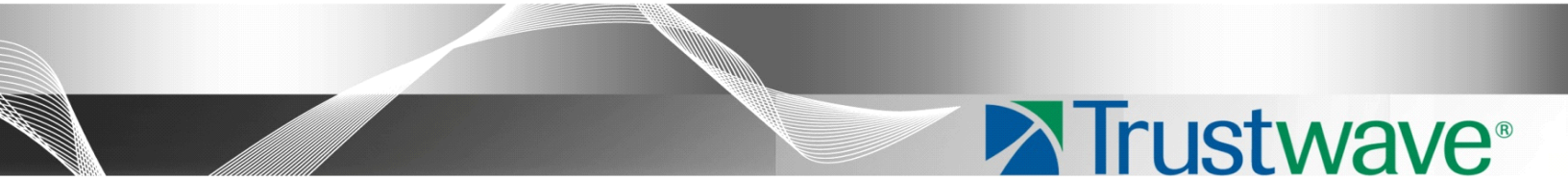


Security Reporter Administrator Guide

Version 3.3.0

Publication Date: 22 August 2013

Legal Notice

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

www.trustwave.com/support/

Trademarks

Part# SR-UG-130822a

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 software 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's Web Filter and/or Secure Web Gateway (SWG) application(s), and security reports from SWG policy servers.

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

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

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

1.2 About this User Guide

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

Note: See the Web Filter User Guide at **h**ttp://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 User Guide is organized into the following sections:

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

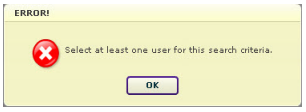
1.3 How to Use this User Guide

1.3.1 Terminology

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

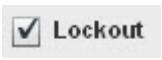
- **accordion** - One of at least two or more like objects, stacked on top of each other in a panel, that expands to fill a box in a panel or collapses closed when clicked.

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

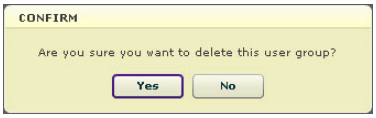


- **button** - An object in a dialog box, alert box, window, or panel that can be clicked with your mouse to execute a command.

- **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.

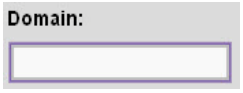


- **dialog box** - A box that opens in response to a command made in a window or panel, and requires your input. You must choose an option by clicking a button (such as "Yes" or "No", or "Next" or

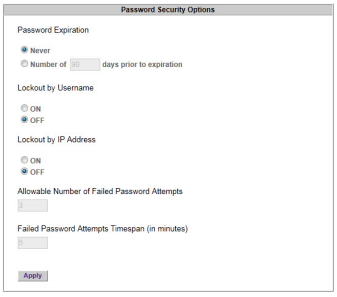


"Cancel") to execute your command. As dictated by this box, you also might need to make one or more entries or selections prior to clicking a button.

- **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.

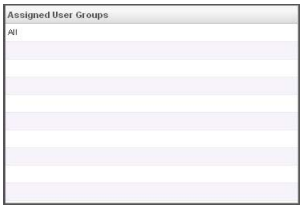


- **frame** - A boxed-in area in a dialog box, window, or panel that can include a group of objects such as fields, text boxes, list boxes, buttons, radio buttons, check boxes, accordions, tables, tabs, and/or tables. Objects within a frame belong to a specific function or group. A frame often is labeled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

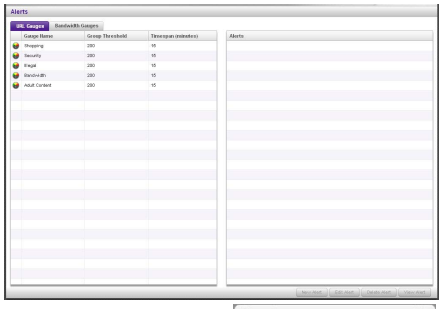


- **icon** - A small image in a dialog box, window, or screen that can be clicked. This object can be a button or an executable file.

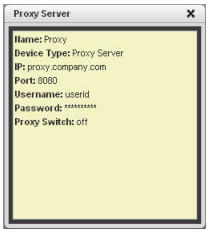
- **list box** - An area in a dialog box, window, or panel that accommodates and/or displays entries of items that can be added or removed.



- **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.



- **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.



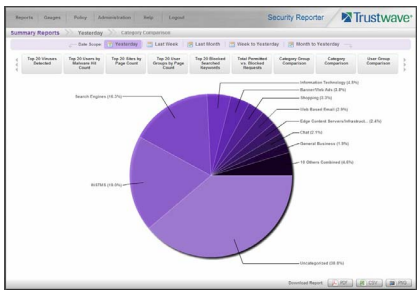
- **pull-down menu** - A field in a dialog box, window, or panel that contains a down arrow to the right. When you click the arrow, a menu of items displays from which you make a selection.

- **radio button** - A small, circular object in a dialog box, window, or screen used for selecting an option. This object allows you to toggle between two choices. By clicking a

radio button, a dot is placed in the circle, indicating that you selected the option. When the circle is empty, the option is not selected.

- **re-size button** - Positioned between two 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.



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

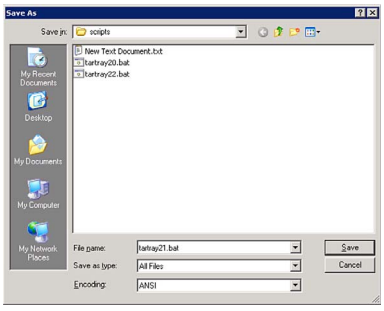
- **tab** - One of at least two objects positioned beside one another that display content specified to its label when clicked. A tab can display anywhere in a panel, usually above a box or list box.

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

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

- **text box** - An area in a dialog box, window, or screen that accommodates your data entry. A text box is a type of field. (See "field".)
- **thumbnail** - A small image in a window or on a screen that when clicked displays the same image enlarged within a window or on the screen.

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



1.4 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.

1.5 Components and Environment

1.5.1 Components

1.5.1.1 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.

1.5.1.2 Software

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

1.5.2 Environment

1.5.2.1 Network Requirements

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

1.5.2.2 Administrator Workstation Requirements

System requirements for the administrator include the following:

Client OS	IE version	Firefox version	Chrome version	Safari version
Windows Vista	9	16	23	N/A
Windows 7	9	16	23	N/A
Macintosh 10.6 (Snow Leopard)	N/A	17	23	5
Macintosh 10.7 (Lion)	N/A	17	23	6
Macintosh 10.8 (Mountain Lion)	N/A	16	23	6

- JavaScript enabled
- Pop-up blocking software, if installed, must be disabled
- Session cookies from the SR server must be allowed in order for the System Configuration console to function properly

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

1.5.2.3 End User Workstation Requirements

System requirements for the end user include the following:

Client OS	IE version	Firefox version	Chrome version	Safari version
Windows XP	8	16	23	N/A
Windows Vista	9	16	23	N/A
Windows 7	9	16	23	N/A
Macintosh 10.6 (Snow Leopard)	N/A	16	23	5
Macintosh 10.7 (Lion)	N/A	16	23	6
Macintosh 10.8 (Mountain Lion)	N/A	16	N/A	6
iPad1 (iOS 5.5)	N/A	N/A	N/A	6
iPad2 (iOS 6)	N/A	N/A	N/A	6
Galaxy Note (Android)	N/A	N/A	N/A	N/A

Client OS	IE version	Firefox version	Chrome version	Safari version
Kindle Fire	N/A	N/A	N/A	N/A
Nexus	N/A	N/A	23	N/A

- JavaScript enabled
- Pop-up blocking software, if installed, must be disabled

1.6 Getting Started

1.6.1 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—the latter if the SR image will be installed on an appliance in your network and running as a virtual machine. The Installation Guide explains how to perform the initial configuration of the SR so that it can be accessed via an IP address or hostname on your network, and communicate with the Web access logging device(s) (Web Filter and/or Secure Web Gateway) to receive logs of end user Internet/network activity.

Note: If you do not have the Installation Guide, contact Trustwave immediately to have a copy sent to you.

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.

1.6.2 Procedures for Logging In, Out

1.6.2.1 Log In

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

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.

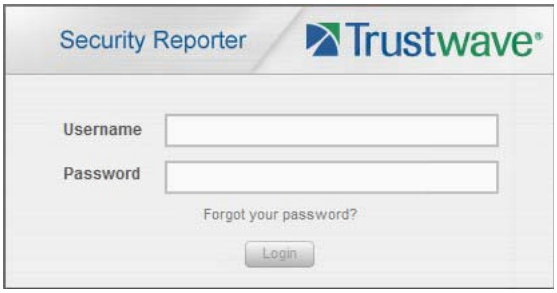
If your browser is set to display in English, Simplified Chinese or Traditional Chinese, the SR user interface will display that language setting by default. However, this language selection can be changed for your user account as described in the Report Manager Administration Section.

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

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

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

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



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

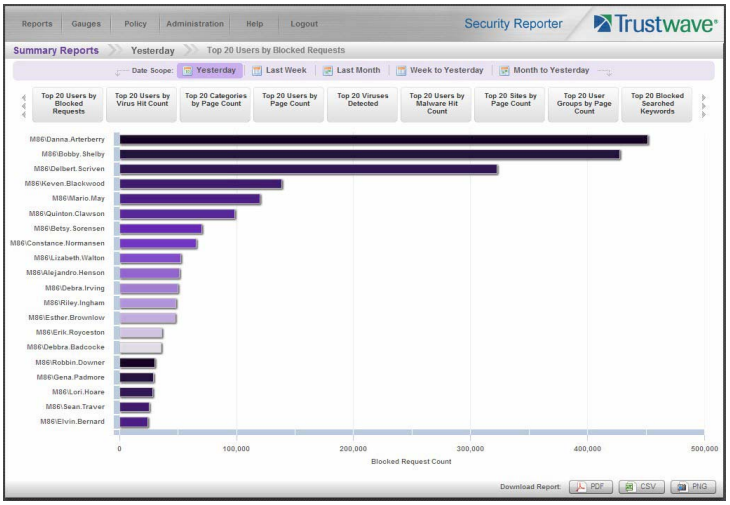
Tip: In any box or screen in the application, press the Tab key on your keyboard to move to the next field. To return to a previous field, press Shift-Tab.

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

6. Click **Login** to display the Summary Reports panel of the Report Manager user interface (if you have permissions to view this panel), or the Drill Down Report Wizard Summary Report panel of the Report Manager user interface (if you do not have permission to view the Summary Report panel):



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 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.

1.6.2.1.1 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.

1.6.2.1.2 Expired Passwords

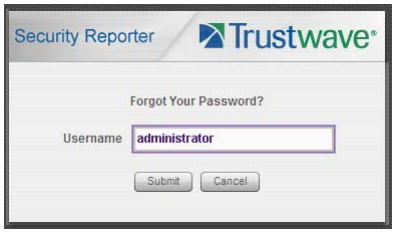
If your password has been set by a global administrator to expire after a specified number of days (System Configuration: Database | Optional Features), upon clicking the **Login** button, the Update Password window opens:

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.

1.6.2.1.3 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:



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:

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.

1.6.2.1.4 Single Sign-On Access

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

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

1.6.2.1.5 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 Security 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.

1.6.2.2 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: Evaluation Mode for information about using the Security Reporter in evaluation mode and/or converting the application to registered mode.

1.6.2.2.1 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:

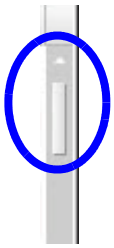
- **Reports** - Hover over this link to open the Reports menu. Global and group administrators can click any Report menu item to view or generate a report, or schedule a report to run.
- **Gauges** (available for Web Filter) - Hover over this link to view menu options for setting and managing URL and bandwidth gauges, and end user Internet activity.
- **Policy** (available for Web Filter) - Hover over this link to view menu options for setting and maintaining policies used for triggering warnings when gauges approach their upper threshold limits.
- **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 in the .pdf format for this application
  - **About...** - Clicking this link opens a pop-up window containing information about the current software Version, and hardware Serial number if this SR is running on 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).

1.6.2.2.2 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.

1.6.2.2.3 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.

1.6.2.2.4 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).

1.6.2.3 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 User Guide. Failure to properly shut down the server can result in data being lost or corrupted.

1.6.3 Technical Support / Product Warranties

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

2 System Configuration Section

2.1 Introduction

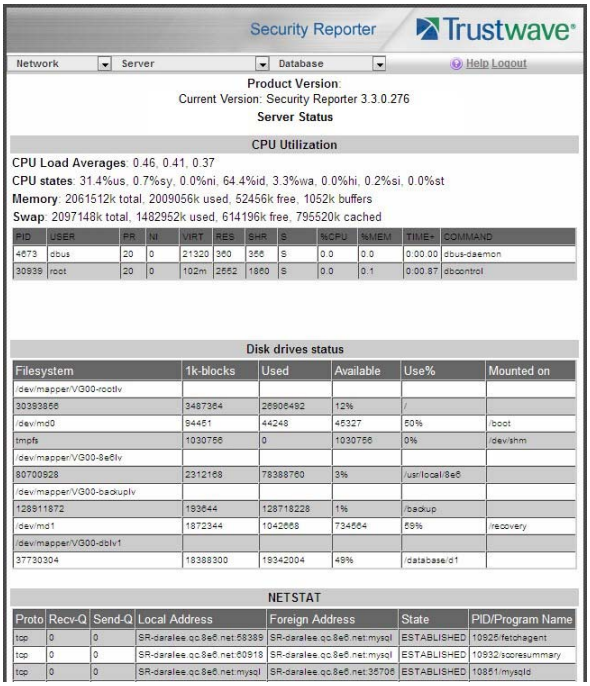
This section of the user guide provides instructions to a global administrator on configuring and managing the SR server.

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

- Executes Installation procedures defined in the Installation Guide booklet
- Provides a suitable environment for the server, including:
    - High speed, HTTPS link to the current logging device
    - Power connection protected by an Uninterruptible Power Supply (UPS)
    - High speed access to the server by authorized client workstations
- Sets up administrators for receiving automatic alerts
- Updates the server with software updates supplied by Trustwave
- Analyzes server statistics
- Utilizes diagnostics for monitoring the server status to ensure optimum functioning of the server
- Configures and administers migration of data from an earlier version of SR (if applicable)

2.2 Access System Configuration

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 (using port 8843) and displays the Server Status screen showing the current status of the SR.

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

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

2.3 Configuring the Server

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

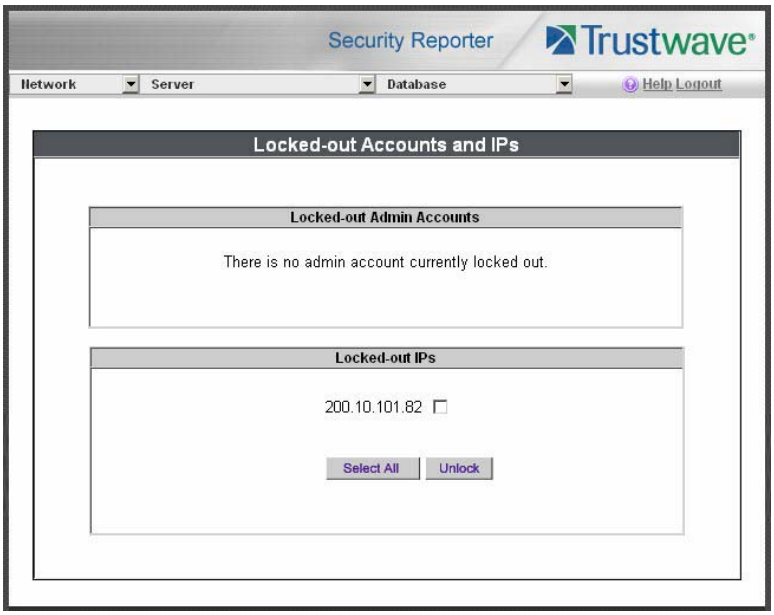
Tip: When making a complete configuration in the System Configuration administrator console, Trustwave recommends you navigate from left to right (Network to Server to Database) in choosing your menu options.

2.3.1 Network Menu

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

2.3.1.1 Locked-out Accounts and IPs screen

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



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

2.3.1.1.1 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 a check box. The Select All and Unlock buttons display at the bottom of the frame.

2.3.1.1.2 Unlock Accounts, IP addresses

To unlock an account/IP address in a frame:

1. Click the check box corresponding to the username/IP address.

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

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

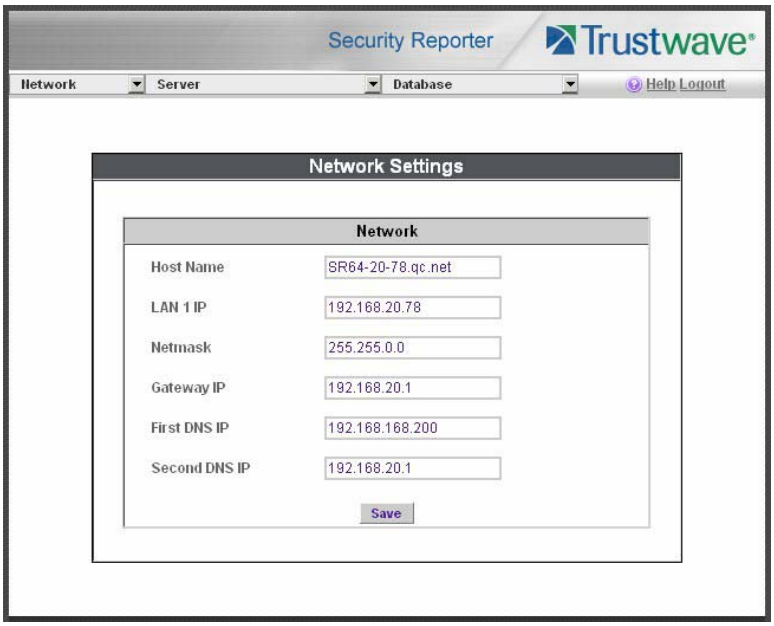
- IP: 'x.x.x.x' has been successfully unlocked.

Note: In the text above, 'xxx' and 'x.x.x.x' represents the unlocked username/IP address.

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

2.3.1.2 Network Settings screen

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



2.3.1.2.1 Set up/Edit IP Addresses

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

1. Enter or edit an IP address in each appropriate field:
   - In the **Host Name** field, enter the address or URL that will be used for accessing the System Configuration administrator console. This entry should include the full, qualified domain name, and the "host" name for the box (i.e. reporter.myserver.com).
   - In the **LAN 1 IP** field, enter the IP address of the SR server on your Local Area Network (LAN 1).
   - In the **Netmask** field, enter the netmask that will define the traffic designated for the LAN.
   - In the **Gateway IP** field, enter the IP address for the default router that will be the main gateway for the entire network segment.

- In the **First DNS IP** field, enter the IP address of the primary Domain Name System (name server). The server will use this IP address to identify other IP addresses on the system, including its own IP address.
- In the **Second DNS IP** field, enter the IP address of the fallback DNS.

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

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

2.3.1.3 Routing Table screen

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

2.3.1.3.1 View a List of Routers

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

2.3.1.3.2 Add a Router

1. In the **Destination** field, enter the IP address of the network to which data packets will be forwarded.
2. At the **Network Mask** pull-down menu, specify the number (1-32) of the subnet mask that will be used for grouping IP addresses on the same local network.

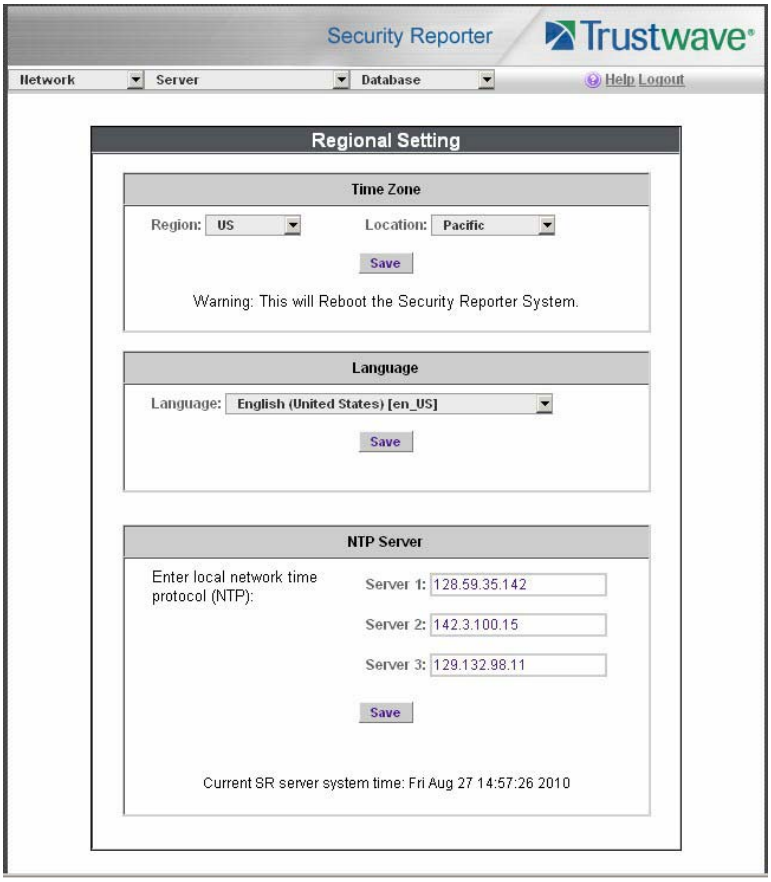
3. In the **Gateway** field, enter the IP address of the portal to which data packets will be transferred to and from the Internet.
4. Click the **Add** button to include your entry in the table. If you have another router to add, follow steps 1-4.
5. Click the **Back** button on the confirmation screen to return to the Routing Table screen.

2.3.1.3.3 Delete a Router

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

2.3.1.4 Regional Setting screen

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



2.3.1.4.1 Specify the Time Zone

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

Caution: 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.

2.3.1.4.2 Specify the Language Set

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

2.3.1.4.3 Specify Network Time Protocol Servers

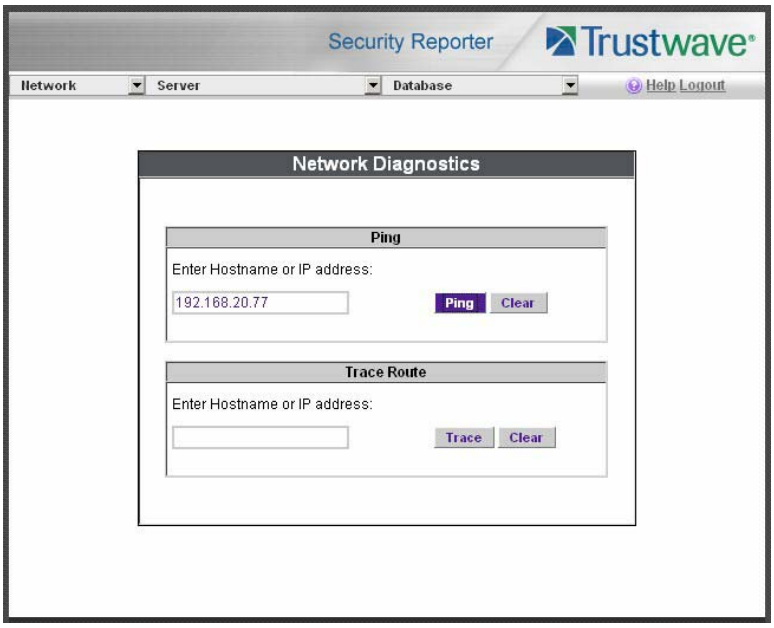
IP addresses of servers running Network Time Protocol (NTP) software are entered in the Server fields, and the Current SR server system time (day, date, HH:MM:SS time format, and year) displays below. NTP is a time synchronization system for computer clocks throughout the Internet. Your SR server will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

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

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

2.3.1.5 Network Diagnostics screen

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

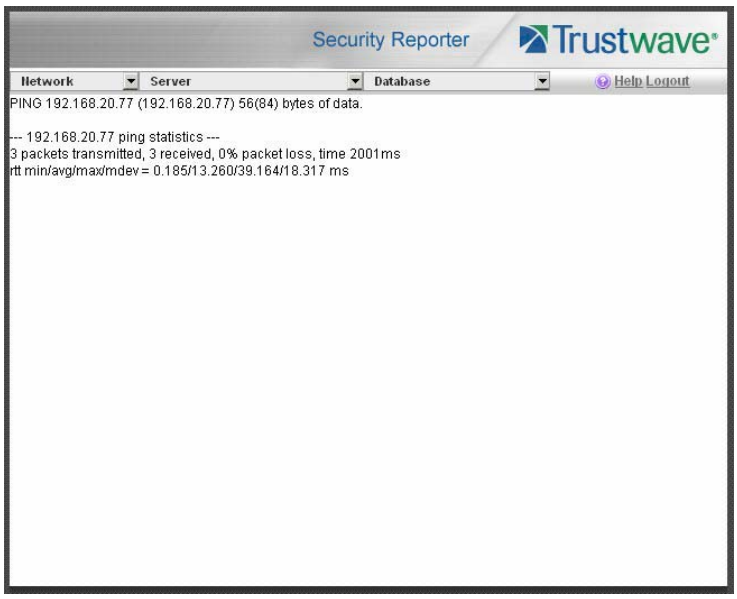


2.3.1.5.1 Ping

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

1. In the Ping frame, enter the IP address or hostname of the specific Internet address to be contacted (pinged).

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



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

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

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

2.3.1.5.2 Trace Route

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

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

1. In the Trace Route frame, enter the IP address or hostname of the specific Internet address to be validated.

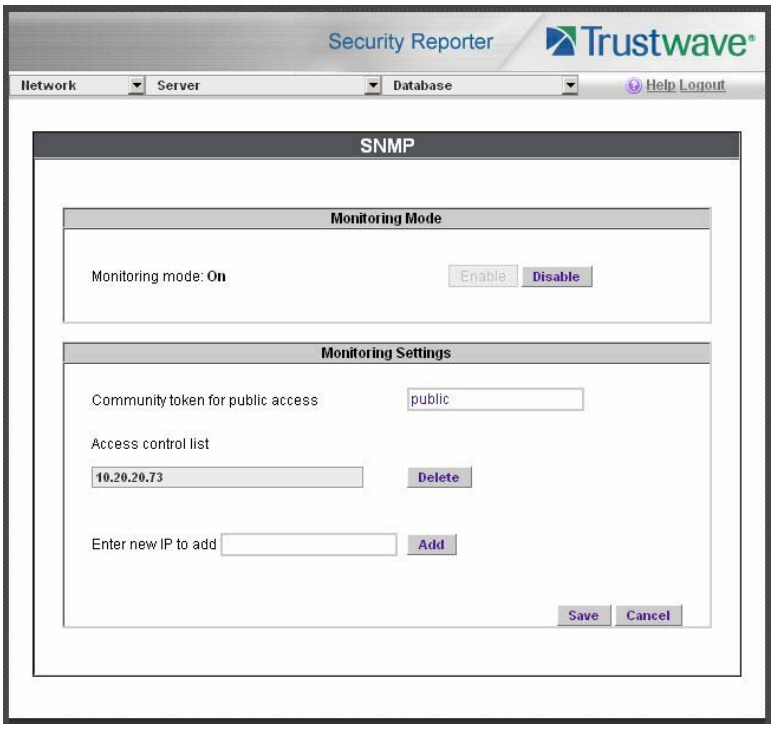
2. Click the **Trace** button to display the results found by the server, as shown on the sample screen:

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

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

2.3.1.6 SNMP screen

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



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

2.3.1.6.1 Enable SNMP

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

2.3.1.6.2 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 would use when requesting access.

