

M86 Security Reporter
EVALUATION GUIDE
Models: 300, 500, 700, 705, 730, 735

M86 SECURITY REPORTER INSTALLATION GUIDE FOR 300, 500, 700, 705, 730, 735 MODELS

© 2010 M86 Security

All rights reserved. Printed in the United States of America

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

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

Trademarks

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

Part# SR-EG-101030

CONTENTS

SECURITY REPORTER EVALUATION GUIDE	1
Product Overview.....	1
Note to Evaluators.	1
Install, Configure, and Test the Security Reporter.	2
About this Evaluation Guide.....	2
SECTION 1: PRODUCTIVITY REPORTS	3
Understand the most common and useful features.	3
Use Custom Category Groups to narrow your search.....	4
How to add a Custom Category Group	4
Use custom User Groups to narrow your search.	5
How to create User Groups	5
Patterns frame	6
IP Ranges frame	7
Single Users/Exclude frame	8
How to Rebuild a User Group	8
Use Security Reporter to conduct an investigation.....	9
Use Summary Reports for a high level overview.....	10
How to generate a Summary Report	11
How to export a Summary Report	13
Use Drill Down Reports for an investigation.....	14
How to generate a Summary Drill Down Report	14
Summary Drill Down Report navigation	15
Count columns and links	15
Bandwidth and Time columns	16
Column sorting tips	17
Record exportation.....	17
Navigation tips.....	17
How to generate a Detail Drill Down Report	18
Detail Drill Down Report navigation	18
Report type columns	18
Detail Drill Down Report exercise	19
Step A: Select a specific user by Category	19
Step B: Sort by “Filter Action” column	19
Step C: Full URL review	19
Step D: Sort by “Content Type”	20
Step E: Sort by “Search String”	20
Create a custom report for a specific user.....	21
How to use the Report Wizard for a single user report	21
Step A: Create either a Summary Report or a Detail Report	21
Step B: Specify the Report Type	22
Summary report	22
Detail report.....	22

Step C: Specify Filters	22
Step D: Specify Other Report Components	23
Step E: Specify when to Generate the Report	23
Step F: Save the Report	24
Export Summary Drill Down Reports.....	27
How to export selected records	27
Step A: Select records to be exported	27
Step B: Specify Data to Export	27
Step C: Export data via Email or PDF Download	27
Email option	27
View and print options.....	28
Sample report file formats	29
Summary Drill Down Reporting tools.....	30
How to use other Summary Drill Down Report tools	30
Limit Detail Result	30
Report fields	30
Type field.....	30
Date Scope and Date fields	30
# Records fields	31
Filter and Filter String fields	32
Sort By and Limit summary result to fields.....	32
Break Type field	32
Format field	32
For additional-break reports only	33
For pie and bar charts only	33
Hide un-Identified IPs checkbox.....	33
E-Mail / For e-mail output only fields.....	34
Commonly used reports.....	35
How to generate a Sample Report	35
Report format	36
Examples of available Sample Reports	37
Sample Report 1: “Top 20 Users by Category/User”	37
Sample Report 2: “Top 20 Sites by User/Site”	37
Sample Report 3: “By Category/User/Site”	38
SECTION 2: REAL TIME REPORTS	39
Understand the most common and useful features.....	39
Monitor URL gauges.....	39
How to drill down into a URL gauge	40
Step A: How to read a URL gauge	40
Gauge Name.....	40
Gauge Score.....	40
Timespan	40
Threat Level	41
Step B: Identify the source of a gauge’s activity	41
Step C: View a list of Threats the end user accessed	42
Step D: View URLs visited by the end user	42
Step E: Further investigate a user’s activity	43
How to view URL Trend Reports	44
Step A: View overall activity in URL gauges	44
Step B: View a line chart for a single URL gauge	45
How to view a pie chart for a URL gauge	46

Monitor Bandwidth gauges.....	47
How to view the Bandwidth gauges Dashboard	47
How to drill down into a Bandwidth gauge	48
Step A: View Bandwidth protocol traffic information	48
Step B: View a user's protocol usage information	48
Step C: View a user's port usage information	49
How to view Bandwidth Trend Chart activity	50
Step A: View overall activity in Bandwidth gauges	50
Step B: View a line chart for a single Bandwidth gauge	51
How to view charts for a specific Bandwidth gauge	52
Get the complete picture.....	53
How to view Overall Ranking of user activity	53
How to create a New Gauge	54
Step A: Select Add/Edit Gauges	54
Step B: Add a New Gauge	54
Step C: Specify Gauge Information	55
Step D: Select users to be monitored by the gauge	56
Step E: Save gauge settings	57
How to create an automated gauge alert	57
Step A: Set up a new alert	57
Step B: Specify Alert Information	59
Step C: Specify criteria in the right side of the panel	60
Step D: Save the alert	60
SECTION 3: SECURITY REPORTS	61
Understand the most common and useful features.....	61
Use security reports for a view of network activity.....	61
How to modify the current report view	62
Page navigation tool	62
Report view icons	62
Create a customized security report.....	64
How to generate a customized security report	64
Step A: Choose a Run option	64
Option 1: Report Settings' Run feature	64
Option 2: Report Wizard's Run feature	64
Step B: Populate the Report Details frame	65
Step C: Use accordions in the Users frame	66
Step D: Run the report	67
Capture the security report in PDF format.....	68
How to export current report view data	68
Step A: Specify records to include in the report	68
Step B: Specify Break Type and URL limitation criteria	68
Step C: Download or email the report	69
Option 1: Download the report	69
Option 2: Email the report	69
Security Report format	70
Save the security report you generated.....	72
How to save a security report	72
Step A: Select Report Settings, Save option	72
Step B: Specify criteria in the Report Details frame	73
Step C: Select the users or group in the Users frame	73

Step D: Populate the Email Settings frame	74
Step E: Save the report	74
Two methods for scheduling security reports.	75
How to use Wizard panels for scheduling reports	75
Step A: Choose the method for scheduling the report	75
Method 1: Use the current report view	75
Method 2: Create a report using the Wizard	76
Step B: Fill in the Report Details frame	76
Step C: Include the users or group in the Users frame	77
Step D: Complete information in the Email Settings frame	77
Step E: Set the schedule for running the report	78
Step F: Save the report	78
How to access and view the Report Schedule panel	79
View Details for a Scheduled Report Run Event	80

SECURITY REPORTER EVALUATION GUIDE

Product Overview

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

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

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

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

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

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

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

Note to Evaluators

Thank you for taking the time to review the M86 Security Reporter (SR) appliance. Your interest in our company and product is greatly appreciated.

This Evaluation Guide is designed to provide product evaluators an efficient way to install, configure and exercise the main product reporting features of the Security Reporter: Productivity Reports, Real Time Reports, and Security Reports.

Install, Configure, and Test the Security Reporter

To install the SR appliance, configure the server, and test the unit to ensure that reporting is operational, please refer to the step-by-step instructions in the M86 Security Reporter Installation Guide provided inside the carton containing the chassis.

Please note that prior to reviewing the SR, the M86 Web Filter and/or M86 Secure Web Gateway (SWG) appliance(s) must already be installed. Either of these appliances are required for this software release in order to send logs to the SR.



NOTE: See the *M86 Web Filter Installation Guide* or *M86 WFR Installation Guide* for information on setting up the Web Filter on your network. See the *M86 SWG Setup and Configuration Guide* for information on setting up the Secure Web Gateway on your network.

About this Evaluation Guide

The M86 Security Reporter Evaluation Guide is divided into three sections to cover each of the basic reporting types:


- Section 1: Productivity Reports
- Section 2: Real Time Reports
- Section 3: Security Reports

SECTION 1: PRODUCTIVITY REPORTS

Understand the most common and useful features

This section of the Evaluation Guide leads the evaluator through the most common and useful features of the Security Reporter, starting with the elements that should be configured first, then moving on to the usage of the many different types of reports available in the SR. You are directed through the normal path of initial setup, and then led through a standard use case that explains how to investigate a violation of your Internet Acceptable Use Policy.

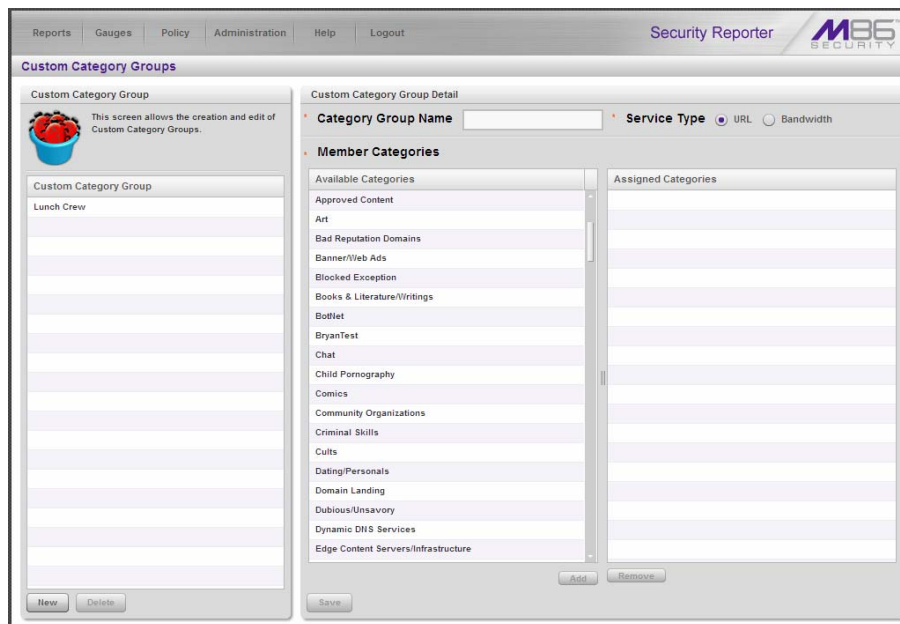
After stepping through this section of the Evaluation Guide, you will understand how to set up powerful reports that can be e-mailed on a regular basis, thus minimizing the effort required for ongoing configuration of the product. In short, by pursuing these exercises, you will discover that the Security Reporter is both easy to use while at the same time best in class in the level of detailed reporting it provides.

 **TIP:** After the SR appliance is installed, allow the Security Reporter to run for several days prior to evaluating reports in order to optimize the evaluation experience. This will allow the SR to accumulate multiple days of data and present more meaningful reports. Having performed these preliminary steps, the SR will function properly on day one of the install with some reports showing no data (e.g. “canned” Summary Reports).

Use Custom Category Groups to narrow your search

Prior to running any reports, there are a few recommended configuration steps that create a more customized experience for the evaluator. The first step is to create Custom Category Groups, which are customized groupings from the M86 Security library of more than 100 filter categories. For example, most customers prefer to set up a category group for those categories that are not allowed under their organization's Acceptable Use Policy. Creating such a category group reduces the time it takes to identify violations of this policy.

To create, edit, or delete a Custom Category Group, navigate to **Administration > Custom Category Groups** to display the Custom Category Groups panel:



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.

How to 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.

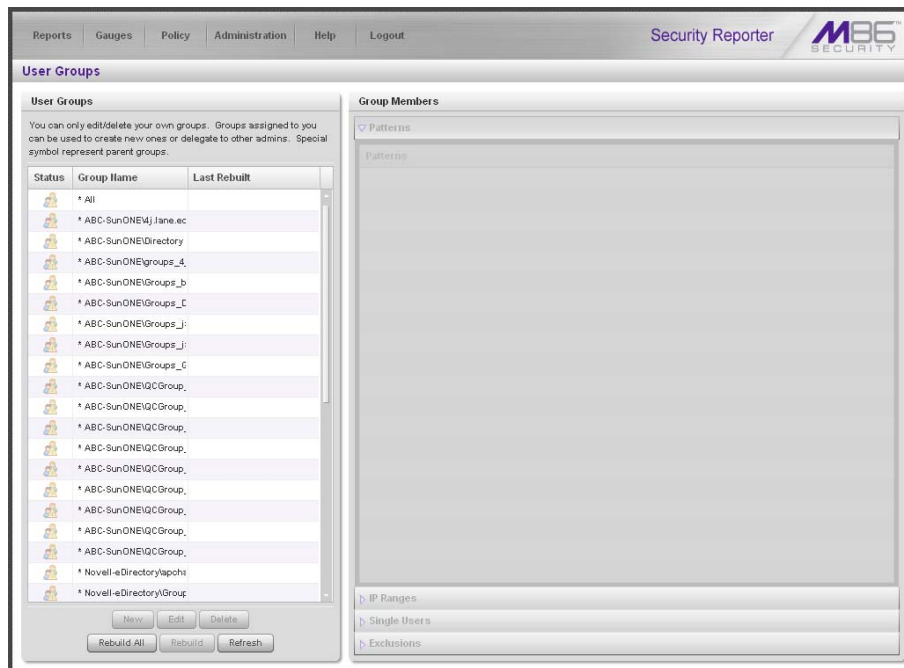
5. Click **Save** to save your settings and to include the name of the group you added in the Custom Category Group list.

Use custom User Groups to narrow your search

The next step is to create User Groups, which are customized groupings of users that reside on the organization's network. For example, most enterprise customers prefer to set up user groups for each department within the company, and education customers prefer to set up separate user groups for each classroom or grade level. Creating these user groups reduces the time it takes to identify the source of violations of your organization's Acceptable Use Policy.

How to create User Groups

To create, edit, or delete a user group, navigate to Administration > **User Groups** to display the User Groups panel:



User Groups panel

The User Groups panel is comprised of two frames used for setting up and maintaining user groupings: User Groups, and Group Members.

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:

New User Group panel

3. Enter at least three characters for the **Group Name** to be used for the new user group.
4. Click the checkbox(es) at the top of the panel to activate the pertinent corresponding frame(s) below: **Patterns**, **IP Ranges**, **Single Users/Exclude**.
5. After making entries in the pertinent frames—as described in the following subsections—click **Save** to save your edits.

Patterns frame

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.

1. To add a pattern to the new user group, 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.

IP Ranges frame

The IP Ranges frame is used for specifying IP ranges to be used by the new group.

Add user group, IP Ranges frame

1. To add an IP address range, 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.

Single Users/Exclude frame

The Single Users/Exclude frame is used for adding one or more users to the group.



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.

The screenshot shows the 'New User Group' dialog box in the Security Reporter application. The 'Single Users / Exclude' tab is selected. The 'Available Users Filter' is empty. The 'Available Users' list contains several IP addresses: 10.1.0.0, 10.1.0.1, 10.1.0.10, 10.1.0.100, and 10.1.0.101. The 'Assigned Users' list shows a list of IP addresses, each preceded by an asterisk, indicating they are auto-assigned users. The list includes: * 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, and * 192.168.20.238.

Add user group, Single Users frame

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.

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.

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.

How to Rebuild a User Group

A user group should be rebuilt if it is edited.

1. To rebuild a user group, 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.

Use Security Reporter to conduct an investigation

Once Custom Category Groups and User Groups have been created, administrators can begin running their first reports. In most cases, administrators will employ the Security Reporter as a forensic tool to determine if anomalous Internet behavior exists in their organization. In order to facilitate this process, the Security Reporter menu structure is organized to follow the normal process flow of an investigation.

1. First, the administrator is greeted by a Dashboard of high-level productivity report information showing data for Blocked Requests and bar graph charts for Top Categories by Requests, Top Security Risks by Requests, Top Blocked Users by Requests, and Top Users by Requests. At a glance, the administrator can see if there is any anomalous behavior that needs investigation.

Additional productivity report content is available by consulting “**Summary Reports.**”

By viewing either of these types of reports, a specific username might be identified as receiving a large number of blocked requests. Or a high rate of traffic might be identified in the “Pornography/Adult Content” category. If something is detected that warrants further investigation, one would then proceed to the “**Drill Down Reports**” section.

2. The next stage of the investigation, Drill Down Reports, lets the administrator probe the multi-dimensional database to target the source of any Internet threat.

For example, if there is unusually high page count in the “Pornography/Adult Content” category, the administrator can drill down into the Category/User section to determine who is viewing this material. Once a specific end user is identified, the administrator can then delve into the detail page view section to see the exact pages that end user has been visiting.

This detailed information provides a wealth of information on the exact time the page was visited, the user’s IP address, whether the site was blocked by the Web Filter or SWG, how it was blocked (e.g. in URL library, blocked keyword, proxy pattern blocking, etc), and the full-length URL. By viewing this detail, the administrator can obtain an accurate gauge of the user’s intent—whether the user repeatedly attempted to go to a forbidden site or whether it was an isolated incident.

3. The last stage of an investigation is to document the long-term activity of a policy violator, since most organizations require more than one or two events to reprimand a user. Once the administrator determines the name of the user and the Web sites visited in the Drill Down Report, the next step is to run a custom report. The administrator can run a specific search of the policy violator for a custom time period by selecting the “**Report Wizard**” option. When generating this type of report, a custom time scope, specific category, and name of a specific end user can be specified.

As an example, the administrator would probably run a custom report for the policy violator by specifying the category “Pornography/Adult Content” and all activity within that category within the last month. The administrator can then save a PDF version of the report for documentation purposes. This custom

report provides the necessary forensic information to support any internal reprimand and to protect the organization in the event the incident goes to court.

To summarize, the aforementioned steps were provided to give the user a most-likely use case for the Security Reporter. The next sub-section provides a more in-depth view of how to navigate within each of the main productivity reporting areas of the Security Reporter: Summary Reports, Drill Down Reports, and Custom Reports.

Use Summary Reports for a high level overview

As previously mentioned, Summary Reports provide an administrator an at-a-glance view of any anomalous behavior that warrants an investigation. These “canned reports” contain pre-generated data for a specified period of time (Yesterday, Last Week, Last Month, Week to Yesterday, or Month to Yesterday) for any of the following report topics or entities showing Internet activity:

- **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) - Bar chart depicting each top end user’s total Mega Bytes for bandwidth requests.
- **Top 20 Users by Virus Hit Count** (for SWG only) - Bar chart report depicting each top end user’s total Virus Count 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 only) - 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.

