Trustwave®

Smart security on demand

Security Reporter Administrator Guide

Version 3.5.0

December 20, 2016

Legal Notice

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/

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.

Formatting Conventions

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

Format and Symbols	Meaning
Blue Underline	A blue underline indicates a Web site or email address.
Bold	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`	Text in this format indicates computer code or information at a command line.
Italics	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.
🔍	**Note:** This symbol indicates information that applies to the task at hand.
💡	**Tip:** This symbol denotes a suggestion for a better or more productive way to use the product.
❗	**Caution:** This symbol highlights a warning against using the product in an unintended manner.

Table of Contents

List of Figures

1 Introductory Section

1.1 Security Reporter

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

Logs of end user Internet activity from the SWG or Web Filter appliances 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, graphical snapshots of network Internet traffic. Drilling down into the URL categories 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 About the *Administrator Guide*

The Security Reporter *Administrator Guide* primarily addresses the network administrator designated to configure and manage the Security Reporter application on the network. This administrator is referred to as the "global administrator" throughout this *Administrator Guide*. In part, this *Administrator Guide* also addresses administrators who manage user groups on the network. These administrators are referred to as "group administrators" throughout this *Guide*. Additional information is provided for administrators of networks that use the SR with the Trustwave Web Filter or Secure Web Gateway to obtain logs from the applications for generating productivity reports and security reports.

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

This *Administrator Guide* is organized into the following sections:

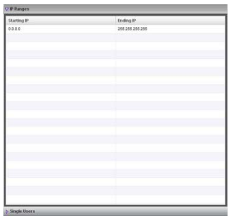
- **Introductory Section** - This section introduces the SR product, explains how to access and use the SR and this *Guide,* and provides information on how to contact the Trustwave Technical Assistance Center.
- **System Configuration Section** - This section pertains to information on configuring and maintaining the administrator console of the SR application.

- **Report Manager Administration Section** - This section pertains to configuring and maintaining the administration side of the SR's Report Manager application.
- **Reports Section** - Refer to this section for information about generating reports based on the log feeds from Web Filter or SWG.
- **Appendices** - Appendix A explains how to disable pop-up blocking software. Appendix B provides information on how to perform hardware maintenance and troubleshoot RAID on the SR chassis. Appendix C explains how to use the SR in the evaluation mode, and how to switch to the registered mode.
- **Index** - This section includes an index of subjects and the first page numbers where they appear in this *Guide*.

1.2.1 Terminology

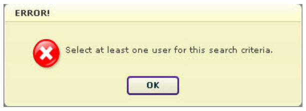
The following terms are used throughout this *Administrator Guide*. Sample images (not to scale) are included for each item.

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



Starting IP	Ending IP
0.0.0.0	255.255.255.255

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

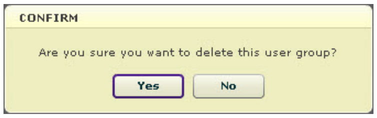

ERROR!

Select at least one user for this search criteria.

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

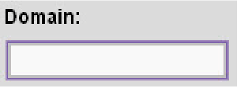
- **check box** - A small square in a dialog box, window, or panel used for indicating whether or not you wish to select an option. This object allows you to toggle between two choices. By clicking in this box, a check mark or an "X" is placed, indicating that you selected the option. When this box is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

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

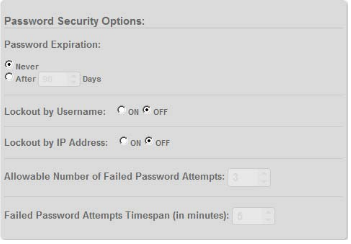

CONFIRM

Are you sure you want to delete this user group?

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



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



Password Security Options:

Password Expiration:

● Never
○ After 90 Days

Lockout by Username: ○ ON ● OFF

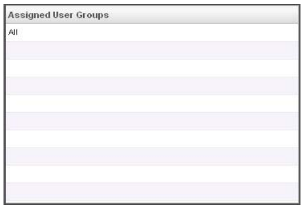
Lockout by IP Address: ○ ON ● OFF

Allowable Number of Failed Password Attempts: 3

Failed Password Attempts Timespan (in minutes): 5

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

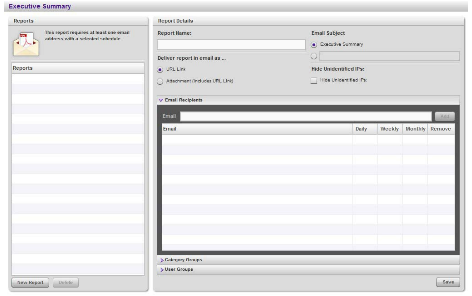
- **list box** - An area in a dialog box, window, or panel that accommodates and/or displays entries of items that can be added or removed.



Assigned User Groups

All

- **panel** - The central portion of a screen that is replaced by a different view when clicking a pertinent link or button. A sub-panel is a boxed-in section within a panel.



Executive Summary

Reports

This report requires at least one email address with a selected schedule.

Reports

Report Details

Report Name:

Deliver report in email as ...

● URL Link
○ Attachment (includes URL Link)

Email Subject

● Executive Summary
○

Hide Unidentified IPs:

□ Hide Unidentified IPs:

Email Recipients

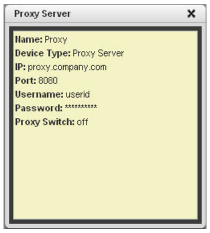
Email

Email	Daily	Weekly	Monthly	Remove

Category Groups

User Groups

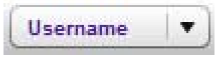
- **pop-up box** or **pop-up window** - A box or window that opens after you click a button in a dialog box, window, or panel. This box or window may display information, or may require you to make one or more entries. Unlike a dialog box, you do not need to choose between options.



Proxy Server

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

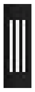
- **pull-down menu** - A field in a dialog box, window, or panel that contains a down arrow to the right. When you click the arrow, a menu of items displays from which you make a selection.



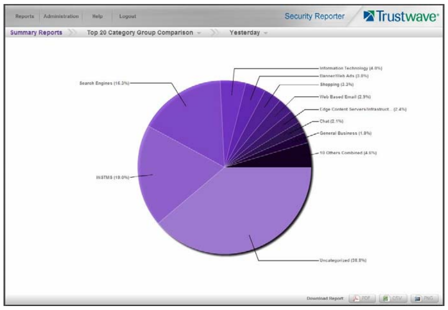
- **radio button** - A small, circular object in a dialog box, window, or screen used for selecting an option. This object allows you to toggle between two choices. By clicking a radio button, a dot is placed in the circle, indicating that you selected the option. When the circle is empty, the option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

● All

- **re-size button** - Positioned between two boxes in a panel, this button enlarges a section or makes that section narrower when clicked and dragged in a specific direction.

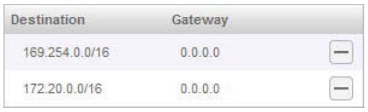


- **screen:** A main object of an application that displays across your monitor. A screen can contain panels, sub-panels, windows, frames, fields, tables, text boxes, list boxes, icons, buttons, and radio buttons.



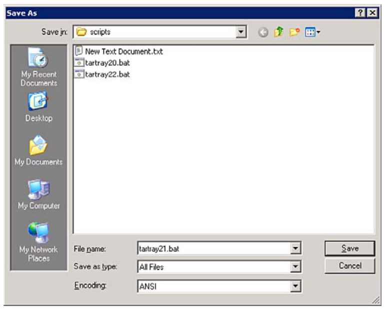
- **tab**: One of at least two objects positioned beside one another that display content as specified by its label when clicked. A tab can display anywhere in a panel, usually above a box or list box.

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



Destination	Gateway	
169.254.0.0/16	0.0.0.0	⊟
172.20.0.0/16	0.0.0.0	⊟

- **text box** - An area in a dialog box, window, or screen that accommodates your data entry. A text box is a type of field. (See “field”.)
- **window** - Can contain frames, fields, text boxes, list boxes, icons, buttons, and radio buttons. Types of windows include ones from the system such as the Save As window, pop-up windows, or login windows.



Save in: scripts

New Text Document.txt
tartray20.bat
tartray22.bat

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

1.3 Overview

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

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

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

1.4 Components and Environment

1.4.1 Components

1.4.1.1 Hardware

- High performance server equipped with RAID

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

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

1.4.1.2 Software

- TrustOS® hardened Linux-based Operating System
- Administrator Graphical User Interface (GUI) console utilized by an authorized administrator to configure and maintain the SR application
- MySQL database

1.4.2 Environment

1.4.2.1 Network Requirements

- Power connection protected by an Uninterruptible Power Supply (UPS)
- HTTPS connection to Trustwave’s software update server
- High speed access to the SR server by authorized client workstations
- Ports 8443 and 8843 must be available for the SR user interface to use

1.4.2.2 Administrator Workstation Requirements

The following browsers are tested and fully supported for access to the SR web interfaces:

- Internet Explorer 11
- Edge 14
- Firefox (current versions)
- Google Chrome (current versions)
- Safari 9 and 10

Tip: Previous browser versions can generally be used for access to the Report Manager. The System Configuration interface requires a HTML5 compliant browser.

Also be aware of the following requirements:

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

- Pop-up blocking software, if installed, must be disabled.

Note: Information about disabling pop-up blocking software can be found in Appendix A.

1.5 Getting Started

1.5.1 Initial Setup

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

Caution: In order to prevent data from being lost or corrupted while the SR is running, the server should be connected to a UPS or other battery backup system.

Once you turn on the SR server, **DO NOT** interrupt the initial boot-up process. This process may take from five to 10 minutes per drive. If the process is interrupted, damage to key files may occur.

1.5.2 Procedures for Logging In, Out

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

1.5.2.0.1 Enter Report Manager’s URL in the Address field

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

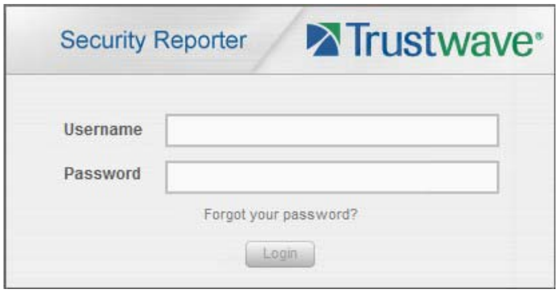
1. Launch an Internet browser window supported by the SR.
2. In the address line of the browser window, enter the address of SR:
   “https://”, the SR server’s IP address or hostname, a colon “**:**” and port number “8443” for a secure network connection. For example:
   - If the IPv4 address is 210.10.131.34, type in `https://210.10.131.34:8443`.
   - If the IPv6 address is 2001:db8:8:4::2, type in `https://[2001:db8:8:4::2]:8443`.

   Tip: IPv6 addresses must be enclosed in square brackets, as shown, with the port number outside the brackets.

   - If the hostname is logo.com, type in `https://logo.com:8443`.

   With a secure connection, the first time you attempt to access the SR’s user interface in your browser you will be prompted to accept the security certificate. In order to accept the security certificate for your browser, follow the instructions at: http://www.trustwave.com/software/8e6/ts/wf-sec-cert.html

3. Press **Enter** or click **Go** to open the login window of the SR user interface:



1.5.2.1 Log In

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

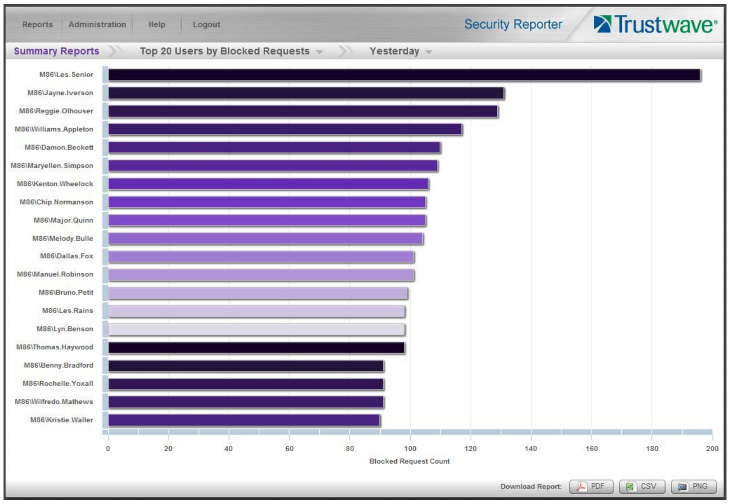
Tip: In any box or screen in the application, press the Tab key on your keyboard to move to the next field. To return to a previous field, press Shift-Tab.

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

Tip: Trustwave recommends administrators who access this application for the first time should change their account password. Administrator usernames and passwords are modified in Report Manager: Administration | Admin Profiles.

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

3. Click **Login** to display the Summary Reports panel of the Report Manager user interface:



Note: On a newly installed unit, SR reporting data is inaccessible and will not display in the dashboard until the SR server is configured, a log generating filter (Web Filter or SWG) is added to the device registry (via Reporter Manager: Administration | Device Registry), logs are transferred to the SR, and the database is built.

Building the database could take about 24 hours. If a software update was recently applied on an existing server, it could take several hours before data is available.

1.5.2.1.1 Re-login

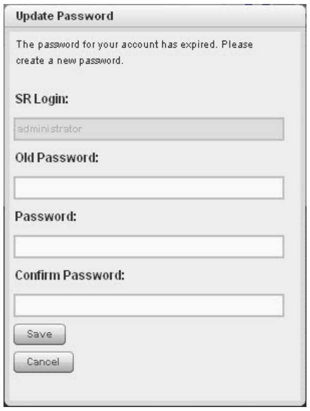
Each session is timed so that it remains active as long as there is activity in the user interface within an eight hour period. You need to log into the application again after an eight hour period of inactivity, or in the event that the SR server was restarted.

If your session in the application is timed out, when you click a button, thumbnail, or menu item in the Report Manager, an alert box opens with a message notifying you that the session timed out.

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

1.5.2.1.2 Expired Passwords

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



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

SR Login: administrator

Old Password:

Password:

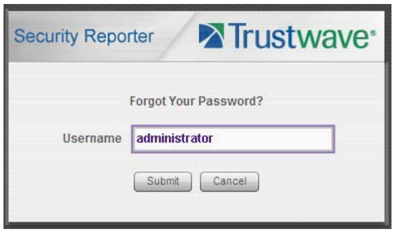
Confirm Password:

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

1.5.2.1.3 Forgot Your Password

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

1. Click the **Forgot your password?** link in the login window to open the Forgot Your Password? window:



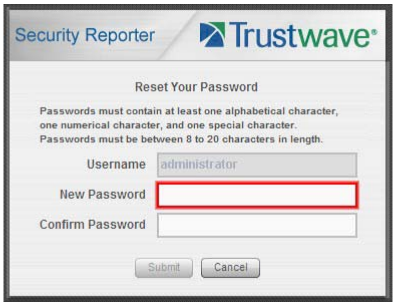
Username: administrator

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

2. Enter your **Username** and then click **Submit** to open an alert box informing you that “An email has been sent with instructions to reset your password.”
3. Click **OK** to close the alert box and then check your email account (set up for your profile in Report Manager: Administration | Admin Profiles) for the “Security Reporter password reset” message.

Note: The action of clicking “OK” displays the original login window.

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



Reset Your Password

Passwords must contain at least one alphabetical character, one numerical character, and one special character. Passwords must be between 8 to 20 characters in length.

Username: administrator

New Password:

Confirm Password:

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

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

1.5.2.1.4 Single Sign-On Access

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

Tip: With a secure connection, the first time you attempt to access the Web Filter (Administration > Web Filter) from within the SR in your browser you may encounter a connection warning. This may occur if you have not accessed the WF with that browser and accepted the security certificate.

To resolve this issue, navigate directly to the Web Filter user interface in your browser. You will be prompted to accept the security certificate. For details of how to accept the security certificate for your browser, follow the instructions at: http://www.trustwave.com/software/8e6/ts/wf-sec-cert.html

1.5.2.1.5 Default Usernames and Passwords

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

Application	Username	Password
Security Reporter	admin	testpass
Web Filter	admin	user3

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

1.5.2.2 User Interface Navigation

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

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

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

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

1.5.2.2.1 Links in the Report Manager Navigation Toolbar

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

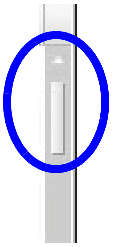
- **Reports** - Hover over this link to open the Reports menu. Global and group administrators can click any Report menu item to view or generate a report, or schedule a report to run.
- **Administration** - Hover over this link to view menu options for setting and maintaining administrator profiles and groups, maintaining the Report Manager, and managing the SR.
- **Help** - Hover over this link to view menu options for assisting you in configuring this SR:
  - **Online Help** - Clicking this link accesses the Web page at trustwave.com containing links to the latest documentation for this application in the .pdf format.
  - **About...** - Clicking this link opens a pop-up window containing information about the current software Version, and hardware Serial number if this SR is running on a Trustwave SR appliance. This criteria can be copied and pasted into an email or online form to be submitted to Trustwave for troubleshooting purposes. Click “Close” to close the pop-up window.
- **Logout** - Click this link to log out of the SR (see Log Out for details on log out procedures).

1.5.2.2.2 Navigation Tips and Conventions

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

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

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



- **Expand, contract a column** - Columns can be expanded or contracted by first hovering over the divider in the column header to display the arrow and double line characters (<-ll->). A column is then expanded or contracted by left-clicking the mouse and dragging the column bar to the right or left.

- **Browser back button, refresh button** - Clicking either the back button in the browser window or the refresh button in your browser will refresh the SR user interface and log you out of the application.
- **Select multiple items in specified windows** - In specified panels, when moving several items from one list box to another, or when deleting several items, the Ctrl and Shift keys can be used to expedite this task.
  - **Ctrl Key** - To select multiple items from a list box, click each item while pressing the Ctrl key on your keyboard.
  - **Shift Key** - To select a block of consecutive items from a list box, click the first item, and then press the Shift key on your keyboard while clicking the last item.

  Once the group of items is selected, click the appropriate button to perform the action on the items.
- **Sort records by another column header** - Records can often be sorted by a different column header by clicking the header for that column. This action sorts the records that display in descending order by that column. Clicking the same column header again sorts the records in ascending order by that column.
- **View tooltip information** - To view information about any object that has a circled “i” icon beside it, hover over the icon to display tooltips that explain how to use that button or field. ⓘ

1.5.2.2.3 Wildcard Searches

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

   Examples:

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

1.5.2.2.4 Links in the System Configuration Navigation Toolbar

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

- **Network** - Select a menu item to access its corresponding page used for creating and maintaining network configuration settings on the SR server.

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

1.5.2.3 Log Out

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

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

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

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

1.5.3 Technical Support / Product Warranties

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

2 System Configuration Section

2.1 Introduction

This section of the *Administrator Guide* provides instructions to assist a global administrator with the tasks required to configure and manage the SR server.

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

- Executes Installation procedures defined in the Installation Guide
- Provides a suitable environment for the server, including:
  - High speed, HTTPS link to the current logging device
  - Power connection protected by an Uninterruptible Power Supply (UPS)
  - High speed access to the server by authorized client workstations
- Sets up and maintains networking for the SR, update servers, and log sources
- Optionally configures email settings and SNMP settings for automatic alerts to administrators
- Updates the server with software updates supplied by Trustwave
- Analyzes server statistics
- Utilizes diagnostics for monitoring the server status to ensure optimum functioning of the server

To perform configuration, a Global Administrator uses the System Configuration Console, the Device Registry, and other screens available from the Administration menu of the Report Manager.

2.2 System Configuration Console

If your account profile is set up as a Global Administrator, you can access the System Configuration administrator console by navigating in the Report Manager to Administration | System Configuration.

The System Configuration user interface launches in a separate window/tab and provides access to configuration screens. By default the Software Update screen displays.

Note: See Section 2.2.7 for information about this screen.

The System Configuration administrator console provides access to a number of basic configuration and diagnostic items. To access an item, select it using the menu at the top of the screen. The menu is organized as follows:

- **General:** Network (routing and diagnostics), Self-Monitoring, SNMP.
- **Application:** Settings (page views and definitions), Lockouts, Password Security, Software Update.

- **Support:** RAID Array status, Tools (Database diagnostics, Support package generation).
- **Restart:** Options to restart system services.
- **Shutdown:** Options to shut down the system.
- **Help:** Access to the latest documentation for SR.
- **Logout:** Option to log out of the System Configuration and Report Manager web applications.

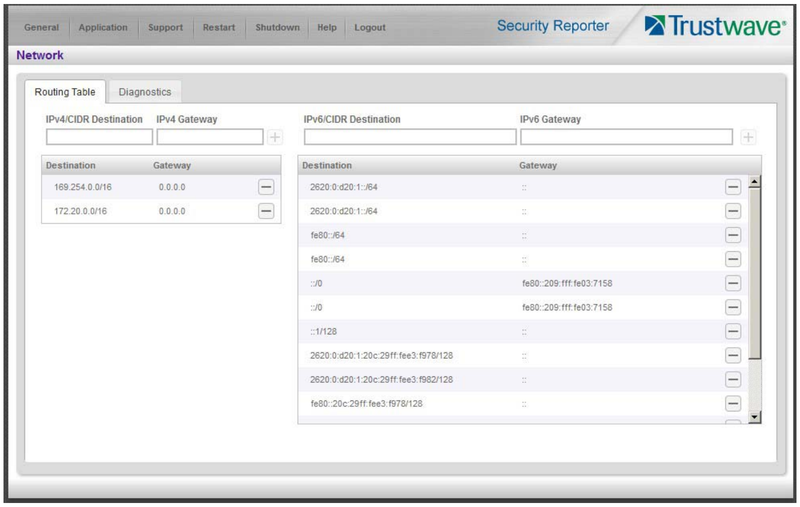
2.2.1 Network screen

To open the Network screen, select **Network** from the General menu.

The Network screen includes routing table setup and network diagnostics. To access these screens, select Network from the General menu. To switch between the Routing Table and Diagnostics, click the tabs at the top of the panel.

2.2.1.1 Routing Table tab

This tab allows you to view, build, and maintain a list of routers that the server will use to communicate with other segments of the network. You will only need to set up a routing table if your local network is interconnected with another network. Each entry in the table is defined as a destination network (IP range in CIDR notation), and the IP address of the gateway for that network. You can use both IPv4 and IPv6 networking, as required.



Destination	Gateway
169.254.0.0/16	0.0.0.0
172.20.0.0/16	0.0.0.0

Destination	Gateway
2620:0:d20:1::/64	::
2620:0:d20:1::/64	::
fe80::/64	::
fe80::/64	::
::/0	fe80::209:fff:fe03:7158
::/0	fe80::209:fff:fe03:7158
::1/128	::
2620:0:d20:1:20c:29ff:fee3:f978/128	::
2620:0:d20:1:20c:29ff:fee3:f982/128	::
fe80::20c:29ff:fee3:f978/128	::

2.2.1.1.1 View a List of Routes

The tab displays two lists of routes (IPv4 and IPv6). Each route that was configured in the routing table displays as a separate row in the table. The Destination column shows the network definition in CIDR notation. The Gateway column shows the IP address of the portal that will transfer data packets to and from the destination network.

2.2.1.1.2 Add a Route

You can add an IPv4 or IPv6 route using boxes at the top of the corresponding list.

1. In the **IP/Destination** field, enter the IP range of the network that can be reached via this route This information should be entered as an address and CIDR prefix (for example, `10.10.10.0/24`).
2. In the **Gateway** field, enter the IP address of the portal to which data packets will be sent when addressed to the destination network.
3. Click the ⊞ button to include your entry in the table. If you have another route to add, follow steps 1-4.

Tip: The data you enter must be in the correct format. The button will be disabled if the data is not well formed.

2.2.1.1.3 Delete a Route

1. Click the ⊟ button of the row corresponding to the route you wish to remove from the routing table.

2.2.1.2 Diagnostics tab

The Diagnostics tab provides two tools that can help you to identify and resolve problems with your network configuration: ping and traceroute.

Tip: To switch between the Routing Table and Diagnostics, use the tabs at the top of the Network panel.

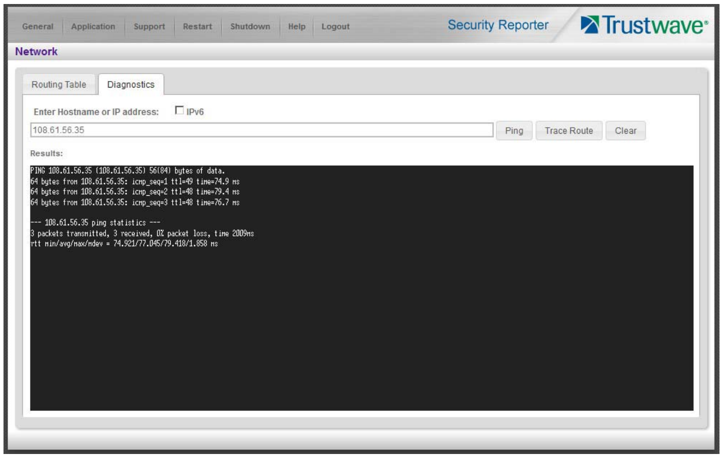
The ping utility is used for verifying whether the server can communicate with a machine at a given IP address within the network, and the speed of the network connection.

The Trace Route tool records each “hop” (trip from one router to another) the data packet made, identifying the IP addresses of gateway computers where the packet stopped en route to its final destination, and the length of time of each hop.

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

To use this tab:

1. Enter a hostname or IP address in the field at the top of the tab.
2. If you entered an IPv6 address, or to contact a host over IPv6, check the box **IPv6**. Otherwise, clear this box.
3. Click the **Ping** button to display the results found by the server, as shown on the sample screen:



Enter Hostname or IP address: ☐ IPv6

108.61.56.35

Results:

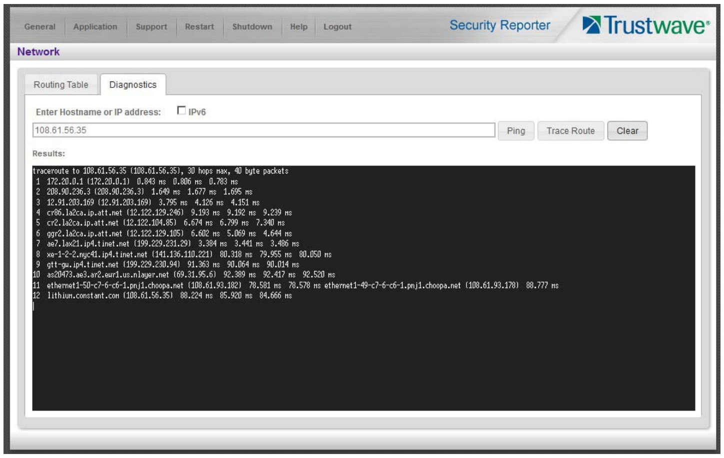
```
PING 108.61.56.35 (108.61.56.35) 56(84) bytes of data.
64 bytes from 108.61.56.35: icmp_seq=1 ttl=49 time=74.9 ms
64 bytes from 108.61.56.35: icmp_seq=2 ttl=48 time=79.4 ms
64 bytes from 108.61.56.35: icmp_seq=3 ttl=48 time=76.7 ms

--- 108.61.56.35 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2009ms
rtt min/avg/max/mdev = 74.921/77.045/79.418/1.858 ms
```

As indicated by the results for the sample entry, the server was able to communicate with the machine at the IP address 108.61.56.35. (This is one of the NTP servers configured in the SR by default). The statistics show that three (3) data packets were transmitted by the server, and three (3) packets were received by the designated machine, for a total of zero (0) percent packet loss.

Tip: If the machine cannot be contacted, be sure that the machine is configured to respond to ping requests and that any intermediate firewall devices are configured to pass ping requests.

4. Click the **Trace** button to display the results found by the server, as shown on the sample screen:



Enter Hostname or IP address: ☐ IPv6

108.61.56.35

Results:

```
traceroute to 108.61.56.35 (108.61.56.35), 30 hops max, 40 byte packets
 1  172.20.0.1 (172.20.0.1)  0.843 ms  0.806 ms  0.783 ms
 2  208.90.236.3 (208.90.236.3)  1.649 ms  1.677 ms  1.695 ms
 3  12.91.203.169 (12.91.203.169)  3.795 ms  4.126 ms  4.151 ms
 4  cr86.la2ca.ip.att.net (12.122.129.246)  9.193 ms  9.192 ms  9.239 ms
 5  cr2.la2ca.ip.att.net (12.122.104.85)  6.674 ms  6.799 ms  7.340 ms
 6  ggr2.la2ca.ip.att.net (12.122.129.105)  6.602 ms  5.069 ms  4.644 ms
 7  ae7.lax21.ip4.tinet.net (199.229.231.29)  3.384 ms  3.441 ms  3.486 ms
 8  xe-1-2-2.nyc41.ip4.tinet.net (141.136.110.221)  80.318 ms  79.955 ms  80.050 ms
 9  gtt-gw.ip4.tinet.net (199.229.230.94)  91.363 ms  90.064 ms  90.014 ms
10  as20473.ae3.ar2.ewr1.us.nlayer.net (69.31.95.6)  92.389 ms  92.417 ms  92.520 ms
11  ethernet1-50-c7-6-c6-1.pnj1.choopa.net (108.61.93.182)  78.581 ms  78.578 ms ethernet1-49-c7-6-c6-1.pnj1.choopa.net (108.61.93.178)  88.777 ms
12  lithium.constant.com (108.61.56.35)  88.224 ms  85.920 ms  84.666 ms
```

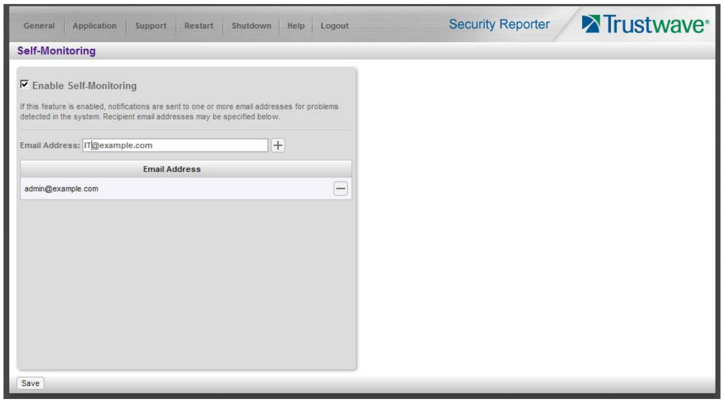
As indicated by the results for the sample entry, the packet made 12 hops. For each line in the report, the hop number displays, followed by the IP address or hostname; the IP address in parentheses; and the maximum, minimum, and average response time in milliseconds.

To check another name or address, click **Clear** and then follow the steps above.

2.2.2 Self-Monitoring screen

To open the Self-Monitoring screen, select **Self-Monitoring** from the General menu.

The Self-Monitoring screen is used to set up and maintain a list of e-mail addresses of contacts who will receive automated notifications about problems with the SR server, as well as system shutdown and restart progress notifications. Possible alerts include situations in which a daemon stops running, software fails to run, corrupted files are detected, or a power outage occurs. Notifications are also sent periodically during system shutdown or restart procedures that take an extended time to complete.



☑ Enable Self-Monitoring

If this feature is enabled, notifications are sent to one or more email addresses for problems detected in the system. Recipient email addresses may be specified below.

Email Address: IT@example.com +

Email Address
admin@example.com −

Save

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

Note: This service depends on correct SMTP server settings. See Section 2.3.3.

2.2.2.1 View a List of Contact E-Mail Addresses

If this feature is currently activated, the configured email addresses display.

2.2.2.2 Set up and Activate Self-Monitoring

1. Check the box **Enable Self-Monitoring.**
2. Enter an email address, and then click + to add the address to the list.
3. To add additional addresses, repeat step 2. Up to five addresses can be entered.
4. Click the **Save** button to activate self-monitoring.

2.2.2.2.1 Remove Recipient from E-mail Notification List

To stop sending alerts and notifications to an e-mail address set up in the list, click the − next to the address, and then click the **Save** button.

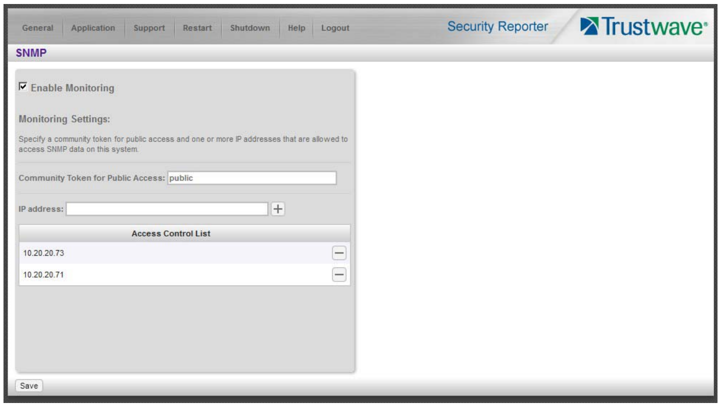
2.2.2.3 Deactivate Self-Monitoring

1. Clear (uncheck) the box **Enable Self-Monitoring.**
2. Click the **Save** button to deactivate self-monitoring. The list of addresses is retained, but no messages will be sent.

2.2.3 SNMP screen

To open the SNMP screen, select **SNMP** from the General menu.

The SNMP screen lets a global administrator use a third party Simple Network Management Protocol (SNMP) product to monitor and manage the working status of the SR over the network.



☑ Enable Monitoring

Monitoring Settings:

Specify a community token for public access and one or more IP addresses that are allowed to access SNMP data on this system.

Community Token for Public Access: public

IP address: ⊞

Access Control List
10.20.20.73 ⊟
10.20.20.71 ⊟

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

2.2.3.1 Enable SNMP

SNMP monitoring is disabled by default. To enable SNMP, check the box **Enable Monitoring** and, after making entries in the other fields as described below, click **Save.**

2.2.3.2 Set up Community Token for Public Access

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

2.2.3.3 Create, Build the Access Control List

1. In the **IP address** field, enter the IP address of a device that is allowed to access SNMP data on this SR.
2. Click ⊞ to include the entry in the Access control list box.

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

2.2.3.4 Maintain the Access Control List

To remove an IP address from the list, click the ⊟ next to that address, and then click **Save**.

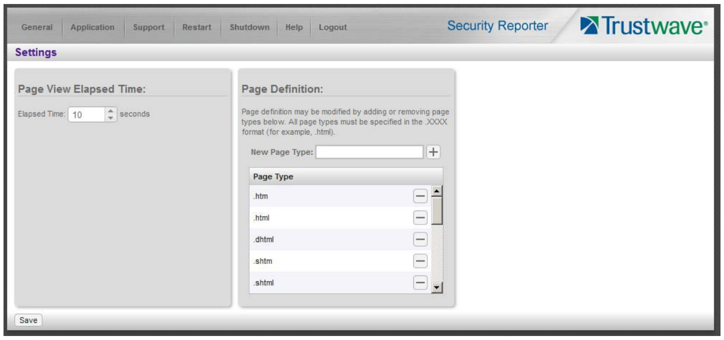
2.2.3.5 Disable SNMP

To disable SNMP, clear (uncheck) the box **Enable Monitoring** and then click **Save.**

2.2.4 Settings screen

To open the Settings screen, select **Settings** from the Application menu.

The Settings screen allows you to configure two settings that affect reporting: Page View elapsed time, and Page definition. If this SR provides reporting for Web Filter, the Settings screen also allows you to specify whether to import Objects log records.



Page View Elapsed Time:

Elapsed Time: 10 seconds

Page Definition:

Page definition may be modified by adding or removing page types below. All page types must be specified in the .XXXX format (for example, .html).

New Page Type:

Page Type
.htm
.html
.dhtml
.shtm
.shtml

2.2.4.1 Page View Elapsed Time panel

The Page View Elapsed Time panel allows to set a time value that is used when reporting the length of a user’s stay at a given Web site, and the number of times the user accesses that site.

2.2.4.1.1 Elapsed Time Rules

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

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

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

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

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

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

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

2.2.4.1.2 Establish the Unit of Elapsed Time for Page Views

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

2.2.4.2 Page Definition panel

The Page Definition panel allows you to specify the types (file extensions) that will be considered as "pages." This setting is used to distinguish between page and object requests in the database. This setting affects calculations for Page Count and Object Count. It also determines which requests will be included in the detail report for Page searches.

2.2.4.2.1 View the Current Page Types

The Page Types list box displays the extensions of files that are considered as pages.

2.2.4.2.2 Remove a Page Type

To remove a page type from the list:

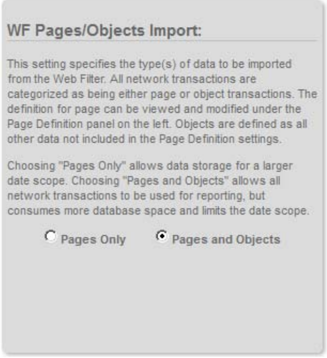
1. Click the ⊟ next to the page extension in the Page Types list box.
2. Click **Save**.

2.2.4.2.3 Add a Page Type

To add a page type to the list:

1. Enter the **New Page Type** extension.
2. Click ⊞ to include the extension in the Page Types list box.
3. Click **Save.**

2.2.4.3 Web Filter Pages or Objects Import



WF Pages/Objects Import:

This setting specifies the type(s) of data to be imported from the Web Filter. All network transactions are categorized as being either page or object transactions. The definition for page can be viewed and modified under the Page Definition panel on the left. Objects are defined as all other data not included in the Page Definition settings.

Choosing "Pages Only" allows data storage for a larger date scope. Choosing "Pages and Objects" allows all network transactions to be used for reporting, but consumes more database space and limits the date scope.

○ Pages Only ● Pages and Objects

If the SR is configured to report on Web Filter data, in the WF Pages/Objects Import frame, indicate whether drill down, Time Usage reports, and scheduled custom reports will include Web page hits only, or both Web page and object hits. Objects include images, graphics, multimedia items, and text item object files.

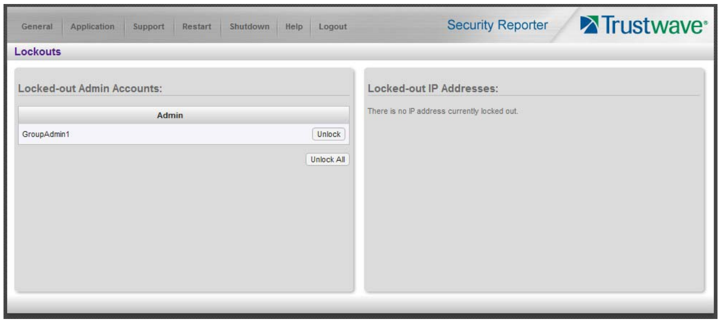
Caution: If “Pages only” is selected, **all** records of objects accessed by end users will be lost for the time period in which this option was enabled. Even if there were objects accessed by end users during that time period, zeroes (“0”) will display for object activity in generated reports.

1. Select one of two radio buttons to specify the type of hits to be included in drill down, Time Usage reports, and scheduled custom reports:
   - “Pages only” - Choose this option to include *only* Web page hits in reports.
   - “Pages and Objects” - Choose this option to include *both* Web page and object hits in reports.
2. Click the **Save** button on the parent frame to apply your setting.

2.2.5 Lockouts screen

To open the Lockouts screen, select **Lockouts** from the Application menu.

The Lockouts screen is used for unlocking accounts or IP addresses of administrators currently locked out of the SR user interface.



Lockouts

Locked-out Admin Accounts:

Admin
GroupAdmin1

Locked-out IP Addresses:

There is no IP address currently locked out.

Note: An account or IP address becomes locked if the Password Security Options feature is enabled in the Password Security screen (see Section 2.2.6), and a user has made the specified number of failed password attempts within the designated timespan.

2.2.5.1 View Locked Accounts, IP addresses

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

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

If there are any locked accounts/IP addresses in a frame, each locked username/IP address displays on a separate line followed by an **Unlock** button. An **Unlock All** button displays at the bottom of the frame.

2.2.5.2 Unlock Accounts, IP addresses

To unlock an account/IP address in a frame:

1. Click the **Unlock** button corresponding to the username/IP address.

Tip: To unlock all accounts/IPs in a frame, click **Unlock All**.

2. Click **Unlock** to unlock the specified accounts/IPs.

2.2.6 Password Security screen

To open the Password Security screen, select **Password Security** from the Application menu.

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

Note: User accounts can be manually unlocked via System Configuration: Network | Lockouts | Locked-out Accounts and IPs (see Section 2.2.5).

1. Enable any of the following options:
   - At the **Password Expiration** field, click the radio button corresponding to either password expiration option:
     - **Never**: Choose this option to set passwords to never expire.
     - **After 'x' Days**: Choose this option to set passwords to expire after the set number of days.

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

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

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

- **Allowable Number of Failed Password Attempts**: With the Lockout by Username and/or Lockout by IP Address option(s) enabled, enter the number of times a user can enter an incorrect password during the interval defined in the Failed Password Attempts Timespan (in minutes) field before being locked out of the SR user interface.

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

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

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

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

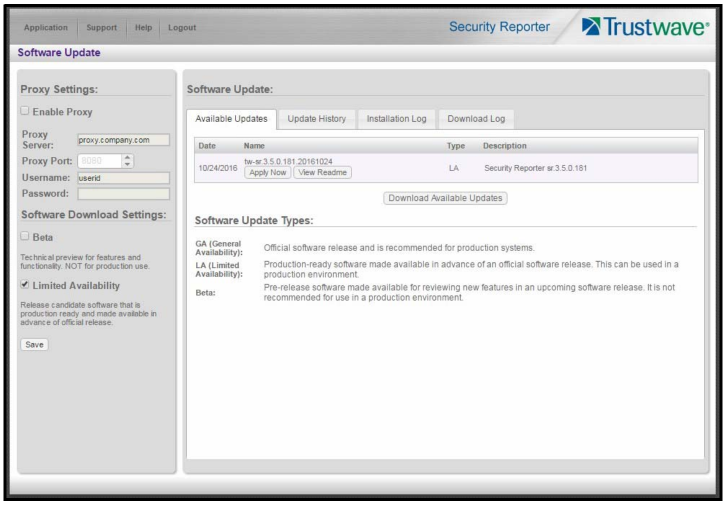
2.2.7 Software Update screen

To open the Software Update screen, select **Software Update** from the Application menu. This screen is the default view when the System Configuration window opens.

