



 **Trustwave®**  
Smart security on demand

# SECURITY REPORTER EVALUATION GUIDE

## VERSION 3.3.10

Publication Date: 10 February 2014

# Legal Notice

Copyright © 2014 Trustwave Holdings, Inc.

All rights reserved. This document is protected by copyright and any distribution, reproduction, copying, or decompilation is strictly prohibited without the prior written consent of Trustwave. No part of this document may be reproduced in any form or by any means without the prior written authorization of Trustwave. While every precaution has been taken in the preparation of this document, Trustwave assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

While the authors have used their best efforts in preparing this document, they make no representation or warranties with respect to the accuracy or completeness of the contents of this document and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the author nor Trustwave shall be liable for any loss of profit or any commercial damages, including but not limited to direct, indirect, special, incidental, consequential, or other damages.

The most current version of this document may be obtained from:

[www.trustwave.com/support/](http://www.trustwave.com/support/)




## Trademarks

Trustwave and the Trustwave logo are trademarks of Trustwave. Such trademarks shall not be used, copied, or disseminated in any manner without the prior written permission of Trustwave.

Part# SR-EG-140210

# Formatting Conventions

This manual uses the following formatting conventions to denote specific information.

Format and Symbols	Meaning
<u>Blue Underline</u>	A blue underline indicates a Web site or email address.
<b>Bold</b>	Bold text denotes UI control and names such as commands, menu items, tab and field names, button and check box names, window and dialog box names, and areas of windows or dialog boxes.
<code>Code</code>	Text in this format indicates computer code or information at a command line.
<i>Italics</i>	Italics are used to denote the name of a published work, the current document, or another document; for text emphasis; or to introduce a new term. In code examples italics indicate a placeholder for values and expressions.
[Square brackets]	In code examples, square brackets indicate optional sections or entries.
	<b>Note:</b> This symbol indicates information that applies to the task at hand.
	<b>Tip:</b> This symbol denotes a suggestion for a better or more productive way to use the product.
	<b>Caution:</b> This symbol highlights a warning against using the product in an unintended manner.

# Table of Contents

Legal Notice . . . . .	ii
Formatting Conventions . . . . .	iii
<b>1 Security Reporter Evaluation Guide</b>	<b>7</b>
1.1 Product Overview . . . . .	7
1.2 Note to Evaluators. . . . .	7
1.3 Install, Configure, and Test the Security Reporter . . . . .	7
1.4 About this Evaluation Guide . . . . .	8
<b>2 Configuration</b>	<b>9</b>
2.1 Understand common configuration elements . . . . .	9
2.2 Use Custom Category Groups to narrow your search . . . . .	9
2.2.1 How to add a Custom Category Group . . . . .	10
2.3 Use custom User Groups to narrow your search . . . . .	11
2.3.1 How to create User Groups. . . . .	11
2.3.1.1 Patterns sub-panel . . . . .	12
2.3.1.2 IP Ranges sub-panel . . . . .	13
2.3.1.3 Single Users/Exclude sub-panel. . . . .	14
2.3.2 How to Rebuild a User Group. . . . .	14
<b>3 Productivity and Security Reports</b>	<b>15</b>
3.1 Use Summary Reports for a high level overview . . . . .	16
3.1.1 How to generate a Summary Report. . . . .	17
3.1.2 How to export a Summary Report. . . . .	19
3.2 Use Drill Down Reports for an investigation . . . . .	19
3.2.1 How to generate a Summary Drill Down Report. . . . .	20
3.2.1.1 Summary Drill Down Report navigation . . . . .	20
3.2.2 How to generate a Detail Drill Down Report . . . . .	22
3.2.2.1 Detail Drill Down Report navigation . . . . .	23
3.2.2.2 Detail Drill Down Report exercise . . . . .	23
3.3 Create a custom report for a specific user . . . . .	24
3.3.1 How to use the Report Wizard for a single user report . . . . .	24
3.3.1.1 Report type . . . . .	25
3.3.1.2 General tab . . . . .	25
3.3.1.3 Grouping and Visibility . . . . .	26
3.3.1.4 Run the report. . . . .	26
3.3.1.5 View details for a user. . . . .	27
3.3.1.6 View report filters . . . . .	28

3.3.1.7 Download the report .....	28
3.3.1.8 Save the report .....	29
<b>4 Report Wizard</b>	<b>31</b>
<hr/>	
4.1 Starting the Report Wizard .....	31
4.1.1 General tab .....	32
4.1.2 Grouping and Visibility .....	33
4.1.2.1 Group and Sort Rows .....	33
4.1.2.2 Column Visibility .....	34
4.1.3 Filters tab .....	34
4.1.4 Wildcard filter examples .....	35
4.1.4.1 Users .....	36
4.1.4.2 Virus Names .....	36
4.1.5 Generating a report .....	36
4.1.6 Saving a report for later use .....	37



# 1 Security Reporter Evaluation Guide

## 1.1 Product Overview

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

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

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

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

## 1.2 Note to Evaluators

Thank you for taking the time to review the Trustwave Security Reporter. 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: Summary reports, Drill down reports, detailed Productivity and Security reports, and the flexible Report Wizard.

## 1.3 Install, Configure, and Test the Security Reporter

The Security Reporter can be installed in your network as an appliance or as a virtual image on a dedicated appliance.

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 Trustwave Security Reporter Appliance Installation Guide provided inside the carton containing the chassis.

To install the SR application in an environment supporting Virtualization Technology, refer to the Security Reporter Virtual Installation Guide downloaded from our public Web site at <http://www.trustwave.com/support/sr/documentation.asp>.

Please note that prior to reviewing the SR, the Trustwave Web Filter and/or Trustwave 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 Trustwave Web Filter Installation Guide or Trustwave WFR Installation Guide for information on setting up the Web Filter on your network. See the Trustwave SWG Setup and Configuration Guide for information on setting up the Secure Web Gateway on your network. be sure HyperTerminal or an equivalent terminal emulator program is installed on your machine.

## 1.4 About this Evaluation Guide

The Trustwave Security Reporter Evaluation Guide includes the following topics:

- Category and User Group configuration
- Productivity and Security Reports
- Report Wizard features and usage



## 2 Configuration

### 2.1 Understand common configuration elements

The first sections of the Evaluation Guide lead 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. In this chapter you are directed through recommended configuration steps. In the following chapter, you are led through a standard use case that explains how to investigate a violation of your Internet Acceptable Use Policy.

After stepping through these sections 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.

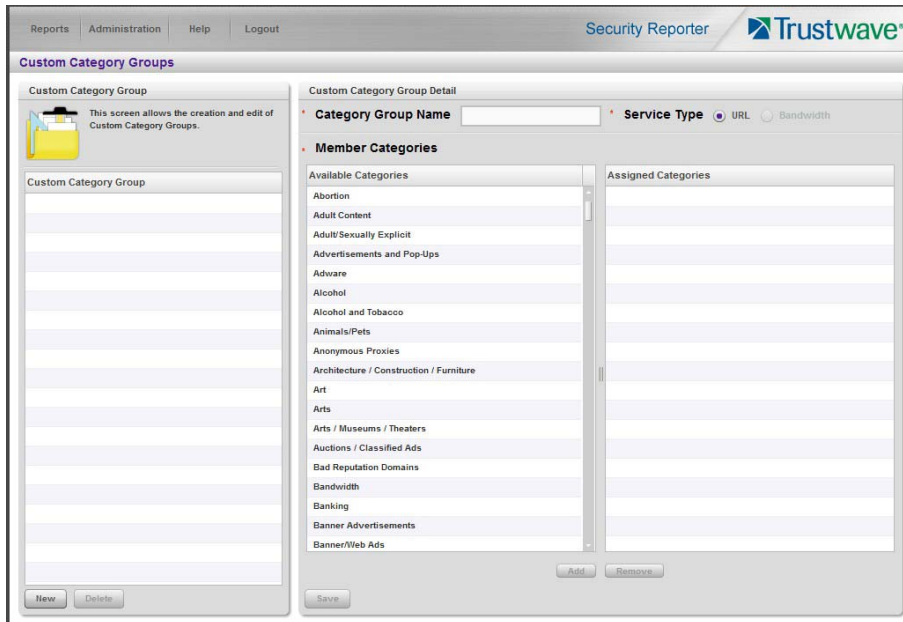


**Tip:** After the SR appliance is installed, allow the Security Reporter to run for several days prior to evaluating reports in order to optimize the evaluation experience. This will allow the SR to accumulate multiple days of data and present more meaningful reports. Having performed these preliminary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

### 2.2 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 Trustwave 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:



The Custom Category Groups panel is comprised of two sub-panels used for setting up and maintaining category groups: Custom Category Group, and Custom Category Group Detail.