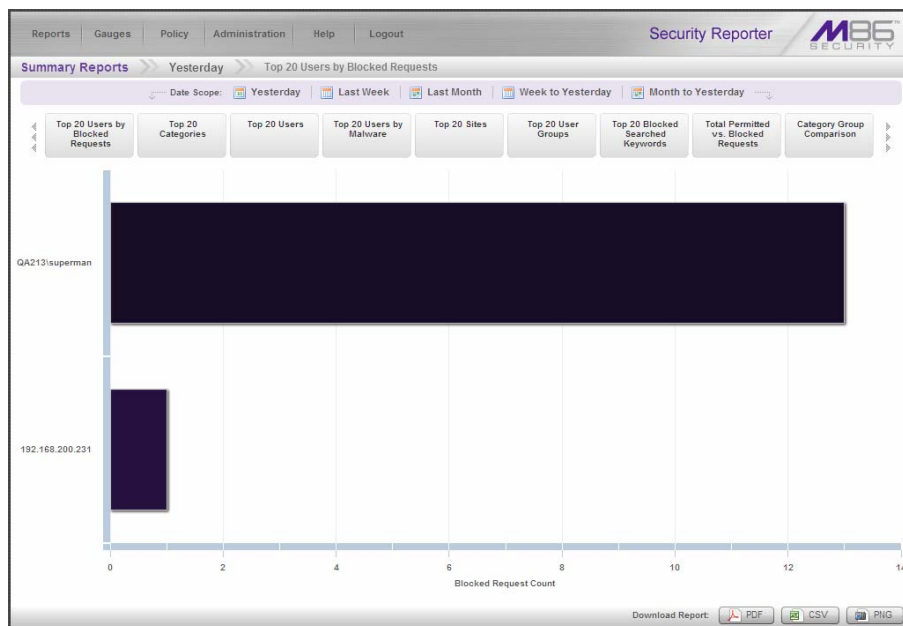
- **Top 20 Sites** - Bar chart report depicting the total Page Count for the most popular sites accessed by end users.
- **Top 20 User Groups** - Bar chart report depicting the total Page Count for the top scoring user groups.
- **Top 20 Blocked Searched Keywords** - Bar chart report depicting the total 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.


Once you have obtained an overview of Internet activity using Summary Reports, you can drill down to access more detailed information about specified end user activity.


How to generate a Summary Report

1. To generate a Summary Report, go to the navigation panel and click **Reports > Summary Reports** to display yesterday's report view showing the Top 20 Users by Blocked Request:



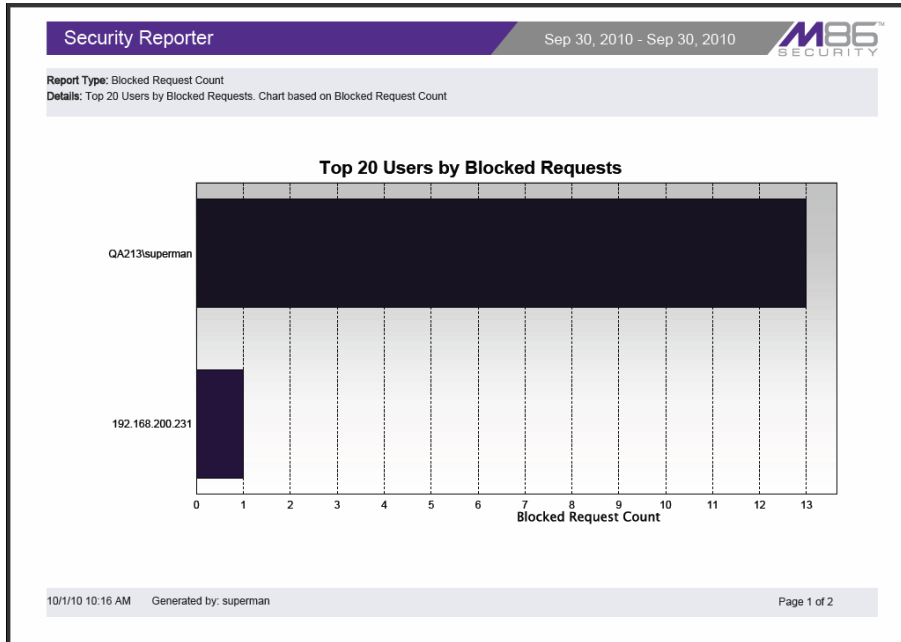
Yesterday's Top 20 Users by Blocked Requests Report

 **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.

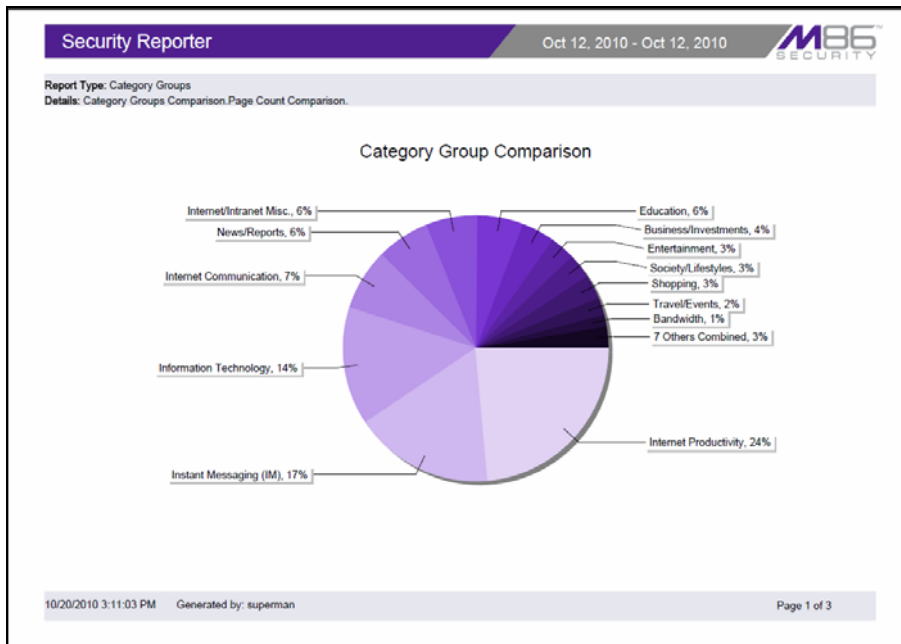
 **TIPS:** Click the left arrows or right arrows at the edges of the dashboard to display thumbnail images that are currently hidden. Mouse over each bar in the bar graph to view the name of graph entry and number of requests for that entry.

2. Click a **Date Scope** tab corresponding to the time period to be included in the report: “Yesterday”, “Last Week”, “Last Month”, “Week to Yesterday”, or “Month to Yesterday”.

3. Click one of the report type thumbnails beneath the Date Scope to display that report view.
4. To see details for the generated Summary Report view, 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):



Sample Bar Chart Summary Report in the PDF format



Sample Pie Chart Summary Report in the PDF format

The header of the generated report includes the date range, Report Type, and criteria Details.

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.

How to export a Summary Report

From the open PDF file, the Summary 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.

Use Drill Down Reports for an investigation

In the event that Summary Reports in the Security Reporter dashboard reveal abnormal activity, the next step in the investigation would be to drill down into the particular category or user information.

This section provides information about “drill down” reports that let you query the database to access more detailed information about end user Internet activity. The following types of reports can be generated:

- **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.

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.

How to generate a Summary Drill Down Report

1. To generate a summary Drill Down Report, go to the navigation panel and click **Reports > Drill Down Reports**, and choose the report type to be generated. The first menu selection is “Categories”; making this selection displays today’s Categories report view by Page Count:

Categories	Category Cou...	IP Count	User Count	Site Count	Bandwidth	Page Count	Object Count	Time HH:MM:S...
<input checked="" type="checkbox"/> Search Engines		57	58	23	0.00 kB	2,505	880	2:22:40
<input checked="" type="checkbox"/> Information Technol		70	70	111	0.00 kB	1,421	6,563	2:48:40
<input checked="" type="checkbox"/> PRODI		14	14	1	0.00 kB	1,119	239	2:18:50
<input checked="" type="checkbox"/> Secure Shell (SSH)		4	4	4	0.00 kB	1,080	0	1:23:40
<input checked="" type="checkbox"/> Financial Institution		11	11	8	0.00 kB	771	50	1:2:50
<input checked="" type="checkbox"/> Flash Video		4	4	77	0.00 kB	788	0	0:32:40
<input checked="" type="checkbox"/> Banner/Web Ads		22	22	81	0.00 kB	741	3,057	1:14:10
<input checked="" type="checkbox"/> Movies & Television		5	5	4	0.00 kB	600	603	0:32:40
<input checked="" type="checkbox"/> Yahoo IM		4	4	5	0.00 kB	581	0	1:34:20
<input checked="" type="checkbox"/> Generic Streaming I		15	15	23	0.00 kB	389	584	0:29:20
<input checked="" type="checkbox"/> Web Based Storage		4	4	3	0.00 kB	357	0	0:59:10
<input checked="" type="checkbox"/> Edge Content Serve		28	28	13	0.00 kB	243	1,006	0:9:30
<input checked="" type="checkbox"/> General Business		22	22	42	0.00 kB	199	1,720	0:16:10
<input checked="" type="checkbox"/> News		18	17	41	0.00 kB	170	707	0:13:50
<input checked="" type="checkbox"/> Web Logs/Personal		9	9	14	0.00 kB	126	6,989	0:19:50
<input checked="" type="checkbox"/> Shopping		10	10	11	0.00 kB	132	727	0:6:0
<input checked="" type="checkbox"/> Entertainment		12	12	14	0.00 kB	129	1,618	0:9:40
<input checked="" type="checkbox"/> Education		14	14	23	0.00 kB	110	235	0:11:50
<input checked="" type="checkbox"/> Online Communities		14	14	3	0.00 kB	83	1,242	0:10:10
<input checked="" type="checkbox"/> Message Boards		7	7	1	0.00 kB	55	75	0:7:0
<input checked="" type="checkbox"/> Reference		11	11	10	0.00 kB	52	205	0:5:10
<input checked="" type="checkbox"/> Image Servers & Im		13	13	10	0.00 kB	44	130	0:7:20

Sample Drill Down Categories Report (summary report)

The report view is horizontally organized into three sections:

- Top section - includes navigational links in the row beneath the navigation toolbar. Beneath this row, **Report Type** tabs let you generate another summary drill down report by clicking that tab (Categories, IPs, Users, Sites, Category Groups, or User Groups). The following information displays beneath this row of tabs: report type, Display criteria, Date, Filter criteria, and Sort by criteria.
 - Main section - includes rows of records returned by the reporting query. Each row is preceded by a checkbox. For each record, filter columns with statistics display (such as Category Count, IP Count, User Count, Site Count, Bandwidth, Page Count, and Object Count), and the Time HH:MM:SS column. Each filter column populated with statistics includes links that if clicked will generate a different report view. Clicking a link in the Page Count or Object Count column will generate a detail drill down report view.
 - Bottom section - includes buttons for customizing the current report view: **Modify**, **Save**, **Export**, **Limited Detail Result**, **Check All**, and **Uncheck All**. The **Go to page** navigation field at far right lets you navigate to a specific page and includes the total pages in the report view.
3. Use the tools in this panel to create the desired drill down view.



NOTE: See 'Summary Drill Down Report navigation' for information on using the reporting elements described in this sub-section.

4. The drill down view can be exported, saved, and/or scheduled to run at a specified time.

Summary Drill Down Report navigation

Continuing from the last section, this section is designed to help the administrator learn how to navigate within the Summary Drill Down Report. The Drill Down report is unique in terms of the seemingly endless ways data can be displayed, but it is important to understand all of the functions within this tool in order to generate meaningful reports.

Count columns and links

In a summary drill down report view, 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.

- **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. In the detail report view, you have the option to exclude Information columns for Category, User IP, User name, Site, Filter Action, Content Type, Content criteria, and Search String by deselecting the corresponding checkboxes via the Column visibility option.

- **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. In the detail report view, you have the option to include Information columns for Category, User IP, User name, Site, Filter Action, Content Type, Content criteria, and Search String by deselecting the corresponding checkboxes via the Column visibility option.

 **NOTE:** If “Pages only” was specified in the Object Count 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 Object Count 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 kB or MB used for each record, if using an SWG only with this SR.
- **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, 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.

Record exportation

In a summary drill down report view, each record is preceded by a checkbox that is populated (selected) by default.

When exporting a report, only selected records are included. To de-select a record, click the checkbox to remove the check mark from that checkbox.

To de-select all records, click **Uncheck All** at the bottom of the panel.

To select all records, click **Check All** at the bottom of the panel.

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 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 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.

How to generate a Detail Drill Down Report

By using the Summary Drill Down Report, the administrator should have narrowed the investigation to a specific category (e.g. “Pornography/Adult Content”) and a specific user name. The next step is to drill down into the detailed URL information to confirm the exact pages visited by the suspected policy violator.

To generate a detail drill down report, select the record and click the link in the “Page Count” column of the Summary Drill Down Report:

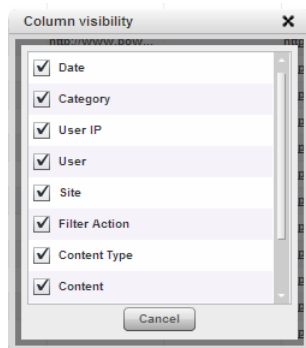
Date	Category	User IP	User	Site	Filter Act...	Content Ty...	Content	Search Str...	URL
10/1/2010 12:00...	Entertainment	208.90.237.246	208.90.237.246	oricon.co.jp	Allowed	Wildcard	http://blog.oricon...		http://blog.oricon...
10/1/2010 12:00...	Entertainment	208.90.237.246	208.90.237.246	sdo.com	Allowed	Wildcard	http://act.dn.sdo...		http://act.dn.sdo...
10/1/2010 12:03...	Entertainment	208.90.237.246	208.90.237.246	www.gg24.de	Allowed	URL	http://www.gg24...		http://www.gg24...
10/1/2010 12:03...	Entertainment	208.90.237.246	208.90.237.246	sdo.com	Allowed	Wildcard	http://act.dn.sdo...		http://act.dn.sdo...
10/1/2010 12:04...	Entertainment	208.90.237.246	208.90.237.246	sdo.com	Allowed	Wildcard	http://act.dn.sdo...		http://act.dn.sdo...
10/1/2010 12:04...	Entertainment	208.90.237.246	208.90.237.246	sdo.com	Allowed	Wildcard	http://act.dn.sdo...		http://act.dn.sdo...
10/1/2010 12:05...	Entertainment	208.90.237.246	208.90.237.246	hovtospentid.com	Allowed	Wildcard	http://www.hovt...		http://www.hovt...
10/1/2010 12:05...	Entertainment	208.90.237.246	208.90.237.246	gossipcenter.com	Allowed	Wildcard	http://www.goss...		http://www.goss...
10/1/2010 12:05...	Entertainment	208.90.237.246	208.90.237.246	hovtospentid.com	Allowed	Wildcard	http://www.hovt...		http://www.hovt...
10/1/2010 12:05...	Entertainment	208.90.237.246	208.90.237.246	hovtospentid.com	Allowed	Wildcard	http://www.hovt...		http://www.hovt...
10/1/2010 12:06...	Entertainment	208.90.237.246	208.90.237.246	cmu.ac.th	Allowed	URL	http://dekmor.cm...		http://dekmor.cm...
10/1/2010 12:06...	Entertainment	208.90.237.246	208.90.237.246	sdo.com	Allowed	Wildcard	http://act.dn.sdo...		http://act.dn.sdo...
10/1/2010 12:06...	Entertainment	208.90.237.246	208.90.237.246	hovtospentid.com	Allowed	Wildcard	http://www.hovt...		http://www.hovt...
10/1/2010 12:07...	Entertainment	208.90.237.246	208.90.237.246	sdo.com	Allowed	Wildcard	http://act.dn.sdo...		http://act.dn.sdo...
10/1/2010 12:07...	Entertainment	208.90.237.246	208.90.237.246	107exito.com.gt	Allowed	URL	http://107exito.c...		http://107exito.c...
10/1/2010 12:08...	Entertainment	208.90.237.246	208.90.237.246	hi-ho.ne.jp	Allowed	URL	http://www.cam...		http://www.cam...
10/1/2010 12:08...	Entertainment	208.90.237.246	208.90.237.246	www.ich-will-be...	Allowed	URL	http://www.ich...		http://www.ich...
10/1/2010 12:08...	Entertainment	208.90.237.246	208.90.237.246	gossipcenter.com	Allowed	Wildcard	http://www.goss...		http://www.goss...
10/1/2010 12:09...	Entertainment	208.90.237.246	208.90.237.246	107exito.com.gt	Allowed	URL	http://107exito.c...		http://107exito.c...
10/1/2010 12:09...	Entertainment	208.90.237.246	208.90.237.246	107exito.com.gt	Allowed	URL	http://107exito.c...		http://107exito.c...
10/1/2010 12:10...	Entertainment	208.90.237.246	208.90.237.246	psiphi.org	Allowed	URL	http://www.psip...		http://www.psip...
10/1/2010 12:11...	Entertainment	208.90.237.246	208.90.237.246	mop.com	Allowed	Wildcard	http://www.mop...		http://www.mop...

Detail Drill Down Report view

Detail Drill Down Report navigation

Report type columns

In the detail report view, 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 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** - 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** - Displays criteria used for determining the categorization of the record, or “N/A” if unclassified.
- **Search String** - 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.

Detail Drill Down Report exercise

For the purpose of this evaluation, follow these steps to witness how the Security Reporter is best in class in terms of the extent of detailed page and object information it provides.

Step A: Select a specific user by Category

If not already completed, click the “Page Count” column link for any record in the Summary Drill Down Report.

Step B: Sort by “Filter Action” column

Clicking the “Filter Action” column header will sort all records by the type of filter action—whether the event was blocked, allowed or warned. Blocked searches will be highlighted in red font for easier detection.

Step C: Full URL review

The full length URL of every Internet search by the users is listed in the “URL” column of the detail page information.

To view record data that displays truncated in a 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.bowers.org/includes/jquery.dropdownPlain.js
	http://www.bower...

Mouse over to view full URL

Click the URL link to launch the actual Web site viewed by the user to verify the content that was accessed.

Step D: Sort by “Content Type”

Sort by the column labeled “Content Type” by clicking that column header. This will sort all records by the search type filtered on the Web Filter or SWG. For example, “**URL**” indicates a page request was blocked or allowed based on the status of that URL in the Web Filter category library and “**Search KW**” indicates a user typed in a prohibited word into a search engine text box. One of M86 Security’s differentiators is “**Proxy Pattern Blocking**,” which will show up in the “Content Type” section if an Internet proxy site was blocked by M86 Security’s proprietary proxy signature detection.

After reviewing a suspected policy violator’s Internet activity in the Detail Drill Down Report, the administrator will have firm evidence on the user’s *intent*, which is critical forensic information to have in the event the investigation moves to the disciplinary phase.

Step E: Sort by “Search String”

Sort by the column labeled “Search String” by clicking that column header. This will sort all records alphabetically for results that include search string information. Search string content includes the actual text typed into a search engine text box on popular search engine sites such as Google, Bing, Yahoo!, YouTube, Ask.com, and MSN. For example, if the end user typed in “recipes for chicken breast” in a search engine request, that entire string will appear in this column, not simply the blocked keywords within the request. This depth of detail helps clarify the intent of the end user, which helps tremendously in investigations.