2.3.1.6.3 Create, Build the Access Control List

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

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

2.3.1.6.4 Maintain the Access Control List

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

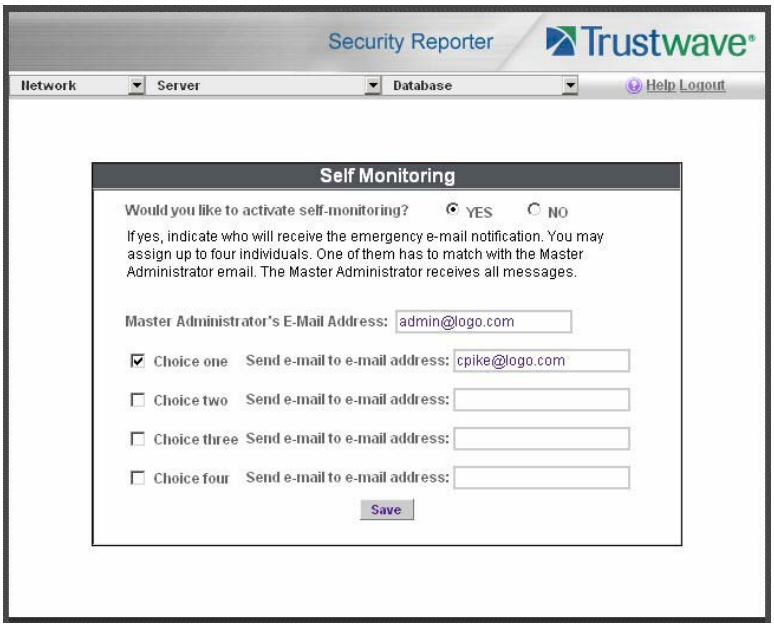
2.3.2 Server Menu

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

Note: If running the SR as a virtual machine, the Hardware Failure Detection screen displays a message indicating the server is not a RAID server.

2.3.2.1 Self Monitoring screen

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



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.

2.3.2.1.1 View a List of Contact E-Mail Addresses

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

2.3.2.1.2 Set up and Activate Self-Monitoring

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

2.3.2.1.3 Remove Recipient from E-mail Notification List

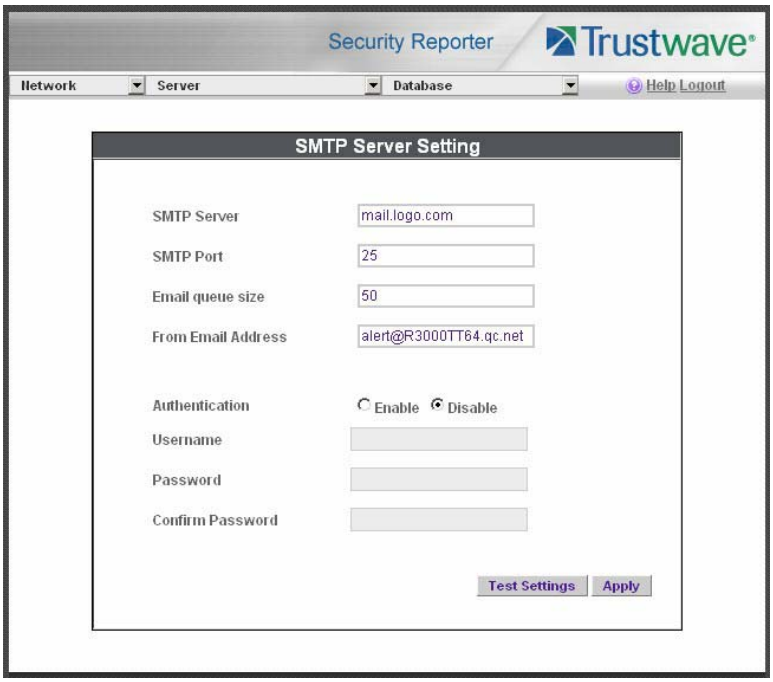
1. To stop sending emergency notifications to an e-mail address set up in the list, remove the check mark from the check box corresponding to the appropriate e-mail address.
2. Click the **Save** button to remove the recipient's name from the e-mail list. The Master Administrator and any remaining e-mail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

2.3.2.1.4 Deactivate Self-Monitoring

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

2.3.2.2 SMTP Server Setting screen

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



2.3.2.2.1 Enter, Edit SMTP Server Settings

1. Enter the **SMTP Server** name, for example: **mail.logo.com**.
2. By default, the **SMTP Port** number used for sending email is *25*. This should be changed if the sending mail connection fails.
3. By default, the **Email queue size** is *50*. This can be changed to specify the maximum number of requests that can be placed into the queue awaiting an available outbound connection.
4. In the **From Email Address** field, enter the email address of the server that will be sending alert email messages to designated administrators.
5. By default, **Authentication** is disabled. Click "Enable" if a username and password are required for logging into the SMTP server. This action activates the fields below.

   Make the following entries:

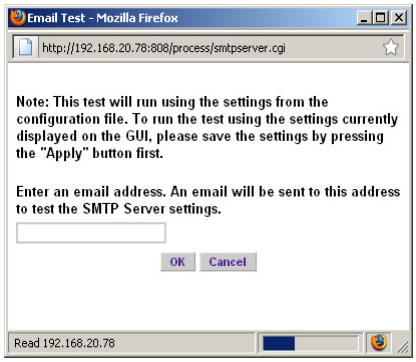
   a. Enter the **Username**.

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

2.3.2.2.2 Verify SMTP Settings

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

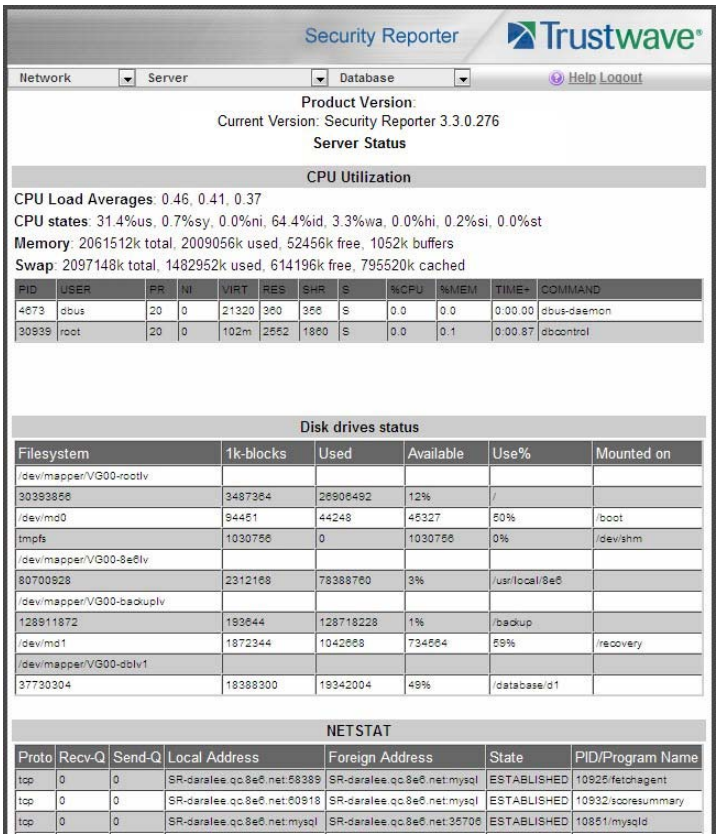
1. Click **Test Settings** to open the dialog box:



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

2.3.2.3 Server Status screen

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



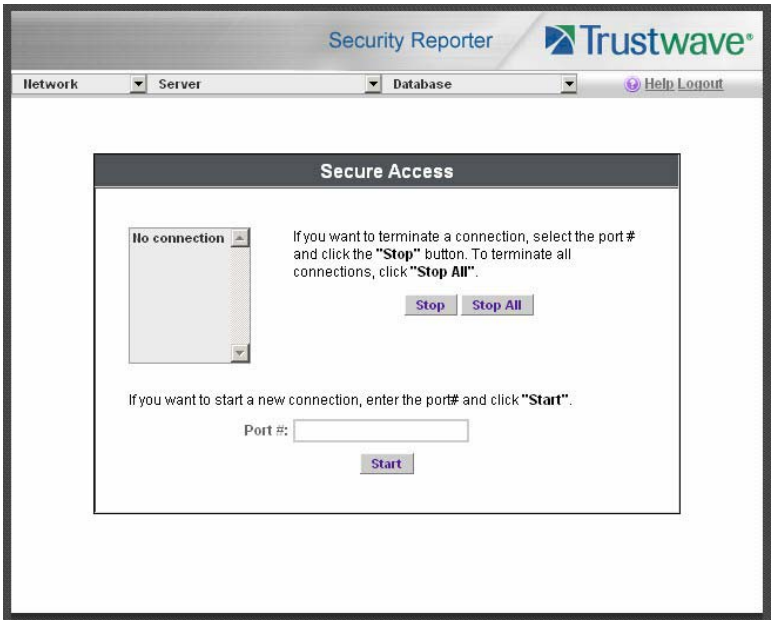
2.3.2.3.1 View the Status of the SR Server

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

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

2.3.2.4 Secure Access screen

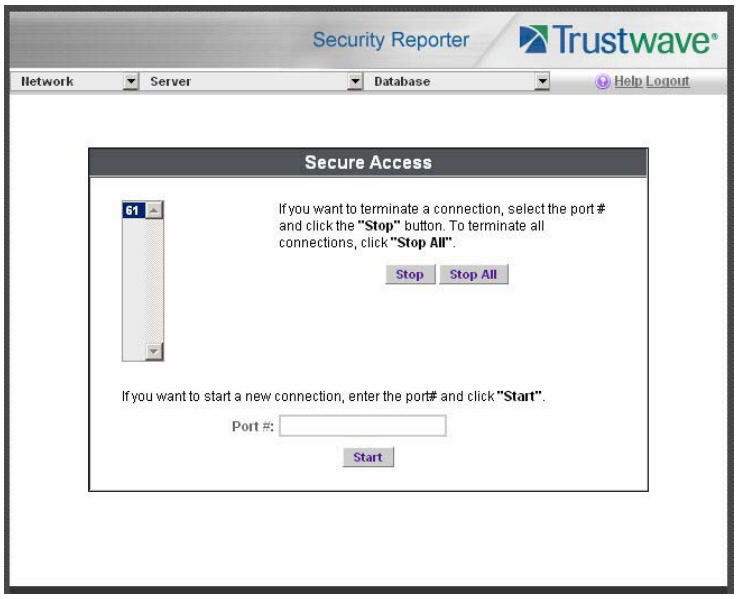
The Secure Access screen displays when the Secure Access option is selected from the Server menu. This screen is primarily used by Trustwave technical Assistance Center representatives to perform maintenance on your server, if your system is behind a firewall that denies access to your server.



2.3.2.4.1 Activate a Port to Access the SR Server

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

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



2.3.2.4.2 Terminate a Port Connection

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

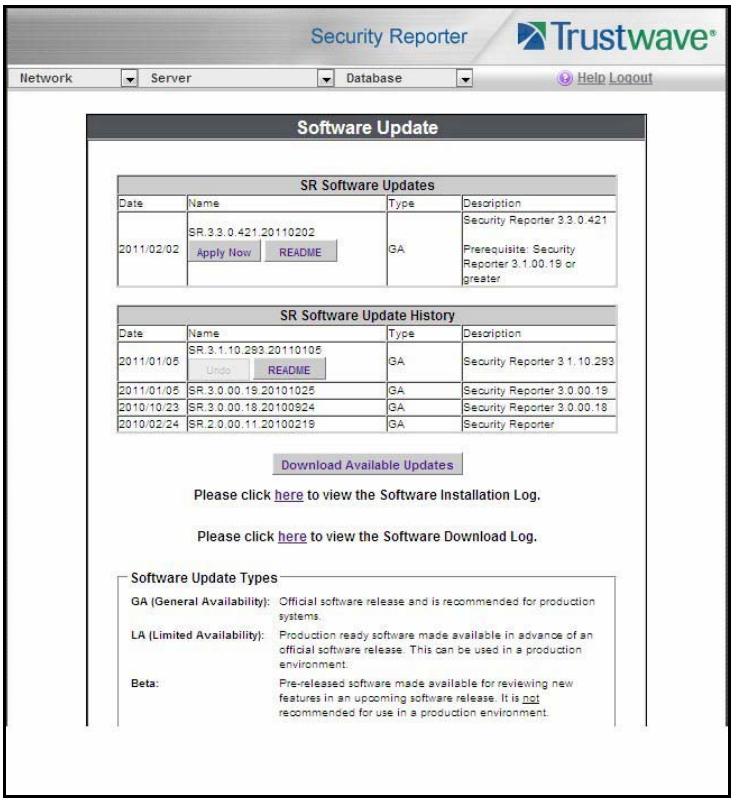
2.3.2.4.3 Terminate All Port Connections

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

2.3.2.5 Software Update screen

The Software Update screen displays when the Software Update option is selected from the Server menu. This screen is used for updating the SR with software updates supplied by Trustwave, verifying the download and/or installation of software updates on the SR, and viewing a list of software updates currently available and/or previously installed on the SR. This screen is also used for accepting LA/Beta

software downloads, if choosing to download Limited Availability (LA) and/or Beta updates for previewing software features to be included in the General Availability (GA) release to be distributed to all SRs.



Note: Definitions for Software Update Types (GA, LA, and Beta) are provided in the frame at the bottom of this screen.

General Availability (GA) software updates are supplied to all current SR units. Limited Availability (LA) and/or Beta software updates are available to SR units that have the feature to download LA and/or Beta software updates enabled, as described in this sub-section and the Software Update Setting screen sub-section.

2.3.2.5.1 View Software Update Criteria

View Installed Software Updates

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

View Available Software Updates

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

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

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

2.3.2.5.2 Install a Software Update

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

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

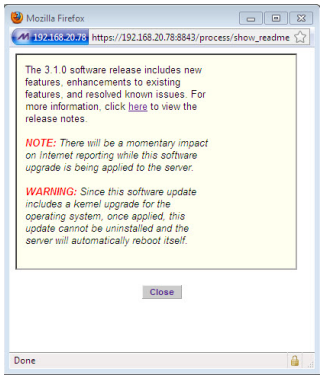
General Software Installation Procedures

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

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

README:

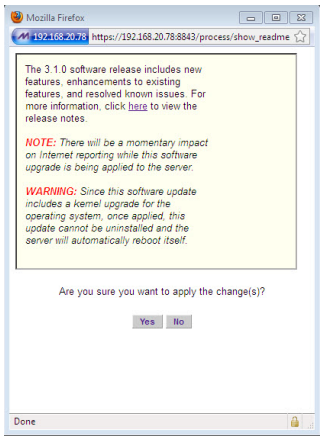
1. Click **README** to open a window containing information about the software release:



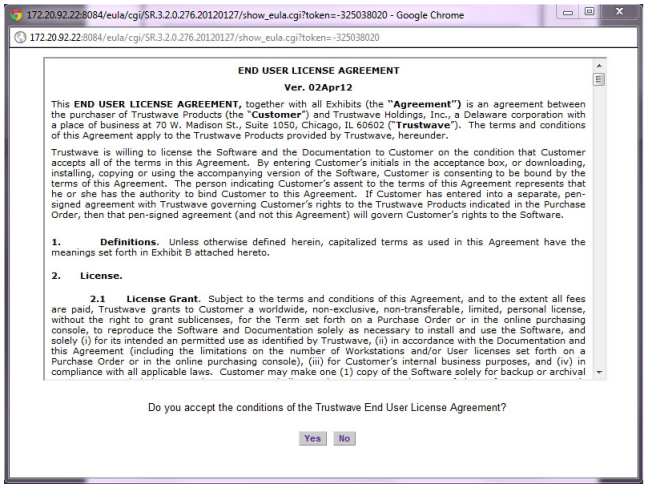
2. After reading the contents of the software release, click **Close** to close the window.

Apply Now:

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

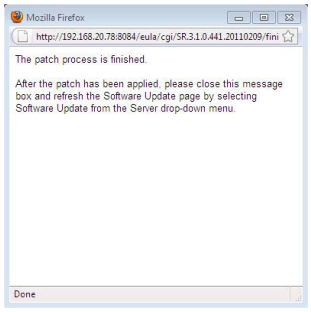


2. Click **Yes** to open the EULA dialog box:



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

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



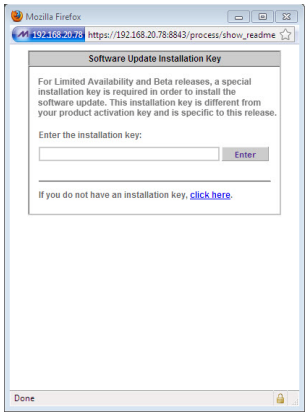
Note: After installing the software update, if a message displays that informs you to reboot the server, you should select the **Restart Software** option on the Shut Down screen.

First Time LA/Beta Software Install Procedures

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

1. In the SR Software Updates frame, two buttons are available for the LA/Beta software update: README and Apply Now.

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



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

Note: The installation key is specific to this software release and is **not** the same as the product activation key which is used for activating the Web Filter to receive ongoing updates.

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

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

Figure 1: Limited Availability acceptance dialog box

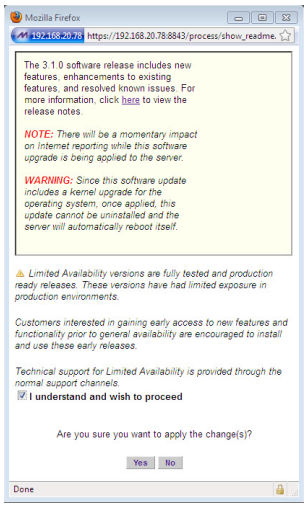
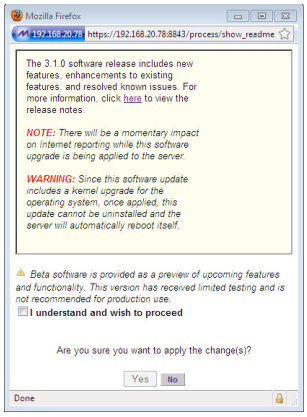


Figure 2: Beta acceptance dialog box



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.

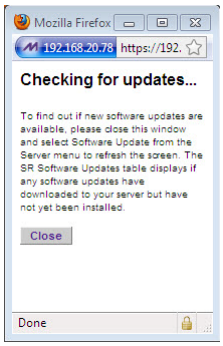
   A successful software installation displays a completion message with notification that the Software Update screen needs to be refreshed via Server | Software Update in order to display the latest software update in the SR Software Update History frame.

2.3.2.5.3 Uninstall the Most Recently Applied Update

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

2.3.2.5.4 Download Available Updates

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

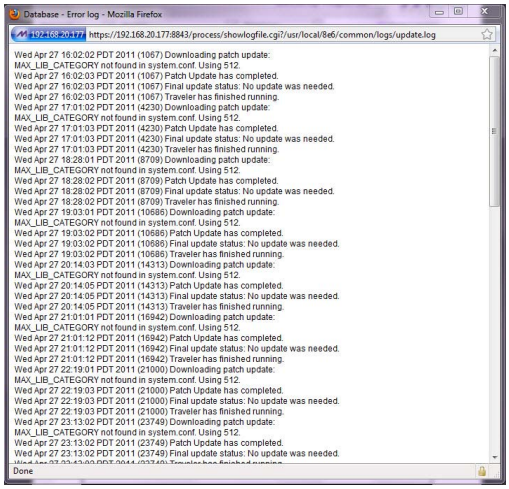


2. Click **Close** to close the window.

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

2.3.2.5.5 View Software Download Log

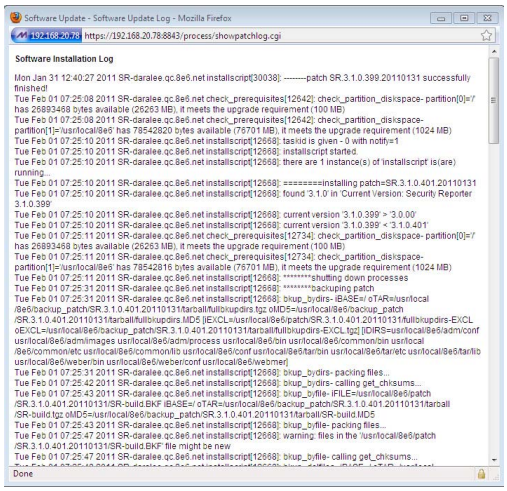
1. To determine whether software updates are being downloaded to the SR, click the Software Download Log link named "**here**" to open the window that shows criteria on the latest software download attempts:



2. Click **Close** to close the window.

2.3.2.5.6 View Software Installation Log

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



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

2.3.2.6 Software Update Setting screen

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

2.3.2.6.1 Specify Proxy Settings

1. In the Proxy Setting frame, by default "Disable" is selected. Click "Enable" if the server is in a proxy server environment.
2. In the **Proxy Server** field, enter the 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. Enter the same password in the **Password** and **Confirm Password** fields.

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

2.3.2.6.2 Download LA, Beta Software Updates

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

Enable LA Software Downloads

By default, the "Limited Availability" 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 SR Software Updates table in the Software Update screen.

If this SR does not have the "Limited Availability" check box enabled, click the "Limited Availability" check box.

Enable Beta Software Downloads

Click the "Beta" check box to enable this SR to receive Beta software updates on an SR used in a non-production environment.

2.3.2.6.3 Save Settings

Click **Save** to save your settings.

2.3.2.7 Shut Down screen

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

2.3.2.7.1 Server Action Selections

- **Restart the Server's Hardware** - The Restart Hardware option should be selected if the server needs to be rebooted—for example, when applying certain hardware configurations. You will need to use this option after an IP address has been entered in the Network Settings screen. 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.

- **Shut Down the Server's Hardware** - The Shutdown Hardware option should only be selected if the server's hardware must be completely shut down—for example, if the server will be physically relocated.

When this option is selected, the server shuts off, and 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.

- **Restart the Server's Software** - The Restart Software option should be selected if daemons fail to run and/or the database needs to be started again. When this option is selected, the MySQL database is rebooted.
- **Shut Down the Server's Software** - The Shutdown Software option should be selected if the MySQL database needs to be shut off and no log files transferred to the server.

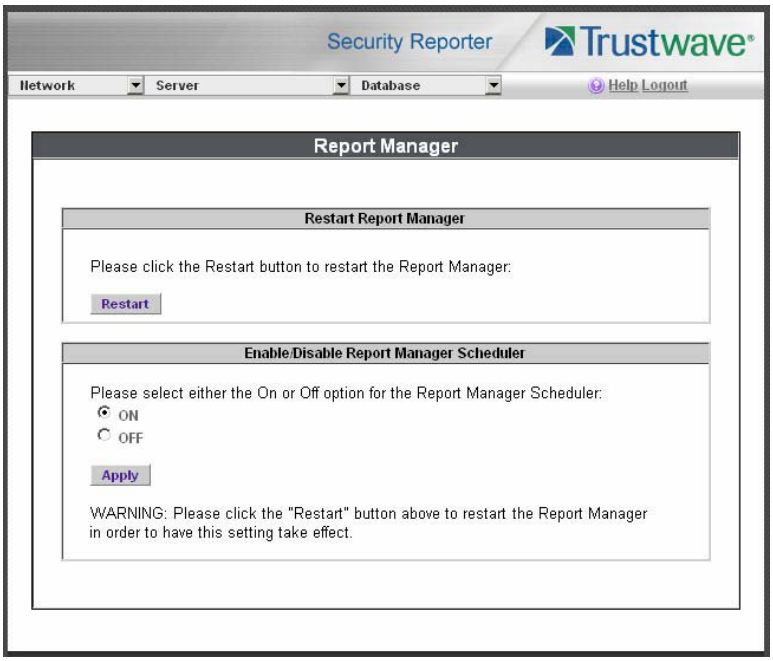
2.3.2.7.2 Perform a Server Action

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

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

2.3.2.8 Report Manager screen

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



2.3.2.8.1 Restart the Report Manager

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

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

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

2.3.2.8.2 Enable/Disable the Report Manager Scheduler

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

2.3.2.9 Hardware Failure Detection screen

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

This screen displays the image for the type of SR appliance used: 300 series Equus model with two hard drives (Figure 3); 500 and 700 series Equus model with four hard drives (Figure 4); 505 IBM model with two hard drives (Figure 5), or 700 series IBM model with an eight hard drive capacity, but using only four hard drives to run SR, with one spare hard drive in the event of a drive failure (Figure 6).