### 2.2.1 How to add a Custom Category Group

1. At the bottom of the Custom Category Group sub-panel, click **New**.
2. In the Custom Category Group Detail sub-panel, 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.

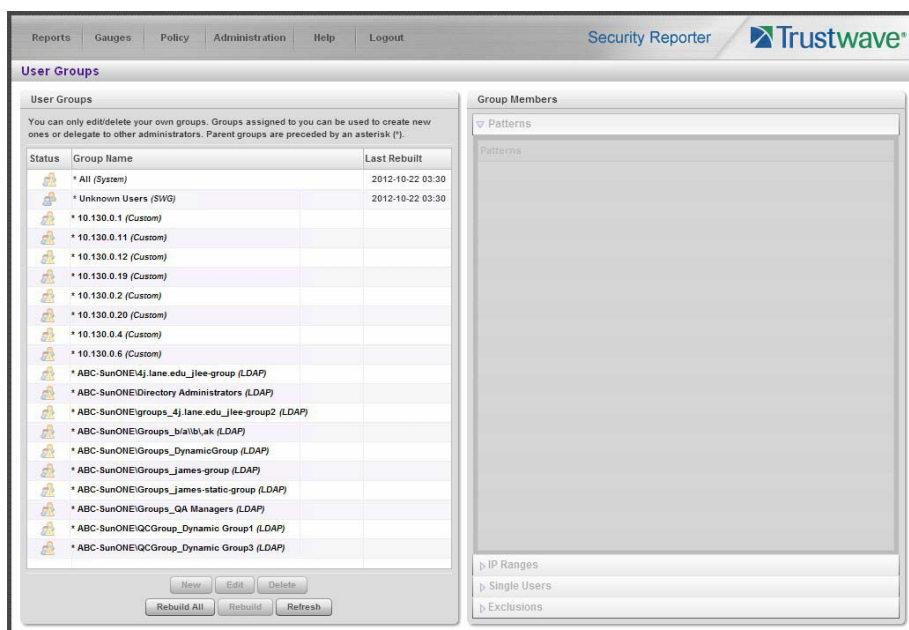
5. Click **Save** to save your settings and to include the name of the group you added in the Custom Category Group list.

## 2.3 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.

### 2.3.1 How to create User Groups

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



The User Groups panel is comprised of two sub-panels 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:

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

### 2.3.1.1 Patterns sub-panel

The Patterns sub-panel 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.

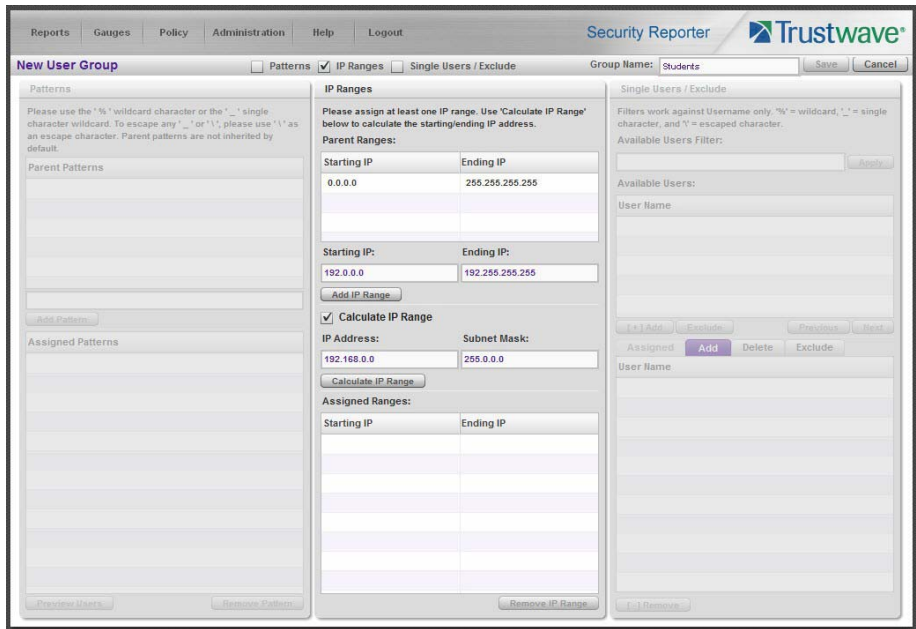
1. To add a pattern to the new user group, do one of the following:
  - To add a pattern included in the base group, select the pattern from the Parent Patterns box to display that pattern in the field below.
  - To add a new pattern, enter the pattern in the field beneath the Parent Patterns box. For 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.

### 2.3.1.2 IP Ranges sub-panel

The IP Ranges sub-panel is used for specifying IP ranges to be used by the new group.



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 sub-panel:
    - i. Enter the **Starting IP** address.
    - ii. Enter the **Ending IP** address.
  - To calculate an IP address range:
    - i. Click the **Calculate IP Range** check box to activate the IP Address and Subnet Mask fields below.
    - ii. Enter the **IP Address**.
    - iii. Enter the **Netmask** which activates the Calculate Range button.
    - iv. 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.

### 2.3.1.3 Single Users/Exclude sub-panel

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



**Note:** 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' configuration window in Trustwave Security Reporter. The 'Single Users / Exclude' tab is active. The 'Available Users' list contains the following IP addresses: 192.168.20.79, 192.168.200.100, 192.168.200.102, 192.168.200.107, and 192.168.200.11. The 'Assigned Users' list is currently empty. The interface includes buttons for 'Add', 'Delete', and 'Exclude' to manage the user list.

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.

### 2.3.2 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.

## 3 Productivity and Security Reports

Once Custom Category Groups and User Groups have been created (as described in the previous section), administrators can begin running their first reports. In most cases, administrators will employ the Security Reporter as a forensic tool to watch for inappropriate or unwanted use of the Internet. The Security Reporter menu structure is organized to follow the normal process flow of an investigation.

1. First, the administrator is greeted by productivity report content in “**Summary Reports.**”

Additional information can be viewed by navigating to Reports | Dashboard where high-level productivity report information shows 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 behavior that needs investigation. For instance, a specific username might be generating a large number of blocked requests, or a high volume of traffic might be identified in the “Pornography/Adult Content” category.

2. The next stage of the investigation, “**Drill Down Reports,**” lets the administrator probe the multi-dimensional database to target the source of any unusual activity.

For example, if the “Pornography/Adult Content” category shows a high page count, 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 use a detail view to see the exact pages that end user has been visiting.

The detail view provides clear information about the exact time the page was visited, the user’s IP address, whether the site was blocked by the Web Filter or SWG, what functionality identified the page (such as a library category, keyword, or proxy pattern), 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 monitor and if necessary document the activity of a policy violator over the long term as required for disciplinary action. 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 use the “**Report Wizard**” to specify a custom time scope, specific category, and name of a specific end user to report on.

For example, the administrator could specify a user, the category “Pornography/Adult Content,” and all activity within that category for the last month. The administrator can save the output as a PDF for documentation purposes. Such a report provides the necessary forensic information to back up any HR action or protect against possible legal challenges.

The following sections provide a more detailed view of how to navigate within each of the main productivity reporting areas of the Security Reporter: Summary Reports, Drill Down Reports, and Report Wizard.



### 3.1 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 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 by Page Count** - Bar chart report depicting the total Page Count in the top requested filtering library categories.
- **Top 20 Users by Page Count** - Bar chart report depicting each top end user’s total Page Count.
- **Top 20 Viruses Detected** (for SWG only) - Bar chart report depicting the top viruses and Virus Count detected by the anti-virus engine.
- **Top 20 Users by Malware by Hit Count** - 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 Trustwave Supplied Categories.