The right (**Software Update**) panel of this screen allows you to update the SR with software updates supplied by Trustwave, verify the download and/or installation of software updates on the SR, and view a list of software updates currently available and/or previously installed on the SR. This screen is also used to accept and apply Limited Availability (LA) and/or Beta updates, if you choose to preview software features to be included in the General Availability (GA) release distributed to all SRs.

The left panel of this screen includes two sections. The **Proxy Settings** section allows you to configure a proxy server that will be used to check for and downloads software updates. The **Software Update Settings** section allows you to choose the types of optional updates that the SR will download and offer for installation. Optional updates include LA and Beta updates.

Figure 1: Software Update Screen



Software Update

Proxy Settings:

□ Enable Proxy

Proxy Server: proxy.company.com
Proxy Port: 8080
Username: userid
Password:

Software Download Settings:

□ Beta

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

☑ Limited Availability

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

Software Update:

Date	Name	Type	Description
10/24/2016	tw-sr.3.5.0.181.20161024 Apply Now View Readme	LA	Security Reporter sr.3.5.0.181

Software Update Types:

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

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

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

Note: Definitions for Software Update Types (GA, LA, and Beta) are provided on the Available Updates tab of the Software Update panel.

General Availability (GA) software updates are supplied to all current SR units. Limited Availability (LA) and/or Beta software updates are available to SR units that have the feature to download LA and/or Beta software updates enabled, as described in Section 2.2.7.10.

2.2.7.1 View Available Updates

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

Tip: The SR checks for updates on a regular schedule. To check for updates manually, see Section 2.2.7.5.

The **Apply Now** and **View Readme** buttons display beside the software update Name. (See the next section for information about these buttons.)

2.2.7.2 Install a Software Update.

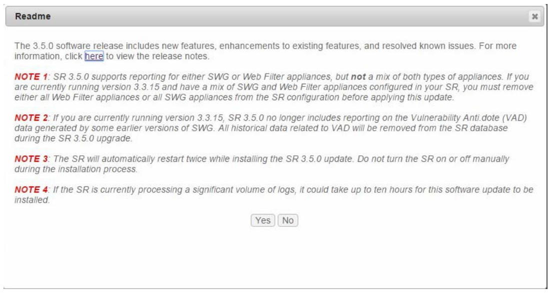
Caution: In most cases, all software updates must be installed in order from oldest to newest.

Note: Be sure to terminate all reports that are currently running or are scheduled to run before applying a software update.

The steps in this sub-section apply to the installation of General Availability software updates, and the application of LA/Beta software updates following the initial LA/Beta software download acceptance procedures (described in Section 2.2.7.3).

In the SR Software Updates frame, two buttons are available: **View Readme** and **Apply Now**.

1. Click **README** to open a window containing information about the software release.



The 3.5.0 software release includes new features, enhancements to existing features, and resolved known issues. For more information, click here to view the release notes.

NOTE 1: *SR 3.5.0 supports reporting for either SWG or Web Filter appliances, but* **not** *a mix of both types of appliances. If you are currently running version 3.3.15 and have a mix of SWG and Web Filter appliances configured in your SR, you must remove either all Web Filter appliances or all SWG appliances from the SR configuration before applying this update.*

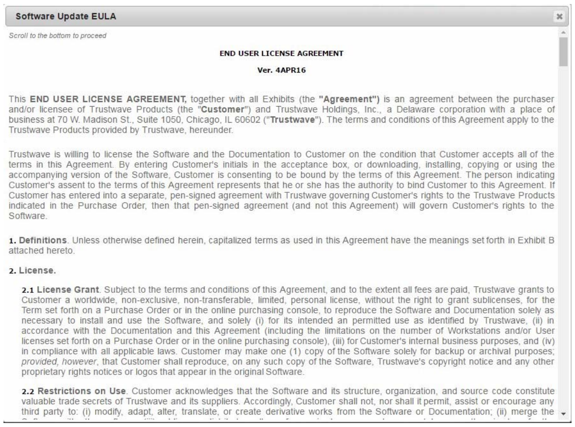
NOTE 2: *If you are currently running version 3.3.15, SR 3.5.0 no longer includes reporting on the Vulnerability Anti.dote (VAD) data generated by some earlier versions of SWG. All historical data related to VAD will be removed from the SR database during the SR 3.5.0 upgrade.*

NOTE 3: *The SR will automatically restart twice while installing the SR 3.5.0 update. Do not turn the SR on or off manually during the installation process.*

NOTE 4: *If the SR is currently processing a significant volume of logs, it could take up to ten hours for this software update to be installed.*

After reading the contents of the software release, click **Close** to close the window.

2. Click **Apply Now** to open the EULA dialog box:



Scroll to the bottom to proceed

END USER LICENSE AGREEMENT

Ver. 4APR16

This **END USER LICENSE AGREEMENT,** together with all Exhibits (the **"Agreement")** is an agreement between the purchaser and/or licensee of Trustwave Products (the "**Customer**") and Trustwave Holdings, Inc., a Delaware corporation with a place of business at 70 W. Madison St., Suite 1050, Chicago, IL 60602 ("**Trustwave**"). The terms and conditions of this Agreement apply to the Trustwave Products provided by Trustwave, hereunder.

Trustwave is willing to license the Software and the Documentation to Customer on the condition that Customer accepts all of the terms in this Agreement. By entering Customer's initials in the acceptance box, or downloading, installing, copying or using the accompanying version of the Software, Customer is consenting to be bound by the terms of this Agreement. The person indicating Customer's assent to the terms of this Agreement represents that he or she has the authority to bind Customer to this Agreement. If Customer has entered into a separate, pen-signed agreement with Trustwave governing Customer's rights to the Trustwave Products indicated in the Purchase Order, then that pen-signed agreement (and not this Agreement) will govern Customer's rights to the Software.

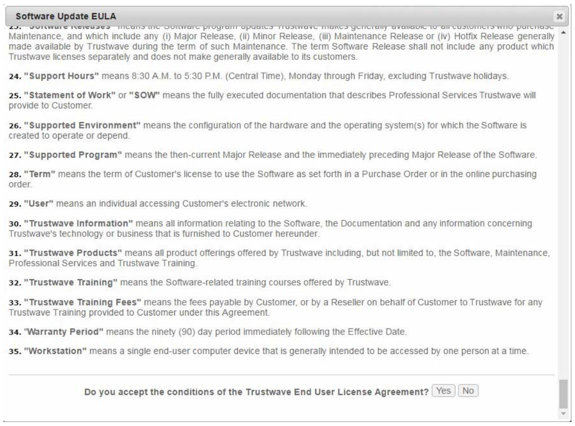
1. Definitions. Unless otherwise defined herein, capitalized terms as used in this Agreement have the meanings set forth in Exhibit B attached hereto.

2. License.

2.1 License Grant. Subject to the terms and conditions of this Agreement, and to the extent all fees are paid, Trustwave grants to Customer a worldwide, non-exclusive, non-transferable, limited, personal license, without the right to grant sublicenses, for the Term set forth on a Purchase Order or in the online purchasing console, to reproduce the Software and Documentation solely as necessary to install and use the Software, and solely (i) for its intended an permitted use as identified by Trustwave, (ii) in accordance with the Documentation and this Agreement (including the limitations on the number of Workstations and/or User licenses set forth on a Purchase Order or in the online purchasing console), (iii) for Customer's internal business purposes, and (iv) in compliance with all applicable laws. Customer may make one (1) copy of the Software solely for backup or archival purposes; *provided, however*, that Customer shall reproduce, on any such copy of the Software, Trustwave's copyright notice and any other proprietary rights notices or logos that appear in the original Software.

2.2 Restrictions on Use. Customer acknowledges that the Software and its structure, organization, and source code constitute valuable trade secrets of Trustwave and its suppliers. Accordingly, Customer shall not, nor shall it permit, assist or encourage any third party to: (i) modify, adapt, alter, translate, or create derivative works from the Software or Documentation; (ii) merge the

3. After reading the contents of the End User License Agreement, scroll to the bottom and click **Yes** if you agree to its terms.



23. "Software Releases" means the Software program updates Trustwave makes generally available to all customers who purchase Maintenance, and which include any (i) Major Release, (ii) Minor Release, (iii) Maintenance Release or (iv) Hotfix Release generally made available by Trustwave during the term of such Maintenance. The term Software Release shall not include any product which Trustwave licenses separately and does not make generally available to its customers.

24. "Support Hours" means 8:30 A.M. to 5:30 P.M. (Central Time), Monday through Friday, excluding Trustwave holidays.

25. "Statement of Work" or **"SOW"** means the fully executed documentation that describes Professional Services Trustwave will provide to Customer.

26. "Supported Environment" means the configuration of the hardware and the operating system(s) for which the Software is created to operate or depend.

27. "Supported Program" means the then-current Major Release and the immediately preceding Major Release of the Software.

28. "Term" means the term of Customer's license to use the Software as set forth in a Purchase Order or in the online purchasing order.

29. "User" means an individual accessing Customer's electronic network.

30. "Trustwave Information" means all information relating to the Software, the Documentation and any information concerning Trustwave's technology or business that is furnished to Customer hereunder.

31. "Trustwave Products" means all product offerings offered by Trustwave including, but not limited to, the Software, Maintenance, Professional Services and Trustwave Training.

32. "Trustwave Training" means the Software-related training courses offered by Trustwave.

33. "Trustwave Training Fees" means the fees payable by Customer, or by a Reseller on behalf of Customer to Trustwave for any Trustwave Training provided to Customer under this Agreement.

34. "Warranty Period" means the ninety (90) day period immediately following the Effective Date.

35. "Workstation" means a single end-user computer device that is generally intended to be accessed by one person at a time.

Do you accept the conditions of the Trustwave End User License Agreement?

4. This action closes the EULA dialog box and begins the software update application process, launching a window showing the progress of the software installation.

A successful software installation restarts the Report Manager. You will need to log in again when prompted:

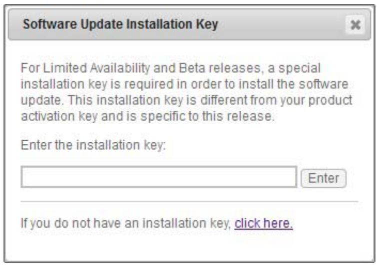
Note: After installing the software update, if a message displays that informs you to reboot the server, you should select the **Restart Software** option on the Restart menu.

2.2.7.3 LA/Beta Software Install Procedures

Installation of Limited Availability or Beta software updates requires additional steps.

1. On the Available Updates tab, two buttons are available for the LA/Beta software update: **View Readme** and **Apply Now**.

   Click **Apply Now** to open the Software Update Installation Key window:



Software Update Installation Key

For Limited Availability and Beta releases, a special installation key is required in order to install the software update. This installation key is different from your product activation key and is specific to this release.

Enter the installation key:

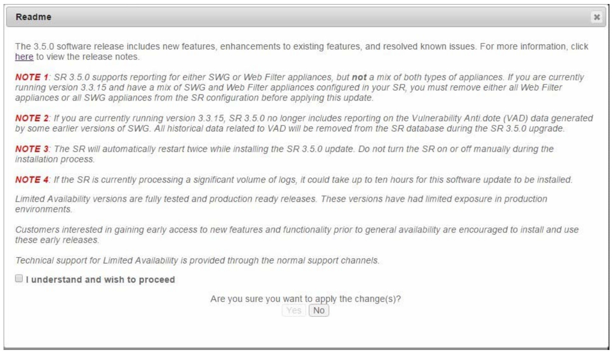
If you do not have an installation key, click here.

2. If you have an installation key for this software version, enter the key in the field and then click **Enter.** If you do not have an installation key, click the link (**click here**) to open the Trustwave Web site where you will need to log in and request an installation key.

Note: The LA or Beta installation key is specific to each software release Major.Minor.Maintenance version (for example, 3.4.0). You will only need to enter this key once (even if you do not complete the update).

3. Click **Enter** to launch the applicable dialog box for accepting the software update type.

Figure 2: Beta acceptance dialog box



Readme

The 3.5.0 software release includes new features, enhancements to existing features, and resolved known issues. For more information, click here to view the release notes.

*NOTE 1: SR 3.5.0 supports reporting for either SWG or Web Filter appliances, but **not** a mix of both types of appliances. If you are currently running version 3.3.15 and have a mix of SWG and Web Filter appliances configured in your SR, you must remove either all Web Filter appliances or all SWG appliances from the SR configuration before applying this update.*

NOTE 2: If you are currently running version 3.3.15, SR 3.5.0 no longer includes reporting on the Vulnerability Anti.dote (VAD) data generated by some earlier versions of SWG. All historical data related to VAD will be removed from the SR database during the SR 3.5.0 upgrade.

NOTE 3: The SR will automatically restart twice while installing the SR 3.5.0 update. Do not turn the SR on or off manually during the installation process.

NOTE 4: If the SR is currently processing a significant volume of logs, it could take up to ten hours for this software update to be installed.

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

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

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

☐ **I understand and wish to proceed**

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

4. Read the description for the software type to be installed (LA or Beta), and then click the check box corresponding to "I understand and wish to proceed".

5. Click **Yes** to close the software acceptance dialog box and to open the End User License Agreement dialog.

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

   A successful software installation restarts the Report Manager. You will need to log in again when prompted.

2.2.7.4 Uninstall the Most Recently Applied Update

On the Update History tab, the most recently applied software update can be unapplied by clicking **Undo**. This action removes the software update from the server.

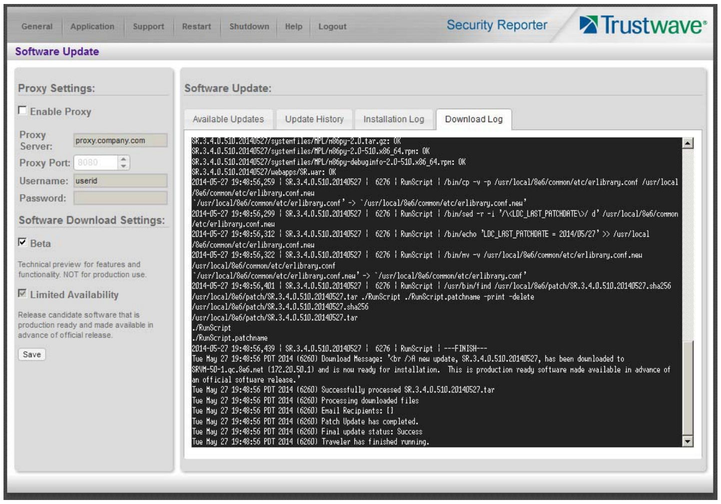
Note: The Undo button may not be available for some updates. For instance, the update from 3.3.15 to 3.4.0 cannot be reversed.

2.2.7.5 Download Available Updates

1. Click **Download Available Updates** on the Available Updates tab to check for the latest software updates. The button is disabled briefly as the check is requested.
2. The check can take several minutes to complete, particularly if new updates are available. You can perform other tasks and return to the Software Update screen in a few minutes or the next day.

2.2.7.6 View Software Download Log

1. To determine whether software updates are being downloaded to the SR, click the Download Log tab.



Proxy Settings:

□ Enable Proxy

Proxy Server: proxy.company.com

Proxy Port: 8080

Username: userid

Password:

Software Download Settings:

☑ Beta

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

☑ Limited Availability

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

Software Update:

```
SR.3.4.0.510.20140527/systemfiles/MPL/m86py-2.0.tar.gz: OK
SR.3.4.0.510.20140527/systemfiles/MPL/m86py-2.0-510.x86_64.rpm: OK
SR.3.4.0.510.20140527/systemfiles/MPL/m86py-debuginfo-2.0-510.x86_64.rpm: OK
SR.3.4.0.510.20140527/webapps/SR.war: OK
2014-05-27 19:48:56,259 | SR.3.4.0.510.20140527 |  6276 | RunScript | /bin/cp -v -p /usr/local/8e6/common/etc/erlibrary.conf /usr/local
/8e6/common/etc/erlibrary.conf.new
`/usr/local/8e6/common/etc/erlibrary.conf' -> `/usr/local/8e6/common/etc/erlibrary.conf.new'
2014-05-27 19:48:56,299 | SR.3.4.0.510.20140527 |  6276 | RunScript | /bin/sed -r -i '/\<LDC_LAST_PATCHDATE\>/ d' /usr/local/8e6/common
/etc/erlibrary.conf.new
2014-05-27 19:48:56,312 | SR.3.4.0.510.20140527 |  6276 | RunScript | /bin/echo 'LDC_LAST_PATCHDATE = 2014/05/27' >> /usr/local
/8e6/common/etc/erlibrary.conf.new
2014-05-27 19:48:56,322 | SR.3.4.0.510.20140527 |  6276 | RunScript | /bin/mv -v /usr/local/8e6/common/etc/erlibrary.conf.new
/usr/local/8e6/common/etc/erlibrary.conf
`/usr/local/8e6/common/etc/erlibrary.conf.new' -> `/usr/local/8e6/common/etc/erlibrary.conf'
2014-05-27 19:48:56,401 | SR.3.4.0.510.20140527 |  6276 | RunScript | /usr/bin/find /usr/local/8e6/patch/SR.3.4.0.510.20140527.sha256
/usr/local/8e6/patch/SR.3.4.0.510.20140527.tar ./RunScript ./RunScript.patchname -print -delete
/usr/local/8e6/patch/SR.3.4.0.510.20140527.sha256
/usr/local/8e6/patch/SR.3.4.0.510.20140527.tar
./RunScript
./RunScript.patchname
2014-05-27 19:48:56,439 | SR.3.4.0.510.20140527 |  6276 | RunScript | ---FINISH---
Tue May 27 19:48:56 PDT 2014 (6260) Download Message: '<br />A new update, SR.3.4.0.510.20140527, has been downloaded to
SRVM-50-1.qc.8e6.net (172.20.50.1) and is now ready for installation.  This is production ready software made available in advance of
an official software release.'
Tue May 27 19:48:56 PDT 2014 (6260) Successfully processed SR.3.4.0.510.20140527.tar
Tue May 27 19:48:56 PDT 2014 (6260) Processing downloaded files
Tue May 27 19:48:56 PDT 2014 (6260) Email Recipients: []
Tue May 27 19:48:56 PDT 2014 (6260) Patch Update has completed.
Tue May 27 19:48:56 PDT 2014 (6260) Final update status: Success
Tue May 27 19:48:56 PDT 2014 (6260) Traveler has finished running.
```

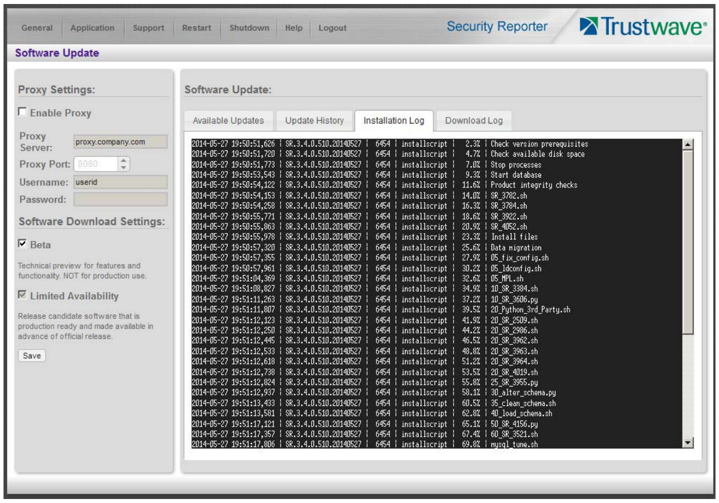
Note: To refresh this log view, select Software Update from the main menu and then click the tab.

2.2.7.7 View Update History

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

2.2.7.8 View Installation Log

1. To determine whether the latest software update has been successfully applied to this SR, click the Installation Log tab:



Proxy Settings:

□ Enable Proxy

Proxy Server: proxy.company.com

Proxy Port: 8080

Username: userid

Password:

Software Download Settings:

☑ Beta

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

☑ Limited Availability

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

Software Update:

```
2014-05-27 19:50:51,626 | SR.3.4.0.510.20140527 |  6454 | installscript |   2.3% | Check version prerequisites
2014-05-27 19:50:51,720 | SR.3.4.0.510.20140527 |  6454 | installscript |   4.7% | Check available disk space
2014-05-27 19:50:51,773 | SR.3.4.0.510.20140527 |  6454 | installscript |   7.0% | Stop processes
2014-05-27 19:50:53,543 | SR.3.4.0.510.20140527 |  6454 | installscript |   9.3% | Start database
2014-05-27 19:50:54,122 | SR.3.4.0.510.20140527 |  6454 | installscript |  11.6% | Product integrity checks
2014-05-27 19:50:54,153 | SR.3.4.0.510.20140527 |  6454 | installscript |  14.0% | SR_3782.sh
2014-05-27 19:50:54,258 | SR.3.4.0.510.20140527 |  6454 | installscript |  16.3% | SR_3784.sh
2014-05-27 19:50:55,771 | SR.3.4.0.510.20140527 |  6454 | installscript |  18.6% | SR_3922.sh
2014-05-27 19:50:55,863 | SR.3.4.0.510.20140527 |  6454 | installscript |  20.9% | SR_4052.sh
2014-05-27 19:50:55,978 | SR.3.4.0.510.20140527 |  6454 | installscript |  23.3% | Install files
2014-05-27 19:50:57,320 | SR.3.4.0.510.20140527 |  6454 | installscript |  25.6% | Data migration
2014-05-27 19:50:57,355 | SR.3.4.0.510.20140527 |  6454 | installscript |  27.9% | 05_fix_config.sh
2014-05-27 19:50:57,961 | SR.3.4.0.510.20140527 |  6454 | installscript |  30.2% | 05_ldconfig.sh
2014-05-27 19:51:04,369 | SR.3.4.0.510.20140527 |  6454 | installscript |  32.6% | 05_MPL.sh
2014-05-27 19:51:08,827 | SR.3.4.0.510.20140527 |  6454 | installscript |  34.9% | 10_SR_3384.sh
2014-05-27 19:51:11,263 | SR.3.4.0.510.20140527 |  6454 | installscript |  37.2% | 10_SR_3606.py
2014-05-27 19:51:11,807 | SR.3.4.0.510.20140527 |  6454 | installscript |  39.5% | 20_Python_3rd_Party.sh
2014-05-27 19:51:12,123 | SR.3.4.0.510.20140527 |  6454 | installscript |  41.9% | 20_SR_2509.sh
2014-05-27 19:51:12,250 | SR.3.4.0.510.20140527 |  6454 | installscript |  44.2% | 20_SR_2986.sh
2014-05-27 19:51:12,445 | SR.3.4.0.510.20140527 |  6454 | installscript |  46.5% | 20_SR_3962.sh
2014-05-27 19:51:12,533 | SR.3.4.0.510.20140527 |  6454 | installscript |  48.8% | 20_SR_3963.sh
2014-05-27 19:51:12,618 | SR.3.4.0.510.20140527 |  6454 | installscript |  51.2% | 20_SR_3964.sh
2014-05-27 19:51:12,738 | SR.3.4.0.510.20140527 |  6454 | installscript |  53.5% | 20_SR_4019.sh
2014-05-27 19:51:12,824 | SR.3.4.0.510.20140527 |  6454 | installscript |  55.8% | 25_SR_3955.py
2014-05-27 19:51:12,937 | SR.3.4.0.510.20140527 |  6454 | installscript |  58.1% | 30_alter_schema.py
2014-05-27 19:51:13,433 | SR.3.4.0.510.20140527 |  6454 | installscript |  60.5% | 35_clean_schema.sh
2014-05-27 19:51:13,581 | SR.3.4.0.510.20140527 |  6454 | installscript |  62.8% | 40_load_schema.sh
2014-05-27 19:51:17,121 | SR.3.4.0.510.20140527 |  6454 | installscript |  65.1% | 50_SR_4156.py
2014-05-27 19:51:17,357 | SR.3.4.0.510.20140527 |  6454 | installscript |  67.4% | 60_SR_3521.sh
2014-05-27 19:51:17,806 | SR.3.4.0.510.20140527 |  6454 | installscript |  69.8% | mysql_tune.sh
```

2.2.7.9 Specify Proxy Settings

You can specify a proxy server if required to download updates.

1. In the Proxy Setting section of the Software Update screen (Figure 1), check the box **Enable Proxy** if the server is in a proxy server environment.
2. In the **Proxy Server** field, enter the hostname of the proxy server.
3. In the **Proxy Port** field, enter the port number of the proxy server.
4. In the **Username** field, enter the username for the proxy account.
5. In the **Password** field, enter the password for the proxy account.

Tip: When you are finished making edits to this screen, click **Save** (below the Software Download Settings section) to save your settings.

2.2.7.10 Software Download Settings

The Software Download Settings section allows you to specify whether or not this SR will receive Limited Availability (LA) and/or Beta software updates. These types of software updates provide previews of software features currently being tested prior to the General Availability software release.

By default, the "Limited Availability" check box is enabled, indicating this SR will receive software updates recommended for use in a production environment only. With this feature enabled, the latest LA software update will automatically download and be available via the Available Updates tab on the Software Update screen.

To change the LA or Beta settings:

1. Click the "Limited Availability" check box to enable or disable visibility of LA updates.

2. Click the “Beta” check box to enable or disable visibility of Beta software updates. Beta updates should only be applied for an SR used in a non-production environment.
3. Click **Save** to save your settings.

2.2.8 RAID Array Status screen

To open the RAID Array Status screen, select **RAID Array Status** from the Support menu.

The RAID Array Status screen displays the status of each drive on the RAID server. If a RAID array requires a rebuild (for instance if a drive was replaced on Equus hardware), you can start rebuilding from this screen.

Note: If you are running the SR as a virtual machine, this screen displays the following message only: “RAID is not available on Virtual Machines.”

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

2.2.8.1 View the Hard Drive Status on Equus Models

The current RAID Array Status displays for all Equus model hard drives:

- HD 1 and HD 2 for 300 series Equus models
- HD 1 through HD 4 for 500 and 700 series Equus models

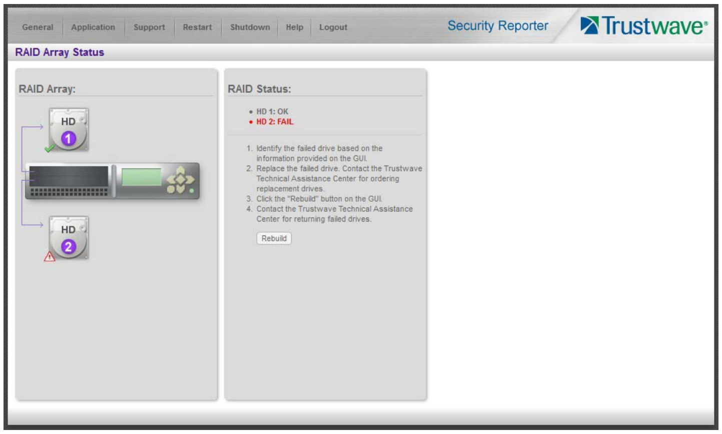
If all hard drives are functioning without failure, the text “OK” displays for each corresponding drive number listed at the right of the screen, and no other text displays.

If any of the hard drives has failed, the message “FAIL” displays for the corresponding drive number listed at the right of the screen.

To replace the failed drive:

1. Identify the failed drive based on the information provided on the GUI.
2. Replace the failed drive.
3. Click on the “Rebuild” button on the GUI.
4. To return a failed drive to Trustwave or to order additional replacement drives, please call the Trustwave Technical Assistance Center.

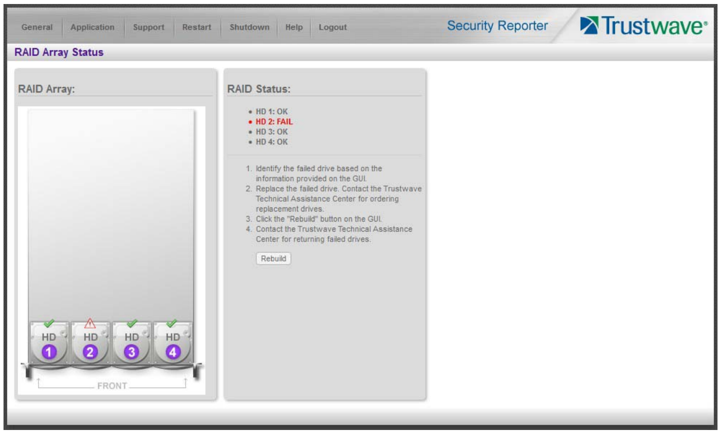
Figure 3: RAID Array Status screen, 300 model



- HD 1: OK
- HD 2: FAIL

1. Identify the failed drive based on the information provided on the GUI.
2. Replace the failed drive. Contact the Trustwave Technical Assistance Center for ordering replacement drives.
3. Click the "Rebuild" button on the GUI.
4. Contact the Trustwave Technical Assistance Center for returning failed drives.

Figure 4: RAID Array Status screen, 500, 700, 730 model



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

1. Identify the failed drive based on the information provided on the GUI.
2. Replace the failed drive. Contact the Trustwave Technical Assistance Center for ordering replacement drives.
3. Click the "Rebuild" button on the GUI.
4. Contact the Trustwave Technical Assistance Center for returning failed drives.

2.2.8.2 View the Hard Drive Status on IBM Models

The current RAID Array Status displays for IBM model hard drives:

- Drives 0 and 1 for the 505 IBM model
- Drives 0 through 7 for 700 series IBM models (the diagram includes eight hard drives, even though the appliance only uses drives 0 through 3 for running SR, with drive 4 used as a backup drive in the event of a hard drive failure).

Optimal status: The text “RAID Volumes Optimal” displays if all pre-configured Physical Disks are functioning in their slots without failure. For each corresponding drive number listed at the right of the screen, the “Online” status displays followed by the hard drive type, manufacturer name, and serial number.

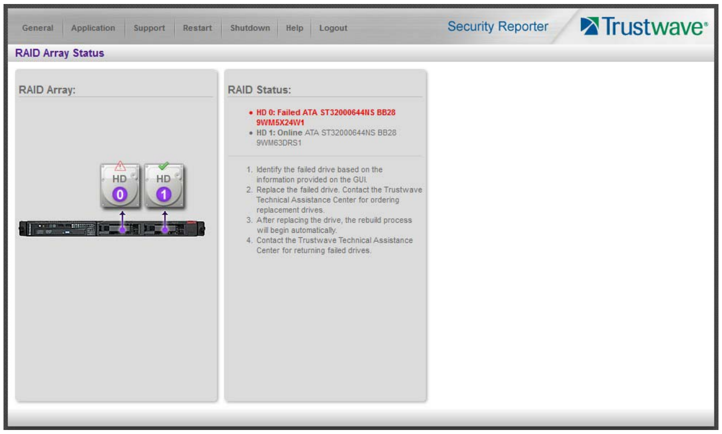
Degraded status: The text “RAID Volumes Degraded” displays if any pre-configured SR hard drive has failed or is missing from its slot—the former status refers to a hard drive that ceases to operate or fails to rebuild upon insertion in the carrier, and the latter status refers to a hard drive that is missing because it was either removed from its carrier or the hard drive bay is unoccupied by default.

For each corresponding drive number listed at the right of the screen, the “Fail” or “Missing” status—as appropriate to the hard drive’s status—displays followed by the hard drive type, manufacturer name, and serial number.

To replace the failed drive:

1. Identify the failed drive based on the information provided on the GUI.
2. Replace the failed drive.
3. After replacing the drive, the rebuild process will begin automatically.
4. To return a failed drive to Trustwave or to order additional replacement drives, please call the Trustwave Technical Assistance Center.

Figure 5: RAID Array Status screen, 505 IBM model



RAID Array Status

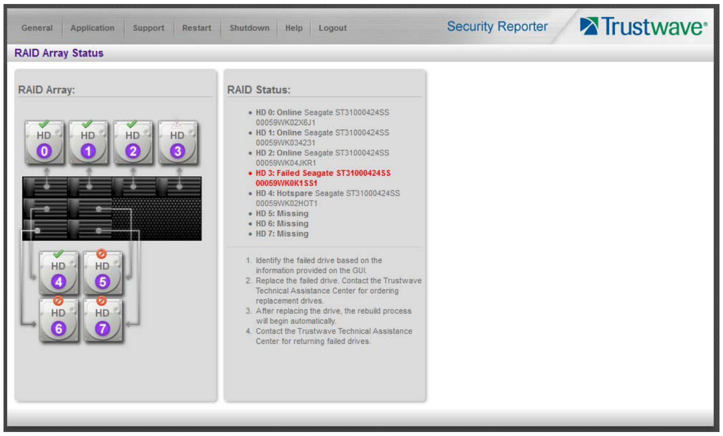
RAID Array:

RAID Status:

- **HD 0: Failed ATA ST32000644NS BB28 9WM5X24W1**
- **HD 1: Online** ATA ST32000644NS BB28 9WM63DRS1

1. Identify the failed drive based on the information provided on the GUI.
2. Replace the failed drive. Contact the Trustwave Technical Assistance Center for ordering replacement drives.
3. After replacing the drive, the rebuild process will begin automatically.
4. Contact the Trustwave Technical Assistance Center for returning failed drives.

Figure 6: RAID Array Status screen, 705 or 735 IBM model



RAID Array Status

RAID Array:

RAID Status:

- **HD 0: Online** Seagate ST31000424SS 00059WK02X6J1
- **HD 1: Online** Seagate ST31000424SS 00059WK034231
- **HD 2: Online** Seagate ST31000424SS 00059WK04JKR1
- **HD 3: Failed Seagate ST31000424SS 00059WK0K1SS1**
- **HD 4: Hotspare** Seagate ST31000424SS 00059WK02HOT1
- **HD 5: Missing**
- **HD 6: Missing**
- **HD 7: Missing**

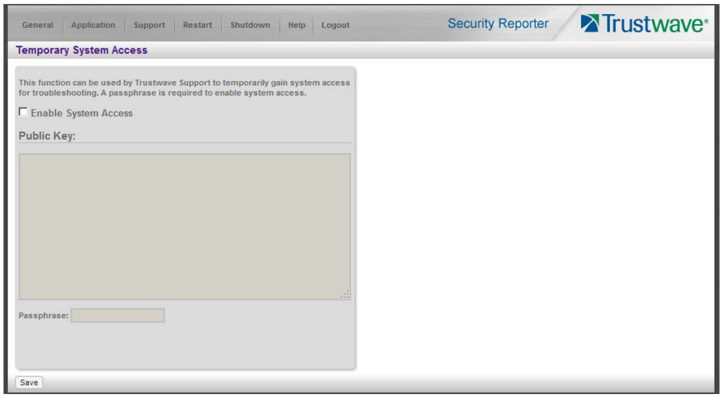
1. Identify the failed drive based on the information provided on the GUI.
2. Replace the failed drive. Contact the Trustwave Technical Assistance Center for ordering replacement drives.
3. After replacing the drive, the rebuild process will begin automatically.
4. Contact the Trustwave Technical Assistance Center for returning failed drives.

2.2.9 Temporary System Access screen

To open the Temporary System Access screen, select **Temporary System Access** from the Support menu. This screen is primarily used by Trustwave Technical Assistance Center representatives to perform maintenance on your server, if your system is behind a firewall that denies access to your server.

Note: By default, temporary system access expires and is de-activated after 30 minutes.

Figure 7: Temporary System Access screen



This function can be used by Trustwave Support to temporarily gain system access for troubleshooting. A passphrase is required to enable system access.

☐ Enable System Access

Public Key:

Passphrase:

2.2.9.1 Activate Temporary Access

1. Check the box Enable System Access.
2. Enter the Public Key and Passphrase (confidential to Trustwave).
3. Click **Save.**

2.2.9.2 Terminate Temporary Access

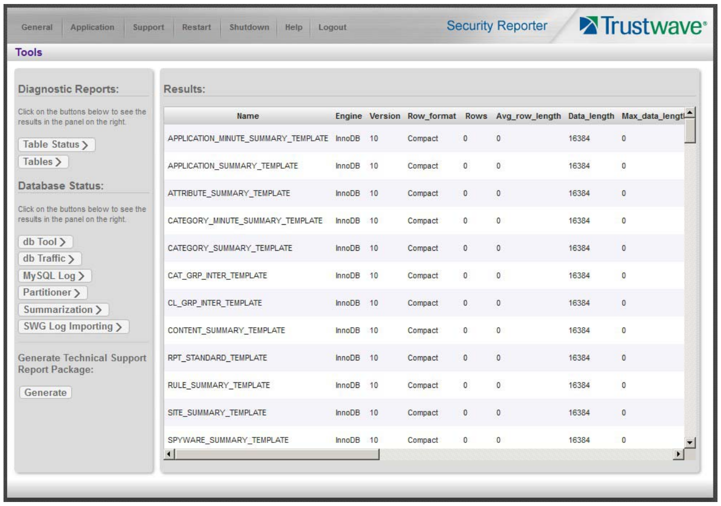
After maintenance has been performed on the server, it is good practice to de-activate access.

1. Clear (uncheck) the box Enable System Access.
2. Click **Save**.

2.2.10 Tools screen

To open the Tools screen, select **Tools** from the Support menu.

The Tools screen allows you to view diagnostic reports and system logs. These logs can help you to troubleshoot problems with the Report Manager application. This screen also includes an option to generate a report package that may be requested by Technical Support as required to investigate any problems with the software.



Name	Engine	Version	Row_format	Rows	Avg_row_length	Data_length	Max_data_lengt
APPLICATION_MINUTE_SUMMARY_TEMPLATE	InnoDB	10	Compact	0	0	16384	0
APPLICATION_SUMMARY_TEMPLATE	InnoDB	10	Compact	0	0	16384	0
ATTRIBUTE_SUMMARY_TEMPLATE	InnoDB	10	Compact	0	0	16384	0
CATEGORY_MINUTE_SUMMARY_TEMPLATE	InnoDB	10	Compact	0	0	16384	0
CATEGORY_SUMMARY_TEMPLATE	InnoDB	10	Compact	0	0	16384	0
CAT_GRP_INTER_TEMPLATE	InnoDB	10	Compact	0	0	16384	0
CL_GRP_INTER_TEMPLATE	InnoDB	10	Compact	0	0	16384	0
CONTENT_SUMMARY_TEMPLATE	InnoDB	10	Compact	0	0	16384	0
RPT_STANDARD_TEMPLATE	InnoDB	10	Compact	0	0	16384	0
RULE_SUMMARY_TEMPLATE	InnoDB	10	Compact	0	0	16384	0
SITE_SUMMARY_TEMPLATE	InnoDB	10	Compact	0	0	16384	0
SPYWARE_SUMMARY_TEMPLATE	InnoDB	10	Compact	0	0	16384	0

The following options are available on this screen:

- Diagnostic Reports
- Database Status
- Technical Support Report Package

2.2.10.1 Diagnostic Reports

Click one of the following buttons to view the selected diagnostic report in the Results panel:

- **Table Status:** This report contains a list of Client table names, and columns of statistics on each table, such as type, size, number of rows, and time created and updated.
- **Tables:** This report contains a list of the names of tables currently in the database.

2.2.10.2 View Database Status Logs

Click one of the following buttons to view the selected database status log in the Results panel:

- **db Tool**: This log shows information about system checks performed on disk usage, free memory, unprocessed files, and daemons.
- **db Traffic**: This log provides information about the daily traffic table.
- **MySQL Log:** This log provides information about the MySQL server.
- **Partitioner**: This log displays results of server partitioning for database expiration.
- **Summarization**: This log shows a summarization of activities from the summarizer database tool.
- **SWG Log Importing**: For a SR providing reporting for SWG, this log displays results of SWG archive log import.
- **WF Log Importing:** For a SR providing reporting for Web Filter, this log displays results of Web Filter log file import.

2.2.10.3 Generate Technical Support Report Package

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

1. In the **Technical Support Report Package** section, click **Generate** to begin generating the report package.
2. After the package has been generated, a Download button displays. Click **Download** to download the .tgz package to your workstation.
3. Email the package to the Trustwave Technical Assistance Center as instructed by your Trustwave technical support representative.

2.2.11 Restart Menu

The Restart menu allows you to request restart of the system or selected processes. The options are:

- **Report Manager:** Restarts the Report Manager software. Any report generation that is currently in progress will be interrupted.
- **Software:** Restarts the Report Manager and database software. This option should be selected if daemons fail to run and/or the database needs to be started again. When this option is selected, the MySQL database is restarted. All data processing that is currently in progress, including summarization and report generation, will be interrupted.

  Note: When the Restart Software option is selected, the server can take several hours to restart, because the system waits for the database to complete current tasks so that it can be stopped safely. This action can take several hours to complete. During this time, status messages are sent by email to the addresses configured on the Self-Monitoring screen (see Section 2.2.2).

- **System:** Restarts the hardware and operating system. All data processing will be interrupted. This option should be selected if a change was made that requires restart (for example, when applying certain hardware configurations). You will also need to use this option if you changed the IP address of the SR (in the SR panel of the Device Registry).

  Note: When the Restart System option is selected, the server can take several hours to restart, because the system waits for the database to complete current tasks so that it can be stopped safely. This action can take several hours to complete. During this time, status messages are sent by email to the addresses configured on the Self-Monitoring screen (see Section 2.2.2).

  During the Hardware Restart process, log files normally transferred to the server are routed to a problem directory in the logging device. When the server is running again, these files are transferred to the server

To perform a restart, select one of the options from the Restart menu. On the warning pop-up, click **Yes** to confirm.