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

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

2.3.2.9.1 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, and instructions for replacing the hard drive display below:

1. Identify the failed drive based on the information provided on the GUI.
2. Replace the failed drive.
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: Hardware Failure Detection screen, 300 model

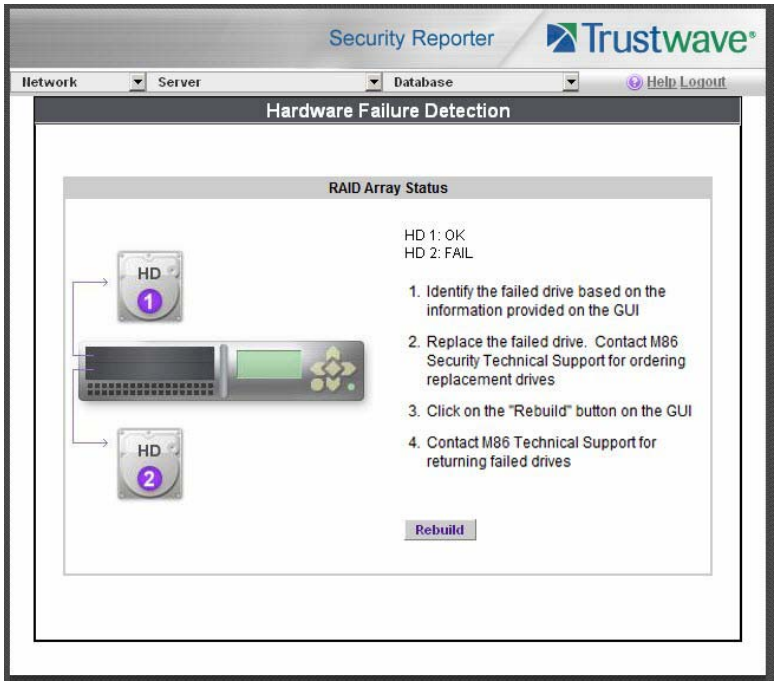
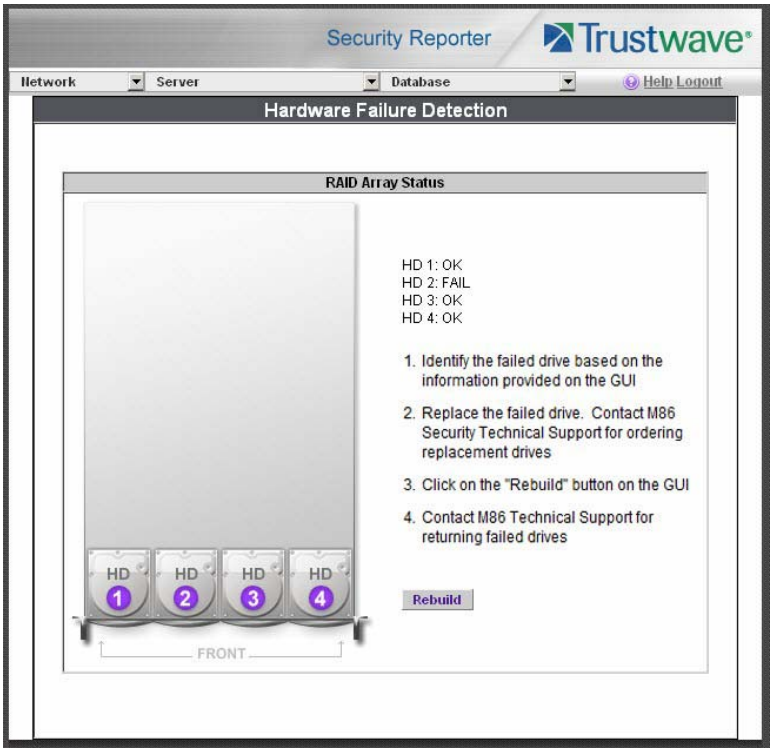


Figure 4: Hardware Failure Detection screen, 500, 700, 730 model



2.3.2.9.2 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 pertains to a hard drive that ceases to operate or fails to rebuild upon insertion in the carrier, and the latter status pertains 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. Instructions for replacing the hard drive display below:

1. Identify the failed drive based on the information provided on the GUI.
2. Replace the failed drive.
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: Hardware Failure Detection screen, 505 IBM model

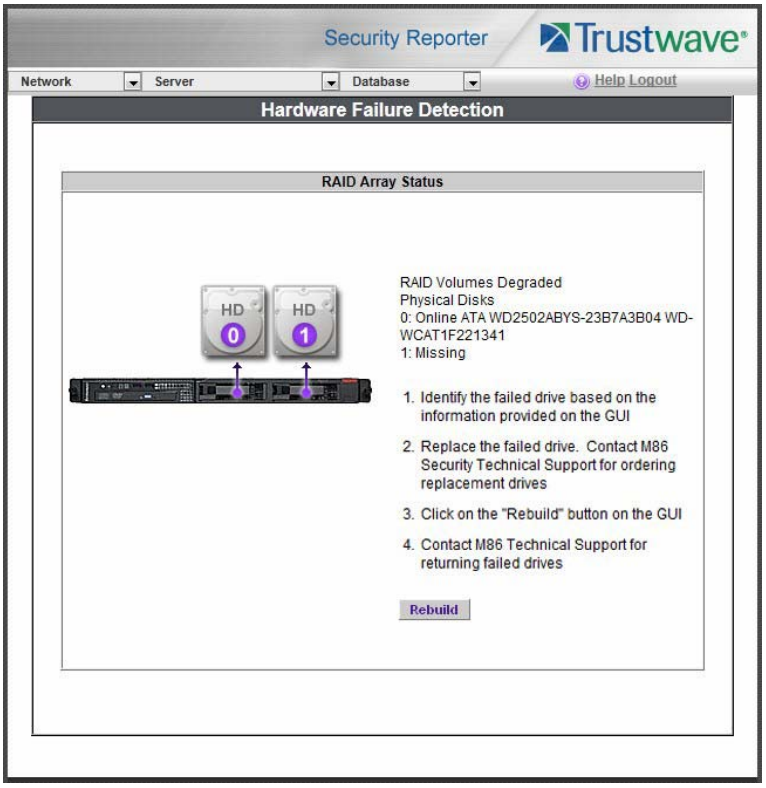
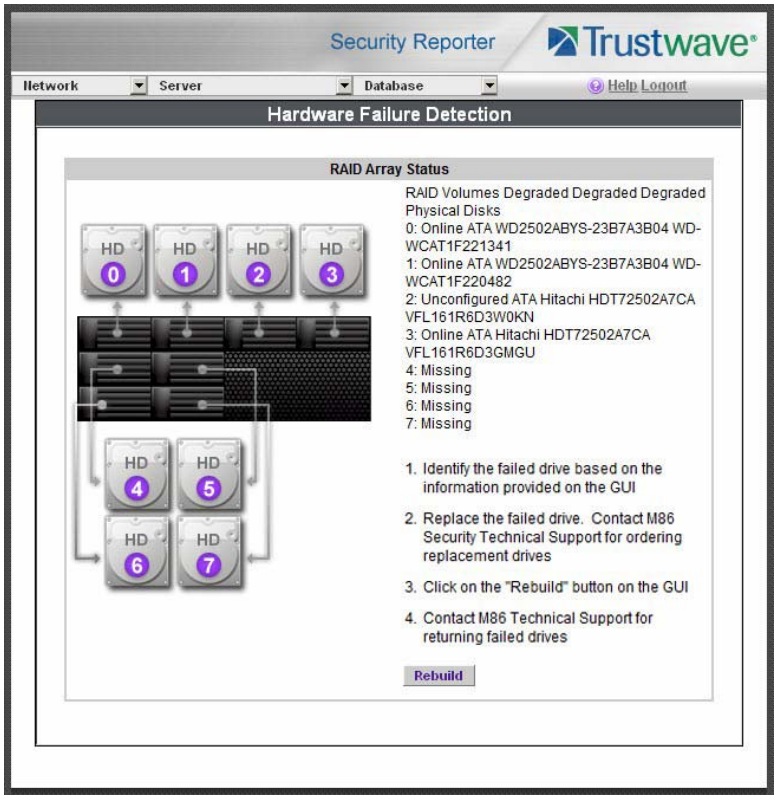


Figure 6: Hardware Failure Detection screen, 705 or 735 IBM model

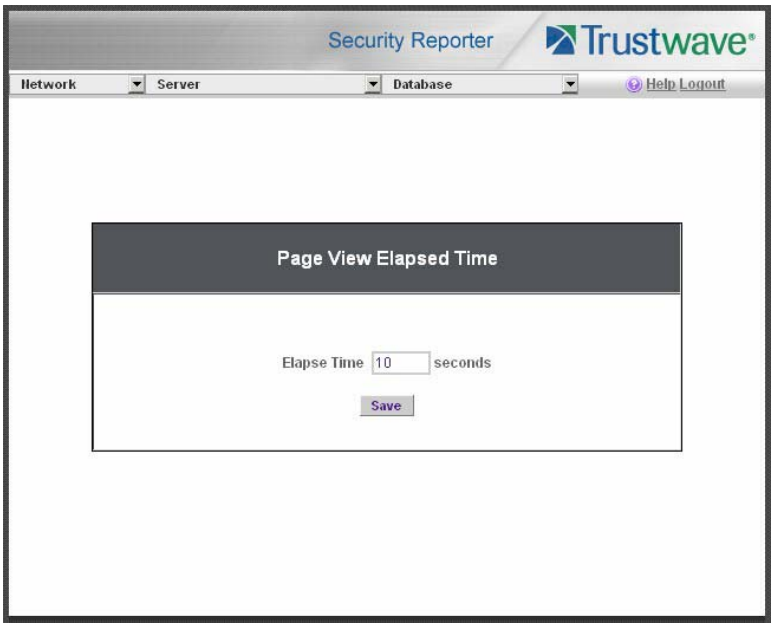


2.3.3 Database Menu

The Database pull-down menu includes options for configuring the database. These options are: Elapsed Time, Page Definition, Tools, Expiration, and Optional Features.

2.3.3.1 Page View Elapsed Time screen

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



2.3.3.1.1 Establish the Unit of Elapsed Time for Page Views

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

2.3.3.1.2 Elapsed Time Rules

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

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

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

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

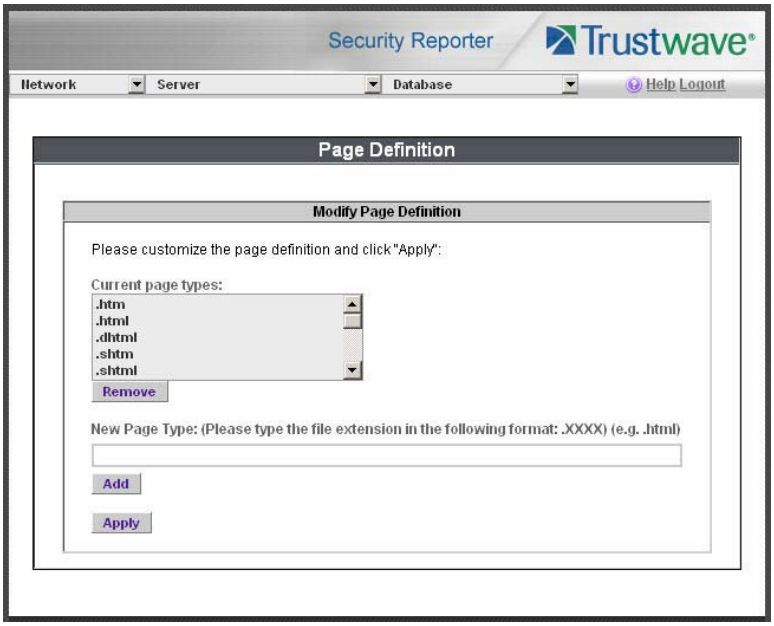
For example, if the value entered at the Elapse Time field is 10 seconds and the user remains at a Web site for 12 seconds, two visits to that site will be logged for him/her.

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

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

2.3.3.2 Page Definition screen

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



2.3.3.2.1 View the Current Page Types

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

2.3.3.2.2 Remove a Page Type

To remove a page type from the detail report:

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

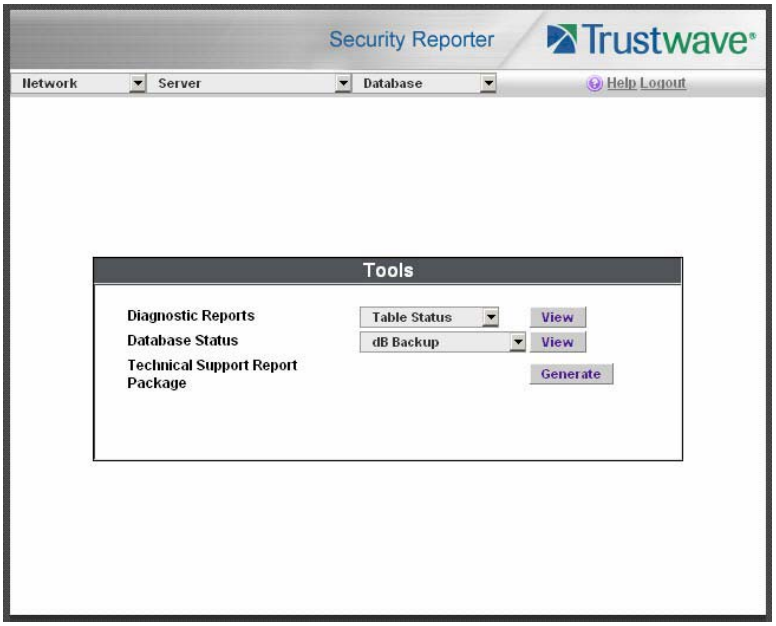
2.3.3.2.3 Add a Page Type

To add a page type in the detail report:

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

2.3.3.3 Tools screen

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



The following options are available on this screen:

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

2.3.3.3.1 View Diagnostic Reports

1. Choose a report from the pull-down menu (Table Status, Process List, Full Process List, Tables, or Daily Summary).
2. Click the **View** button to view the selected diagnostic report in a window:
   - **Table Status** - This report contains a list of Client table names, and columns of statistics on each table, such as type, size, number of rows, and time created and updated.
   - **Process List** - This report shows a list of current SQL queries in the database, in an abbreviated format.

- **Full Process List** - This report shows a list of current SQL queries in the database, in the full format that includes all columns of data.
- **Tables** - This report contains a list of the names of tables currently in the database.
- **Daily Summary** - This report shows the date range of summary tables currently in the database.

3. Click the "X" in the upper right corner of the window to close it.

2.3.3.3.2 View Database Status Logs

1. Choose a database status log from the pull-down menu.
2. Click the **View** button to view the selected database status log in a window:
   - **db Tool** - This log shows information about system checks performed on disk usage, free memory, unprocessed files, and daemons.
   - **db Traffic** - This log provides information about the daily traffic table.
   - **Error Entry - Web Filter** (for Web Filter) - This log displays a list of Web Filter query errors.
   - **File Watch Log** (for Web Filter) - This log shows a list of records that were imported from one machine to another.
   - **MYSQL Log** - This log provides information pertaining to the MySQL server.
   - **Partitioner** - This log displays results of server partitioning for database expiration.
   - **Software Installation Log** - This log gives information about recent software updates that have installed on this SR.
   - **Software Download Log** - This log gives information about recent software updates that have downloaded to this SR.
   - **Summarization** - This log shows a summarization of activities from the summarizer database tool.
   - **SWG Log Importing** (for SWG) - This log displays results of SWG archive log importation.
   - **WF Log Importing** (for Web Filter) - This log displays results of WF archive log importation.
3. Click the "X" in the upper right corner of the window to close it.

2.3.3.3.3 Generate Technical Support Report Package

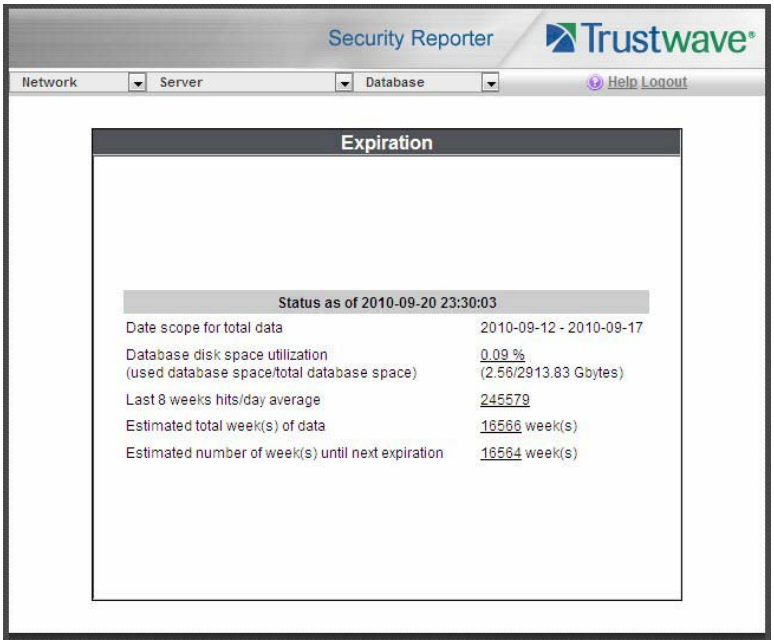
When troubleshooting the SR unit with Trustwave Technical Support, a diagnostic report can be generated and submitted to Trustwave for further analysis. This report contains files with information about the 'health' of the unit.

1. At the **Technical Support Report Package** field, click **Generate** to begin generating the report package.
2. After the package has generated, the "Successfully generated tech support log" window opens with the message to download the file to email to the Trustwave Technical Assistance Center. Click **Download** to download the .tgz package to your machine.

3. Email the package to the Trustwave Technical Assistance Center as instructed by your Trustwave technical support representative.

2.3.3.4 Expiration screen

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



Note: The database is backed up automatically each week,

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

2.3.3.4.1 Expiration Rules

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

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

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

Once data expires, it cannot be recovered.

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

2.3.3.4.2 View Data Storage Statistics

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

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

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

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

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

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

Note: If the server has not yet expired any data, a "0" (zero) displays in this field.

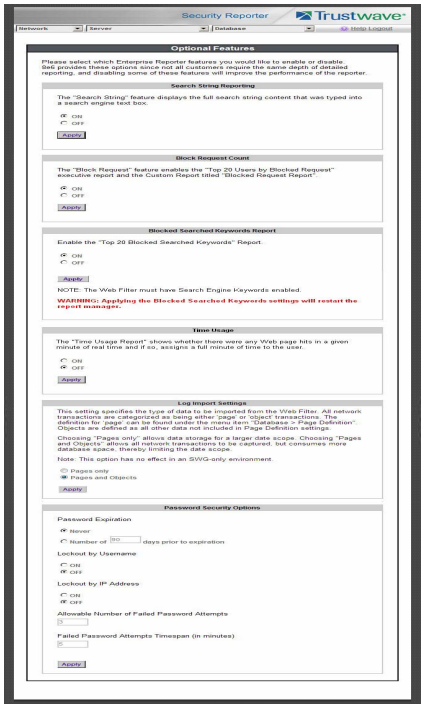
- **Estimated total week(s) of data** - The estimated number of weeks of data the server will store. This number is affected by end user hits/day and the storage capacity of the server.
- **Estimated number of week(s) until next expiration** - The estimated number of weeks from this week that data on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

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

2.3.3.5 Optional Features screen

The Optional Features screen displays when Optional Features is selected from the Database menu. This screen is used to specify log import settings (for WF only). This screen also is used for configuring password security rules to affect users who access the SR user interface.

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



2.3.3.5.1 Enable Page and/or Object Count

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

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 **Apply** to apply your setting.

2.3.3.5.2 Enable, Configure Password Security Option

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

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

1. Enable any of the following options:

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

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

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

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

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

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

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

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

2.4 Migrating Data

If this SR has been updated from version 3.2 to version 3.3, data formats are changed. If you want to report on historical data using the version 3.3 reporting framework, you must migrate the data to the new format. Data from the old version can be backed up, then migrated to the new format.

Migrated data is available for reporting in the current Report Manager and scheduled reports.

Data that is not migrated can still be accessed using a limited version of the version 3.2 Report Manager, which is also included in this release. For more details, see Section 2.5.

2.4.1 Choosing What To Migrate

Depending on the amount of data being migrated, migration could be a time-consuming process creating additional load on the SR. To minimize this load, Trustwave suggests that you leave most or all of the summarized historical data in the version 3.2 format and use the 3.2 Report Manager to access it (for details, see Section 2.5).

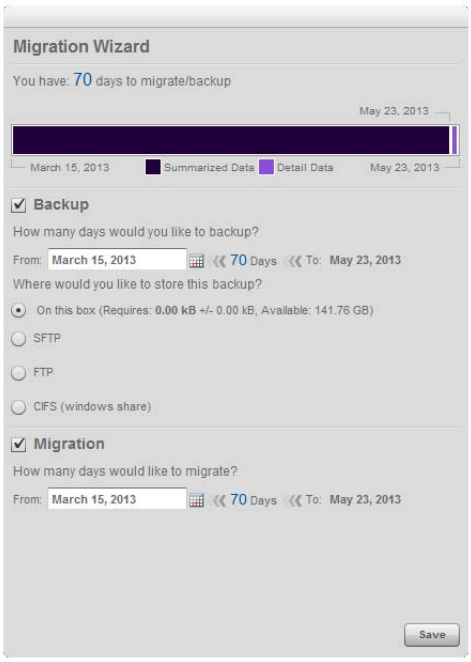
Note: You should migrate any un-summarized data. This data will not be available for reporting in the old interface. If you do not migrate it, it will not be available for any reporting.

If you want to make historical data available in the new framework, first migrate the data for a short duration to determine the speed of migration and effect on server load.

You can change the migration settings at any time, as described below.

2.4.2 Migration Wizard

When you first log on to SR 3.3 as a Global administrator, you are presented with a migration wizard window:



This window shows the available summarized and detail (unsummarized) data that you can back up and migrate. Backup will be completed before migration.

Note: After you have made your initial selections in this window and saved them, you can revisit and edit your selections later. Even if you choose to initially opt out of migration and/or backup, you can configure these options at a later time.

To configure backup:

1. Click to check the box **Backup.**
2. Use the calendar control to select the starting (oldest) date for backup. Backup always ends with the latest available data.
3. Choose a location for the backup by selecting a radio button:
   - **On this box:** This option stores the backup on the SR server. The estimated required space and available space is shown.
   - SFTP: This option copies the data to another server using SFTP. When you select this option, you can enter a user name password, host name, port (default port 22), and path on the remote server. After entering this information, click **Test** to validate access.
   - FTP: This option copies the data to another server using FTP. When you select this option, you can enter a user name password, host name, port (default port 21), and path on the remote server. After entering this information, click **Test** to validate access.
   - CIFS (Windows share): This option copies the data to another server over CIFS. When you select this option, you can enter a user name password, host name, and path on the remote server. After entering this information, click **Test** to validate access.

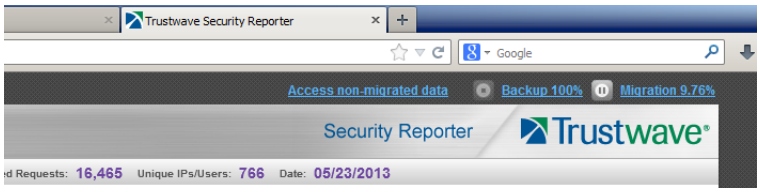
To configure migration:

1. Click to check the box Migration.
2. Use the calendar control to select the starting (oldest) date for migration. Migration always ends with the latest available data.

Once you have configured the above settings, click Save to start the backup and migration processing, and to access the main Report Manager window.

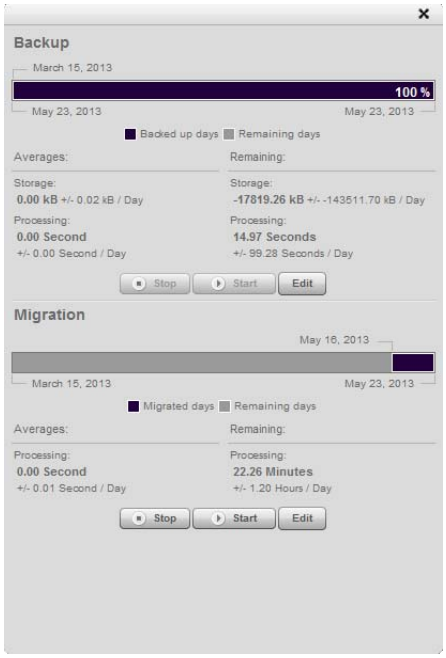
2.4.3 Monitoring Migration Progress

If you are logged on as a Global Administrator, the progress of backup and migration displays at the top right of the Report Manager window:



You can use the Pause, Stop, or Start button for each process to control activity. You can also adjust the schedule of a stopped process.

Click the Backup or Migration link to see details in a new window. From the new window you can stop, start, or edit settings (as in the wizard described above).