In the next section, this guide will go through the final step in a typical investigation—creating a custom report for a specific user via the Report Wizard.

Create a custom report for a specific user

After reviewing the detail drill down report, if the administrator is confident that an individual has violated the Internet Acceptable Use Policy (AUP), the most common step to take next is to run a custom report for this specific individual that covers a greater time period. While there are several ways to accomplish this in the Security Reporter, this guide will focus on the most commonly used method—the productivity **Report Wizard**.

How to use the Report Wizard for a single user report

The Report Wizard option provides an intuitive setup process for generating custom reports for one time use, or for recurrence at scheduled time periods. The “Report Wizard” option is available by navigating to **Reports > Report Wizard**:

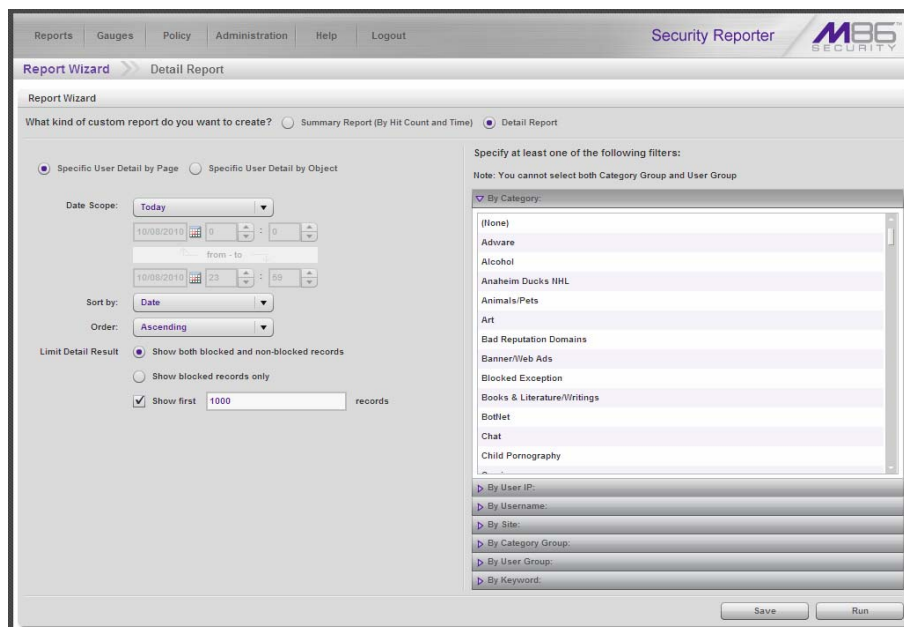
The screenshot shows the 'Report Wizard' panel in the Security Reporter application. The top navigation bar includes 'Reports', 'Gauges', 'Policy', 'Administration', 'Help', and 'Logout'. The main title is 'Report Wizard' with a sub-tab for 'Summary Report'. Below the title, there are two radio buttons: 'Summary Report (By Hit Count and Time)' (selected) and 'Detail Report'. The 'Type' dropdown is set to 'Categories'. The 'Date Scope' is set to 'Today'. There are two date pickers: the first is for 'from' (08/27/2010) and the second is for 'to' (08/27/2010). Under '# Records', 'Show all records' is selected. The 'Sort by' dropdown is set to 'Page Count'. On the right, there is a 'Filters (optional):' section with a note: 'Note: You cannot select both Category Group and User Group'. Below this, there are several expandable filter sections: 'By Category' (expanded), 'By User IP', 'By Username', 'By Site', 'By Category Group', and 'By User Group'. The 'By Category' list includes: (None), Adware, Alcohol, Anaheim Ducks NHL, Animals/Pets, Art, Bad Reputation Domains, Banner/Web Ads, Blocked Exception, Books & Literature/Writings, Bot/Iet, Chat, Child Pornography, Comics, and more. At the bottom right, there are 'Save' and 'Run' buttons.

Report Wizard panel for summary reports

Step A: Create either a Summary Report or a Detail Report

Select one of two available custom productivity 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.



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; for this exercise, choose “Categories” or “Sites”.

In this exercise, narrow your results for the specified user by choosing the **Filters (optional)** accordion for “By User IP” or “By Username”, as 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—for this exercise, “By User IP” or “By Username”—as described in Step C.

Step C: Specify Filters

For this exercise, choose either of these filters:

- **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.
- **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 report, select the username and click the right arrow (>) to move the username into the Added user names list box.

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 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 report, indicate whether results will be sorted in “Ascending” or “Descending” order.
- **Limit Detail Result** - For a detail 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.
- **Save** - Click this button to go to the Save Report panel where you save your report criteria now but generate your report later.


Step F: Save the Report

1. Click the **Save** button to display the Basic Options tab of the **Report Wizard > Save Report** panel:

The screenshot displays the 'Report Wizard' window with the 'Save Report' panel open. The 'Basic Options' tab is selected. The 'Report Info' section contains 'Save Name' and 'Description' text boxes. The 'E-Mail' section includes 'To', 'Cc', 'Bcc', 'Subject', and 'Body' text boxes, a 'Hide un-identified IPs' checkbox, an 'Output type' dropdown menu (set to 'E-Mail As Attachment'), and a 'Format' dropdown menu (set to 'PDF'). The 'Filters' section lists various criteria like Category, User IP, Users, Site, Category Group, User Group, and Keywords, all currently set to 'N/A'. At the bottom right, there are three buttons: 'Save and Schedule', 'Save and Email', and 'Save Only'.

Report Wizard's Save Report panel Basic Options tab

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.
 - **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:
 - **Break Type** - Available selections are based on the type of report specified.
 - For summary reports, at the **For additional-break reports only** field, if a selection was made in the Break Type field, specify the top count option to be used in the **# Records** and **Sort By** fields.
 - For a summary report, **For pie and bar charts only**, the activated **Generate using** field lets you select the count column sort option.
 - For detail 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 report:

Report Wizard's Schedule Report panel

- Enter a **Name** for the event.
- Select the **Report to Run** from the list.
- 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).
- Select the **Start Time** for the report: 1 - 12 for the hour, 0 - 59 for the minutes, and AM or PM.



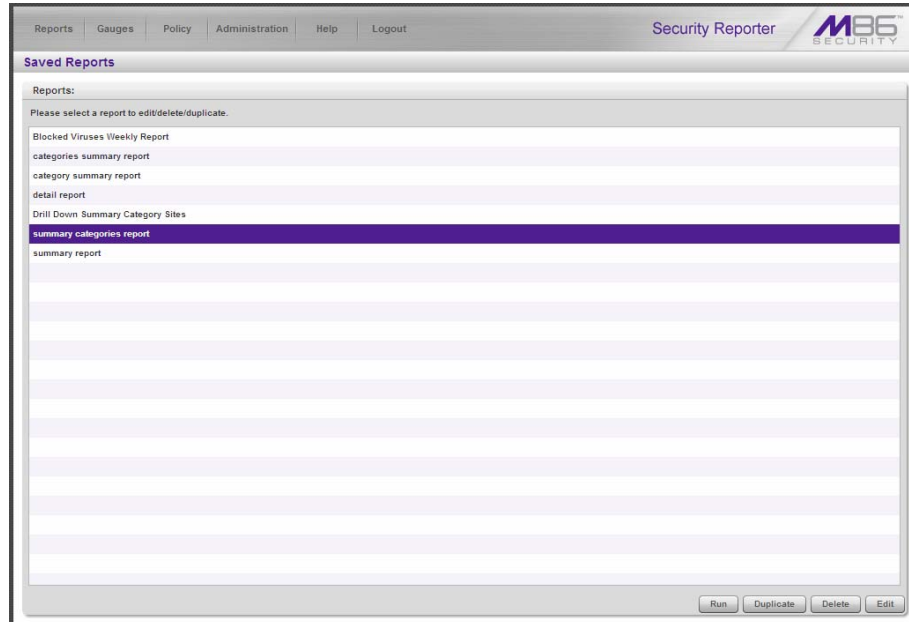
NOTE: The default Start Time is 8:00 AM. If you wish to run a report today and this time has already passed, be sure to select a future time.

- 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.



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.



Saved Reports panel

- **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.

Export Summary Drill Down Reports

For this exercise, you will learn how to export a customized Summary Drill Down Report.

How to export selected records

Step A: Select records to be exported

To only include specific records in the report, click the **Uncheck All** button at the bottom of the panel, and then click the checkboxes corresponding to the records to be exported.

Step B: Specify Data to Export

1. Click the **Export** button to open the Export pop-up box:

Summary drill down Export pop-up box

2. At the **Data to Export** field pull-down menu, specify the amount of data to be exported. For this exercise, choose “Only selected rows on this page”.

Step C: Export data via Email or PDF Download

1. Make selections and/or entries in all fields in the Export pop-up box.
2. Click the **Email** or **Download** button to close this pop-up box and to export the data—via email or to your workstation—in the specified file format.

Email option

The email option for exporting 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 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 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** - Highlight 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)

To close the report file window, click the "X" in the upper right corner of the window.

Sample report file formats

The following report file formats are available for emailing and viewing: “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 user-names 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.

PDF

This is a sample of the Category Groups report in the PDF format, saved with a .pdf file extension:

Security Reporter		Oct 07, 2010 - Oct 07, 2010		M86 SECURITY				
Sort Order: Date, ascending		Category Groups						
Category Group: Internet Communication								
Date	Category	IP	User	Site	Filter Action	Contact Type	Content	Filter String
10/7/2010 12:09:26 AM	Chat	10.1.0.11	testDomain\User19210	meebo.com	Allowed	Wildcard	http://www.meebo.com /	
http://www.meebo.com/mcmd/events								
10/7/2010 12:09:27 AM	Chat	10.1.0.46	testDomain\User50031	yahoo.com	Allowed	URL	http://shttp.msg.yahoo.com/	
http://shttp.msg.yahoo.com/hotfly/								
10/7/2010 12:09:28 AM	Chat	10.1.0.97	testDomain\User94874	yahoo.com	Allowed	URL	http://shttp.msg.yahoo.com/	
http://shttp.msg.yahoo.com/hotfly/								
10/7/2010 12:09:28 AM	Web Based Email	10.1.0.77	testDomain\User65740	getemail.sympatico.ca	Allowed	URL	http://getemail.sympatico.ca/	
http://getemail.sympatico.ca/GetTips?PageName=fix&locale=en_CA_jsp								
10/7/2010 12:09:29 AM	Chat	10.1.0.111	testDomain\User50962	userplane.com	Allowed	Wildcard	http://02.myspaace.presence.userplane.com/	
http://02.myspaace.presence.userplane.com/1/1163828587212/1/FAdE+XovXDcveeEWeb5vGSHdn8B5eouPnU1jygMsrFXkaARX55RQJLlYDI								
10/7/2010 12:09:29 AM	Chat	10.1.0.155	testDomain\User72001	userplane.com	Allowed	Wildcard	http://03.myspaace.presence.userplane.com/	
http://03.myspaace.presence.userplane.com/1/1163828570566/1Ujy07ab2Y2TUyaNAebztAB6CY/sicv4FmRFQzme#MxBVL2HtveWsfPJQLnP4								
10/7/2010 12:09:29 AM	Web Based Email	10.1.0.128	testDomain\User70362	google.com	Allowed	URL	http://mail.google.com/mail/7ik-Baa4d1967&view=6&search=mailbox&start=0&th=10eed40c2a28fp=0&auto=1&vv=5&rq=ym&at=79171e814cab0194-10eecc47d01&zz=U6vje5-vahjd	
http://mail.google.com/mail/7ik-b00e3d35ad&view=6&search=mailbox&start=0&th=10eeda394b66fp=0&auto=1&vv=40&rq=ym&at=9e0c0bec7ec27e7-10ee70f556&zz=xsx1jk-zzehtge								
10/7/2010 12:09:31 AM	Chat	10.1.0.204	testDomain\User28185	meebo.com	Allowed	Wildcard	http://www36.meebo.com/	
http://www36.meebo.com/mcmd/omv								
10/7/2010 12:09:31 AM	Chat	10.1.0.222	testDomain\User69437	meebo.com	Allowed	Wildcard	http://www.meebo.com /	
http://www.meebo.com/mcmd/events								
10/7/2010 2:24:10 PM		Generated by: administrator		Filter: None		Page 1 of 91		

Category Groups report, PDF format

Examples of other report formats are provided in the M86 Security Reporter User Guide.

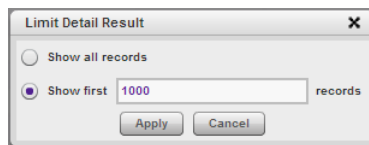
Summary Drill Down Reporting tools

The Security Reporter has a variety of different reporting options. In a fashion similar to the specific user report creation process, administrators can also create custom reports from any Drill Down Report view. These reports can be set up to be automatically emailed to the administrator on a regular basis in a variety of formats (e.g. PDF, Excel, etc.).

How to use other Summary Drill Down Report tools

Limit Detail Result

1. Click the **Limit Detail Result** button to open the Limit Detail Result pop-up box:



Limit Detail Result pop-up box

2. Indicate the limit for the set of records to be returned by selecting 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.
3. Indicate the number of records to be included in a set by making an entry in the blank field, represented here by the 'X'.
4. Click **Apply** to apply your settings in the current report view and to close this pop-up box.

Report fields

Type field

The Type field is used for specifying the report type by which the generated report view will be sorted. This field is available in the Modify Report pop-up box via the Modify button.

At the **Type** field, make a selection from the pull-down menu for one of the available report types: "Categories", "IPs", "Users", "Sites", "Category Groups", "User Groups", and the current report format displayed.

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. Depending on the scope selected, the From Date and To Date fields are used in conjunction with this field. These fields are available in the Modify Report pop-up box via the Modify button, and in the Save Report pop-up window via the Save button.

At the **Date Scope** field, make a selection from the pull down menu for the time frame you wish to use in your query: “Today”, “Month to Date”, “Monthly”, “Year to Date”, “Daily”, “Yesterday”, “Month to Yesterday”, “Year to Yesterday”, “Last Week”, “Last Weekend”, “Current Week”, “Last Month”. Reports can be run for any data saved in the SR’s memory.

- **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.

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.

These fields are available via the Modify Report option, and in the Advanced Options tab of the Save option.

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 and Limit summary result to fields

The sort fields are used for specifying the report view column by which the generated report will be sorted.

At the **Sort By** field, make a selection from the pull-down menu for one of the available sort options: “Name of ‘x’”, “Category Count”, “IP Count”, “User Count”, “Site Count”, “Page Count”, “Object Count”, “Time”, “Hit Count”, “Bandwidth”.

If the “Name of ‘x’” option is selected, the **Limit summary result to field** displays. Make a selection from the pull-down menu for one of the available choices for which the summary report results will be limited: “Top Category Count”, “Top IP Count”, “Top User Count”, “Top Site Count”, “Top Page Count”, “Top Object Count”, “Top Time”, “Top Hit Count”, “Top Bandwidth”.

Break Type field

The Break Type field is used for indicating the manner in which records will display for the specified report view when exported. This field is available in the Export pop-up box, and in the Advanced Options tab of the Save option.

Choose from the available report selections at the **Break Type** 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-break report types such as “Users/Sites”, triple-break 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. This field is available in the Export pop-up box via the Export button, and in the Save Report pop-up window via the Save button.

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)”, and “Excel (English)”.

For additional-break reports only

The # Records and Sort By fields are used when exporting double-break and triple-break 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 Break Type 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.

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”.

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 Break type 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”.

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.

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.

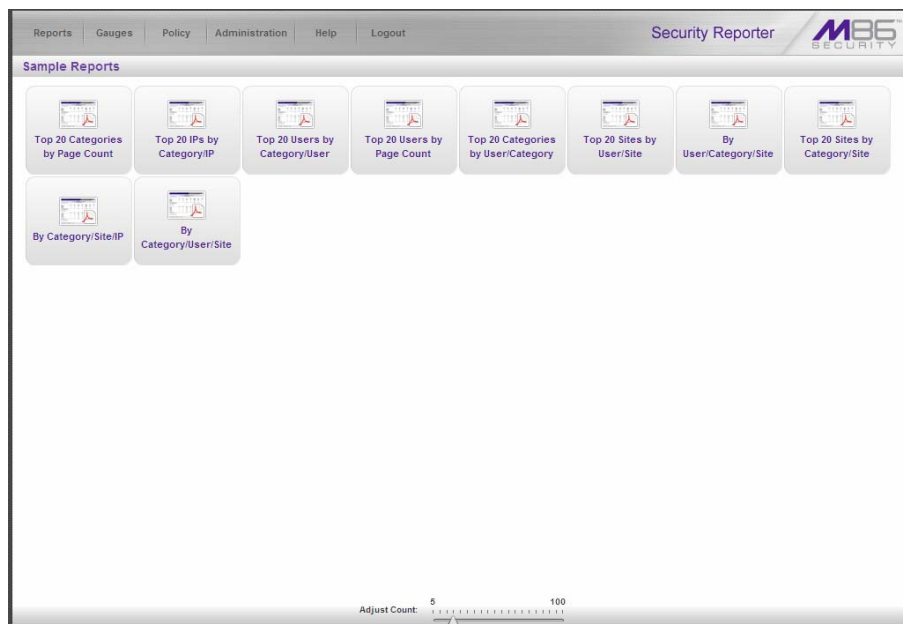
Commonly used reports

Though this portion of the Evaluation Guide is primarily designed to lead the evaluator through the process of an investigation using common productivity reports, there are many other useful features to explore in Security Reporter productivity reports. Below is a summary of some of the other custom reports an administrator can create and have automatically emailed on a regular basis in order to be kept up to date on Internet threats arising from within the organization.

M86 Security has created 10 different sample report formats to help first time users understand the various types of reports available in the Security Reporter. For purposes of this Evaluation Guide, only three of the 10 are described in detail below. A description of all other sample reports is available in the Security Reporter User Guide.

How to generate a Sample Report

1. From the Reports menu, choose **Sample Reports**:



Sample Reports

2. Click one of the following thumbnails to open a separate browser window containing the generated Sample Report in the PDF format:
 - **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**
3. From the open PDF file, 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.
 4. Click the “X” in the upper right corner of the report window to close it.

Report format

The report header contains the following information: “Security Reporter” and date range for today’s date (MM/DD/YYYY format); 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 (kB 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 (MM/DD/YYYY) and time (HH:MM:SS AM/PM) the report was generated; **Generated by:** manager’s login ID; **Filter: None; Page** number.

Examples of available Sample Reports

Sample Report 1: “Top 20 Users by Category/User”

This report shows the top 20 users for each of the categories in the M86 Security library. This is a useful tool to quickly scan for excessive use of any category.