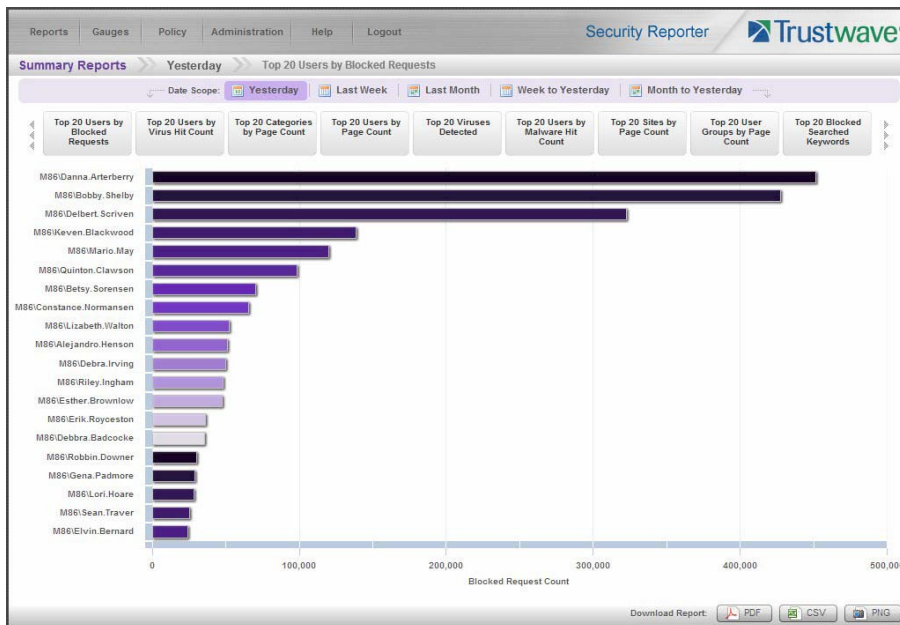
- **Top 20 Sites by Page Count** - Bar chart report depicting the total Page Count for the most popular sites accessed by end users.
- **Top 20 User Groups by Page Count** - Bar chart report depicting the total Page Count for the top scoring user groups.
- **Total Permitted vs. Blocked Requests** - Pie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

### 3.1.1 How to generate a Summary Report

1. To generate a Summary Report, navigate to Reports | Summary Reports to display yesterday's report view showing the Top 20 Users by Blocked Requests:



**Note:** 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.



**Tip:** 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):

Figure 1: Sample Bar Chart Summary Report in the PDF format

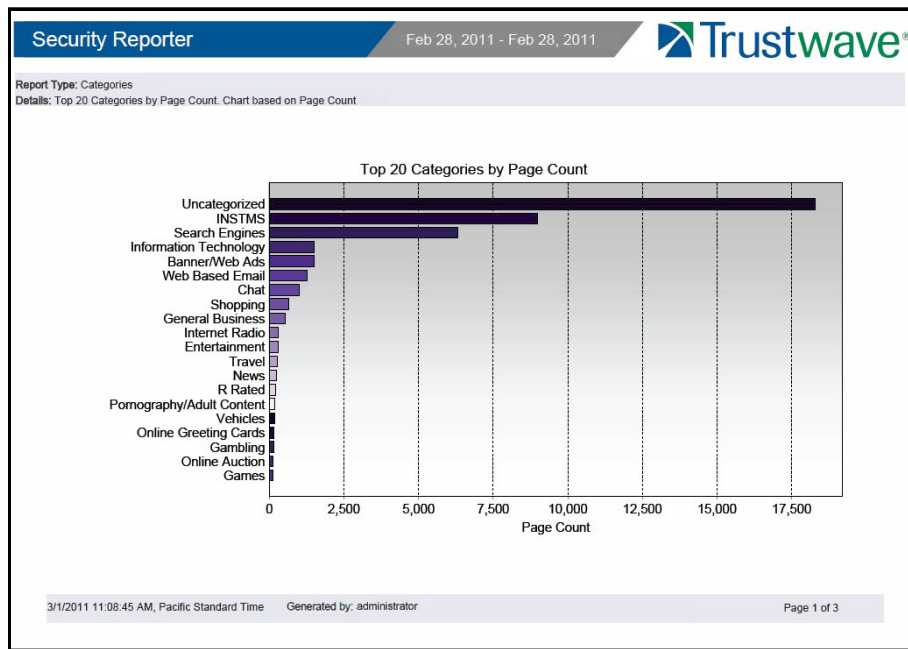
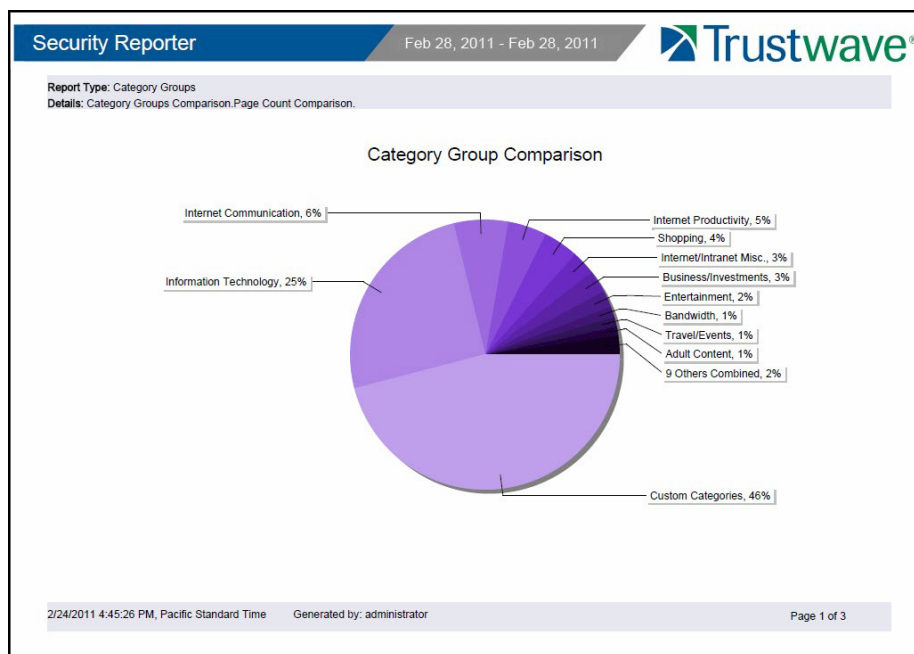


Figure 2: Sample Pie Chart Summary Report in the PDF format



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

The footer of the report includes the date and time the report was generated, time zone, 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 Requests 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.
- All other reports - Count columns and corresponding totals for all reports. Grand Total and Count display at the end of the report.

### 3.1.2 How to export a Summary Report

From the open PDF file, you can print or save the Summary Report:

- 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 (Page) As... to open the Save As dialog box, and proceed with standard save procedures.