2.2.12 Shutdown Menu

The options on the Shutdown menu allow you to shut down the server. This action should only be selected if the server's hardware must be completely shut down (for example, if the server will be physically relocated). When you perform a shutdown, the server shuts off. Log files normally transferred to the server will be routed to a problem directory in the logging device. When the server is rebooted, these files will be transferred to the server.

To perform a shutdown, select Quick Shutdown or Graceful Shutdown from the Shutdown menu. On the warning pop-up, *carefully read the description* of the selected shutdown type. If you want to proceed, click **Yes** to confirm.

Caution: Each type of shutdown has advantages and disadvantages.

- **Quick shutdown can result in data corruption,** because database activity is terminated without waiting. However, this action normally completes in 15 minutes or less.
- **Graceful shutdown** is a safer option because the system waits for the database to complete current tasks so that it can be stopped safely. This action can take several hours to complete. During this time, status messages are sent by email to the addresses configured on the Self-Monitoring screen (see Section 2.2.2).

2.3 Device Registry

The Device Registry panel is used to view information about devices connected to the SR, to edit application settings, and to add or delete an SWG, a LDAP server, or a Web Filter device to/from the registry.

This function is available to global administrators.

Note: SR can be used to produce reports from either SWG data or Web Filter data, but not both at the same time.

At least one SWG policy server or Web Filter must be added to the device registry to produce reports. If no SWG or Web Filter was specified during the wizard installation process, you can add devices on this panel.

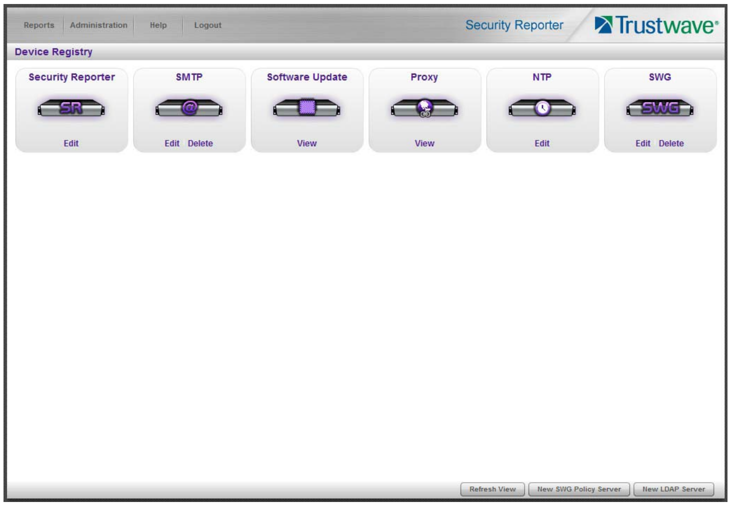
A LDAP server can be added if required for use with SWG.

In the unlikely case that you want to change between SWG and Web Filter:

- To change the data source from SWG to Web Filter, delete all SWG and LDAP server devices before adding a Web Filter.
- To change the data source from Web Filter to SWG, delete all Web Filter devices before adding a SWG.

Caution: When you remove a SWG or Web Filter device from Device Registry, **all associated reporting data and reports are removed from the SR.**

To display the Device Registry screen, from the main menu of the Report Manager, choose **Administration > Device Registry**.



Each icon on this screen represents a device or external service that can communicate with the SR. All device icons include at least one of the following links: View, Edit, Delete.

At the bottom of the panel the following buttons display:

- **Refresh View**: Click this button to update the list of icons.
- **New SWG Policy Server**: Click this button to add an SWG policy server to the device registry.

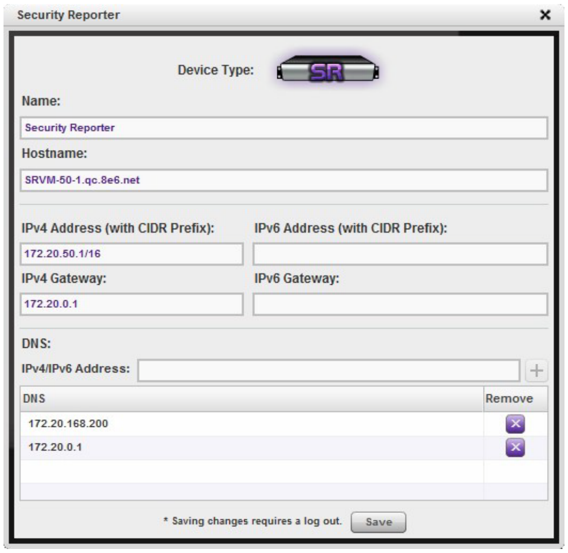
Note: SWG policy servers are the source of data for SR reports. At least one SWG policy server must be added to the device registry. If an SWG policy server was not specified during the wizard installation process, please add this device now.

- **New LDAP Server** (enabled only if an SWG has been added to the device registry): Click this button to add an LDAP server to the device registry.
- **New SMTP Server** (Available if no SMTP server is present in the device registry): Click this button to add a SMTP server to the device registry.
- **New Web Filter:** Click this button to add a Web Filter to the device registry.

2.3.1 SR device

The Security Reporter device entry allows you to view and edit basic network settings for the SR server. These settings include names, IPv4 and IPv6 addresses, and DNS settings.

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



Device Type:

Name: Security Reporter

Hostname: SRVM-50-1.qc.8e6.net

IPv4 Address (with CIDR Prefix): 172.20.50.1/16

IPv6 Address (with CIDR Prefix):

IPv4 Gateway: 172.20.0.1

IPv6 Gateway:

DNS:

IPv4/IPv6 Address:

DNS	Remove
172.20.168.200	☒
172.20.0.1	☒

* Saving changes requires a log out.

2.3.1.1 Set up/Edit Names

In the Name field, enter a friendly name for this SR appliance.

In the **Host Name** field, enter the address or URL that will be used for accessing the SR application. This entry should normally include the fully qualified domain name and the host name for the server (for example, reporter.example.com).

Tip: Ensure that the name is resolvable through DNS. You can use a simple hostname (without domain parts) as long as this is resolvable within the network.

2.3.1.2 Set up/Edit IP Addresses

You can use either or both of IPv4 and IPv6 networking with the SR.

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

1. Enter or edit an IPv4 or IPv6 address in each appropriate field:
    - In the **IPv4 Address** field, enter the IPv4 address of the SR server on your Local Area Network (LAN 1), and the network mask (in CIDR notation) for the local segment. For example, `172.20.50.1/16` indicates the IP address (172.20.50.1) and a class B network (16 bits or 255.255.0.0 in netmask notation).
    - In the **IPv4 Gateway** field, enter the IPv4 address for the default router that will be the main gateway for the network segment.
    - In the **IPv6 Address** field, enter the IPv6 address of the SR server on your Local Area Network (LAN 1), and the network mask (in CIDR notation) for the local segment. For example, `2001:db8:85a3::85a4/64` indicates the IP address (2001:db8:85a3:0:0:0:0:85a4) and an IPv6 lan of 64 bits.

- In the **IPv6 Gateway** field, enter the IPv6 address for the default router that will be the main gateway for the network segment.
- In the **DNS** section, enter the IPv4 or IPv6 address of the primary Domain Name System (name server) in the address field, and then click ⊞. You can repeat this action to enter two additional fallback DNS server addresses.

Note: Enter the addresses in order with the primary server first. The system tries to resolve names using the first server listed, and only uses other entries if the first server does not respond within a set time.

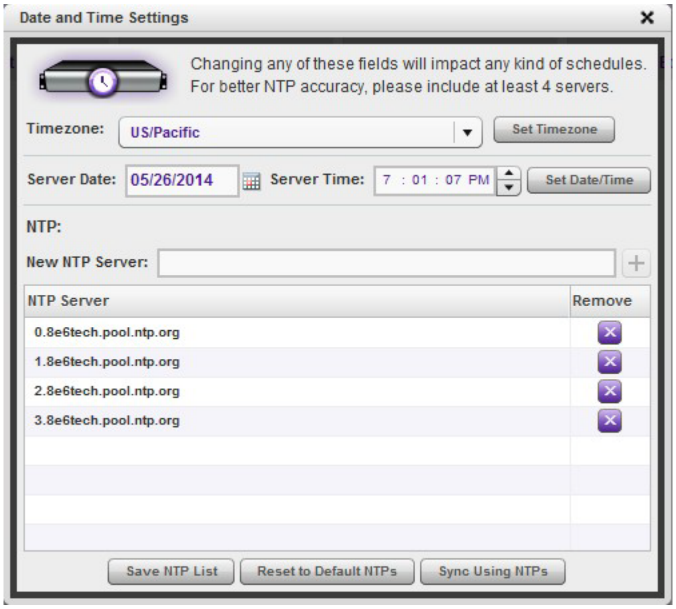
- To remove a DNS server address, click the corresponding ☒ button.

2. Be sure each IP address is correct, and then click **Save**.

Note: When you save these changes the system will restart Report Manager. You will be redirected to the login page and you must log in again.

2.3.2 Date and Time Settings

The Date and Time Settings pop-up displays when you edit the NTP item in the Device Registry.



Date and Time Settings

Changing any of these fields will impact any kind of schedules. For better NTP accuracy, please include at least 4 servers.

Timezone: US/Pacific

Server Date: 05/26/2014 Server Time: 7 : 01 : 07 PM

NTP:

New NTP Server:

NTP Server	Remove
0.8e6tech.pool.ntp.org	☒
1.8e6tech.pool.ntp.org	☒
2.8e6tech.pool.ntp.org	☒
3.8e6tech.pool.ntp.org	☒

This pop-up allows you to specify the time zone, server date and time, and network time servers to maintain accurate time.

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

2.3.2.1 Specify the Time Zone

1. From the **Timezone** menu, select your region, country and zone from the available choices.

2. To apply your change, click **Set Timezone**.

Caution: Setting the timezone initiates a Software Restart as described in Section 2.2.11. This action can take several hours to complete. You should apply this setting at an appropriate time. For more details of the restart action and available notifications, see Section 2.2.11.

2.3.2.2 Set the Server Date and Time

The date and time currently set on the server display in the Server Date and Server Time fields.

1. To set the date, click the Server Date field to open a calendar control.
   - Navigate the control using the arrows, and click the correct date to enter it in the field.
2. To set the time, click any number in the Server Time field to highlight it.
   - Enter the new value, or use the arrows to the right of the field to change the value.
   - Repeat the process for each value you want to change.
3. To apply changes, click **Set Date/Time.**

Caution: Your changes will not be applied until you click this button.

2.3.2.3 Specify Network Time Protocol Servers

NTP is a time synchronization system for computer clocks throughout the Internet. Your SR server will update its time setting by getting the time from the NTP servers you select.

Hostnames or IP addresses of servers running Network Time Protocol (NTP) software display in a list. Four server names are entered by default. The time update will use the first available server in the list.

If you wish to use different NTP servers, follow these steps:

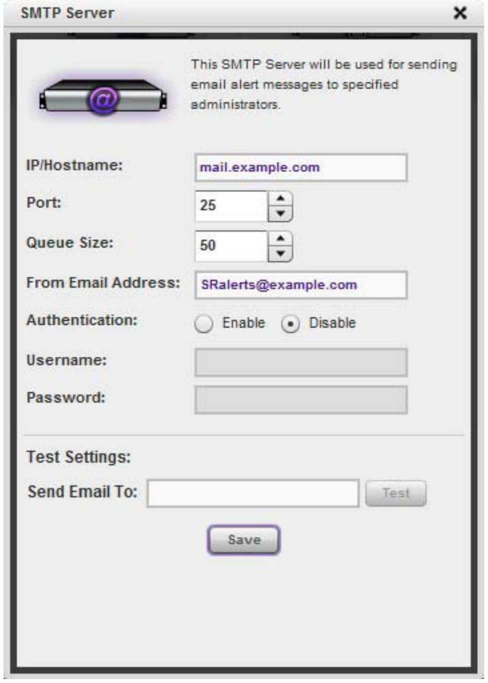
1. To add a server, in the New NTP Server field, enter the IP address or DNS name of a NTP server. Click the ⊞ to add the server to the list.
2. To remove a server, click the ☒ for its entry in the list.
3. To save changes to the list, click **Save NTP List**.

To restore the default list of servers, click **Reset to Default NTPs.**

To update the time immediately using the servers listed, click **Sync Using NTPs**.

2.3.3 SMTP Server Setting screen

The SMTP Server Setting screen displays when you click **New SMTP Server** or edit the SMTP item in Device Registry. This screen allows you to specify settings for the email connection that can be used to send alert messages to specified administrators.



This SMTP Server will be used for sending email alert messages to specified administrators.

IP/Hostname: mail.example.com

Port: 25

Queue Size: 50

From Email Address: SRalerts@example.com

Authentication: ○ Enable ● Disable

Username:

Password:

Test Settings:

Send Email To:

2.3.3.1 Enter, Edit SMTP Server Settings

1. In the **IP/Hostname field**, enter the IPv4 or IPv6 address, or resolvable host name of the SMTP Server that should be used.

   Tip: Some examples are:

   - IPv4: `10.10.0.1`
   - IPv6: `2001:db8::ff00:42:8329`
   - Hostname (DNS): `mail.example.com`

2. By default, the **SMTP Port** number used for sending email is 25. Change this port if required to match the settings on the server you selected.
3. By default, the email **Queue Size** is 50. You can alter this setting as required to specify the maximum number of requests that can be placed into the queue awaiting an available outbound connection.
4. In the **From Email Address** field, enter the email address you want to appear as the source of email messages to designated administrators.
5. By default, **Authentication** is disabled. If a username and password are required for logging into the SMTP server, click **Enable.** This action activates the **Username** and **Password** fields. Enter a valid username and password.
6. Click **Save** to apply your settings.

2.3.3.2 Verify SMTP Settings

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

1. Enter the email address in the **Send Email To** field.
2. Click **Test** to process your request. If all SMTP settings are correct, the test email should be received at the specified address.

2.3.3.3 Remove SMTP Settings

If you do not want to send any email from this SR, you can remove the SMTP server settings. To remove the settings, click **Delete** on the SMTP Server item in Device Registry. When the SMTP server is removed, the **New SMTP Serve**r button displays at the bottom of the Device Registry screen so that you can add settings if required.

2.3.4 SWG Policy Server Device Management

You can use SR to report on data from one or more SWG policy servers.

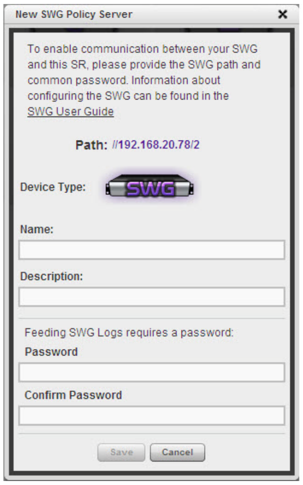
Any LDAP servers used with the SWG(s) should also be added to the device registry. See Section 2.3.5.

Adding the first SWG Policy Server (if one was not added during the installation process) requires additional steps that are not required when adding additional SWG Policy Servers.

Caution: Trustwave recommends backing up and saving current SR data in a location off the server before adding or removing an SWG device in the device registry.

2.3.4.1 Add the first Policy Server to the device registry

1. If no SWG Policy Server was added during the SR Wizard installation process and none has been subsequently added to this device registry, click **New SWG Policy Server** at the bottom of the Device Registry panel to open the New SWG Policy Server window:



New SWG Policy Server

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

Path: //192.168.20.78/2

Device Type: SWG

Name:

Description:

Feeding SWG Logs requires a password:

Password

Confirm Password

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

Tip: Make a note of the Path. You will need this information when you configure the SWG to send reporting data to this SR.

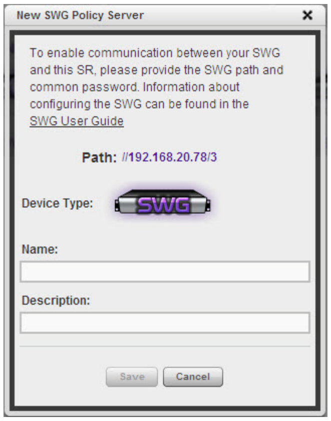
2. Enter a **Name** for the device and/or a **Description** for the device.

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

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

2.3.4.2 Add another Policy Server to the device registry

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



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

Path: //192.168.20.78/3

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

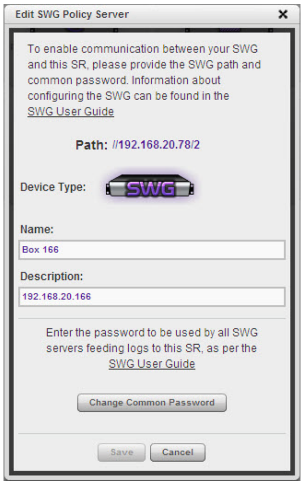
Tip: Make a note of the Path. You will need this information when you configure the SWG to send reporting data to this SR.

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

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

2.3.4.3 Edit Policy Server criteria, change password

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



Edit SWG Policy Server

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

Path: //192.168.20.78/2

Device Type: SWG

Name: Box 166

Description: 192.168.20.166

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

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

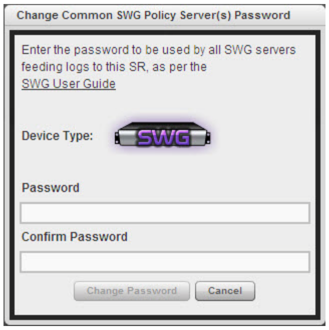
2. The following actions can be performed in this window:

   - Make entries or edits in the following fields:

     - **Name:** Name for the device.

     - **Description**: Description of the device.

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



Change Common SWG Policy Server(s) Password

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

Device Type: SWG

Password

Confirm Password

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

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

     iii. Click **Change Password** to save your entries, close this window, and return to the Edit SWG Policy Server window.

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

2.3.4.4 Delete a Policy Server from the device registry

Caution: If you remove an SWG device, **all data from that device** for Time Usage Reports, Summary Reports, Summary Drill Down Reports and Detail Drill Down Reports **will be purged.**

Trustwave recommends backing up and saving current SR data in a location off the server before adding or removing an SWG device in the device registry.

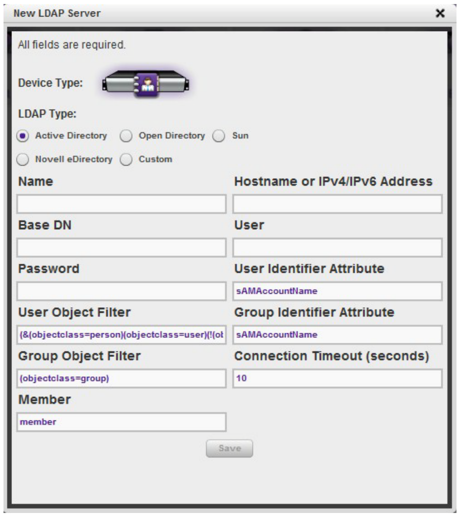
1. Go to the SWG server icon in the Device Registry panel and click **Delete** to open the CONFIRM dialog box with a message asking if you want to delete this device.
2. Click **Yes** to delete the SWG device from the registry, and to remove the SWG server icon from the Device Registry panel. Click **No** if you do not want to delete the device.

2.3.5 LDAP Server Device Management

Any LDAP servers used with the SWG(s) should be added to the device registry.

2.3.5.1 Add an LDAP Server to the device registry

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



New LDAP Server ×

All fields are required.

Device Type:

LDAP Type:

● Active Directory ○ Open Directory ○ Sun

○ Novell eDirectory ○ Custom

Name	Hostname or IPv4/IPv6 Address
Base DN	User
Password	User Identifier Attribute
	sAMAccountName
User Object Filter	Group Identifier Attribute
(&(objectclass=person)(objectclass=user)(!(ot	sAMAccountName
Group Object Filter	Connection Timeout (seconds)
(objectclass=group)	10
Member	
member	

2. Make entries in the following fields:
   - **LDAP Type**: Active Directory, Open Directory, Sun, Novell eDirectory, Custom
   - **Name**: Label assigned to the LDAP server
   - **Base DN**: Root of the LDAP database to be queried using the LDAP syntax, e.g. *DC=domain,DC=com*, or *o=server-org*. The entry in this field is case sensitive.
   - **Password**: LDAP server password
   - **User Object Filter**: Identify user objects, if necessary
   - **Group Object Filter**: Identify group objects, if necessary
   - **Member**: Specify membership attributes, if necessary

- **Hostname or IPv4/IPv6 Address**: The resolvable name, or IPv4 or IPv6 address, of the LDAP server.
- **User**: Enter the authorized user's full LDAP Distinguished Name. For example, enter the entire string in a format such as:

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

  or

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

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

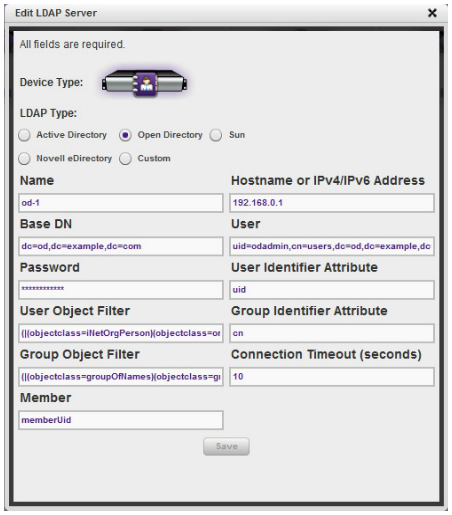
2.3.5.2 Import LDAP Group profiles

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

Tip: If the importation process failed, make edits in the LDAP server window and run the import process again.

2.3.5.3 View, edit LDAP Server device criteria

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



Edit LDAP Server ✕

All fields are required.

Device Type:

LDAP Type:

○ Active Directory ● Open Directory ○ Sun

○ Novell eDirectory ○ Custom

Name: od-1

Hostname or IPv4/IPv6 Address: 192.168.0.1

Base DN: dc=od,dc=example,dc=com

User: uid=odadmin,cn=users,dc=od,dc=example,dc

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

User Identifier Attribute: uid

User Object Filter: (|(objectclass=iNetOrgPerson)(objectclass=or

Group Identifier Attribute: cn

Group Object Filter: (|(objectclass=groupOfNames)(objectclass=gı

Connection Timeout (seconds): 10

Member: memberUid

Save

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

2. Edit any of the fields in this window.
3. Click **Save** to save your edits and to close the window.

2.3.5.4 Delete an LDAP Server from the device registry

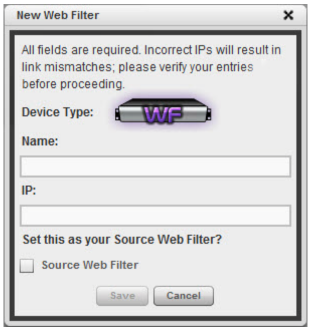
1. Go to the LDAP server icon in the Device Registry panel and click **Delete** to open the CONFIRM dialog box with a message asking if you want to delete this device.
2. Click **Yes** to delete the LDAP server device from the registry, and to remove the LDAP server icon from the Device Registry panel.

2.3.6 Web Filter Device Maintenance

2.3.6.1 Add a Web Filter to the device registry

Note: You cannot add a Web Filter if an SWG or LDAP server is currently configured.

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



New Web Filter

All fields are required. Incorrect IPs will result in link mismatches; please verify your entries before proceeding.

Device Type:

Name:

IP:

Set this as your Source Web Filter?

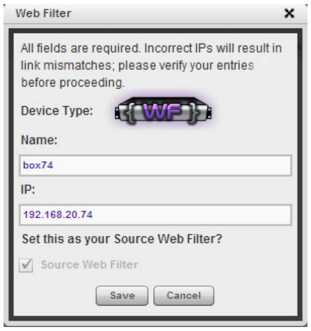
☐ Source Web Filter

2. Enter the server **Name**.
3. Enter the **IP** address of the server.
4. If this Web Filter will be the source server, click the **Source Web Filter** check box.

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

2.3.6.2 View, edit Web Filter device criteria

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



Web Filter

All fields are required. Incorrect IPs will result in link mismatches; please verify your entries before proceeding.

Device Type: WF

Name: box74

IP: 192.168.20.74

Set this as your Source Web Filter?

☑ Source Web Filter

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

2. Edit any of the following:

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

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

2.3.6.3 Delete a Web Filter from the device registry

Caution: If you remove a device, **all data from that device** for Time Usage Reports, Summary Reports, Summary Drill Down Reports and Detail Drill Down Reports **will be purged.**

Trustwave recommends backing up and saving current SR data in a location off the server before adding or removing a Web Filter device in the device registry.

1. Go to the Web Filter server icon in the Device Registry panel and click **Delete** to open the CONFIRM dialog box with a message asking if you want to delete this device.
2. Click **Yes** to delete the Web Filter device from the registry, and to remove the Web Filter server icon from the Device Registry panel.

Tip: If you want to change the current source Web Filter, use the edit function to specify a different Web Filter as the source server before deleting the Web Filter currently designated as the source server. A source Web Filter cannot be deleted until all target Web Filters have been removed.

2.3.7 View Other Device Criteria

The Device Registry panel also includes view only access for the Software Update server and Proxy Server.

To view a summary of configuration for either of these items, click the View link for that item.

To configure the Proxy Server (used to access software updates), see the Software Updates item in System Configuration.

Software Update settings cannot be changed by customers.

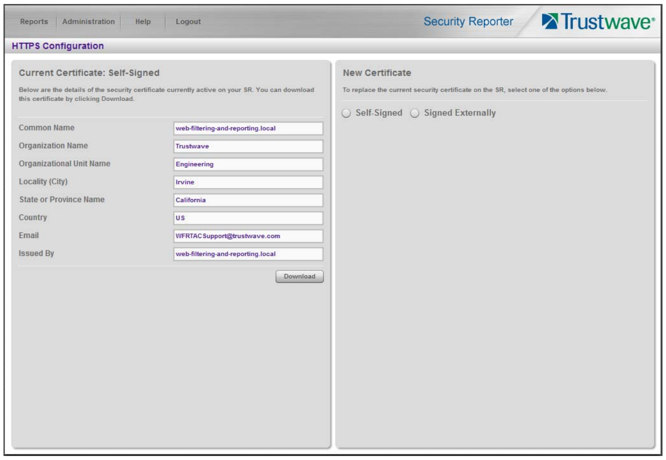
2.4 HTTPS Configuration

By default the SR provides a self-signed Secure Sockets Layer (SSL) certificate to allow secure HTTPS communications between the SR and administrator workstations. A global administrator uses the HTTPS Configuration panel to perform the following tasks:

- To generate a customized self-signed SSL certificate
- To create a request for a trusted SSL certificate and then upload the signed certificate
- To download the installed certificate so that it can be distributed to administrator workstations (to allow trust for self-signed certificates where the workstations cannot determine if the certificate is trusted)

Caution: If the DNS name of the SR changes, a new certificate must be created and possibly added to each client workstation's trusted certificate list.

In the navigation toolbar, hover over the Administration menu link and select **HTTPS Configuration** to open the HTTPS Configuration window. The left panel shows the currently installed certificate.



HTTPS Configuration

Current Certificate: Self-Signed

Below are the details of the security certificate currently active on your SR. You can download this certificate by clicking Download.

Common Name	web-filtering-and-reporting.local
Organization Name	Trustwave
Organizational Unit Name	Engineering
Locality (City)	Irvine
State or Province Name	California
Country	US
Email	WFRTACSupport@trustwave.com
Issued By	web-filtering-and-reporting.local

New Certificate

To replace the current security certificate on the SR, select one of the options below.

○ Self-Signed ○ Signed Externally

2.4.1 Download the Installed Certificate

To download the current SSL certificate from the SR to your workstation, on the left panel click **Download**.

You can distributed the downloaded certificate to administrator workstations as a trusted certificate.

2.4.2 Generate a Self-Signed Certificate for the SR

You can generate a self-signed Secure Socket Layer certificate for the SR to match the identity of the SR server and your organization.

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

1. On the right panel of the HTTPS Configuration window, click **Self-Signed**.
2. Complete all fields using appropriate values.
    - **Common Name**: Hostname of the server, such as `sr.example.local`.

- **Organization Name**: Name of your organization, such as `Example`.
- **Organizational Unit Name**: Name of your department, such as `Administration`.
- **Locality (City)**: Name of your organization's city or principality, such as `Orange`.
- **State or Province Name**: Full name of your state or province, such as `California`.
- **Country**: Two-character code for your country, such as `US`.
- **Email**: Network administrator email address.

3. Click **Apply.** Accept the warning presented. The SSL certificate will be stored on the SR, and the Report Manager will be restarted. All connections to the SR will now use this certificate. Administrators who connect must install the certificate as trusted on their workstations (or make a security exception) in order for their machines to communicate with the SR website.

Note: Although the Security Reporter login window may re-display right away, the service will take a few minutes to restart.

If you do not want to generate and apply the certificate, click **Back** or navigate away from the page.

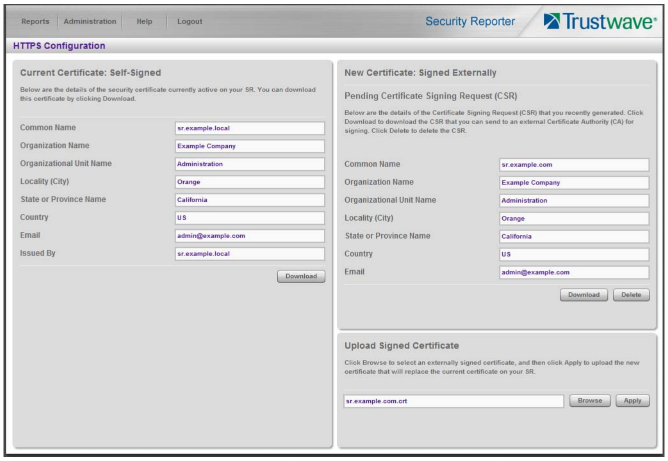
4. Once the SR has restarted, log in and navigate to the HTTPS panel to download the certificate for distribution to workstations.

2.4.3 Use a Third Party Certificate for the SR

You can use a certificate signed by a Certificate Authority that matches the identity of the SR server and your organization. Using a signed certificate allows administrator workstations to recognize the certificate automatically.

2.4.4 Create a CSR

1. On the right panel of the HTTPS Configuration window, click **Signed Externally**.



HTTPS Configuration

Current Certificate: Self-Signed

Below are the details of the security certificate currently active on your SR. You can download this certificate by clicking Download.

Common Name	sr.example.local
Organization Name	Example Company
Organizational Unit Name	Administration
Locality (City)	Orange
State or Province Name	California
Country	US
Email	admin@example.com
Issued By	sr.example.local

New Certificate: Signed Externally

Pending Certificate Signing Request (CSR)

Below are the details of the Certificate Signing Request (CSR) that you recently generated. Click Download to download the CSR that you can send to an external Certificate Authority (CA) for signing. Click Delete to delete the CSR.

Common Name	sr.example.com
Organization Name	Example Company
Organizational Unit Name	Administration
Locality (City)	Orange
State or Province Name	California
Country	US
Email	admin@example.com

Upload Signed Certificate

Click Browse to select an externally signed certificate, and then click Apply to upload the new certificate that will replace the current certificate on your SR.

sr.example.com.crt

2. Complete all fields using appropriate values.

- **Common Name**: Hostname of the server, such as `sr.example.com`.
- **Organization Name**: Name of your organization, such as `Example`.

- **Organizational Unit Name**: Name of your department, such as `Administration`.
- **Locality (City)**: Name of your organization's city or principality, such as `Orange`.
- **State or Province Name**: Full name of your state or province, such as `California`.
- **Country**: Two-character code for your country, such as `US`.
- **Email**: Network administrator email address.

3. Click **Generate** to generate the Certificate Signing Request

Note: If you do not want to generate a CSR, click **Back** or navigate away from the page.

2.4.4.1 Download the CSR, Submit to Certificate Authority

1. On the New Certificate: Signed Externally panel (shown above), click **Download** to download the CSR that you created to your machine. Select a location.
2. Click **Save CSR** to save the CSR to your machine.

Tip: If you do not want to use the CSR, click **Delete** to remove the CSR from the SR.

Do not delete a CSR that you have submitted to a CA for signing, because the CSR must be present in order to upload the signed response from the CA.

3. Submit the CSR to a Certificate Authority authorized to sign SSL certificates..

Tip: Trustwave is a Certificate Authority. See https://ssl.trustwave.com/

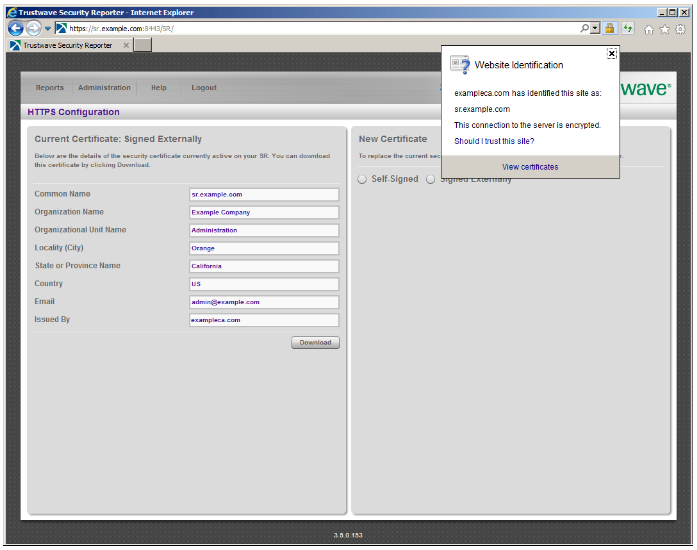
2.4.4.2 Upload the Signed SSL Certificate to SR

When you receive the signed SSL certificate, prepare a certificate file and upload it to the SR.

1. On your workstation, launch a text editor such as Notepad.
2. Copy and paste the contents of the certificate into a text file in the following order:
   a. SSL certificate received from the CA.
   b. Intermediate certificate(s) as provided by the CA.
   c. Root certificate of the CA. (You might not need to paste the Root Certificate, because most CA root certificates are already available with major web browsers).
3. Save the contents of the text file with a .cer or .crt extension.
4. On the Upload Signed Certificate panel, click **Browse**, and browse to the file you just saved.
5. Click **Apply** to load the certificate on the SR.

Caution: Applying the certificate will restart the Report Manager.

6. Once the SR has restarted, log in and navigate to the HTTPS panel to verify that the certificate has been updated. In most cases a CA signed certificate will be trusted by workstations with no further action.



Current Certificate: Signed Externally

Below are the details of the security certificate currently active on your SR. You can download this certificate by clicking Download.

Common Name	sr.example.com
Organization Name	Example Company
Organizational Unit Name	Administration
Locality (City)	Orange
State or Province Name	California
Country	US
Email	admin@example.com
Issued By	exampleca.com

To replace the current sec

exampleca.com has identified this site as:

sr.example.com

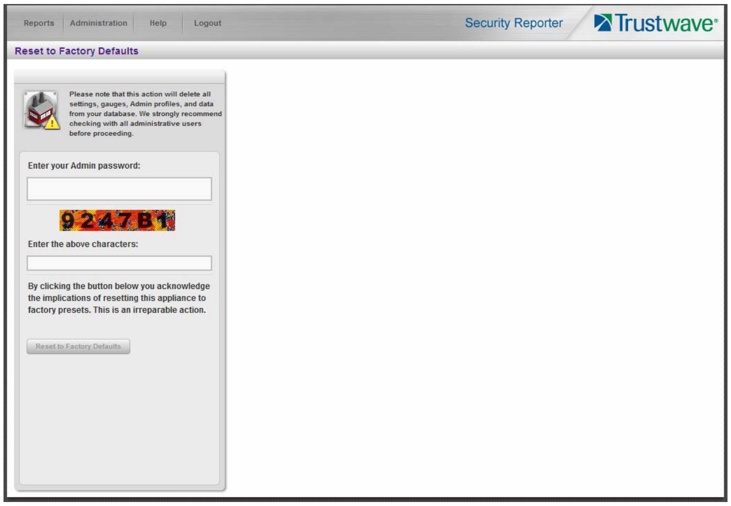
This connection to the server is encrypted.

7. You can click **Download** to retrieve the certificate and distribute it to workstations if required.

2.5 Reset to Factory Defaults panel

A global administrator uses the Reset to Factory Defaults panel, if necessary, to restore the SR to default settings for the application as originally shipped by Trustwave. (Any software updates that you may have been applied will be removed.)

In the navigation toolbar, hover over the Administration menu link and select **Reset to Factory Defaults** to display the Reset to Factory Defaults panel:



Please note that this action will delete all settings, gauges, Admin profiles, and data from your database. We strongly recommend checking with all administrative users before proceeding.

Enter your Admin password:

Enter the above characters:

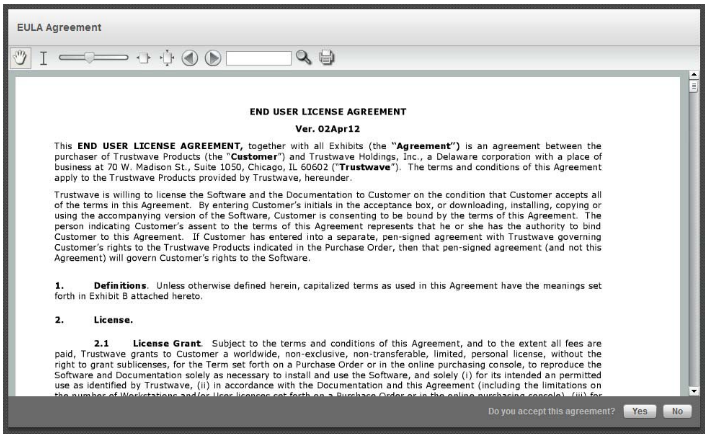
By clicking the button below you acknowledge the implications of resetting this appliance to factory presets. This is an irreparable action.

Caution: This process deletes all settings and data from the SR.

- **All settings** made on the SR, including administrator and group configuration, will be purged and cannot be restored. The SR will also be set to evaluation mode.
- **All data** in the reporting database will be purged and cannot be recovered.
- The reset action is irreversible.

2.5.1 Reset SR to factory defaults

1. **Enter your Admin password** that was created during the SR wizard hardware installation process.
2. **Enter the above characters** displayed beneath the Admin password security characters.
3. Click **Reset to Factory Defaults** to reset the SR application and to display the SR's End User License Agreement window:



END USER LICENSE AGREEMENT

Ver. 02Apr12

This **END USER LICENSE AGREEMENT,** together with all Exhibits (the **"Agreement")** is an agreement between the purchaser of Trustwave Products (the "**Customer**") and Trustwave Holdings, Inc., a Delaware corporation with a place of business at 70 W. Madison St., Suite 1050, Chicago, IL 60602 ("**Trustwave**"). The terms and conditions of this Agreement apply to the Trustwave Products provided by Trustwave, hereunder.

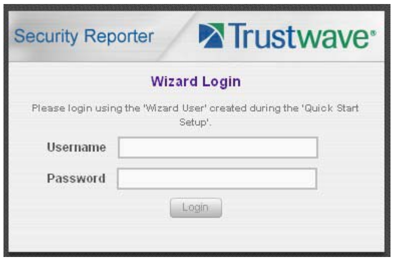
Trustwave is willing to license the Software and the Documentation to Customer on the condition that Customer accepts all of the terms in this Agreement. By entering Customer's initials in the acceptance box, or downloading, installing, copying or using the accompanying version of the Software, Customer is consenting to be bound by the terms of this Agreement. The person indicating Customer's assent to the terms of this Agreement represents that he or she has the authority to bind Customer to this Agreement. If Customer has entered into a separate, pen-signed agreement with Trustwave governing Customer's rights to the Trustwave Products indicated in the Purchase Order, then that pen-signed agreement (and not this Agreement) will govern Customer's rights to the Software.

1. **Definitions**. Unless otherwise defined herein, capitalized terms as used in this Agreement have the meanings set forth in Exhibit B attached hereto.

2. **License.**

2.1 **License Grant**. Subject to the terms and conditions of this Agreement, and to the extent all fees are paid, Trustwave grants to Customer a worldwide, non-exclusive, non-transferable, limited, personal license, without the right to grant sublicenses, for the Term set forth on a Purchase Order or in the online purchasing console, to reproduce the Software and Documentation solely as necessary to install and use the Software, and solely (i) for its intended an permitted use as identified by Trustwave, (ii) in accordance with the Documentation and this Agreement (including the limitations on the number of Workstations and/or User licenses set forth on a Purchase Order or in the online purchasing console), (iii) for

4. After reading the contents of the EULA, click **Yes** to accept it and to go to the Wizard Login window:



Security Reporter

Wizard Login

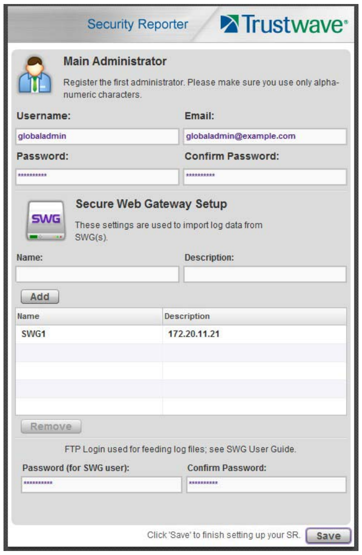
Please login using the 'Wizard User' created during the 'Quick Start Setup'.

Username

Password

2.5.2 Wizard panel

1. In the Wizard Login window, type in the **Username** created during the wizard hardware installation process.
2. Type in the **Password** created for the Username during the wizard hardware installation process.
3. Click **Login** to display the wizard panel:



Security Reporter

Main Administrator

Register the first administrator. Please make sure you use only alpha-numeric characters.

Username: globaladmin

Email: globaladmin@example.com

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

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

Secure Web Gateway Setup

These settings are used to import log data from SWG(s).

Name:

Description:

Name	Description
SWG1	172.20.11.21

FTP Login used for feeding log files; see SWG User Guide.

Password (for SWG user): **********

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

Click 'Save' to finish setting up your SR.