Security Reporter		Oct 25, 2010 - Oct 25, 2010		M86 SECURITY					
Category/Users									
All Categories sorted by Page Count, descending									
Top 20 Users by Page Count in each Category table									
Category: Search Engines									
Users	IP Count	Site Count	Bandwidth	Page Count	Object Count	Time (HH:MM:SS)	Hit Count	Blocked Hits	
M8@derek.etrod	1	2	0.00 kB	967	209	0:55:50	1,176	0	
M8@lus.curet	1	17	0.00 kB	648	274	0:41:0	922	0	
M8@mark.keh	1	9	0.00 kB	569	61	0:22:50	630	0	
M8@charles.fladger	1	7	0.00 kB	549	108	0:33:30	657	0	
M8@leah.roberts	1	16	0.00 kB	532	1,235	0:30:50	1,767	0	
M8@brandy.rochelle	1	6	0.00 kB	515	95	0:16:50	610	0	
M8@david.courson	1	4	0.00 kB	509	106	0:30:0	615	0	
208.90.238.30	1	12	0.00 kB	474	816	0:19:20	1,280	0	
M8@david.femmon	1	3	0.00 kB	463	42	0:10:40	505	0	
M8@robert.voccola	2	6	0.00 kB	270	19	0:9:40	289	0	
208.90.237.35	1	11	0.00 kB	268	56	0:19:30	324	0	
208.90.239.19	1	1	0.00 kB	261	0	0:8:50	261	0	
208.90.237.45	1	8	0.00 kB	258	256	0:12:50	514	0	
M8@rodney.miller	1	7	0.00 kB	256	63	0:11:50	319	0	
M8@rony.kordosky	1	10	0.00 kB	250	142	0:14:20	392	0	
208.90.237.37	1	6	0.00 kB	226	33	0:8:0	259	0	
M8@andy.khuu	1	3	0.00 kB	219	53	0:11:20	272	0	
M8@ray.burgess	1	8	0.00 kB	210	123	0:18:0	333	0	
M8@jennifer.stock	1	3	0.00 kB	205	57	0:11:50	262	0	
M8@nia.mcknight	1	1	0.00 kB	190	0	0:8:40	190	0	
Total for Search Engines									
User Count: 20 sorted by Page Count, descending	21		140	0.00 kB	7,839	3,748	6:35:40	11,587	0
Category: Windows Live Messenger									
Users	IP Count	Site Count	Bandwidth	Page Count	Object Count	Time (HH:MM:SS)	Hit Count	Blocked Hits	
10/25/2010 3:46:12 PM Generated by: superman Filter: None Page 1 of 50									

Sample Category/Users report

Sample Report 2: “Top 20 Sites by User/Site”

This report will document the top 20 sites visited for every user in the organization. This is a useful tool in monitoring the high level Web activity of users, and can help fine-tune sites the administrator allows users to access.

Security Reporter		Oct 25, 2010 - Oct 25, 2010					M86 SECURITY		
User/Sites									
All Users sorted by Page Count, descending									
Top 20 Sites by Page Count in each User table									
User:208.90.238.11									
Sites	Category Count	IP Count	Bandwidth	Page Count	Object Count	Time (HH:MM:SS)	Hit Count	Blocked Hits	
alphatrade.com	1	1	0.00 kB	6,377	3	8:21:10	6,380	0	
facebook.com	1	1	0.00 kB	962	137	1:45:40	1,099	0	
98.136.48.67	1	1	0.00 kB	511	0	1:23:30	511	0	
scorecardresearch.com	1	1	0.00 kB	426	52	0:17:0	478	0	
charitseat.net	1	1	0.00 kB	252	0	0:34:50	252	0	
nubiconproject.com	1	1	0.00 kB	181	237	0:7:20	418	0	
gravatator.com	2	1	0.00 kB	151	0	0:2:40	151	0	
google.com	3	1	0.00 kB	143	13	0:6:50	156	0	
fmpub.net	2	1	0.00 kB	141	1	0:3:20	142	0	
gizmodo.com	3	1	0.00 kB	127	43	0:5:0	170	0	
doubleclick.net	1	1	0.00 kB	123	622	0:6:50	745	0	
statemeter.com	1	1	0.00 kB	120	39	0:6:50	159	0	
comregister.com	1	1	0.00 kB	104	363	0:4:20	497	0	
grawler.com	3	1	0.00 kB	98	111	0:11:0	209	0	
fbcdn.net	1	1	0.00 kB	96	741	0:6:40	837	0	
contextweb.com	1	1	0.00 kB	86	1	0:4:40	87	0	
feedburner.com	1	1	0.00 kB	84	1	0:3:30	85	0	
twitter.com	1	1	0.00 kB	83	77	0:6:30	180	0	
techdirt.com	2	1	0.00 kB	79	68	0:7:0	147	0	
freedom.com	2	1	0.00 kB	79	337	0:2:40	416	0	
Total for 208.90.238.11		30	20	0.00 kB	10,223	2,676	13:53:20	13,099	0
Site Count: 20 sorted by Page Count, descending									
User:M86ishari.bourdon									
Sites	Category Count	IP Count	Bandwidth	Page Count	Object Count	Time (HH:MM:SS)	Hit Count	Blocked Hits	
10/25/2010 3:50:36 PM Generated by: superman Filter: None Page 1 of 93									

Sample User/Sites report

Sample Report 3: “By Category/User/Site”

This is an example of a triple break report that shows all activity on the network, broken out by category, then user, and then site. This is a useful report if the administrator is looking for an all-encompassing view of Internet activity within the organization. However, please note that this is usually a very lengthy report since it captures all user information by site.

Security Reporter		Oct 25, 2010 - Oct 25, 2010					M86 SECURITY	
Category/User/Sites								
All Categories sorted by Page Count, descending								
All Sites in each User table								
Category:Search Engines								
User:208.90.237.101								
Sites	IP Count	Bandwidth	Page Count	Object Count	Time (HH:MM:SS)	Hit Count	Blocked Hits	
google.com	1	0.00 kB	131	22	0:6:20	153	0	
live.com	1	0.00 kB	0	174	0:0:0	174	0	
74.125.39.101	1	0.00 kB	0	1	0:0:0	1	0	
googleapis.com	1	0.00 kB	0	1	0:0:0	1	0	
Total for 208.90.237.101		4	0.00 kB	131	198	0:6:20	329	0
Site Count: 4 sorted by Page Count, descending								
Category:Search Engines								
User:208.90.237.16								
Sites	IP Count	Bandwidth	Page Count	Object Count	Time (HH:MM:SS)	Hit Count	Blocked Hits	
google.com	1	0.00 kB	2	0	0:0:20	2	0	
Total for 208.90.237.16		1	0.00 kB	2	0	0:0:20	2	0
Site Count: 1 sorted by Page Count, descending								
Category:Search Engines								
User:208.90.237.18								
Sites	IP Count	Bandwidth	Page Count	Object Count	Time (HH:MM:SS)	Hit Count	Blocked Hits	
google.com	1	0.00 kB	51	0	0:2:40	51	0	
10/25/2010 3:53:09 PM Generated by: superman Filter: None Page 1 of 688								

Sample Category/User/Sites report

SECTION 2: REAL TIME REPORTS

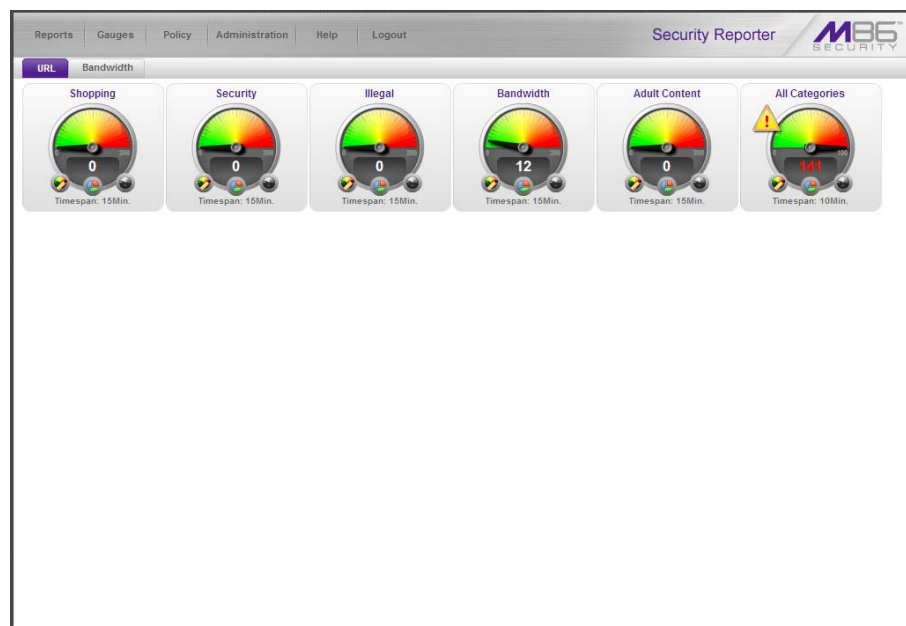
Real time reporting features are available if using a Web Filter with your Security Reporter.

Understand the most common and useful features


In this section of the Evaluation Guide, you will learn how to read URL Dashboard gauges that target areas on your network that could potentially endanger its security and/or usurp most of its bandwidth, and how to identify users who are violating your organization's policies and prevent them from continuing to pursue such activities.

Monitor URL gauges

When clicking **Gauges** in the navigation toolbar, the URL Dashboard displays:



URL dashboard with URL gauges

 **NOTE:** The bandwidth gauges dashboard is displayed by clicking the Bandwidth button to the right of the URL button above the dashboard. The bandwidth gauges dashboard shows you end user activity for bandwidth protocols set up to be monitored by the Security Reporter. More about bandwidth gauges is described later in this section of the Evaluation Guide.

Each URL gauge represented in the Dashboard is comprised of library categories and monitors a targeted user group's access of URLs in a specified library category.

How to drill down into a URL gauge

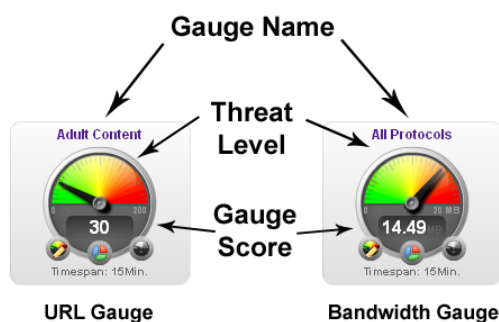
This exercise will step you through the manual monitoring of users in real time via the URL gauges Dashboard. Note that this is simply one of many ways to use SR to monitor insider threats. There is also a robust automated alert component that does not require the system administrator to be monitoring gauges in order to be notified of a violation in process.

Step A: How to read a URL gauge

The graphic and sub-sections below describe how to read gauges on the URL gauges Dashboard:


Gauge Name

The gauge name is the customized name of the gauge created by the administrator. SR has five default sample gauges that correspond to five of M86's super-categories: Shopping, Security, Illegal, Bandwidth and Adult Content. Administrators can create their own gauges as well as delete the default gauges.



Gauge Score

The gauge score is the large number in the center of the gauge that is based upon the number of URL page hits (see NOTE below) that occur in this specific category in a given period of time.

 **NOTES:** In addition to page hits, SR also counts “blocked object” hits. For reference, “pages hits” are files that typically end in .html and represent a main page view. “Object hits” are files that typically end in .gif or .jpg and represent image files.

To streamline your task, SR does not track a score for “non-blocked objects,” since these gauges are designed to provide a clear picture of how many times a user has requested a page, and objects are images hosted within a page. SR includes blocked object data to cover instances in which harmful images are hosted on a non-harmful site.

Timespan

Each gauge monitors events in real time for a window of time between one and 60 minutes. This timespan is customizable by the administrator. For example, if a gauge is set for 15 minutes, that gauge will indicate the number of page hits for the last 15 minutes of time. For example, if the current time is 12:00, the gauge score will reflect all activity from 11:45 to 12:00. Once the time is 12:01, the gauge will reflect all activity from 11:46 to 12:01.

Threat Level

The colored threat level indicates the current state of threat based on the customizable ceiling created by the administrator. For example, if the administrator creates a gauge with a threshold of 100, when the score reaches 67 the gauge dial will move into the red threat level section, the score will turn red, and a yellow warning triangle symbol will appear and begin to flash.



These gauges are designed to provide an intuitive reminder when a specific category gauge is experiencing abnormal levels of activity so the administrator can react quickly.

Step B: Identify the source of a gauge's activity

Each gauge is comprised of one or more gauge components—derived from library categories in the Web Filter. Sometimes end user activity in a single component is responsible for driving a gauge's score.

To identify the source of a gauge's activity, from the URL dashboard you can either click the gauge or right-click the gauge and then select "View Gauge Ranking":

Performing either of the two aforementioned actions on the gauge will open the Gauge Ranking panel showing a list of all end users affecting this gauge's components, and all affected components in this gauge:

User Name	Bandwidth	Liability	Others	Productivity	Security	Total
9AMfranklin	0	0	2	10	100	126
192.168.30.87	0	0	2	10	74	91
192.168.30.80	0	0	27	40	14	81
192.168.30.85	30	0	18	6	0	52
192.168.30.86	0	0	1	2	14	17
192.168.30.74	0	0	18	0	0	16
192.168.30.84	0	0	0	0	0	8
Novell30201USER	0	0	0	5	2	7

Open the Gauge Ranking panel

If a single component is affecting the entire gauge, you can investigate activity in that component by drilling down into the component with the highest score.

Step C: View a list of Threats the end user accessed

In the Gauge Ranking panel, click the highest score in a column for a component; this action displays the Category View User panel showing a list of All Categories accessed by the selected end user for the gauge component:

The screenshot shows the 'Category View User' panel for user 192.168.30.92. The 'Categories' table is as follows:

Categories	Total
Banner/Web Ads	55
Web Based Email	28
Image Servers & Image Search Engines	12
Free Hosts	4
Yahoo IM	2

The 'URLs' table is empty, with a header containing 'URLs' and 'Timestamp'.

View a list of Threats accessed by the user for that gauge

Step D: View URLs visited by the end user

Click a library category to display a list of associated, categorized URLs visited by the end user:

The screenshot shows the 'Category View User' panel with 'Banner/Web Ads' selected in the 'Categories' table. The 'URLs' table contains the following entries:

URLs	Timestamp
http://ads.blueitium.com/iframe375/BaAFU_FgAMR2MAAAAAAF2GqAAAAAAqACOAIA...	2010-09-23 10:19:17
http://ad.yieldmanager.com/iframe375/BaAFU_FgAMR2MAAAAAAF2GqAAAAAAqACOAIA...	2010-09-23 10:19:17
http://ad.yieldmanager.com/imp?_PVID=upQF2Hj8evlVvzobQTIqMUwE10FrvRUybiAUABZ...	2010-09-23 10:19:17
http://ads.blueitium.com/iframe375/BaAFU_FgAMR2MAAAAAAF2GqAAAAAAqACOAIA...	2010-09-23 10:19:17
http://ad.yieldmanager.com/imp?_PVID=upQF2Hj8evlVvzobQTIqMUwE10FrvRUybiAUABZ...	2010-09-23 10:19:17
http://ad.yieldmanager.com/ist?_PVID=upQF2Hj8evlVvzobQTIqMUwE10FrvRUybiAUABZ3...	2010-09-23 10:19:09
http://ad.yieldmanager.com/ist?_PVID=upQF2Hj8evlVvzobQTIqMUwE10FrvRUybiAUABZ3...	2010-09-23 10:19:09
http://ad.yieldmanager.com/imp?_PVID=c25Rv9G%5RlqVzobQTIqMUwMJ0FrvRUybiAEAB...	2010-09-23 10:19:00
http://ad.doubleclick.net/ad/112988.159462.7724395949521/B4630459.18;sz=180...	2010-09-23 10:19:00
http://ad.yieldmanager.com/imp?_PVID=c25Rv9G%5RlqVzobQTIqMUwMJ0FrvRUybiAEAB...	2010-09-23 10:19:00
http://ad.doubleclick.net/ad/113285.yahoo.com/B2343920.470;sz=425x600;dcscpt=...	2010-09-23 10:19:00
http://ad.yieldmanager.com/ist?_PVID=c25Rv9G_RlqVzobQTIqMUwMJ0FrvRUybiAEAB_T...	2010-09-23 10:19:00
http://ad.yieldmanager.com/ist?_PVID=c25Rv9G_RlqVzobQTIqMUwMJ0FrvRUybiAEAB_T...	2010-09-23 10:19:00
http://ad.doubleclick.net/ad/113285.yahoo.com/B2343920.470;sz=425x600;dcscpt=...	2010-09-23 10:19:00
http://ad.yieldmanager.com/imp?_PVID=8e2oItG%5RlqVzobQTIqMUwDQGFrvRUybi%5f...	2010-09-23 10:18:55
http://ad.yieldmanager.com/imp?_PVID=8e2oItG%5RlqVzobQTIqMUwDQGFrvRUybi%5f...	2010-09-23 10:18:55
http://ad.yieldmanager.com/imp?_PVID=8e2oItG%5RlqVzobQTIqMUwDQGFrvRUybi%5f...	2010-09-23 10:18:55
http://ad.yieldmanager.com/imp?_PVID=8e2oItG%5RlqVzobQTIqMUwDQGFrvRUybi%5f...	2010-09-23 10:18:55
http://ad.yieldmanager.com/imp?_PVID=8e2oItG%5RlqVzobQTIqMUwDQGFrvRUybi%5f...	2010-09-23 10:18:55
http://ad.yieldmanager.com/imp?_PVID=8e2oItG%5RlqVzobQTIqMUwDQGFrvRUybi%5f...	2010-09-23 10:18:55
http://ad.yieldmanager.com/imp?_PVID=8e2oItG%5RlqVzobQTIqMUwDQGFrvRUybi%5f...	2010-09-23 10:18:55
http://ad.yieldmanager.com/imp?_PVID=8e2oItG%5RlqVzobQTIqMUwDQGFrvRUybi%5f...	2010-09-23 10:18:55

View URLs for the selected threat

Any URL in this list can be clicked to display the contents viewed by the end user.

Step E: Further investigate a user's activity

Now that you've identified the current trend of Internet activity on your network and targeted key participants engaging in undesired Internet usage, you can further investigate a specific end user's activity and then take the appropriate steps for disciplinary action.


To access Internet usage data for a single end user with a high score, return to the Gauge Ranking table by clicking the greyish-white Back button at the bottom left of the panel. Click the User Name link for that user to display the User Summary panel:

Gauge Name	Total
Bandwidth	12
All Categories	2
Illegal	0
Adult Content	0
Shopping	0
Security	0

View the user's gauge activity in the User Summary panel

A list of groups to which the user belongs displays to the left, and a list of gauges displays to the right, showing the user's score for each gauge.