Note: Migration can consume significant processing resource, so you may want to pause it if server load is heavy.

2.5 Accessing Non-Migrated Data

All administrators can access the non-migrated data using a link at the top of the Report Manager window. If this link is not present, all data has been migrated.

Accessing the non-migrated data launches the previous (version 3.2) Report Manager.

The following functions of the Report Manager are available:

- Drill Down Reports
- Security Reports
- Saved Reports
- Report Schedule

System configuration, User Group management, and Admin Profiles are NOT available.

For assistance with the version 3.2 reports, see the Administrator Guide for version 3.2.

3 Report Manager Administration Section

3.1 Introduction

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

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

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

The Report Manager's Administration menu consists of the following options:

- Group, Profile Management - Section 3.2 explains how to set up user groups whose Internet activity will be monitored by group administrators; how to set up a global administrator account; and how to set up a group administrator account.
- Database Management - Section 3.3 explains how to configure the server to use a secure network connection; view a list of user profiles (if using a Web Filter); view administrator activity; manage the profiles of devices connected to the server; maintain Report Manager processes; analyze data storage on the server; and remove all profiles and configuration settings in the Report Manager.
- Report Configuration - Section 3.4 explains how to create and manage Custom Category Groups used for monitoring end user Internet activity, and configure general report settings.

3.2 Group, Profile Management

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

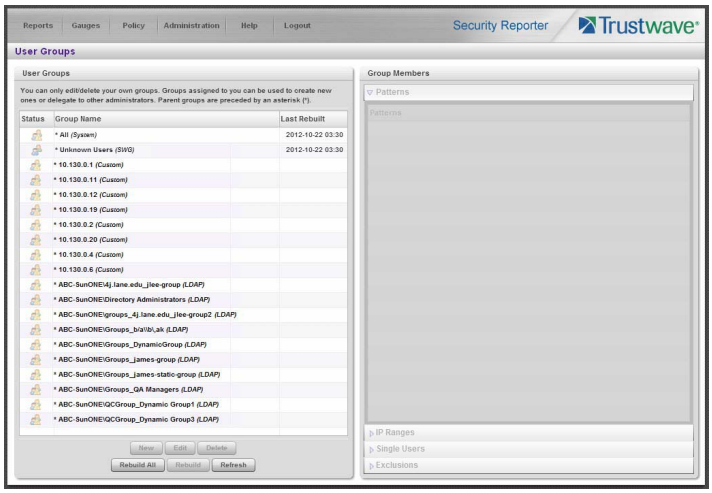
3.2.1 User Groups panel

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.

A group administrator can set up user groups once he/she is given an account with permissions to access User Groups, as detailed later.

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, which includes the User Groups sub-panel to the left and its Group Members target sub-panel to the right:



Names of user groups previously added by the administrator and corresponding user group types ("System", "Custom", "LDAP", "SWG", or "Unknown") display in the User Groups sub-panel.

For a global administrator—and any group administrator assigned this user group by a global administrator—"All *(System)*" displays as the first record in the list by default. This user group includes all user groups on this SR, both imported and non-imported. 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 Web Filter or SWG, "SWG" displays for an SWG user group, and "Unknown" displays for a user who is not included in a user group.

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

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 a Web Filter or SWG using IP group authentication or the following LDAP server types:

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

If using a Web Filter:

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

3.2.1.1 View User Group Information

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

Note: User groups are automatically rebuilt daily.

3.2.1.1.1 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.

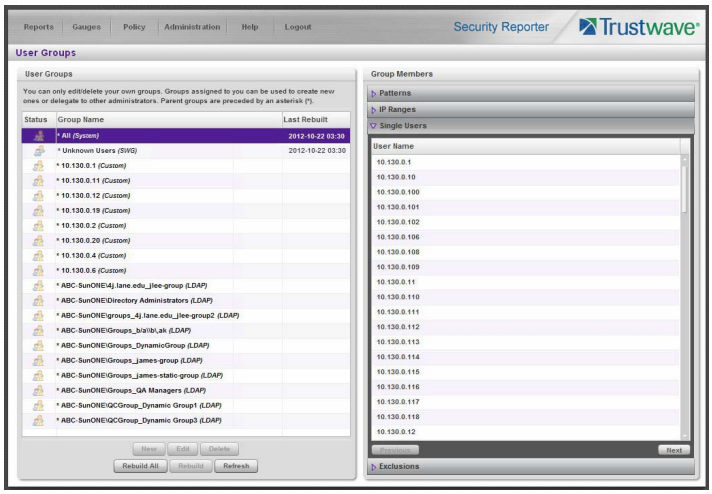
 - The user groups icon with an exclamation point indicates the user group cannot be rebuilt on demand.

3.2.1.1.2 View a list of members in a user group

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

1. Select the user group from the User Groups sub-panel by clicking its Group Name to highlight that record. Based on this selection, the Group Members sub-panel to the right becomes activated along with the following buttons in the section below, based on the status of the user group:
   - If the selected user group is ready to be rebuilt, this action activates all buttons (New, Edit, Delete, Rebuild, Rebuild All, Refresh).
   - If the selected user group was not imported and cannot be rebuilt on demand, this action activates the New, Edit, Delete, Rebuild All, and Refresh buttons.
   - If the selected user group was imported and cannot be rebuilt on demand, this action activates the New, Rebuild All, and Refresh buttons only.
2. Click an accordion in the Group Members sub-panel to open it and view pertinent information:
   - Patterns accordion - View patterns previously set up for that user group.
   - IP Ranges accordion - View Starting IP and Ending IP ranges previously added for that user group.
   - Single Users accordion - View a list of User Names and IP Addresses for individual users previously selected from the Available Users list for that user group.

- Exclusions accordion - View a list of User Names and IP Addresses for individual users previously selected from the Available Users list to be excluded from that user group.

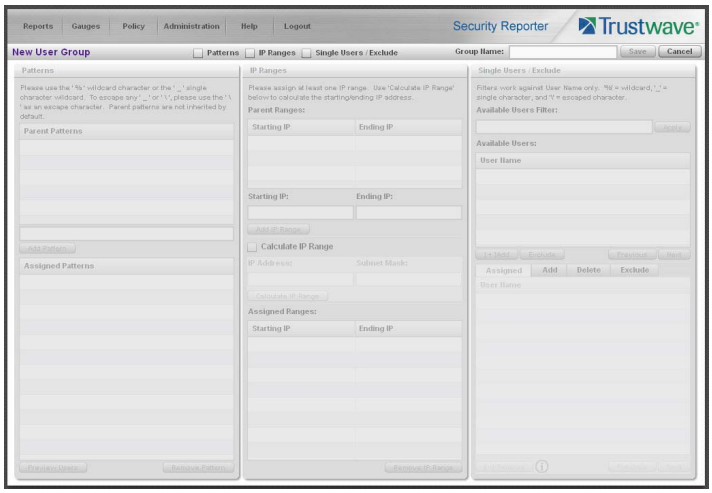


Note: If using the LDAP user authentication method, usernames display in the User Name column. If using IP groups, IP addresses of user machines display instead of usernames.

3.2.1.2 Add a User Group

To add a new user group:

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



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

3. Enter at least three characters for the **Group Name** to be used for the new user group; this action activates the Save button.

4. Click the check box(es) to activate the pertinent corresponding box(es) below: **Patterns**, **IP Ranges**, **Single Users/Exclude**.

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

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

3.2.1.2.1 Patterns sub-panel

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

Note: Since user group data is stored by 'domain\username', the pattern search will return all results found in that format.

Add a new pattern

To add a pattern to the new user group:

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

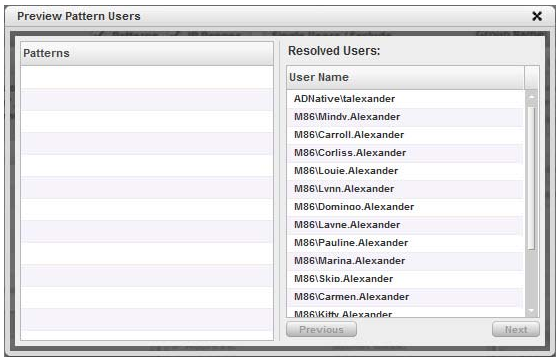
Tip: Follow steps 1 and 2 above to include additional patterns for the new user group.

View users resolved by the pattern

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

1. Select the pattern from the Assigned Patterns list box.

2. Click **Preview Users** to open the Preview Pattern Users window that shows the Patterns box to the left and the Resolved Users box to the right:



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

3. Click the "X" in the upper right corner to close this window.

Remove a pattern

To remove a pattern in the Assigned Patterns list box:

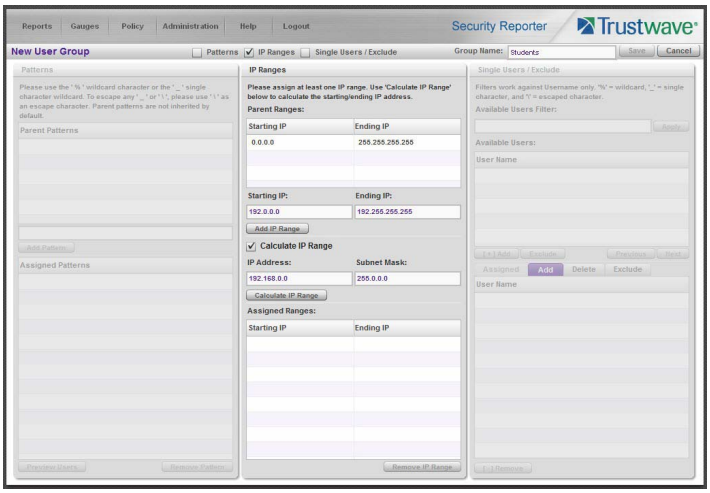
1. In the Patterns box, select the pattern from the Assigned Patterns list box to highlight it.
2. Click **Remove Pattern** to remove that pattern from the list box.

3.2.1.2.2 IP Ranges sub-panel

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

Note: If using IP group authentication, parent ranges do not display in this sub-panel unless an IP range was originally set up for this user group's parent user group. To set up the first parent user group to include an IP

range, "All" user groups must be used as the base group.



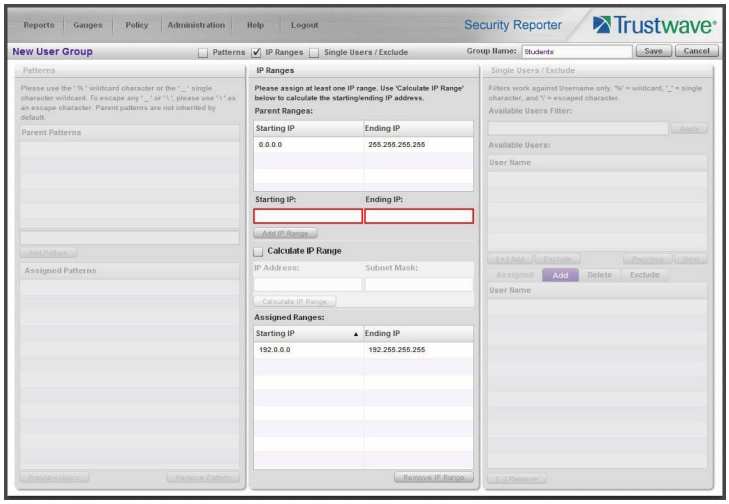
Specify an IP range

To add an IP address range:

1. Do one of the following:

- To make a selection from Parent Ranges, click the row in the Parent Ranges box to highlight and select that row, and also to add that Starting IP and Ending IP range in the Starting IP and Ending IP fields below. If necessary, edits can be made to these fields.
- To add an IP address range without selecting from the Parent Ranges sub-panel:
  a. Enter the **Starting IP** address.
  b. Enter the **Ending IP** address.
- To calculate an IP address range:
  a. Click the **Calculate IP Range** check box to activate the IP Address and Subnet Mask fields below.
  b. Enter the **IP Address**.
  c. Enter the **Netmask** which activates the Calculate Range button.
  d. Click **Calculate IP Range** to display the Starting IP and Ending IP in the fields above.

2. Click **Add IP Range** to include that IP range in the Assigned Ranges list box below:



Remove an IP address range

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

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

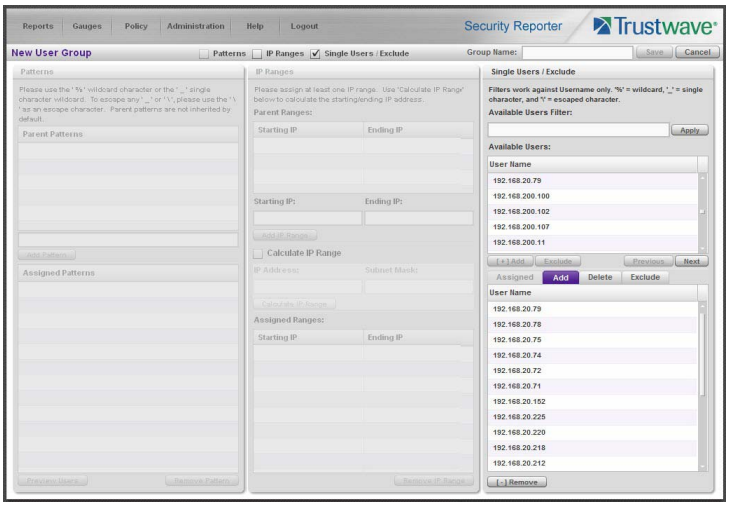
3.2.1.2.3 Single Users/Exclude sub-panel

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

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

A username preceded by an asterisk (*) indicates an auto-assigned user that can only be removed by

adjusting the pattern or IP range for that user's group.



Add one or more individual users

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

To use the **Available Users Filter**:

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

To make selections from the Available Users sub-panel:

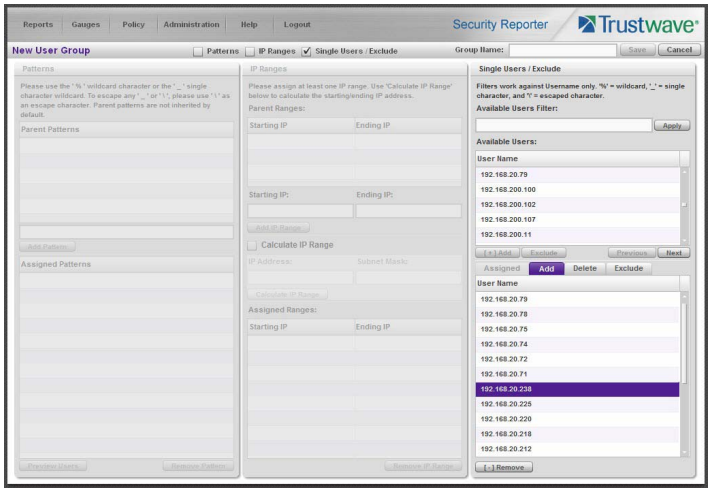
1. Select one or more IPs from the list to highlight the record(s).
2. Click **[+] Add** to include the selected user(s) in the Add tab.

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

Remove users from the Add tab

To remove users from this user group:

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



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

3.2.1.3 Edit a User Group

Note: Global administrators can edit any user group. Group administrators can only edit user groups assigned to them.

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 showing activated sub-panels—i.e. if the Patterns sub-panel had settings made in it, that sub-panel is activated; if the Single Users sub-panel was the only sub-panel with settings made in it, that sub-panel is activated. Any sub-panel without settings made in it displays greyed-out.
3. Make any of these edits:
   - To make entries in a sub-panel that is not yet activated, click the available check box to activate that sub-panel: **Patterns**, **IP Ranges**, **Single Users/Exclude**.
   - Make any of these edits in a sub-panel:
     - Patterns sub-panel - Add or remove a pattern.
     - IP Ranges sub-panel - Add or remove an IP address range.
     - Single Users/Exclude sub-panel - Add or remove one or more users.

Note: When editing the Single Users/Exclude sub-panel, users who are added display in the Add tab, and users who are removed display in the Delete tab.

   - If necessary, edit the name of the user group in the **Group Name** field.
4. Click **Save** to save your edits and to return to the User Groups panel.

3.2.1.4 Rebuild the User Group

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

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

3.2.1.5 Delete a User Group

Note: A user group can be deleted by any administrator that it is assigned to. A base group cannot be deleted. After deleting a user group, the Rebuild function should be executed.

To delete a user group:

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.

Caution: If the user group to be deleted is assigned to any other administrator, that user group will be removed from that administrator's User Groups list as well as your User Groups list.

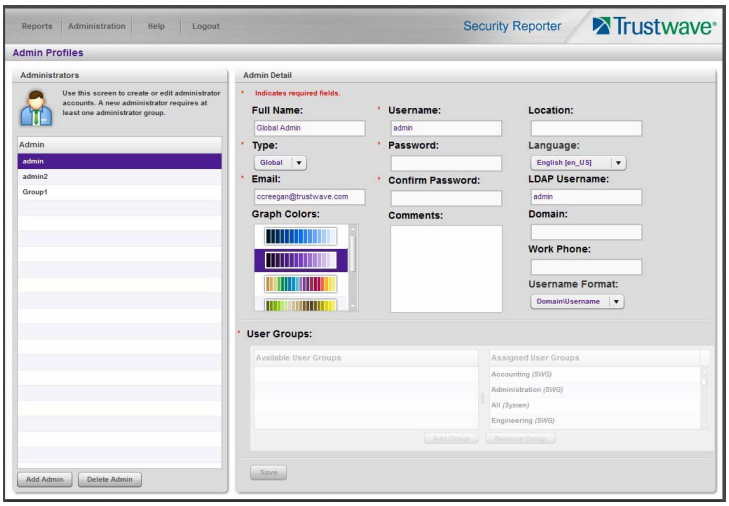
Tip: Click No to close the dialog box and to return to the User Groups panel.

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

3.2.2 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 work with specific user groups that are assigned to them.

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



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 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.

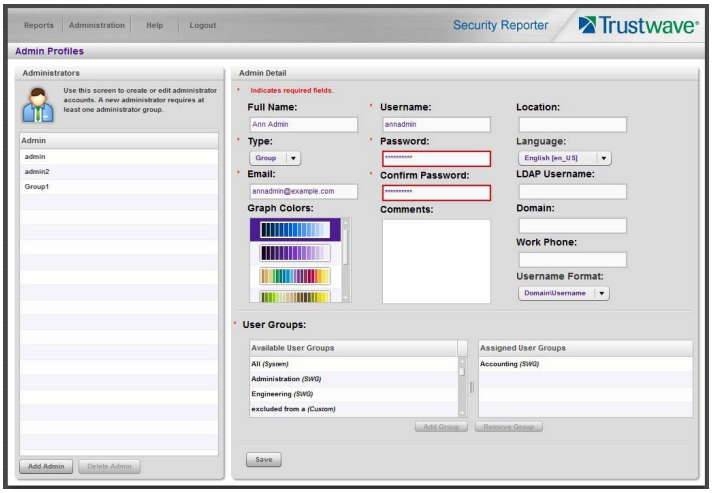
At the right side of this panel is the Admin Detail sub-panel, used for adding an administrator profile, viewing an existing administrator's account information, and modifying or deleting an administrator profile, as necessary.

If logged in as a group administrator without privileges to create other administrator profiles, the Administrators list box in the Administrators sub-panel displays only the name of the current user.

3.2.2.1 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:



- Optional: Type in the group administrator's **Full Name**.
- Select the administrator **Type** (Global or Group).
- Type in the group administrator's **Email** address.
- Optional: Select another report color scheme from the available **Graph Colors** choices.
- Type in the **Username** the group 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 group 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 group administrator's account.
- Optional: Type in identifying information about the group administrator's physical office **Location**.
- Optional: If necessary, select the language from the **Language** menu (English, Simplified Chinese, Traditional Chinese).

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

- Optional: If the administrator has an Active Directory LDAP account, 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 group administrator is registered.

Note: If the group administrator will be using the System Tray feature to be alerted to user activity, the LDAP Username and Domain entered in these fields should be the same as the username and password the group administrator uses to authenticate on his/her workstation.

See Real Time Reports Section: Alerts, Lockout Management and Appendix D: System Tray Alerts: Setup, Usage

for details on setting up and using the System Tray feature.

- Optional: Type in the group administrator's **Work Phone** number, 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. In the User Groups section, select the user group(s) that should be available to the group 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.

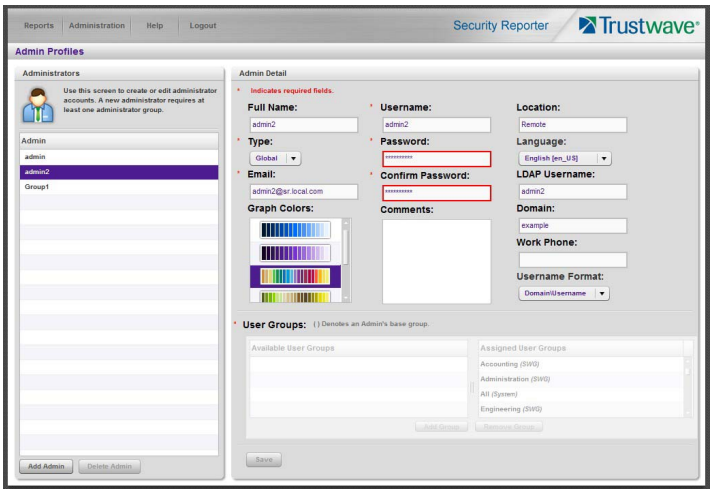
Tip: To remove any user group from the Assigned User Groups list box, select the user group(s), and then click Remove Group to remove the user group(s).

4. After selecting each user group to be assigned to the group administrator, click **Save** to add the Username for the new administrator to the Administrators list box.

3.2.2.2 View, Edit Admin Detail

3.2.2.2.1 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:



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

3.2.2.2.2 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, Language selection, Username Format selection, and User Groups selection.

Caution: As a group administrator you can remove groups from your Assigned User Groups. However, once the change is saved, you will permanently lose access to the removed groups. You cannot re-add a group even if it was previously assigned to you.

If you have unintentionally removed a group from your assigned groups, contact a Global Administrator for assistance.

- The following information can be added, modified, or deleted: Full Name, Comments, Location information, and LDAP Username or Domain name—the latter two fields are available if using LDAP—and Work Phone number.
- 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.

3.2.2.3 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 group 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 group administrator profile.

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

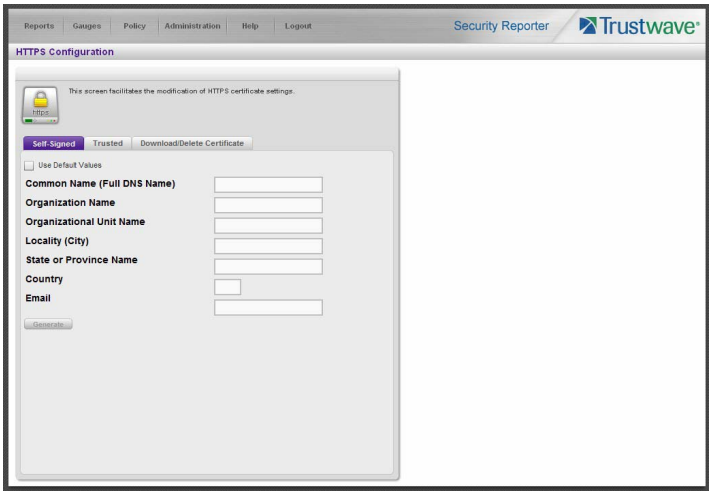
3.3 Database Management

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

3.3.1 HTTPS Configuration panel

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

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



3.3.1.1 Generate a Self-Signed Certificate for the SR

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

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. Do the following:
   - click the check box corresponding to **Use Default Values** to grey-out the tab, or
   - make entries in these fields:
     a. **Common Name (Full DNS Name)** - Hostname of the server, such as `logo.com`.
     b. **Organization Name** - Name of your organization, such as `Logo`.
     c. **Organizational Unit Name** - Name of your department, such as `Administration`.
     d. **Locality (City)** - Name of your organization's city or principality, such as `Orange`.
     e. **State or Province Name** - Full name of your state or province, such as `California`.
     f. **Country** - Two-character code for your country, such as `US`.
     g. **Email** - Your email address.
2. Click **Create** to generate the SSL certificate to be stored on the SR, and to restart the Report Manager. Hereafter, group administrators must accept the security certificate on their workstations in order for their machines to communicate with the Report Manager and/or System Configuration administrator console.

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

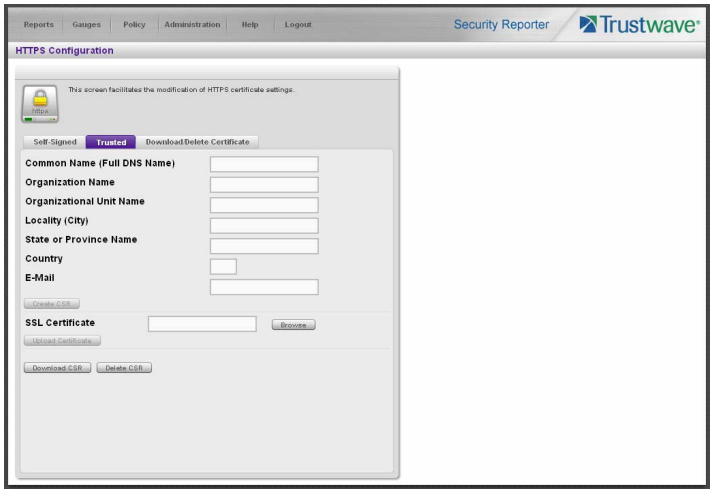
3.3.1.2 Create, Upload a Third Party Certificate

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

3.3.1.2.1 Create a CSR

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

1. Click the Trusted tab:



2. Make entries in these fields:

   a. **Common Name (Full DNS Name)** - Hostname of the SR server, such as `logo.com`.

   b. **Organization Name** - Name of your organization, such as `Logo`.

   c. **Organizational Unit Name** - Name of your department, such as `Administration`.