2.5.2.1 Main Administrator

In the Main Administrator section, type in the following information: **Username**, **Email** address, **Password**, **Confirm Password**.

Note: The username 'admin' cannot be used, since it is the default username.

2.5.2.2 Secure Web Gateway Setup

Note: Secure Web Gateway Setup entries are only required if one or more Secure Web Gateway Policy Servers will be used with this SR.

It is not necessary to enter the SWG information during this Wizard setup process. You can enter or edit it later in SR device registry, as described in the Device Registry panel sub-section. As a minimum you should enter the password in the Wizard.

1. In the Secure Web Gateway Setup section, type in the **Name** and/or **Description** for the Secure Web Gateway server, and then click **Add** to include the server criteria in the list box below.

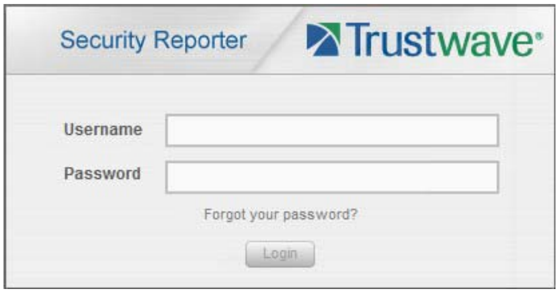
Tip: To remove the SWG from the list box, select it and then click **Remove**.

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

Note: The password entered in this field must be added in the user interface of each SWG that will send logs to this SR, as explained in the SWG's Management Console Reference Guide.

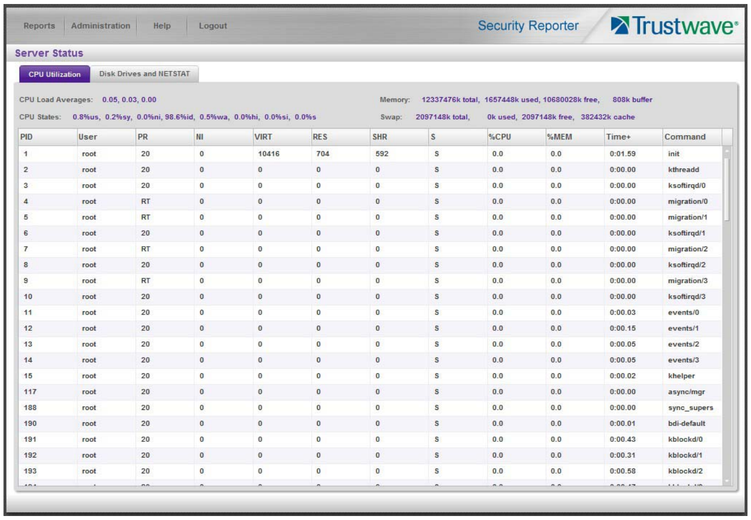
2.5.2.3 Save Entries

Click **Save** to save your entries and to go to the SR login window:



2.6 Server Status

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



Server Status

CPU Load Averages: 0.05, 0.03, 0.00

Memory: 12337476k total, 1657448k used, 10680028k free, 808k buffer

CPU States: 0.8%us, 0.2%sy, 0.0%ni, 98.6%id, 0.5%wa, 0.0%hi, 0.0%si, 0.0%s

Swap: 2097148k total, 0k used, 2097148k free, 382432k cache

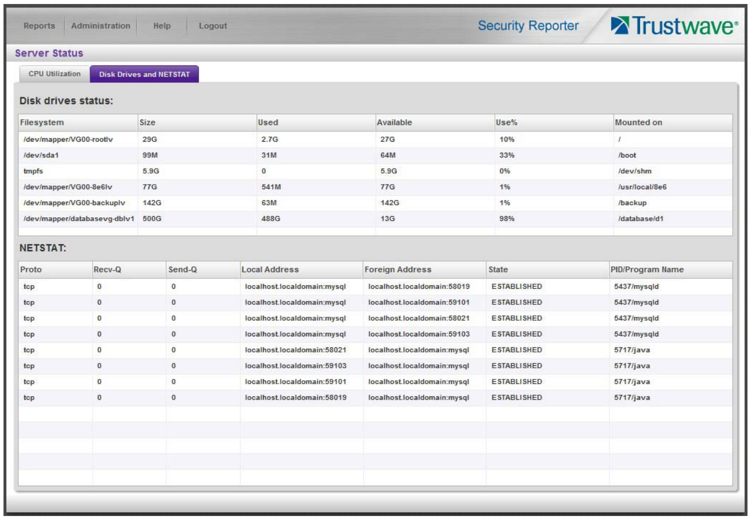
PID	User	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	Time+	Command
1	root	20	0	10416	704	592	S	0.0	0.0	0:01.59	init
2	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kthreadd
3	root	20	0	0	0	0	S	0.0	0.0	0:00.00	ksoftirqd/0
4	root	RT	0	0	0	0	S	0.0	0.0	0:00.00	migration/0
5	root	RT	0	0	0	0	S	0.0	0.0	0:00.00	migration/1
6	root	20	0	0	0	0	S	0.0	0.0	0:00.00	ksoftirqd/1
7	root	RT	0	0	0	0	S	0.0	0.0	0:00.00	migration/2
8	root	20	0	0	0	0	S	0.0	0.0	0:00.00	ksoftirqd/2
9	root	RT	0	0	0	0	S	0.0	0.0	0:00.00	migration/3
10	root	20	0	0	0	0	S	0.0	0.0	0:00.00	ksoftirqd/3
11	root	20	0	0	0	0	S	0.0	0.0	0:00.03	events/0
12	root	20	0	0	0	0	S	0.0	0.0	0:00.15	events/1
13	root	20	0	0	0	0	S	0.0	0.0	0:00.05	events/2
14	root	20	0	0	0	0	S	0.0	0.0	0:00.05	events/3
15	root	20	0	0	0	0	S	0.0	0.0	0:00.02	khelper
117	root	20	0	0	0	0	S	0.0	0.0	0:00.00	async/mgr
188	root	20	0	0	0	0	S	0.0	0.0	0:00.00	sync_supers
190	root	20	0	0	0	0	S	0.0	0.0	0:00.01	bdi-default
191	root	20	0	0	0	0	S	0.0	0.0	0:00.43	kblockd/0
192	root	20	0	0	0	0	S	0.0	0.0	0:00.31	kblockd/1
193	root	20	0	0	0	0	S	0.0	0.0	0:00.58	kblockd/2

2.6.1 CPU Utilization

This tab provides global CPU load averages, CPU states, and memory and swap statistics. The list shows details for each running process.

2.6.2 Disk Drives and NETSTAT

This screen provides disk drive and network information.



Server Status

Disk drives status:

Filesystem	Size	Used	Available	Use%	Mounted on
/dev/mapper/VG00-rootlv	29G	2.7G	27G	10%	/
/dev/sda1	99M	31M	64M	33%	/boot
tmpfs	5.9G	0	5.9G	0%	/dev/shm
/dev/mapper/VG00-8e6lv	77G	541M	77G	1%	/usr/local/8e6
/dev/mapper/VG00-backuplv	142G	63M	142G	1%	/backup
/dev/mapper/databasevg-dblv1	500G	488G	13G	98%	/database/d1

NETSTAT:

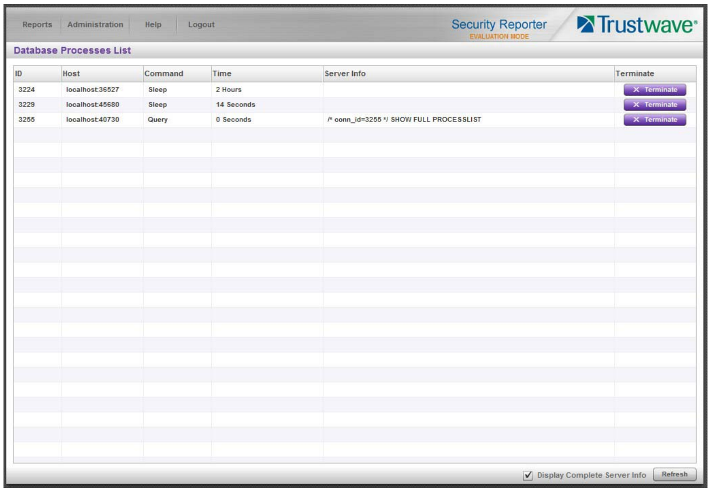
Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program Name
tcp	0	0	localhost.localdomain:mysql	localhost.localdomain:58019	ESTABLISHED	5437/mysqld
tcp	0	0	localhost.localdomain:mysql	localhost.localdomain:59101	ESTABLISHED	5437/mysqld
tcp	0	0	localhost.localdomain:mysql	localhost.localdomain:58021	ESTABLISHED	5437/mysqld
tcp	0	0	localhost.localdomain:mysql	localhost.localdomain:59103	ESTABLISHED	5437/mysqld
tcp	0	0	localhost.localdomain:58021	localhost.localdomain:mysql	ESTABLISHED	5717/java
tcp	0	0	localhost.localdomain:59103	localhost.localdomain:mysql	ESTABLISHED	5717/java
tcp	0	0	localhost.localdomain:59101	localhost.localdomain:mysql	ESTABLISHED	5717/java
tcp	0	0	localhost.localdomain:58019	localhost.localdomain:mysql	ESTABLISHED	5717/java

- Disk drives status: provides data on the status of each drive of the operating system
- NETSTAT: displays information about currently active network connections by address and port

2.7 Database Processes List panel

A global administrator uses the Database Processes List panel to view a list of processes currently running on the SR or to halt a process that is currently running.

In the navigation toolbar, hover over the Administration menu link and select **Database Processes List** to display the Database Processes List panel. To update the information on this panel, click **Refresh** at the bottom of the panel.



Database Processes List

ID	Host	Command	Time	Server Info	Terminate
3224	localhost:36527	Sleep	2 Hours		✕ Terminate
3229	localhost:45680	Sleep	14 Seconds		✕ Terminate
3255	localhost:40730	Query	0 Seconds	/* conn_id=3255 */ SHOW FULL PROCESSLIST	✕ Terminate

☑ Display Complete Server Info

2.7.1 View Full Processes Info

To see more detailed information, check the box **Display Complete Server Info** at the bottom of the panel, and then click **Refresh**.

2.7.2 View Details on a Process

Each row in the list includes the following information: process identification number (ID) on the MySQL server; Hostname or IP address of the server, and port connected to the database; the state of the last Command issued by the user ("Query" or "Sleep"); the amount of Time in seconds the process has remained in its current state, and SQL statement for a process currently running (Server Info). At the end of each row is the Terminate option.

Tip: Click the **Refresh** button to refresh the list of records.

2.7.3 Terminate a Process

Select the process to be terminated and click **Terminate**.

Caution: Be sure that you do not terminate the wrong process.

3 Report Manager Administration Section

3.1 Introduction

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

Note: Before configuring the Report Manager, a global administrator must fully configure the SR server (as described in the previous section of this *Administrator Guide*).

The Report Manager’s Administration menu includes the following functions:

- System Setup: Device Registry, HTTPS configuration, and reset to factory defaults are covered in Section 2.
- Group and Profile Management: Section 3.2 explains how to set up user groups whose Internet activity will be monitored by group administrators. Section 3.3 shows how to set up administrator accounts (global or group administrators).
- Monitoring and database storage: Section 3.4 explains how to view administrator activity; Section 3.5 explains how to view the database storage consumed.
- Report Configuration: Section 3.6 explains how to create and manage Custom Category Groups used for monitoring end user Internet activity, and configure general report settings.

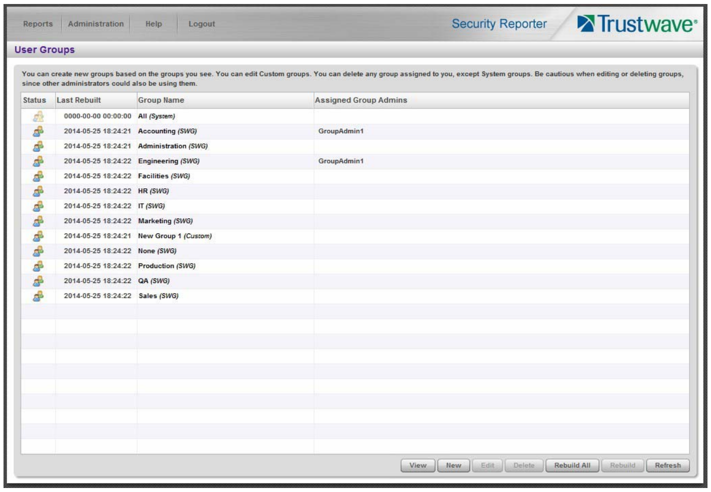
3.2 User Group Management

This section describes the User Groups panel, accessed from the Administration menu of the Report Manager.

On this panel, Group Administrators can view groups assigned to them, but they cannot make any changes. Global Administrators can use all functions described.

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

1. In the navigation toolbar, hover over the Administration menu link to display topics available to you.
2. Click **User Groups** to display the User Groups panel:



User Groups

You can create new groups based on the groups you see. You can edit Custom groups. You can delete any group assigned to you, except System groups. Be cautious when editing or deleting groups, since other administrators could also be using them.

Status	Last Rebuilt	Group Name	Assigned Group Admins
	0000-00-00 00:00:00	All *(System)*	
	2014-05-25 18:24:21	Accounting *(SWG)*	GroupAdmin1
	2014-05-25 18:24:21	Administration *(SWG)*	
	2014-05-25 18:24:22	Engineering *(SWG)*	GroupAdmin1
	2014-05-25 18:24:22	Facilities *(SWG)*	
	2014-05-25 18:24:22	HR *(SWG)*	
	2014-05-25 18:24:22	IT *(SWG)*	
	2014-05-25 18:24:22	Marketing *(SWG)*	
	2014-05-25 18:24:21	New Group 1 *(Custom)*	
	2014-05-25 18:24:22	None *(SWG)*	
	2014-05-25 18:24:22	Production *(SWG)*	
	2014-05-25 18:24:22	QA *(SWG)*	
	2014-05-25 18:24:22	Sales *(SWG)*	

User groups previously imported or added by the administrator display in the list. For each group name, the group type ("System", "Custom", "LDAP", or "SWG") displays in parentheses after the name.

For a global administrator, "All (System)" displays as the first record in the list by default. This user group includes all users on this SR.

The "Custom" user group type displays for any non-imported user group created by an administrator, "LDAP" displays for an LDAP user group used by the SWG, and "SWG" displays for an SWG user group.

Notes:

- A global administrator will see all user groups, and a group administrator will only see user groups that are assigned to him/her.
- The special group "All *(System)*" that was visible to global administrators in previous versions is no longer present.
- A Custom user group name appended with "-DUPLICATE" indicates that this SWG user group no longer exists on the SWG, but was still found on the SR. In this scenario, the administrator should confirm that this user group record is no longer needed, and then delete it from the list of user groups in the User Groups sub-panel.

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

Note: The SR will import user groups from an SWG using IP group authentication or the following LDAP server types:

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

3.2.1 View User Group Information

For each group in the User Groups list, the following information displays: Status icon, Group Name, the date the user group was Last Rebuilt on demand (YYYY-MM-DD HH:MM) if applicable, and a list of assigned Group Administrators.

Note: User groups are automatically rebuilt daily.

3.2.1.0.1 User group status key

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

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

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

3.2.1.1 View a list of members in a user group

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

1. On the User Groups panel, select (highlight) any group.
2. Click **View** to view the group members.
3. The IP and User panels show the included (or excluded) IP addresses and users.

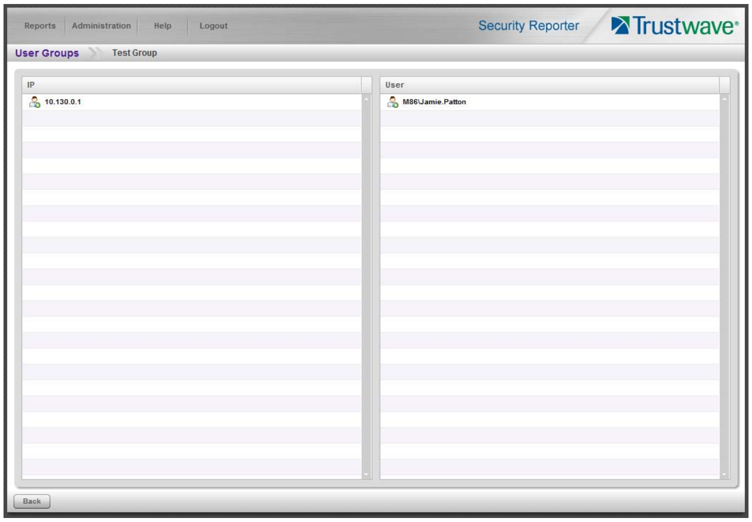
Notes:

In the Selected items, an entry marked with a green + is included in the group. An entry marked with a red - is excluded from the group.

All entries that originate from imported groups will display in the Users list, including items that are only known by their IP address.

For more help and examples on the User Group panel see the **Learn More** link from the text at the top of the panel.

4. To return to the User Groups panel, click **Back.**



IP	User
10.130.0.1	M86\Jamie.Patton

3.2.2 Add a User Group

To add a new user group:

1. From the User Groups list, select (highlight) an existing user group to be used as the base group for creating the new user group.

Tip: To begin with an empty group, select the **All** group.

2. Click **New**.

3. Enter at least three characters for the group **Name** (at the top of the screen). This action activates the Save button.

4. On the User Group panel:

Tip: For more help and examples on the User Group panel see the **Learn More** link from the text at the top of the panel.

   a. At the top of the panel, click the IP or User item type tab to work with that item type. A group can contain items of one or both types.

   b. The Selected Items list is initially populated with the IP addresses or Users that are members of the base group.

   c. 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). For the IP type, you can also enter ranges in CIDR notation (for example, `10.160.0.0/24` or `2001:db8::/32`).

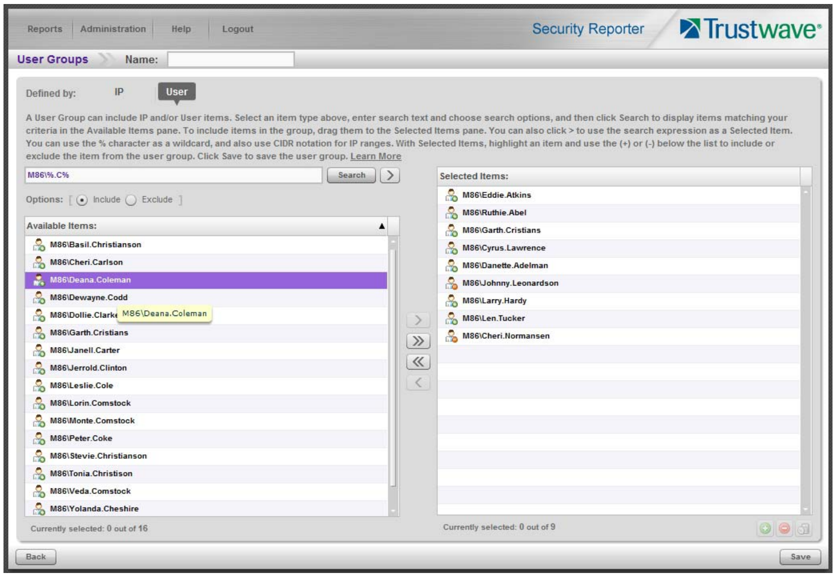
   d. Choose a search option (Include or Exclude) to indicate whether you want to find items that match, or do not match, the search terms.

   e. Use the search text in one of two ways:

- Click **Search** to perform the query. Results appear in the Available Items list box below. You can add one or more filters from the list to Selected Items.

- Click the > button to add the search text directly to Selected Items. The text including any wildcards will be evaluated each time the groups is used for a report.

f. To add items from Available Items to Selected Items, select and drag the items, or click to select, and then click the single right arrow > to move the filter(s) to the Selected Items list box. Use the double right arrow » to move all items.



Name:

Defined by: User

A User Group can include IP and/or User items. Select an item type above, enter search text and choose search options, and then click Search to display items matching your criteria in the Available Items pane. To include items in the group, drag them to the Selected Items pane. You can also click > to use the search expression as a Selected Item. You can use the % character as a wildcard, and also use CIDR notation for IP ranges. With Selected Items, highlight an item and use the (+) or (-) below the list to include or exclude the item from the user group. Click Save to save the user group. Learn More

M86\%.C%

Options: [● Include ○ Exclude]

Available Items:

M86\Basil.Christianson
M86\Cheri.Carlson
M86\Deana.Coleman
M86\Dewayne.Codd
M86\Dollie.Clarke
M86\Garth.Cristians
M86\Janell.Carter
M86\Jerrold.Clinton
M86\Leslie.Cole
M86\Lorin.Comstock
M86\Monte.Comstock
M86\Peter.Coke
M86\Stevie.Christianson
M86\Tonia.Christison
M86\Veda.Comstock
M86\Yolanda.Cheshire

Currently selected: 0 out of 16

Selected Items:

M86\Eddie.Atkins
M86\Ruthie.Abel
M86\Garth.Cristians
M86\Cyrus.Lawrence
M86\Danette.Adelman
M86\Johnny.Leonardson
M86\Larry.Hardy
M86\Len.Tucker
M86\Cheri.Normansen

Currently selected: 0 out of 9

Tip: To remove any item or items from the Selected Items 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 Item from the group.

- To include items matching a Selected Item, 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 Item, 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 group must have at least one Included Selected Item. If you remove all included items from the group, +% (include all items) is added automatically. When you add an Included Selected Item, +% is removed automatically.

6. When you have finished editing both the IPs and Users lists, click **Save** to save your edits, and to re-display the User Groups panel where the user group you added now displays in the list.

3.2.3 Edit a User Group

You can edit Custom groups.

To edit a user group:

1. From the main User Groups panel, select the user group from the list in the User Groups sub-panel.
2. Click **Edit** to display the User Group panel.
3. Add or remove items as described above.
4. Click **Save** to save your edits and to return to the User Groups panel.

3.2.4 Rebuild User Group(s)

After editing a user group, you should rebuild it to ensure that all select items are included.

You can also rebuild one or more groups (including imported groups) at any time

Rebuilding an imported group ensures that it reflects any recent changes on the source device.

To rebuild all groups, click **Rebuild All** at the bottom of the sub-panel.

To rebuild an individual group:

1. In the User Groups sub-panel, select the user group to be rebuilt.
2. Click **Rebuild** to initiate the rebuild process for that user group.

After a few minutes, click the **Refresh** button to refresh the display in the panel. Note that the Last Rebuilt column for user groups you rebuilt now displays the date and time of the rebuild.

3.2.5 Delete a User Group

To delete a user group (except System groups):

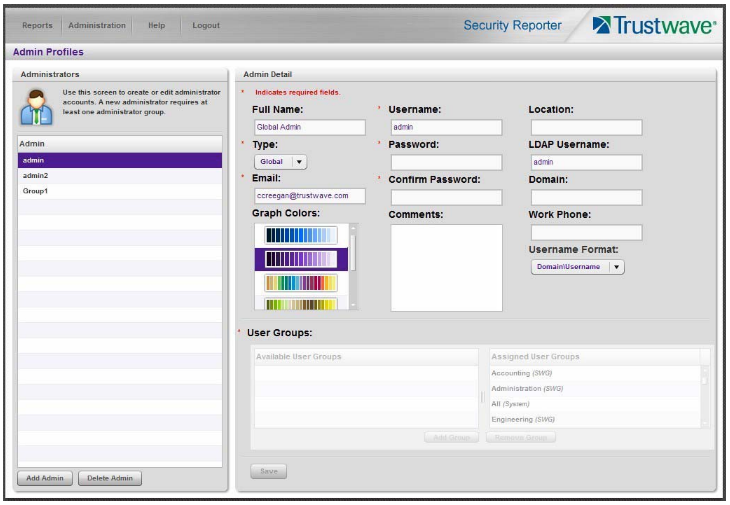
1. In the User Groups sub-panel, select the user group from the User Groups list.
2. Click **Delete** to open the Confirm dialog box asking if you want to delete this user group.
3. Click **Yes** to confirm the deletion, and to remove the user group from the User Groups list. (Click **No** to keep the group unchanged.)

3.3 Admin Profiles panel

As a global administrator, you can create global and group administrators. Global administrators have the same permissions as the default global administrator and can manage all system functions as well as working with specific user groups. Group administrators can only work with the specific user groups that are assigned to them.

As a Group Administrator you can use this panel only to review your own profile and make limited changes.

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



Admin Profiles

Administrators

Use this screen to create or edit administrator accounts. A new administrator requires at least one administrator group.

Admin: admin, admin2, Group1

Admin Detail

* Indicates required fields.

Full Name: Global Admin

* Username: admin

Location:

* Type: Global

* Password:

LDAP Username: admin

* Email: ccreegan@trustwave.com

* Confirm Password:

Domain:

Graph Colors:

Comments:

Work Phone:

Username Format: Domain\Username

* User Groups:

Available User Groups	Assigned User Groups
	Accounting *(SWG)*
	Administration *(SWG)*
	All *(System)*
	Engineering *(SWG)*

If logged in as a global administrator, at the left side of this panel, the Administrators list box in the Administrators sub-panel displays usernames of all administrator accounts previously set up in this panel.

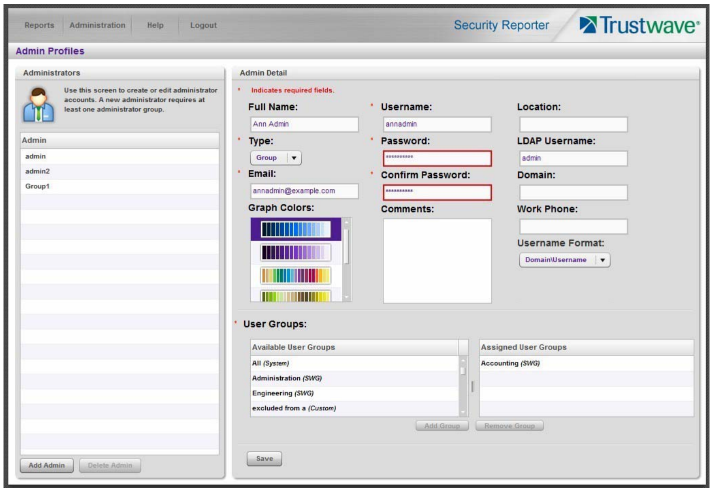
Note: In addition to seeing usernames set up and saved by the administrator in this panel, a global administrator will also see the username established during the wizard hardware installation process.

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

3.3.1 Add an Administrator Profile

1. If you are a Global Administrator, at the bottom of the Administrators sub-panel, you can click **Add Admin** to clear and reset the Admin Detail sub-panel.

2. In the Admin Detail sub-panel, make the following entries or selections as appropriate:



Admin Profiles

Administrators

Use this screen to create or edit administrator accounts. A new administrator requires at least one administrator group.

Admin: admin, admin2, Group1

Admin Detail

* Indicates required fields.

Full Name: Ann Admin

* Username: annadmin

Location:

* Type: Group

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

LDAP Username: admin

* Email: annadmin@example.com

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

Domain:

Graph Colors:

Comments:

Work Phone:

Username Format: Domain\Username

* User Groups:

Available User Groups	Assigned User Groups
All *(System)*	Accounting *(SWG)*
Administration *(SWG)*	
Engineering *(SWG)*	
excluded from a *(Custom)*	

- Optional: Type in the administrator's **Full Name**.

- Select the administrator **Type** (Global or Group).
- Type in the administrator's **Email** address.
- Optional: Select another report color scheme from the available **Graph Colors** choices.
- Type in the **Username** the administrator will use to access the SR user interface. This entry will display in the Administrators list when the record is saved.
- Type in the **Password** the administrator will use in conjunction with the Username, and enter that same password again in the **Confirm Password** field. These entries display as asterisks for security purposes.
- Optional: Type in any **Comments** to be associated with the administrator's account.
- Optional: Type in identifying information about the administrator's physical office **Location**.
- Optional: If the administrator has an Active Directory LDAP account, username, and domain, type in the alphanumeric group administrator's **LDAP Username** exactly as set up on the Active Directory domain in which he/she is registered.
- Optional: If an entry was made in the LDAP Username field, type in the exact characters for the LDAP Active Directory **Domain** name in which the administrator is registered.
- Optional: Type in the administrator's **Work Phone** number, using digits only.
- Optional: If necessary, specify the **Username Format** used on the LDAP server by making a selection from the available choices—Domain\Username, Username\Domain, Username, Domain.

3. *(For group administrators only)* In the User Groups section, select the user group(s) that should be available to the administrator:

Note: This step applies only for group administrators. A global administrator always has access to all groups.

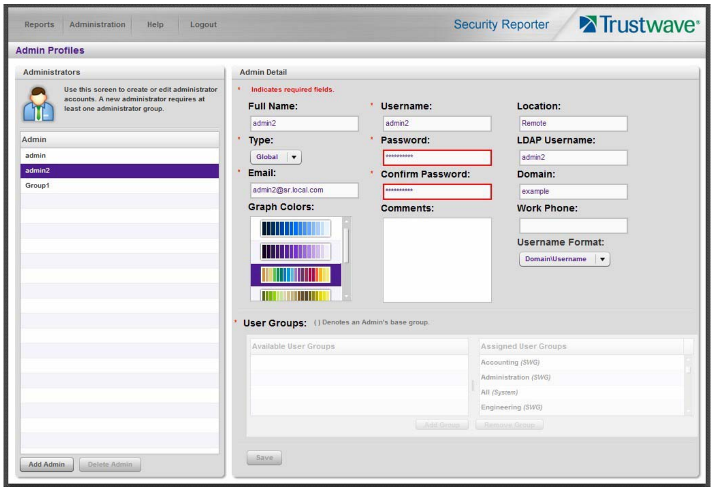
- In the Available User Groups list box, click the user group(s) to highlight your selection(s), and to activate the Add Group button.
- Click **Add Group** to include the user group(s) in the Assigned User Groups list box.

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

4. Click **Save** to add the Username for the new administrator to the Administrators list box.

3.3.2 View Admin Details

If you are a Global Administrator, in the Administrators list box, select the administrator's Username to view that user's profile information in the Admin Detail sub-panel:



Admin Profiles

Administrators

Use this screen to create or edit administrator accounts. A new administrator requires at least one administrator group.

Admin
admin
admin2
Group1

Admin Detail

* Indicates required fields.

Full Name: admin2
* Type: Global
* Email: admin2@sr.local.com
Graph Colors:
* Username: admin2
* Password: **********
* Confirm Password: **********
Comments:
Location: Remote
LDAP Username: admin2
Domain: example
Work Phone:
Username Format: Domain\Username

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

Available User Groups

Assigned User Groups
Accounting (SWG)
Administration (SWG)
All (System)
Engineering (SWG)

If you are a Group administrator, you can only view the information for your own account.

3.3.2.1 Edit Account Info

1. In the populated Admin Detail sub-panel:
   - The following information can be updated: Email address, Graph Colors, Username, Password and Confirm Password entries, Username Format selection, and User Groups selection..

Note: A Group Administrator cannot change the groups assigned to them.

   - The following information can be added, modified, or deleted: Full Name, Comments, Location information, Work Phone number, and LDAP Username or Domain name (if using LDAP).
   - A global administrator also has the ability to modify the Administrator Type selection. A global administrator can change any global administrator to a group administrator, including himself/herself. However at least one administrator must be set as a global administrator at all times. If only one global administrator exists, that account cannot be demoted to group administrator.
2. After making any modifications, click **Save** to save your edits.

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

3.3.3 Delete Admin

Only a global administrator can delete an admin profile.

Caution: Deleting an administrator also deletes any saved reports and schedules that were created by that administrator. Be sure that these reports and schedules are not required before proceeding. You cannot delete all global administrators; at least one global administrator must be set up at all times.

1. In the Administrators list box, select the administrator’s Username.

2. Click **Delete Admin** to open the Confirm dialog box with a message asking if you want to delete this administrator profile.

Tip: Clicking Cancel closes the dialog box without removing the administrator profile.

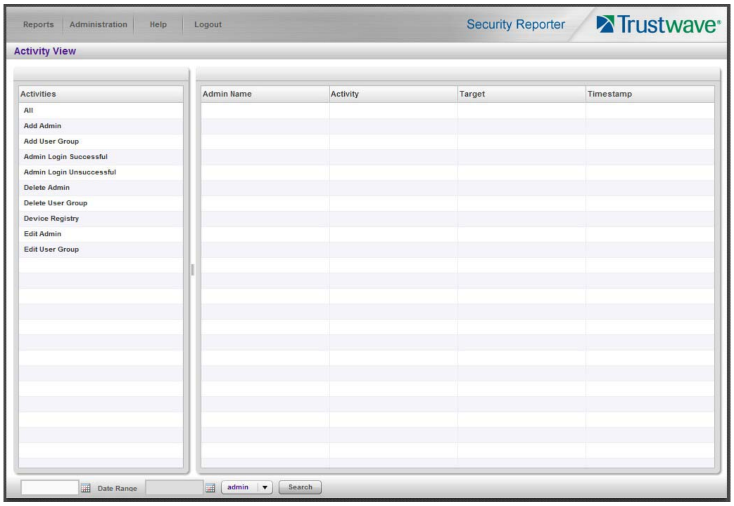
3. Click **Yes** to close the dialog box and to remove the administrator from the system.

3.4 Activity View panel

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

Note: A Global Administrator can search for activities performed by all administrators. A Group Administrator can only search for their own activities.

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



The Activities sub-panel displays to the left and the empty target sub-panel displays to the right. Below these sub-panels is the Date Range field, the administrator usernames menu, and Search button.

3.4.1 Perform a Search on a Specified Activity

To perform a search on a specified activity:

1. Select the type of Activity from available choices in the list.

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

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

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

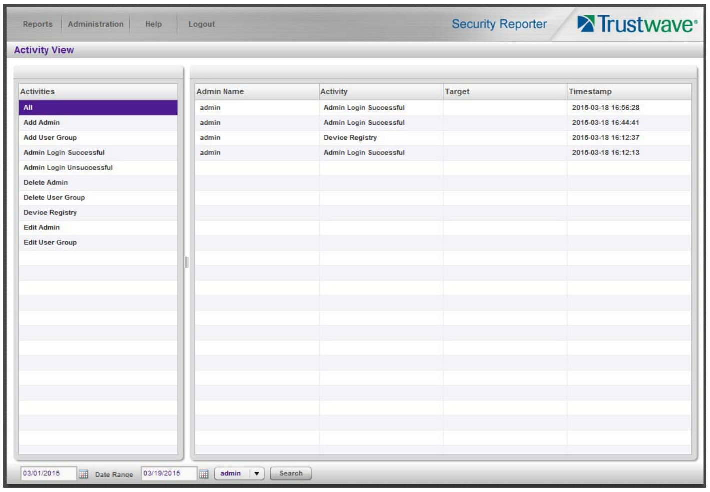
3. Click the starting date to select it and to close the calendar pop-up window. This action populates the field to the left of the calendar icon with the selected date.

4. Click the ▦ calendar icon on the right to open the larger calendar for the current month, with today's date highlighted.

5. Click the ending date to select it and to close the calendar pop-up window. This action populates the field to the left of the calendar icon with the selected date.

6. To view the activity of a specified administrator (if you are a Global Administrator), select the username from the pull-down menu.

7. Click **Search** to display the specified records for the selected dates in the results list:



Activities
All
Add Admin
Add User Group
Admin Login Successful
Admin Login Unsuccessful
Delete Admin
Delete User Group
Device Registry
Edit Admin
Edit User Group

Admin Name	Activity	Target	Timestamp
admin	Admin Login Successful		2015-03-18 16:56:28
admin	Admin Login Successful		2015-03-18 16:44:41
admin	Device Registry		2015-03-18 16:12:37
admin	Admin Login Successful		2015-03-18 16:12:13

03/01/2015 ▦ Date Range 03/19/2015 ▦ admin ▼ Search

3.4.2 Search results

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

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

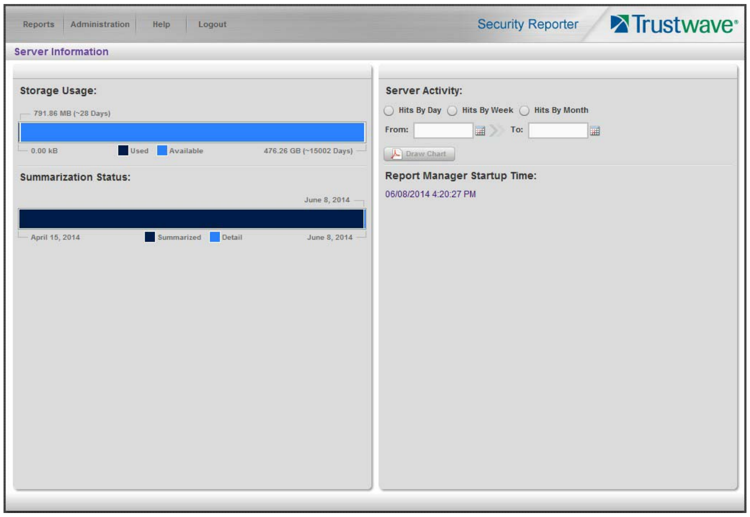
The Target field displays information only as applicable for any of the following actions executed by the administrator (Admin Name), such as:

- administrator name for Add/Edit/Delete Admin
- group name for Add/Edit/Delete Admin Group

3.5 Server Information panel

A global administrator uses the Server Information panel to obtain details about data storage on the SR Server, the time the Report Manager was last restarted, and the SR Server's IP address and current software version number. If the SR is in Evaluation Mode, this panel also provides the Activation functionality.

In the navigation toolbar, hover over the Administration menu link and select **Server Information** to display the Server Information panel:



Server Information

Storage Usage:

791.86 MB (~28 Days)

0.00 kB ■ Used ■ Available 476.26 GB (~15002 Days)

Summarization Status:

June 8, 2014

April 15, 2014 ■ Summarized ■ Detail June 8, 2014

Server Activity:

○ Hits By Day ○ Hits By Week ○ Hits By Month

From: To:

Report Manager Startup Time:

06/08/2014 4:20:27 PM

The panel includes the following information: Storage Usage, Summarization Status, Server Activity, and Report Manager Startup Time. In Evaluation Mode, an additional section titled Activation displays, and the Storage Usage section includes a note about the data available for reporting..

Note: If the SR server is newly installed, server statistics will be available after they are initially correlated for the server, immediately after midnight. If you do not see appropriate statistics after 24 hours, please contact your system administrator.

3.5.1 Registered Mode and Evaluation Mode

Registered Mode is the standard setting for an SR server that has been activated online and registered by Trustwave. An SR in registered mode will store as much data as allocated for data storage on its hard drive—and on its attached storage device, if applicable to the hardware model of the SR server. When the SR is close to reaching its maximum capacity of data storage (as determined by the SR when making its daily check of available storage space), the oldest week of data (from Sunday through Saturday) is dropped from the database.

Evaluation mode refers to an SR which has not yet been activated. In Evaluation Mode, data is stored as for Registered Mode, but a maximum of 14 days of the most recent data is actually available for reporting.

Note: See Appendix C for more information about the Evaluation Mode and activation.

3.5.2 Storage Usage

The Storage Usage section graphically displays the total storage available on the SR, divided into Used and Available storage. A label above the graph indicates the amount of storage used (in MB or GB), and the number of days of data included. A label below the graph indicates the total storage, and an estimate of the total number of days of data that can be stored (based on prior usage).

3.5.3 Summarization Status

The Summarization Status section graphically displays the status of data summarization. Summarized data is pre-processed to allow quicker generation of reports. Labels on the graph indicate the dates of the earliest data, the latest summarized data, and the most recent data.

3.5.4 Report Manager Startup Time

The Report Manager Startup Time indicates the last time the Report Manager was restarted.

Note: This information is useful for troubleshooting manually generated reports. If your reports are not displaying, it may be that the Report Manager has restarted and terminated the report generation process.

3.5.5 Server Activity

In the Server Activity section, specify the type of chart you wish to generate that provides details on the number of hits within a designated time period. A “hit” is any page and/or object an end user accesses as the result of entering a URL in his/her browser window.

1. Specify the time period for the chart you wish to draw:
   a. Click the radio button corresponding to **Hits By Day**, **Hits By Week**, or **Hits By Month**.
   b. At the **From** and **To** fields, make a selection for the date range using the calendar icons:
      - Click the 📅 calendar icon to open the larger calendar for the current month, with today’s date highlighted.

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

      - Click the date to select it and to close the calendar window. This action populates the field to the left of the calendar icon with the selected date.
2. Click the **Draw Chart** button to open a window that displays the chart of your selection in the PDF file format.

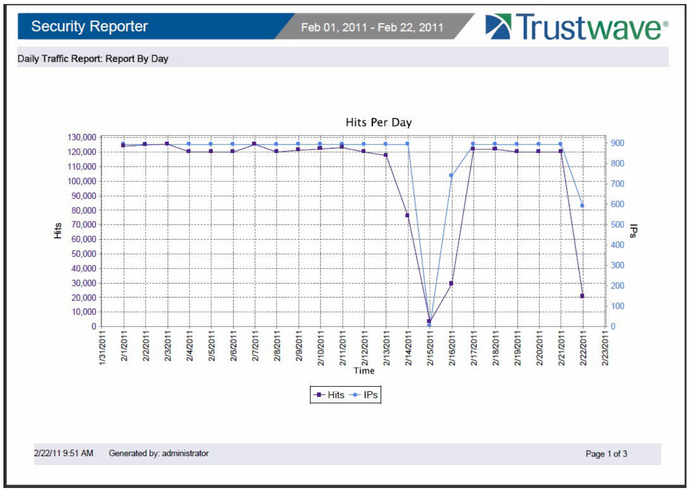
   The header section includes the title of the chart and date range. The footer section includes the date and time the chart was generated (shown in the MM/DD/YYYY HH:MM AM/PM format), the login ID of the person who generated the chart (Generated by) and the Page number and page range.

