[illegible]				
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/pages/fb/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

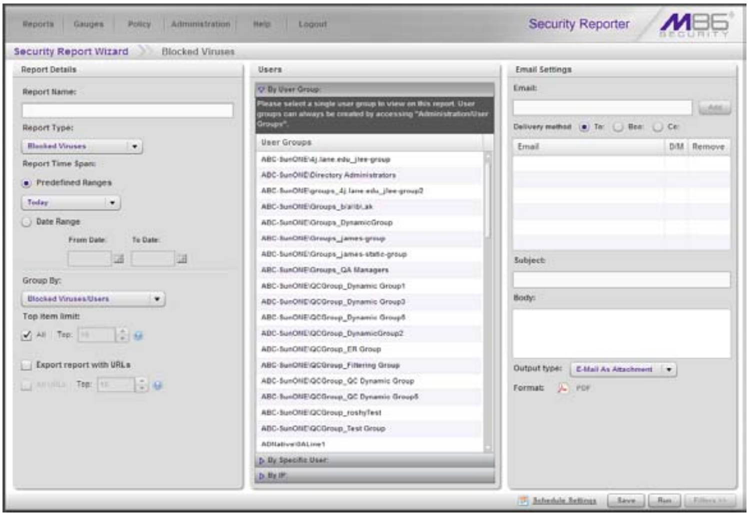
Fig. 6:1-17 Sample PDF for detail Security Report

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

Chapter 2: Security Report Wizard

The Security Report Wizard lets you customize any of the basic four Security Reports, and schedule these reports to run on a regular basis.

In the navigation toolbar, mouse over the Reports menu link, choose Security Reports, and then select **Report Wizard** to open the Security Report Wizard panel:



Report Type: Blocked Viruses

● Predefined Ranges: Today

○ Date Range

Group By: Blocked Viruses/Users

☑ All

☐ Export report with URLs

Please select a single user group to view on this report. User groups can always be created by accessing "Administration/User Groups".

ABC-SunONE\4j.lane.edu_jlee-group
ABC-SunONE\Directory Administrators
ABC-SunONE\groups_4j.lane.edu_jlee-group2
ABC-SunONE\Groups_b\a\b\.ak
ABC-SunONE\Groups_DynamicGroup
ABC-SunONE\Groups_james-group
ABC-SunONE\Groups_james-static-group
ABC-SunONE\Groups_QA Managers
ABC-SunONE\QCGroup_Dynamic Group1
ABC-SunONE\QCGroup_Dynamic Group3
ABC-SunONE\QCGroup_Dynamic Group5
ABC-SunONE\QCGroup_DynamicGroup2
ABC-SunONE\QCGroup_ER Group
ABC-SunONE\QCGroup_Filtering Group
ABC-SunONE\QCGroup_QC Dynamic Group
ABC-SunONE\QCGroup_QC Dynamic Group5
ABC-SunONE\QCGroup_roshyTest
ABC-SunONE\QCGroup_Test Group
ADNative\QALine1

Delivery method ● To: ○ Bcc: ○ Cc:

Output type: E-Mail As Attachment

Format: PDF

Fig. 6:2-1 Security Report Wizard panel

Create a Custom Security Report

Specify Report Details

In the Report Details frame, specify general information for the security report to be generated:

1. Type in the **Report Name**.
2. 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 selecting this default option, make a choice 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 selecting this option, use the calendar icons to set the date range.

4. If necessary, specify the **Group By** report type selection from the available choices in the pull-down menu.

5. Indicate the **Top item limit** to be included in the report; by default “All” is selected. To modify this selection, uncheck this box and specify the **Top** number of items.

6. 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

Select Users

In the Users frame, 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:

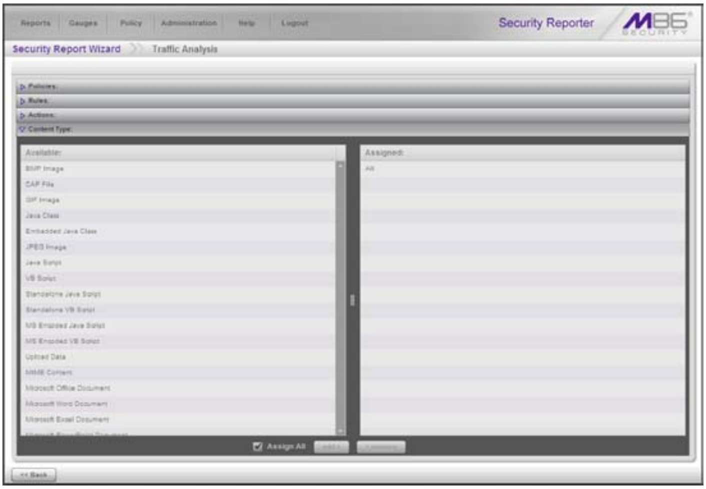


Fig. 6:2-2 Security Report Wizard Filters option

***TIP**: At the bottom left of the panel, click **<< Back** at any time to return to the Security Report Wizard 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.

***TIPS**: Multiple records can be selected by clicking each record while pressing the Ctrl key on your keyboard. Blocks of records can be selected by clicking the first record, and then pressing the Shift key on your keyboard while clicking the last record.*

*To remove the record(s), select the record(s) from the Assigned list box and click **< remove**.*

- 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.

Specify Email Settings

In the Email Settings frame:

1. 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”.

***TIP**: To remove an email address, click the “**X**” in the **Remove** column of the list box.*

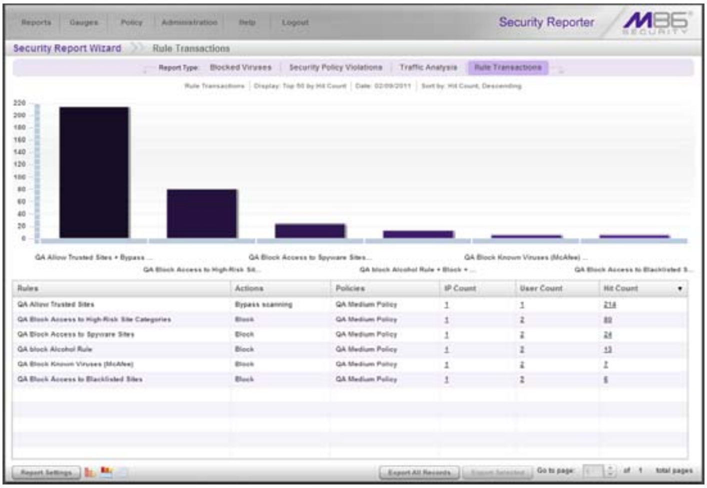
***NOTE**: Follow the above procedures for each email to be added.*

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** to be used for the PDF report file in the email: “E-Mail As Attachment” or “E-Mail As Link”.

Schedule, Run a Report using the Wizard

Once security report settings have been made using the Security Report Wizard, choose one of two reporting options by clicking the button at the bottom right of the panel:

- **Schedule Settings** - Click this button to open the Schedule Settings pop-up window (see Fig. 6:1-14) and follow the procedures in Report Settings Options: Schedule a Security Report to Run from Chapter 1.
- **Run** - Click this button to generate the security report. The finished report view displays in the panel:



Rule Transactions | Display: Top 50 by Hit Count | Date: 02/09/2011 | Sort by: Hit Count, Descending

Rules	Actions	Policies	IP Count	User Count	Hit Count ▼
QA Allow Trusted Sites	Bypass scanning	QA Medium Policy	1	1	214
QA Block Access to High-Risk Site Categories	Block	QA Medium Policy	1	2	80
QA Block Access to Spyware Sites	Block	QA Medium Policy	1	2	24
QA block Alcohol Rule	Block	QA Medium Policy	1	2	13
QA Block Known Viruses (McAfee)	Block	QA Medium Policy	1	2	7
QA Block Access to Blacklisted Sites	Block	QA Medium Policy	1	2	6

Fig. 6:2-3 Generated Security Report view

The report can now be:

- Exported by selecting one of the export options (see Export a Security Report in Chapter 1), and a PDF of the report downloaded to your machine.
- Saved by going to the Report Settings menu and selecting the Save option (see Report Settings Options: Save a Security Report in Chapter 1).

APPENDICES SECTION

Appendix A

Disable Pop-up Blocking Software

An administrator with pop-up blocking software installed on his/her workstation will need to disable pop-up blocking in order to use the System Configuration console.