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

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

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

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

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

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

3.3.1.2.2 Download the CSR, Submit to Agency

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

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

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

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

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

3.3.1.2.3 Upload the Signed SSL Certificate to SR

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

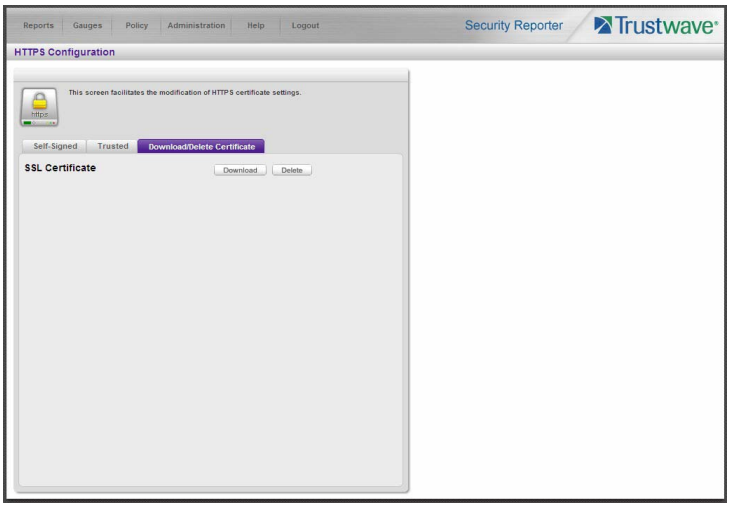
1. Launch Notepad on your machine.
2. Copy and paste the contents of the certificate into Notepad in the following order:
   a. SSL certificate
   b. Intermediate certificate(s)—this step is not required if you have a Single Root SSL Certificate
   c. Root certificate
3. Save the contents of the Notepad file with a .cer extension.
4. In the Trusted tab, go to the **SSL Certificate** field and click **Browse** to find the .cer file you just saved.
5. Click **Upload** to load the certificate on the SR.

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

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

3.3.1.3 Download, Delete a Third Party Certificate

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



3.3.1.3.1 Download the SSL Certificate

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

The certificate can now be distributed to group administrator workstations.

3.3.1.3.2 Delete the SSL Certificate

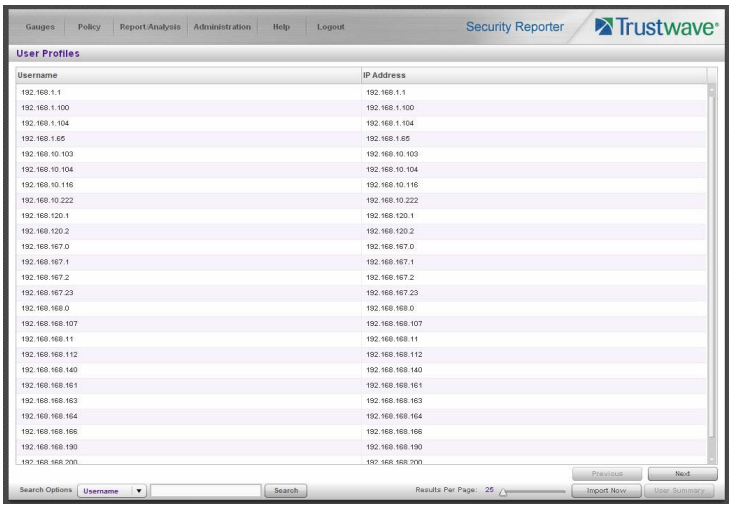
To delete the third party certificate from the SR, go to the Download/Delete Certificate tab and click **Delete** to remove the certificate from the SR.

3.3.2 User Profiles panel

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

Note: The User Profiles panel is available to global administrators only.

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



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

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

3.3.2.1 Search the User Database

1. Specify search criteria by making a selection from the **Search Options** pull-down menu:

   - **Username** - This selection performs a search by an end user's username.

- **IP Address** - This selection performs a search by an end user's IP address.

2. Make an entry in the blank field to the right:
   - If Username was selected, enter a username.
   - If IP Address was selected, enter an IP address.
3. Click **Search** to display a record that matches your criteria.

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

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

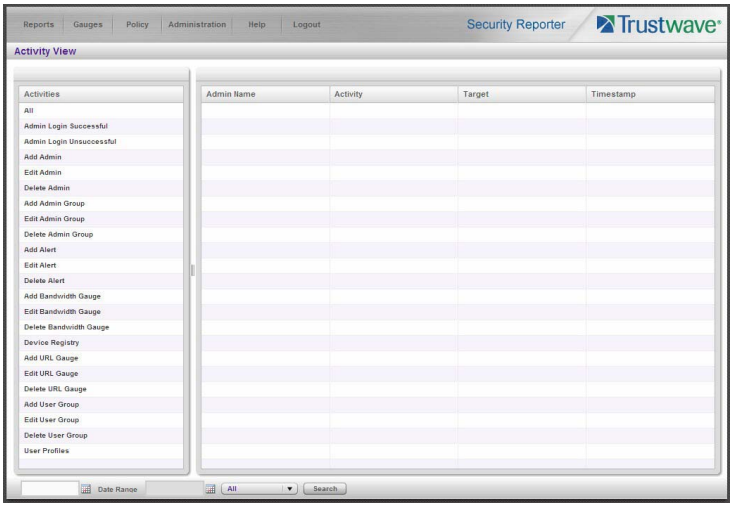
3.3.2.1.1 View End User Activity

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

3.3.3 Activity View panel

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

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.

3.3.3.1 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: All, Admin Login Successful, Admin Login Unsuccessful, Add Admin, Edit Admin, Delete Admin, Add Admin Group, Edit Admin Group, Delete Admin Group, Add Alert, Edit Alert, Delete Alert, Add Bandwidth Gauge, Edit Bandwidth Gauge, Delete Bandwidth Gauge, Device Registry, Add URL Gauge, Edit URL Gauge, Delete URL Gauge, Add User Group, Edit User Group, Delete User Group, User Profiles.

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

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

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

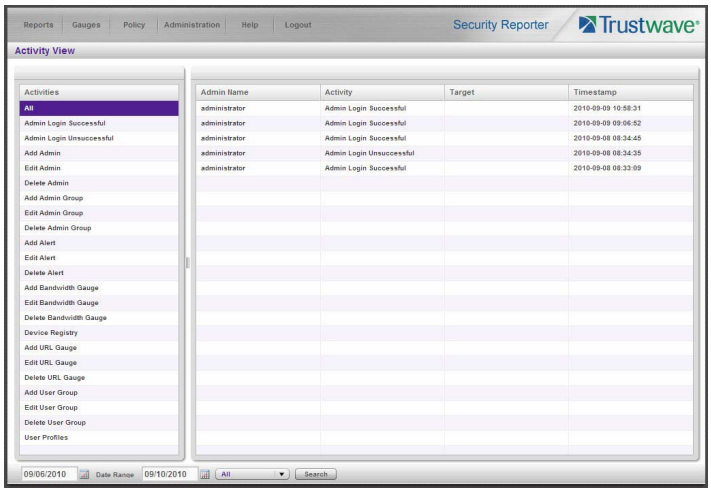
3. Click the starting date to select it and to close the calendar pop-up window. This action populates the field to the left of the calendar icon with the selected date.

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

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

6. To view the activity of a specified administrator, select the username from the pull-down menu.

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



3.3.3.1.1 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:

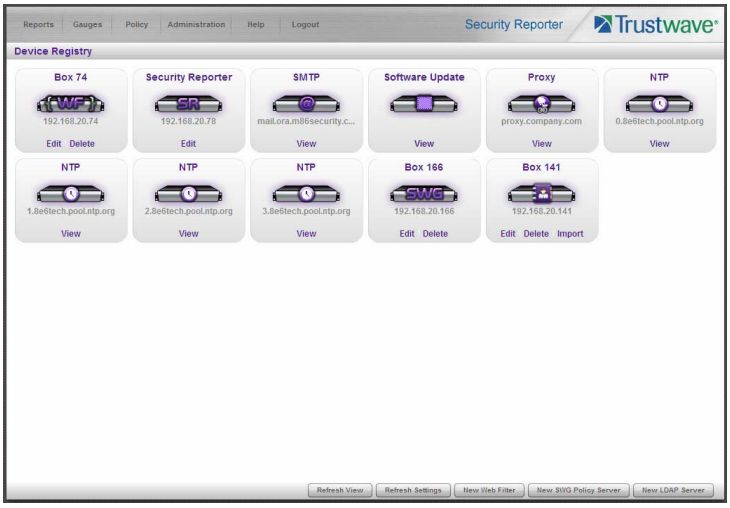
- administrator name for Add/Edit/Delete Admin
- group name for Add/Edit/Delete Admin Group
- alert name for Add/Edit/Delete Alert
- gauge name for Add/Edit/Delete URL/Bandwidth Gauge.

3.3.4 Device Registry panel

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

This function is available to global administrators.

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



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

At the bottom of the panel the following buttons display:

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

- **New LDAP Server** (enabled only if an SWG has been added to the device registry) - Click this button to add an LDAP server to the device registry.

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

3.3.4.1 Removing/adding Web Filter, SWG devices

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

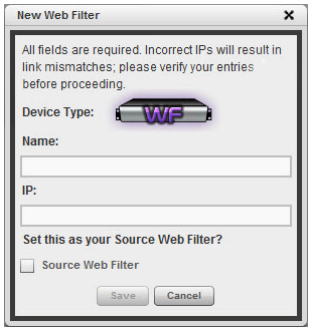
Device(s) listed in registry	Change(s) made to registry	Result
SWG	Remove SWG	All data for Time Usage Reports, Summary Reports, Summary Drill Down Reports and Detail Drill Down Reports will be purged.
SWG	Retain SWG and add Web Filter	All data for Time Usage Reports, Summary Reports, Summary Drill Down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

Caution: For any scenario specified above that would result in data being purged from the Security Reporter, Trustwave recommends backing up and saving current SR data off the server before adding or removing the designated device from the device registry.

3.3.4.2 Web Filter Device Maintenance

3.3.4.2.1 Add a Web Filter to the device registry

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



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

Tip: Click **Cancel** to close this window.

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

3.3.4.2.2 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:

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.

Tip: Click **Cancel** to close this window.

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

3.3.4.2.3 Delete a Web Filter from the device registry

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

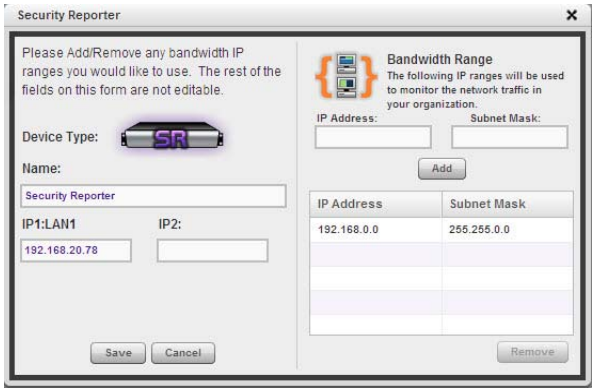
Note: Click **No** to close the dialog box.

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

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

3.3.4.3 Security Reporter Maintenance

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



The following displays at the left side of this window: Device Type (SR), Name of the application (Security Reporter), and IP1:LAN1 and IP2:LAN2 address(es), if entered during—or subsequently to—the wizard hardware installation process.

The following displays at the right side of this window: Enable Real-time Reporting checkbox (available only if a Web Filter device is configured), Bandwidth Range IP Address and Subnet Mask fields, and buttons for adding or removing a range of IP addresses the SR application will monitor for network traffic.

Note: Bandwidth Range criteria is only required if a Web Filter and Real-time Reporting will be used with this SR. Real-time Reporting is disabled by default for all new and updated installations.

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

3.3.4.3.1 Add, remove a bandwidth range

1. Do the following in the Bandwidth Range section:

- To add a bandwidth IP address range:

  a. Type in the **IP Address**.
  b. Type in the **Subnet Mask**.
  c. Click **Add** to add the bandwidth IP range in the list box.

- To remove a bandwidth IP address range:

  a. Select the IP address range from the list box; this action activates the Remove button.
  b. Click **Remove** to remove the IP address range.

Tip: Click **Cancel** to close the window without saving your entries.

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

3.3.4.3.2 Enable or disable Real-time Reporting

Real-time Reporting includes the gauges and other objects described in Section 5 of this *Guide*. These features are available when the SR is used to report on data from a Web Filter device. These features are disabled by default.

Caution: Real-time Reporting consumes significant processing power and other resources. Data processing will be slower, and generation of Productivity and Security reports will be less responsive, if Real-time Reporting is enabled.

To enable or disable Real-time Reporting:

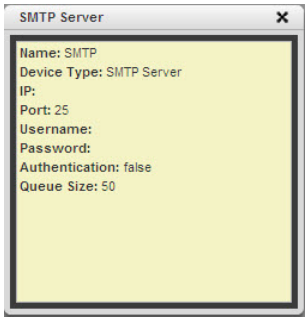
1. Check, or uncheck, the box **Enable Real-time Reporting**.
2. To apply the change, log out of the SR interface and log in again.

3.3.4.4 View Other Device Criteria

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

3.3.4.4.1 View SMTP device criteria

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



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

2. Click the "X" in the upper right corner to close this window.

3.3.4.4.2 View Software Update Server device criteria

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

3.3.4.4.3 View Proxy Server device criteria

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

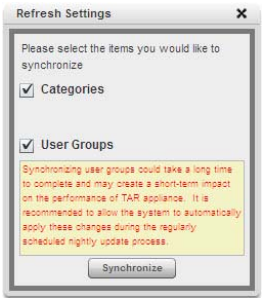
3.3.4.4.4 View NTP Server device criteria

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

3.3.4.5 Refresh Settings

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

1. Click **Refresh Settings** to open the Refresh Settings window:



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

- **Categories** - Make this selection to synchronize Trustwave supplied library category updates and custom library categories from the source Web Filter to the SR.
- **User Groups** - Make this selection to synchronize LDAP user group information on the source Web Filter to the SR.

Tip: Click the "X" in the upper right corner of this window to close it.

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

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

3.3.4.6 SWG Policy Server Device Maintenance

3.3.4.6.1 Add the first Policy Server to the device registry

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

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.

3.3.4.6.2 Add another Policy Server to the device registry

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

   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.

3.3.4.6.3 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:

   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:

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

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

c) 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.

3.3.4.6.4 Delete a Policy Server from the device registry

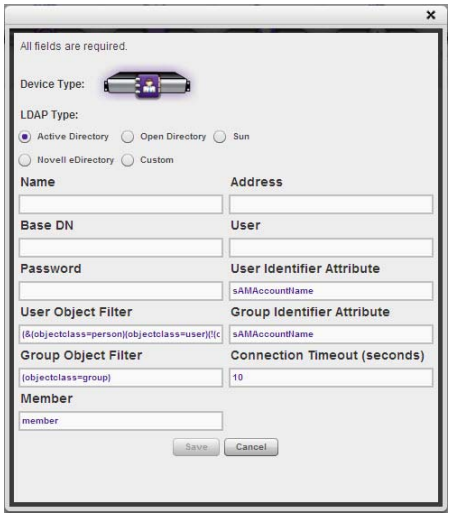
1. Go to the SWG server icon in the Device Registry panel and click **Delete** to open the CONFIRM dialog box with a message asking if you want to delete this device.
2. Click **Yes** to delete the SWG device from the registry, and to remove the SWG server icon from the Device Registry panel. Click **No**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

3.3.4.7 LDAP Server Device Management

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

3.3.4.7.1 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:



   The Device Type image displays.

2. Make entries in the following fields:

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

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

Tip: Click **Cancel** to close this window.

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

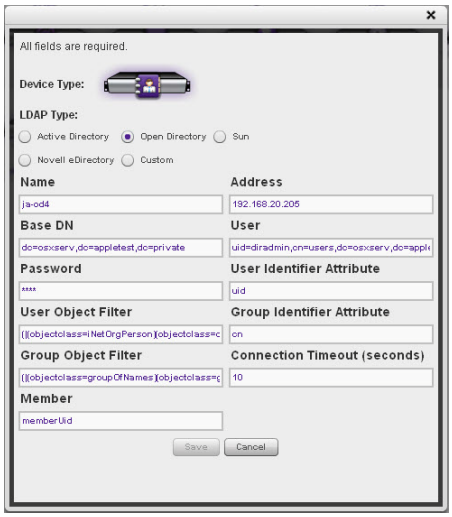
3.3.4.7.2 Import LDAP Group profiles

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.

3.3.4.7.3 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:



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.

Tip: Click **Cancel** to close this window.

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

3.3.4.7.4 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.

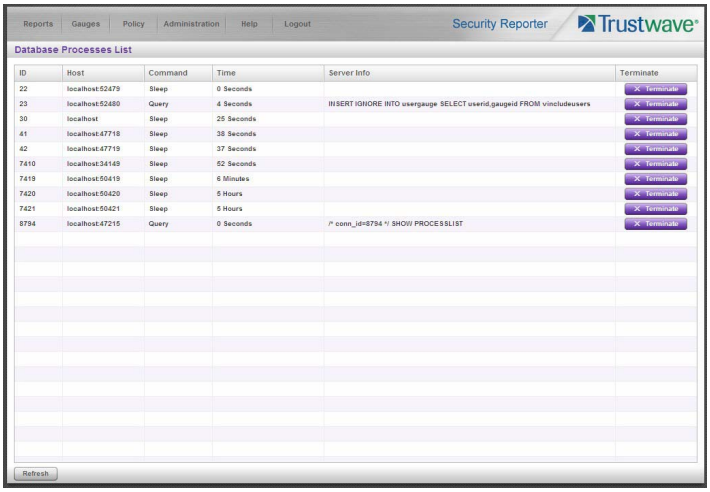
Note: Click **No** to close the dialog box.

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

3.3.5 Database Processes List panel

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

In the navigation toolbar, hover over the Administration menu link and select **Database Processes List** to display the Database Processes List panel:



3.3.5.1 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.

3.3.5.2 Terminate a Process

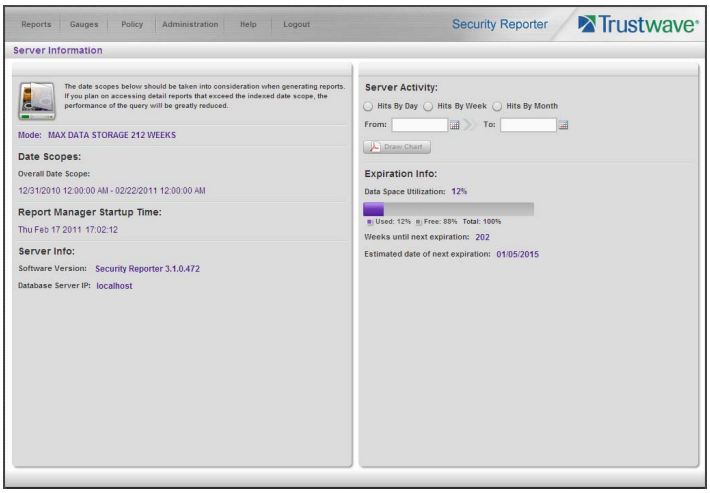
Select the process to be terminated and click **Terminate**.

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

3.3.6 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.

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



The panel is comprised of six sections: Mode (this section does not display for an SR in evaluation mode), Date Scopes, Report Manager Startup Time, Server Info, Server Activity, and Expiration Info.

Note: If the SR server is newly installed, server statistics will be available after they are initially correlated for the server, immediately after midnight. If this problem persists, please contact your system administrator.

3.3.6.1 Mode

3.3.6.1.1 Registered Mode and Evaluation Mode

The Mode section displays information about an SR in registered mode: the maximum number of weeks of data storage ("MAX DATA STORAGE 'X' WEEKS"—in which 'X' represents the number of weeks).

Registered mode pertains to an SR server that has been activated online and registered by 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 routine 30-minute check of available storage space—the oldest week of data (from Sunday through Saturday) is dropped from the database.

Evaluation mode is used during the evaluation period of an SR, which, by default, provides a maximum of three weeks of the most recent data for reporting.

Note: See the Expiration screen in the System Configuration Section for more information about data expiration. See also Appendix C: Evaluation Mode for information about using the SR in the evaluation mode.

3.3.6.2 Date Scopes

The Date Scopes section displays the Overall Date Scope of data stored on the SR. This date scope includes the range for the period of stored data, using the MM/DD/YYYY format.

3.3.6.3 Report Manager Startup Time

The Report Manager Startup Time section contains the following information pertaining to the last time the Report Manager was restarted, using the MM/DD/YYYY HH:MM:SS AM/PM format.

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.

3.3.6.4 Server Info

The Server Info section contains the following SR server information: **Software Version** number and **Database Server IP** address—or the label "localhost" that designates the SR as the host server for the Report Manager.

3.3.6.5 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 by doing the following:

   a. Click the radio button corresponding to **Hits By Day**, **Hits By Week**, or **Hits By Month**.

   b. At the **From** and **To** fields, make a selection for the date range using the calendar icons:

   - Click the calendar icon to open the larger calendar for the current month, with today's date highlighted.

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

   - Click the date to select it and to close the calendar 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.

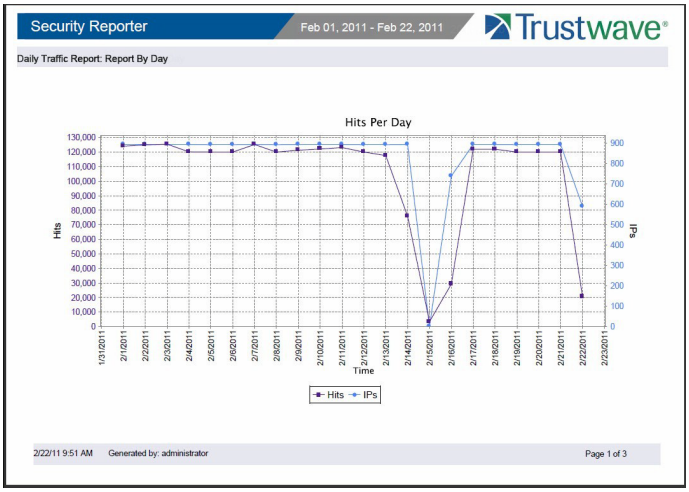
   The header section includes the title of the chart and date range. The footer section includes the date and time the chart was generated (shown in the MM/DD/YYYY HH:MM AM/PM format), the login ID of the person who generated the chart (Generated by) and the Page number and page range.

   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.

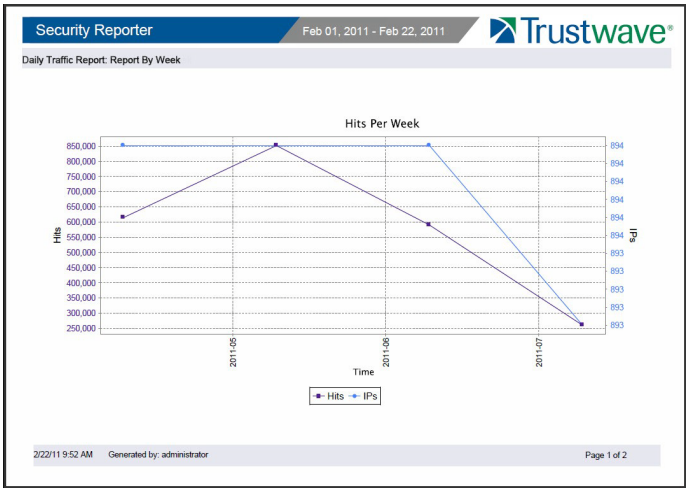
   Rows of report details indicate the time measurement (Day, Week, or Month), the exact Number of Hits corresponding to each unit of time, and the Total Records.

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

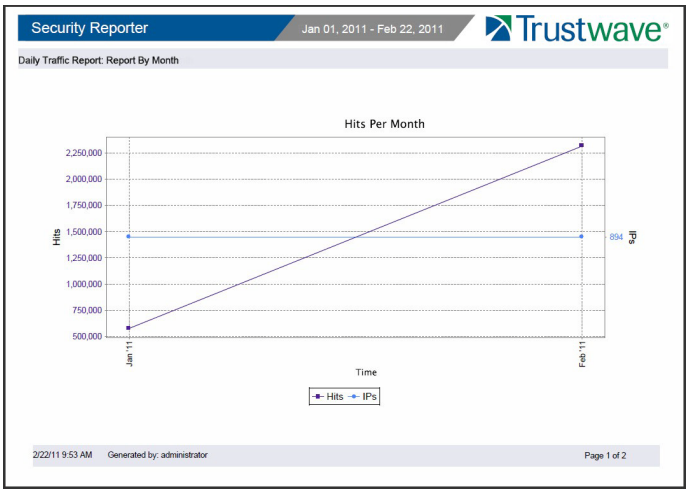
   - **Hits Per Day** - If you selected Hits By Day, days within the date range are plotted on the graph, grouped into equal time intervals. The summary shows the Number of Hits (in purple) and Number of IPs (in blue) for a specified Day (MM/DD/YYYY).



- **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.



- **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.



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.

3.3.6.6 Expiration Info

In the Expiration Info section, the following data displays:

- **Data Space Utilization** - The percentage of database storage space currently being used on the SR. Beneath this line is a colored bar depicting the percentage of data "Used" (purple) and "Free" (grey). A key displays beneath the colored bar to indicate the percentage of data both "Used" and "Free", and "Total" data percentage.
- **Weeks until next expiration** - The number of weeks from this week that data on the SR will expire.