## 3.2 Use Drill Down Reports for an investigation

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

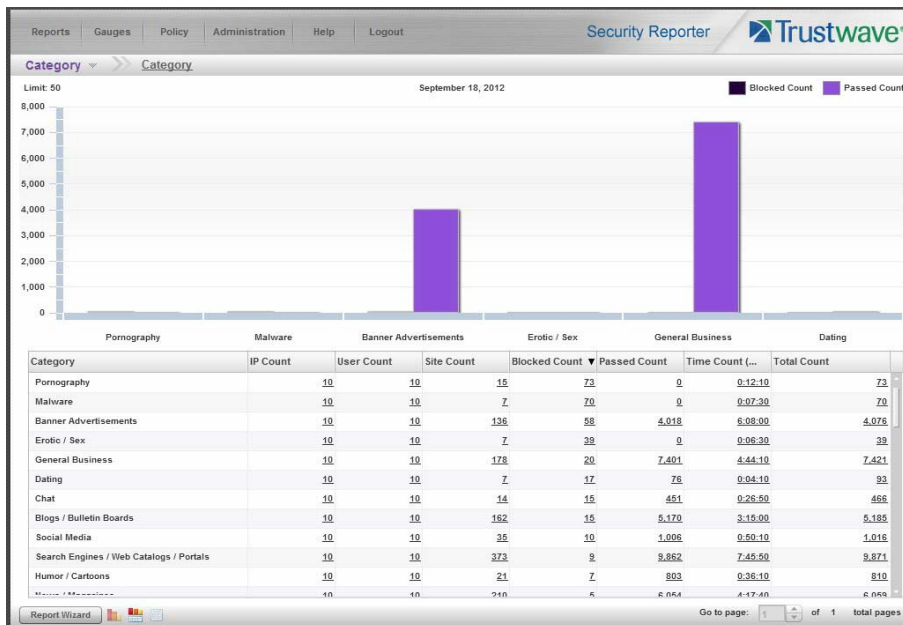
This section provides information about “drill down” reports that let you query the database to access more detailed information about end user Internet activity. The following types of reports can be generated:

- **Category:** Features data for sites in each filter category accessed by end users.
- **Content Type:** Includes end user Internet access of objects utilizing an excessive amount of network bandwidth.
- **Rule:** Includes each instance in which an end user triggered a threshold in an SWG Security Policy.
- **Spyware:** Provides information for each instance in which an end user accessed content containing spyware.
- **Violation:** Provides information on each instance in which an end user breached a security policy.
- **Virus:** Includes details for each instance of a blocked virus detected from end user Internet/network activity.
- **Vulnerability Anti.Dote:** Provides details for each instance of real-time vulnerability detection resulting from end user Internet/network activity.

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.

### 3.2.1 How to generate a Summary Drill Down Report

1. To generate a summary Drill Down Report, navigate to Reports | Drill Down and choose the report type to be generated. The first menu selection is “Category”; making this selection displays today’s Category report view by Page Count:



2. The top portion of the report view includes a breadcrumb trail showing the path to the report. The first item at the left of the trail is a menu allowing you to select Drill Down report types. Beneath this row, a bar chart depicts the first six records for the current report type.



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

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

3. Use the tools at the bottom portion of the report view panel to modify the current report view, creating the desired drill down view.

#### 3.2.1.1 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.

##### 3.2.1.1.1 Count columns and links

Count columns display after the column containing the record name. Clicking a specific link in a record’s Count column gives more in-depth analysis on a given record displayed in the current view. Clicking a link

in the Blocked Count, Passed Count, Bandwidth (SWG only), Time Count, Blocked Count, or Total Count column generates a detail drill down report view.

- **IP Count** - Displays the number of user IPs pertinent to the record in the report.
- **User Count** - Displays the number of usernames pertinent to the record in the report.
- **Site Count** - Displays the number of sites accessed by users for the pertinent record in the report. This figure is based on the root name of the site. For example, if a user visits [www.espn.com](http://www.espn.com), [www.msn.com](http://www.msn.com), and [www.fox-sports.com](http://www.fox-sports.com), that user will have visited three pages. If that same user additionally visits [www.espn.com/scores](http://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.
- **Blocked Count** - Displays the number of blocked pages and/or objects for each record in the table.



**Note:** The blocked pages count in a record indicates the total number of individual web 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 are served from other sites, these items also would factor into the page count. In categories that use a lot of pop-up ads—such as porn, gambling, and other related sites—the page count usually exceeds the number of objects per page.

The blocked objects count in a record indicates the number of objects on all web pages visited. 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.

When you click a link in this column for a specific record, the detail report view displays blocked records in red text, and includes hyperlinks to blocked pages/objects.

- **Passed Count** - Displays the number of passed (allowed) pages and/or objects for each record in the table.

When you click a link in this column for a specific record, the detail report view displays passed records and includes hyperlinks to passed pages/objects.

- **Total Count** - Displays the sum of blocked and passed column counts for each record in the table.

When you click a link in this column for a specific record, the detail report view displays blocked records in red text, and passed records in black text, for all objects pertinent to that selection, including hyperlinks to pages/objects.

### 3.2.1.1.2 Column sorting tips

To sort summary report view records in ascending/descending order by a specified column, click that column's header.

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.

### 3.2.1.1.3 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.

### 3.2.2 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 (such as “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 “Blocked Count,” “Passed Count”, or “Total Count” column of the Summary Drill Down Report:

August 6, 2013						
Date	Category	IP	User	Action	Policy	URL
8/6/2013 12:02:13 AM	Banner Advertisements	10.130.0.108	M86Jacquelyn.Ready	None	Load test medium poli...	<a href="http://ads.addynamix...">http://ads.addynamix...</a>
8/6/2013 12:03:02 AM	Banner Advertisements	10.130.1.163	M86Zane.Tollemache	None	Load test medium poli...	<a href="http://a.websponsors...">http://a.websponsors...</a>
8/6/2013 12:03:07 AM	Banner Advertisements	10.130.0.9	M86Deana.Coleman	None	Load test medium poli...	<a href="http://counters.honest...">http://counters.honest...</a>
8/6/2013 12:05:05 AM	Banner Advertisements	10.130.1.151	M86Angeline.Southers	None	Load test medium poli...	<a href="http://c7.zedo.com/ad...">http://c7.zedo.com/ad...</a>
8/6/2013 12:05:28 AM	Banner Advertisements	10.130.0.73	M86Debbie.Boon	Block	Load test medium poli...	<a href="http://network.realme...">http://network.realme...</a>
8/6/2013 12:05:57 AM	Banner Advertisements	10.130.0.21	M86Cathie.Bloxham	None	Load test medium poli...	<a href="http://adserver.yahoo...">http://adserver.yahoo...</a>
8/6/2013 12:06:10 AM	Banner Advertisements	10.130.1.100	M86Jodie.Victorson	None	Load test medium poli...	<a href="http://images.trafficmp...">http://images.trafficmp...</a>
8/6/2013 12:06:17 AM	Banner Advertisements	10.130.0.135	M86Gaylon.Baldwin	None	Load test medium poli...	<a href="http://launch.adserver...">http://launch.adserver...</a>
8/6/2013 12:06:27 AM	Banner Advertisements	10.130.1.76	M86Meryl.Scrivener	None	Load test medium poli...	<a href="http://http.edge.ru4.co...">http://http.edge.ru4.co...</a>
8/6/2013 12:06:34 AM	Banner Advertisements	10.130.1.240	M86Fidel.Toovv	Block	Load test medium poli...	<a href="http://pagead2.google...">http://pagead2.google...</a>
8/6/2013 12:06:51 AM	Banner Advertisements	10.130.1.81	M86Tab.Benjaminson	None	Load test medium poli...	<a href="http://ads.adsaq.com/...">http://ads.adsaq.com/...</a>
8/6/2013 12:07:38 AM	Banner Advertisements	10.130.1.58	M86Jeremy.Honeysett	None	Load test medium poli...	<a href="http://ad.trafficmp.com...">http://ad.trafficmp.com...</a>
8/6/2013 12:07:53 AM	Banner Advertisements	10.130.0.158	M86Hiram.Tyson	Block	Load test medium poli...	<a href="http://rad.msn.com/AD...">http://rad.msn.com/AD...</a>
8/6/2013 12:08:18 AM	Banner Advertisements	10.130.0.184	M86Danette.Adelman	None	Load test medium poli...	<a href="http://ads.web.aol.co...">http://ads.web.aol.co...</a>
8/6/2013 12:08:52 AM	Banner Advertisements	10.130.0.161	M86Janell.Carter	Block	Load test medium poli...	<a href="http://counters.honest...">http://counters.honest...</a>
8/6/2013 12:09:27 AM	Banner Advertisements	10.130.0.235	M86Randall.Scott	Block	Load test medium poli...	<a href="http://rad.doubleclick...">http://rad.doubleclick...</a>
8/6/2013 12:10:31 AM	Banner Advertisements	10.130.1.22	M86Terrence.Garrod	None	Load test medium poli...	<a href="http://adv.vebmd.com...">http://adv.vebmd.com...</a>
8/6/2013 12:10:46 AM	Banner Advertisements	10.130.0.93	M86Nelson.Hilton	Block	Load test medium poli...	<a href="http://r1.adserver.co...">http://r1.adserver.co...</a>
8/6/2013 12:11:08 AM	Banner Advertisements	10.130.1.53	M86Dominick.Vipond	Block	Load test medium poli...	<a href="http://rad.msn.com/AD...">http://rad.msn.com/AD...</a>
8/6/2013 12:12:37 AM	Banner Advertisements	10.130.0.67	M86Zane.Tollemache	Block	Load test medium poli...	<a href="http://pagead2.google...">http://pagead2.google...</a>
8/6/2013 12:13:31 AM	Banner Advertisements	10.130.1.55	M86Marita.Lane	Block	Load test medium poli...	<a href="http://ebay.doubleclick...">http://ebay.doubleclick...</a>
8/6/2013 12:13:56 AM	Banner Advertisements	10.130.1.192	M86Stacy.Sexton	Block	Load test medium poli...	<a href="http://sel.as-us.falka...">http://sel.as-us.falka...</a>
8/6/2013 12:14:58 AM	Banner Advertisements	10.130.1.143	M86Darwin.Roach	None	Load test medium poli...	<a href="http://as.casalemedia...">http://as.casalemedia...</a>
8/6/2013 12:15:18 AM	Banner Advertisements	10.130.1.207	M86Danny.Kevinson	Block	Load test medium poli...	<a href="http://rad.msn.com/AD...">http://rad.msn.com/AD...</a>
8/6/2013 12:15:32 AM	Banner Advertisements	10.130.1.222	M86Les.Senior	Block	Load test medium poli...	<a href="http://rad.msn.com/AD...">http://rad.msn.com/AD...</a>