This appendix provides instructions on how to disable pop-up blocking software for the supported browser types (Internet Explorer, Firefox, Chrome, and Safari) and the following products: Yahoo! Toolbar, Google Toolbar, AdwareSafe, and Windows XP Service Pack 2 (SP2).

Browser Pop-up Blockers

Internet Explorer 7.0 and 8.0

In the Internet Explorer toolbar, navigate to **Tools > Pop-up Blocker**.

If you wish to disable all pop-up blocking, be sure the **Turn Off Pop-up Blocker** selection is enabled.

If you wish to block all pop-ups except those from URLs you choose to whitelist, enable **Turn On Pop-up Blocker** and then navigate to **Pop-up Blocker Settings**, adding the SR's URL in the Allowed sites list box.

Mozilla Firefox 3.6

1. In the Firefox toolbar, navigate to **Tools > Options... > Content** tab.
2. Uncheck the “Block pop-up windows” checkbox, or click **Exceptions...** and then add the SR's URL in the Allowed Sites - Pop-ups window.

Google Chrome 9.0

1. In the Chrome toolbar, navigate to the **‘wrench’ icon > Options > Under the Hood** tab.
2. Click **Content settings... > Pop-ups**.
3. Choose either:
   - **Allow all sites to show pop-ups**

   or

   - **Do not allow any site to show pop-ups (recommended) > Exceptions...**, adding the SR's URL to the Pop-up Exceptions box.

Safari 4.0 and 5.0

In the Safari toolbar, navigate to the Safari menu and deselect “Block Pop-Up Windows” to disable pop-up blocking.

Yahoo! Toolbar Pop-up Blocker

Add the Client to the White List

If the Client was previously blocked by the Yahoo! Toolbar, it can be moved from the black list and added to the white list so that it will always be allowed to pass. To do this:

1. Go to the Yahoo! Toolbar and click the pop-up icon to open the pop-up menu:

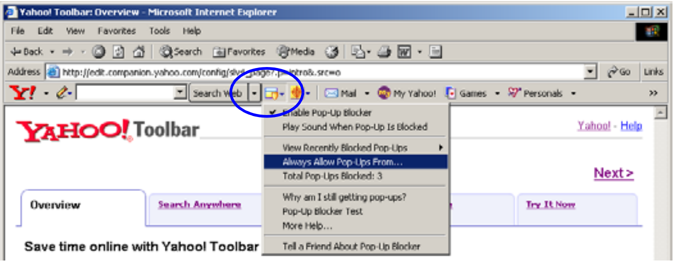
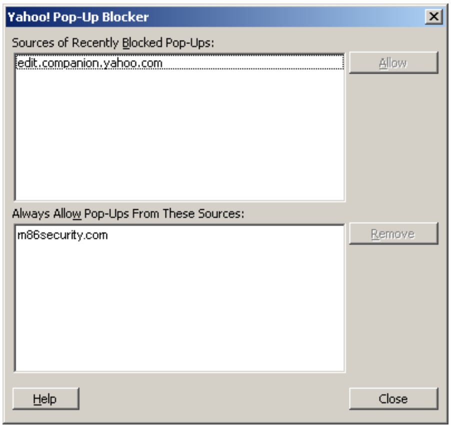

Yahoo! Toolbar: Overview - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://edit.companion.yahoo.com/config/slv_page?.p=intro&.src=o
Go Links
Search Web
Mail My Yahoo! Games Personals
✓ Enable Pop-Up Blocker
Play Sound When Pop-Up Is Blocked
View Recently Blocked Pop-Ups
Always Allow Pop-Ups From...
Total Pop-Ups Blocked: 3
Why am I still getting pop-ups?
Pop-Up Blocker Test
More Help...
Tell a Friend About Pop-Up Blocker
YAHOO! Toolbar
Yahoo! - Help
Next >
Overview
Search Anywhere
Try It Now
Save time online with Yahoo! Toolbar

Fig. A-1 Select menu option Always Allow Pop-Ups From

2. Choose Always Allow Pop-Ups From to open the Yahoo! Pop-Up Blocker dialog box:


Yahoo! Pop-Up Blocker
Sources of Recently Blocked Pop-Ups:
Allow
Always Allow Pop-Ups From These Sources:
Remove
Help
Close

edit.companion.yahoo.com

m86security.com

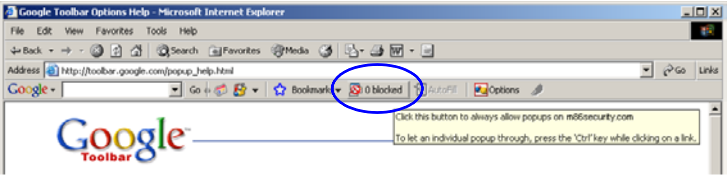
Fig. A-2 Allow pop-ups from source

3. Select the source from the Sources of Recently Blocked Pop-Ups list box to activate the Allow button.
4. Click **Allow** to move the selected source to the Always Allow Pop-Ups From These Sources list box.
5. Click **Close** to save your changes and to close the dialog box.

Google Toolbar Pop-up Blocker

Add the Client to the White List

To add the Client to the white list so that it will always be allowed to pass, go to the Google Toolbar and click the Pop-up blocker button:

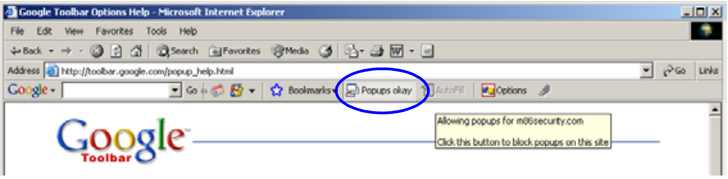

Google Toolbar Options Help - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://toolbar.google.com/popup_help.html
Go Links
Google Go Bookmarks 0 blocked AutoFill Options
Google Toolbar

Click this button to always allow popups on m86security.com

To let an individual popup through, press the 'Ctrl' key while clicking on a link.

Fig. A-3 Pop-up blocker button enabled

Clicking this icon toggles to the Pop-ups okay button, adding the Client to your white list:


Google Toolbar Options Help - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://toolbar.google.com/popup_help.html
Go Links
Google Go Bookmarks Popups okay AutoFill Options
Google Toolbar

Allowing popups for m86security.com

Click this button to block popups on this site

Fig. A-4 Pop-ups okay button enabled

AdwareSafe Pop-up Blocker

Disable Pop-up Blocking

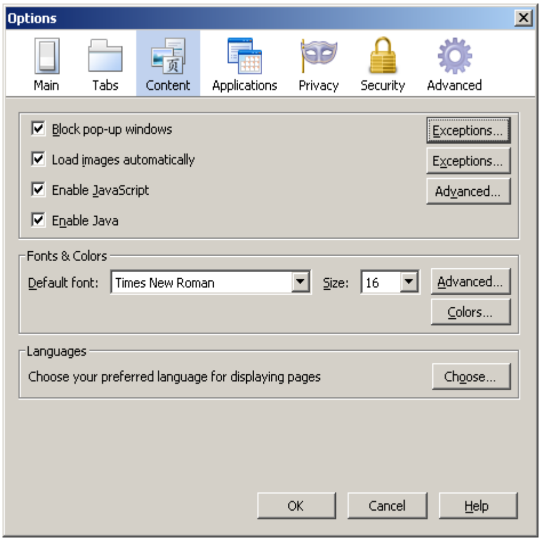
AdwareSafe's SearchSafe toolbar lets you toggle between enabling pop-up blocking (# popups blocked) and disabling pop-up blocking (Popup protection off) by clicking the pop-up icon.

1. In the IE browser, go to the SearchSafe toolbar and click the icon for # popups blocked to toggle to Popup protection off. This action turns off pop-up blocking.
2. After you are finished using the Client, go back to the SearchSafe toolbar and click the icon for Popup protection off to toggle back to # popups blocked. This action turns on pop-up blocking again.