   The chart image includes a graph illustrating the general Number of Hits (in purple) and Number of IPs that generated those hits (in blue) for each unit of Time in the specified period.

Rows of report details indicate the time measurement (Day, Week, or Month), the exact Number of Hits corresponding to each unit of time, and the Total Records.

Depending on the time frame specified, this chart may be several pages in length.

- **Hits Per Day:** If you selected Hits By Day, days within the date range are plotted on the graph, grouped into equal time intervals. The summary shows the Number of Hits (in purple) and Number of IPs (in blue) for a specified Day (MM/DD/YYYY).

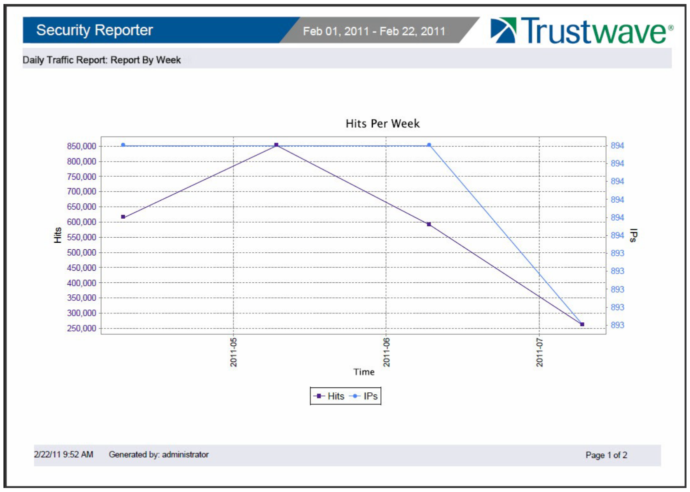


Security Reporter Feb 01, 2011 - Feb 22, 2011 Trustwave®

Daily Traffic Report: Report By Day

2/22/11 9:51 AM Generated by: administrator Page 1 of 3

- **Hits Per Week:** If you selected Hits By Week, each week within the date range is plotted on the graph. The summary shows the general Number of Hits (in purple) and Number of IPs that generated those hits (in blue) for a specified Week (YYYY-WW). Weeks are numbered 01-52. For example, 2011-05 indicates the fifth week in the year 2011—or the first week of February 2011, which included days 1-5.

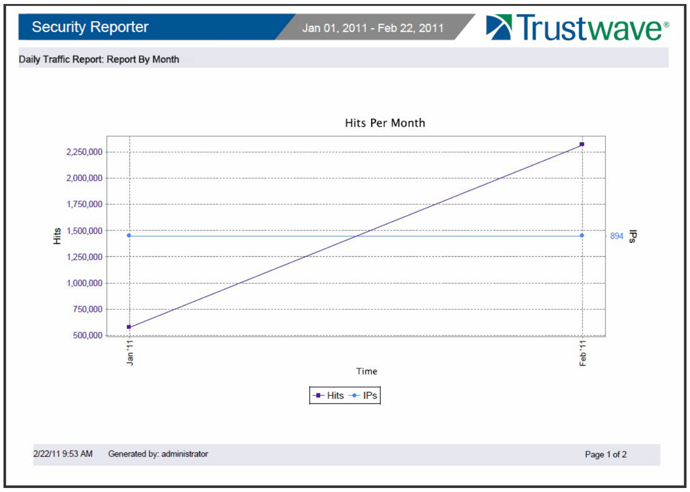


Security Reporter Feb 01, 2011 - Feb 22, 2011 Trustwave®

Daily Traffic Report: Report By Week

2/22/11 9:52 AM Generated by: administrator Page 1 of 2

- **Hits Per Month:** If you selected Hits By Month, each month within the date range is plotted on the graph. The summary shows the general Number of Hits (in purple) and Number of IPs that generated those hits (in blue) for a specified Month (Month ’YY). Month names are abbreviated.



Security Reporter Jan 01, 2011 - Feb 22, 2011

Daily Traffic Report: Report By Month

2/22/11 9:53 AM Generated by: administrator Page 1 of 2

3. You now have the option to do any of the following:

   - Print the chart: Click the print icon to open the Print dialog box, and proceed with standard print procedures.
   - Save the chart: Click the save icon to open the Save a Copy dialog box, and proceed with standard save procedures.
   - Close the chart window: Click the “X” in the upper right corner to close the chart window.
   - Generate a new chart: Make new entries in the Server Information panel.

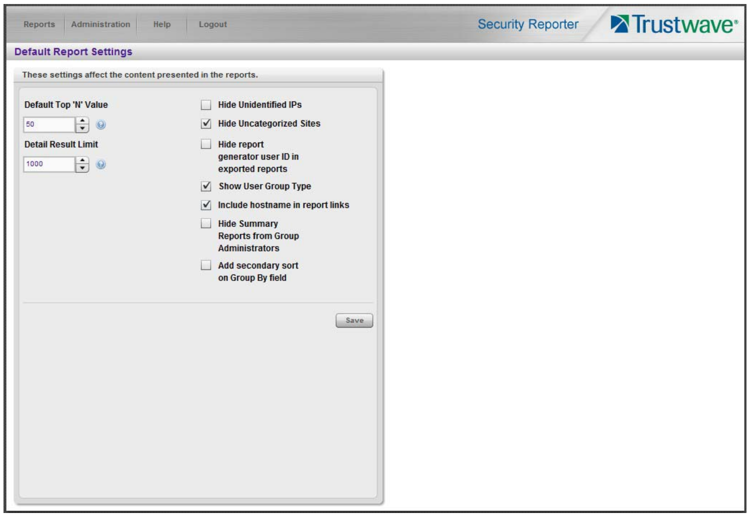
3.6 Report Configuration

The following panels from the Administration menu of the Report Manager are described in this section: Default Report Settings and Custom Category Groups.

3.6.1 Default Report Settings panel

A global administrator uses the Default Report Settings panel to specify various settings to be used in reports.

In the navigation toolbar, hover over the Administration menu link and select **Default Report Settings** to display the Default Report Settings panel:



Default Report Settings

These settings affect the content presented in the reports.

Default Top 'N' Value: 50

Detail Result Limit: 1000

☐ Hide Unidentified IPs
☑ Hide Uncategorized Sites
☐ Hide report generator user ID in exported reports
☑ Show User Group Type
☑ Include hostname in report links
☐ Hide Summary Reports from Group Administrators
☐ Add secondary sort on Group By field

3.6.1.1 Set New Defaults

1. Enter the **Default Top 'N' Value** (the number of records that will be generated by default for summary reports). The original default value is 50 records.

2. Enter the maximum number of records that will be included in a detail report's **Detail Result Limit**. If the number of records from a query exceeds the limit established in this field, the overflow will be included in the next set of records. The default is 1000 records per set.

3. By default, the **Hide Unidentified IPs** check box is de-selected. This setting indicates that activity on machines not assigned to specific users *will* be included in reports such as summary, blocked, and dashboard reports.

   If you wish to exclude activity from machines not assigned to specific users, check this box.

Note: This setting does not affect drill down reports. You can choose to include or exclude activity from Unidentified IPs for each drill down report you create.

4. By default, the **Hide Uncategorized Sites** check box is selected. This indicates that uncategorized sites will not be displayed or counted in drill down reports.

   If you wish to include uncategorized sites in drill down reports, check this box.

5. By default, the **Hide report generator user ID in exported reports** check box is de-selected. This setting indicates that the username of the person who creates a drill down report will be included in the footer of generated reports.

   If you wish to exclude the username of the reporter from drill down reports, check the box.

6. By default, the **Show User Group Type** check box is selected. This setting indicates that for reports in which user groups are grouped by group name, the type of user group ("System", "Custom", "LDAP", or "SWG") will display in parentheses following the name of the user group.

   If you wish to exclude user group types from reports grouped by user group names, un-check the box.

7. By default, the **Include hostname in report links** check box is de-selected. This setting allows you to include the hostname of the SR in place of its IP address in the report links for downloaded and emailed reports. The setting applies only to drill down reports.

   If you wish to use the hostname in drill down report links, check the box.

8. By default, the **Hide Summary Reports from Group Administrators** check box is de-selected. This setting allows you to block access to all summary reports for all Group Administrators (allowing access only to Global Administrators).

   If you wish to hide the summary reports from Group Administrators, check the box.

9. By default, the **Add secondary sort on Group By field** check box is de-selected. This setting will additionally sort report results on the Group By field where they have the same value in the primary sort field.

   If you wish to perform the secondary sort, check this box.

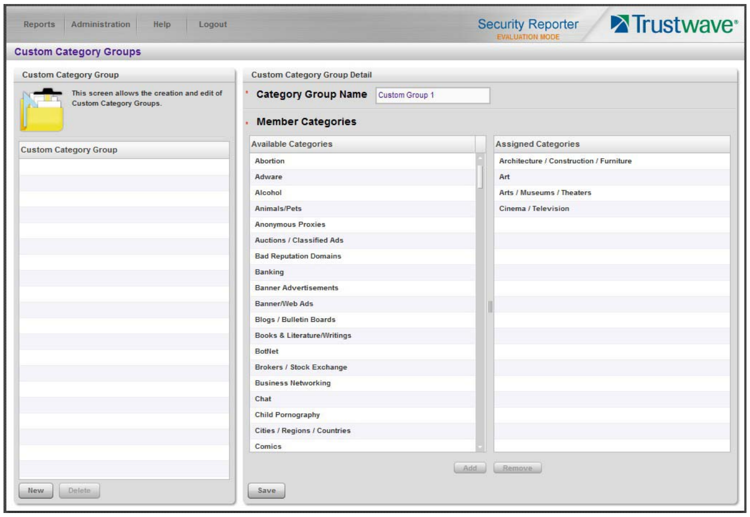
   Note: The secondary sort makes report generation slower. Applying the secondary sort ensures that when a limited number of detail rows is specified, the same items are returned each time a report is generated. Without the secondary sort, detail records can be in random order. The secondary sort also makes the results easier to review.

10. Click **Save** to save your settings in the Default Report Settings panel.

3.6.2 Custom Category Groups panel

The Custom Category Groups option is used for defining a customized group of filter categories, if you wish to run reports only using certain filter categories.

In the navigation toolbar, hover over the Administration menu link and select **Custom Category Groups** to display the Custom Category Groups panel:



Custom Category Groups

Custom Category Group

This screen allows the creation and edit of Custom Category Groups.

Custom Category Group

Custom Category Group Detail

* Category Group Name: Custom Group 1

* Member Categories

Available Categories	Assigned Categories
Abortion	Architecture / Construction / Furniture
Adware	Art
Alcohol	Arts / Museums / Theaters
Animals/Pets	Cinema / Television
Anonymous Proxies	
Auctions / Classified Ads	
Bad Reputation Domains	
Banking	
Banner Advertisements	
Banner/Web Ads	
Blogs / Bulletin Boards	
Books & Literature/Writings	
BotNet	
Brokers / Stock Exchange	
Business Networking	
Chat	
Child Pornography	
Cities / Regions / Countries	
Comics	

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.

3.6.2.1 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. In the Member Categories frame, select Available Categories from the list and click **Add** to move the selection(s) to the Assigned Categories list box

Note: At least one library category must be selected when creating a group.

Tip: To remove one or more library categories from the Assigned Categories list box, make your selection(s), and then click **Remove** to remove the selection(s).

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

3.6.2.2 Modify a Custom Category Group

1. Select the Custom Category Group name from the list box by clicking on your choice to highlight it.
2. Make your edits:
   - To modify the Custom Category Group name, edit the **Category Group Name** in the Custom Category Group Detail sub-panel.
   - To remove an item from the Assigned Categories list box, select the item to select it, and then click **Remove**.
   - To add an item, select it from the Available Categories list box, and then click Add.
3. Click **Update** to save your modification(s).

3.6.2.3 Delete a Category Group

1. Select the Custom Category Group name from the list box by clicking on your choice to highlight it.
2. Click **Delete** to remove the Custom Category Group name from the list box.

4 Reports Section

4.1 Introduction

This section of the *Administrator Guide* provides instructions to administrators on how to utilize the Report Manager to create, view, save and schedule the different types of reports based on the logging data from one or more data sources (SWG policy servers or Web Filters).

The Report Manager includes the following functionality:

- A High Level Overview: Section 4.2 shows you how to view report data in the Dashboard, and how to access pre-generated Summary Reports that provide a high level overview of end user Internet and network activity.
- Drill Down Reports: Section 4.3 provides instructions on using tools to generate summary and detail Drill Down Reports that give you more information on specific end user activity.
- Customize, Maintain Reports: Section 4.4 tells you how to generate customized drill down reports using the Report Wizard, maintain saved drill down reports for ongoing usage, and set up a Report Schedule for running saved drill down reports on a regular basis.
- Specialized Reports: Section 4.5 informs you of three specialized types of reports you can generate: Executive Summary Reports, Blocked Request Reports, and Time Usage Reports.

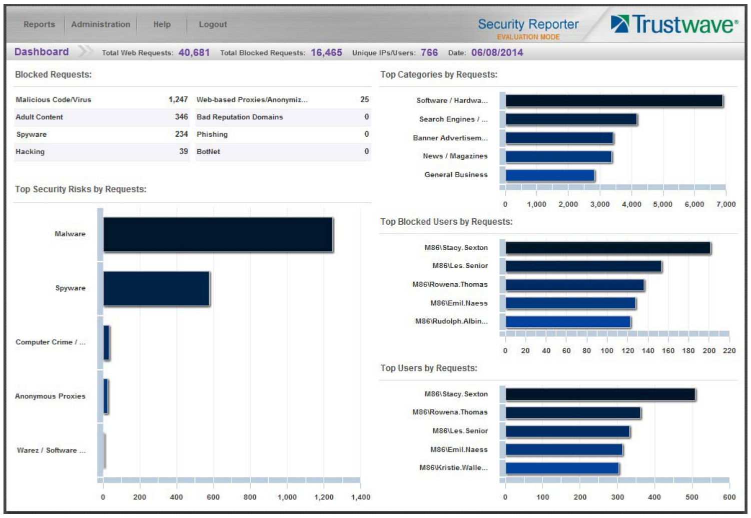
4.2 A High Level Overview

This section describes the Dashboard and Summary Reports accessed from the Reports menu of the Report Manager. These tools give you a high level overview of how end users are currently using the Internet and network resources.

4.2.1 Dashboard

The Dashboard provides statistics and bar charts depicting the top end user requests in various drill-down report categories.

To view the Dashboard, select **Reports | Dashboard** in the navigation toolbar:



Total Web Requests: 40,681 Total Blocked Requests: 16,465 Unique IPs/Users: 766 Date: 06/08/2014

Blocked Requests:

Malicious Code/Virus	1,247	Web-based Proxies/Anonymiz...	25
Adult Content	346	Bad Reputation Domains	0
Spyware	234	Phishing	0
Hacking	39	BotNet	0

At the top of the panel, the following information displays for the current period: Total Web Requests, Total Blocked Requests, Unique IPs/Users, and Date.

The following information displays in the center of the panel:

- **Blocked Requests**: Top eight blocked library categories requested by end users, and the corresponding number of end user requests.
- **Top Categories by Requests**: Top five requested library categories and a bar chart depicting the number of end user requests.
- **Top Security Risks by Requests**: Top five requested Security group library categories and a bar chart depicting the number of end user requests.
- **Top Blocked Users by Requests**: Top five end users with blocked library category requests and a bar chart depicting the number of these end user requests.
- **Top Users by Requests**: Top five end users with library category requests and a bar chart depicting the number of these end user requests.

Tip: Hover over each bar in the bar graph to view the title of the graph entry and the exact value of that entry.

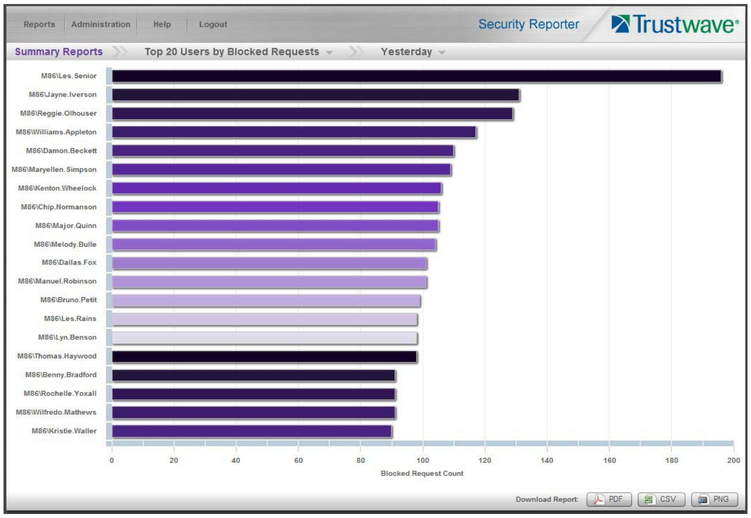
Once you have a high level overview of end user activity on the network, you can use drill-down reports to obtain more information about specific end user trends and activity.

4.2.2 Summary Reports

Summary Reports use pre-generated data to quickly display bar charts or pie charts of end user Internet/network activity for a specified report type within a designated period of time prior to today.

Summary Reports are available to all administrators by default. Access for group administrators can be controlled using a setting on the Default Report Settings panel (see Section 3.6.1).

By default, yesterday's report view showing the Top 20 Users by Blocked Requests displays in the panel:



Note: On a newly installed SR unit, the panel will not show a report until some data has been imported and summarized. If there was no activity for a given report type, the message “No Data to display.” displays in the panel.

Tip: Hover over each bar in the bar graph to view the title of the graph entry and the exact value of the entry.

To select a different summary period or summary report type, click the period name or report type name to view a menu.

4.2.2.1 Summary Report types

To view a menu of summary reports and select a report to view, click the report type name in the title bar.

Available Summary Reports are as follows:

- **Application Control** (SWG only)

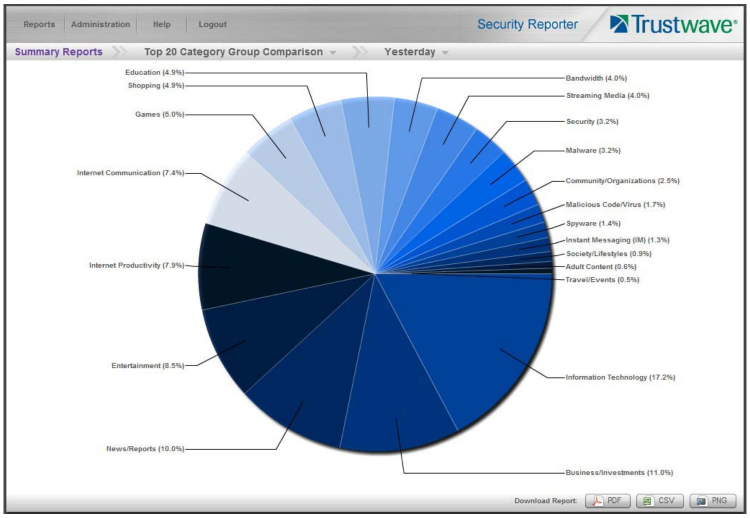
  Note: These reports provide information about end user activity and SWG blocking of activity related to common Web based applications, such as social media. For details of the Application Control feature in SWG, see the SWG *Application Control User Brief* and other SWG documents.

  - **Application Usage Summary:** Pie chart report depicting the percentages of hits for the different Applications.
  - **Top 20 Application Users by Hit Count:** Bar chart report depicting each top end user’s total Application hits (both Blocked and Allowed) as detected by the SWG.
  - **Top 20 Application Users by Bandwidth Consumption:** Bar chart depicting each top end user’s total Megabytes for bandwidth specific to Application hits.
  - **Top 20 Users by Blocked Application Actions:** Bar chart report depicting each top end user’s Blocked Count for Application Action requests.
  - **Top 20 Application Actions:** Bar chart report depicting the top Action types.

  - **Top 20 Blocked Application Actions:** Bar chart report depicting the top Action request types that were blocked by the SWG.
- **Category & Category Group**
  - **Top 20 Categories by Page Count:** Report depicting the total Page Count in the top requested filtering library categories. You can select presentation as a Pie Chart or Bar Chart.
  - **Total Passed 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.
- **Site**
  - **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 Sites by Bandwidth**: Bar chart report depicting the total Bandwidth consumed for the most popular sites accessed by end users.
- **User & User Group**
  - **Top 20 Users by Blocked Requests**: Bar chart report depicting each top end user's total Page Count for Blocked and Warn Blocked requests.
  - **Top 20 Users by Bandwidth Consumption** (SWG only): Bar chart depicting each top end user's total Megabytes for bandwidth requests.
  - **Top 20 Users by Page Count:** Bar chart report depicting each top end user's total Page Count.
  - **Top 20 Users by Malware Hit Count**: Bar chart report depicting each top end user's total Malware Count (both Blocked and Permitted) detected by the filtering device. For Web Filter, the count includes hits 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. For SWG, results reflect library contents mapped to the Trustwave Supplied Categories.
  - **Top 20 Users by Virus Hit Count** (SWG only): Bar chart report depicting each top end user's total Virus Count (both Blocked and Permitted) detected by the anti-virus engine.
  - **Top 20 User Groups by Page Count**: Report depicting the total Page Count for the top scoring user groups. You can select presentation as a Pie Chart or Bar Chart.
- **Virus**
  - **Top 20 Viruses Detected** (SWG only): Bar chart report depicting the top viruses and Virus Count detected by the anti-virus engine.

4.2.2.2 Modify the Summary Report view

The report view displays either a bar chart or pie chart graph based on the selected report type.



Use any the following tools to modify the report view:

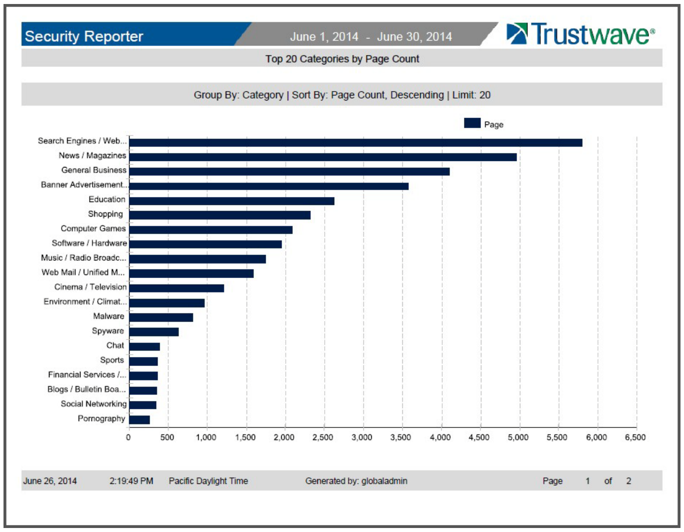
- **Date Scope:** Use the date menu to display data for another period: Yesterday (default), Last Week, Last Month, Current Week, Current Month
- **Report type:** Use the report menu to view another report.

4.2.2.3 Download or Export a Summary Report

At the bottom of the report view, click a **Download Report** option for PDF, CSV, or PNG to generate a report in the specified file format (.pdf, .csv, or .png).

4.2.2.3.1 PDF format

Clicking the **PDF** button opens a separate browser window containing the Summary Report in the .pdf format:


Security Reporter June 1, 2014 - June 30, 2014

Top 20 Categories by Page Count

Group By: Category | Sort By: Page Count, Descending | Limit: 20

June 26, 2014 2:19:49 PM Pacific Daylight Time Generated by: globaladmin Page 1 of 2

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, 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 totaling less than one percent are grouped together under the “Others Combined” label.

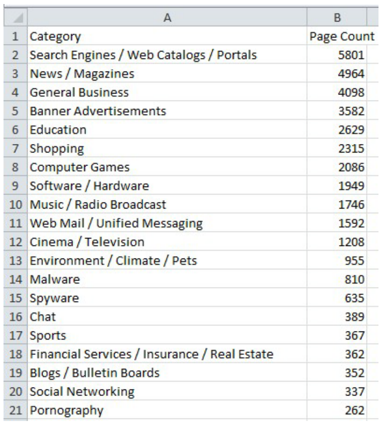
The body of the pages following the first page of the bar or pie chart report includes the following information:

- 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.

The report can be exported by printing it or saving it to your machine.

4.2.2.3.2 CSV format

Clicking the **CSV** button opens a separate browser window containing the Summary Report in the .csv format, or offers to save the file (depending on your browser settings).



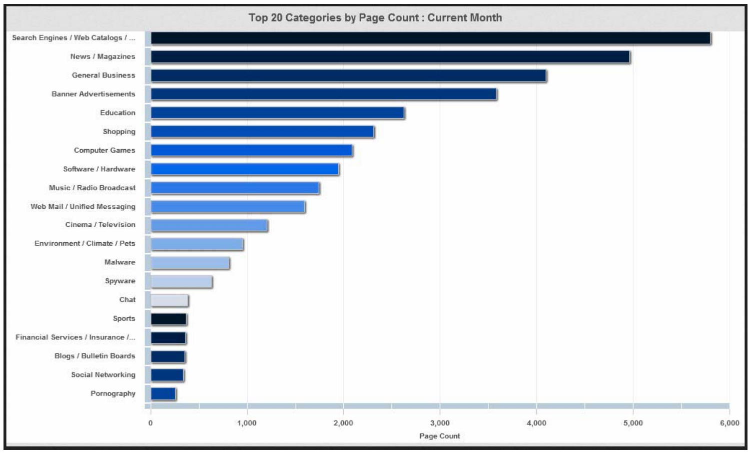
	A	B
1	Category	Page Count
2	Search Engines / Web Catalogs / Portals	5801
3	News / Magazines	4964
4	General Business	4098
5	Banner Advertisements	3582
6	Education	2629
7	Shopping	2315
8	Computer Games	2086
9	Software / Hardware	1949
10	Music / Radio Broadcast	1746
11	Web Mail / Unified Messaging	1592
12	Cinema / Television	1208
13	Environment / Climate / Pets	955
14	Malware	810
15	Spyware	635
16	Chat	389
17	Sports	367
18	Financial Services / Insurance / Real Estate	362
19	Blogs / Bulletin Boards	352
20	Social Networking	337
21	Pornography	262

The report includes a row containing column labels, followed by rows of user data with values corresponding to each column.

No header or footer rows are included, by design. You can import the file directly into a spreadsheet or database.

4.2.2.3.3 PNG format

Clicking the **PNG** button opens a separate browser window containing the Summary Report in the .png format:



The generated report includes the report title followed by a graphical chart image:

- Bar chart: Name of category, username, username path, URL or site IP address, user group name, or blocked user request, and corresponding bar graph. Beneath the bar graph are count indicators and a label describing the type of Count used in the report.
- Pie chart: Color-coded pie graph showing a maximum of 15 categories or user groups. Any categories or user groups with page counts totaling less than one percent are grouped together under the “Others Combined” label.

The report can be exported by printing it or saving it to your machine.

4.3 Drill Down Reports

This section provides information about generating drill down reports that let you query the database to access more detailed information about end user Internet activity.

The two basic reports that administrators can generate with customizations are the summary drill down report and the detail drill down report. Report views for these reports are executed via Reports | Drill Down from the Report Manager user interface:

- **Application Control** (SWG only): Provides information about end user activity and SWG blocking of activity related to common Web based applications.

Note: For details of the Application Control feature in SWG, see the SWG *Application Control User Brief* and other SWG documents.

- **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** (SWG only): 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.

Note: The Report Wizard feature for drill down reports is discussed in detail in Section 4.4.

Once you have generated a drill down report view, you can customize your view, save the view, export the view, and/or schedule the report to run at a designated time.

Note: Before you begin generating report views for these reports, we recommend that you review this section in order to become familiar with available views, and the tools and components used to create summary drill down reports and detail drill down reports customized to your specifications.

4.3.1 Generate a Drill Down Report

To generate a drill down report:

1. Choose one of the following report types from the Reports | Drill Down menu for the summary drill down report you wish to view (depending on logging device): Application Control, Category, Content Type, Rule, Spyware, Violation, Virus. A report for yesterday’s data will be generated.

Note: As the report is generating, the processing message displays. After the report has finished being generated, if no records are available an alert box opens with a message informing you that no records were returned.

2. Once the generated summary drill down report has loaded in the panel, use the tools in the panel to create the desired drill down view. To change the date range and other options, click **Report Wizard** at the bottom left of the panel.

Note: A detail drill down report view is generated by clicking a link in the Blocked Count, Passed Count, Bandwidth (SWG only), Time Count, Blocked Count, or Total Count column corresponding to a specific record displayed in the current summary drill down report view.

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

4.3.2 Summary Drill Down Report View

Summary drill down report views provide a snapshot of end user activity for a specified report type and defined date of activity recorded by the SR.

For each report type, the report type name in the breadcrumb navigation section—beneath the navigation toolbar—includes a drop-down menu for accessing the other reports available from the Drill Down menu.

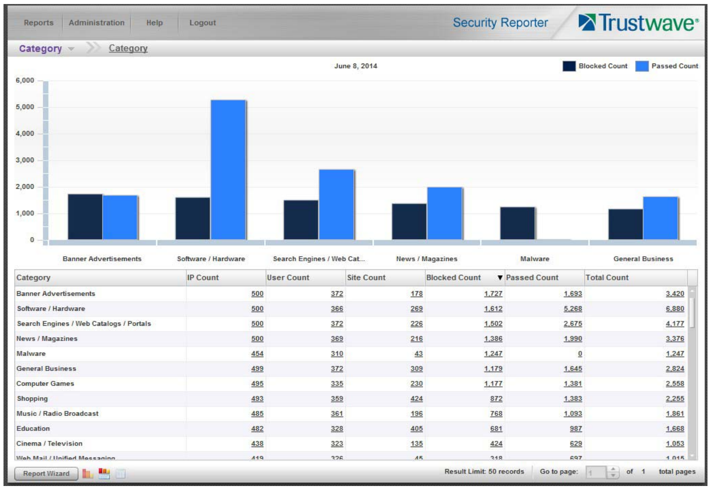
The following information displays at the top of the report view: date (using the month name DD, YYYY format), and Blocked Count and Passed Count key.

Beneath this row, a bar chart depicts the first six sets of records for the current report type.

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

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

The bottom portion of the report view panel includes tools for viewing another page of records (if applicable), or accessing the Report Wizard to download, email, save, or re-run the report.



Category	IP Count	User Count	Site Count	Blocked Count ▼	Passed Count	Total Count
Banner Advertisements	500	372	178	1,727	1,693	3,420
Software / Hardware	500	366	269	1,612	5,268	6,880
Search Engines / Web Catalogs / Portals	500	372	226	1,502	2,675	4,177
News / Magazines	500	369	216	1,386	1,990	3,376
Malware	454	310	43	1,247	0	1,247
General Business	499	372	309	1,179	1,645	2,824
Computer Games	495	335	230	1,177	1,381	2,558
Shopping	493	359	424	872	1,383	2,255
Music / Radio Broadcast	485	361	196	768	1,093	1,861
Education	482	328	405	681	987	1,668
Cinema / Television	438	323	135	424	629	1,053
Web Mail / Unified Messaging	419	326	45	318	697	1,015

Tip: To refresh the current report view, select the same report name from the report type menu in the breadcrumb navigation bar.

4.3.2.1 Summary Report View Tools and Tips

4.3.2.1.1 Report type menu

The report type menu lets you choose a summary drill down report to view: Application Control, Category, Content Type, Rule, Spyware, Violation, Virus.

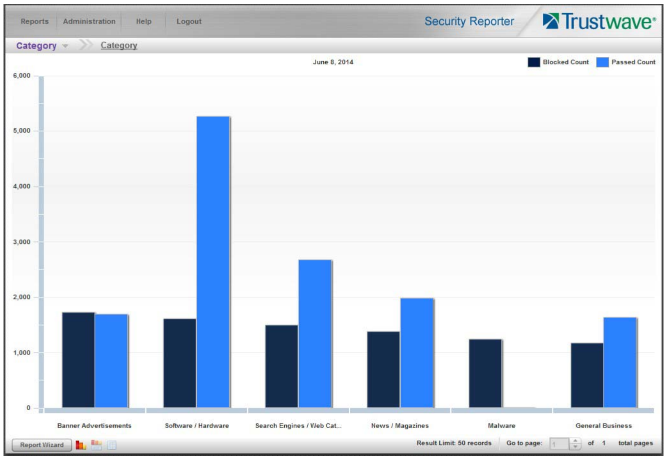
4.3.2.1.2 Summary Drill Down Report Wizard

Click **Report Wizard** to access the Report Wizard for the current report type (see Section 4.4.1).

4.3.2.1.3 Report view option icons

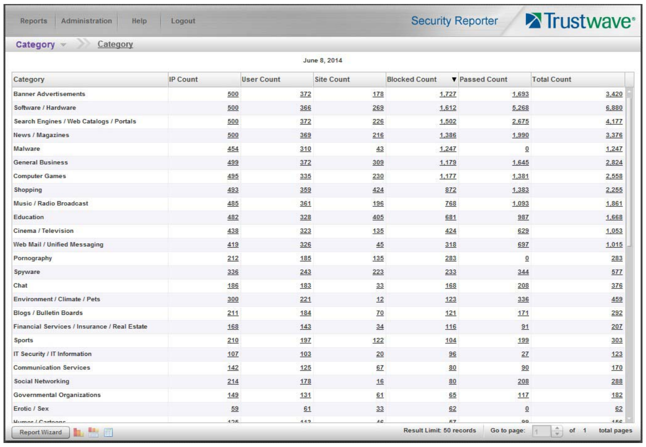
Click the following report view icon to change the report view display:

- Click this icon to display only the top six sets of bars:



- Click this icon to display the top six sets of bars and table of records.

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



June 8, 2014

Category	IP Count	User Count	Site Count	Blocked Count ▼	Passed Count	Total Count
Banner Advertisements	500	372	178	1,727	1,693	3,420
Software / Hardware	500	366	269	1,612	5,268	6,880
Search Engines / Web Catalogs / Portals	500	372	226	1,502	2,675	4,177
News / Magazines	500	369	216	1,386	1,990	3,376
Malware	454	310	43	1,247	0	1,247
General Business	499	372	309	1,179	1,645	2,824
Computer Games	495	335	230	1,177	1,381	2,558
Shopping	493	359	424	872	1,383	2,255
Music / Radio Broadcast	485	361	196	768	1,093	1,861
Education	482	328	405	681	987	1,668
Cinema / Television	438	323	135	424	629	1,053
Web Mail / Unified Messaging	419	326	45	318	697	1,015
Pornography	212	185	135	283	0	283
Spyware	336	243	223	233	344	577
Chat	186	183	33	168	208	376
Environment / Climate / Pets	300	221	12	123	336	459
Blogs / Bulletin Boards	211	184	70	121	171	292
Financial Services / Insurance / Real Estate	168	143	34	116	91	207
Sports	210	197	122	104	199	303
IT Security / IT Information	107	103	20	96	27	123
Communication Services	142	125	67	80	90	170
Social Networking	214	178	16	80	208	288
Governmental Organizations	149	131	61	65	117	182
Erotic / Sex	59	61	33	62	0	62
Humor / Cartoons	126	113	46	57	99	156

Result Limit: 50 records of 1 total pages

4.3.2.1.4 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.

- **Channel name:** The column heading displays the channel name or type of report (such as Category or Virus). The data for each item is the item name recorded (such as a content category or virus name).

- **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, 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.

- **Blocked Count**: Displays the number of blocked pages and/or objects for each record in the table.

  By clicking 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.

Note: The number of blocked pages in a record is 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.

The number of blocked objects in a record is 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.

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

  By clicking 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.

  By clicking 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.

4.3.2.1.5 Bandwidth and Time Count columns

In a summary drill down report view, the Bandwidth and Time Count columns provide additional information about a record.

- **Bandwidth** (SWG only): This column displays the amount of bandwidth in GB or MB used for each record.

- **Time Count (h:mm:ss):** For the Category report type, this column 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.

4.3.2.1.6 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.

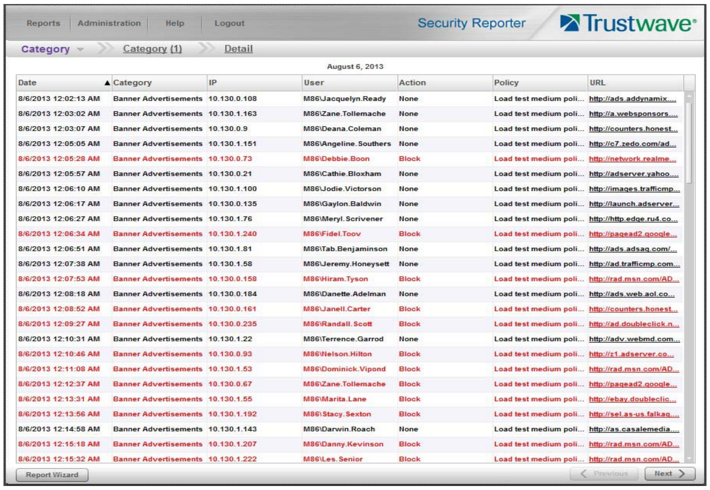
Click another column header to sort records by that specified column.

4.3.2.1.7 Other navigation tips

See Section 4.3.4 for information about navigating the current report view using breadcrumb trails and the **Go to page ‘x’ of ‘x’ total pages** field.

4.3.3 Detail Drill Down Report View

Detail drill down report views provide information on pages or objects accessed by end users within a specific time period. The report view is horizontally organized into a similar format as the summary drill down report view. The example below is a report on SWG activity:



August 6, 2013

Date	Category	IP	User	Action	Policy	URL
8/6/2013 12:02:13 AM	Banner Advertisements	10.130.0.108	M86\Jacquelyn.Ready	None	Load test medium poli...	http://ads.addynamix....
8/6/2013 12:03:02 AM	Banner Advertisements	10.130.1.163	M86\Zane.Tollemache	None	Load test medium poli...	http://a.websponsors....
8/6/2013 12:03:07 AM	Banner Advertisements	10.130.0.9	M86\Deana.Coleman	None	Load test medium poli...	http://counters.honest...
8/6/2013 12:05:05 AM	Banner Advertisements	10.130.1.151	M86\Angeline.Southers	None	Load test medium poli...	http://c7.zedo.com/ad...
8/6/2013 12:05:28 AM	Banner Advertisements	10.130.0.73	M86\Debbie.Boon	Block	Load test medium poli...	http://network.realme...
8/6/2013 12:05:57 AM	Banner Advertisements	10.130.0.21	M86\Cathie.Bloxham	None	Load test medium poli...	http://adserver.yahoo....
8/6/2013 12:06:10 AM	Banner Advertisements	10.130.1.100	M86\Jodie.Victorson	None	Load test medium poli...	http://images.trafficmp...
8/6/2013 12:06:17 AM	Banner Advertisements	10.130.0.135	M86\Gaylon.Baldwin	None	Load test medium poli...	http://launch.adserver...
8/6/2013 12:06:27 AM	Banner Advertisements	10.130.1.76	M86\Meryl.Scrivener	None	Load test medium poli...	http://http.edge.ru4.co...
8/6/2013 12:06:34 AM	Banner Advertisements	10.130.1.240	M86\Fidel.Toov	Block	Load test medium poli...	http://pagead2.google...
8/6/2013 12:06:51 AM	Banner Advertisements	10.130.1.81	M86\Tab.Benjaminson	None	Load test medium poli...	http://ads.adsaq.com/...
8/6/2013 12:07:38 AM	Banner Advertisements	10.130.1.58	M86\Jeremy.Honeysett	None	Load test medium poli...	http://ad.trafficmp.com...
8/6/2013 12:07:53 AM	Banner Advertisements	10.130.0.158	M86\Hiram.Tyson	Block	Load test medium poli...	http://rad.msn.com/AD...
8/6/2013 12:08:18 AM	Banner Advertisements	10.130.0.184	M86\Danette.Adelman	None	Load test medium poli...	http://ads.web.aol.co...
8/6/2013 12:08:52 AM	Banner Advertisements	10.130.0.161	M86\Janell.Carter	Block	Load test medium poli...	http://counters.honest...
8/6/2013 12:09:27 AM	Banner Advertisements	10.130.0.235	M86\Randall.Scott	Block	Load test medium poli...	http://ad.doubleclick.n...
8/6/2013 12:10:31 AM	Banner Advertisements	10.130.1.22	M86\Terrence.Garrod	None	Load test medium poli...	http://adv.webmd.com...
8/6/2013 12:10:46 AM	Banner Advertisements	10.130.0.93	M86\Nelson.Hilton	Block	Load test medium poli...	http://z1.adserver.co...
8/6/2013 12:11:08 AM	Banner Advertisements	10.130.1.53	M86\Dominick.Vipond	Block	Load test medium poli...	http://rad.msn.com/AD...
8/6/2013 12:12:37 AM	Banner Advertisements	10.130.0.67	M86\Zane.Tollemache	Block	Load test medium poli...	http://pagead2.google...
8/6/2013 12:13:31 AM	Banner Advertisements	10.130.1.55	M86\Marita.Lane	Block	Load test medium poli...	http://ebay.doubleclic...
8/6/2013 12:13:56 AM	Banner Advertisements	10.130.1.192	M86\Stacy.Sexton	Block	Load test medium poli...	http://sel.as-us.falkag....
8/6/2013 12:14:58 AM	Banner Advertisements	10.130.1.143	M86\Darwin.Roach	None	Load test medium poli...	http://as.casalemedia....
8/6/2013 12:15:18 AM	Banner Advertisements	10.130.1.207	M86\Danny.Kevinson	Block	Load test medium poli...	http://rad.msn.com/AD...
8/6/2013 12:15:32 AM	Banner Advertisements	10.130.1.222	M86\Les.Senior	Block	Load test medium poli...	http://rad.msn.com/AD...

As in the summary drill down report view, the top portion of the detail drill down report view includes the breadcrumb navigation section with menu for all report types. The date displays below.