Note: If using the SR in evaluation mode, the text "(IF REGISTERED)" is included in the label to indicate the number of weeks of data that would be stored on the SR if the server was activated and running in registered mode. (See Registered Mode and Evaluation Mode in this sub-section.)

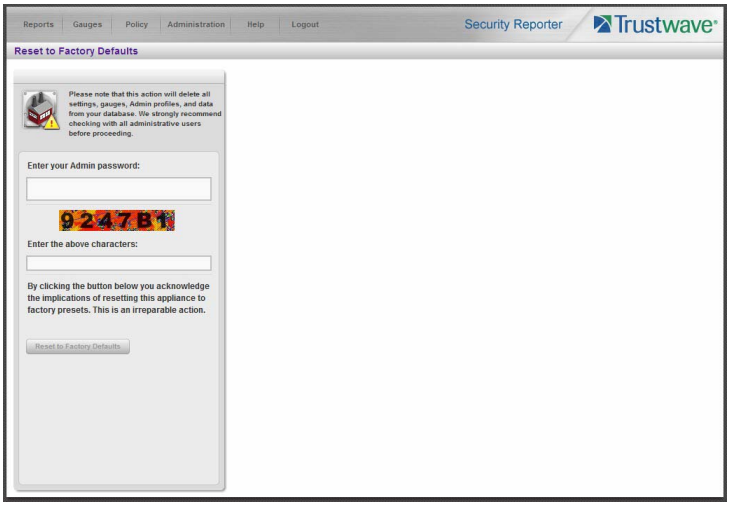
- **Estimated date of next expiration** - the date scheduled for the next automatic database expiration (MM/DD/YYYY format).

Note: If using the SR in evaluation mode, the text "(IF REGISTERED)" is included in the label to indicate the number of weeks of data that would be stored on the SR if the server was activated and running in registered mode. (See Registered Mode and Evaluation Mode in this sub-section.)

3.3.7 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 current software update level of the application.

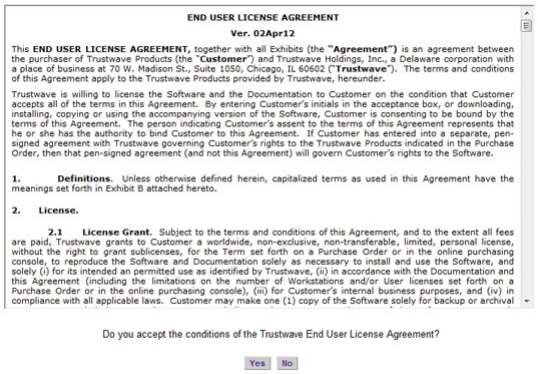
In the navigation toolbar, hover over the Administration menu link and select **Reset to Factory Defaults** to display the Reset to Factory Defaults panel:



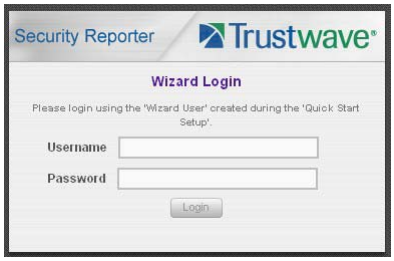
Caution: When using this option, all settings made on the SR—including administrator, group, and real time gauge configuration settings and alerts—will be purged and cannot be restored. The SR will also be set to evaluation mode.

3.3.7.1 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:

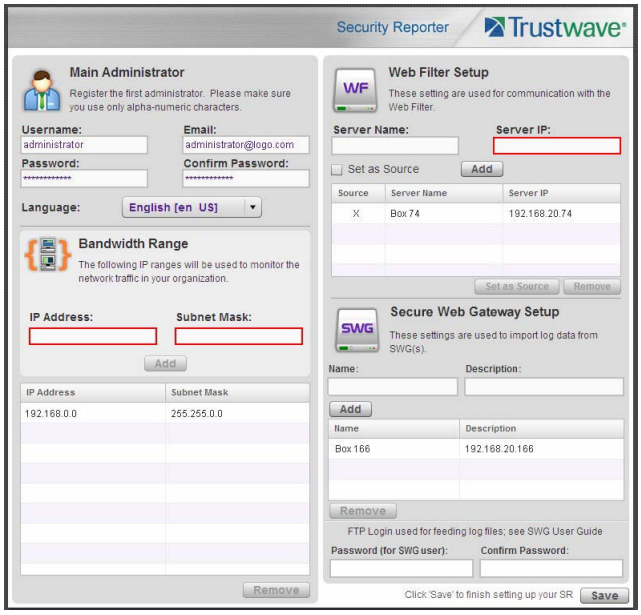


4. After reading the contents of the EULA, click **Yes** to accept it and to go to the Wizard Login window:



3.3.7.2 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:



3.3.7.2.1 Main Administrator

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

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

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

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

Tip: The Language setting field is also available in the Admin Profiles panel, accessible to each administrator and sub-administrator. See Admin Profiles panel in this Section for information about making Language setting changes.

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

3.3.7.2.2 Bandwidth Range and Web Filter Setup

Note: Web Filter details must be entered if one or more Web Filters will be used with this SR. Bandwidth Range entry is optional and only applies if Web Filters will be used with this SR.

These entries are not required during this Wizard setup process. They can also be configured in the device registry, as described in the Device Registry panel sub-section.

1. In the Bandwidth Range section (optional), type in the **IP Address** and **Subnet Mask**, and then click **Add** to include the bandwidth IP address range in the list box below.

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

2. In the Web Filter Setup section type in the **Server Name** and **Server IP** address, indicate if this Web Filter will be **Set as Source**, and then click **Add** to include the server criteria in the list box below.

Tip: To add another Web Filter, follow the instructions in this sub-section. To remove a Web Filter from the list box, select it and then click **Remove**.

To make a Web Filter the Source server—if no Web Filter in the list has yet been specified as the Source server, or if the IP address of the Source server has changed—select the Web Filter from the list box and then click **Set as Source**.

3.3.7.2.3 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.

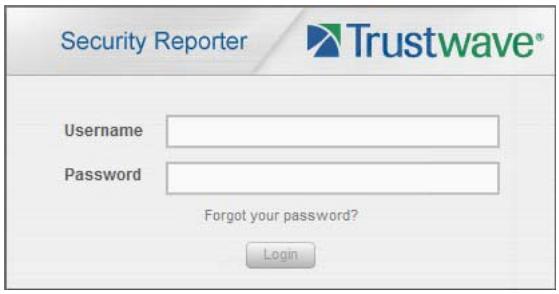
Tip: To remove the SWG from the list box, select it and then click **Remove**.

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.

3.3.7.2.4 Save Entries

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



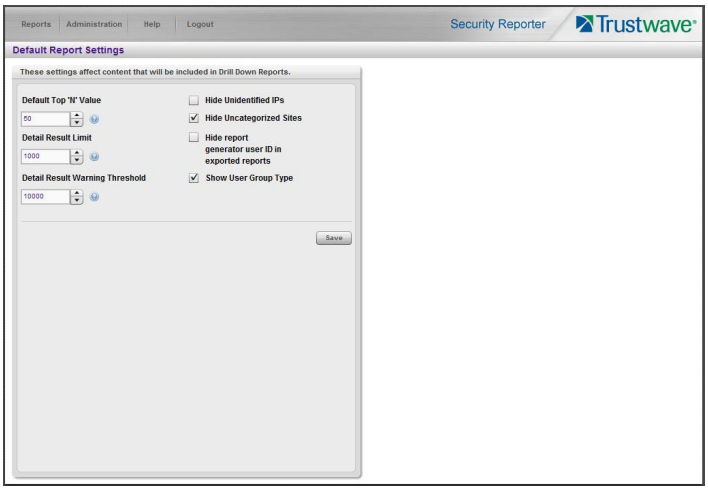
3.4 Report Configuration

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

3.4.1 Default Report Settings panel

A global administrator uses the Default Report Settings panel for specifying 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:



3.4.1.1 Set New Defaults

1. Enter the **Default Top 'N' Value** of records that will be generated for summary reports. The default is "50" records.
2. Enter the maximum number of records that will be included in a detail report's **Detail Result Limit**. If the number of records from a query exceeds the limit established in this field, the overflow will be included in the next set of records. The default is "1000" records per set.

3. Enter the maximum number of records that can be returned by a detail report query before triggering the **Detail Result Warning Threshold** message. This warning message indicates that the number of records exceeds the number specified in this field. The default is "10000" records.
4. By default, the **Hide Unidentified IPs** 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.

5. 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.
6. 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.

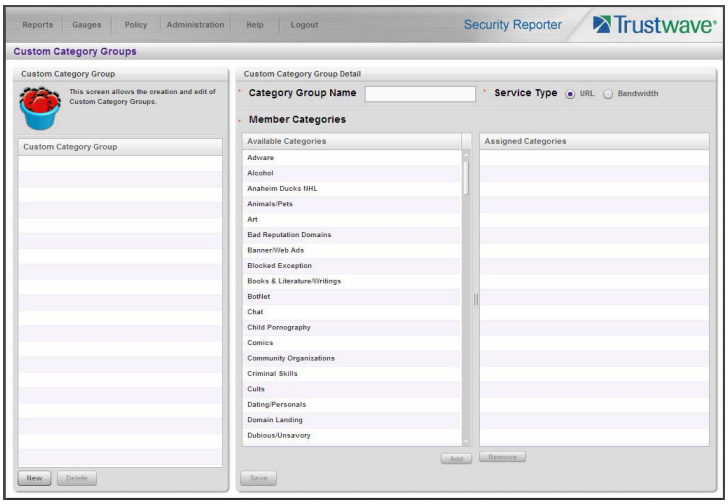
   If you wish to exclude the username of the reporter from drill down reports, check the box.
7. By default, the **Show User Group Type** check box is selected. This setting indicates that for reports in which user groups are grouped by group name, the type of user group ("System", "Custom", "LDAP", or "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.
8. Click the **Save** button to save your settings in the Default Report Settings panel.

3.4.2 Custom Category Groups panel

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

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



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

3.4.2.1 Add a Custom Category Group

1. At the bottom of the Custom Category Group sub-panel, click **Add**.
2. In the Custom Category Group Detail sub-panel, type in the **Category Group Name**.
3. Specify the **Service Type** to use: "URL" or "Bandwidth".
4. Include the following **Member Categories** based on the Service Type selection:
   - URL - Select Available Categories from the list and click **Add** to move the selection(s) to the Assigned Categories list box.
   - Bandwidth - In the **Port Number** field, type in a specific value in the pre-populated field, and/or use the up/down arrow buttons to increment/decrement the current value by one, and then click **Add Port** to move the selection to the Assigned Ports list box.

Note: At least one library category/protocol/port must be selected when creating a gauge.

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

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

3.4.2.2 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 update the assigned selections in the list box, select the item to select it, and then click **Remove** to remove it.

3. Click **Update** to save your modification(s).

3.4.2.3 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 Productivity and Security Reports Section

4.1 Introduction

This section of the user guide provides instructions to administrators on how to utilize the Report Manager to:

- generate productivity report views and interpret results using logs from a Web Filter and/or an SWG application
- generate security report views and interpret results if using an SWG

Note: Reports unique to environments that only use a Web Filter are addressed in the Real Time Reports Section.

For Web Filter and SWG environments, the Reports menu consists of the following options:

- A High Level Overview - Section 4.2 shows you how to view productivity report data in the Dashboard and canned 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.

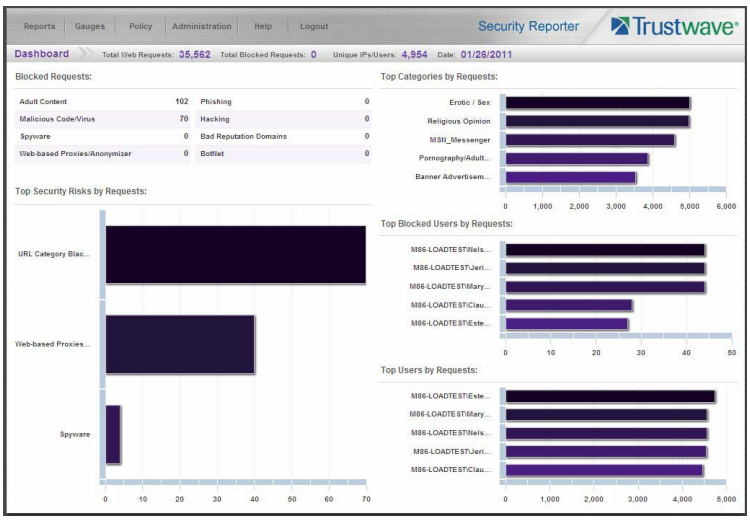
4.2 A High Level Overview

The following productivity reporting topics from the Reports menu of the Report Manager are described in this section: Dashboard, and Summary Reports. 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 productivity report categories.

The Dashboard displays by selecting Reports | Dashboard in the navigation toolbar:



Note: If using both a Web Filter and an SWG, only Web Filter log results display.

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

The following information displays in the center of the panel:

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

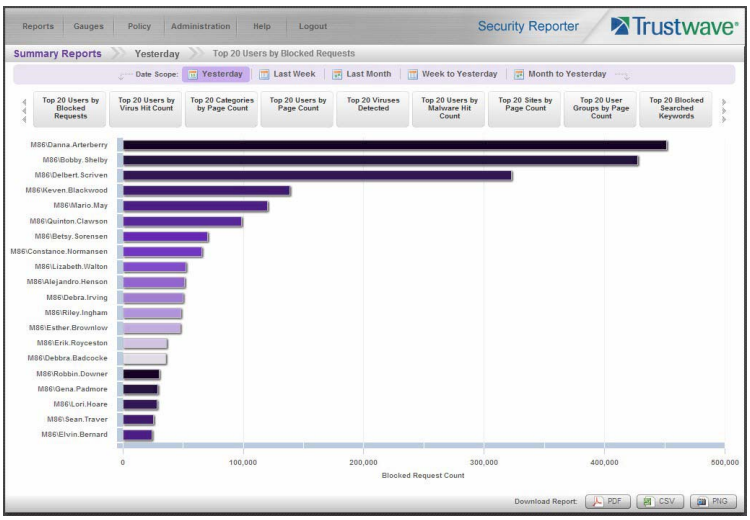
Tip: Hover over each bar in the bar graph to view the name of graph entry and number of requests for that entry.

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

4.2.2 Summary Reports

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

Summary Reports are available to group administrators assigned the privilege to access the Reports | Summary menu selection. 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 any thumbnail images or bar chart report. If there was no activity for a given report type, the message "No Data to display." displays in the panel.

If the Blocked Requests Report feature is disabled in System Configuration | Database | Optional Features | Blocked Request Count frame, yesterday's Top 20 Categories report view displays by default instead.

Tip: Click the left arrows or right arrows at the edges of the dashboard to display thumbnail images that are currently hidden. Click the tab for the specified time period (Yesterday, Last Week, Last Month, Week to Yesterday, Month to Yesterday) to change the Date Scope.

Hover over each bar in the bar graph to view the name of graph entry and number of requests for that entry.

4.2.2.1 Summary Report types

Available Summary Reports are as follows by clicking the thumbnail for the corresponding report type:

- **Top 20 Users by Blocked Requests** - Bar chart report depicting each top end user's total Page Count for Blocked and Warn Blocked requests. If using a Web Filter only, this report is available if the Block Request Count feature is enabled in the Optional Features screen in the System Configuration administrator console.
- **Top 20 Users by Bandwidth Consumption** (for SWG only environments) - Bar chart depicting each top end user's total Megabytes for bandwidth requests.

Note: The thumbnail for this report will not display in any environment with a Web Filter.

- **Top 20 Users by Virus Hit Count** (for SWG) - Bar chart report depicting each top end user's total Virus Count (both Blocked and Permitted) detected by the anti-virus engine.
- **Top 20 Categories by Page Count** - Bar chart report depicting the total Page Count in the top requested filtering library categories.

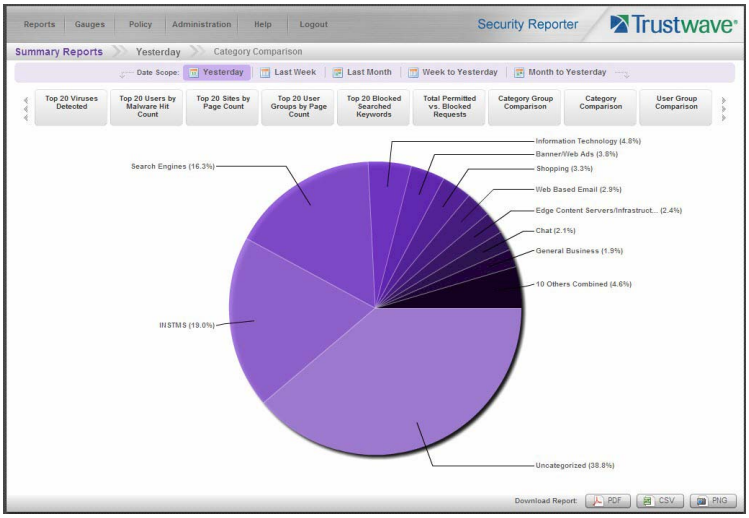
- **Top 20 Users by Page Count** - Bar chart report depicting each top end user's total Page Count.
- **Top 20 Viruses Detected** (for SWG) - Bar chart report depicting the top viruses and Virus Count detected by the anti-virus engine.
- **Top 20 Users by Malware Hit Count** - Bar chart report depicting each top end user's total "Blocked" and "Permitted" Hit Count from the following categories in the Security, Internet Productivity, and Internet Communication (Instant Messaging) category groups: BotNet, Malicious Code/Virus, Bad Reputation Domains, Spyware, Adware, and IRC.

Note: For SWG users, results that display in the Top 20 Users by Malware report reflect library contents mapped to the Trustwave Supplied Categories.

- **Top 20 Sites by Page Count** - Bar chart report depicting the total Page Count for the most popular sites accessed by end users.
- **Top 20 User Groups by Page Count** - Bar chart report depicting the total Page Count for the top scoring user groups.
- **Total Permitted vs. Blocked Requests** - Pie chart report depicting the total Page Count for all filtering categories Permitted to pass and all filtering categories set up to be Blocked.
- **Category Group Comparison** - Pie chart report depicting the total Page Count in each top scoring filtering category group.
- **Category Comparison** - Pie chart report depicting the total Page Count in each top scoring filtering category.
- **User Group Comparison** - Pie chart report depicting the total Page Count in each top scoring user group.

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** - Click one of these tabs at the top of the panel to display data for another period: Yesterday (default), Last Week, Last Month, Week to Yesterday, or Month to Yesterday
- Report type thumbnails - Click one of the report type thumbnails beneath the Date Scope to display that report view.

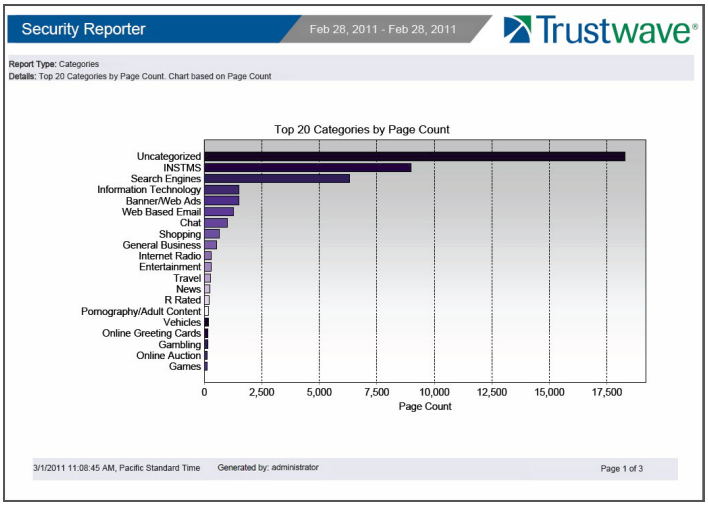
Tip: Click the left arrows or right arrows at the edges of the dashboard to display thumbnail images that are currently hidden.

4.2.2.3 Download, Export a Summary Report

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

4.2.2.3.1 PDF format

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



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

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

The body of the first page of the report includes the following information:

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

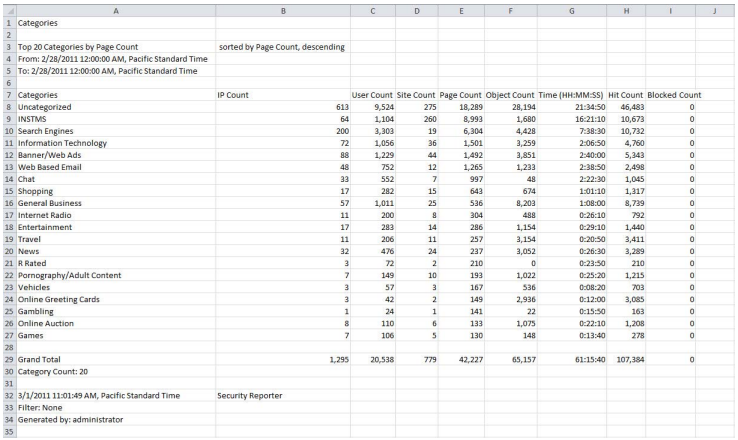
The body of the pages following the first page of the bar or pie chart report includes the following information:

- Top 20 Users by Blocked 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:



	A	B	C	D	E	F	G	H	I	J
1	Categories									
2										
3	Top 20 Categories by Page Count	sorted by Page Count, descending								
4	From: 2/28/2011 12:00:00 AM, Pacific Standard Time									
5	To: 2/28/2011 12:00:00 AM, Pacific Standard Time									
6										
7	Categories	IP Count	User Count	Site Count	Page Count	Object Count	Time (HH:MM:SS)	Hit Count	Blocked Count	
8	Uncategorized	613	9,524	275	18,289	28,194	21:34:50	46,483	0	
9	INSTMS	64	1,104	260	8,993	1,680	16:21:10	10,673	0	
10	Search Engines	200	3,303	19	6,304	4,428	7:38:30	10,732	0	
11	Information Technology	72	1,056	36	1,501	3,259	2:06:50	4,760	0	
12	Banner/Web Ads	88	1,229	44	1,492	3,851	2:40:00	5,343	0	
13	Web Based Email	48	752	12	1,265	1,233	2:38:50	2,498	0	
14	Chat	33	552	7	997	48	2:22:30	1,045	0	
15	Shopping	17	282	15	643	674	1:01:10	1,317	0	
16	General Business	57	1,011	25	536	8,203	1:08:00	8,739	0	
17	Internet Radio	11	200	8	304	488	0:26:10	792	0	
18	Entertainment	17	283	14	286	1,154	0:29:10	1,440	0	
19	Travel	11	206	11	257	3,154	0:20:50	3,411	0	
20	News	32	476	24	237	3,052	0:26:30	3,289	0	
21	R Rated	3	72	2	210	0	0:23:50	210	0	
22	Pornography/Adult Content	7	149	10	193	1,022	0:25:20	1,215	0	
23	Vehicles	3	57	3	167	536	0:08:20	703	0	
24	Online Greeting Cards	3	42	2	149	2,936	0:12:00	3,085	0	
25	Gambling	1	24	1	141	22	0:15:50	163	0	
26	Online Auction	8	110	6	133	1,075	0:22:10	1,208	0	
27	Games	7	106	5	130	148	0:13:40	278	0	
28										
29	Grand Total	1,295	20,538	779	42,227	65,157	61:15:40	107,384	0	
30	Category Count: 20									
31										
32	3/1/2011 11:01:49 AM, Pacific Standard Time	Security Reporter								
33	Filter: None									
34	Generated by: administrator									
35										

The header of the generated report includes the Report Type, report description, sort criteria, From/To date and time range (MM/D/YYYY HH:MM:SS AM/PM format), and time zone for the reporting period and location.

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

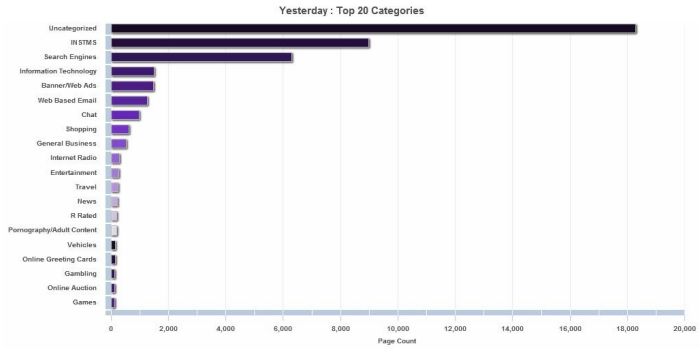
The Grand Total and Counts display after the last row of user data.

The footer of the report includes the date, time, and time zone in which the report was generated (MM/D/YYYY HH:MM:SS AM/PM, time zone code), product name, Filter specifications, and the login ID of the user who generated the report (Generated by).

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

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 totalling less than one percent are grouped together under the "Others Combined" label.

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

4.3 Drill Down Reports

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

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

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

- **Vulnerability Anti.Dote** - Provides details for each instance of real-time vulnerability detection resulting from end user Internet/network activity.

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 productivity or security 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: Category, Content Type, Rule, Spyware, Violation, Virus, Vulnerability Anti.Dote.

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.

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 for productivity and security reports 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.