Mozilla Firefox Pop-up Blocker

Add the Client to the White List

1. From the Firefox browser, go to the toolbar and select **Tools > Options** to open the Options dialog box.
2. Click the Content tab at the top of this box to open the Content section:



☑ Block pop-up windows

☑ Load images automatically

☑ Enable JavaScript

☑ Enable Java

Fonts & Colors

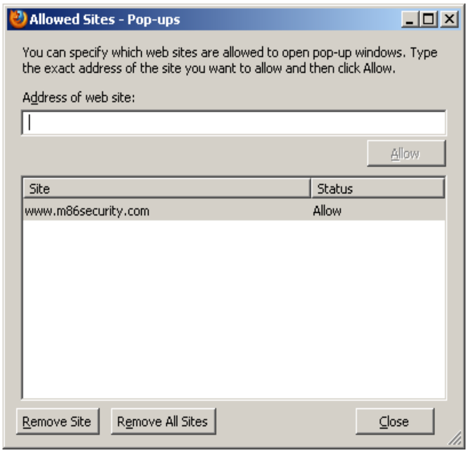
Default font: Times New Roman Size: 16

Languages

Choose your preferred language for displaying pages

Fig. A-5 Mozilla Firefox Pop-up Windows Options

3. With the “Block pop-up windows” checkbox checked, click the **Exceptions...** button at right to open the Allowed Sites - Pop-ups box:



Allowed Sites - Pop-ups

You can specify which web sites are allowed to open pop-up windows. Type the exact address of the site you want to allow and then click Allow.

Address of web site:

Site	Status
www.m86security.com	Allow

Fig. A-6 Mozilla Firefox Pop-up Window Exceptions

4. Enter the **Address of the web site** to let the client pass.
5. Click **Allow** to add the URL to the list box section below.
6. Click **Close** to close the Allowed Sites - Pop-ups box.
7. Click OK to close the Options dialog box.

Windows XP SP2 Pop-up Blocker

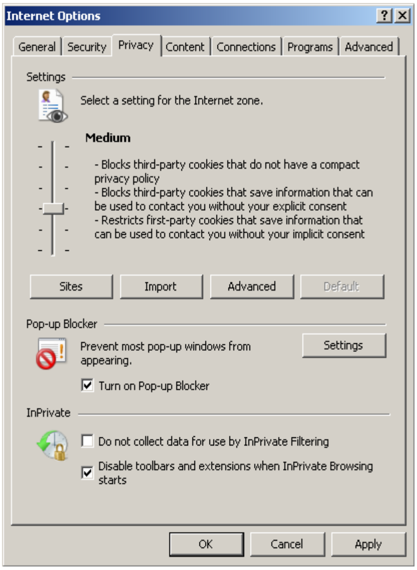
This sub-section provides information on setting up pop-up blocking and disabling pop-up blocking in Windows XP SP2.

Set up Pop-up Blocking

There are two ways to enable the pop-up blocking feature in the IE browser.

Use the Internet Options dialog box

1. From the IE browser, go to the toolbar and select **Tools > Internet Options** to open the Internet Options dialog box.
2. Click the Privacy tab:



Settings

Select a setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that save information that can be used to contact you without your explicit consent
- Restricts first-party cookies that save information that can be used to contact you without your implicit consent

Pop-up Blocker

Prevent most pop-up windows from appearing.

☑ Turn on Pop-up Blocker

InPrivate

☐ Do not collect data for use by InPrivate Filtering

☑ Disable toolbars and extensions when InPrivate Browsing starts

Fig. A-7 Enable pop-up blocking

3. In the Pop-up Blocker frame, check “Turn on Pop-up Blocker”.

4. Click **Apply** and then click **OK** to close the dialog box.

Use the IE Toolbar

In the IE browser, go to the toolbar and select **Tools > Pop-up Blocker > Turn On Pop-up Blocker**:

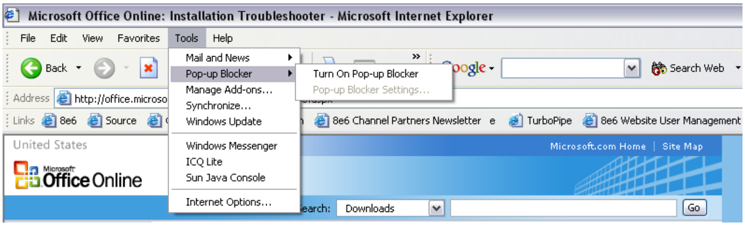

Microsoft Office Online: Installation Troubleshooter - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address http://office.microso
Links 8e6 Source
Mail and News
Pop-up Blocker
Manage Add-ons...
Synchronize...
Windows Update
Windows Messenger
ICQ Lite
Sun Java Console
Internet Options...
Turn On Pop-up Blocker
Pop-up Blocker Settings...
Search Web
8e6 Channel Partners Newsletter
TurboPipe
8e6 Website User Management
United States
Microsoft Office Online
Microsoft.com Home | Site Map
earch: Downloads
Go

Fig. A-8 Toolbar setup

When you click Turn On Pop-up Blocker, this menu selection changes to Turn Off Pop-up Blocker and activates the Pop-up Blocker Settings menu item.

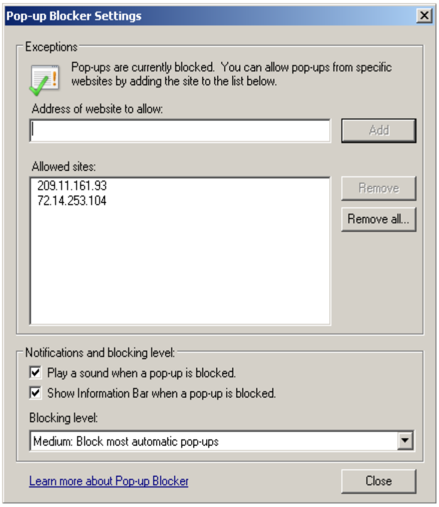
You can toggle between the On and Off settings to enable or disable pop-up blocking.

Add the Client to the White List

There are two ways to disable pop-up blocking for the Client and to add the Client to your white list.

Use the IE Toolbar

1. With pop-up blocking enabled, go to the toolbar and select **Tools > Pop-up Blocker > Pop-up Blocker Settings** to open the Pop-up Blocker Settings dialog box:



Pop-up Blocker Settings

Exceptions

Pop-ups are currently blocked. You can allow pop-ups from specific websites by adding the site to the list below.

Address of website to allow:

Allowed sites:
209.11.161.93
72.14.253.104

Notifications and blocking level:

☑ Play a sound when a pop-up is blocked.

☑ Show Information Bar when a pop-up is blocked.

Blocking level:
Medium: Block most automatic pop-ups

Fig. A-9 Pop-up Blocker Settings

2. Enter the **Address of website to allow**, and click **Add** to include this address in the Allowed sites list box. Click **Close** to close the dialog box. The Client has now been added to your white list.

Use the Information Bar

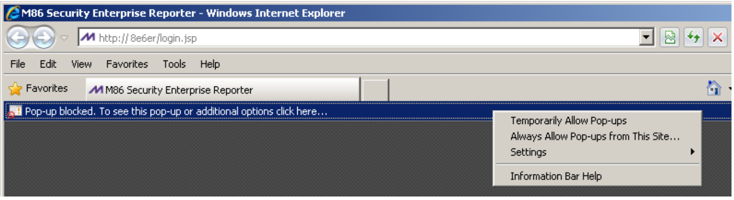
With pop-up blocking enabled, the Information Bar can be set up and used for viewing information about blocked pop-ups or allowing pop-ups from a specified site.

Set up the Information Bar

1. Go to the toolbar and select **Tools > Pop-up Blocker > Pop-up Blocker Settings** to open the Pop-up Blocker Settings dialog box (see Fig. A-9).
2. In the Notifications and Filter Level frame, click the checkbox for “Show Information Bar when a pop-up is blocked.”
3. Click **Close** to close the dialog box.

Access the Client

1. Click the Information Bar for settings options:



M86 Security Enterprise Reporter - Windows Internet Explorer

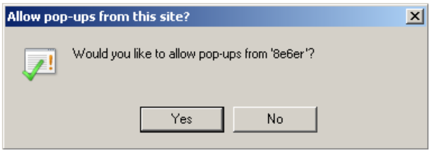
http:// 8e6er/login.jsp

Pop-up blocked. To see this pop-up or additional options click here...

File
Edit
View
Favorites
Tools
Help
Favorites
M86 Security Enterprise Reporter
Temporarily Allow Pop-ups
Always Allow Pop-ups from This Site...
Settings
Information Bar Help

Fig. A-10 Information Bar menu options

2. Select Always Allow Pop-ups from This Site—this action opens the Allow pop-ups from this site? dialog box:



Allow pop-ups from this site?