To drill down and view activity in any gauge the user affected, select the gauge, and then click the Category View button at the bottom of the panel to display the Category View User panel (the panel shown in steps C and D in this section).

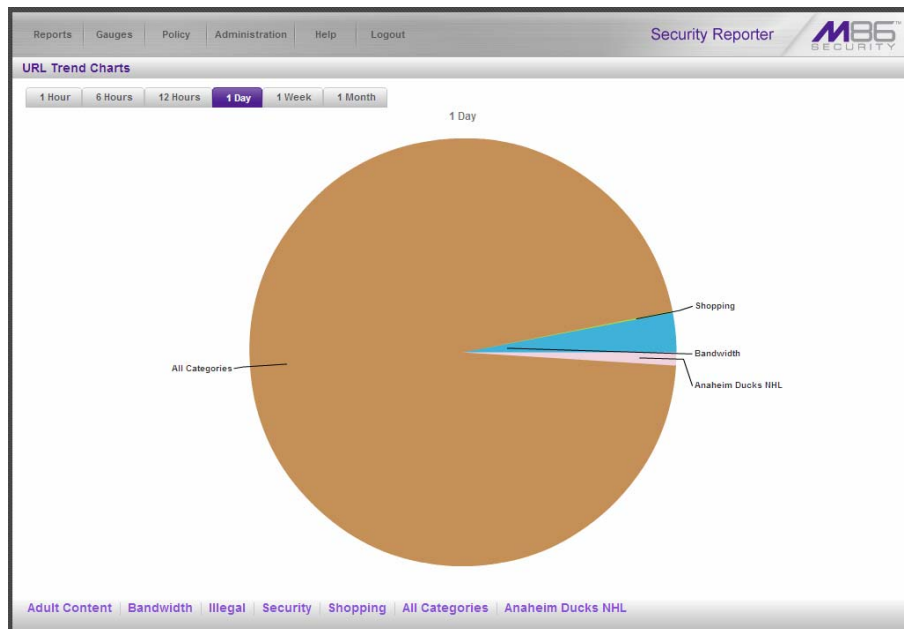
 **NOTE:** *There is also a way to automatically lock out the user that will be demonstrated later in this document.*

How to view URL Trend Reports

SR lets you generate historical trend reports that show activity by URL threats for a specified time period. These trend reports are helpful for monitoring improvement of activity in a certain library category as well as providing a good tool for setting appropriate thresholds for each URL gauge.

Step A: View overall activity in URL gauges

Navigate to **Reports > URL Trend Charts** to display the URL Trend Charts panel:



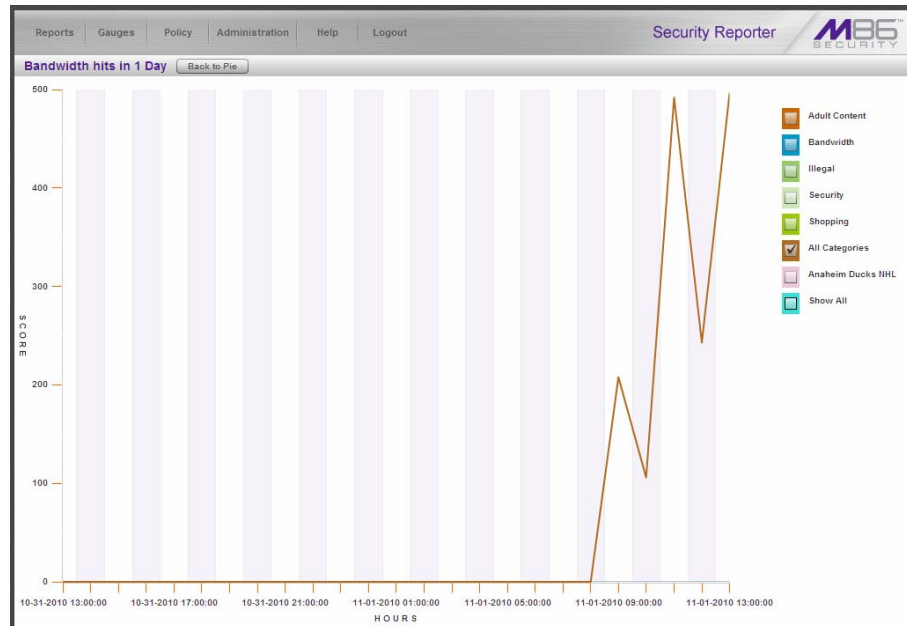
URL Trend Charts panel

The pie trend chart is divided into pie slices named for each gauge in which there was activity. The size of each slice is determined by the amount of activity in that gauge for the designated time period, in comparison to activity in all other URL gauges during that same time period. All activity is translated into a percentage figure, with the total activity for all slices equaling 100 percent.

You can change the time span represented in the trend chart by clicking one of five other tabs at the top of the chart. Choices range from the last hour to the last month of data.

Step B: View a line chart for a single URL gauge

To uncover more information about activity in a particular gauge, click the pie slice for that gauge to view a line chart depicting that gauge's activity within the specified time period:



View activity for a specified gauge

TIP: You can also go to the bottom of the pie chart and click a tab for a gauge to access the line chart for that gauge within the specified time period.

The score and minutes in which activity occurred display, represented by a line graph. The chart can be modified by clicking checkboxes to the right to include lines in the chart depicting activity in other gauges.

How to view a pie chart for a URL gauge

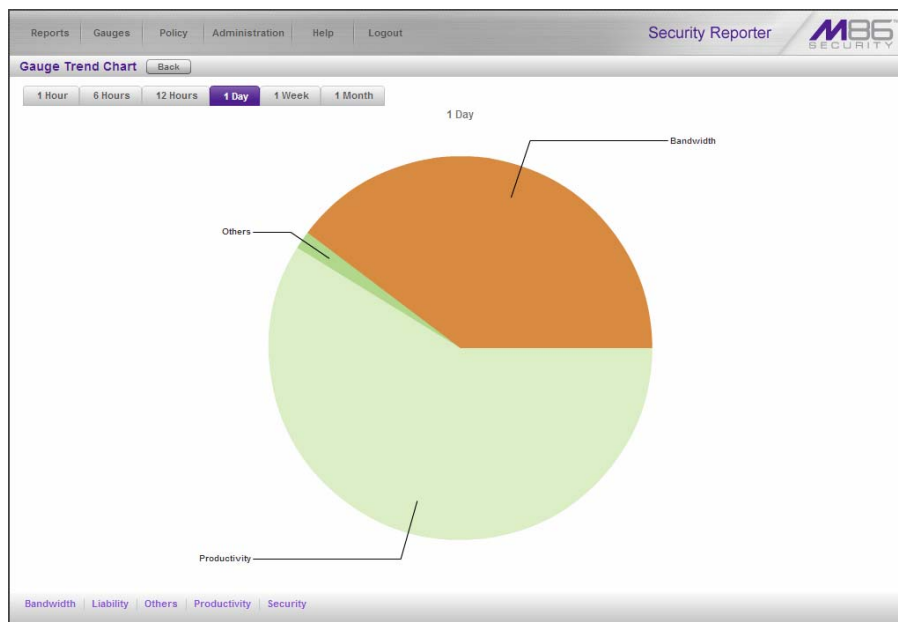
Now that you know how to access a pie trend chart showing overall gauge activity and how to drill down to view a line chart for a specific gauge, you will next learn how to access a pie chart for a specific gauge.

1. Go to the URL gauges Dashboard and click the middle icon at the bottom of the gauge:



The gauge Trend Charts icon

2. The action of clicking the Trend Charts icon displays a pie Gauge Trend Chart for that gauge:



Gauge Trend Chart

Note the pie slices in this trend chart are named for each gauge component in which there was activity.

The time span represented in the trend chart can be changed by clicking one of five other tabs at the top of the chart.

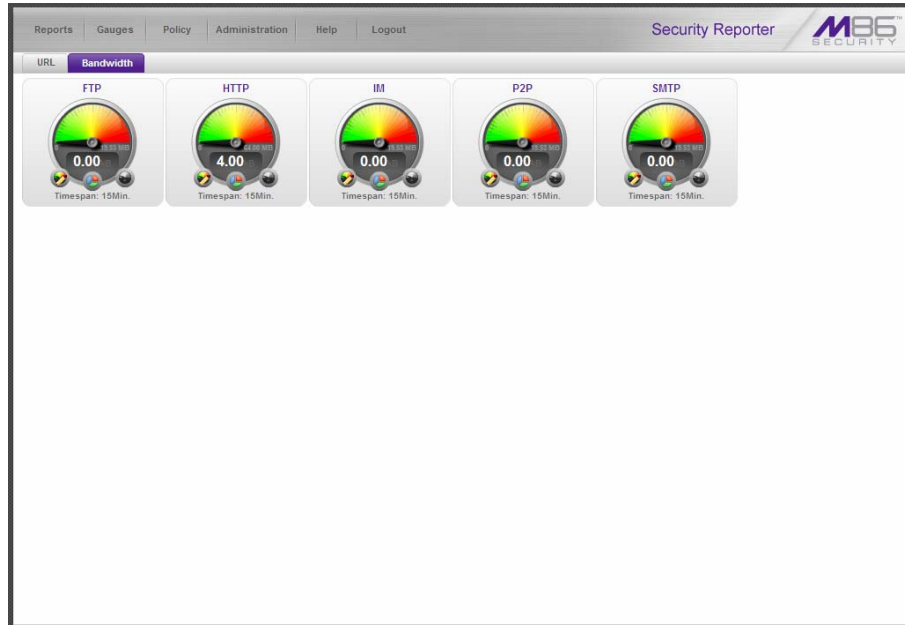
Click a pie slice or tab beneath the pie chart to drill down into that gauge component and view a line chart showing that gauge component's activity within the specified time period.

Monitor Bandwidth gauges

Once you've seen how URL gauges help you monitor end user Internet traffic, you will probably want to explore the ways bandwidth gauges help you monitor inbound and outbound bandwidth usage on your network.

How to view the Bandwidth gauges Dashboard

The bandwidth gauges Dashboard gives you an overview of current end user bandwidth activity on your network. To display this panel, first select **Gauges** and then click the Bandwidth tab above the Dashboard:



Bandwidth gauges Dashboard

Default bandwidth gauges include the following protocol gauges: FTP, HTTP, IM, P2P and SMTP. Protocol gauges are comprised of ports. For example, the FTP protocol includes ports 20 and 21.

Note the score in the middle of each gauge. This score shows the amount of bandwidth traffic in bytes (kB, MB, GB).

As with URL gauges, from this panel you can drill down to view end user activity in a bandwidth gauge and view trend charts on bandwidth gauge activity.

How to drill down into a Bandwidth gauge

Looking at the bandwidth gauges Dashboard, you can see at a glance which bandwidth gauge has the highest score. To identify the end users affecting that gauge, you will need to drill down into that gauge.

Step A: View Bandwidth protocol traffic information

In the bandwidth gauges Dashboard, click a high-scoring gauge to display the Gauge Ranking table showing all end user traffic for that protocol:

User Name	110	25	Total
192.168.20.77	0.00 kB	3.00 kB	3.00 kB

View bandwidth used by each end user for the protocol

To the right of the User Name column are port numbers that comprise the protocol. The number of bytes of bandwidth used by each user displays in these columns.

Step B: View a user’s protocol usage information

To drill down and view a user’s bandwidth usage in all bandwidth gauge protocols, click a User Name to display the User Summary panel.

In the Gauge Readings frame to the right side in this panel, click the Bandwidth Gauges tab to display each bandwidth Gauge Name and its corresponding Inbound, Outbound, and Total bytes of traffic used by that end user for that gauge:

The screenshot shows the 'User Summary' panel for user 192.168.20.77. It features a 'Group Membership' list on the left and a 'Gauge Readings' table on the right. The 'Gauge Readings' table is titled 'Bandwidth Gauges' and displays data for various protocols.

Gauge Name	Inbound	Outbound	Total
HTTP	3.00 kB	1.00 kB	4.00 kB
SMTP	1.00 kB	2.00 kB	3.00 kB
FTP	0.00 kB	0.00 kB	0.00 kB
P2P	0.00 kB	0.00 kB	0.00 kB
IM	0.00 kB	0.00 kB	0.00 kB

At the bottom right of the table, the 'Score Total' is displayed as 7.00 kB.

User Summary panel showing the user's bandwidth protocol usage

Step C: View a user's port usage information

Now drill down and view a user's port usage for a particular gauge. In the Gauge Readings frame, click the Gauge Name to activate the **Category View** button. Click that button to display the Category View User panel:

The screenshot shows the 'Category View User' panel for user 192.168.20.77, specifically for the HTTP gauge. It displays a table of port usage categories.

Ports	Inbound	Outbound	Total
443	3.00 kB	1.00 kB	4.00 kB

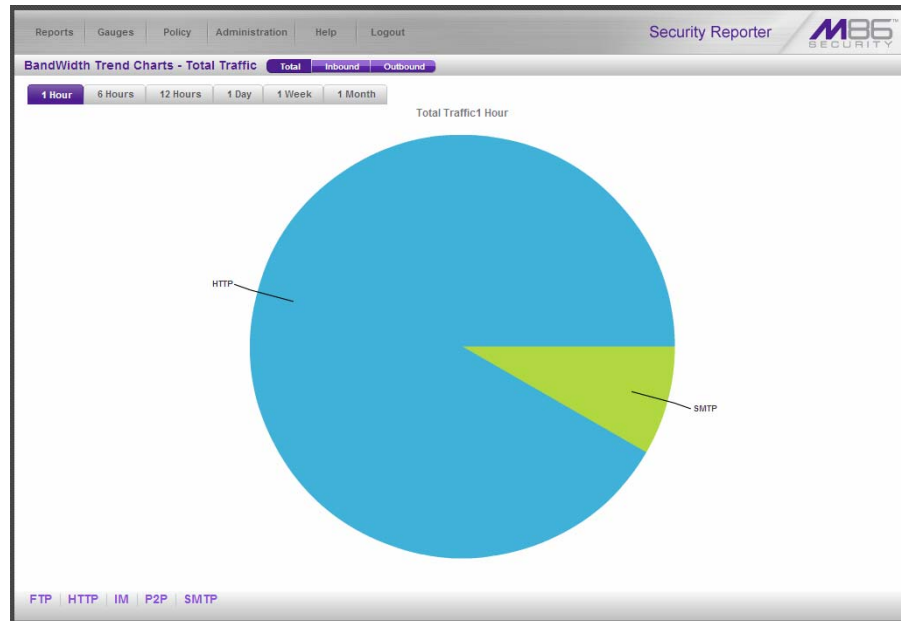
Category View User panel showing the user's port usage

How to view *Bandwidth Trend Chart* activity

As you have seen with URL gauges, in addition to drilling down into a gauge to find out which end users are driving that gauge's activity, you can get an overall picture of a bandwidth gauge's current activity by generating a trend chart.

Step A: View overall activity in Bandwidth gauges

Navigate to **Reports > Bandwidth Trend Charts** to display the BandWidth Trend Charts panel:




BandWidth Trend Charts panel

The pie trend chart is divided into pie slices named for each bandwidth gauge in which there was activity. The size of each slice is determined by the amount of activity in that gauge for the designated time period, in comparison to activity in all other bandwidth gauges during that same time period. All activity is translated into a percentage figure, with the total activity for all slices equaling 100 percent.

You can change the time span represented in the trend chart by clicking one of five other tabs at the top of the chart. Choices range from the last hour to the last month of data.

Step B: View a line chart for a single Bandwidth gauge

To learn more about the activity for a particular gauge, click the pie slice for that gauge to view a line chart depicting that gauge's activity within the specified time period:

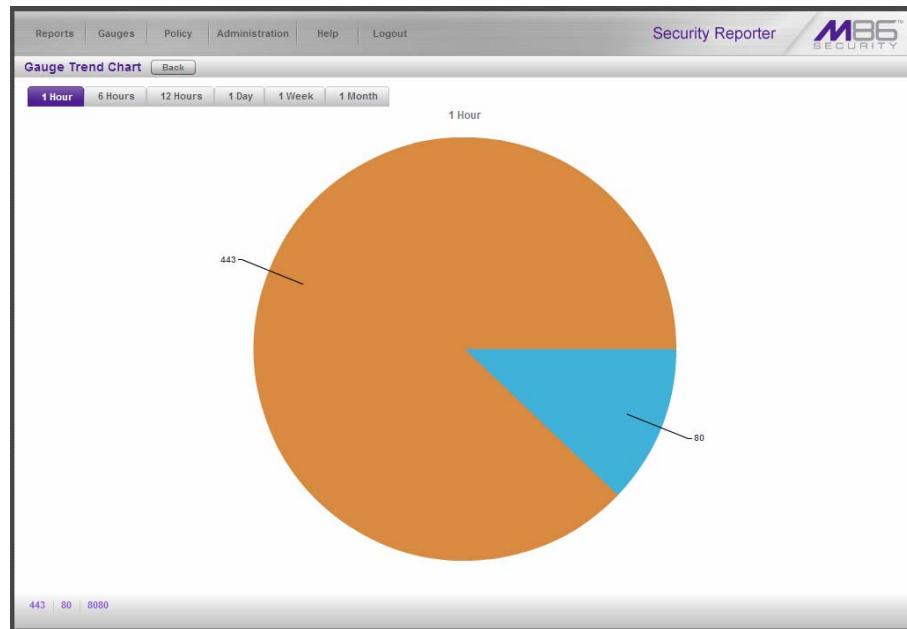
 **NOTE:** The "score" on bandwidth gauges is based on the number bytes of bandwidth consumed; not page hits, as with URL gauges.