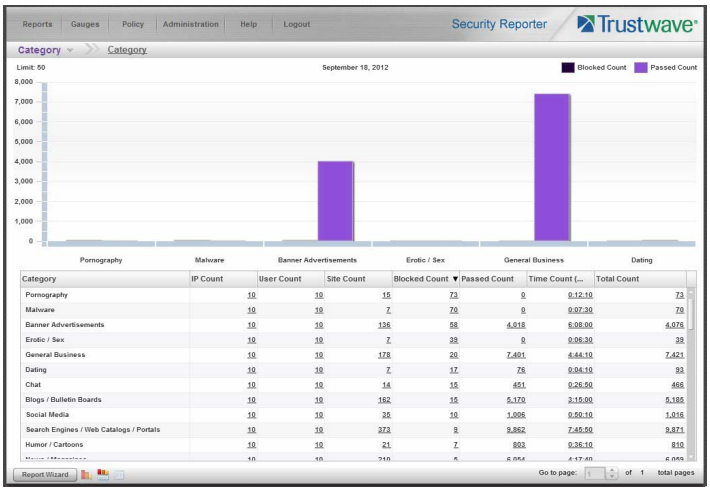
The following information displays at the top of the report view: date (using the month name DD, YYYY format), and Blocked Count and Passed Count key.

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 pertinent 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.



Tip: To refresh the current report view, select the same report name from the report type menu in the bread-crumb 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: Category, Content Type, Rule, Spyware, Violation, Virus, Vulnerability Anti.Dote.

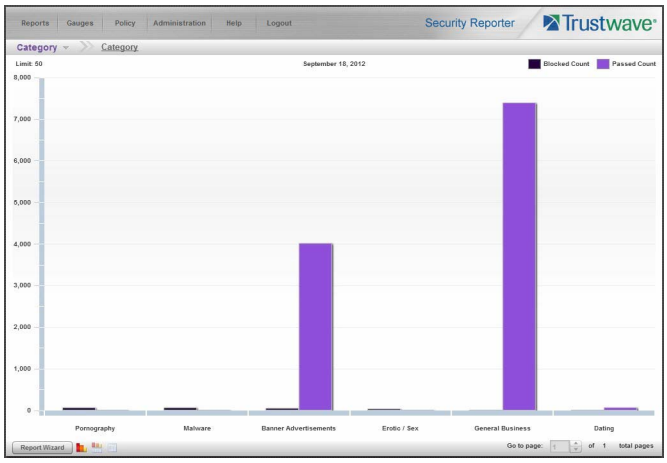
4.3.2.1.2 Summary Drill Down Report Wizard

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

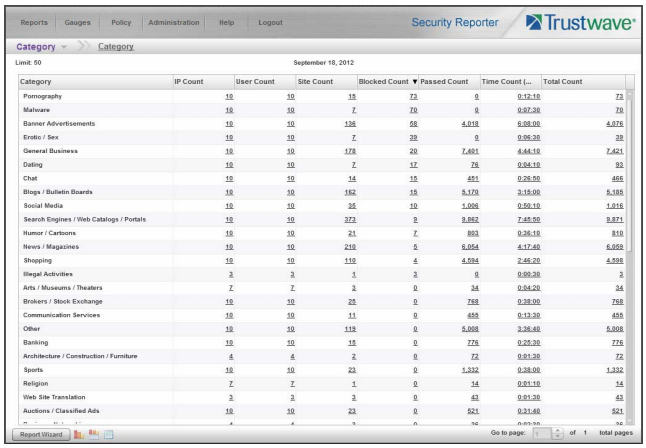
Click the following report view icon to change the report view display:

-  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:



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.

- **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 pertains to 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 pertains to 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.

If "Pages only" was specified in the Log Import Settings frame of the Optional Features screen in the System Configuration user interface, all records of objects accessed by end users will be lost for the time period in which this option was enabled. Even if there were objects accessed by end users during that time period, zeroes ("0") will display in the Object Count column in the report. See the Optional Features sub-section of the System Configuration Section for information about Log Import Settings frame options.

- **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** - If using an SWG only with this SR, for all report types except the Category report type, this column displays the amount of bandwidth in GB or MB used for each record.

Note: The Bandwidth column does not display if a Web Filter is used with this SR—with or without an SWG.

- **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.

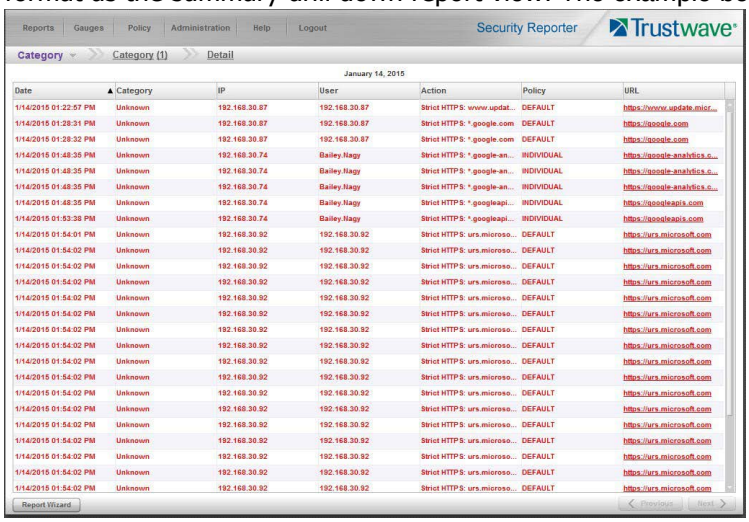
Click another column header to sort records by that specified column.

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 for productivity and security reports 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 Web Filter activity:



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: Date, report type name, IP, User, Action, Policy, Bandwidth (if using an SWG only), Site, URL, Type, Blocked. A record displayed in red text indicates a blocked URL request.

- **Date** - Displays the date of the record using the M/D/YYYY HH:MM:SS AM/PM format.
- **IP** - Displays the IP address of the end user for the request.
- **User** - Displays the username of the end user for the request. The entry in this column might include the user IP address, or the path and username (e.g. "logo\admin\jsmith").

- **Action** - If using a Web Filter, this column displays the type of filter action applied by the Web Filter and additional details, if applicable. 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

  If using an SWG, this column displays the type of action applied by SWG, such as Block, Bypass Scanning, Allow content and scan containers, Unknown, or None.
- **Policy** - If using an SWG, this column displays the name of the policy used by the SWG for this request.
- **Bandwidth** - This column displays if using an SWG only, and shows the amount of bandwidth used in the user's request.
- **Site** - Displays the URL for the user's request (e.g. "coors.com").
- **URL** - Displays the link for the page/object for the end user's request.
- **Type** - Displays the kind of requested item: "Object" or "Page".
- **Blocked** - Displays "True" if the request was blocked, or "False" if the request passed.

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.

4.3.3.2.3 Truncated data viewing tip

To view the entire text that displays truncated in a detail report view column, hover over the column to view the entire string of data in the column for a given record:

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

At the bottom right of the panel, **Previous** and **Next** buttons display. If the report has additional pages of content, you can step through the pages by clicking these buttons.

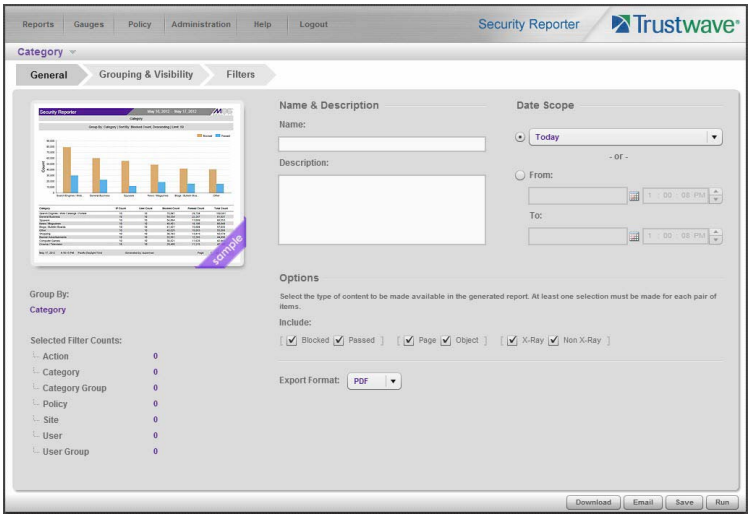
4.4 Customize, Maintain Reports

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

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:



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 (Category, Content Type, Rule, Spyware, Violation, Virus, Vulnerability Anti.Dote) 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 single level report

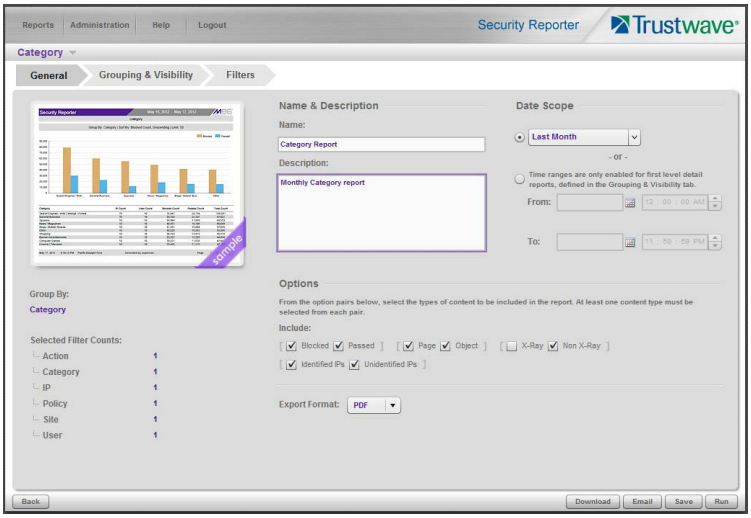
4.4.1.2 Build the report

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 data 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
   c. Select an **Export Format** used for download or email. Available selections are PDF (default), HTML, XLS, or CSV.

Tip: For very large reports, consider using CSV format. This 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 "Today".

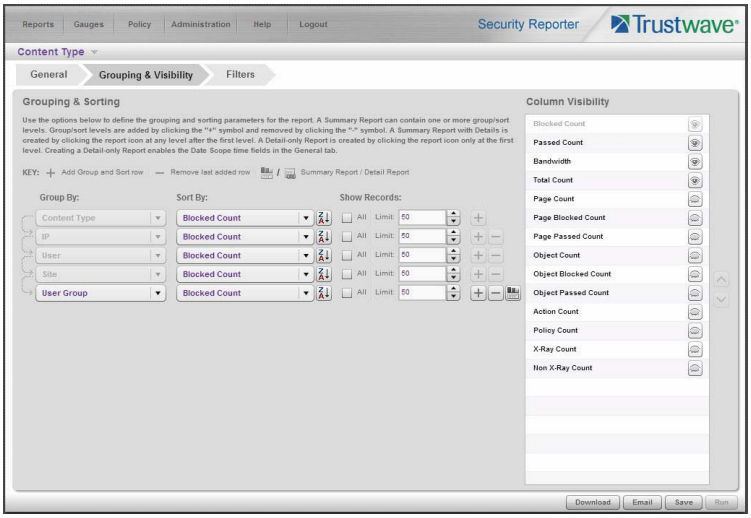


2. In the Grouping & Visibility tab:

   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 and Sorting icons:

-  - This icon indicates the report level will be sorted in ascending order. Click this icon to sort the report level in descending order.
-  - 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.

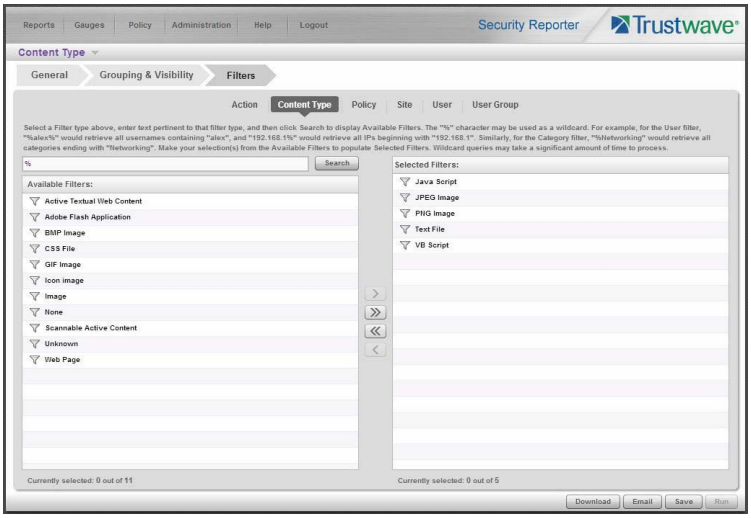
b. In the search field, enter a search term. You can use the % character one or more times as a wildcard (matching one or more characters).

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.



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.

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

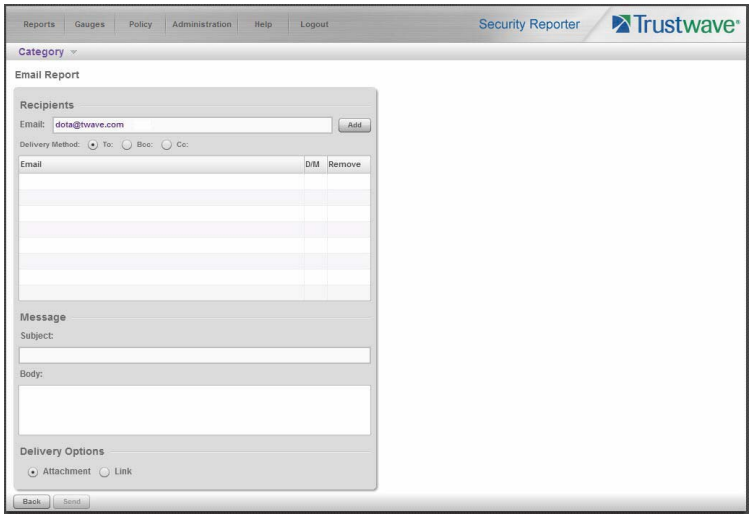
Note: Any Selected Filters items that include the wildcard character % will be evaluated for new matching data each time the report is run. This function is useful for reports on use names, malware names, or any data set that could include new members.

4.4.1.2.1 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):



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 the "X" 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.

For these reports, the bottom portion of the report view panel includes **< Previous** and **Next >** buttons used to navigate through a report view with multiple screens of records available to view. These buttons replace the page selection control.

4.4.1.3 Report Samples

The SR can generate hundreds of different types of reports based on the different criteria specified, in the PDF, HTML, XLS, and CSV formats. The following are some typical types of reports generated in the default PDF format.

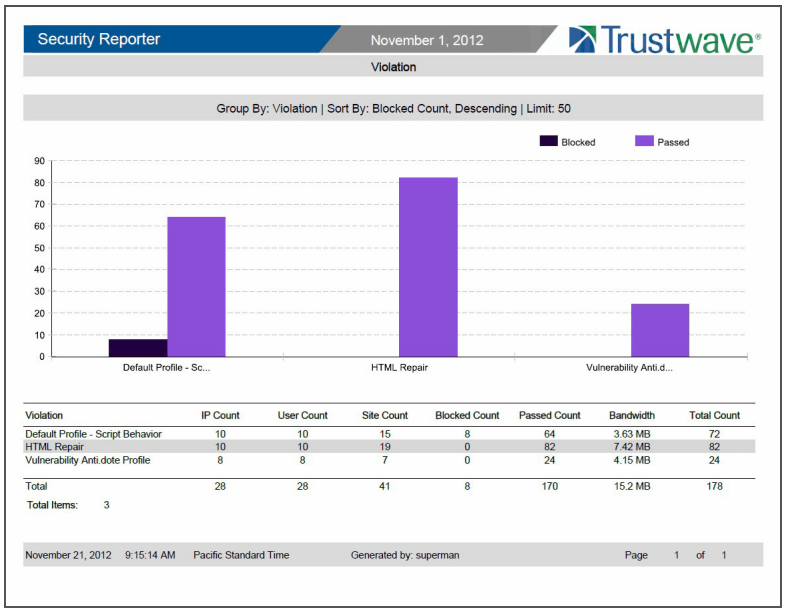
Tip: For very large reports, consider using CSV format. This format minimizes the resources needed to generate the report. XLS is the least efficient format. For more details see Trustwave Knowledge Base article Q16151.

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

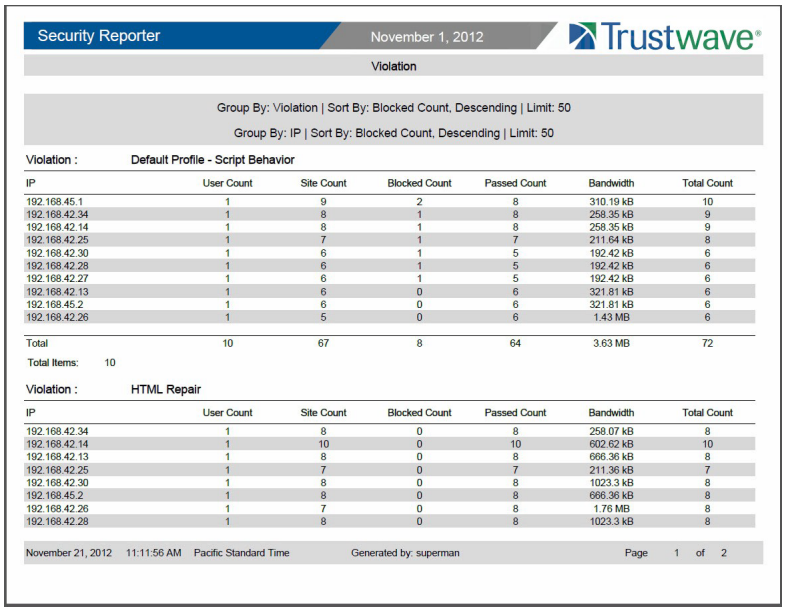


4.4.1.3.2 Multiple-level summary report

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

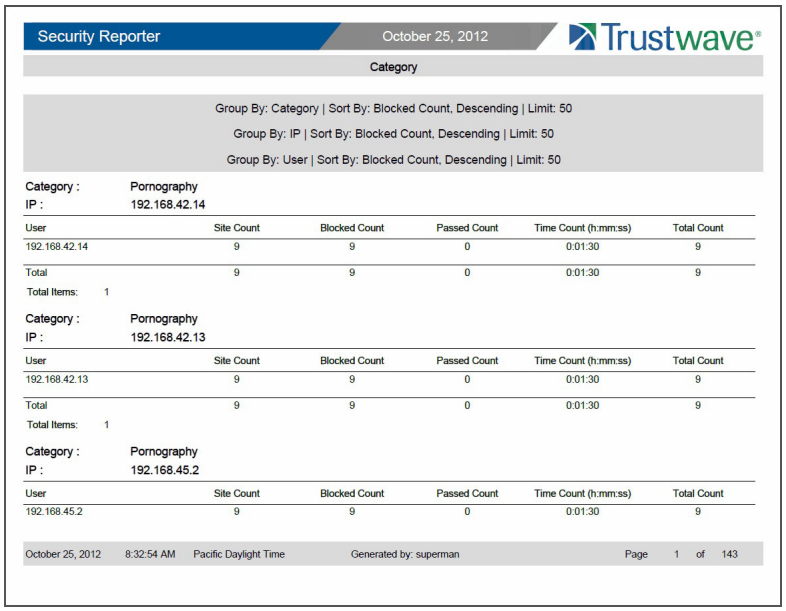
IP	User Count	Site Count	Blocked Count	Passed Count	Bandwidth	Total Count
192.168.45.1	1	9	2	8	310.19 kB	10
192.168.42.34	1	8	1	8	258.35 kB	9
192.168.42.14	1	8	1	8	258.35 kB	9
192.168.42.25	1	7	1	7	211.64 kB	8
192.168.42.30	1	6	1	5	192.42 kB	6
192.168.42.28	1	6	1	5	192.42 kB	6
192.168.42.27	1	6	1	5	192.42 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

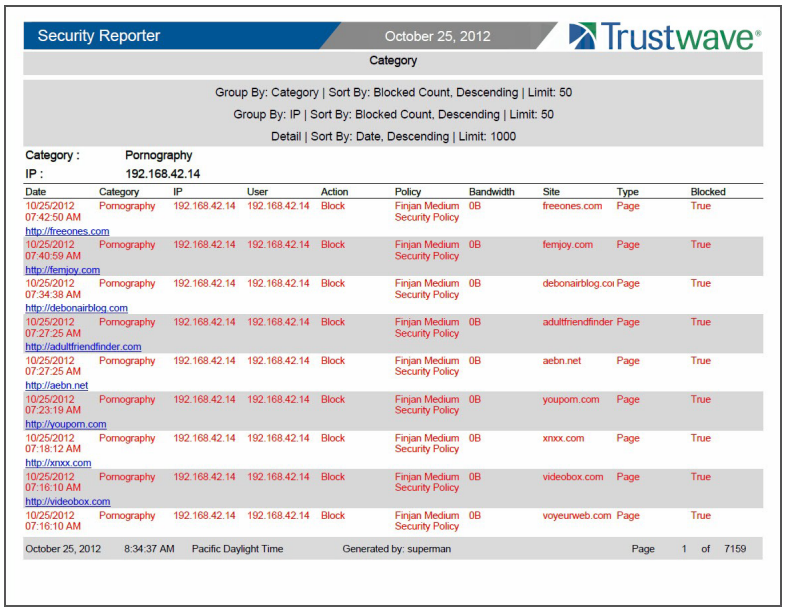
October 25, 2012 8:32:54 AM Pacific Daylight Time Generated by: superman Page 1 of 143

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 the entire 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 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
Detail | Sort By: Date, Descending | Limit: 1000

Category : Pornography
IP : 192.168.42.14

Date	Category	IP	User	Action	Policy	Bandwidth	Site	Type	Blocked
10/25/2012 07:42:50 AM http://freeones.com	Pornography	192.168.42.14	192.168.42.14	Block	Finjan Medium Security Policy	0B	freeones.com	Page	True
10/25/2012 07:40:59 AM http://femjoy.com	Pornography	192.168.42.14	192.168.42.14	Block	Finjan Medium Security Policy	0B	femjoy.com	Page	True
10/25/2012 07:34:38 AM http://debonairblog.com	Pornography	192.168.42.14	192.168.42.14	Block	Finjan Medium Security Policy	0B	debonairblog.co	Page	True
10/25/2012 07:27:25 AM http://adultfriendfinder.com	Pornography	192.168.42.14	192.168.42.14	Block	Finjan Medium Security Policy	0B	adultfriendfinder	Page	True
10/25/2012 07:27:25 AM http://aebn.net	Pornography	192.168.42.14	192.168.42.14	Block	Finjan Medium Security Policy	0B	aebn.net	Page	True
10/25/2012 07:23:19 AM http://youporn.com	Pornography	192.168.42.14	192.168.42.14	Block	Finjan Medium Security Policy	0B	youporn.com	Page	True
10/25/2012 07:18:12 AM http://xnxx.com	Pornography	192.168.42.14	192.168.42.14	Block	Finjan Medium Security Policy	0B	xnxx.com	Page	True
10/25/2012 07:16:10 AM http://videobox.com	Pornography	192.168.42.14	192.168.42.14	Block	Finjan Medium Security Policy	0B	videobox.com	Page	True
10/25/2012 07:16:10 AM	Pornography	192.168.42.14	192.168.42.14	Block	Finjan Medium Security Policy	0B	voyeurweb.com	Page	True

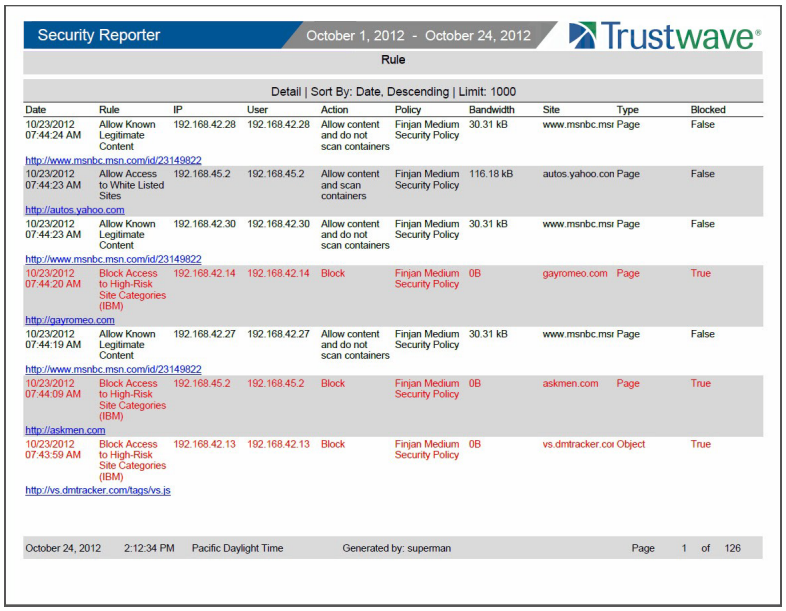
October 25, 2012 8:34:37 AM Pacific Daylight Time Generated by: superman Page 1 of 7159

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.

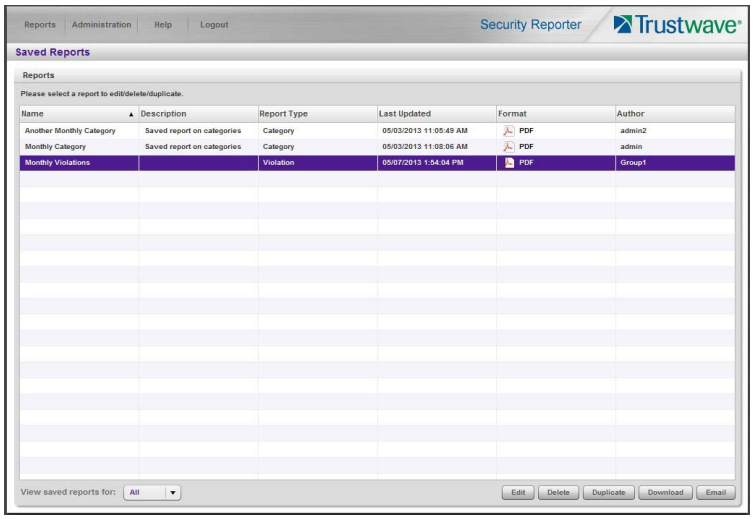
- Footer: Date and time, and time zone; Generated by username (if specified for inclusion in the report); Page number and page range



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:



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.