Would you like to allow pop-ups from '8e6er'?

Fig. A-11 Allow pop-ups dialog box

3. Click **Yes** to add the Client to your white list and to close the dialog box.

***NOTE**: To view your white list, go to the Pop-up Blocker Settings dialog box (see Fig. A-9) and see the entries in the Allowed sites list box.*

Appendix B

RAID and Hardware Maintenance

This appendix is divided into three parts: Hardware Components, Server Interface, and Troubleshooting—in the event of a failure in one of the drives, power supplies, or fans.

NOTE*: As part of the ongoing maintenance procedure for your RAID server, M86 recommends that you always have a spare drive and spare power supply on hand.*

Contact M86 Technical Support for replacement hard drives and power supplies.

Part 1: Hardware Components

The chassis of each model consists of the following components:

300 Model	500 Models	700, 730 Models
2 hard drives	4 hard drives	4 hard drives
1 power supply	1 power supply	2 power supplies
1 cooling fan	3 cooling fans	4 cooling fans

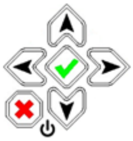
NOTES*: If troubleshooting models 705 and 735, please visit IBM's Systems Support Web site at* ***http://www.ibm.com/systems/support/*** *. These models use IBM System x3620 M3 hardware, so your query should specify* ***IBM System x > System x3620 M3*** *.*

IBM System x3620 M3 Type 7376 Installation and User's Guide contains instructions on viewing and using LED indicators and buttons on SR models 705 and 735. As of September 2010, this document was made available at ***http://www-947.ibm.com/support/entry/portal/docdisplay?brand=5000008&lndocid=MIGR-5084233***

Part 2: Server Interface

Front Control Panel on a 300 model

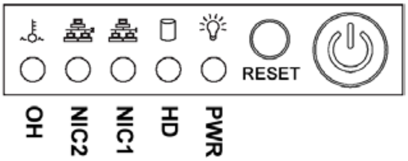
The keypad on the front of the server is used for performing basic server functions.



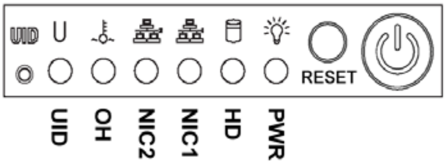
- **Boot up** - Depress and hold the check-mark key for 3 seconds.
- **Reboot** - Depress and hold the check-mark key for 10 seconds.
- **Shut down** - Depress and hold the ‘X’ key for 10 seconds.

Front control panels on 500, 700, and 730 models

Control panel buttons, icons, and LED indicators display on the right side of the 500, 700, and 730 model front panel. The buttons let you perform a function on the unit, while an LED indicator corresponding to an icon alerts you to the status of that feature on the unit.



500 chassis front panel



700 chassis front panel

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

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

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

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

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

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

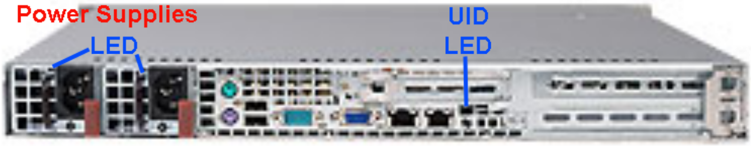
Power (icon) – The LED is unlit when the server is turned off. A steady green LED indicates power is being supplied to the unit’s power supplies. (See also Rear of chassis.) (See Power supply failure in the Troubleshooting sub-section for information on detecting a power supply failure and resolving this problem.)

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

Rear panel on 700 and 730 models

Power Supplies (LED indicators) – The power supplies are located at the right on the rear of the chassis. An LED indicator is located above each of the power plugs. (See Power supply failure in the Troubleshooting sub-section for information on detecting a power supply failure and resolving this problem.)

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



Part 3: Troubleshooting

The text in this section explains how the server alerts the administrator to a failed component, and what to do in the event of a failure.

Hard drive failure

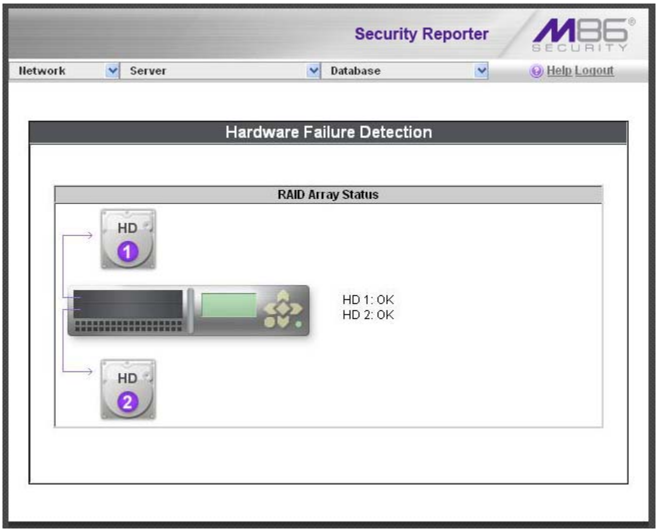
Step 1: Review the notification email

If a hard drive fails, a notification email is sent to the administrator of the server. This email identifies the failed hard drive by its number (HD ‘X’). Upon receiving this alert, the administrator should verify the status of the drives by first going to the Hardware Failure Detection screen in the System Configuration console.

⚠ ***WARNING**: Do not attempt to remove any of the drives from the unit at this time. Verification of the failed drive should first be made in the System Configuration console before proceeding, as data on the server will be lost in the event that the wrong drive is removed from the unit.*

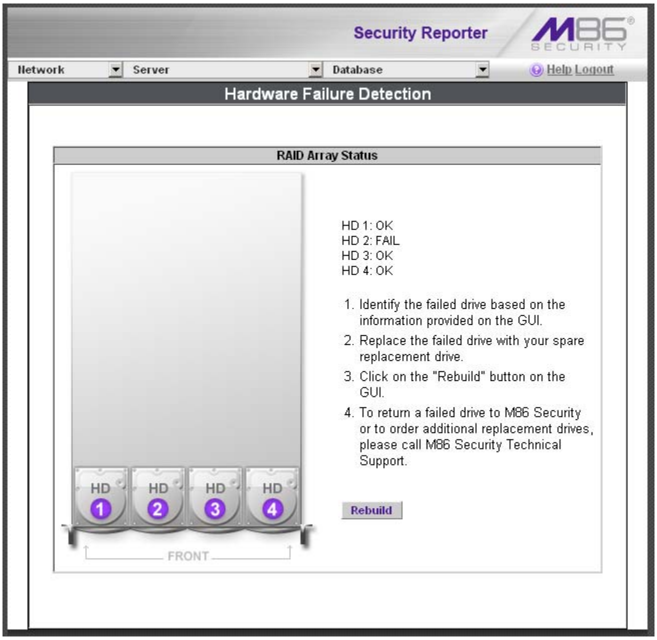
Step 2: Verify the failed drive in the Admin console

The Hardware Failure Detection screen in the System Configuration console is accessible via the **Server > Hardware Failure Detection** menu selection:



HD 1: OK
HD 2: OK

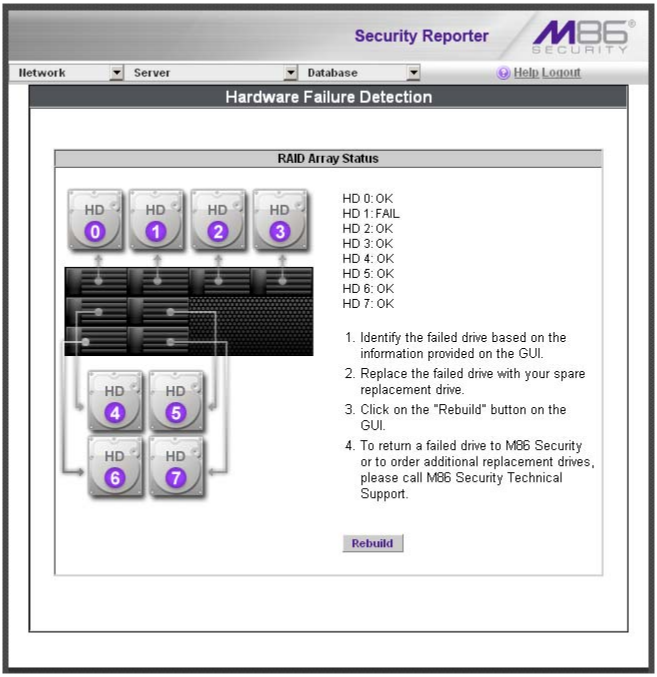
Fig. B1 Hardware Failure Detection screen, 300 model



HD 1: OK
HD 2: FAIL
HD 3: OK
HD 4: OK

1. Identify the failed drive based on the information provided on the GUI.
2. Replace the failed drive with your spare replacement drive.
3. Click on the "Rebuild" button on the GUI.
4. To return a failed drive to M86 Security or to order additional replacement drives, please call M86 Security Technical Support.