Line chart for a bandwidth gauge

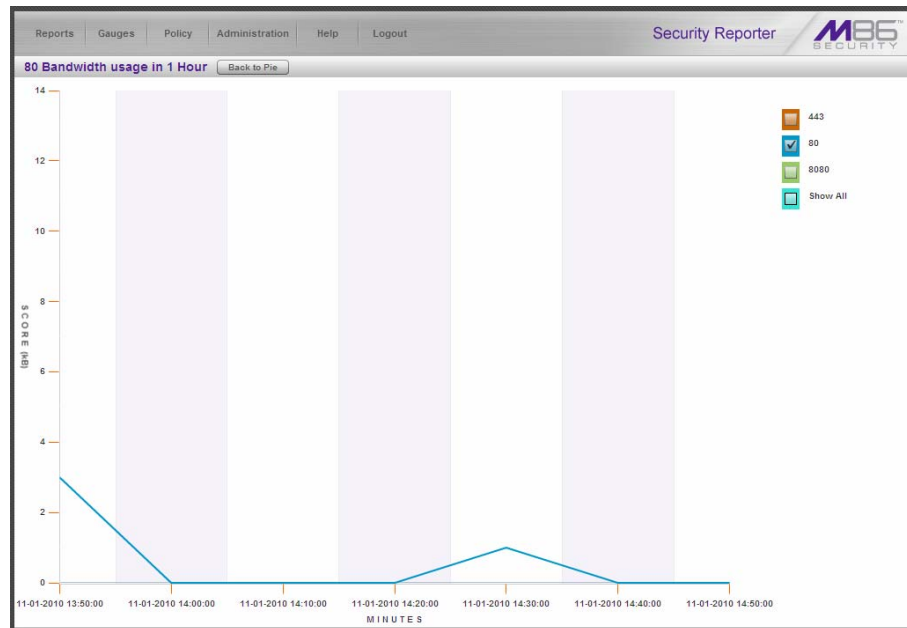
How to view charts for a specific Bandwidth gauge

In the bandwidth gauges Dashboard, click the Trend Charts icon in the bottom middle of the gauge to display a pie trend chart for that gauge:



Bandwidth Gauge Trend Chart for a specified protocol (HTTP)

Click the pie slice or tab below to view a line chart showing traffic for that port:



Line chart for a specified port

Get the complete picture

As you have seen so far, the real time reporting section of the SR user interface lets you monitor URL and bandwidth gauge activity on your network. Analyzing data from both sources will give you a complete picture of the user's Internet usage behavior.

How to view Overall Ranking of user activity

The first step in finding out which end users are most actively driving gauges is to consult the Overall Ranking table that shows you a list of users affecting URL gauges and Bandwidth gauges, all in one panel. This ranking table is accessed by navigating to **Gauges > Overall Ranking**:

URL		Bandwidth	
User Name	Score	User Name	Score
192.168.200.201	2967	192.168.168.71	5.54 MB 586 kB
192.168.200.45	1015	192.168.200.163	590 kB 176 kB
192.168.30.170	883	192.168.200.31	679 kB 80 kB
192.168.30.177	507	192.168.41.1	349 kB 71 kB
192.168.30.33	221	192.168.30.85	261 kB 16 kB
192.168.20.204	185	192.168.200.208	147 kB 102 kB
192.168.200.31	166	192.168.30.86	149 kB 51 kB
192.168.41.1	104	192.168.20.143	81 kB 21 kB
192.168.30.85	34	192.168.30.80	74 kB 16 kB
192.168.200.208	14	192.168.200.66	56 kB 22 kB
192.168.30.86	10	192.168.200.225	10 kB 65 kB
192.168.20.143	9	192.168.30.84	56 kB 17 kB
192.168.30.80	8	192.168.200.95	19 kB 40 kB
192.168.200.86	7	192.168.200.90	48 kB 9 kB
192.168.200.225	4	192.168.200.131	32 kB 18 kB
192.168.30.84	1	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	8 kB 6 kB
		192.168.30.33	6 kB 1 kB
		192.168.20.204	6 kB 1 kB
		192.168.20.212	5 kB 1 kB

Overall Ranking table

Note the URL frame to the left includes the User Name and Score of each user with activity in one or more URL gauges. The Bandwidth frame to the right includes the User Name and number of bytes of Inbound and Outbound traffic used by that end user in one or more bandwidth gauges. Users listed in each frame are ranked in order by their scores.

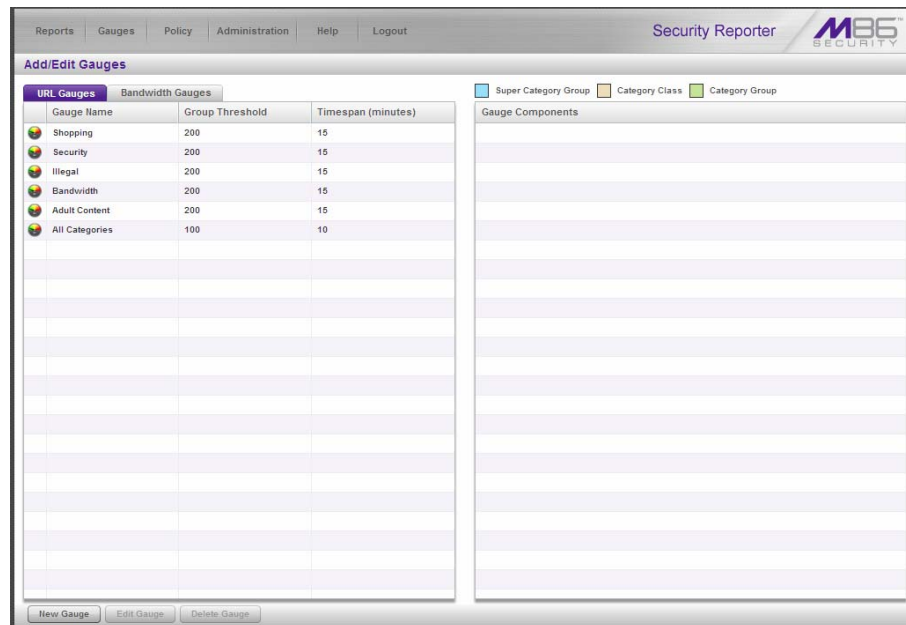
Clicking a User Name link takes you to the User Summary panel where more details about that end user's activity can be viewed, and action can be taken to restrict or prevent that end user's Internet/network activities.

How to create a New Gauge

After working with the URL and bandwidth gauges for awhile, you may want to customize the default gauges or create your own to more effectively monitor the type of traffic on your network.

Step A: Select Add/Edit Gauges

In order to create a new custom gauge, navigate to **Gauges > Add/Edit Gauges** to display the panel by that name:



Select Add/Edit Gauges

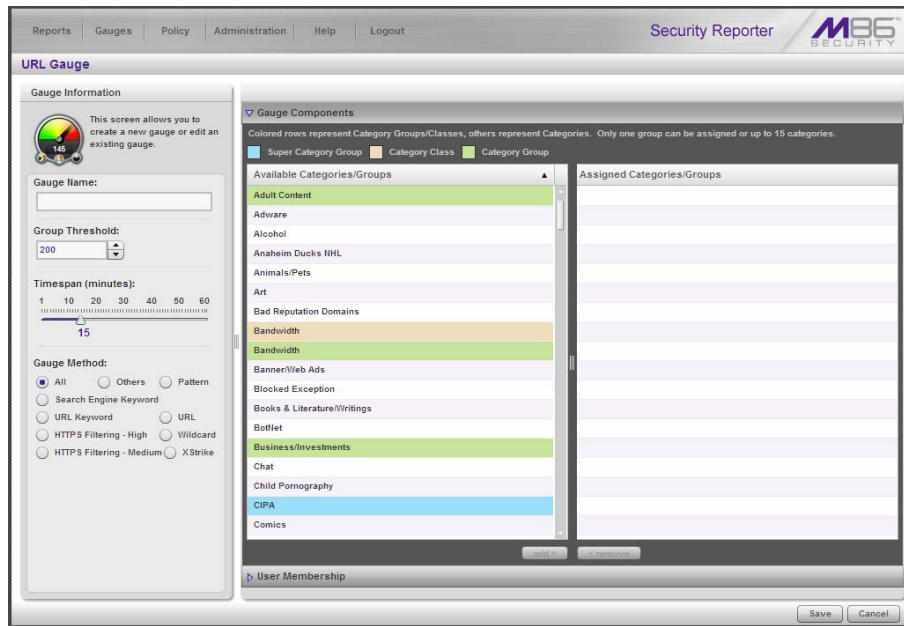
By default the URL Gauges tab displays, showing the list of URL gauges in the frame to the left. If you wish to create a bandwidth gauge, click the Bandwidth Gauges tab to display the list of bandwidth gauges in this frame.

Note that only five bandwidth gauges can be used at a time. If you wish to create a bandwidth gauge, an existing bandwidth gauge must first be deleted.

Step B: Add a New Gauge

Click the **New Gauge** button to display the URL Gauge or Bandwidth Gauge panel, as appropriate to the selection made in the previous panel.

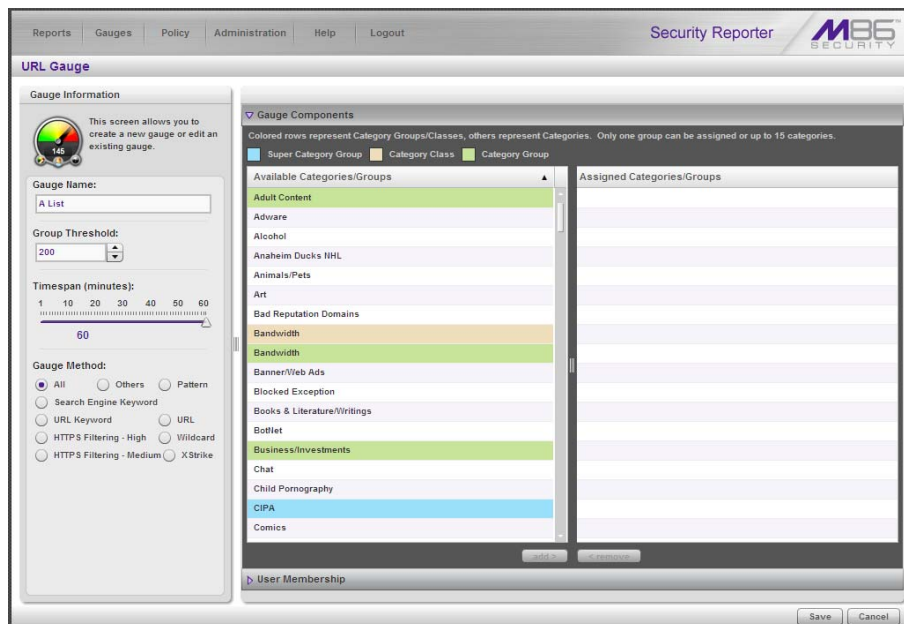
This is an example of the URL Gauge panel:



Add a New URL Gauge

Step C: Specify Gauge Information

Set parameters for the custom gauge by making the following entries/selections in the Gauge Information frame at the left side of the panel:

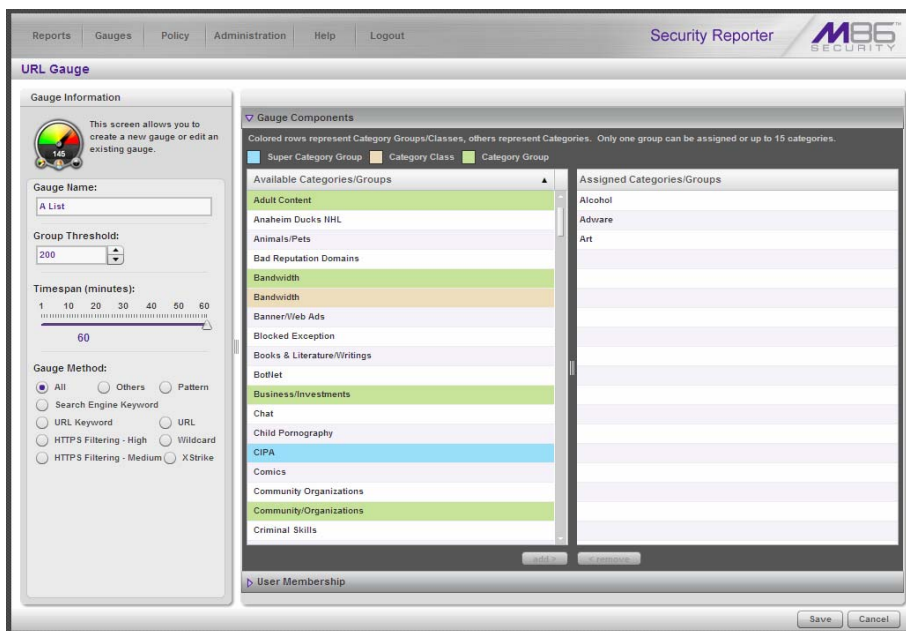


Define Gauge Information and Gauge Components in the URL Gauge panel

In the URL Gauge panel, do the following:

1. Type in a name in the **Gauge Name** field.
2. Leave the **Group Threshold** value at '200'.
3. Set a **Timespan** of '60' minutes by moving the slider tool to the right.
4. Leave the **Gauge Method** as 'All'.

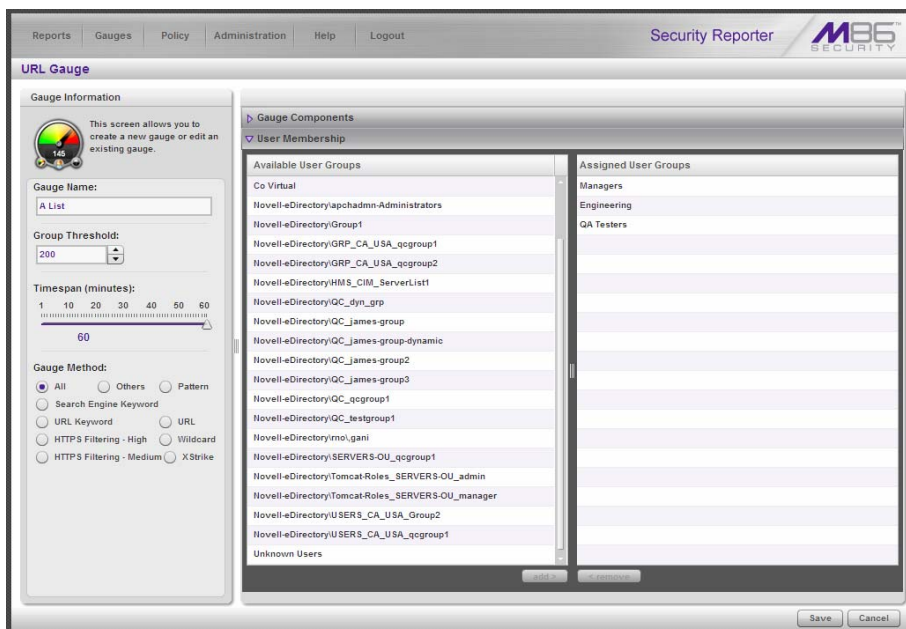
- In the Gauge Components accordion at the right side of the panel, go to the Available Categories/Groups box and move the “Adware”, “Alcohol” and “Art” selections into the Available Categories/Groups list box by selecting each category and then clicking the **add >** button.



Define Gauge Information and Gauge Components

Step D: Select users to be monitored by the gauge

- Click the User Membership accordion (located beneath the Gauge Components accordion) to open it:




Select users to be monitored by this gauge (sample URL Gauge panel)

- From the Available User Groups box, choose the user groups whose activity will be monitored by this gauge, and then click the **add >** button.

Step E: Save gauge settings

Once you click **Save**, the Add/Edit Gauges panel redisplay and includes the Gauge Name of the gauge you just added. Your new gauge is now ready to show traffic.

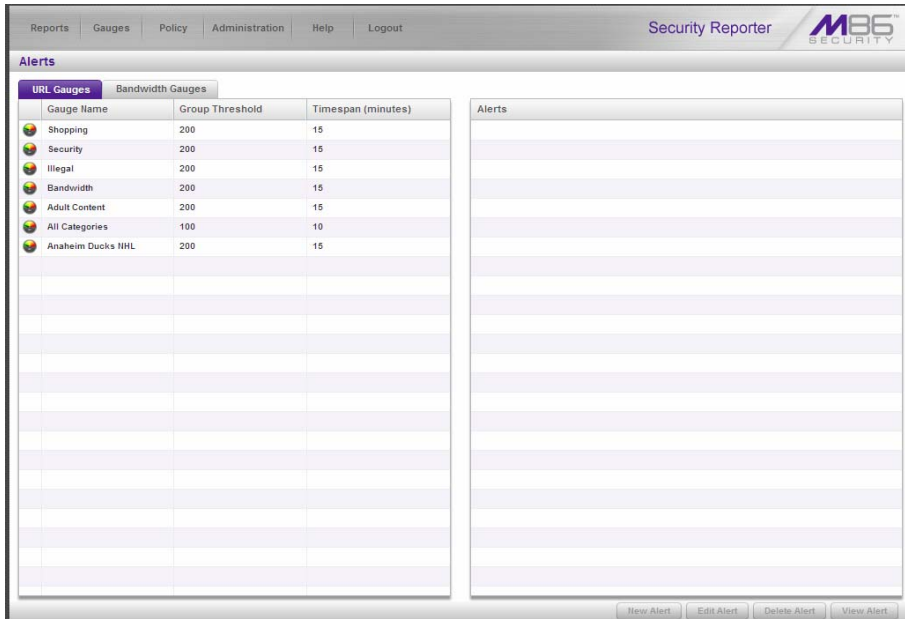
 **NOTE:** The initial gauge setup may take a few minutes. Once setup is complete, the gauge will report data in real time.

How to create an automated gauge alert

This section will step you through the process of creating an automated threshold per user, so you can be automatically notified via email and the violating user will be automatically locked out once a threshold is exceeded.