**Note:** Blocked records display in red text in the detail drill down report table.



### 3.2.2.1 Detail Drill Down Report navigation

#### 3.2.2.1.1 Report type columns

Detail reports include the following columns: Date, report type name, IP, User, Action, Policy, URL. A record displayed in red text indicates a blocked URL request.

- **Date** - Displays the date of the record using the M/D/YYYY HH:MM:SS AM/PM format.
- **IP** - Displays the IP address of the end user for the request.
- **User** - Displays the username of the end user for the request. The entry in this column might include the user IP address, or the path and username (e.g. "logo\admin\jsmith").
- **Action** - If using a Web Filter, this column displays the type of filter action used by the Web Filter: "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.
- **Policy** - If using an SWG, this column displays the name of the policy used by the SWG for this request.
- **URL** - Displays the link for the page/object for the end user's request.
- **Type** - Displays the kind of requested item: "Object" or "Page".

#### 3.2.2.2 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.

##### 3.2.2.2.1 Select a specific action by Category

If not already completed, click the "Blocked Count," "Passed Count", or "Total Count" column link for any record in the Summary Drill Down Report.

##### 3.2.2.2.2 Sort by "Action" column

Clicking the "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.

##### 3.2.2.2.3 Review the full URL

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:



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

### 3.2.2.4 Refine the view with the Report Wizard

From the detail drill down view you can continue directly to the Report Wizard. Click the **Report Wizard** button at the bottom left of the report. The wizard will be pre-populated with filter and date selections that reflect the current on screen view. You can edit the settings to further customize the view.

## 3.3 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. To create this report, use the **Report Wizard**.

### 3.3.1 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.

To access the Report Wizard, navigate to Reports | Drill Down | Report Wizard, or click the Report Wizard button at the bottom left of summary drill down reports.



This section provides basic information about how to create simple single level reports. For more details of the report wizard, see Section 4.

### 3.3.1.1 Report type

If you start the wizard from Reports | Drill Down | Report Wizard, you can select a type of report in the sub-menu or the type menu at the top left above the wizard tabs.

For demonstration purposes select a **Category** report.

### 3.3.1.2 General tab

On the General tab of the wizard, select a date scope option:

- **Pre-selected Date Scope:** Click the upper radio button, then use the menu to pick a period such as **Today** or **Current month**.
- **Date and Time Range:** Click the lower radio button, and then use the date controls to select a specific starting and ending date. If you are planning a single level detail report you can also specify starting and ending times.



**Note:** Detail reports for large date scopes can take a long time to run. If you have a significant amount of data in your evaluation installation, choose a short scope (or few categories) to ensure you see results quickly. In production you would normally use scheduled or email delivered reports for large scopes.

To enable saving of the report, enter a name. (A name is not required if you plan to download, email, or run the report without saving).

On the General tab you can also limit the report with Options, and select an export format. For detailed coverage of these settings, see Section 4.

### 3.3.1.3 Grouping and Visibility

On the Grouping & Visibility tab of the wizard, you can select grouping and sorting options, number of records, and visible columns. For the purpose of this exercise, use the default option of a single level summary report.



**Note:** You can also generate a detail report directly from the wizard. This option is covered in Section 4.

The screenshot shows the 'Grouping & Visibility' tab in the Trustwave Security Reporter interface. The 'Grouping & Sorting' section includes a 'Group By' dropdown set to 'Category', a 'Sort By' dropdown set to 'Blocked Count', and a 'Show Records' dropdown set to '50'. There are also buttons for 'Add Group and Sort row', 'Remove last added row', and 'Summary Report / Detail Report'. The 'Column Visibility' section on the right lists various metrics with eye icons to toggle their visibility in the report output.

- **Group By:** This menu setting determines the heading of each detail row. For summary reports, by default the grouping follows the report type. To easily find information about a specific user, on the Group By menu select **User**.
- **Sort By:** This menu setting determines the order of detail rows. To find information about users with high numbers of blocks, use the default setting **Blocked Count**.
- **Sort Order:** The button following the Sort By column allows you to select the order of sorting. To find information about users with high numbers of blocks, use the default setting **Descending order**.
- **Show Records:** To quickly find the users with high numbers of blocks, use the default value of **50 records**.
- **Column Visibility:** Use the control at the right of the tab to select the columns in the report output. Click an “eye” to show or hide the corresponding column. An open eye indicates the column is included in the output.

### 3.3.1.4 Run the report

After making selections on the Grouping & Visibility tab, click **Run** at the bottom right to generate a summary report. The default output appears as below.

User	IP Count	Site Count	Blocked Count	Passed Count	Total Count
M86Les.Senior	10	200	512	0	512
M86Stacy.Sexton	13	220	506	0	506
M86Jocelyn.Ogden	10	204	433	0	433
M86Nan.Huddleson	7	190	393	0	393
M86Jacquelyn.Ready	8	185	388	0	388
M86Lorelei.Hobson	8	210	382	0	382
M86Williams.Appleton	6	158	380	0	380
M86Les.Rains	8	188	374	0	374
M86Una.Rey	7	174	364	0	364
M86Darwin.Roach	8	191	363	0	363
M86Stacey.Sands	8	189	362	0	362
M86Leticia.Mallory	7	182	362	0	362
M86Reggie.Olthouser	6	167	360	0	360
M86Dallas.Fox	8	170	360	0	360
M86Virginia.Walsh	8	174	358	0	358
M86Don.James	7	184	356	0	356
M86Lyn.Benson	8	185	352	0	352
M86Kristina.Summerfield	7	171	351	0	351
M86Javier.Totter	7	177	349	0	349
M86Tonia.Christison	6	171	344	0	344
M86Teddy.Leonardsson	7	168	341	0	341
M86Stewart.Voll	8	178	341	0	341
M86Betty.Normanson	6	160	340	0	340
M86Bruno.Petit	6	179	339	0	339
M86Michael.Babin	6	167	338	0	338

### 3.3.1.5 View details for a user

From the summary report view, to create a detail report click the **Blocked Count** entry to view details of blocked requests for a user of interest.