Fig. B-2 Hardware Failure Detection window



Hardware Failure Detection

RAID Array Status

HD 0: OK
HD 1: FAIL
HD 2: OK
HD 3: OK
HD 4: OK
HD 5: OK
HD 6: OK
HD 7: OK

1. Identify the failed drive based on the information provided on the GUI.
2. Replace the failed drive with your spare replacement drive.
3. Click on the "Rebuild" button on the GUI.
4. To return a failed drive to M86 Security or to order additional replacement drives, please call M86 Security Technical Support.

Fig. B-3 Hardware Failure Detection screen, 705 or 735 IBM model

The Hardware Failure Detection window displays the current RAID Array Status for all the hard drives (HD) at the right side of the window.

Normally, when both hard drives are functioning without failure, the text “OK” displays to the right of the hard drive number, and no other text displays in the window.

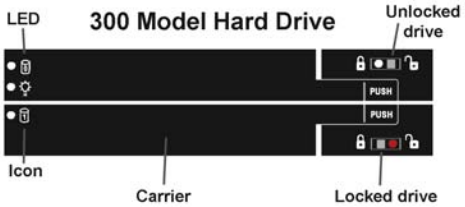
However, if a hard drive has failed, the message “FAIL” displays to the right of the hard drive number.

Before taking any action in this window, proceed to Step 3.

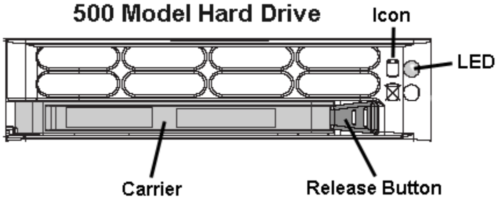
NOTE*: For SR models 705 and 735, please consult IBM System x3620 M3 Type 7376 Installation and User's Guide for hard drive replacement instructions.*

Step 3: Replace the failed hard drive

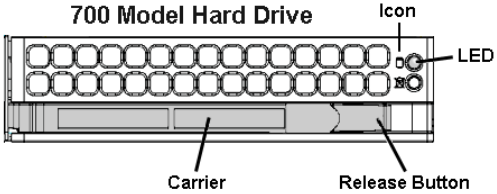
After verifying the failed hard drive in the Administrator console, go to the server to replace the drive.



300 model hard drive carrier



500 model hard drive carrier



700 and 730 model hard drive carrier

On a 300 model, be sure the carrier is unlocked, then press the section on the carrier handle labeled PUSH to release the carrier handle. On a 500, 700, or 730 model, press the red release button to release the carrier handle.

Extend the carrier handle fully by pulling it out towards you. Pull out the failed drive and replace it with your spare replacement drive. Push the drive into its slot, and press the carrier back in place.

NOTE*: Contact Technical Support if you have any questions about replacing a failed hard drive.*

Step 4: Rebuild the hard drive

Once the failed hard drive has been replaced, return to the Hardware Failure Detection screen in the System Configuration console, and click **Rebuild** to proceed with the rebuild process.

***WARNING**: When the RAID array reconstruction process begins, the System Configuration console will close and the hard drive will become inaccessible.*

Step 5: Contact Technical Support

Contact Technical Support to order a new replacement hard drive and for instructions on returning your failed hard drive to M86.

Power supply failure

Step 1: Verify the power supply has failed

The administrator of the server is alerted to a power supply failure on the 500, 700, and 730 chassis by an audible alarm and an amber power supply LED—or an unlit LED—on the front of the chassis.

***NOTES**: A steady amber power supply LED on a 500, 700, or 730 chassis also may indicate a disconnected or loose power supply cord. Verify that the power supply cord is plugged in completely before removing a power supply.*

For SR models 705 and 735, please consult IBM System x3620 M3 Type 7376 Installation and User's Guide for power supply replacement instructions.

Step 2: Contact Technical Support

Contact Technical Support for assistance with installing the replacement power supply, or to order a new replacement power supply, or for instructions on returning your failed power supply to M86.

If you have a 700 or 730 model and wish to replace this hot swappable power supply unit yourself, proceed to Step 3.

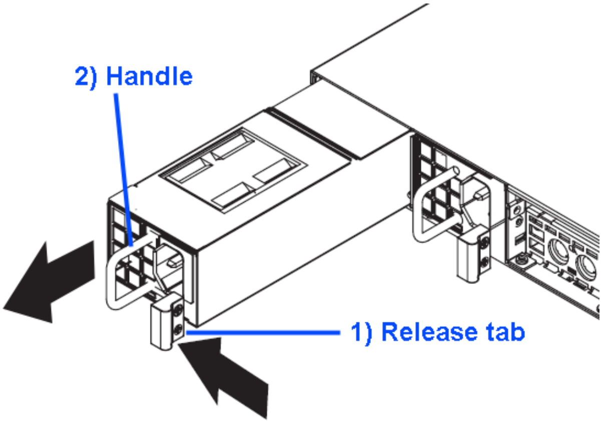
⚠ ***WARNING****: Be sure the correct failed power supply has been identified. Removing the wrong power supply will cause the system to crash.*

Step 3: Unplug the power cord

To prevent electrical shock to yourself and damage to the unit, unplug the power cord from the failed 700 series power supply module. Proceed to Step 4.

Step 4: Replace a failed hot swap power supply

Remove the failed 700 or 730 power supply by locating the red release tab and pushing it to the left (1), then pulling the curved metal handle on the power supply module towards you (2).



700 or 730 model power supply module

Note that an audible alarm sounds and the LED is unlit when the power supply module is disengaged. Replace the failed power supply with your spare replacement power supply module. The alarm will turn off and the LED will be a steady green when the replacement power supply module is securely locked in place.

Fan failure

Identify a fan failure

A flashing red LED on a 500, 700, or 730 model indicates a fan failure. If this displays on your unit, contact Technical Support for an RMA (Return Merchandise Authorization) number and for instructions on returning the unit to M86.

A steady red LED (on and not flashing) on a 500, 700, or 730 model indicates an overheating condition, which may be caused by cables obstructing the airflow in the system or the ambient room temperature being too warm. Check the routing of the cables and make sure all fans are present and operating normally. The LED will remain steady as long as the overheating condition exists.

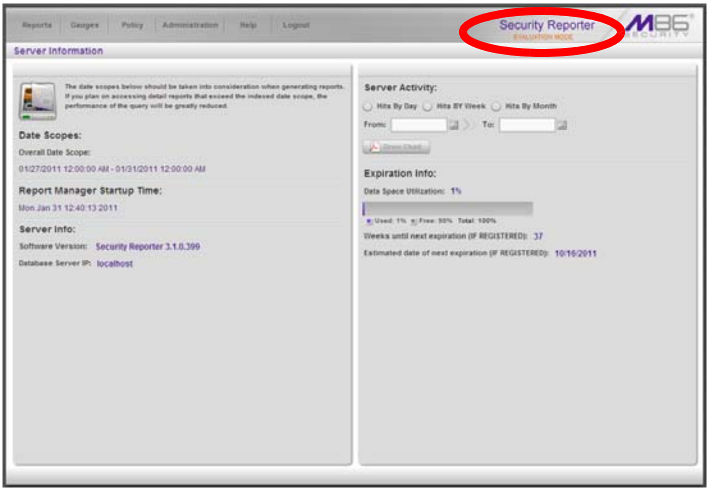
Appendix C

Evaluation Mode

By default, the SR is set to evaluation mode. This appendix explains how to use the SR in evaluation mode, and how to register the SR to function in registered mode.