Step A: Set up a new alert

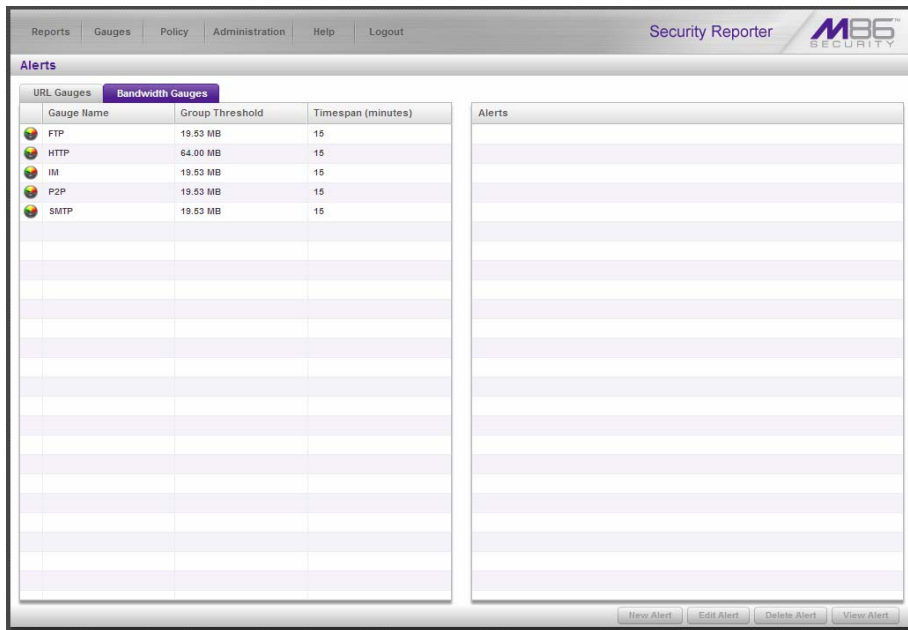
1. Navigate to **Policy > Alerts** to display the panel by the same name:



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

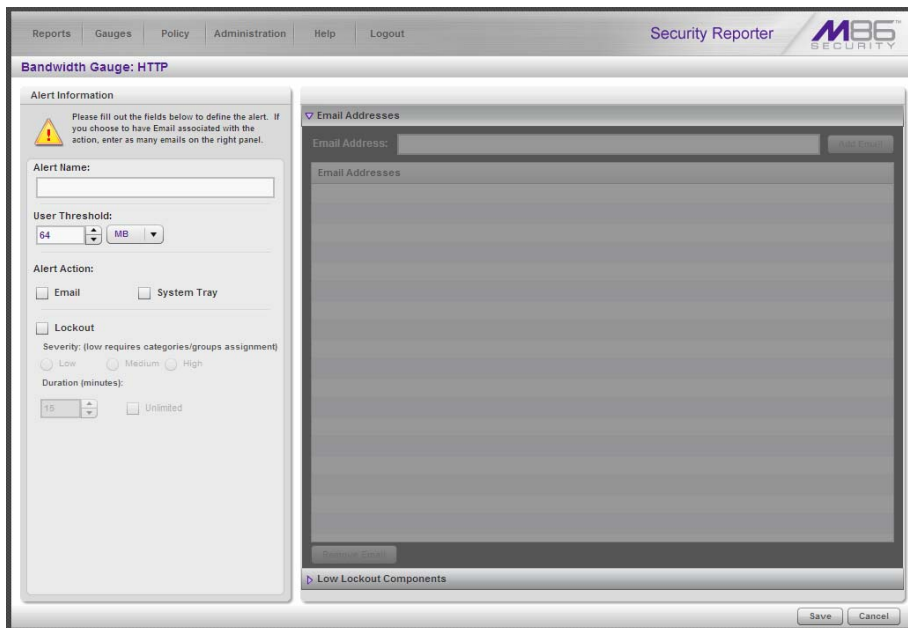
Select the Alerts option (sample Alerts panel with URL Gauges tab selected)

2. By default the URL Gauges tab displays, showing all gauges currently in use. To create an alert for bandwidth gauges, click the Bandwidth Gauges tab:



Select the Alerts option (sample Alerts panel with Bandwidth Gauges tab selected)

3. Choose the Gauge Name from the list in the left side of the panel, and then click **New Alert** to display the next panel where you set parameters for the alert:



Add a New Alert (sample Bandwidth Gauges panel)

Step B: Specify Alert Information

Set parameters for the alert by making the following entries/selections in the Alert Information frame at the left side of the panel:


The screenshot shows the 'Security Reporter' interface with the 'Alert Information' panel for a 'Bandwidth Gauge: HTTP' alert. The panel includes the following fields and options:

- Alert Name:** HTTP Bandwidth Gauge Alert
- User Threshold:** 64 MB
- Alert Action:**
 - Email
 - System Tray
 - Lockout
- Severity:** (low requires categories/groups assignment)
 - Low
 - Medium
 - High
- Duration (minutes):** 15
 - Unlimited

The 'Email Addresses' panel on the right is empty, with an 'Add Email' button at the top right. At the bottom of the panel, there are 'Save' and 'Cancel' buttons.

Specify Alert Information (sample Bandwidth Gauges panel)

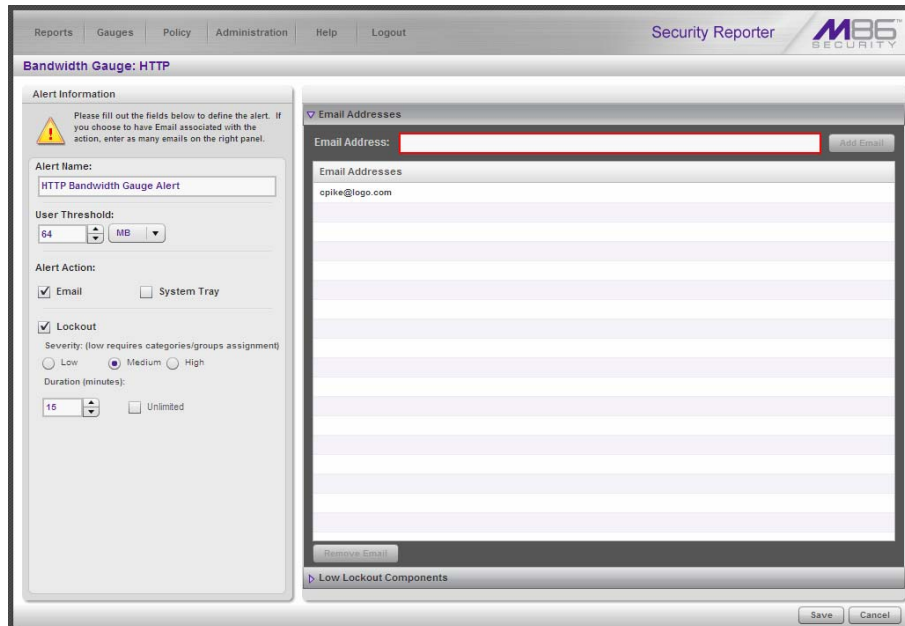
1. Type in a name in the **Alert Name** field.
2. Specify the **User Threshold** value. This numeric value is the number of times each user will be allowed to visit categories monitored by the gauge before triggering an alert.
3. Enable **Alert Action** checkboxes for “Email” and “Lockout.”
4. Select a **Severity** level (“Low”, “Medium”, or “High”). This section is only enabled when the Lockout checkbox is selected.
 - For a URL gauge, a “Low” selection will lock out the user by the categories monitored by the specified URL gauge only. For a bandwidth gauge, a “Low” selection will lock out the user by the protocols or ports monitored by the specified bandwidth gauge.
 - A “Medium” selection will lock out the user from Internet access altogether.
 - A “High” selection will lock out the users from all network protocols, so they cannot access the Internet, send e-mails, use instant messaging, or use P2P or FTP.

 **NOTES:** Time-based lockouts can be set for a range of 30 minutes, one hour to eight hours, or unlimited.

System Tray will not be shown in this demo, but if this feature is enabled, the administrator with an LDAP username, password and domain will see a system tray alert in the desktop system tray when an alert has been triggered. This applies to Active Directory environments only.

Step C: Specify criteria in the right side of the panel

If the Email Addresses accordion is closed, click to open it. Type in an **Email Address** and click the **Add Email** button. This is the address of the person who will be notified when an alert is triggered. You can add multiple email addresses.



The screenshot displays the 'Bandwidth Gauge: HTTP' configuration window in the Security Reporter. The interface is divided into two main sections. On the left, the 'Alert Information' section includes a warning icon and instructions to fill out fields. Fields include 'Alert Name' (set to 'HTTP Bandwidth Gauge Alert'), 'User Threshold' (set to '04 MB'), 'Alert Action' (with 'Email' and 'System Tray' checkboxes, 'Email' is checked), 'Lockout' (with 'Low', 'Medium', and 'High' radio buttons, 'Medium' is selected), and 'Duration (minutes)' (set to '15' with an 'Unlimited' checkbox). On the right, the 'Email Addresses' section features an 'Email Address' input field (highlighted with a red box) and an 'Add Email' button. Below the input field is a list box containing the email address 'cpike@logo.com'. At the bottom of the window are 'Save' and 'Cancel' buttons.

Specify email criteria (sample Bandwidth Gauges panel)

For a URL gauge alert, if a “Low” Lockout was specified, click the Low Lockout Components accordion to open it. Go to the Available Categories/Groups list box and move your selection(s) into the Assigned Categories/Groups list box by selecting each category and then clicking the **add >** button.

Step D: Save the alert

Click **Save** to save your settings and to display the Alerts panel with the new alert added.

SECTION 3: SECURITY REPORTS

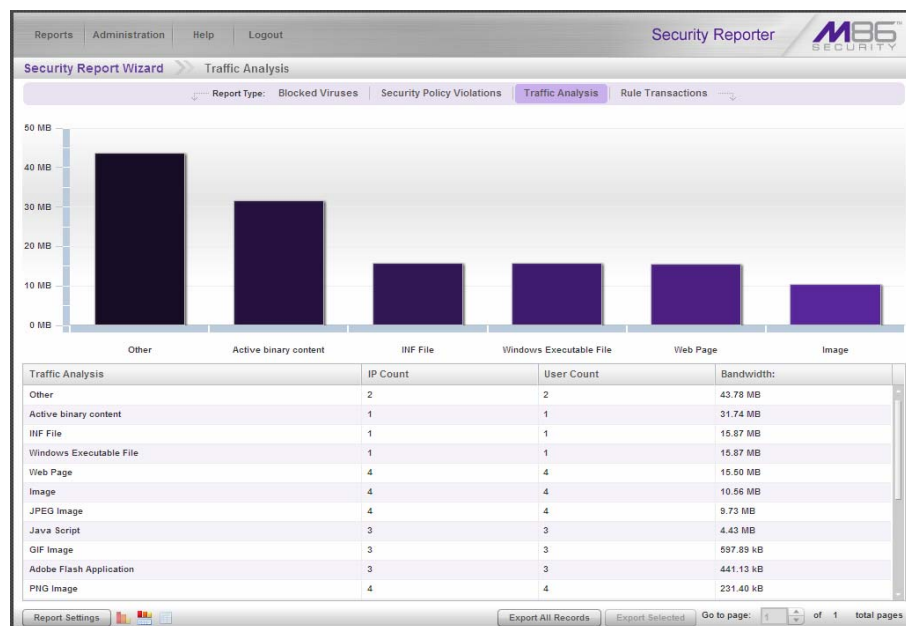
Security reporting features are available if using an SWG with your Security Reporter.

Understand the most common and useful features

This section of the Evaluation Guide supplies the evaluator information on employing basic tools in the Security Reporter to generate security reports using log feeds of an SWG appliance running software versions 9.2.x and higher. You will learn how the flexibility of the security report views lets you display different report types without switching to another panel, or readily access the Report Wizard to modify the current report view. As with productivity reports, security reports generated in the Security Reporter are easily customizable and can be saved, exported, or scheduled to run on a regular basis.

Use security reports for a view of network activity

The four basic security report types—Blocked Viruses, Security Policy Violations, Traffic Analysis, and Rule Transactions—are accessible via **Reports > Security Reports**. Each report type provides a bar chart showing the top six security offenders for the given report. This at-a-glance information lets you see which areas of the network need to be safeguarded most:




Rule Transactions security report

The four security report types contain the following information:

- **Blocked Viruses** - Includes details for each instance of each blocked virus detected from end user Internet/network activity.
- **Security Policy Violations** - Provides information on each instance in which an end user breached a security policy.

- **Traffic Analysis** - Shows activity for end user access of objects utilizing an excessive amount of network bandwidth.
- **Rule Transactions** - Includes each instance in which an end user triggered a threshold in an SWG Security Policy.

For each report type, by default the top portion of the report view includes tabs for all security Report Types. Beneath these tabs, a bar chart depicts the first six records for the current report type.

 **TIPS:** Clicking one of the Report Type tabs takes you to that report type.

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.

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


How to modify the current report view

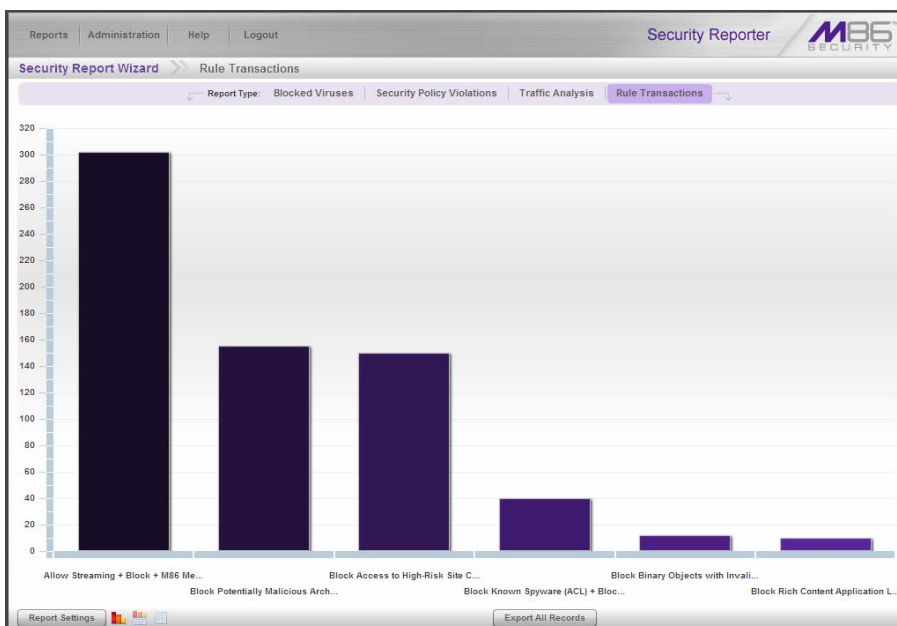
Page navigation tool

If more than one page is included in the report, the **Go to page 'x' of 'x' total pages** field at the bottom right of the panel lets you specify the page number to display in the report view, using the designated page range for reference.



Report view icons

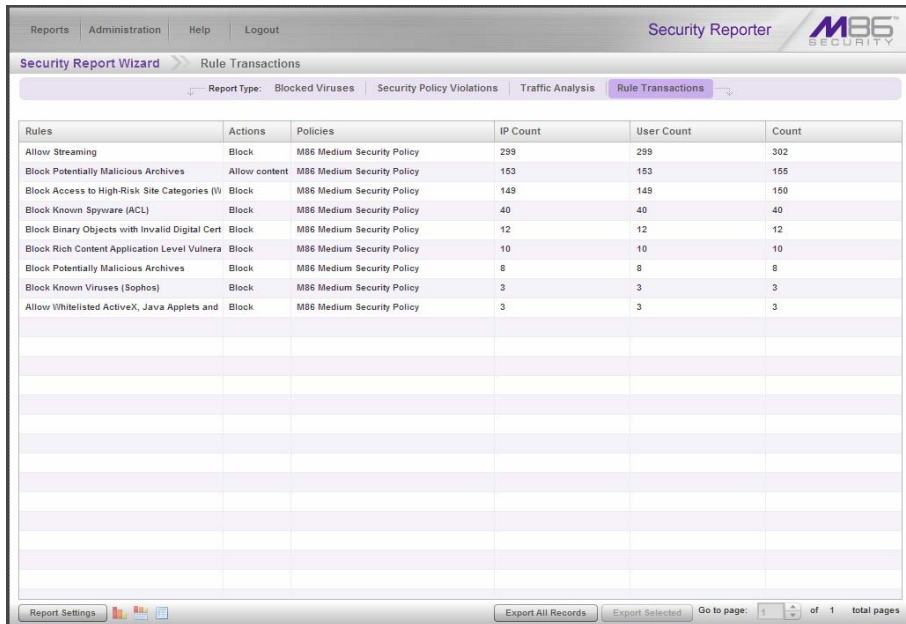
Icons at the bottom left of the panel let you view either chart or record data in the current report view:

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



Sample top six bar chart view

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



Rules	Actions	Policies	IP Count	User Count	Count
Allow Streaming	Block	M86 Medium Security Policy	299	299	302
Block Potentially Malicious Archives	Allow content	M86 Medium Security Policy	153	153	155
Block Access to High-Risk Site Categories (IV)	Block	M86 Medium Security Policy	149	149	150
Block Known Spyware (ACL)	Block	M86 Medium Security Policy	40	40	40
Block Binary Objects with Invalid Digital Cert	Block	M86 Medium Security Policy	12	12	12
Block Rich Content Application Level Vulnera	Block	M86 Medium Security Policy	10	10	10
Block Potentially Malicious Archives	Block	M86 Medium Security Policy	8	8	8
Block Known Viruses (Sophos)	Block	M86 Medium Security Policy	3	3	3
Allow Whitelisted ActiveX, Java Applets and	Block	M86 Medium Security Policy	3	3	3

Sample records only view

Create a customized security report

In addition to using one of the four basic security reports, you can generate a customized security report containing content relevant to the area of your network you wish to target.

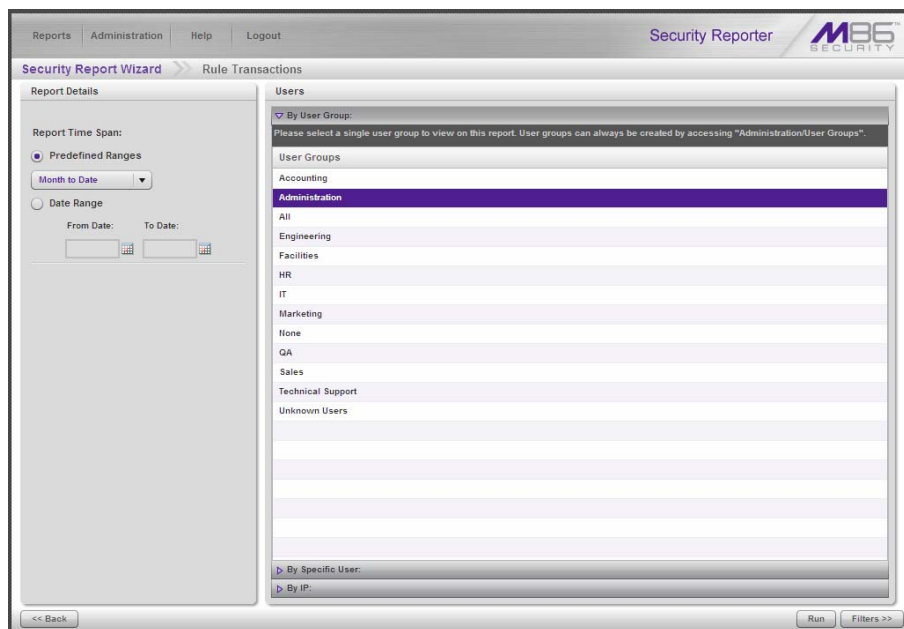
How to generate a customized security report

There are two methods for creating a customized security report. One method is by using the Report Settings' Run feature, and the other method is by generating a report view using the Report Wizard.