Date	Category	IP	User	Action	Policy	URL
6/15/2013 06:13:01 AM	Education	10.130.1.242	M86Les.Senior	Block	Load test medium poli...	http://www.lexile.com...
6/15/2013 06:29:11 AM	Search Engines / Web...	10.130.1.242	M86Les.Senior	Block	Load test medium poli...	http://search.yahoo.co...
6/15/2013 07:27:39 AM	Education	10.130.1.242	M86Les.Senior	Block	Load test medium poli...	http://www.starfall.co...
6/15/2013 07:37:39 AM	Banner Advertisements	10.130.1.242	M86Les.Senior	Block	Load test medium poli...	http://ad.doubleclick.n...
6/15/2013 08:09:12 AM	Other	10.130.1.242	M86Les.Senior	Block	Load test medium poli...	http://media.admarket...
6/15/2013 08:19:07 AM	Banner Advertisements	10.130.0.174	M86Les.Senior	Block	Load test medium poli...	http://ad.doubleclick.n...
6/15/2013 09:13:04 AM	Malware	10.130.1.242	M86Les.Senior	Block	Load test medium poli...	http://bz2.gator.com/g...
6/15/2013 11:16:22 AM	Computer Games	10.130.1.242	M86Les.Senior	Block	Load test medium poli...	http://www.cartoonnet...
6/15/2013 11:27:56 AM	Pornography	10.130.1.242	M86Les.Senior	Block	Load test medium poli...	http://www.vifanbbs.c...
6/15/2013 11:37:23 AM	News / Magazines	10.130.0.174	M86Les.Senior	Block	Load test medium poli...	http://spe.atdmt.com/d...
6/15/2013 12:11:37 PM	Education	10.130.1.242	M86Les.Senior	Block	Load test medium poli...	http://dist-1mg.usarmy...
6/15/2013 12:19:51 PM	Computer Games	10.130.1.242	M86Les.Senior	Block	Load test medium poli...	http://www.disney.go...
6/15/2013 12:50:05 PM	Environment / Climate...	10.130.0.174	M86Les.Senior	Block	Load test medium poli...	http://visaapidata.veat...
6/15/2013 12:54:00 PM	Other	10.130.0.174	M86Les.Senior	Block	Load test medium poli...	http://www.m-ms.com...
6/15/2013 01:03:40 PM	Banner Advertisements	10.130.0.174	M86Les.Senior	Block	Load test medium poli...	http://mediamgr.uqc.c...
6/15/2013 01:17:39 PM	Software / Hardware	10.130.0.174	M86Les.Senior	Block	Load test medium poli...	http://www.dell.com/...
6/15/2013 01:19:13 PM	Shopping	10.130.1.242	M86Les.Senior	Block	Load test medium poli...	http://www.diecastfir...
6/15/2013 01:48:09 PM	Computer Games	10.130.1.242	M86Les.Senior	Block	Load test medium poli...	http://www.nick.com/...
6/15/2013 01:59:25 PM	Pornography	10.130.1.242	M86Les.Senior	Block	Load test medium poli...	http://www.vifanbbs.c...
6/15/2013 02:04:47 PM	Search Engines / Web...	10.130.0.174	M86Les.Senior	Block	Load test medium poli...	http://ar.athvola.com/c...
6/15/2013 02:04:47 PM	Search Engines / Web...	10.130.0.174	M86Les.Senior	Block	Load test medium poli...	http://ar.athvola.com/c...
6/15/2013 02:05:01 PM	Spyware	10.130.1.171	M86Les.Senior	Block	Load test medium poli...	http://message.real.co...
6/15/2013 02:05:01 PM	Software / Hardware	10.130.1.171	M86Les.Senior	Block	Load test medium poli...	http://message.real.co...
6/15/2013 02:10:46 PM	Malware	10.130.1.242	M86Les.Senior	Block	Load test medium poli...	http://bz2.gator.com/g...
6/15/2013 02:18:09 PM	Music / Radio Broadc...	10.130.1.63	M86Les.Senior	Block	Load test medium poli...	http://www.sonatricks...

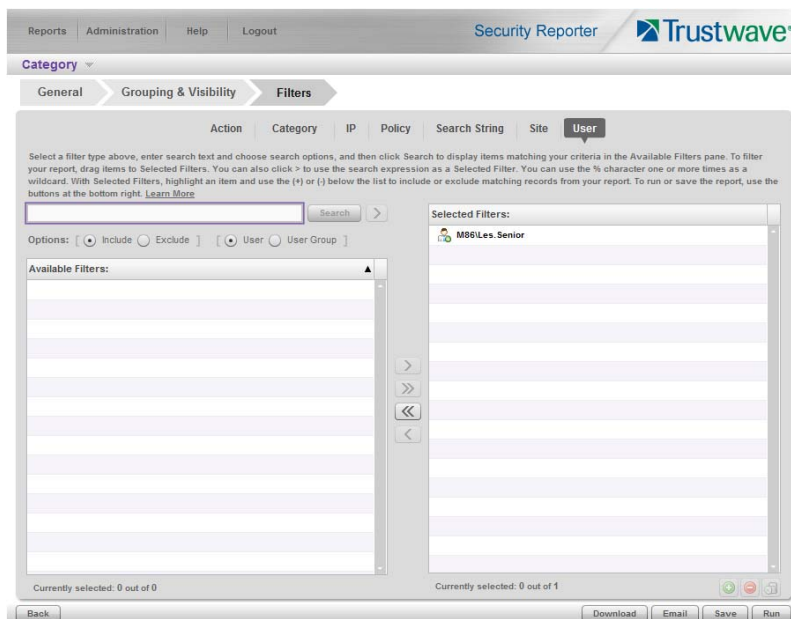
In the detail report view:

- Click any column header to sort by that column
- Use the scroll bar at the right to view the records on a page
- Use the **Previous** and **Next** buttons at the bottom right to view additional pages

### 3.3.1.6 View report filters

In the detail report view, click **Report Wizard** at the bottom left to return to the Wizard. Selections in the wizard are updated according to the selections you made while navigating through the data on screen.

- On the **General** tab, note that the “Passed” option is unchecked (because you chose to view Blocked items).
- On the **Grouping & Visibility** tab, note that the Group By setting and record limit have changed, and the selected report type is now a Detail report.
- On the **Filters** tab, click the **User** filter to review the user selection. This selection reflects the user you clicked. For details of how to set filters using this tab, see Section 4.



### 3.3.1.7 Download the report

To download a copy of the detail report, click **Download** at the bottom right of any Report Wizard tab. By default the download is in PDF format. You can change the format from a menu on the General tab of the wizard.

The output generated for download includes full details of URLs and any other columns you specified.