Report Manager Banner

In evaluation mode, the Report Manager banner displays ‘EVALUATION MODE’ beneath the Security Reporter name/link:



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

Date Scopes:

Overall Date Scope:

01/27/2011 12:00:00 AM - 01/31/2011 12:00:00 AM

Report Manager Startup Time:

Mon Jan 31 12:40:13 2011

Server Info:

Software Version: Security Reporter 3.1.0.399

Database Server IP: localhost

Server Activity:

○ Hits By Day ○ Hits BY Week ○ Hits By Month

From: To:

Expiration Info:

Data Space Utilization: 1%

Used: 1% Free: 99% Total: 100%

Weeks until next expiration (IF REGISTERED): 37

Estimated date of next expiration (IF REGISTERED): 10/16/2011

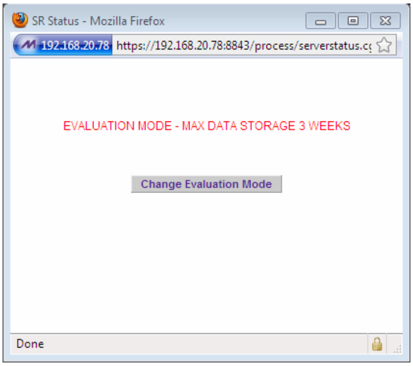
Fig. C-1 Server Information panel in evaluation mode

Mouse 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 Fig. C-2) as described in the next sub-section.

***NOTE**: The System Configuration administrator console is only available to users with permissions set up to access it.*

System Configuration Console

For an SR unit currently in evaluation mode, whenever the **Server > Server Status** screen is accessed, the SR Status pop-up box opens:



SR Status - Mozilla Firefox

192.168.20.78 https://192.168.20.78:8843/process/serverstatus.cg

EVALUATION MODE - MAX DATA STORAGE 3 WEEKS

Change Evaluation Mode

Done

Fig. C-2 SR Status pop-up box

The SR will store data for the period specified in the pop-up box: “EVALUATION MODE - MAX DATA STORAGE ‘X’ WEEKS”—in which ‘X’ represents the maximum number of weeks in the SR’s data storage scope.

You have the option to either use the SR in the evaluation mode, or change the evaluation mode in one of two ways—by extending the evaluation period, or by registering the SR so that it can be used in the registered mode.

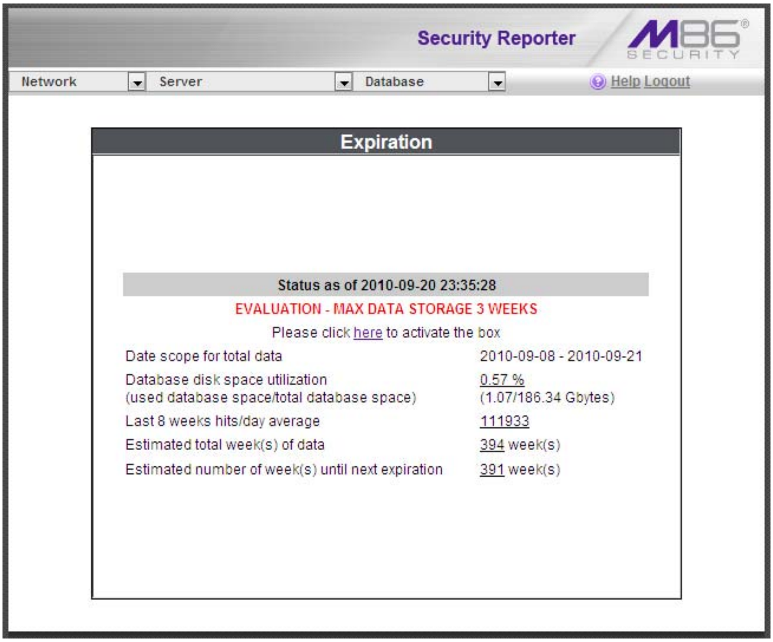
***NOTE**: The message: “EVALUATION MODE - MAX DATA STORAGE ‘X’ WEEKS” also displays at the top of the Expiration screen in the System Configuration console. Refer to the Expiration screen sub-section in Chapter 2 of the System Configuration Section for more information about data storage and expiration.*

Use the Server in the Evaluation Mode

To use the unit in evaluation mode, click the "X" in the upper right corner of the SR Status pop-up box to close it.

Expiration screen

When navigating to **Database > Expiration**, the Expiration screen displays additional information in evaluation mode:



Status as of 2010-09-20 23:35:28

EVALUATION - MAX DATA STORAGE 3 WEEKS

Please click here to activate the box

Date scope for total data	2010-09-08 - 2010-09-21
Database disk space utilization (used database space/total database space)	0.57 % (1.07/186.34 Gbytes)
Last 8 weeks hits/day average	111933
Estimated total week(s) of data	394 week(s)
Estimated number of week(s) until next expiration	391 week(s)

Fig. C-3 Expiration screen

The following message displays 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). This message is followed by a line stating: “Please click here to activate the box.”

Clicking the link “here” is used for activating the SR to function in registered mode.

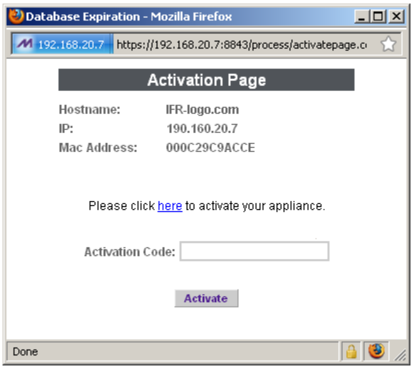
***NOTE**: The Status date and time and EVALUATION message do not display on a newly installed server, or a server that has just been reset to factory default settings. (See Reset to Factory Defaults panel in Chapter 2 of the Report Manager Administration Section for information about resetting the server to factory default settings.)*

Change the Evaluation Mode

After the designated evaluation period has expired, you may extend your evaluation period, or register the unit and use it in the registered mode. There are two ways to change the evaluation mode from the System Configuration console:

- in the SR Status pop-up box (see Fig. C-1), click **Change Evaluation Mode**
- in the Evaluation screen, click the link (“here”) in the message at the top of the screen: “Please click here to activate the box”.

By clicking the button or link, the Activation Page pop-up box opens:



Database Expiration - Mozilla Firefox
192.168.20.7
https://192.168.20.7:8843/process/activatepage.c
Activation Page

Hostname: IFR-logo.com
IP: 190.160.20.7
Mac Address: 000C29C9ACCE

Please click here to activate your appliance.

Activation Code:

Fig. C-4 Activation Page pop-up box

Activation Page

1. In the Activation Page pop-up box, the **Hostname** of the Server, **IP** address, and **Mac Address** (Media Access Control address) display.
2. In the message “Please click here to activate your appliance.”, click the link ‘**here**’ to open the Product Activation page at the M86 Security Web site.
3. In this Web page:

   a. Enter your following information: Contact Details, Company Information, and Security Reporter Information.

   b. Choose the Activation Type: "Evaluation Extension" or "Full Activation."
4. Click **Send Information**. After M86 obtains your information, a technical support representative will issue you an activation code.
5. Return to the Activation Page (see Fig. C-4) and enter the activation code in the **Activation Code** field.
6. Click **Activate** to display the confirmation message in the Activation Page pop-up box:
   - If extending the evaluation period for the unit, the following message displays: “It is now in evaluation mode (‘X’ weeks)!” in which ‘X’ represents the number of weeks in the new evaluation period.
   - If registering the unit, the following message displays: “Your box has been activated!”
7. Click the ‘X’ in the upper right corner to close the Activation Page pop-up box.

Appendix D

System Tray Alerts: Setup, Usage

This appendix explains how to set up and use the feature for System Tray alerts. An SR Alert is triggered in an administrator's System Tray if an end user's Internet usage has reached the upper threshold established for a gauge set up by that administrator.

This feature is only available to administrators using an LDAP username, account, and domain, and is not available if using IP groups authentication.

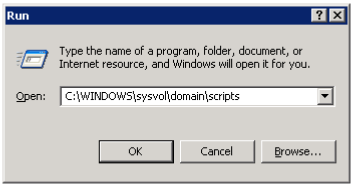
NOTE*: In order to use this feature, the LDAP Username and Domain set up in the administrator's profile account (see Admin Profiles panel from Chapter 1 of the Report Manager Administrator Section) must be the same one he/she uses when logging into his/her workstation.*

LDAP server configuration

Create the System Tray logon script

Before administrators can use the System Tray Alert feature, an administrator with permissions on the LDAP server must first create a logon script on the LDAP server for authenticating administrators.