Step A: Choose a Run option

Option 1: Report Settings' Run feature

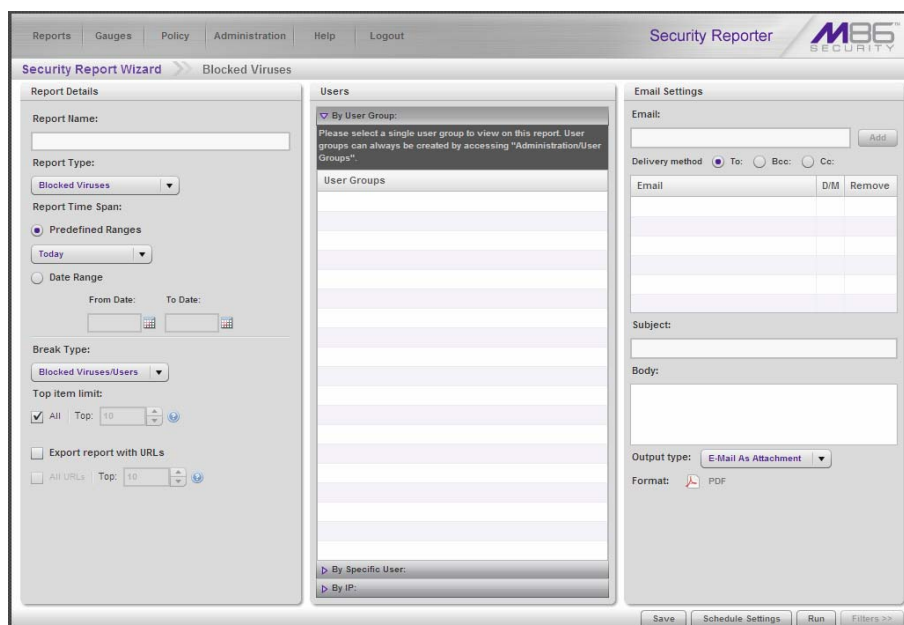
In the security report view, mouse over **Report Settings** and choose **Run** to display the Security Report Wizard panel for that report:



Report Settings Run option

Option 2: Report Wizard's Run feature

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



Security Report Wizard panel

Step B: Populate the Report Details frame

1. In the Report Details frame, if using the Report Wizard to create the report, choose the **Report Type** from the pull-down menu (“Blocked Viruses”, “Security Policy Violations”, “Traffic Analysis”, “Rule Transactions”); by default “Blocked Viruses” displays.
2. Specify the **Report Time Span** by choosing one of two options:
 - **Predefined Ranges** - If using the Report Wizard to create and run a new report, this option is selected by default. If choosing this option, make a selection from the pull-down menu: “Today” (default), “Month to Date”, “Year to Date”, “Yesterday”, “Month to Yesterday”, “Year to Yesterday”, “Last Week”, “Last Weekend”, “Current Week”, “Last Month”.
 - **Date Range** - If using the Report Settings’ Run feature, this option is selected by default. If choosing this option, use the calendar icons to set the date range.
3. If using the Report Wizard to create the report:
 - a. Specify the **Break Type** from the available choices in the pull-down menu.
 - b. 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.
 - c. By default, **Export report with URLs** is de-selected. Click this checkbox to select this option, and then specify the number of URLs to export:
 - **All URLs** - Check this checkbox to export all URLs
 - **Top** - Specify the number of top URLs to be exported

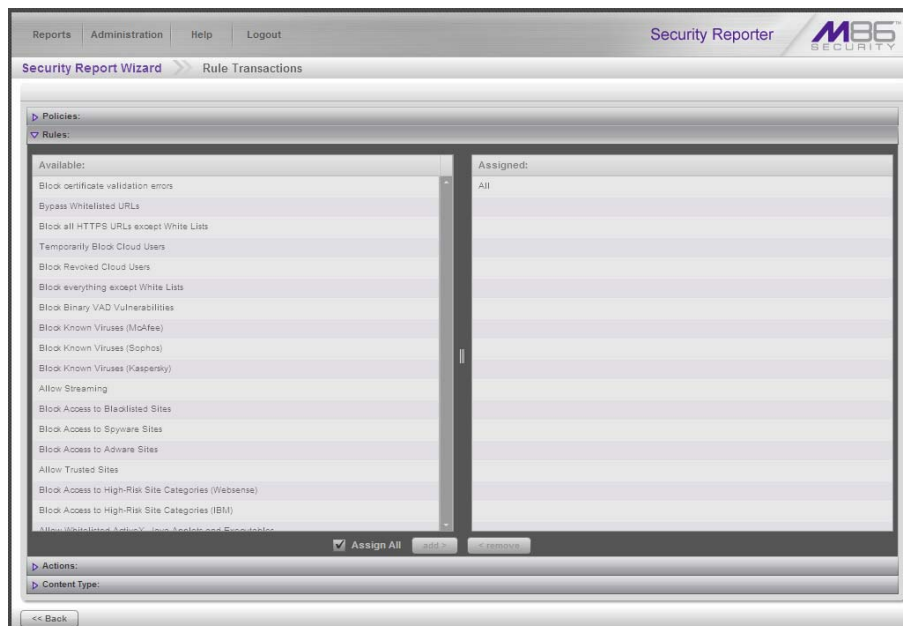
Step C: Use accordions in the Users frame

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:

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

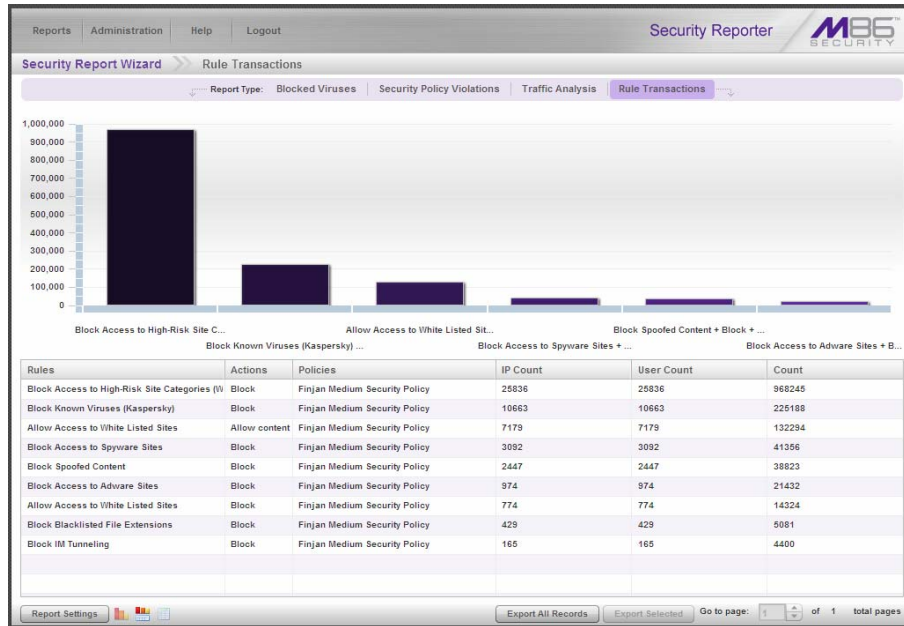


Report Filters option

2. Choose a filter type from an available accordion (Policies, Rules, Action, Content Type) and indicate criteria to use in the filter:
 - Select one or more records from the Available list box and click **add >** to move the record(s) to the Assigned list box.
 - Click the “Assign All” checkbox to select all records and grey-out the panel.
3. Click **<< Back** to return to the Security Report Wizard panel.

Step D: Run the report

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



Generated Security Report view

The report can now be exported by selecting one of the two export options.

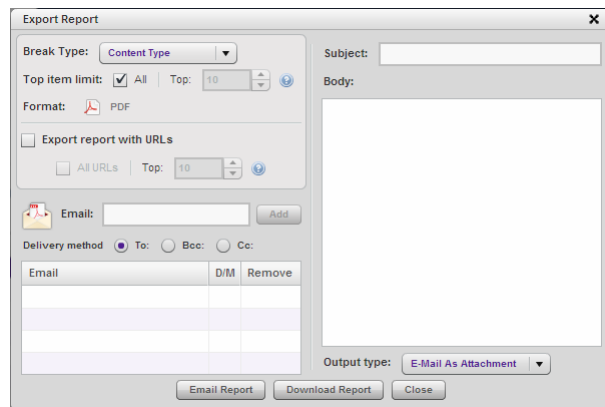
Capture the security report in PDF format

How to export current report view data

From the current report view, you can select specified records or all records to be exported in the PDF format, and then download or email the PDF on demand.

Step A: Specify records to include in the report

In the current report view, select the records to be included in the report by either clicking **Export All Records**, or choosing specific records from the table and then clicking **Export Selected**. Clicking either button opens the Export Report pop-up window:



Export Report pop-up window

Step B: Specify Break Type and URL limitation criteria

1. In the Export Report pop-up window, specify the **Break Type** 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. To modify this selection, uncheck this box and specify the **Top** number of items to be included in the exported report.
3. By default, **Export report with URLs** is de-selected. Click this checkbox to select this option, and then specify the number of URLs to export:
 - **All URLs** - Check this checkbox to export all URLs
 - **Top** - Specify the number of top URLs to be exported

Step C: Download or email the report

Now you must choose whether to download or email the report.

Option 1: Download the report

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

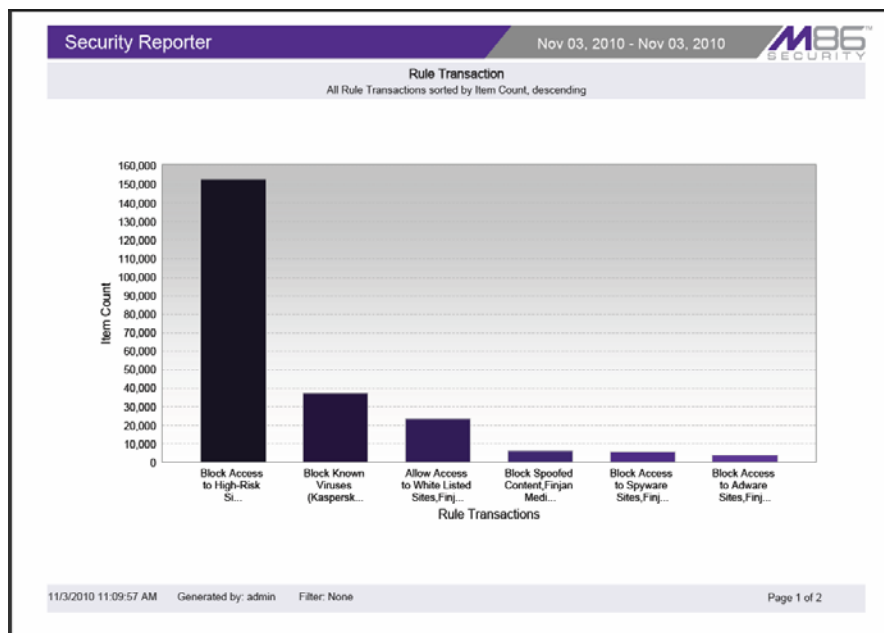
Option 2: Email the report

To email the report:

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".
3. Enter the **Subject** for the email message.
4. If you wish, enter text to be included in the **Body** of the message.
5. Specify the **Output type** for the email: "E-Mail As Attachment" or "E-Mail As Link".
6. Click **Email Report** to send the email to the specified recipient(s).

Security Report format

The generated Security Report PDF file includes the following information:



Sample PDF for Rule Transaction Security Report, page 1

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

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), Filter information, and Page number and page range.

The body of the first page of the report includes a bar chart showing the top six graphs with count indicators, and the report name.

The body of pages following the first page of the report includes the report name and list of records with the corresponding Item Count for each record. For break type reports, the Total displays at the end of each section.

For non-break type Rule Transaction reports, Policy and Action column data precede Item Count column data.

At the end of the report, the Grand Total displays for all records. For Rule Transaction reports, the total Count displays beneath the Grand Total.

Security Reporter		Nov 03, 2010 - Nov 03, 2010		M86 SECURITY
Rule Transaction				
All Rule Transactions sorted by Item Count, descending				
Rule Transactions	Policy	Action	Item Count	
Block Access to High-Risk Site Categories (Websites)	Finjan Medium Security Policy	Block	153,283	
Block Known Viruses (Kaspersky)	Finjan Medium Security Policy	Block	37,540	
Allow Access to White Listed Sites	Finjan Medium Security Policy	Allow content and scan containers	23,454	
Block Spoofed Content	Finjan Medium Security Policy	Block	6,175	
Block Access to Spyware Sites	Finjan Medium Security Policy	Block	5,646	
Block Access to Adware Sites	Finjan Medium Security Policy	Block	3,944	
Allow Access to White Listed Sites	Finjan Medium Security Policy	Block	2,481	
Block IM Tunneling	Finjan Medium Security Policy	Block	903	
Block Blacklisted File Extensions	Finjan Medium Security Policy	Block	638	
Grand Total			234,035	
Count: 9				

11/3/2010 11:09:57 AM Generated by: admin Filter: None Page 2 of 2

Sample PDF for Rule Transaction Security Report, page 2

Save the security report you generated

How to save a security report

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

Step A: Select Report Settings, Save option

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

The screenshot displays the Security Reporter interface with the Security Report Wizard panel open. The panel is titled "Security Report Wizard" and "Rule Transactions". It is divided into three main sections:

- Report Details:** Includes a "Report Name" field, "Report Time Span" options (Predefined Ranges or Date Range), "Break Type" (Rules/Users), and "Top item limit" (All, Top: 10).
- Users:** A list of user groups with "All" selected. The list includes: User Groups, Accounting, Administration, All, Co Virtual, Engineering, Facilities, HR, IT, Marketing, None, QA, Sales, Technical Support, and Unknown Users.
- Email Settings:** Includes "Email" field, "Delivery method" (To, Bcc, Cc), "Subject", "Body", "Output type" (E-Mail As Attachment), and "Format" (PDF).

At the bottom of the panel, there are buttons for "<< Back" and "Save", along with a "Filters >>" button.

Report Settings Save option

Step B: Specify criteria in the Report Details frame

1. In the Report Details frame, type in the **Report Name**.
2. Specify the **Report Time Span** by choosing one of two options:
 - **Predefined Ranges** - If choosing this option, make a selection from the pull-down menu: “Today” (default), “Month to Date”, “Year to Date”, “Yesterday”, “Month to Yesterday”, “Year to Yesterday”, “Last Week”, “Last Weekend”, “Current Week”, “Last Month”.
 - **Date Range** - This option is selected by default. If choosing this option, use the calendar icons to set the date range.
3. Specify the **Break Type** from the available choices in the pull-down menu.
4. 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.
5. By default, **Export report with URLs** is de-selected. Click this checkbox to select this option, and then specify the number of URLs to export:
 - **All URLs** - Check this checkbox to export all URLs
 - **Top** - Specify the number of top URLs to be exported

Step C: Select the users or group in the Users frame

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:

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

Step D: Populate the Email Settings frame

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

Step E: Save the report

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

Two methods for scheduling security reports

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

How to use Wizard panels for scheduling reports

Step A: Choose the method for scheduling the report

Method 1: Use the current report view

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

The screenshot shows the Security Reporter interface with the Security Report Wizard panel open for 'Rule Transactions'. The panel is divided into three main sections:

- Report Details:** Includes fields for Report Name, Report Time Span (Predefined Ranges or Date Range), Break Type, and Top item limit. The Date Range is set from 11/04/2010 to 11/04/2010. The Top item limit is set to 10.
- Users:** A list of user groups is displayed, with 'All' selected. The list includes Accounting, Administration, All, Engineering, Facilities, HR, IT, Marketing, None, QA, Sales, Technical Support, and Unknown Users.
- Email Settings:** Includes fields for Email, Delivery method (To, Bcc, Cc), Subject, and Body. The Output type is set to 'E-Mail As Attachment' and the Format is set to PDF.

At the bottom of the panel, there are buttons for '<< Back', 'Save', 'Schedule Settings', and 'Filters >>'.

Report Settings Save option

Method 2: Create a report using the Wizard

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

Security Report Wizard panel

Step B: Fill in the Report Details frame

In the Report Details frame:

1. Type in the **Report Name**.
2. If using the Report Wizard to generate and schedule a report, 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 using the Report Wizard to generate and save a report, this option is selected by default. If choosing this option, make a selection from the pull-down menu: “Today” (default), “Month to Date”, “Year to Date”, “Yesterday”, “Month to Yesterday”, “Year to Yesterday”, “Last Week”, “Last Weekend”, “Current Week”, “Last Month”.
 - **Date Range** - If using the Report Settings Schedule feature, this option is selected by default. If choosing this option, use the calendar icons to set the date range.
4. Specify the **Break Type** 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

Step C: Include the users or group in the Users frame

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:

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

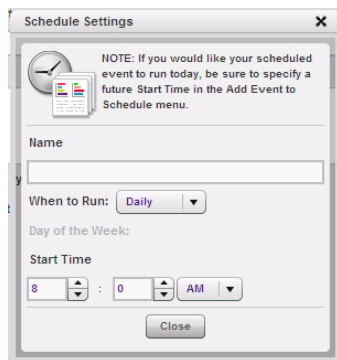
Step D: Complete information in the Email Settings frame

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”.
3. Type in the **Subject** for the email message.
4. If you wish, enter text to be included in the **Body** of the message.
5. Specify the **Output type** for the email: “E-Mail As Attachment” or “E-Mail As Link”.

Step E: Set the schedule for running the report

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



Schedule Settings pop-up window

2. Enter a **Name** for the report run event you are scheduling.
3. 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).
4. Select the **Start Time** for the report: 1 - 12 for the hour, 0 - 59 for the minutes, and AM or PM.
5. Click **Close** to save your settings and close the pop-up window.

Step F: Save the report

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

How to access and view the Report Schedule panel


The Report Schedule panel is used for maintaining a schedule for generating a customized productivity or security report.

Navigate to **Reports > Report Schedule** to display the Report Schedule panel:

Name	Interval	Last Run	Next Run	Custom Report Name	Start Time
Blocked Viruses Weekly Report	Weekly	10/08/2010 2:05:00 PM	10/15/2010 2:05:00 PM	Blocked Viruses Weekly Report	2:05 PM
Instant Message Summary Report	Weekly	10/12/2010 9:00:00 AM	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	10/12/2010 8:30:00 AM	Sites Report	8:30 AM

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 for the report to run.

 **NOTE:** Records in this panel may include summary productivity reports, detail productivity reports, and security reports.

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:


The screenshot shows the Security Reporter interface with the 'Report Schedule' panel. The panel contains a table of scheduled reports and a details pane on the right.

Name	Interval	Last Run	Next Run	Custom Report Name	Start Time
Blocked Viruses V	Weekly	10/08/2010 2:05:01	10/15/2010 2:05:01	Blocked Viruses Weekly Report	2:05 PM
Instant Message	Weekly		10/12/2010 9:00:01	Drill Down Summary Category Sites	9:00 AM
Weekly Summary	Weekly		10/12/2010 8:30:01	Sites Report	8:30 AM

The details pane on the right includes a 'Name' field, a 'Report to Run' list with the following items: 'Blocked Viruses Weekly Report', 'categories summary report', 'Drill Down Summary Category Sites', and 'Sites Report'. Below this is a 'When to Run' dropdown set to 'Daily', a 'Day of the Week' field, and a 'Start Time' field set to '8:00 AM'. Buttons for 'Add Event', 'Delete', 'Refresh', 'Save', and 'Cancel' are also visible.

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.