4.3.3.1 Detail report columns

Detail reports include the following columns by default: Date, Channel or report type name, IP, User, Action, Policy, URL. A record displayed in red text indicates a blocked URL request. Other columns, including a Blocked column (True or False), are available for selection in the Report Wizard Grouping and Visibility tab.

- **Date**: Displays the date of the record using the M/D/YYYY HH:MM:SS AM/PM format.
- **Channel name:** The column heading displays the channel name or type of report (such as Category or Virus). The data for each item is the item name recorded (such as a content category or virus name).
- **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:** Displays the action (if any) taken by the logging device.

  If the data to be reported on comes from an SWG, many actions could be reported, including Block, Bypass Scanning, Allow content and scan containers, Unknown, None.

If the data to be reported on comes from a Web Filter, actions and additional details could be shown. The filtering method could be one of the following: Search KW (Search Keyword), URL KW (URL Keyword), URL, Wildcard (URL wildcard), Strict HTTPS, Moderate HTTPS, X-Strike, Pattern, File Type. The additional details would include the URL or keyword for the filtering method applied. For example: `Wildcard:HTTPS://*.google.com`

- **Policy** (SWG only): 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.

4.3.3.2 Detail Report View Tools and Tips

4.3.3.2.1 Column sorting tips

To sort detail 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.

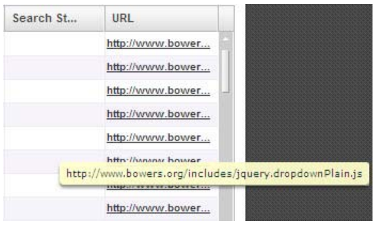
4.3.3.2.2 URL viewing tip

Click the URL for a specified record to view the page or object currently indexed in the SR's memory.

Caution: Visiting a URL can present a security risk if the content of the visited page is malicious. Use caution, particularly when viewing URLs that were blocked for security reasons.

4.3.3.2.3 Truncated data viewing tip

To view the entire text that displays truncated in a detail report view column, you can adjust the width of the columns by dragging the column separators. You can also hover over the column to view the entire string of data in the column for a given record:



Search St...	URL
	http://www.bower...
	http://www.bower...
	http://www.bower...
	http://www.bower...
	http://www.bower...
	http://www.bower...
	http://www.bower...
	http://www.bower...

http://www.bowers.org/includes/jquery.dropdownPlain.js

4.3.4 Report View Navigation and Usage

Understanding how to use report view tools is paramount to generating a report containing relevant content, since the usage of these tools determines the results of your query.

As you will learn from the rest of this section, report view tools along with report view components help you create the desired report view. This report view can then be exported, saved, and/or scheduled to run at a specified time.

4.3.4.1 Report view breadcrumb trail links

When generating a report view and modifying that report view to create another report view, a trail of breadcrumb links remain in the row beneath the navigation toolbar. Clicking a specified level in the trail link returns you to that prior report view.

4.3.4.2 Page navigation

If the report has multiple pages of content, you can step through pages using the controls at the bottom right of the panel.

- For summary reports, a **Go to page** control displays.
- For detail reports, **Previous** and **Next** buttons display.

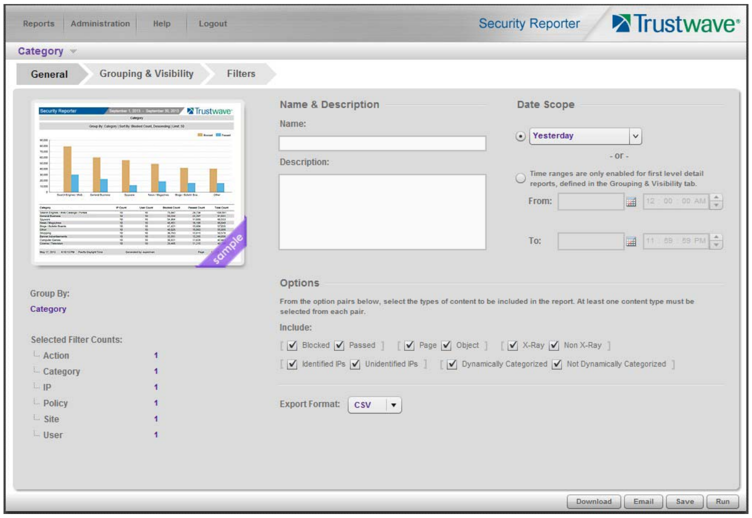
4.4 Customize and Maintain Reports

The following report topics from the Reports menu of the Report Manager are described in this section: Report Wizard, Saved Reports, and Report Schedule.

4.4.1 Report Wizard

The Report Wizard lets you generate a customized drill down report, querying the database for hits, pages, or objects viewed by end users.

In the navigation toolbar, hover over the Reports menu link and navigate to Drill Down | Report Wizard to display the Drill Down Report Wizard panel (the Category report type is selected by default):



Group By:
Category

Selected Filter Counts:
Action 1
Category 1
IP 1
Policy 1
Site 1
User 1

Name & Description
Name:
Description:

Date Scope
● Yesterday
- or -
○ Time ranges are only enabled for first level detail reports, defined in the Grouping & Visibility tab.
From: 12 : 00 : 00 AM
To: 11 : 59 : 59 PM

Options
From the option pairs below, select the types of content to be included in the report. At least one content type must be selected from each pair.
Include:
[☑ Blocked ☑ Passed] [☑ Page ☑ Object] [☑ X-Ray ☑ Non X-Ray]
[☑ Identified IPs ☑ Unidentified IPs] [☑ Dynamically Categorized ☑ Not Dynamically Categorized]

Export Format: CSV

4.4.1.1 Basic screen elements

As with the Drill Down report panels, the Report Wizard includes a drop-down menu in the breadcrumb navigation bar that opens when you hover over the report type name. This menu lets you choose from any of the other report types (Application Control, Category, Content Type, Rule, Spyware, Violation, Virus) and upon selecting a report type, the wizard for that report type displays.

Beneath the report type name are the following tabs:

- **General:** lets you specify the Date Scope, included content options, Export Format, and report Name & Description. Also summarizes grouping and filtering selections made in the other two tabs.
- **Grouping & Visibility:** lets you specify whether the report will be a summary or detail report, set one or more levels of grouping, choose how content will be grouped and sorted at each level, choose the number of records to return, and choose which columns will display.
- **Filters:** lets you limit the report to specific data, or data matching wildcards, for one or more filter types.

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

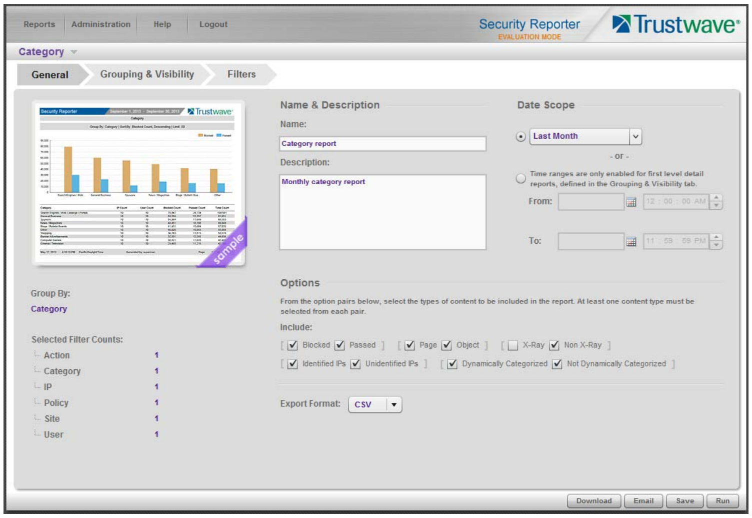
- **Back**: returns you to the report view from which you accessed the Report Wizard (this button does not display if the Report Wizard was accessed from the main menu)
- **Download**: generates and downloads the report in the Export Format specified in the General tab
- **Email**: opens the Email Report 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 report with a single level of grouping

4.4.1.2 Build the report

1. In the General tab:
    a. Enter a report **Name** and optional **Description** (this information is only used if the report is saved).
    b. Optionally limit the report by unchecking a selection from one or more pairs of **Options** if you do not wish to include that content in the report. You cannot uncheck both options of a pair. Options include:
        - Blocked/Passed: whether the request was blocked, or allowed
        - Page/Object: whether the request was for a page or another type of content
        - X-Ray/Non X-Ray (SWG only): whether the action was applied to the request, or is only shown as a “what-if” (X-Ray)
        - Identified IPs/Unidentified IPs: whether the source IP was identified with a specific username
        - Dynamically Categorized/Not Dynamically Categorized (SWG only): whether the result was categorized dynamically by TextCensor.
    c. Select an **Export Format** used for download or email. Available selections are CSV (default), PDF, HTML, or XLS.

Tip: CSV format minimizes the resources needed to generate the report. XLS is the least efficient format. For more details see Trustwave Knowledge Base article Q16151.

d. Specify the **Date Scope.** You can choose a pre-defined selection (Today, Yesterday, Current Week, Current Month, Current Year, Last Week, Last Weekend, Last Month), or enter a specific date range using the calendar pop-up boxes in the From and To fields. You can enter a specific time range if a single-level detail report is set in the Grouping & Visibility tab. The date scope will be set from the range you specified on the report from which you opened the wizard. For a new report the date scope is set to “Yesterday”.



Name & Description

Name: Category report

Description: Monthly category report

Date Scope

● Last Month

- or -

○ Time ranges are only enabled for first level detail reports, defined in the Grouping & Visibility tab.

From: 12 : 00 : 00 AM

To: 11 : 59 : 59 PM

Group By: Category

Selected Filter Counts:

Action	1
Category	1
IP	1
Policy	1
Site	1
User	1

Options

From the option pairs below, select the types of content to be included in the report. At least one content type must be selected from each pair.

Include:

[☑ Blocked ☑ Passed] [☑ Page ☑ Object] [□ X-Ray ☑ Non X-Ray]

[☑ Identified IPs ☑ Unidentified IPs] [☑ Dynamically Categorized ☑ Not Dynamically Categorized]

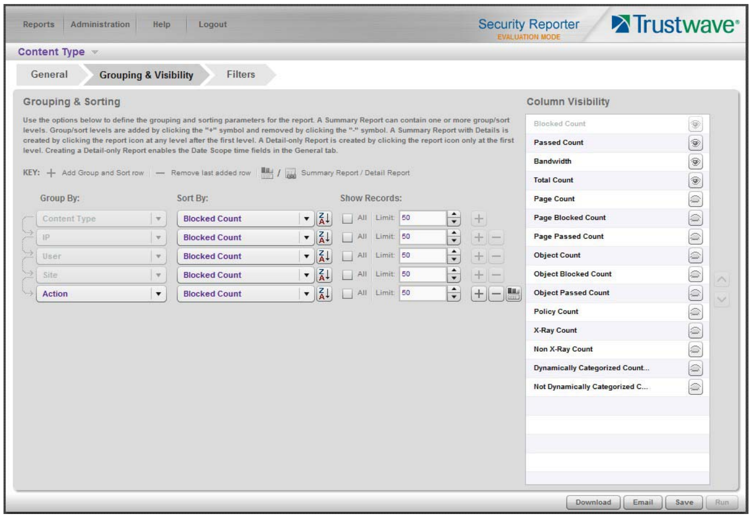
Export Format: CSV

2. In the Grouping & Visibility tab:

a. By default one grouping row displays. You can modify grouping and sorting by selecting another **Group By** and/or **Sort By** option. You can specify the **Show Records** quantity (All or Limit ‘X’ records).

Tip: Group By menu selections include Category Group and User Group, so you can report on customized category or user groups.

b. At the end of the first row, indicate whether this report will be a single level detail only report by clicking the report icon. Choose to create a multi-level report by clicking the ‘+’ icon.



Grouping & Sorting

Use the options below to define the grouping and sorting parameters for the report. A Summary Report can contain one or more group/sort levels. Group/sort levels are added by clicking the "+" symbol and removed by clicking the "-" symbol. A Summary Report with Details is created by clicking the report icon at any level after the first level. A Detail-only Report is created by clicking the report icon only at the first level. Creating a Detail-only Report enables the Date Scope time fields in the General tab.

KEY: + Add Group and Sort row — Remove last added row / Summary Report / Detail Report

Group By:	Sort By:	Show Records:	
Content Type	Blocked Count	□ All Limit: 50	+
IP	Blocked Count	□ All Limit: 50	+ —
User	Blocked Count	□ All Limit: 50	+ —
Site	Blocked Count	□ All Limit: 50	+ —
Action	Blocked Count	□ All Limit: 50	+ —

Column Visibility

- Blocked Count
- Passed Count
- Bandwidth
- Total Count
- Page Count
- Page Blocked Count
- Page Passed Count
- Object Count
- Object Blocked Count
- Object Passed Count
- Policy Count
- X-Ray Count
- Non X-Ray Count
- Dynamically Categorized Count...
- Not Dynamically Categorized C...

Grouping and Sorting icons:

- AZ↓ This icon indicates the report level will be sorted in ascending order. Click this icon to sort the report level in descending order.

- ZA↓ This icon indicates the report level will be sorted in descending order. Click this icon to sort the report level in ascending order.

- + Click this icon to add a group/sort level to the report.

- − Click this icon to remove the group/sort level from the report.

- ▦ Click this icon to make this report a detail report.

- ▤ Click this icon to make this report a summary report.

Note:

- You can create a summary only report, a summary report with detail, or a detail only report.
- The report icon at the end of the row toggles the report selection between a summary and a detail report.
- A summary report with detail is created by clicking the detail report icon after all report levels have been added.
- When you specify a detail report, the report icon toggles to the detail report icon, the Group By field in the current row displays “Detail” and becomes greyed-out, and the Column Visibility selections change to accommodate detail report columns. Detail columns generally present information about individual items. No additional rows can be added below a detail row.
- When you specify a summary report, the report icon toggles to the summary report icon, the Group By field in the current row displays the default selection, and the Column Visibility selections change to accommodate summary report columns. Summary columns generally present counts of items. Additional rows can be added.
- When you create a summary report with detail or a detail only report, the Search String option on the Filters tab is activated.
- When you create a detail only report, the time range fields in the Date Scope of the General tab are activated.

c. The Column Visibility list box shows all available column selections for the report. To modify the report output:

- Click the corresponding ‘eye’ icon to the right of a column name to make a column visible (open eye) or invisible (closed eye).

- Click a column name to highlight it and then click the up/down arrow, or drag the column name, to reposition the column. The order from top to bottom indicates order from left to right on the report.

Column Visibility icons:

- 👁 This icon indicates the column will be included in the report. Click this icon to exclude the column from the report.

- ◡ This icon indicates the column will not be included in the report. Click this icon to include the column in the report.

Note: No matter where the column name is positioned in this list, only columns with the ‘open eye’ icon will be included in the report output.

3. In the Filters tab:

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

a. By default, the filter type corresponding to the current report type is selected in the tab row at the top of the screen. Click any filter type tab to work with that filter type. You can filter on more than one type.

b. 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).

Note: The search is case sensitive.

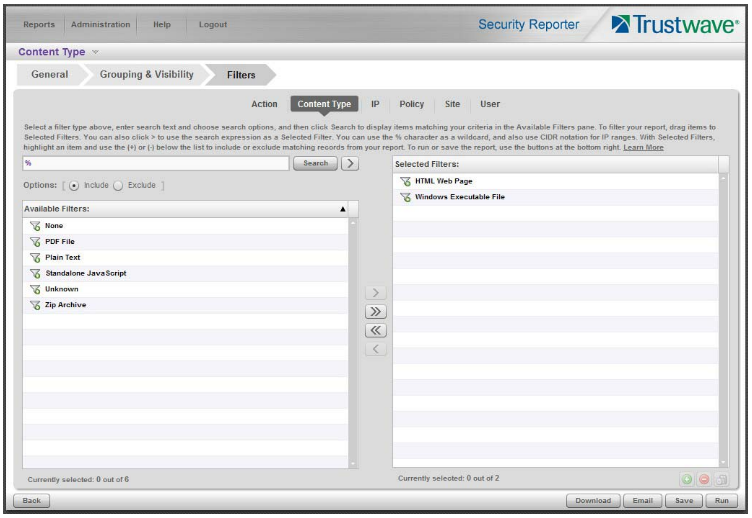
c. Choose search options using the radio buttons below the search field. The available options depend on the filter type. Include/Exclude is always available (used to indicate whether you want to find items that match, or do not match, the search terms). For details of other options see the Learn More link.

d. 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.

e. 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.



Select a filter type above, enter search text and choose search options, and then click Search to display items matching your criteria in the Available Filters pane. To filter your report, drag items to Selected Filters. You can also click > to use the search expression as a Selected Filter. You can use the % character as a wildcard, and also use CIDR notation for IP ranges. With Selected Filters, highlight an item and use the (+) or (-) below the list to include or exclude matching records from your report. To run or save the report, use the buttons at the bottom right. Learn More

%

Available Filters:
- None
- PDF File
- Plain Text
- Standalone JavaScript
- Unknown
- Zip Archive

Currently selected: 0 out of 6

Selected Filters:
- HTML Web Page
- Windows Executable File

Currently selected: 0 out of 2

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.

4. 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. If you remove all included filters from the group, +% (include all items) is added automatically. When you add an Included Selected Filter, +% is removed automatically.

5. Click a button to perform the specified action: Download, Email, Save, or Run. (Run is available only for a report with a single level of grouping.)

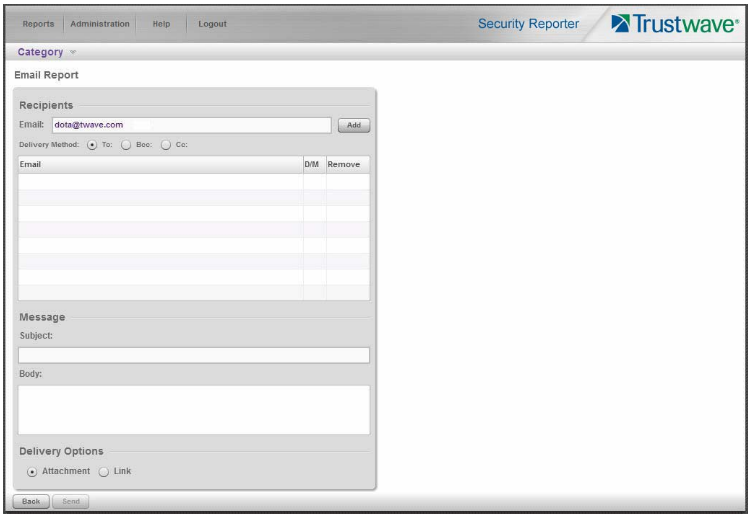
Note: Any Selected Filters items that include the wildcard character % will be evaluated for new matching data each time the report is run. This function is useful for reports on use names, malware names, or any data set that could include new members.

4.4.1.2.1 Download the report

Click **Download** to begin the process of exporting the report in the format specified by the Export Format field on the General tab. When the report is finished being processed, it will be downloaded to your workstation. The exported report can be printed and/or saved using the tools in the downloaded report file.

4.4.1.2.2 Email the report

1. Click **Email** to open the Email Report panel, used for entering email criteria to send the report to the designated recipient(s):



Email: dota@twave.com

Delivery Method: ● To: ○ Bcc: ○ Cc:

● Attachment ○ Link

2. In the Recipients section, the Email address for the user logged into the SR displays by default, and the Delivery Method “To” is selected.
   a. At your option, select a different **Delivery Method** (Bcc, Cc).
   b. If desired, enter a different **Email** address.
   c. Click **Add** to include the email address with the specified delivery method in the list box below.

Tip: Click ✖ to remove the email address.

3. In the Message section:
   a. Enter **Subject** information.
   b. At your option, enter text in the **Body** area box.
4. By default, the Delivery Options section specifies an “Attachment” to the email message. If desired, select “Link” to include only a hyperlink to the report.
5. Click **Send** to initiate the process for generating the report and return to the previous screen, or click **Back** to return to the previous screen. The report will be emailed—in the Export Format specified in the General tab of the Report Wizard—after it has been generated.

4.4.1.2.3 Save the report

After entering all report criteria, including the report Name in the General tab, click **Save** to save the current report to the Saved Reports panel. The saved report is accessible via Reports | Saved and can be edited or deleted at any time.

4.4.1.2.4 Run the report

In a single level report, the option is available to click **Run** to display a Drill Down report view based on your current settings. This report view can be modified by clicking **Report Wizard** and making edits to the settings previously made.

If the report has multiple pages of content, you can step through pages using the controls at the bottom right of the panel.

- For summary reports, a **Go to page** control displays.
- For detail reports, **Previous** and **Next** buttons display.

4.4.1.3 Exported Report Samples

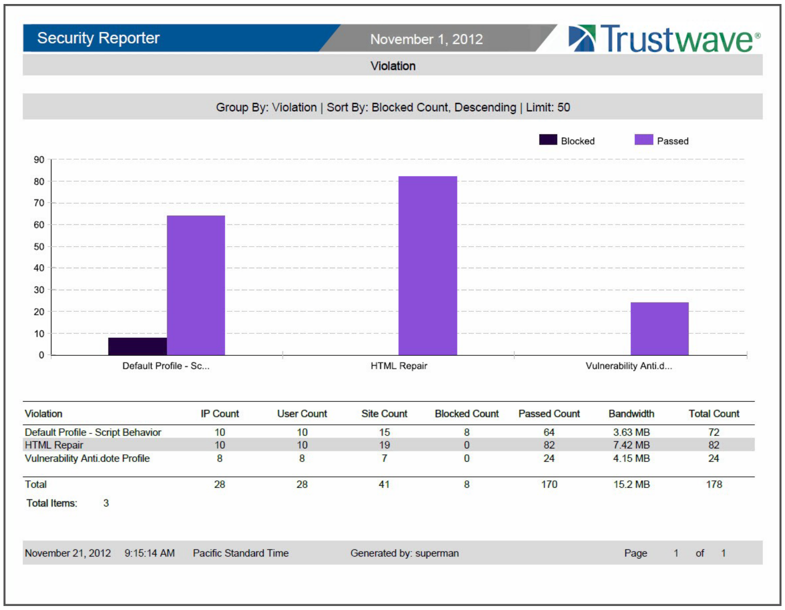
The SR can generate hundreds of different types of reports based on the different criteria specified, in the CSV, PDF, HTML, and XLS formats. The following are some typical types of reports generated and exported in the PDF format.

Tip: CSV is the default format because this format minimizes the resources needed to generate the report. PDF has higher presentation quality but consumes additional resources. XLS is the least efficient format. For more details see Trustwave Knowledge Base article Q16151.

4.4.1.3.1 Single level summary report

The single level summary drill down report includes the following information:

- Header: The product name and date; report type name; Group By, Sort By and sort order, and record Limit
- Chart section: Top six sets of bar charts with a color-coded key
- Records section: Column headers, rows of records, Total amounts for each column, and Total Items (records)
- Footer: Date and time, and time zone; Generated by username (if specified for inclusion in the report); Page number and page range



Security Reporter November 1, 2012 Trustwave

Violation

Group By: Violation | Sort By: Blocked Count, Descending | Limit: 50

Violation	IP Count	User Count	Site Count	Blocked Count	Passed Count	Bandwidth	Total Count
Default Profile - Script Behavior	10	10	15	8	64	3.63 MB	72
HTML Repair	10	10	19	0	82	7.42 MB	82
Vulnerability Anti.dote Profile	8	8	7	0	24	4.15 MB	24
Total	28	28	41	8	170	15.2 MB	178

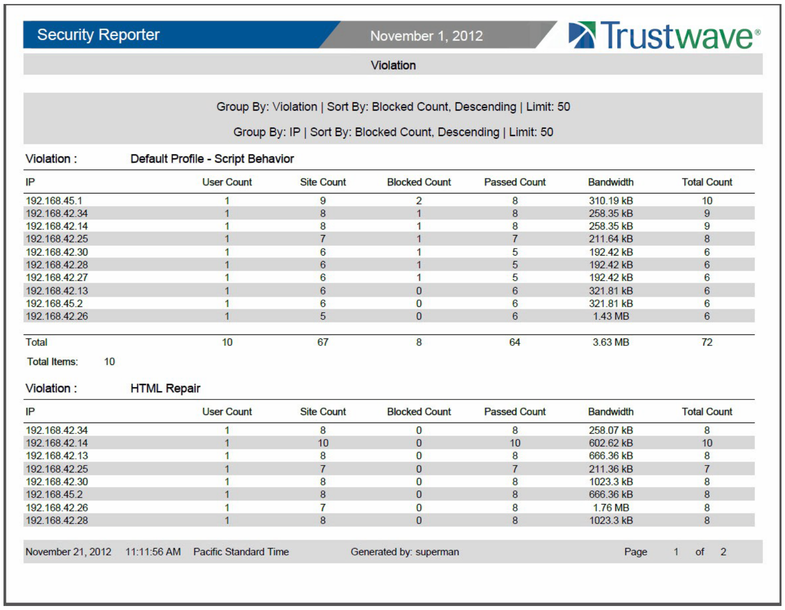
Total Items: 3

November 21, 2012 9:15:14 AM Pacific Standard Time Generated by: superman Page 1 of 1

4.4.1.3.2 Multiple-level summary report

A multiple-level summary drill down report includes the following information:

- Header: The product name and date; report type name; Group By, Sort By and sort order, and record Limit for each report level
- Records section: Group By information for each report level, column headers, rows of records, Total amounts for each column, and Total Items (records)
- Footer: Date and time, and time zone; Generated by username (if specified for inclusion in the report); Page number and page range



Security Reporter November 1, 2012 Trustwave

Violation

Group By: Violation | Sort By: Blocked Count, Descending | Limit: 50

Group By: IP | Sort By: Blocked Count, Descending | Limit: 50

Violation : Default Profile - Script Behavior

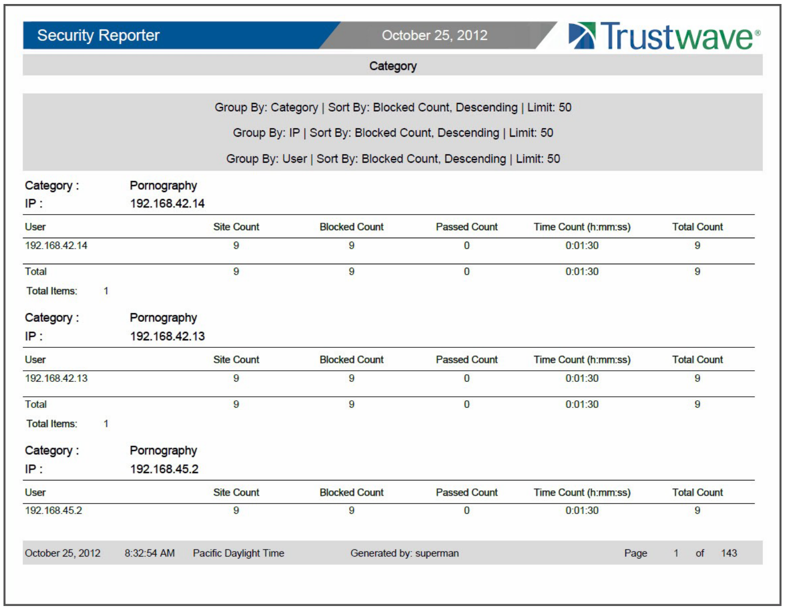
IP	User Count	Site Count	Blocked Count	Passed Count	Bandwidth	Total Count
192.168.45.1	1	9	2	8	310.19 kB	10
192.168.42.34	1	8	1	8	258.35 kB	9
192.168.42.14	1	8	1	8	258.35 kB	9
192.168.42.25	1	7	1	7	211.64 kB	8
192.168.42.30	1	6	1	5	192.42 kB	6
192.168.42.28	1	6	1	5	192.42 kB	6
192.168.42.27	1	6	1	5	192.42 kB	6
192.168.42.13	1	6	0	6	321.81 kB	6
192.168.45.2	1	6	0	6	321.81 kB	6
192.168.42.26	1	5	0	6	1.43 MB	6
Total	10	67	8	64	3.63 MB	72

Total Items: 10

Violation : HTML Repair

IP	User Count	Site Count	Blocked Count	Passed Count	Bandwidth	Total Count
192.168.42.34	1	8	0	8	258.07 kB	8
192.168.42.14	1	10	0	10	602.62 kB	10
192.168.42.13	1	8	0	8	666.36 kB	8
192.168.42.25	1	7	0	7	211.36 kB	7
192.168.42.30	1	8	0	8	1023.3 kB	8
192.168.45.2	1	8	0	8	666.36 kB	8
192.168.42.26	1	7	0	8	1.76 MB	8
192.168.42.28	1	8	0	8	1023.3 kB	8

November 21, 2012 11:11:56 AM Pacific Standard Time Generated by: superman Page 1 of 2



Security Reporter October 25, 2012 Trustwave®

Category

Group By: Category | Sort By: Blocked Count, Descending | Limit: 50

Group By: IP | Sort By: Blocked Count, Descending | Limit: 50

Group By: User | Sort By: Blocked Count, Descending | Limit: 50

Category : Pornography
IP : 192.168.42.14

User	Site Count	Blocked Count	Passed Count	Time Count (h:mm:ss)	Total Count
192.168.42.14	9	9	0	0:01:30	9
Total	9	9	0	0:01:30	9

Total Items: 1

Category : Pornography
IP : 192.168.42.13

User	Site Count	Blocked Count	Passed Count	Time Count (h:mm:ss)	Total Count
192.168.42.13	9	9	0	0:01:30	9
Total	9	9	0	0:01:30	9

Total Items: 1

Category : Pornography
IP : 192.168.45.2

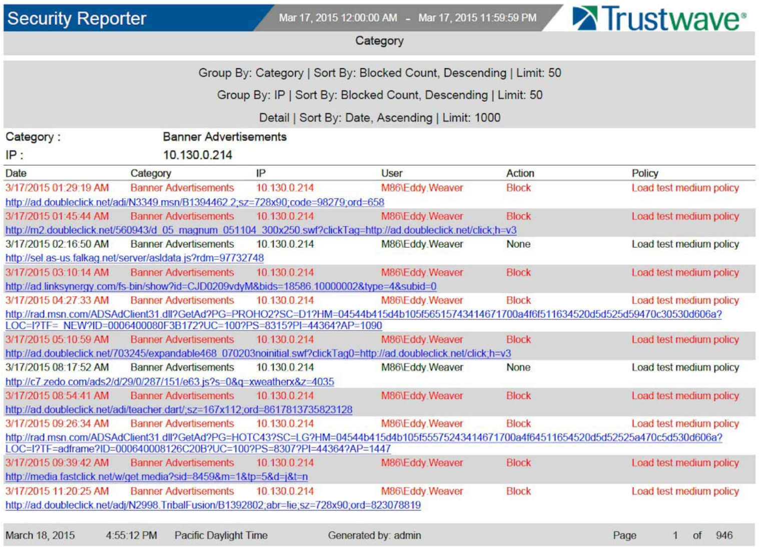
User	Site Count	Blocked Count	Passed Count	Time Count (h:mm:ss)	Total Count
192.168.45.2	9	9	0	0:01:30	9

October 25, 2012 8:32:54 AM Pacific Daylight Time Generated by: superman Page 1 of 143

4.4.1.3.3 Summary report with detail

A summary drill down report with detail includes the following information:

- Header: The product name and date; report type name; Group By, Sort By and sort order, and record Limit for each summary report level; Detail report, Sort By and sort order, and record Limit for each report level
- Records section: Group By information for each report level, column headers, rows of records with the associated URL for each record, and Total Items (records) in each group. Blocked request records display in red text.
- Footer: Date and time, and time zone; Generated by username (if specified for inclusion in the report); Page number and page range



Security Reporter Mar 17, 2015 12:00:00 AM - Mar 17, 2015 11:59:59 PM Trustwave®

Category

Group By: Category | Sort By: Blocked Count, Descending | Limit: 50

Group By: IP | Sort By: Blocked Count, Descending | Limit: 50

Detail | Sort By: Date, Ascending | Limit: 1000

Category : Banner Advertisements

IP : 10.130.0.214

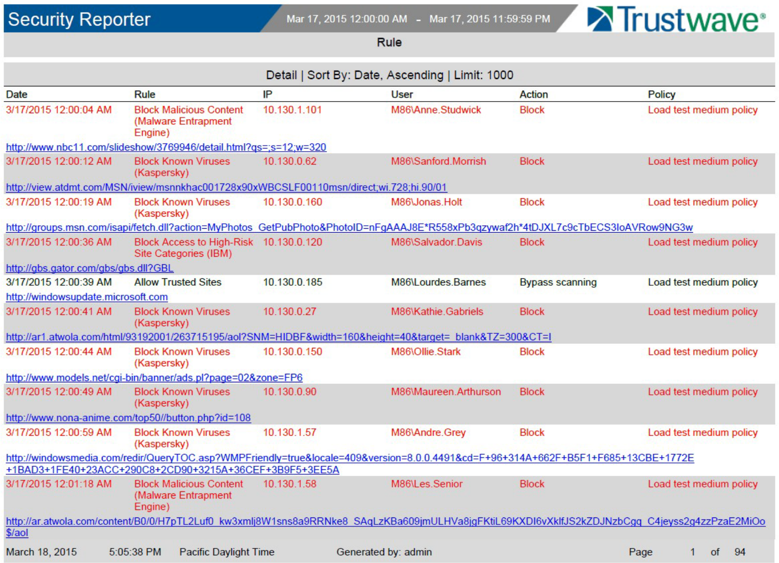
Date	Category	IP	User	Action	Policy
3/17/2015 01:29:19 AM	Banner Advertisements	10.130.0.214	M86\Eddy.Weaver	Block	Load test medium policy
http://ad.doubleclick.net/adi/N3349.msn/B1394462.2;sz=728x90;code=98279;ord=658					
3/17/2015 01:45:44 AM	Banner Advertisements	10.130.0.214	M86\Eddy.Weaver	Block	Load test medium policy
http://m2.doubleclick.net/560943/d_05_magnum_051104_300x250.swf?clickTag=http://ad.doubleclick.net/click;h=v3					
3/17/2015 02:16:50 AM	Banner Advertisements	10.130.0.214	M86\Eddy.Weaver	None	Load test medium policy
http://sel.as-us.falkag.net/server/asldata.js?rdm=97732748					
3/17/2015 03:10:14 AM	Banner Advertisements	10.130.0.214	M86\Eddy.Weaver	Block	Load test medium policy
http://ad.linksynergy.com/fs-bin/show?id=CJD0209vdyM&bids=18586.10000002&type=4&subid=0					
3/17/2015 04:27:33 AM	Banner Advertisements	10.130.0.214	M86\Eddy.Weaver	Block	Load test medium policy
http://rad.msn.com/ADSAdClient31.dll?GetAd?PG=PROHO2?SC=D1?HM=04544b415d4b105f56515743414671700a4f6f511634520d5d525d59470c30530d606a?LOC=I?TF=_NEW?ID=0006400080F3B172?UC=100?PS=8315?PI=44364?AP=1090					
3/17/2015 05:10:59 AM	Banner Advertisements	10.130.0.214	M86\Eddy.Weaver	Block	Load test medium policy
http://ad.doubleclick.net/703245/expandable468_070203noinitial.swf?clickTag0=http://ad.doubleclick.net/click;h=v3					
3/17/2015 08:17:52 AM	Banner Advertisements	10.130.0.214	M86\Eddy.Weaver	None	Load test medium policy
http://c7.zedo.com/ads2/d/29/0/287/151/e63.js?s=0&q=xweatherx&z=4035					
3/17/2015 08:54:41 AM	Banner Advertisements	10.130.0.214	M86\Eddy.Weaver	Block	Load test medium policy
http://ad.doubleclick.net/adi/teacher.dart/;sz=167x112;ord=8617813735823128					
3/17/2015 09:26:34 AM	Banner Advertisements	10.130.0.214	M86\Eddy.Weaver	Block	Load test medium policy
http://rad.msn.com/ADSAdClient31.dll?GetAd?PG=HOTC43?SC=LG?HM=04544b415d4b105f55575243414671700a4f64511654520d5d52525a470c5d530d606a?LOC=I?TF=adframe?ID=000640008126C20B?UC=100?PS=8307?PI=44364?AP=1447					
3/17/2015 09:39:42 AM	Banner Advertisements	10.130.0.214	M86\Eddy.Weaver	Block	Load test medium policy
http://media.fastclick.net/w/get.media?sid=8459&m=1&tp=5&d=j&t=n					
3/17/2015 11:20:25 AM	Banner Advertisements	10.130.0.214	M86\Eddy.Weaver	Block	Load test medium policy
http://ad.doubleclick.net/adj/N2998.TribalFusion/B1392802;abr=!ie;sz=728x90;ord=823078819					

March 18, 2015 4:55:12 PM Pacific Daylight Time Generated by: admin Page 1 of 946

4.4.1.3.4 Single level detail report

The single level detail drill down report includes the following information:

- Header: The product name and date; report type name; Detail report, Sort By and sort order, and record Limit
- Records section: Column headers, rows of records with associated URL for each record, and Total Items (records). Blocked request records display in red text.
- Footer: Date and time, and time zone; Generated by username (if specified for inclusion in the report); Page number and page range



Security Reporter Mar 17, 2015 12:00:00 AM - Mar 17, 2015 11:59:59 PM Trustwave®

Rule

Detail | Sort By: Date, Ascending | Limit: 1000

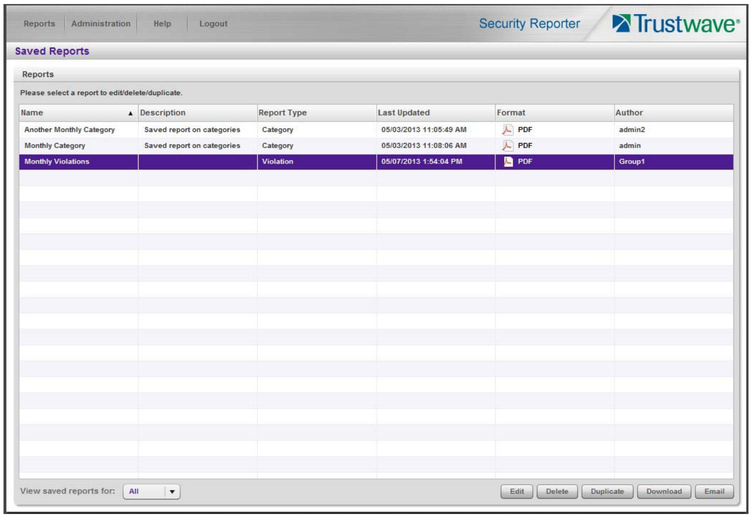
Date	Rule	IP	User	Action	Policy
3/17/2015 12:00:04 AM	Block Malicious Content (Malware Entrapment Engine)	10.130.1.101	M86\Anne.Studwick	Block	Load test medium policy
http://www.nbc11.com/slideshow/3769946/detail.html?qs=;s=12;w=320					
3/17/2015 12:00:12 AM	Block Known Viruses (Kaspersky)	10.130.0.62	M86\Sanford.Morrish	Block	Load test medium policy
http://view.atdmt.com/MSN/iview/msnnkhac001728x90xWBCSLF00110msn/direct;wi.728;hi.90/01					
3/17/2015 12:00:19 AM	Block Known Viruses (Kaspersky)	10.130.0.160	M86\Jonas.Holt	Block	Load test medium policy
http://groups.msn.com/isapi/fetch.dll?action=MyPhotos_GetPubPhoto&PhotoID=nFgAAAJ8E*R558xPb3qzywaf2h*4tDJXL7c9cTbECS3IoAVRow9NG3w					
3/17/2015 12:00:36 AM	Block Access to High-Risk Site Categories (IBM)	10.130.0.120	M86\Salvador.Davis	Block	Load test medium policy
http://gbs.gator.com/gbs/gbs.dll?GBL					
3/17/2015 12:00:39 AM	Allow Trusted Sites	10.130.0.185	M86\Lourdes.Barnes	Bypass scanning	Load test medium policy
http://windowsupdate.microsoft.com					
3/17/2015 12:00:41 AM	Block Known Viruses (Kaspersky)	10.130.0.27	M86\Kathie.Gabriels	Block	Load test medium policy
http://ar1.atwola.com/html/93192001/263715195/aol?SNM=HIDBF&width=160&height=40&target=_blank&TZ=300&CT=I					
3/17/2015 12:00:44 AM	Block Known Viruses (Kaspersky)	10.130.0.150	M86\Ollie.Stark	Block	Load test medium policy
http://www.models.net/cgi-bin/banner/ads.pl?page=02&zone=FP6					
3/17/2015 12:00:49 AM	Block Known Viruses (Kaspersky)	10.130.0.90	M86\Maureen.Arthurson	Block	Load test medium policy
http://www.nona-anime.com/top50//button.php?id=108					
3/17/2015 12:00:59 AM	Block Known Viruses (Kaspersky)	10.130.1.57	M86\Andre.Grey	Block	Load test medium policy
http://windowsmedia.com/redir/QueryTOC.asp?WMPFriendly=true&locale=409&version=8.0.0.4491&cd=F+96+314A+662F+B5F1+F685+13CBE+1772E+1BAD3+1FE40+23ACC+290C8+2CD90+3215A+36CEF+3B9F5+3EE5A					
3/17/2015 12:01:18 AM	Block Malicious Content (Malware Entrapment Engine)	10.130.1.58	M86\Les.Senior	Block	Load test medium policy
http://ar.atwola.com/content/B0/0/H7pTL2Luf0_kw3xmlj8W1sns8a9RRNke8_SAqLzKBa609jmULHVa8jgFKtiL69KXDI6vXklfJS2kZDJNzbCgq_C4jeyss2g4zzPzaE2MiOo$/aol					

March 18, 2015 5:05:38 PM Pacific Daylight Time Generated by: admin Page 1 of 94

4.4.2 Use Saved Drill Down Reports

The Saved Reports option lets you view, edit, or copy data in a report, or download, email or delete a report.

Navigate to Reports | Saved to display the Saved Reports panel:



Please select a report to edit/delete/duplicate.