1. From the taskbar of the LDAP server, go to: **Start > Run** to open the Run dialog box:



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: C:\WINDOWS\sysvol\domain\scripts

Fig. D-1 Run dialog box

2. In the Run dialog box, type in the path to the scripts folder: **C:\WINDOWS\sysvol\domain\scripts**.

3. Click **OK** to open the scripts folder:

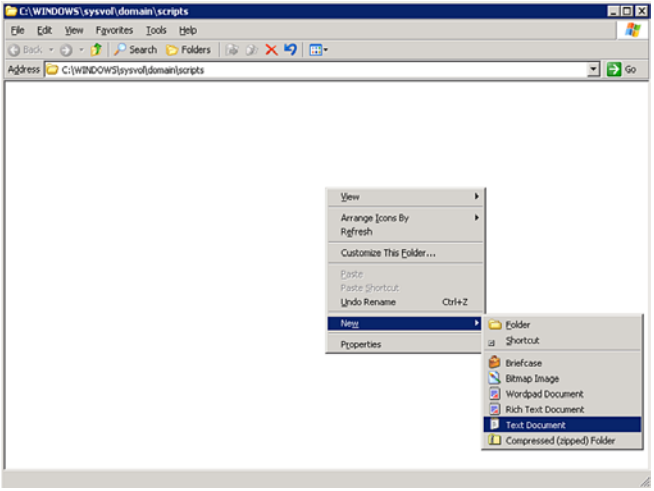
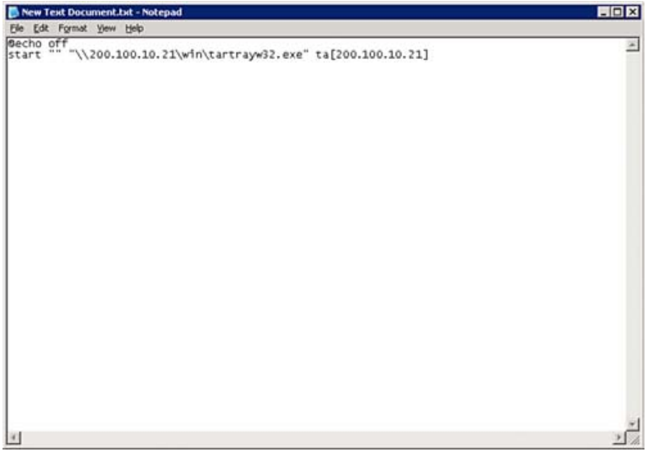


Fig. D-2 C:\WINDOWS\sysvol\domain\scripts window

4. Right-click in this Windows folder to open the pop-up menu.

5. Select **New > Text Document** to launch a New Text Document:



```
@echo off
start "" "\\200.100.10.21\win\tartrayw32.exe" ta[200.100.10.21]
```

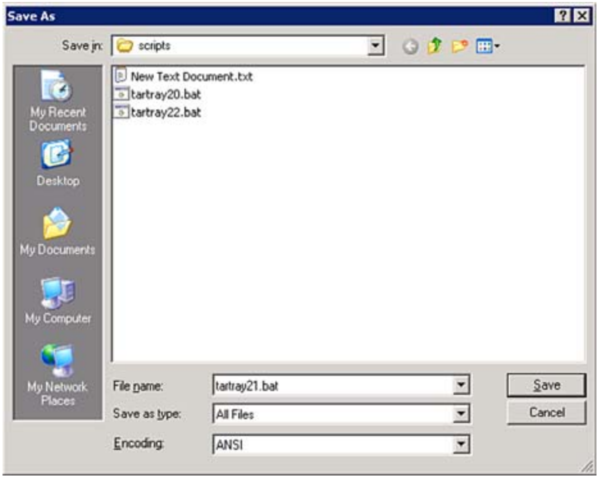
Fig. D-3 New Text Document

6. Type the following text in the blank document file:

   @echo off
   start “” “\\X.X.X.X\win\tartrayw32.exe” ta[X.X.X.X]

   in which “X.X.X.X” represents the IP address of the SR server, and “\win\tartrayw32.exe” refers to the location of the SR Tray Alert executable file on the SR server.

7. Go to: **File > Save As** to open the Save As window:



Save in: scripts

New Text Document.txt
tartray20.bat
tartray22.bat

File name: tartray21.bat
Save as type: All Files
Encoding: ANSI

Fig. D-4 Save As dialog box

8. In the **File name** field, type in the name for the file using the “filename.bat” format. For example: ***tartray21.bat***.

NOTE*: Be sure that the Save as type field has “All Files” selected.*

9. Click **Save** to save your file and to close the window.

Assign System Tray logon script to administrators

With the ".bat" file created, the administrator with permissions on the LDAP server can now begin to assign the System Tray logon script to as many administrators as needed.

1. From the taskbar of the LDAP server, go to: **Start > Programs > Administrative Tools > Active Directory Users and Computers** to open the Active Directory Users and Computers folder:

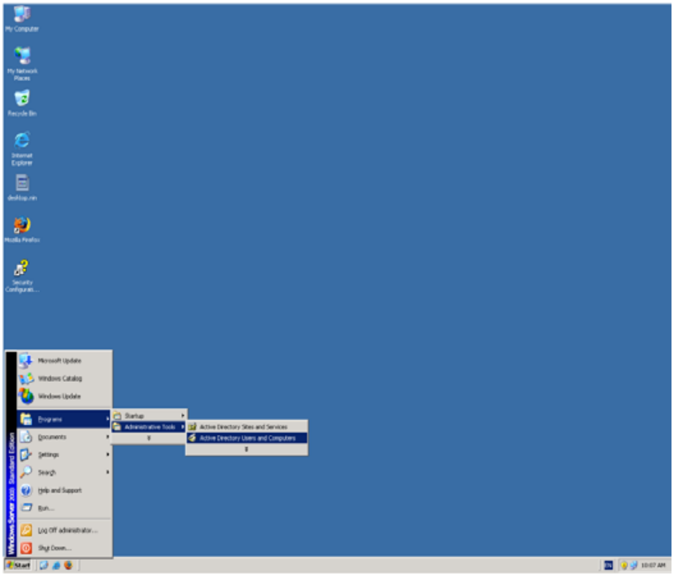
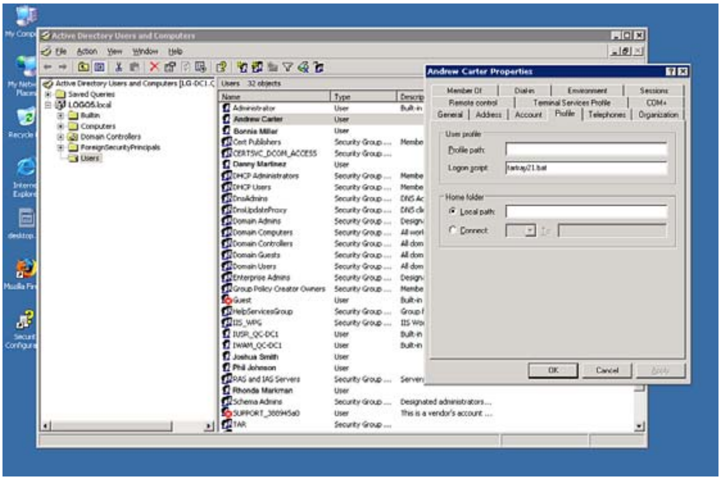


Fig. D-5 Programs > Administrative Tools > Active Directory Users

2. In the Active Directory Users and Computers folder, double-click the administrator's Name in the Users list to open the Properties dialog box for his/her profile:



Active Directory Users and Computers
File
Action
View
Window
Help
Active Directory Users and Computers [LG-DC1.C
Saved Queries
LOGOS.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users
Users 32 objects

Name	Type	Descrip
Administrator	User	Built-in
Andrew Carter	User	
Bonnie Miller	User	
Cert Publishers	Security Group ...	Membe
CERTSVC_DCOM_ACCESS	Security Group ...	
Danny Martinez	User	
DHCP Administrators	Security Group ...	Membe
DHCP Users	Security Group ...	Membe
DnsAdmins	Security Group ...	DNS Ac
DnsUpdateProxy	Security Group ...	DNS cli
Domain Admins	Security Group ...	Design
Domain Computers	Security Group ...	All work
Domain Controllers	Security Group ...	All dom
Domain Guests	Security Group ...	All dom
Domain Users	Security Group ...	All dom
Enterprise Admins	Security Group ...	Design
Group Policy Creator Owners	Security Group ...	Membe
Guest	User	Built-in
HelpServicesGroup	Security Group ...	Group f
IIS_WPG	Security Group ...	IIS Wo
IUSR_QC-DC1	User	Built-in
IWAM_QC-DC1	User	Built-in
Joshua Smith	User	
Phil Johnson	User	
RAS and IAS Servers	Security Group ...	Servers
Rhonda Markman	User	
Schema Admins	Security Group ...	Designated administrators...
SUPPORT_388945a0	User	This is a vendor's account ...
TAR	Security Group ...	