Security Reporter		January 1, 2013 - December 31, 2013		Trustwave®	
Category					
Date	Category	IP	User	Action	Policy
8/5/2013 03:15:15 AM	General Business	10.130.1.58	M86Les.Senior	Block	Load test medium policy
<a href="http://view.atdmt.com/AVE/View/misnknkcom010200074awe/direct/wl.309.hi.60.01/">http://view.atdmt.com/AVE/View/misnknkcom010200074awe/direct/wl.309.hi.60.01/</a>					
8/5/2013 03:15:23 AM	IT Security / IT Information	10.130.1.63	M86Les.Senior	Block	Load test medium policy
<a href="http://liveupdate.symantecliveupdate.com/mnitrn.flg">http://liveupdate.symantecliveupdate.com/mnitrn.flg</a>					
8/5/2013 03:31:30 AM	Other	10.130.0.174	M86Les.Senior	Block	Load test medium policy
<a href="http://store1.yimg.com/looxide_1803_3022418">http://store1.yimg.com/looxide_1803_3022418</a>					
8/5/2013 03:34:03 AM	Web Mail / Unified Messaging	10.130.1.58	M86Les.Senior	Block	Load test medium policy
<a href="http://us.f403.mail.yahoo.com/yml/ShowFolder?rb=Inbox&amp;reset=1&amp;Y=34736&amp;Y=1">http://us.f403.mail.yahoo.com/yml/ShowFolder?rb=Inbox&amp;reset=1&amp;Y=34736&amp;Y=1</a>					
8/5/2013 03:54:30 AM	Search Engines / Web Catalogs / Portals	10.130.1.183	M86Les.Senior	Block	Load test medium policy
<a href="http://us.a1.yimg.com/us.yimg.com/wl/fscodes/031016/ct_yad_031016.js">http://us.a1.yimg.com/us.yimg.com/wl/fscodes/031016/ct_yad_031016.js</a>					
8/5/2013 04:09:07 AM	Humor / Cartoons	10.130.1.63	M86Les.Senior	Block	Load test medium policy
<a href="http://www.medialunchbox.com/funny-pictures/139.html">http://www.medialunchbox.com/funny-pictures/139.html</a>					
8/5/2013 04:16:21 AM	Search Engines / Web Catalogs / Portals	10.130.1.63	M86Les.Senior	Block	Load test medium policy
<a href="http://us.d11.yimg.com/download.yahoo.com/0/0/mv/promo/1096500875.cab">http://us.d11.yimg.com/download.yahoo.com/0/0/mv/promo/1096500875.cab</a>					
8/5/2013 04:18:47 AM	General Business	10.130.1.171	M86Les.Senior	Block	Load test medium policy
<a href="http://ax.phobos.apple.com.edgesuite.net/WebObjects/MZStore.wa/wa.com.apple.ingle.appserver.client.MZiTunesClientCheck/version">http://ax.phobos.apple.com.edgesuite.net/WebObjects/MZStore.wa/wa.com.apple.ingle.appserver.client.MZiTunesClientCheck/version</a>					
8/5/2013 04:20:23 AM	Financial Services / Insurance / Real Estate	10.130.1.63	M86Les.Senior	Block	Load test medium policy
<a href="http://www.burstinet.com/cgi-bin/sr/re9838a.cgi?v=2_0&amp;sz=468e60AT726v90A/210044RETURN_CODE/US/">http://www.burstinet.com/cgi-bin/sr/re9838a.cgi?v=2_0&amp;sz=468e60AT726v90A/210044RETURN_CODE/US/</a>					
8/5/2013 04:38:19 AM	News / Magazines	10.130.1.171	M86Les.Senior	Block	Load test medium policy
<a href="http://ad.doubleclick.net/ad/jN2949.AKOA.Yahoo/B1206509.41.sz=728x90.dcopt=rdi.click=http://us.ard.yahoo.com/SIG=11u40u22/M=308687.5349708.6476479.54/Demv/S=150000261/N=EXP=1096639694/A=2341730/R=C=abr=aw.ont=1096653194498336">http://ad.doubleclick.net/ad/jN2949.AKOA.Yahoo/B1206509.41.sz=728x90.dcopt=rdi.click=http://us.ard.yahoo.com/SIG=11u40u22/M=308687.5349708.6476479.54/Demv/S=150000261/N=EXP=1096639694/A=2341730/R=C=abr=aw.ont=1096653194498336</a>					
8/5/2013 04:44:44 AM	Web Mail / Unified Messaging	10.130.1.171	M86Les.Senior	Block	Load test medium policy
<a href="http://us.rd.yahoo.com/req/loquid_rym/http://mail.yahoo.com">http://us.rd.yahoo.com/req/loquid_rym/http://mail.yahoo.com</a>					
8/5/2013 04:57:27 AM	Malware	10.130.1.227	M86Les.Senior	Block	Load test medium policy
<a href="http://updates.hotbar.com/updates/hotbar/hostol/buttons/v3.0/sg623/business_promo.zip">http://updates.hotbar.com/updates/hotbar/hostol/buttons/v3.0/sg623/business_promo.zip</a>					
8/5/2013 05:04:47 AM	Web Mail / Unified Messaging	10.130.0.174	M86Les.Senior	Block	Load test medium policy
<a href="http://us.f418.mail.yahoo.com/yml/login?rand=cl17p7dfq02">http://us.f418.mail.yahoo.com/yml/login?rand=cl17p7dfq02</a>					
August 19, 2013	4:22:50 PM	Pacific Daylight Time	Generated by: admin		Page 14 of 38

### 3.3.1.8 Save the report

If you want to run the same report again or schedule it to be run repeatedly, click **Save** at the bottom right to save the report.

You can modify any parameters before saving the report.

You can edit, run, or download saved reports by navigating to **Reports | Saved** from the main menu.



## 4 Report Wizard

The Report Wizard is a powerful tool that allows you to tailor reports to your specific needs. Once you have created a report format and parameters you can save the report to be run later. You can also schedule reports to run periodically.

### 4.1 Starting the Report Wizard

To start the Wizard, navigate to Reports | Drill Down | Report Wizard. Then, select a report type from the menu at the top left of the wizard.

You can also start the wizard by navigating to any of the summary reports under Reports | Drill Down (such as Category or Rule), and then clicking the Report Wizard button at the lower left of the screen.

Report types are defined as follows:

- **Category** - Features data for sites in each filter category accessed by end users.
- **Content Type** - Includes end user Internet access of objects utilizing an excessive amount of network bandwidth.
- **Rule** - Includes each instance in which an end user triggered a threshold in an SWG Security Policy.
- **Spyware** - Provides information for each instance in which an end user accessed content containing spyware.
- **Violation** - Provides information on each instance in which an end user breached a security policy.
- **Virus** - Includes details for each instance of a blocked virus detected from end user Internet/network activity.
- **Vulnerability Anti.Dote** - Provides details for each instance of real-time vulnerability detection resulting from end user Internet/network activity.

The Wizard includes three tabs: General, Grouping & Visibility, and Filters.

The following buttons are included at the bottom of the screen for all tabs:

- **Back**: returns you to the report view from which you accessed the report wizard (this button does not display if the Report Wizard was accessed from the main menu)
- **Download**: generates and downloads the report in the Export Format specified in the General tab
- **Email**: opens the Email Report page to allow you to enter options required to generate and send the report to specified email addresses
- **Save**: saves the currently selected report options from all tabs to Saved reports
- **Run**: generates a report to the screen using the selected options from all tabs. This option is available only for a single level report



### 4.1.1 General tab

On the General tab of the wizard, you can see summary information about the Group By and Filters settings.

You can enter or select from the following items:

- **Name & Description:** A name is required for reports you plan to save. Description text is optional.
- **Date Scope:** You can choose from pre-configured date scopes by selecting the top radio button and choosing from the menu. You can enter a specific date range (and a time range in some cases) by selecting the bottom radio button.



**Tip:** If you plan to save a report and run it repeatedly, use one of the pre-configures scopes such as “last week.”

- **Options:** You can select types of content by choosing from the following items. At least one of each pair must be selected.
  - **Blocked/Passed:** choose one or both to include requests that were blocked and/or passed.
  - **Page/Object:** choose one or both to include pages and/or objects.



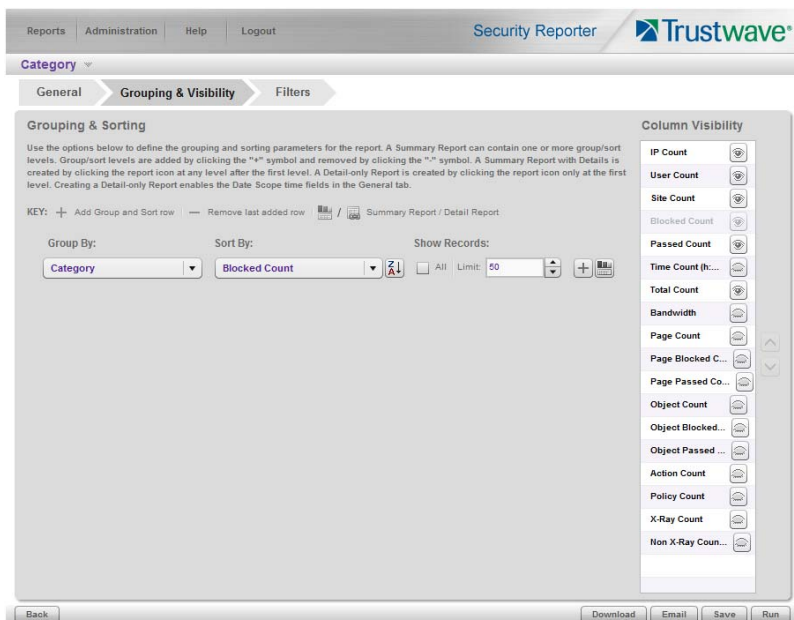
**Tip:** To review and configure which requests are counted as pages or objects, see Administration | System Configuration | Database | Page Definition.