Name ▲	Description	Report Type	Last Updated	Format	Author
Another Monthly Category	Saved report on categories	Category	05/03/2013 11:05:49 AM	PDF	admin2
Monthly Category	Saved report on categories	Category	05/03/2013 11:08:06 AM	PDF	admin
Monthly Violations		Violation	05/07/2013 1:54:04 PM	PDF	Group1

View saved reports for: All

For Group Administrators, this panel displays any reports created by the logged on administrator.

For Global Administrators, by default this panel displays reports created by the logged on administrator. A Global Administrator can also view and work with reports created by other administrators.

Note: When a Global Administrator edits a report created by a Group Administrator, the available groups include ONLY the groups available to the original creator. When a report is saved, the Author does not change.

- To list reports created by others, use the menu at the bottom left of the screen. Choose a specific user name, or choose “All” to view all saved reports.

Note: This menu only displays for Global Administrators.

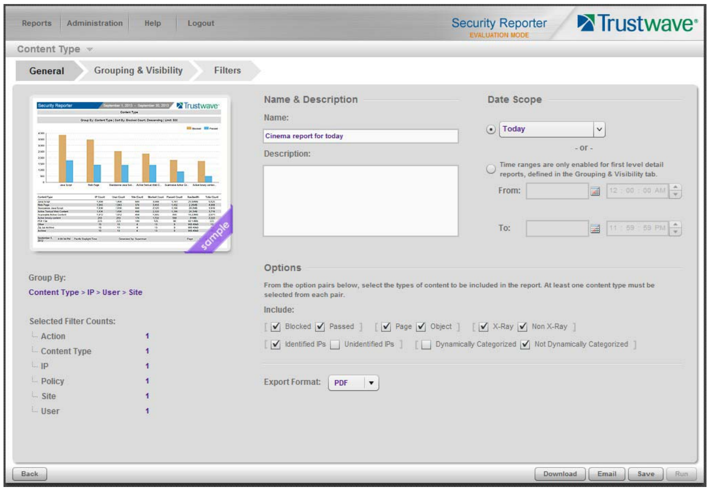
For each report record listed in the table, the following information displays: report Name, Description (if entered and saved for the report), Report Type (Application Control, Category, Content Type, Rule, Spyware, Violation, Virus), Last Updated, Format (such as PDF, HTML, XLS, CSV), and Author.

To perform any action in this panel, select the report name from the list to activate the buttons at the bottom right corner: Edit, Delete, Duplicate, Download, and Email.

Tip: On the Report Wizard panel discussed in this sub-section, click **Back** to return to the Saved Reports panel without saving your edits or performing any other action.

4.4.2.1 Edit a Saved Drill Down Report

1. With the drill down report name selected in the Saved Reports table, click **Edit** to display the Report Wizard panel, populated with settings from the saved report:



Name & Description

Name: Cinema report for today

Description:

Date Scope

● Today

- or -

○ Time ranges are only enabled for first level detail reports, defined in the Grouping & Visibility tab.

From: 12 : 00 : 00 AM

To: 11 : 59 : 59 PM

Group By:
Content Type > IP > User > Site

Selected Filter Counts:

Action	1
Content Type	1
IP	1
Policy	1
Site	1
User	1

Options

From the option pairs below, select the types of content to be included in the report. At least one content type must be selected from each pair.

Include:

[☑ Blocked ☑ Passed] [☑ Page ☑ Object] [☑ X-Ray ☑ Non X-Ray]

[☑ Identified IPs □ Unidentified IPs] [□ Dynamically Categorized ☑ Not Dynamically Categorized]

Export Format: PDF

Note: Refer to the Report Wizard sub-section for more information on making entries in the fields in this panel.

2. After making your edits in the tabs in the Report Wizard, click **Save**.

4.4.2.2 Copy a Saved Drill Down Report

The copy feature is a great time saver, letting you work with pre-populated settings from a saved drill down report.

1. With the report name selected in the Saved Reports table, click **Duplicate** to display the Report Wizard panel, populated with settings from the saved report.

Note: The Name field displays the text “Copy of ‘X’”, in which ‘X’ represents the report name of the report being copied. Edit this text if you wish to modify this report name.

2. After making your selections and entries in the panel, click **Save** to receive a confirmation specifying the report was saved.

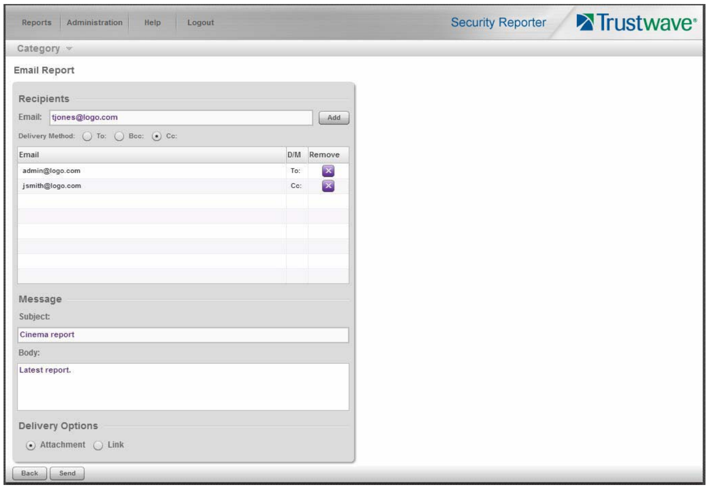
Tip: When a Global Administrator copies and edits a report that was created by another user, all groups are available. When a duplicated report is first saved, the author of the copy is set to the administrator performing this action.

4.4.2.3 Download a Saved Drill Down Report

With the report name selected in the Saved Reports table, click **Download** to obtain an on demand copy of the latest report in the Export Format (PDF, HTML, XLS, CSV) specified in the General tab of the Report Wizard.

4.4.2.4 Email a Drill Down Report

1. With the report name selected in the Saved Reports table, click **Email** to display the Email Report panel of the Report Wizard:



Email Report

Recipients

Email: tjones@logo.com Add

Delivery Method: ○ To: ○ Bcc: ● Cc:

Email	D/M	Remove
admin@logo.com	To:	☒
jsmith@logo.com	Cc:	☒

Message

Subject: Cinema report

Body: Latest report.

Delivery Options

● Attachment ○ Link

Note: Refer to the Report Wizard: Email the report sub-section for more information on making entries in the fields in this panel.

2. Specify criteria for emailing the report, and then click **Send** to email the report to the designated email address(es) after the report has been generated.

4.4.2.5 Delete a Drill Down Report

To remove the report from Saved Reports—and Report Schedule, if applicable—table(s):

1. With the report name selected in the Reports table, click **Delete** to open the Confirmation dialog box with a message asking if you wish to delete the report, and notifying you that in doing so any associated event schedule will also be deleted.

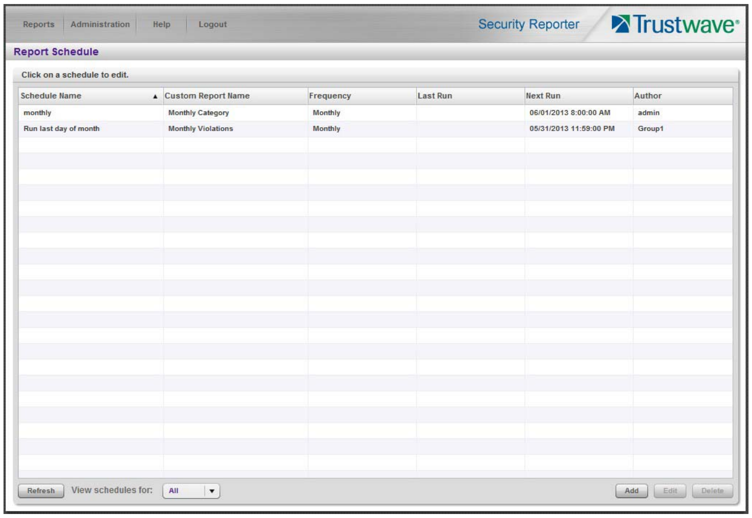
2. Click **Yes** to close the dialog box and delete the report.

Note: If a report is scheduled to run via the Report Schedule option, deleting the report removes it from the Report Schedule list. See Manage Drill Down Report Scheduling for more information about scheduled reports.

4.4.3 Manage Drill Down Report Scheduling

The Report Schedule option is used for maintaining a schedule for generating and distributing a customized report.

Navigate to Reports | Report Schedule to display the Report Schedule panel:



Schedule Name	Custom Report Name	Frequency	Last Run	Next Run	Author
monthly	Monthly Category	Monthly		06/01/2013 8:00:00 AM	admin
Run last day of month	Monthly Violations	Monthly		05/31/2013 11:59:00 PM	Group1

For Group Administrators, this panel displays any schedules created by the logged on administrator.

For Global Administrators, by default this panel displays reports created by the logged on administrator. A Global Administrator can also view and work with reports saved by other administrators.

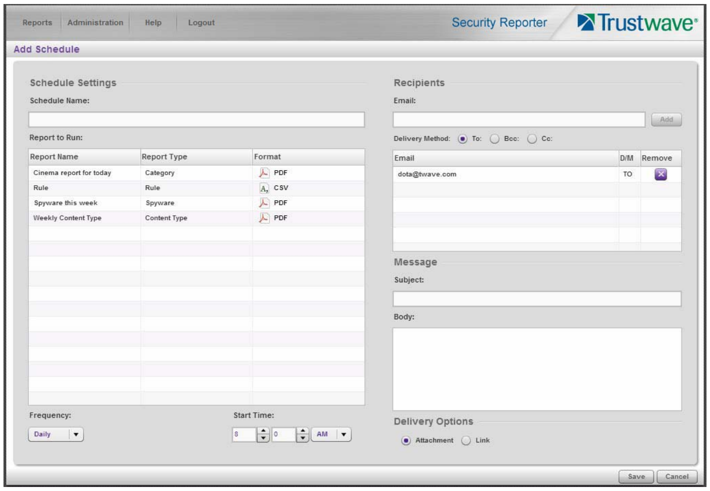
Tip: To list schedules created by others, use the menu at the bottom left of the screen. Choose a specific user name, or choose “All” to view all saved schedules.

This panel is comprised of a table of report schedule records with buttons at the bottom. The following columns of information display for each record: Schedule Name, Custom Report Name, Frequency for running the report, dates and times of the Last Run and Next Run (MM/DD/YYYY H:MM:SS AM/PM time format), and Author.

Click the **Refresh** button to refresh the list of records, which de-selects any selected record.

4.4.3.1 Add a Drill Down Report Schedule

1. In the Report Schedule panel, click **Add** to display the Add Schedule panel:



Report Name	Report Type	Format
Cinema report for today	Category	PDF
Rule	Rule	CSV
Spyware this week	Spyware	PDF
Weekly Content Type	Content Type	PDF

Email	D/M	Remove
dota@twave.com	TO	☒

2. Enter a **Schedule Name** for the report schedule.
3. Select the **Report to Run** from the list.
4. Select the **Frequency** from the pull-down menu (“Daily”, “Weekly”, “Monthly”, or “Once”) for running the report.

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

   If Weekly, specify the **Day of the Week** from the pull-down menu (Sunday - Saturday), and the **Start Time** (1 - 12 for the hour, 0 - 59 for the minutes, and AM or PM).

   If Monthly, specify the date by either choosing the day of the month from the pull-down menu (1 - 31), or clicking the **Last Day** check box.

   If Once:

   a. Specify the date by either accepting today’s date, or clicking the calendar icon to choose the date from the calendar pop-up box to populate the field.

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

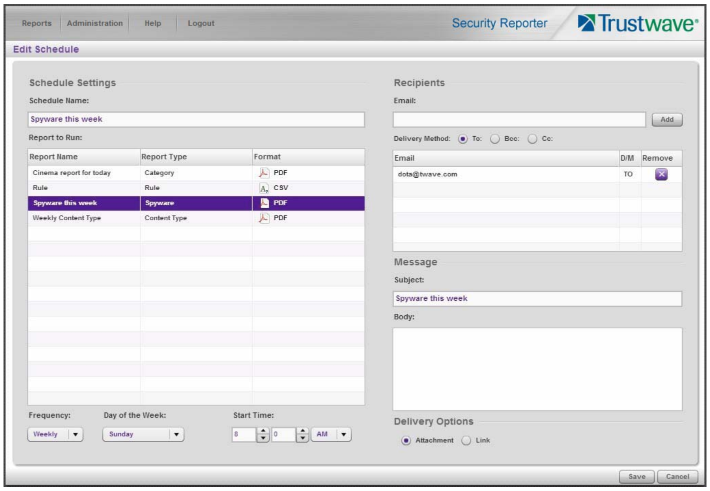
Note: The default Start Time is 8:00 AM. If you wish to run a report today and this time has already passed, be sure to select a future time.

Tip: Click **Cancel** to return to the Report Schedule panel without saving your edits.

5. Click **Save** to add the scheduled event to the Report Schedule.

4.4.3.2 Edit a Drill Down Report Schedule

1. To edit criteria for a report schedule, select the record from the list, and then click **Edit** to display the Edit Schedule panel:



Edit Schedule

Schedule Settings

Schedule Name: Spyware this week

Report to Run:

Report Name	Report Type	Format
Cinema report for today	Category	PDF
Rule	Rule	CSV
Spyware this week	Spyware	PDF
Weekly Content Type	Content Type	PDF

Frequency: Weekly

Day of the Week: Sunday

Start Time: 8 0 AM

Recipients

Email:

Delivery Method: ● To: ○ Bcc: ○ Cc:

Email	D/M	Remove
dota@twave.com	TO	☒

Message

Subject: Spyware this week

Body:

Delivery Options

● Attachment ○ Link

This panel includes the Schedule Settings section to the left (Schedule Name field, selected schedule record highlighted in the Report to Run table, and Frequency and Start Time information for running the report), and email information sections to the right.

2. Edit any of the following criteria:
   - **Schedule Name**
   - **Frequency** (Daily, Weekly, Monthly, Once) for scheduling the report to run:
     - Daily: Choose the **Start Time** (hour, minute, AM/PM) for running the report
     - Weekly: Select the day of the week (Sunday - Saturday) and **Start Time** for running the report
     - Monthly: Choose the date (1 - 31), or click the **Last Day** check box
     - Once: The date field is populated with today's date (MM/DD/YYYY format) and includes the calendar icon which, when clicked, opens the calendar pop-up box used for choosing a different date. Also specify the **Start Time** for running the report.

Tip: Click **Cancel** if you wish to return to the Report Schedule panel without saving your edits.

3. Click **Save** to display the updated criteria in the Report Schedule panel.

Note: When a Global Administrator edits a schedule created by a Group Administrator, the Author does not change.

4.4.3.3 Delete a Drill Down Report Schedule

1. In the Report Schedule panel, select the report schedule record from the list and click the **Delete**; this action opens a dialog box with a message asking if you wish to delete the schedule for running that report.
2. Click **Yes** to close the dialog box and remove the scheduled event from the list.

Tip: Click **Cancel** to return to the Report Schedule panel without deleting the record from the list of reports scheduled to run.

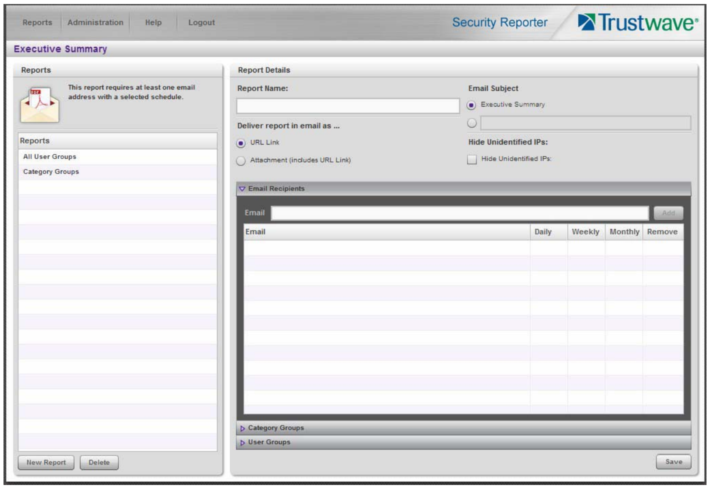
4.5 Specialized Reports

This section describes Executive Summary Reports, Blocked Request Reports, and Time Usage Reports.

4.5.1 Executive Summary

The Executive Summary option is used to set up daily, weekly, and/or monthly bar and line chart reports that will be delivered by email to users you specify, showing activity in library category groups or user groups of your choice.

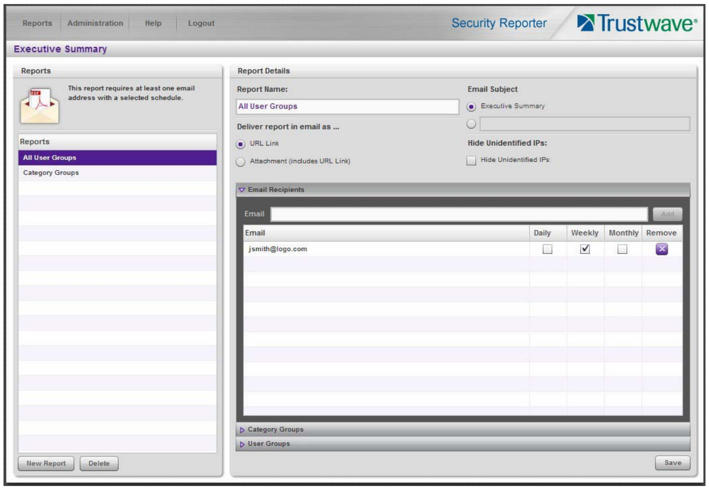
In the navigation toolbar, hover over the Reports menu link and select **Executive Summary** to display the Executive Summary panel:



This panel contains the Reports sub-panel listing saved report names, and the Report Details sub-panel used for configuring reports.

4.5.1.1 View, Edit Report Settings

1. In the Reports sub-panel, select the report name to display report setting criteria in the Report Details sub-panel.

   Report Name: All User Groups

   ● URL Link

   ○ Attachment (includes URL Link)

   ● Executive Summary

   □ Hide Unidentified IPs:

Email	Daily	Weekly	Monthly	Remove
jsmith@logo.com	□	☑	□	☒

   The following information displays and can be viewed and edited: Report Name, Email Subject criteria, Deliver report in email as... selection, Hide Unidentified IPs choice, Email Recipients list and report delivery schedule, and Category Groups and/or User Groups selection(s).

2. Click **Save** to update any modifications made to these report settings.

4.5.1.2 Add a New Report

1. At the bottom of the Reports sub-panel, click **New Report** to clear the panel.

2. At the top of the Report Details sub-panel, enter the **Report Name** to be used.

3. In the **Deliver report in email as...** section, by default the “URL Link” option is selected, indicating the email will only include a URL link to the report.

   To specify that both a URL link to the report and an attachment of the report will be included in the email, choose the “Attachment (includes URL Link)” option.

4. In the **Email Subject** section, by default the “Executive Summary” option is selected, indicating the subject line to be used in the email.

   To create a custom subject line for the email, select the radio button to the left of the blank field below, and make an entry in the text box for the subject line to be used in the email.

5. In the **Hide Unidentified IPs** section, by default the **Hide Unidentified IPs** check box is de-selected. This indicates that activity on machines not assigned to specific users will be included in reports.

   If you wish to exclude activity from machines not assigned to specific users, click in the check box to enter a check mark.

   Note: If you enable this feature, the generated report will only hide hit counts for IP addresses in sections of the report labeled “Users.” IP hit counts **will be included** for all other sections of the report, such as those labeled “Category”, etc.

6. In the Email Recipients accordion, specify the user(s) to receive the report and the frequency of delivery.

   a. Click in the empty field and type in the **Email** address.

   b. Click **Add** to clear the field and to add the email address in the list box below.

   c. By default, checkmarks populate the frequency check boxes: **Daily**, **Weekly**, **Monthly**. This indicates reports will be emailed to the recipient at the specified intervals. To change these settings, click the check box to remove the selection.

   Follow the steps above to add additional recipients.

   Tip: To remove a recipient from the list of users authorized to receive reports, click the ‘X’ in the **Remove** column.

7. Click to open the Category Groups and/or User Groups accordion(s) and specify groups for inclusion in the report:

   - In the Category Groups accordion, select the category group(s) from the Available Trustwave Category Groups and Custom Category Groups, and then click **Add Category Group** to move the selection(s) to the Selected list box.

     By default, the following categories are included in the Selected list box: Adult Content, Security, and Illegal/Questionable.

   Tip: Multiple category groups can be selected by clicking each category group while pressing the Ctrl key on your keyboard. Blocks of category groups can be selected by clicking the first category group, and then pressing the Shift key on your keyboard while clicking the last category group.

   To remove a category group from the Selected list box, select the category group and then click **Remove Category Group**.

- In the User Groups accordion, select the user group(s) from the Available User Groups, and then click **Add User Group** to move the selection(s) to the Selected list box.

Tip: Multiple user groups can be selected by clicking each user group while pressing the Ctrl key on your keyboard. Blocks of user groups can be selected by clicking the first user group, and then pressing the Shift key on your keyboard while clicking the last user group.

To remove a user group from the Selected list box, select the user group and then click **Remove User Group**.

8. Click **Save** to save all settings made in this panel and to include the new report in the Reports list box.

4.5.1.3 Sample Executive Summary report

The recipient of the Executive Summary report receives an email containing a link to the report, and a .pdf attachment of the report, if specified (if the size of the .pdf file is within the limits).

Links are available for the following time frame:

- Daily reports (14 days)
- Weekly reports (30 days)
- Monthly reports (90 days)

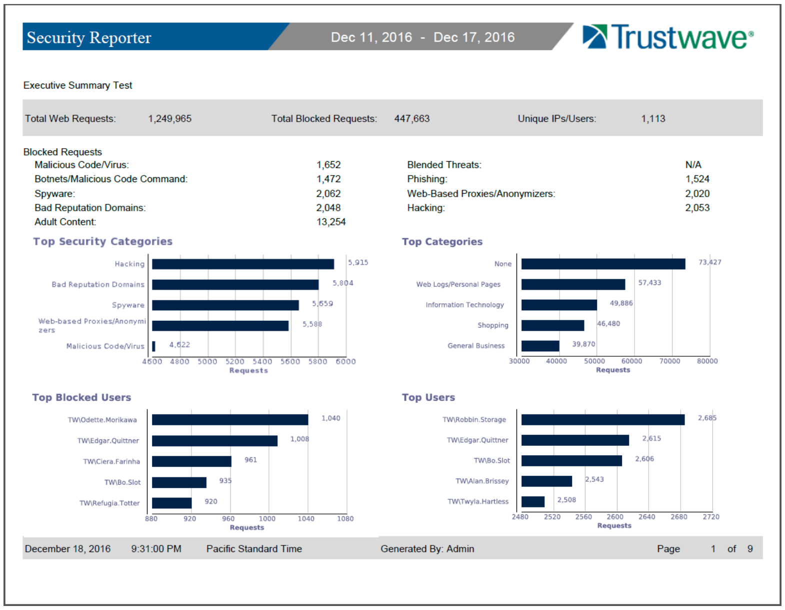
The header of the generated report includes the title and date range. The footer includes the page number and page range.

The first page includes statistics for the following: Total Web Requests, Total Blocked Requests, Unique IPs/Users.

Total Blocked Requests are given for the following library categories: Malicious Code/Virus, Botnets/Malicious Code Command, Spyware, Bad Reputation Domains, Adult Content, Blended Threats, Phishing, Web-based Proxies/Anonymizers, Hacking.

Note: Blended Threats is not currently used and displays “N/A.”

Bar charts for Top Security Risks (library categories), Top Categories, Top Blocked Users, and Top Users show the top five categories/users and their corresponding total Requests.



Security Reporter Dec 11, 2016 - Dec 17, 2016 Trustwave®

Executive Summary Test

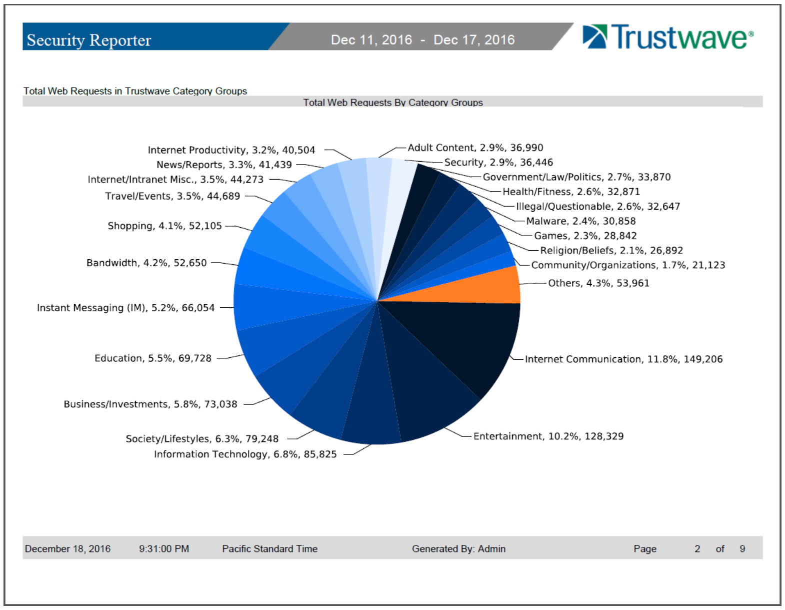
Total Web Requests:	1,249,965	Total Blocked Requests:	447,663	Unique IPs/Users:	1,113

Blocked Requests

Malicious Code/Virus:	1,652	Blended Threats:	N/A
Botnets/Malicious Code Command:	1,472	Phishing:	1,524
Spyware:	2,062	Web-Based Proxies/Anonymizers:	2,020
Bad Reputation Domains:	2,048	Hacking:	2,053
Adult Content:	13,254		

December 18, 2016 9:31:00 PM Pacific Standard Time Generated By: Admin Page 1 of 9

The second page includes a pie chart depicting Total Web Requests for Trustwave Category Groups. Each category group in the chart is represented by a pie slice and shows the number of requests and overall percentage for that pie slice.



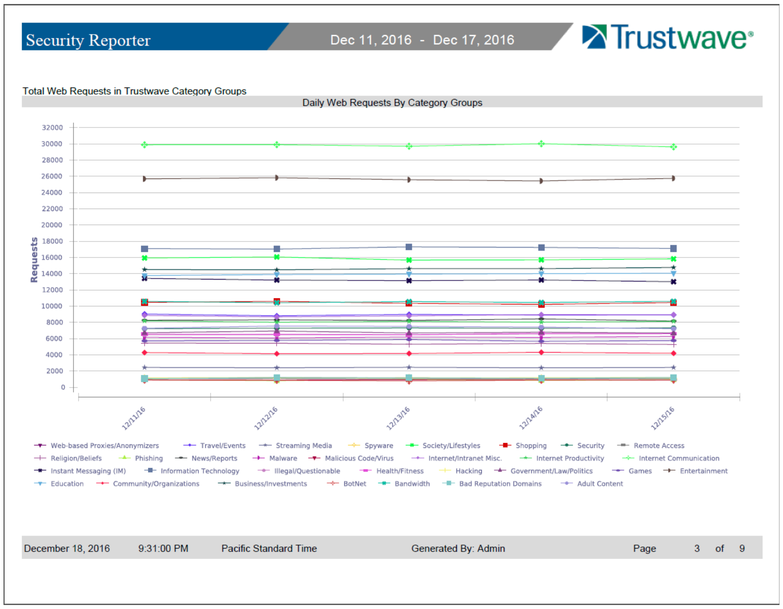
Security Reporter Dec 11, 2016 - Dec 17, 2016 Trustwave®

Total Web Requests in Trustwave Category Groups

Total Web Requests By Category Groups
Adult Content, 2.9%, 36,990
Security, 2.9%, 36,446
Government/Law/Politics, 2.7%, 33,870
Health/Fitness, 2.6%, 32,871
Illegal/Questionable, 2.6%, 32,647
Malware, 2.4%, 30,858
Games, 2.3%, 28,842
Religion/Beliefs, 2.1%, 26,892
Community/Organizations, 1.7%, 21,123
Others, 4.3%, 53,961
Internet Communication, 11.8%, 149,206
Entertainment, 10.2%, 128,329
Information Technology, 6.8%, 85,825
Society/Lifestyles, 6.3%, 79,248
Business/Investments, 5.8%, 73,038
Education, 5.5%, 69,728
Instant Messaging (IM), 5.2%, 66,054
Bandwidth, 4.2%, 52,650
Shopping, 4.1%, 52,105
Travel/Events, 3.5%, 44,689
Internet/Intranet Misc., 3.5%, 44,273
News/Reports, 3.3%, 41,439
Internet Productivity, 3.2%, 40,504

December 18, 2016 9:31:00 PM Pacific Standard Time Generated By: Admin Page 2 of 9

In Weekly and Monthly reports, the next page provides a line chart for Daily Web Requests by Category Groups. Each category group in the chart is represented by a colored symbol that can be identified by the key at the bottom of the page. The range of Requests is shown to the left of the chart, and the days (M/D/YY) are shown beneath the chart.



Security Reporter | Dec 11, 2016 - Dec 17, 2016

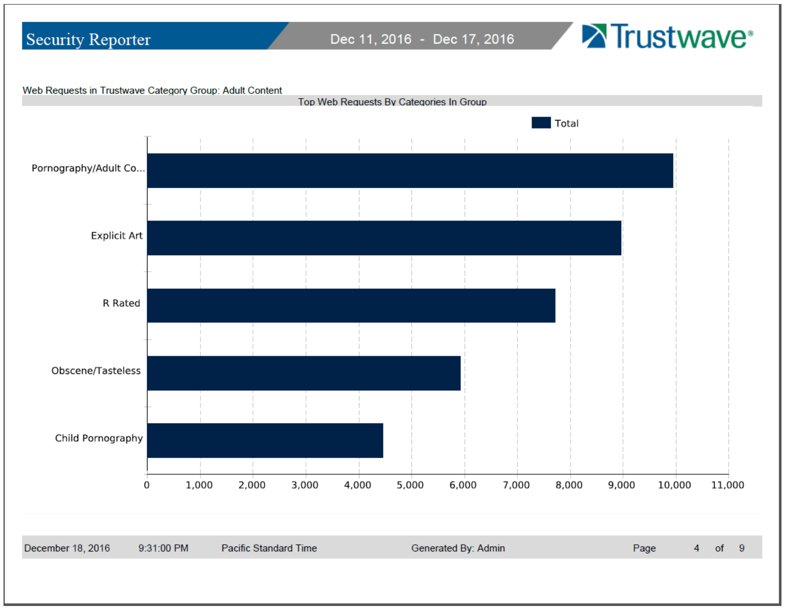
Total Web Requests in Trustwave Category Groups

Daily Web Requests By Category Groups

December 18, 2016 9:31:00 PM Pacific Standard Time Generated By: Admin Page 3 of 9

The remainder of the report provides two pages of information about each Category Group that was selected for inclusion in the report.

- The first page for each Group is a bar chart depicting Top Web Requests By Categories In Group. Up to 15 affected library categories in the group are named in the Categories list to the left, and each library category is represented in the chart by a bar and corresponding number of requests. The range of Requests is shown beneath the chart.



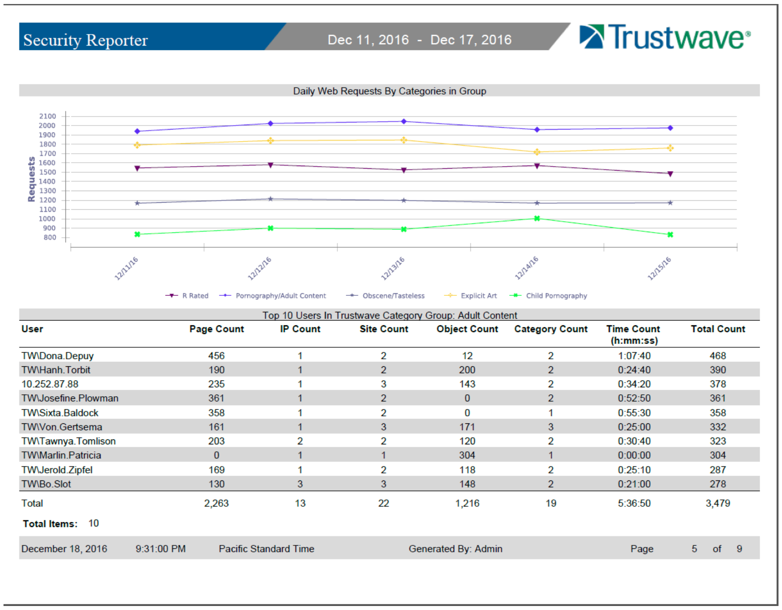
Security Reporter | Dec 11, 2016 - Dec 17, 2016

Web Requests in Trustwave Category Group: Adult Content

Top Web Requests By Categories In Group

December 18, 2016 9:31:00 PM Pacific Standard Time Generated By: Admin Page 4 of 9

- The second page for each group includes one or two items depending on the period covered.



Security Reporter   Dec 11, 2016 - Dec 17, 2016   Trustwave

Daily Web Requests By Categories in Group

Top 10 Users In Trustwave Category Group: Adult Content

User	Page Count	IP Count	Site Count	Object Count	Category Count	Time Count (h:mm:ss)	Total Count
TW\Dona.Depuy	456	1	2	12	2	1:07:40	468
TW\Hanh.Torbit	190	1	2	200	2	0:24:40	390
10.252.87.88	235	1	3	143	2	0:34:20	378
TW\Josefine.Plowman	361	1	2	0	2	0:52:50	361
TW\Sixta.Baldock	358	1	2	0	1	0:55:30	358
TW\Von.Gertsema	161	1	3	171	3	0:25:00	332
TW\Tawnya.Tomlison	203	2	2	120	2	0:30:40	323
TW\Marlin.Patricia	0	1	1	304	1	0:00:00	304
TW\Jerold.Zipfel	169	1	2	118	2	0:25:10	287
TW\Bo.Slot	130	3	3	148	2	0:21:00	278
Total	2,263	13	22	1,216	19	5:36:50	3,479

Total Items: 10

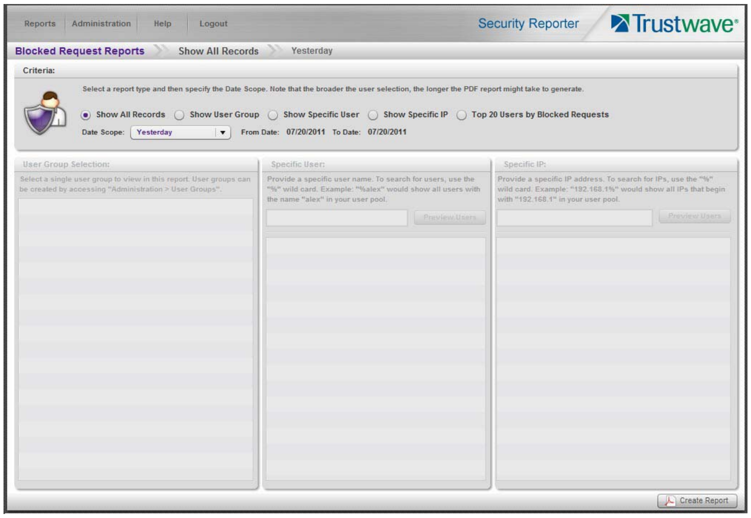
December 18, 2016   9:31:00 PM   Pacific Standard Time   Generated By: Admin   Page 5 of 9

- Weekly and Monthly reports provide a line chart for Daily Web Requests by Categories in Group. Each library category in the chart is represented by a colored symbol that can be identified by the key below the chart. The range of Requests is shown to the left of the chart, and the days (M/D/YY) are shown beneath the chart.
- All reports provide a table listing the Top 10 Users In Category Group for the period, along with each user's corresponding Page Count, IP Count, Site Count, Category Count, Time HH:MM:SS, and Hit Count.

4.5.2 Blocked Request Reports

The Blocked Request Reports option provides information about blocked URLs that end users attempted to access within a specified time period.

In the navigation toolbar, hover over the Reports menu link and select **Blocked Request** to display the Blocked Request Reports panel:



Criteria:

Select a report type and then specify the Date Scope. Note that the broader the user selection, the longer the PDF report might take to generate.

● Show All Records ○ Show User Group ○ Show Specific User ○ Show Specific IP ○ Top 20 Users by Blocked Requests

Date Scope: Yesterday From Date: 07/20/2011 To Date: 07/20/2011

User Group Selection:

Select a single user group to view in this report. User groups can be created by accessing "Administration > User Groups".

Specific User:

Provide a specific user name. To search for users, use the "%" wild card. Example: "%alex" would show all users with the name "alex" in your user pool.

Specific IP:

Provide a specific IP address. To search for IPs, use the "%" wild card. Example: "192.168.1%" would show all IPs that begin with "192.168.1" in your user pool.

4.5.2.1 Generate a Blocked Request Report

To generate a Blocked Request Report:

1. In the Criteria sub-panel, specify the type of report to be generated by clicking the radio button corresponding to that option, and—if necessary—making entries/selections in pertinent fields:
    - **Show All Records**: If you select this option, the Date Scope field displays “Yesterday” and yesterday’s date.
    - **Show User Group**: If you select this option, select the user group from the User Group Selection list box below. The Date Scope field displays “Yesterday” and yesterday’s date.
    - **Show Specific User**: If you select this option, enter the username—or a portion of the username with the ‘%’ wildcard—in the Specific User sub-panel, and then click **Preview Users** to display results in the list box below. Select the user, and then make a selection from the **Date Scope** field to display the date range for that time period: Yesterday, Last Week, Last Month, Current Week, Current Month.
    - **Show Specific IP**: If you select this option, enter the IP address—or a portion of the IP address with the ‘%’ wildcard—in the Specific IP sub-panel, and then click **Preview Users** to display results in the list box below. Select the user IP address, and then make a selection from the **Date Scope** field to display the date range for that time period: Yesterday, Last Week, Last Month, Current Week, Current Month.
    - **Top 20 Users by Blocked Requests:** If you select this option, make a selection from the **Date Scope** field to display the date range for that time period: Yesterday, Last Week, Last Month, Current Week, Current Month.
2. Click **Create Report** to generate the report view in the PDF format.

As with other reports exported in the PDF format, this report can be saved and/or printed.

Note: If there is no data available—or if data is available for only a partial number of days within the date scope range—a message displays indicating that no records are available.

If a new user group with existing usernames or IP addresses was added, data for that user group will not be available for viewing on the current day. Data for the following viewing options are available according to this schedule:

- Yesterday: available by the next day
- Current Week, Current Month: shows data up to the previous day
- Last Week: available by the next Sunday
- Last Month: available by the first of next month.

If a new user group with new users was added, by the next day only the "Yesterday" viewing option will contain data available for viewing. All other viewing options will not be available until the full length of time indicated by the viewing option has transpired.

4.5.2.2 View the Blocked Request Report

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

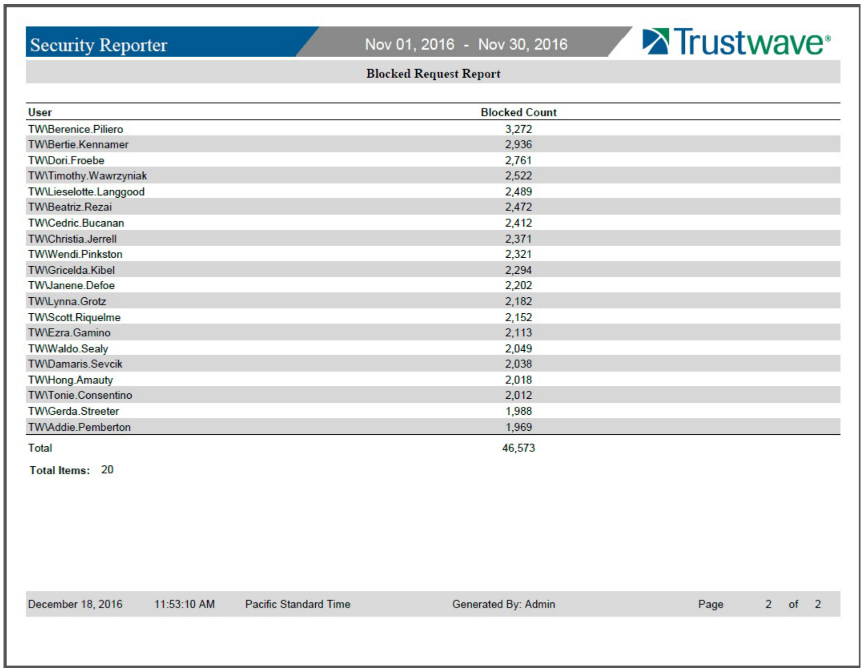
'RESULTS FOR: the date' displays above the NAME column header if the report criteria is other than "Top 20 Users by Blocked Requests".

In the body of the report, rows of records display beneath the following column headers: end user NAME, IP address (if the report criteria is other than "Top 20 Users by Blocked Requests"), and Blocked Count quantity.

If the report was generated for any criteria other than "Top 20 Users by Blocked Requests", the Total for Day count displays beneath each section.

The footer of the report includes the Date and Time the report was generated, and Page number.

The Total Count for all blocked requests displays at the end of the report.