Profile path:

Logon script: tartray21.bat

● Local path:

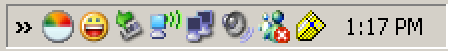
○ Connect:

Fig. D-6 Properties dialog box, Active Directory Users folder

3. In the Properties dialog box, click the Profile tab to display its contents.
4. In the **Login script** field, type in the “.bat” filename. For example: ***tartray21.bat***.
5. Click **Apply** to save your entry.
6. Click **OK** to close the dialog box.
7. Click the “X” in the upper right corner of the folder to close the window.

Administrator usage of System Tray

Once the System Tray logon script has been added to the administrator's profile, when the administrator logs on his/her workstation, the System Tray Alert icon (pictured to the far left in the image below) automatically loads in his/her System Tray:



***NOTE**: The System Tray Alert icon will not load in the System Tray if the SR server is not actively running.*

Use the System Tray Alert icon's menu

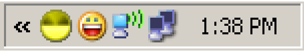
When right-clicking the System Tray Alert icon, the following pop-up menu items display:

- SR Admin Interface - clicking this menu selection launches a browser window containing the SR user interface's login window.
- Reconnect - clicking this menu selection re-establishes the System Tray Alert icon's connection to the SR server, resetting the status of the System Tray Alert icon to the standard setting.
- Exit - clicking this menu selection removes the System Tray Alert icon from the System Tray.

Status of the System Tray Alert icon

If there are no alerts for any gauges set up by the administrator, the following message displays when mousing over the standard System Tray Alert icon: "Connected. No Alerts."

However, if an alert is triggered, the System Tray Alert icon changes in appearance from the standard gauge to a yellow gauge (pictured to the far left in the image below):

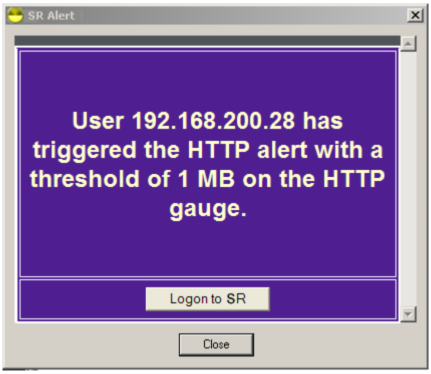


The following message appears briefly above the yellow gauge: "New M86 SR Alert!" The following message displays whenever mousing over this icon: "New M86 SR Alert".

If more than one alert is triggered for the administrator, the message reads: "New M86 SR Alert! (X Total)", in which "X" represents the total number of new alerts. The following message displays whenever mousing over this icon: "X New M86 SR Alerts", in which "X" represents the total number of new alerts.

View System Tray alert messages

1. Double-click the SR Tray Alert notification icon to open the SR Alert box:



User 192.168.200.28 has triggered the HTTP alert with a threshold of 1 MB on the HTTP gauge.

Fig. D-7 SR Alert

This box contains the following message: “User (username/IP address) has triggered the (Alert Name) alert with a threshold of X (in which “X” represents the alert threshold) on the (URL dashboard gauge name) gauge.”

The Logon to SR button displays beneath this message, followed by the Close button.

If more than one alert was triggered, the alert box includes the following message and button to the right of the Close button: “X more alerts” (in which “X” represents the number of additional alerts), and the Next >> button.

2. Click **Logon to SR** to launch the SR login window (see Fig. 1:1-1).

   If there are additional alerts, click **Next >>** to view the next SR Alert. Each time the Next >> button is clicked, the number of remaining alerts to be viewed decreases by one. The Next >> button no longer displays after the last alert is viewed.

3. Click **Close** to close the SR Alert box.

Appendix E

Glossary

This glossary includes definitions for terminology used in this user guide.

base group - A user group consisting of end users whose network activities are monitored by the designated group administrator(s). Only the creator of the base group can modify the base group, delegate the base group to another group administrator, or delete the base group.

canned report - A pre-processed report that includes statistics of end user Internet/network traffic prior to the current day.

custom category - A unique library category on the Web Filter that includes URLs, URL keywords, and/or search engine keywords to be blocked. On the SR, global administrators can create and manage custom library categories and sync them to the source Web Filter.

detail drill down report - One of two types of basic reports—the other report type being a “summary drill down report”—that provides information on objects or pages an end user viewed within the specified time period.

FTP - File Transfer Protocol is used for transferring files from one computer to another on the Internet or an intranet.

global administrator - An authorized administrator of the network who maintains all aspects of the SR. The global administrator configures the SR, sets up user groups, administrator groups and group administrators, and performs routine maintenance on the server.

group administrator - An authorized administrator of the SR who maintains user group, administrator groups, group administrator profiles, and gauges.

group by report type - A report that includes two or more sets of report type criteria, such as User/Sites or Category/ IPs or Category/Site/Users.

hit count - the number of pages and/or objects end users access as the result of entering URLs in a browser window.

HTTP - Hyper Text Transfer Protocol is used for transferring files via the World Wide Web or an intranet.

instant messaging - IM involves direct connections between workstations either locally or across the Internet.

library category - A list of URLs, URL keywords, and search engine keywords set up to be blocked.

LDAP - One of two authentication method protocols that can be used with the SR. Lightweight Directory Access Protocol (LDAP) is a directory service protocol based on entries (Distinguished Names). The other authentication method that can be used with the SR is IP groups.

object count - The number of objects end users access on a Web page, including images, graphics, multimedia items, and text items. The number of objects on a page is generally higher than the number of pages a user visits.

page count - The number of Web pages end users access, which can exceed the number of objects per page in categories that use a lot of pop-up ads (porn, gambling, and other related sites). A user may visit only one site, but visit 20 pages on that site if the page has pop-up ads or banner ads that link to other pages.

peer-to-peer - P2P involves communication between computing devices—desktops, servers, and other smart devices—that are linked directly to each other.

protocol - A type of format for transmitting data between two devices. LDAP is a type of authentication method protocol.

search engine - A program that searches Web pages for specified keywords and returns a list of the pages or services where the keywords were found.

SMTP - Simple Mail Transfer Protocol is used for transferring email messages between servers.

summary drill down report - One of two types of basic reports—the other report type being a “detail drill down report”—that provides a synopsis of end user Internet activity for the specified time period.

synchronization - A process by which two or more machines run in parallel to each other. User filtering profiles and library configurations on the source Web Filter can be set up to be synchronized between the source Web Filter and the SR.

TCP - An abbreviation for Transmission Control Protocol, one of the core protocols of the Internet protocol suite. Using TCP, applications on networked hosts can create connections to one another, over which streams of data can be exchanged.

time count - The amount of time end users spend on a given Web page, including the number of times that page is refreshed by either the user or a banner ad.

Time Usage Report count - The amount of time end users spend on the Internet, based on the Time Usage algorithm. For each user, the number of seconds from the log is dropped, and any unique minute within a given hour counts as one minute.

Traveler - M86 Security’s executable program that downloads updates to the SR at a scheduled time.

UDP - An abbreviation for User Data Protocol, one of the core protocols of the Internet protocol suite. Using UDP, programs on networked computers can send short messages (sometimes known as datagrams) to one another.

URL - An abbreviation for Uniform Resource Locator, the global address of Web pages and other resources on the Internet. A URL is comprised of two parts. The first part of the address specifies which protocol to use (such as "http"). The second part specifies the IP address or the domain name where the resource is located (such as “203.15.47.23” or "m86security.com").

Web access logging device - The device feeding logs to the SR—e.g. M86 Web Filter or M86 Secure Web Gateway (SWG).

INDEX