- **X-Ray/Non X-Ray (SWG only):** choose one or both to include X-Ray (what-if) and/or applied rules.
- **Identified IPs/Unidentified IPs:** choose one or both to include requests from IP addresses that are associated with a known user and/or IP addresses that are not associated with a user.
- **Export Format:** For reports you plan to download or email, you can choose a file format.



### 4.1.2 Grouping and Visibility

On the Grouping & Visibility tab of the wizard, you can select grouping and sorting options, number of records, and visible columns.



#### 4.1.2.1 Group and Sort Rows



- **Group By:** This menu setting determines the heading (first column) of each summary row. By default the grouping follows the report type such as Category. Detail reports are not grouped. For detail reports, the group by setting is “Detail.”
- **Sort By:** This menu setting determines the initial order of detail rows.
- **Sort Order:** The button following the Sort By column allows you to select the default order of sorting. Click to change the order.



Indicates the report level will be sorted in ascending order.



Indicates the report level will be sorted in descending order.

- **Show Records:** You can choose to show all records, or limit the records to a specific number. By default summary reports limit to 50 items, and detail reports limit to 1000 items.
- **Add a row:** Click the  on the last row to add a new row below. Click the  on the last row to remove that row.



**Note:** Multi-level reports can take a long time to generate.

- **Summary or detail report:** On the last (or only) row, you can click the button to change between summary and detail output. Other rows are always generated as summaries.



Indicates a summary report.



Indicates a detail report.

#### 4.1.2.2 Column Visibility

Use the control at the right of the tab to select the columns in the report output. Click an “eye” to show or hide the corresponding column. An open eye indicates the column is included in the output. The “sort by” column is always set to visible.

#### 4.1.3 Filters tab

This tab of the wizard allows you to refine your report based on data of one or more types. Types include:

- The report type that you selected from the main menu or from the report type menu above the tabs (such as Category, Content Type, or Virus).
- **Action:** The action logged by the device you are reporting on.
- **IP:** The source IP of the request.
- **Policy:** The filtering or security policy that was triggered.
- **Search String** (available only for reports with a Detail row): Search terms present in the URL string, for supported search engines.
- **Site:** The target site of the request.
- **User:** The identified user who made the request.




Click any filter type tab to work with that filter type. You can filter on more than one type.

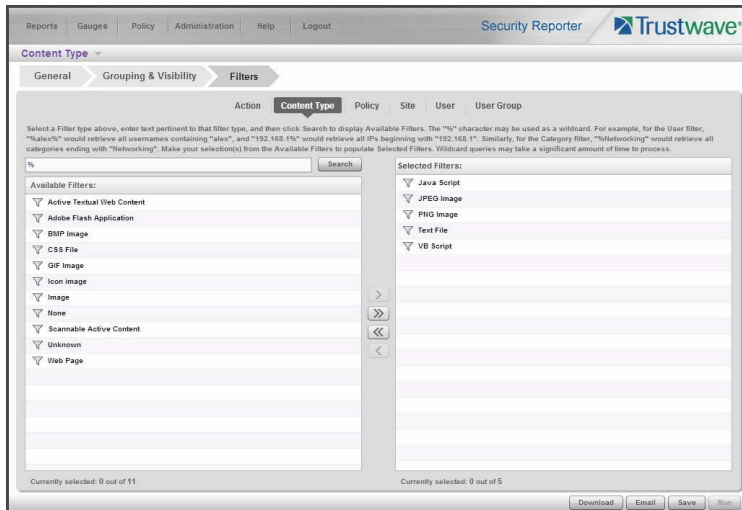



**Tip:** For more help and examples on the Filters tab, see the **Learn More** link from the text at the top of the tab.

To set up a filter:

1. In the search field, enter a search term. You can use the % character one or more times as a wildcard (matching one or more characters).
2. Choose search options using the radio buttons below the search field. The available options depend on the filter type. Include/Exclude is always available (used to indicate whether you want to find items that match, or do not match, the search terms). For details of other options see the Learn More link.
3. Use the search text in one of two ways:
  - Click **Search** to perform the query. Results appear in the Available Filters list box below. You can add one or more filters from the list to Selected Filters.

- Click the  button to add the search text directly to Selected Filters. The text including any wildcards will be evaluated each time the report is run.
4. To add items from Available Filters to Selected Filters, select and drag the items, or click to select, and then click the single right arrow  to move the filter(s) to the Selected Filters list box. Use the double right arrow  to move all items.



**Tip:** To remove any filter from the Selected Filters list box, select the items and click the single left arrow (or click the trash icon  at the bottom of the list). Use the double left arrow to remove all items.

5. You can include or exclude items matching a Selected Filter from the report.

- To include items matching a Selected Filter, highlight it and then click the  at the bottom of the list. The item icon shows the green + to indicate it is included.
- To exclude items matching a Selected Filter, highlight it and then click the  at the bottom of the list. The item icon shows the red - to indicate it is excluded.



**Tip:** Each filter type must have at least one Included Selected Filter.

6. Click a button to perform the specified action: Download, Email, Save, or Run.




**Note:** Any Selected Filters items that include the wildcard character % will be evaluated for new matching data each time the report is run. This function is useful for reports on use names, malware names, or any data set that could include new members.

#### 4.1.4 Wildcard filter examples


These examples show the difference between specific and wildcard filters.

#### 4.1.4.1 Users

1. Run the Report Wizard for any report type.
2. On the Filters tab, select the User filter type. Enter a search of `a%` (with search options Include and User).
3. Click Search to populate the Available Filters, and move all results to the Selected Filters.
  - If you save and run the resulting report, it will always include information for users with a name beginning in A that already existed when the report was created.
4. Remove the items from Selected Filters, and click the  (next to Search) to add the search expression to the Selected Filters.
  - If you save and run the resulting report, it will include information for users with a name beginning in A, including new users that were not present in the logs when you created the report.

#### 4.1.4.2 Virus Names

This example applies to SWG virus data.

1. Run the Report Wizard for Virus.
2. On the Filters tab, select the Virus filter type. Enter a search of `%worm%` (with search option Include).
3. Click Search to populate the Available Filters, and move all results to the Selected Filters.
  - If you save and run the resulting report, it will always include only the items that were available when the report was created. If no worm virus has been reported, you cannot save a useful report.
4. Remove the items from Selected Filters, and click the  (next to Search) to add the search expression to the Selected Filters.
  - If you save and run the resulting report, it will include any virus with a name containing the word "worm", including new items that were not logged when you created the report. Even if no worm virus has been reported previously, you can still save a report for future use.

#### 4.1.5 Generating a report

To generate a report immediately:

- For a single level report, click **Run** to generate and display the report on the screen
- For any report, click **Download** to generate the report to a file (in the format specified on the General tab) and download it to the workstation. The SR interface will be locked while the report is being generated.
- For any report, click **Email** to generate the report to a file and send the file (or a link) by email. The report will be generated in the background and you can continue to work. For full information about the email facility, see the *Security Reporter Administrator Guide*.

#### 4.1.6 Saving a report for later use

To save a report, click **Save**.



**Tip:** To save a report you must have given it a name (on the General tab of the wizard).

You can access saved reports by navigating to Reports | Saved.

You can schedule saved reports to run by navigating to Reports | Schedule.

For full information about how to use saved reports, see the *Security Reporter Administrator Guide*.

**About Trustwave®**

Trustwave is a leading provider of compliance, Web, application, network and data security solutions delivered through the cloud, managed security services, software and appliances. For organizations faced with today's challenging data security and compliance environment, Trustwave provides a unique approach with comprehensive solutions that include its TrustKeeper® portal and other proprietary security solutions. Trustwave has helped hundreds of thousands of organizations—ranging from Fortune 500 businesses and large financial institutions to small and medium-sized retailers—manage compliance and secure their network infrastructures, data communications and critical information assets.

Trustwave is headquartered in Chicago with offices worldwide. For more information, visit

<https://www.trustwave.com>.