Security Reporter Nov 01, 2016 - Nov 30, 2016 Trustwave

Blocked Request Report

User	Blocked Count
TW\Berenice.Piliero	3,272
TW\Bertie.Kennamer	2,936
TW\Dori.Froebe	2,761
TW\Timothy.Wawrzyniak	2,522
TW\Lieselotte.Langgood	2,489
TW\Beatriz.Rezai	2,472
TW\Cedric.Bucanan	2,412
TW\Christia.Jerrell	2,371
TW\Wendi.Pinkston	2,321
TW\Gricelda.Kibel	2,294
TW\Janene.Defoe	2,202
TW\Lynna.Grotz	2,182
TW\Scott.Riquelme	2,152
TW\Ezra.Gamino	2,113
TW\Waldo.Sealy	2,049
TW\Damaris.Sevcik	2,038
TW\Hong.Amauty	2,018
TW\Tonie.Consentino	2,012
TW\Gerda.Streeter	1,988
TW\Addie.Pemberton	1,969
Total	46,573

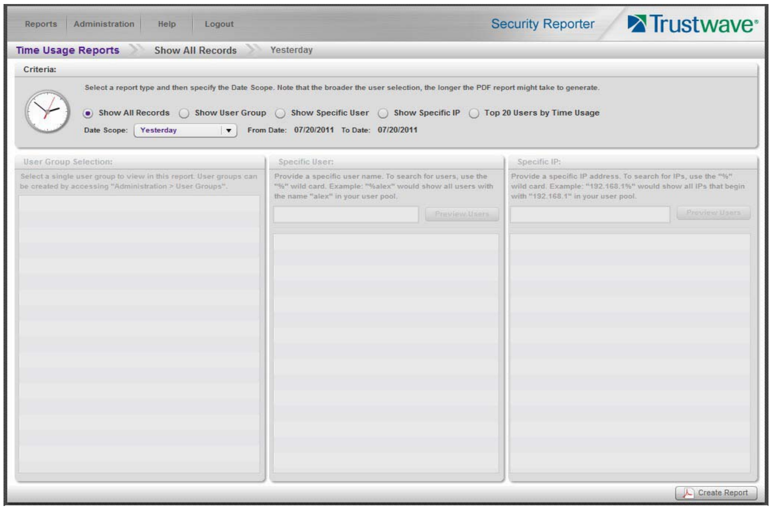
Total Items: 20

December 18, 2016 11:53:10 AM Pacific Standard Time Generated By: Admin Page 2 of 2

4.5.3 Time Usage Reports

The Time Usage Reports summarize end user Internet usage activity for a specified time period, based on the Time Usage algorithm. This algorithm calculates the amount of time an end user spent accessing a given page or object, disregarding the number of seconds per hit, and counting each unique minute of Web time as one minute. Using this algorithm, an end user could never have more than 24 hours of Web time within a given 24-hour period.

In the navigation toolbar, hover over the Reports menu link and select **Time Usage** to display the Time Usage Reports panel:



Select a report type and then specify the Date Scope. Note that the broader the user selection, the longer the PDF report might take to generate.

● Show All Records ○ Show User Group ○ Show Specific User ○ Show Specific IP ○ Top 20 Users by Time Usage

Date Scope: Yesterday From Date: 07/20/2011 To Date: 07/20/2011

User Group Selection:

Select a single user group to view in this report. User groups can be created by accessing "Administration > User Groups".

Specific User:

Provide a specific user name. To search for users, use the "%" wild card. Example: "%alex" would show all users with the name "alex" in your user pool.

Specific IP:

Provide a specific IP address. To search for IPs, use the "%" wild card. Example: "192.168.1%" would show all IPs that begin with "192.168.1" in your user pool.

4.5.3.1 Generate a Time Usage Report

To generate a Time Usage report:

1. In the Criteria sub-panel, specify the type of report to be generated by clicking the radio button corresponding to that option, and—if necessary—making entries/selections in pertinent fields:
   - **Show All Records**: If you select this option, the Date Scope field displays “Yesterday” and yesterday’s date.
   - **Show User Group**: If you select this option, select the user group from the User Group Selection list box below. The Date Scope field displays “Yesterday” and yesterday’s date.
   - **Show Specific User**: If you select this option, enter the username—or a portion of the username with the ‘%’ wildcard—in the Specific User sub-panel, and then click **Preview Users** to display results in the list box below. Select the user, and then make a selection from the **Date Scope** field to display the date range for that time period: Yesterday, Last Week, Last Month, Current Week, Current Month.
   - **Show Specific IP**: If you select this option, enter the IP address—or a portion of the IP address with the ‘%’ wildcard—in the Specific IP sub-panel, and then click **Preview Users** to display results in the list box below. Select the user IP address, and then make a selection from the **Date Scope** field to display the date range for that time period: Yesterday, Last Week, Last Month, Current Week, Current Month.
   - **Top 20 Users by Time Usage:** If you select this option, make a selection from the **Date Scope** field to display the date range for that time period: Yesterday, Last Week, Last Month, Current Week, Current Month.
2. Click **Create Report** to generate the report view in the PDF format.

   As with other reports exported in the PDF format, this report can be saved and/or printed.

Note: If there is no data available (or if data is not available for all days in the date range you specified), a message displays indicating that no records are available.

If a new user group with existing usernames or IP addresses was added, data for that user group will not be available for viewing on the current day. Data for the following viewing options are available according to this schedule:

- Yesterday: available by the next day
- Current Week, Current Month: includes data up to the previous day
- Last Week: available by the next Sunday
- Last Month: available by the first of next month.

If a new user group with new users was added, by the next day only the “Yesterday” viewing option will contain data available for viewing. All other viewing options will not be available until the full length of time indicated by the viewing option has transpired.

4.5.3.2 View the Time Usage Report

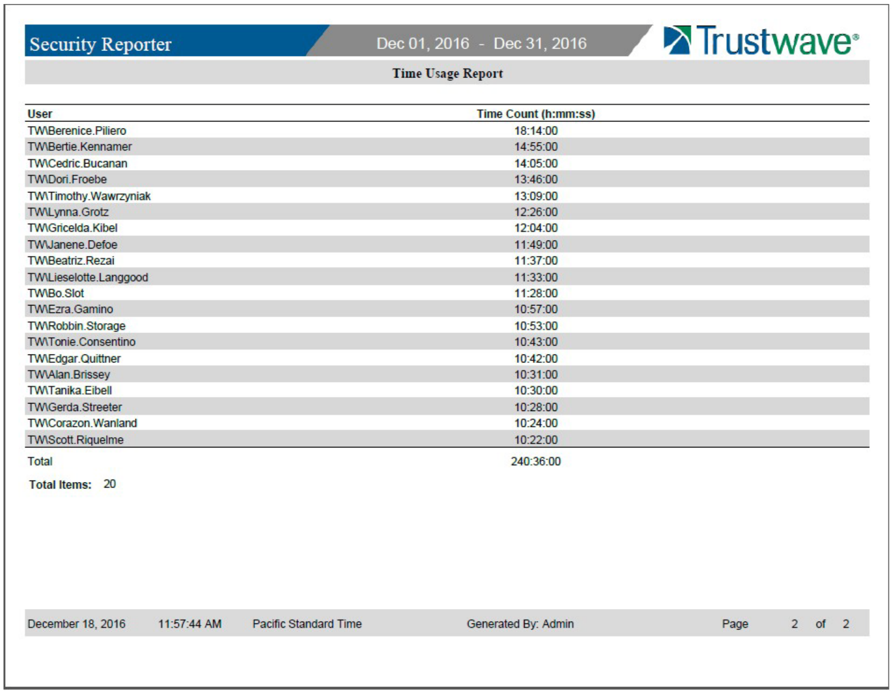
The header of the generated Time Usage report includes the date range, Report Type, and Details criteria.

The body of the report includes the end user NAME, TIME USAGE time totals in days, hours, and minutes, and any other relative criteria, such as username path or IP address.

The Total Records displays at the end of each section.

The footer of the report includes the Date and Time the report was generated, and Page number.

The Total Time for this Date Scope in days, hours, and minutes displays at the end of the report.



Security Reporter Dec 01, 2016 - Dec 31, 2016

Time Usage Report

User	Time Count (h:mm:ss)
TW\Berenice.Piliero	18:14:00
TW\Bertie.Kennamer	14:55:00
TW\Cedric.Bucanan	14:05:00
TW\Dori.Froebe	13:46:00
TW\Timothy.Wawrzyniak	13:09:00
TW\Lynna.Grotz	12:26:00
TW\Gricelda.Kibel	12:04:00
TW\Janene.Defoe	11:49:00
TW\Beatriz.Rezai	11:37:00
TW\Lieselotte.Langgood	11:33:00
TW\Bo.Slot	11:28:00
TW\Ezra.Gamino	10:57:00
TW\Robbin.Storage	10:53:00
TW\Tonie.Consentino	10:43:00
TW\Edgar.Quittner	10:42:00
TW\Alan.Brissey	10:31:00
TW\Tanika.Eibell	10:30:00
TW\Gerda.Streeter	10:28:00
TW\Corazon.Wanland	10:24:00
TW\Scott.Riquelme	10:22:00
Total	240:36:00

Total Items: 20

December 18, 2016 11:57:44 AM Pacific Standard Time Generated By: Admin Page 2 of 2

4.5.3.3 Time Usage algorithm

For each end user included in the report, the number of seconds from the log is dropped, and each unique minute within a given hour counts as one minute.

In the following example, the end user shows a total of seven minutes of Time Usage:

```
12:00:01www.trustwave.com
12:00:10www.abc.com
12:01:00www.trustwave.com
12:02:04www.whitepages.com
12:05:58www.yellowpages.com
12:05:58www.yellowpages.com/714.jsp
12:05:59www.yellowpages.com/phone_number.gif
12:07:03www.google.com
12:07:33www.yahoo.com
12:08:23www.news.com
12:08:30www.usatoday.com
12:08:59www.usatoday.com/usa.gif
12:09:00www.usatoday.com/ca.gif
```

```
12:09:01www.yahoo.com
12:09:02http://200.100.10.65:88
12:09:03www.abc.com
12:09:04www.nbc.com
```

The total for this end user is based on a nine-minute time span that includes 17 entries in the log, and seven unique minute entries: 00, 01, 02, 05, 07, 08, and 09.

Appendices

Appendix A: Disable Pop-up Blocking Software

An administrator with pop-up blocking software installed on his/her workstation should disable pop-up blocking in order to best use the System Configuration console.

This appendix provides instructions on how to disable pop-up blocking software for current versions of the supported browser types (Internet Explorer, Firefox, Chrome, and Safari) and the Google Toolbar.

A.1 Browser Pop-up Blockers

A.1.1 Internet Explorer

1. In the Internet Explorer toolbar, navigate to Tools | Pop-up Blocker (or from the “gear” menu at top right of the window, select Internet options | Privacy).
2. If you want to disable all pop-up blocking, be sure the Turn Off Pop-up Blocker selection is enabled, or uncheck the box “Turn on Pop-up Blocker”.
3. If you want to block all pop-ups except those from URLs you choose to whitelist, enable Turn On Pop-up Blocker and then navigate to Pop-up Blocker Settings, adding the SR's URL in the Allowed sites list box.

A.1.2 Edge

1. From the menu (...) at the top right of the window, click Settings.
2. Click View advanced settings.
3. In the Advanced settings menu, click the Block pop-ups slider to disable all pop-up blocking

Note: If you want to use a whitelist to allow pop-ups from sites you specify, use Internet Explorer to configure the settings. These settings will also apply in Edge.

A.1.3 Mozilla Firefox

1. In the Firefox menu bar (or menu at the top right of the window), navigate to Tools | Options | Content tab.
2. Uncheck the “Block pop-up windows” check box, or click **Exceptions...** and then add the SR's URL in the Allowed Sites - Pop-ups window.

A.1.4 Google Chrome

1. From the menu at the top right of the window, navigate to Settings | Show advanced settings.
2. Under Privacy, click Content settings and scroll to the Pop-ups section.
3. Choose either:

- Allow all sites to show pop-ups

or

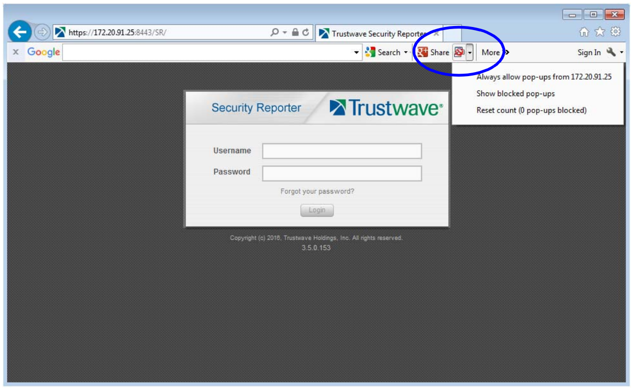
- Do not allow any site to show pop-ups (recommended) | Manage exceptions..., adding the SR's URL to the Pop-up Exceptions box.

A.1.5 Safari

In the Safari toolbar, navigate to Preferences | Security, and de-select “Block pop-up windows” to disable pop-up blocking.

A.2 Google Toolbar Pop-up Blocker

To add the SR site to the allowed list so that pop-ups will be permitted, while viewing the site go to the Google Toolbar and click the Pop-up blocker button.


https://172.20.91.25:8443/SR/
Trustwave Security Reporter
Google
Search
Share
More
Sign In
Always allow pop-ups from 172.20.91.25
Show blocked pop-ups
Reset count (0 pop-ups blocked)
Security Reporter
Trustwave
Username
Password
Forgot your password?
Login

Copyright (c) 2016, Trustwave Holdings, Inc. All rights reserved.
3.5.0.153

Appendix B: RAID and Hardware Maintenance

This appendix is divided into three parts: Hardware Components, Server Interface, and Troubleshooting—in the event of a failure in one of the drives, power supplies, or fans.

Note: As part of the ongoing maintenance procedure for your RAID server, Trustwave recommends that you always have a spare drive and spare power supply on hand.

Contact the Trustwave Technical Assistance Center for replacement hard drives and power supplies.

Note: For help with troubleshooting models 505, 705 or 735, please visit IBM’s Systems Support Web site at http://www.ibm.com/systems/support/ .

Model 505 uses IBM System x3250 M3 hardware, so your query should specify IBM System x | System x3250 M3. IBM System x3250 M3 Types 4251, 4252, and 4261 Installation and User's Guide contains instructions on viewing and using LED indicators and buttons on SR model 505. As of July 2011, this document was made available at http://www-947.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5082564&brandind=5000008.

Models 705 and 735 use IBM System x3620 M3 hardware, so your query should specify IBM System x | System x3620 M3. IBM System x3620 M3 Type 7376 Installation and User's Guide contains instructions on viewing and using LED indicators and buttons on SR models 705 and 735. As of July 2011, this document was made available at http://www-

947.ibm.com/support/entry/portal/docdisplay?brand=5000008&lndocid=MIGR-5084233.

B.1 Part 1: Hardware Components

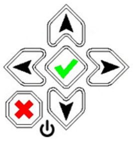
The chassis of each model consists of the following components:

300 Model	500 Models	700,730 Models
2 hard drives	4 hard drives	4 hard drives
1 power supply	1 power supply	2 power supplies
1 cooling fan	3 cooling fans	4 cooling fans

B.2 Part 2: Server Interface

B.2.1 Front Control Panel on a 300 model

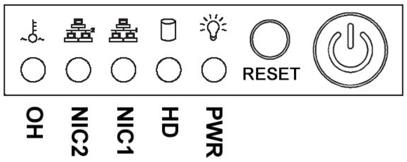
The keypad on the front of the server is used for performing basic server functions.



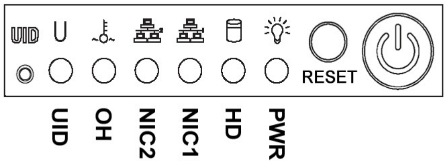
- **Boot up** - Depress and hold the checkmark key for 3 seconds.
- **Reboot** - Depress and hold the checkmark key for 10 seconds.
- **Shut down** - Depress and hold the 'X' key for 10 seconds.

B.2.2 Front control panels on 500, 700, and 730 models

Control panel buttons, icons, and LED indicators display on the right side of the 500, 700, and 730 model front panel. The buttons let you perform a function on the unit, while an LED indicator corresponding to an icon alerts you to the status of that feature on the unit.



500 chassis front panel



700 chassis front panel

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

UID (button) and **U** icon – On a 700 model, when the UID button is pressed, a steady blue LED displays on both the front and rear of the chassis. These indicators are used for easy location of the chassis in a large stack configuration. The LED remains on until the button is pressed a second time.

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

NIC2 (icon) – A flashing green LED indicates network activity on LAN2. On a 500 model, the LED is a steady green with link connectivity, and unlit if there with no link connectivity.

NIC1 (icon) – A flashing green LED indicates network activity on LAN1. On a 500 model, the LED is a steady green with link connectivity, and unlit if there with no link connectivity.

HDD (icon) – In addition to displaying in the control panel, this icon also displays on the front panel on each hard drive carrier. Hard drive activity is indicated by a flashing amber LED in the control panel, and a flashing green LED on a drive carrier. An unlit LED on a drive carrier may indicate a hard drive failure. (See Hard drive failure in the Troubleshooting sub-section for information on detecting a hard drive failure and resolving this problem.)

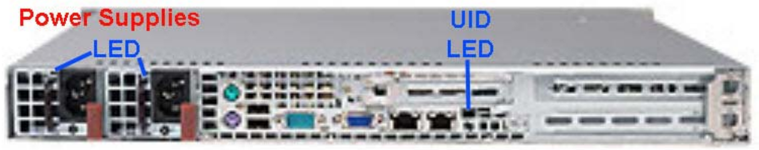
Power (icon) – The LED is unlit when the server is turned off. A steady green LED indicates power is being supplied to the unit's power supplies. (See also Rear of chassis.) (See Power supply failure in the Troubleshooting sub-section for information on detecting a power supply failure and resolving this problem.)

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

B.2.3 Rear panel on 700 and 730 models

Power Supplies (LED indicators) – The power supplies are located at the right on the rear of the chassis. An LED indicator is located above each of the power plugs. (See Power supply failure in the Troubleshooting sub-section for information on detecting a power supply failure and resolving this problem.)

UID (LED indicator) – On the rear of the 700 series chassis, to the right of the LAN ports, a steady blue UID LED indicator displays when the UID button on the control panel is pressed. This LED remains lit until the UID button is pressed again.



B.3 Part 3: Troubleshooting

The text in this section explains how the server alerts the administrator to a failed component, and what to do in the event of a failure.

B.3.1 Hard drive failure

B.3.1.1 Review the notification email

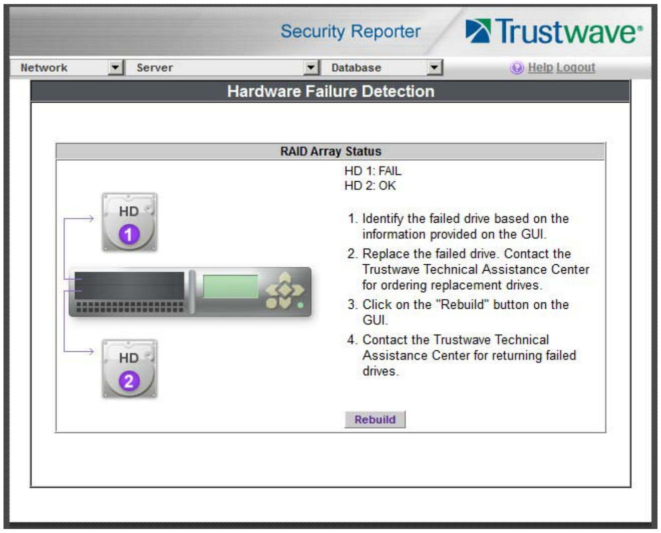
If a hard drive fails, a notification email is sent to the administrator of the server. This email identifies the failed hard drive by its number. Upon receiving this alert, the administrator should verify the status of the drives by first going to the Hardware Failure Detection screen in the System Configuration console.

Caution: Do not attempt to remove any of the drives from the unit at this time. Verification of the failed drive should first be made in the System Configuration console before proceeding, as data on the server will be lost in the event that the wrong drive is removed from the unit.

Verify the failed drive in the Admin console

The Hardware Failure Detection screen in the System Configuration console is accessible via the **Server | Hardware Failure Detection** menu selection:

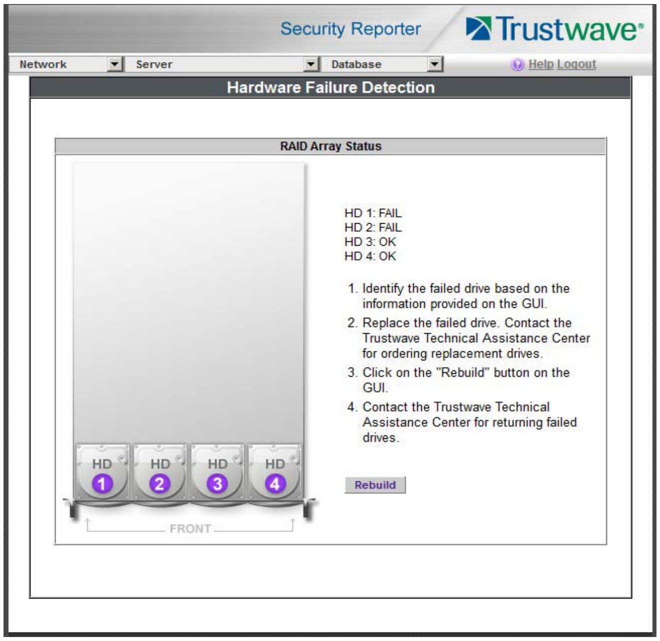
Figure 8: Hardware Failure Detection screen, 300 model



HD 1: FAIL
HD 2: OK

1. Identify the failed drive based on the information provided on the GUI.
2. Replace the failed drive. Contact the Trustwave Technical Assistance Center for ordering replacement drives.
3. Click on the "Rebuild" button on the GUI.
4. Contact the Trustwave Technical Assistance Center for returning failed drives.

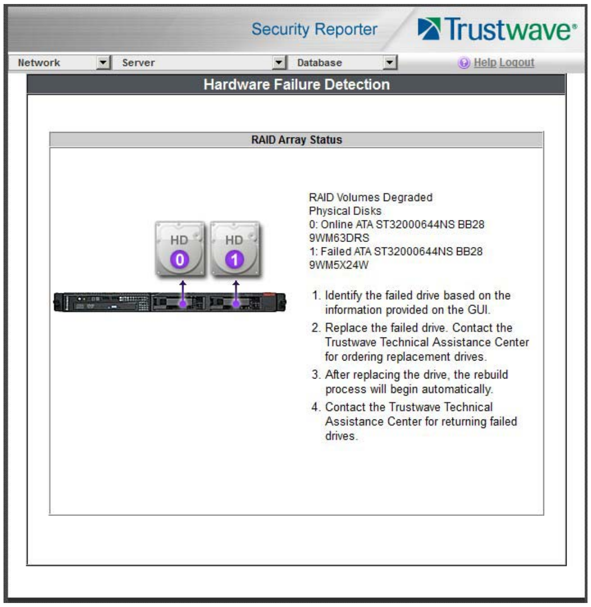
Figure 9: Hardware Failure Detection window, 500, 700, 730 model



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

1. Identify the failed drive based on the information provided on the GUI.
2. Replace the failed drive. Contact the Trustwave Technical Assistance Center for ordering replacement drives.
3. Click on the "Rebuild" button on the GUI.
4. Contact the Trustwave Technical Assistance Center for returning failed drives.

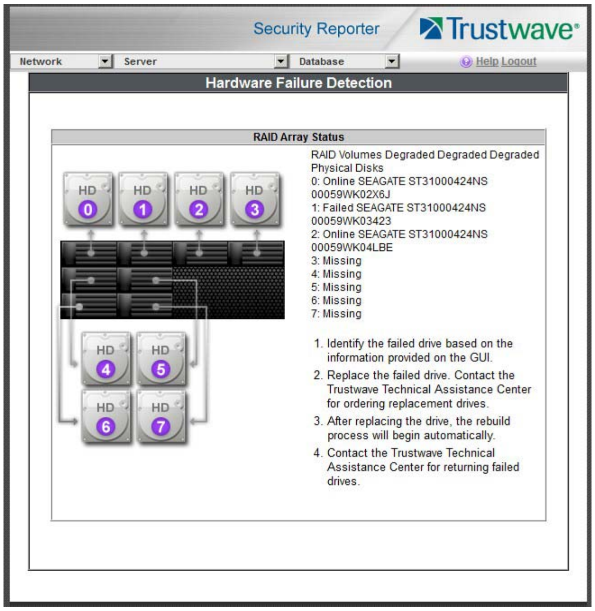
Figure 10: Hardware Failure Detection screen, 505 IBM model



RAID Volumes Degraded
Physical Disks
0: Online ATA ST32000644NS BB28
9WM63DRS
1: Failed ATA ST32000644NS BB28
9WM5X24W

1. Identify the failed drive based on the information provided on the GUI.
2. Replace the failed drive. Contact the Trustwave Technical Assistance Center for ordering replacement drives.
3. After replacing the drive, the rebuild process will begin automatically.
4. Contact the Trustwave Technical Assistance Center for returning failed drives.

Figure 11: Hardware Failure Detection screen, 705 or 735 IBM model



Hardware Failure Detection

RAID Array Status

RAID Volumes Degraded Degraded Degraded
Physical Disks
0: Online SEAGATE ST31000424NS
00059WK02X6J
1: Failed SEAGATE ST31000424NS
00059WK03423
2: Online SEAGATE ST31000424NS
00059WK04LBE
3: Missing
4: Missing
5: Missing
6: Missing
7: Missing

1. Identify the failed drive based on the information provided on the GUI.
2. Replace the failed drive. Contact the Trustwave Technical Assistance Center for ordering replacement drives.
3. After replacing the drive, the rebuild process will begin automatically.
4. Contact the Trustwave Technical Assistance Center for returning failed drives.

B.3.1.2 Hard drive failure on Equus SR models 300, 500, 700, 730

For Equus models, the Hardware Failure Detection window displays the current RAID Array Status for all hard drives (HD) at the right side of the window.

Normally, when all hard drives are functioning without failure, the text “OK” displays to the right of the hard drive number, and no other text displays in the window.

However, if a hard drive has failed, the message “FAIL” displays to the right of the hard drive number.

Before taking any action in this window, replace the drive.

B.3.1.3 Hard drive failure on IBM SR model 505

For IBM SR model 505, the Hardware Failure Detection window displays the current RAID Array Status for the hard drives (0 - 1) at the right side of the window.

Normally, when all hard drives are functioning without failure, the text “RAID Volumes Optimal” displays above with an “Online” status corresponding to each hard drive.

However, if a hard drive has failed, the text “RAID Volumes Degraded” displays above with a “Fail” status corresponding to the failed hard drive.

Note: A “Missing” status displays if a hard drive was removed from its carrier.

Before taking any action in this window, replace the drive.

B.3.1.4 Hard drive failure on IBM SR models 705, 735

For IBM SR models 705 and 735, the Hardware Failure Detection window displays the current RAID Array Status for all the hard drives (0 - 7) at the right side of the window.

Normally, when all hard drives are functioning without failure, the text “RAID Volumes Optimal” displays above with an “Online” status corresponding to each hard drive.

However, if a hard drive has failed, the text “RAID Volumes Degraded” displays above with a “Fail” status corresponding to the failed hard drive.

Note: A “Missing” status displays if a hard drive was either removed from its carrier or the hard drive bay is unoccupied by default. For models 705 and 735, unoccupied default drives include drives 4 through 7.

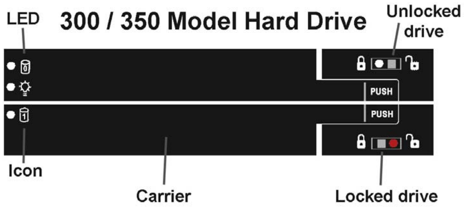
Before taking any action in this window, replace the drive.

B.3.1.5 Replace the failed hard drive

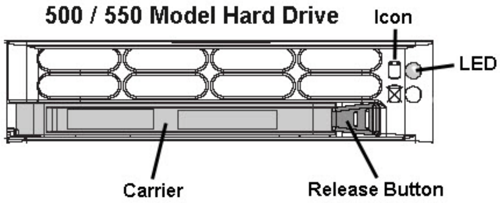
After verifying the failed hard drive in the Administrator console, go to the server to replace the drive.

B.3.1.6 Drive replacement on Equus SR models 300, 500, 700, 730

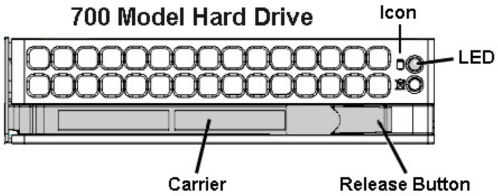
On a 300 model, be sure the carrier is unlocked, then press the section on the carrier handle labeled PUSH to release the carrier handle. On a 500, 700, or 730 model, press the red release button to release the carrier handle.



300 model hard drive carrier



500 model hard drive carrier



700 and 730 model hard drive carrier

Extend the carrier handle fully by pulling it out towards you. Pull out the failed drive and replace it with your spare replacement drive. Push the drive into its slot, and press the carrier back in place.

Note: Contact the Trustwave Technical Assistance Center if you have any questions about replacing a failed hard drive.

After replacing the failed hard drive, proceed to section B.3.1.9.

B.3.1.7 Drive replacement on IBM SR model 505

For SR model 505, please consult IBM System x3250 M3 Types 4251, 4252, and 4261 Installation and User's Guide for hard drive replacement instructions.

After replacing the failed hard drive, proceed to section B.3.1.9 .

B.3.1.8 Drive replacement on IBM SR models 705, 735

For SR models 705 and 735, please consult IBM System x3620 M3 Type 7376 Installation and User's Guide for hard drive replacement instructions.

After replacing the failed hard drive, proceed to the next section.

B.3.1.9 Rebuild the hard drive on Equus SR models 300, 500, 700, 730

Drive rebuild on Equus SR models 300, 500, 700, 730

Once the failed hard drive has been replaced, return to the Hardware Failure Detection screen in the System Configuration console, and click **Rebuild** to proceed with the rebuild process. When the rebuild process begins, a message displays indicating the drive rebuild is in progress and Hardware Failure Detection functionality has been suspended. The RAID rebuild could take a couple of hours before it is completed.

B.3.1.10 Rebuild the hard drive on IBM SR models 505, 705, 735

Once the failed hard drive has been replaced, return to the Hardware Failure Detection screen in the System Configuration console that now displays an “Unconfigured” drive status for the replaced drive. Note that it could take up to an hour before the drive rebuild process initializes, at which time a message will display indicating the drive rebuild is in progress and Hardware Failure Detection functionality has been suspended. The RAID rebuild could take a couple of hours before it is completed.

B.3.1.11 Contact the Trustwave Technical Assistance Center

Contact the Trustwave Technical Assistance Center to order a new replacement hard drive and for instructions on returning your failed hard drive to Trustwave.

B.3.2 Power supply failure

B.3.2.1 Verify the power supply has failed

The administrator of the server is alerted to a power supply failure on the 500, 700, and 730 chassis by an audible alarm and an amber power supply LED—or an unlit LED—on the front of the chassis.

Note: A steady amber power supply LED on a 500, 700, or 730 chassis also may indicate a disconnected or loose power supply cord. Verify that the power supply cord is plugged in completely before removing a power supply.

For SR model 505, please consult IBM System x3250 M3 Types 4251, 4252, and 4261 Installation and User's Guide for power supply replacement instructions.

For SR models 705 and 735, please consult IBM System x3620 M3 Type 7376 Installation and User's Guide for power supply replacement instructions.

B.3.2.2 Contact the Trustwave Technical Assistance Center

Contact the Trustwave Technical Assistance Center for assistance with installing the replacement power supply, or to order a new replacement power supply, or for instructions on returning your failed power supply to Trustwave.

If you have a 700 or 730 model and wish to replace this hot swappable power supply unit yourself, proceed to the next section.

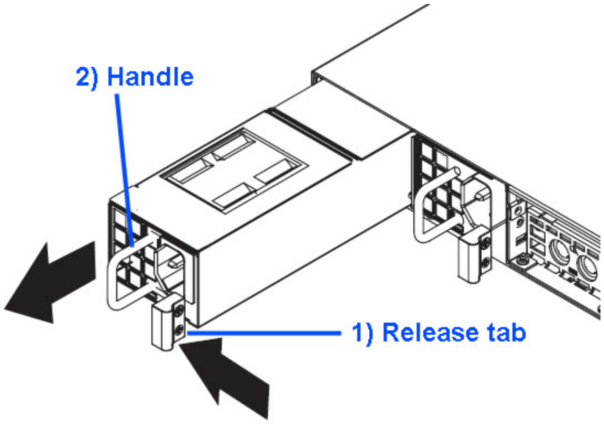
Caution: Be sure the correct failed power supply has been identified. Removing the wrong power supply will cause the system to crash.

B.3.2.3 Unplug the power cord

To prevent electrical shock to yourself and damage to the unit, unplug the power cord from the failed 700 series power supply module.

B.3.2.4 Replace a failed hot swap power supply

Remove the failed 700 or 730 power supply by locating the red release tab and pushing it to the left (1), then pulling the curved metal handle on the power supply module towards you (2).



Note that an audible alarm sounds and the LED is unlit when the power supply module is disengaged. Replace the failed power supply with your spare replacement power supply module. The alarm will turn off and the LED will be a steady green when the replacement power supply module is securely locked in place.

B.3.3 Fan failure

B.3.3.1 Identify a fan failure

A flashing red LED on a 500, 700, or 730 model indicates a fan failure. If this displays on your unit, contact the Trustwave Technical Assistance Center for an RMA (Return Merchandise Authorization) number and for instructions on returning the unit to Trustwave.

A steady red LED (on and not flashing) on a 500, 700, or 730 model indicates an overheating condition, which may be caused by cables obstructing the airflow in the system or the ambient room temperature being too warm. Check the routing of the cables and make sure all fans are present and operating normally. The LED will remain steady as long as the overheating condition exists.

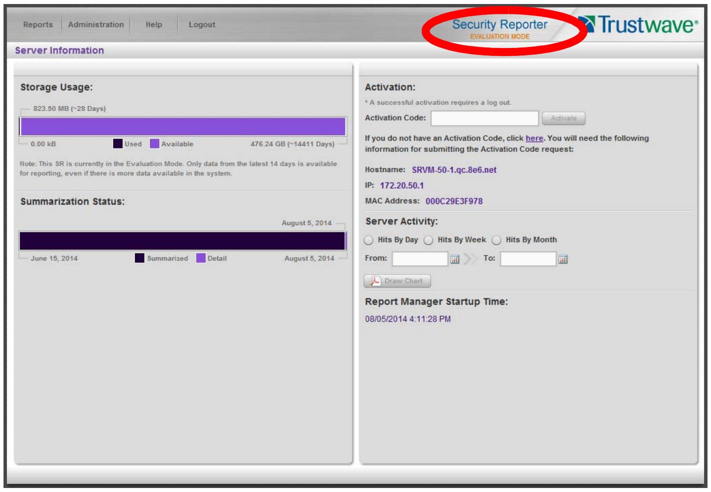
Appendix C: Evaluation Mode

By default, the SR is set to evaluation mode. Evaluation mode limits the available reports to the most recent 14 days of data. Data for earlier dates is stored but cannot be reported on. Evaluation mode is only available for a limited time.

This appendix explains how to request an extension of evaluation, or to register the SR.

C.1 Report Manager Banner

In evaluation mode, the Report Manager banner displays 'EVALUATION MODE' beneath the Security Reporter name/link.



Server Information

Storage Usage:

823.50 MB (~28 Days)

0.00 kB ■ Used ■ Available 476.24 GB (~14411 Days)

Note: This SR is currently in the Evaluation Mode. Only data from the latest 14 days is available for reporting, even if there is more data available in the system.

Summarization Status:

August 5, 2014

June 15, 2014 ■ Summarized ■ Detail August 5, 2014

Activation:

* A successful activation requires a log out.

Activation Code:

If you do not have an Activation Code, click here. You will need the following information for submitting the Activation Code request:

Hostname: SRVM-50-1.qc.8e6.net

IP: 172.20.50.1

MAC Address: 000C29E3F978

Server Activity:

○ Hits By Day ○ Hits By Week ○ Hits By Month

From: To:

Report Manager Startup Time:

08/05/2014 4:11:28 PM

Hover over the '**EVALUATION MODE**' link to display a definition of 'Evaluation Mode'. Click this link to launch the SR Server Information screen.

Note: The Server Information screen is available to all administrators through this link (the Administration menu item is visible only to Global Administrators).

In Evaluation Mode, the Storage Usage section of the Server Information screen includes a note about the data available for reporting.

C.2 Server Information Screen

For an SR unit currently in evaluation mode, the Server Information screen includes the Activation section, as shown above. You have the option to either use the SR in the evaluation mode, or to change the evaluation mode in one of two ways: by extending the evaluation period, or by registering the SR so that it can be used in the registered mode.

C.2.1 Change the Evaluation Mode

When the designated evaluation period has expired or is about to expire, you can request an extension to your evaluation period, or register the unit and use it in the registered mode.

1. In the Activation section of the sever information screen, you will find the **Hostname** of the Server, **IP** address, and **MAC Address** (hardware address of the LAN1 network interface).
2. In the message "If you do not have an Activation Code, click here.", click the link '**here**' to open the Product Activation page at the Trustwave Web site.
3. In this Web page:
    a. Enter your following information: Contact Details, Company Information, and Security Reporter Information.
    b. Choose the Activation Type: "Evaluation Extension" or "Full Activation."
4. Click **Send Information**. Trustwave will review the request and issue you an activation code (subject to contractual considerations).
5. When you receive the code, return to the Activation Page and enter the activation code in the **Activation Code** field.
6. Click **Activate** to display the confirmation message in the Activation Page pop-up box:
    - If you have extended the evaluation period for the unit, the following message displays: "It is now in evaluation mode ('X' days)!" where 'X' represents the number of days in the new evaluation period.
    - If you have registered the unit, the following message displays: "Your box has been activated!"

Glossary

base group

A user group consisting of end users whose network activities are monitored by the designated group administrator(s). Only the creator of the base group can modify the base group, delegate the base group to another group administrator, or delete the base group.

canned report

A pre-processed report that includes statistics of end user Internet/network traffic prior to the current day.

custom category

A unique library category on the Web Filter that includes URLs, URL keywords, and/or search engine keywords to be blocked. On the SR, global administrators can create and manage custom library categories and sync them to the source Web Filter.

detail drill down report

One of two types of basic reports—the other report type being a “summary drill down report”—that provides information on objects or pages an end user viewed within the specified time period.

FTP

File Transfer Protocol is used for transferring files from one computer to another on the Internet or an intranet.

global administrator

An authorized administrator of the network who maintains all aspects of the SR. A global administrator configures the SR, sets up user groups, administrator groups and group administrators, and performs routine maintenance on the server.

group administrator

An authorized administrator of the SR who maintains user group, administrator groups, and group administrator profiles.

group by report type

A report that includes two or more sets of report type criteria, such as User/Sites or Category/IPs or Category/Site/Users.

hit count

the number of pages and/or objects end users access as the result of entering URLs in a browser window.

HTTP

Hyper Text Transfer Protocol is used for transferring files via the World Wide Web or an intranet.

instant messaging

IM involves direct connections between workstations either locally or across the Internet.

library category

A list of URLs, URL keywords, and search engine keywords set up to be blocked.

LDAP

One of two authentication method protocols that can be used with the SR. Lightweight Directory Access Protocol (LDAP) is a directory service protocol based on entries (Distinguished Names). The other authentication method that can be used with the SR is IP groups.

object count

The number of objects end users access on a Web page, including images, graphics, multimedia items, and text items. The number of objects on a page is generally higher than the number of pages a user visits.

page count

The number of Web pages end users access, which can exceed the number of objects per page in categories that use a lot of pop-up ads (porn, gambling, and other related sites). A user may visit only one site, but visit 20 pages on that site if the page has pop-up ads or banner ads that link to other pages.

peer-to-peer

P2P involves communication between computing devices—desktops, servers, and other smart devices—that are linked directly to each other.

protocol

A type of format for transmitting data between two devices. LDAP is a type of authentication method protocol.

search engine

A program that searches Web pages for specified keywords and returns a list of the pages or services where the keywords were found.

SMTP

Simple Mail Transfer Protocol is used for transferring email messages between servers.

summary drill down report

One of two types of basic reports—the other report type being a “detail drill down report”—that provides a synopsis of end user Internet activity for the specified time period.

synchronization

A process by which two or more machines run in parallel to each other. User filtering profiles and library configurations on the source Web Filter can be set up to be synchronized between the source Web Filter and the SR.

TCP

An abbreviation for Transmission Control Protocol, one of the core protocols of the Internet protocol suite. Using TCP, applications on networked hosts can create connections to one another, over which streams of data can be exchanged.

time count

The amount of time end users spend on a given Web page, including the number of times that page is refreshed by either the user or a banner ad.

Time Usage Report count

The amount of time end users spend on the Internet, based on the Time Usage algorithm. For each user, the number of seconds from the log is dropped, and any unique minute within a given hour counts as one minute.

Traveler

Trustwave's executable program that downloads updates to the SR at a scheduled time.

UDP

An abbreviation for User Data Protocol, one of the core protocols of the Internet protocol suite. Using UDP, programs on networked computers can send short messages (sometimes known as datagrams) to one another.

URL

An abbreviation for Uniform Resource Locator, the global address of Web pages and other resources on the Internet. A URL is comprised of two parts. The first part of the address specifies which protocol to use (such as "http"). The second part specifies the IP address or the domain name where the resource is located (such as "203.15.47.23" or "trustwave.com").

Web access logging device

The device feeding logs to the SR: Trustwave Web Filter or Trustwave Secure Web Gateway (SWG).

Index

About Trustwave®

Trustwave helps businesses fight cybercrime, protect data and reduce security risk. With cloud and managed security services, integrated technologies and a team of security experts, ethical hackers and researchers, Trustwave enables businesses to transform the way they manage their information security and compliance programs. More than three million businesses are enrolled in the Trustwave TrustKeeper® cloud platform, through which Trustwave delivers automated, efficient and cost-effective threat, vulnerability and compliance management. Trustwave is headquartered in Chicago, with customers in 96 countries. For more information about Trustwave, visit https://www.trustwave.com.