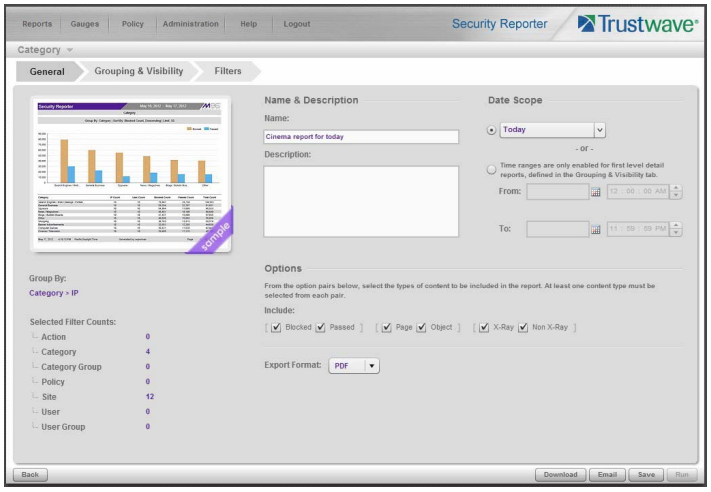
For each report record listed in the table, the following information displays: report Name, Description (if entered and saved for the report), Report Type (Category, Content Type, Rule, Spyware, Violation, Virus, Vulnerability Anti.Dote), Last Updated, Format (such as PDF, HTML, XLS, CSV), and Author.

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:



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.

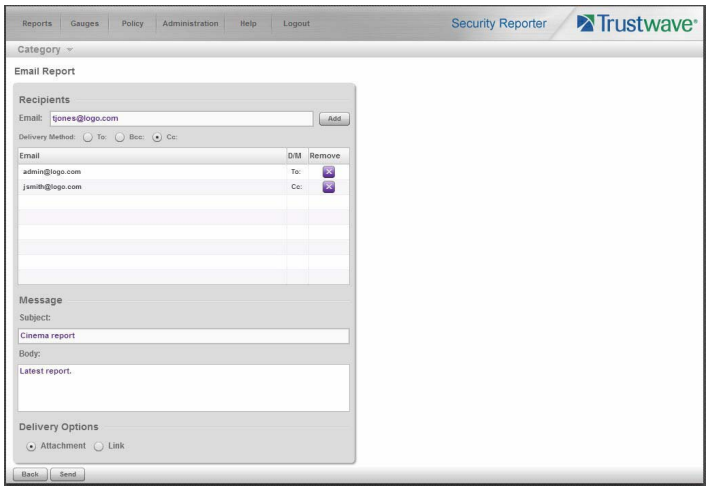
Tip: When a Global Administrator copies and edits a report that was created by another user, all groups are available. When a duplicated report is first saved, the author of the copy is set to the administrator performing this action.

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:



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.

Tip: Click **No** to close the dialog box without deleting the report.

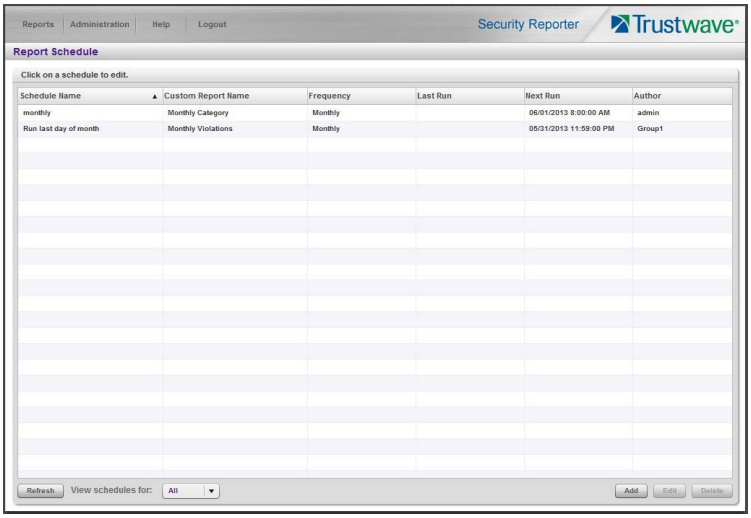
Note: If a report is scheduled to run via the Report Schedule option, deleting the report removes it from the Report Schedule list. See Manage Drill Down Report Scheduling for more information about scheduled reports.

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.

Note: See the Productivity and Security Reports Section for information about setting and maintaining schedules for security reports and advanced reports.

Navigate to Reports | Report Schedule to display the Report Schedule panel:



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 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.

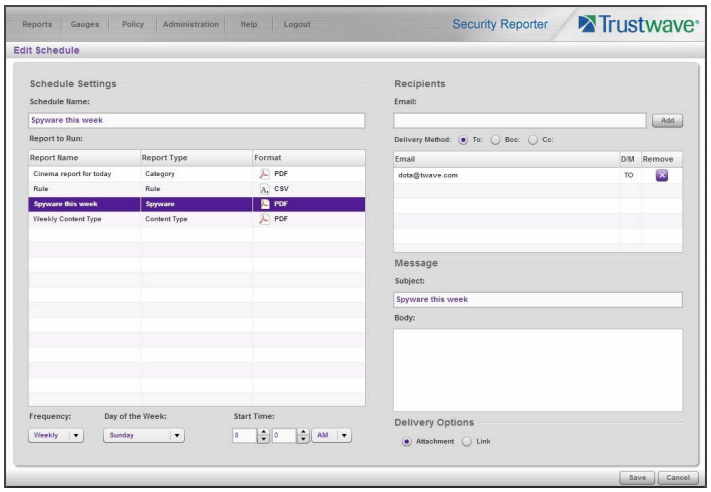
This panel is comprised of a table of report schedule records with buttons at the bottom. The following columns of information display for each record: Schedule Name, Custom Report Name, Frequency for running the report, dates and times of the Last Run and Next Run (MM/DD/YYYY H:MM:SS AM/PM time format), and Author.

Click the **Refresh** button to refresh the list of records, which de-selects any selected record.

Note: To enable or disable the Report Manager to run scheduled reports, see the Report Manager screen subsection of the System Configuration Section in this User Guide.

4.4.3.1 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:



   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.

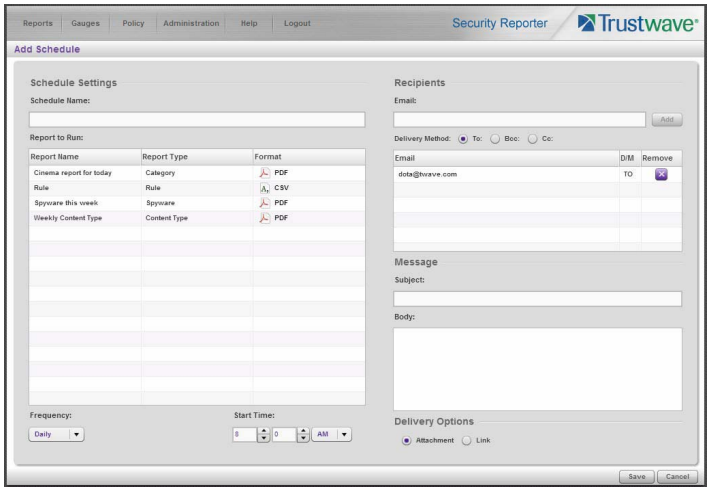
Tip: Click **Cancel** if you wish to return to the Report Schedule panel without saving your edits.

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.

4.4.3.2 Add a Drill Down Report Schedule

1. In the Report Schedule panel, click **Add** to display the Add Schedule panel:



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.

6. Click **Save** to add the scheduled event to the Report Schedule.

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.

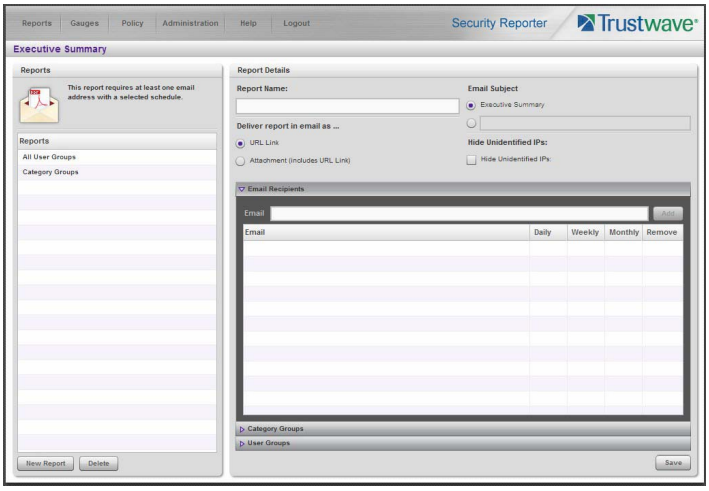
4.5 Specialized Reports

The following types of productivity reports from the Reports menu of the Report Manager are described in this section: Executive Summary Reports, Blocked Request Reports, and Time Usage Reports.

4.5.1 Executive Summary

The Executive Summary option is used for specifying email addresses of users authorized to receive daily, weekly, and/or monthly bar and line chart productivity reports showing activity in library category groups or user groups of your choice.

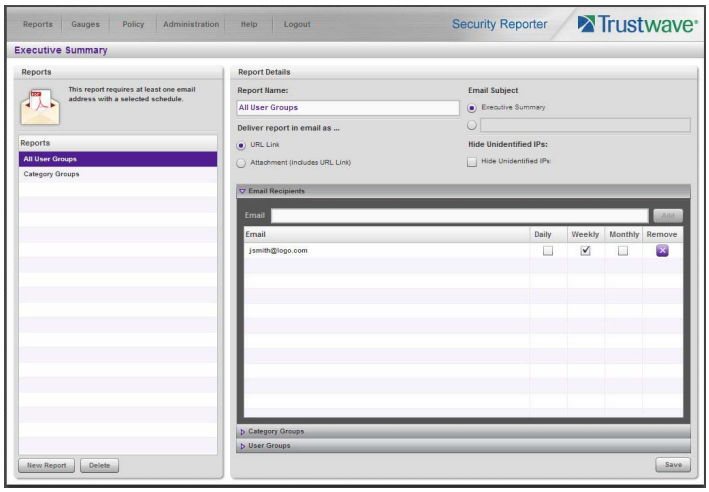
In the navigation toolbar, hover over the Reports menu link and select **Executive Summary** to display the Executive Summary panel:



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.



   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 enabling this feature, the generated report will only hide hit counts for IP addresses in sections of the report labeled "Users." IP hit counts **will be included** for all other sections of the report, such as those labeled "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)

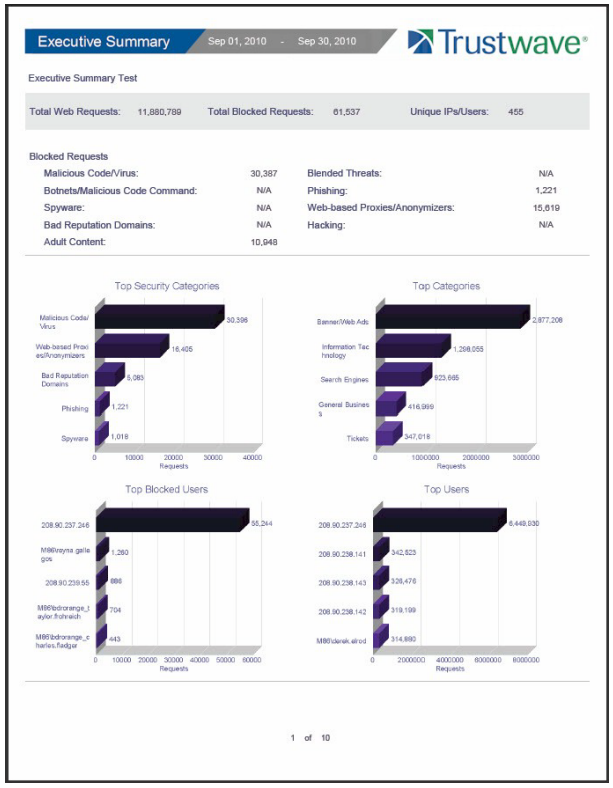
The header of the generated report includes the title and date range. The footer includes the page number and page range.

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."

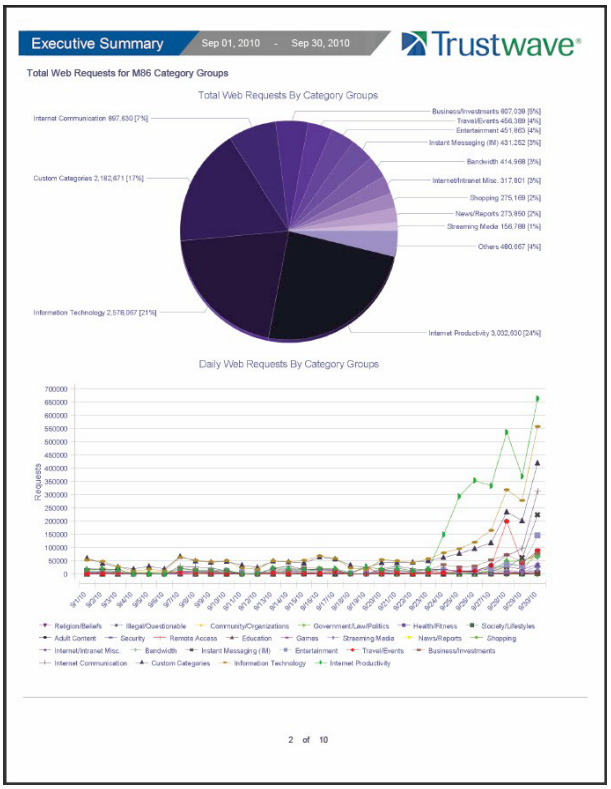
Bar charts for Top Security Risks (library categories), Top Categories, Top Blocked Users, and Top Users show the top five categories/users and their corresponding total Requests.



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.

For Weekly and Monthly reports, the bottom half of the second page includes a line chart for Daily Web Requests by Category Groups. Each category group in the chart is represented by a colored symbol that

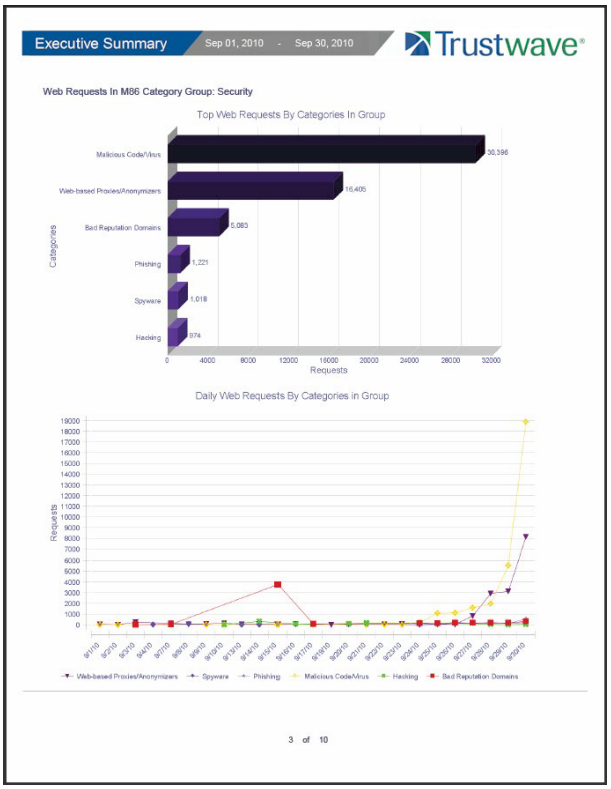
can be identified by the key at the bottom of the page. The range of Requests is shown to the left of the chart, and the days (M/D/YY) are shown beneath the chart.



The third page includes a bar chart depicting Top Web Requests By Categories In Group 'X', in which 'X' represents the name of the category group. The top 15 affected library categories in the group are named in the Categories list to the left, and each library category is represented in the chart by a bar and corresponding number of requests. The range of Requests is shown beneath the chart.

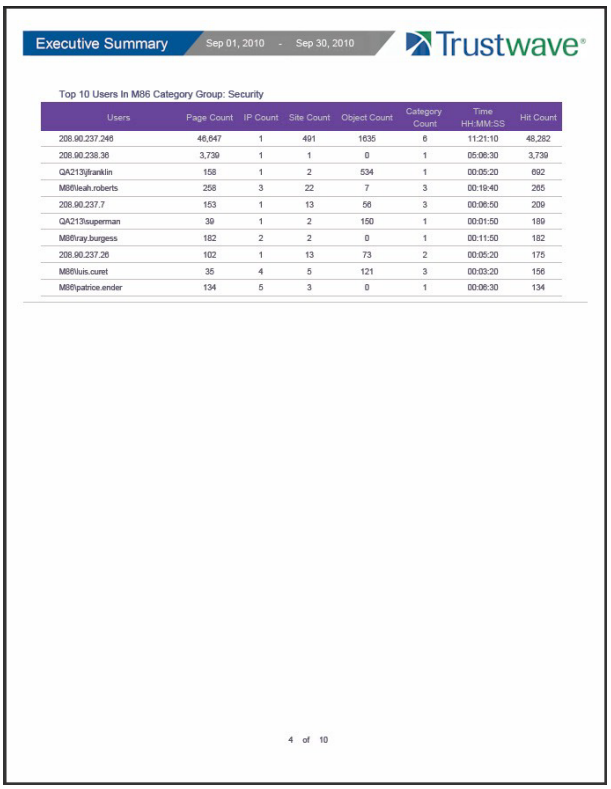
For Weekly and Monthly reports, the bottom half of the third page includes a line chart for Top Daily Web Requests by Categories in Group. Each library category in the chart is represented by a colored symbol

that can be identified by the key at the bottom of the page. The range of Requests is shown to the left of the chart, and the days (M/D/YY) are shown beneath the chart.



For Daily reports, the bottom half of the third page includes a chart showing the Top 10 Users In Category Group 'X', in which 'X' represents the name of the category group. The top 10 Users are listed in this chart, along with each user's corresponding Page Count, IP Count, Site Count, Category Count, Time HH:MM:SS, and Hit Count.

For Weekly and Monthly reports, the fourth page includes the Top 10 Users In Category Group 'X' chart:



Executive Summary Sep 01, 2010 - Sep 30, 2010 Trustwave

Top 10 Users In M86 Category Group: Security

Users	Page Count	IP Count	Site Count	Object Count	Category Count	Time HH:MM:SS	Hit Count
208.90.237.246	46,647	1	491	1635	6	11:21:10	48,282
208.90.238.36	3,739	1	1	0	1	05:08:30	3,739
QA213\jfranklin	158	1	2	534	1	00:05:20	692
M86\leah.roberts	258	3	22	7	3	00:19:40	265
208.90.237.7	153	1	13	56	3	00:06:50	209
QA213\superman	39	1	2	150	1	00:01:50	189
M86\ray.burgess	182	2	2	0	1	00:11:50	182
208.90.237.26	102	1	13	73	2	00:05:20	175
M86\luis.curet	35	4	5	121	3	00:03:20	156
M86\patrice.ender	134	5	3	0	1	00:06:30	134

4 of 10

The balance of the report is comprised of statistics for each of the remaining category groups, represented by report page 3, and page 4 for Weekly and Monthly reports.

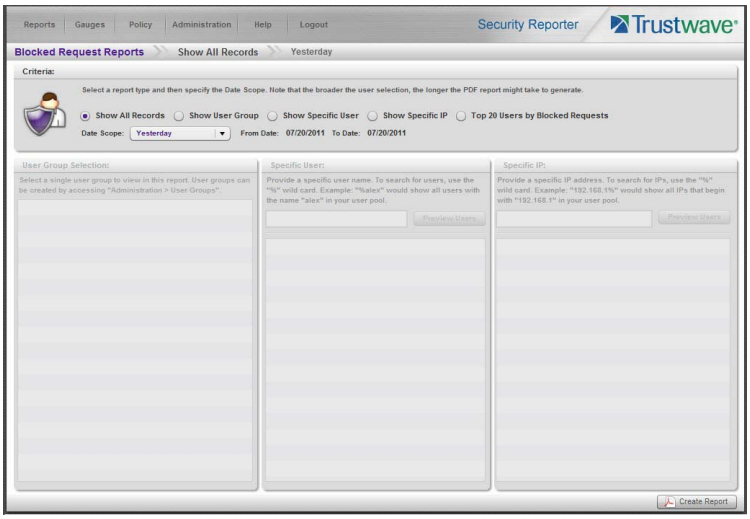
4.5.2 Blocked Request Reports

The Blocked Request Reports option is used for obtaining results of blocked URLs end users attempted to access within a specified time period.

Note: If using a Web Filter only, the Blocked Request Reports option does not display if the Block Request Count feature is disabled in the System Configuration administrator console.

Refer to the Optional Features screen sub-section of the System Configuration Section of this user guide for information about enabling or disabling the Block Request Count feature.

In the navigation toolbar, hover over the Reports menu link and select **Blocked Request** to display the Blocked Request Reports panel:



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 choosing this option, the Date Scope field displays "Yesterday" and yesterday's date.
   - **Show User Group** - If choosing this option, select the user group from the User Group Selection list box below. The Date Scope field displays "Yesterday" and yesterday's date.
   - **Show Specific User** - If choosing this option, enter the username—or a portion of the username with the '%' wildcard—in the Specific User 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 choosing 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 choosing this option, make a selection from the **Date Scope** field to display the date range for that time period: Yesterday, Last Week, Last Month, 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.

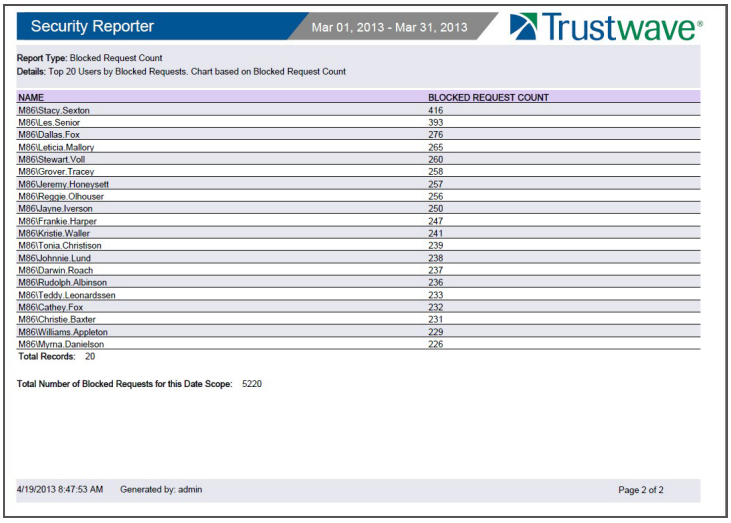
'RESULTS FOR: the date' displays above the NAME column header if the report criteria is other than "Top 20 Users by Blocked Requests".

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 Mar 01, 2013 - Mar 31, 2013 Trustwave

Report Type: Blocked Request Count
Details: Top 20 Users by Blocked Requests. Chart based on Blocked Request Count

NAME	BLOCKED REQUEST COUNT
M86\Stacy.Sexton	416
M86\Les.Senior	393
M86\Dallas.Fox	276
M86\Leticia.Mallory	265
M86\Stewart.Voll	260
M86\Grover.Tracey	258
M86\Jeremy.Honeysett	257
M86\Reggie.Olhouser	256
M86\Jayne.Iverson	250
M86\Frankie.Harper	247
M86\Kristie.Waller	241
M86\Tonia.Christison	239
M86\Johnnie.Lund	238
M86\Darwin.Roach	237
M86\Rudolph.Albinson	236
M86\Teddy.Leonardssen	233
M86\Cathey.Fox	232
M86\Christie.Baxter	231
M86\Williams.Appleton	229
M86\Myrna.Danielson	226

Total Records: 20

Total Number of Blocked Requests for this Date Scope: 5220

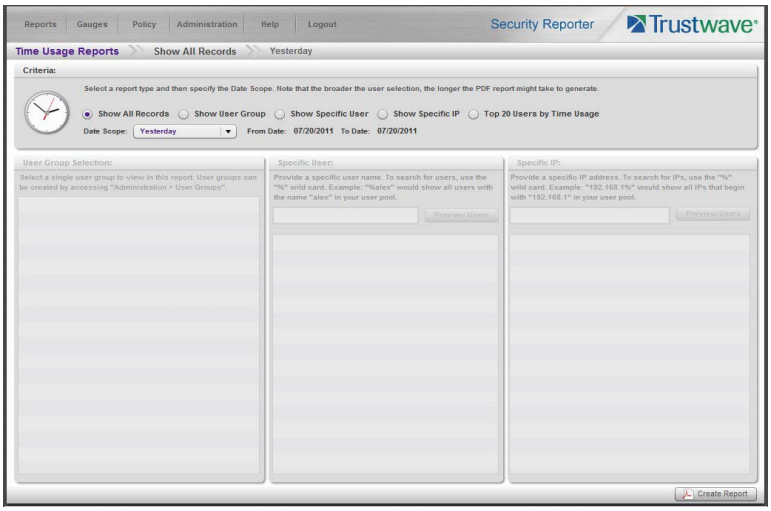
4/19/2013 8:47:53 AM Generated by: admin Page 2 of 2

4.5.3 Time Usage Reports

The Time Usage Reports option is used for obtaining end user Internet usage activity for a specified time period, based on the Time Usage algorithm. This algorithm calculates the amount of time an end user spent accessing a given page or object, disregarding the number of seconds per hit, and counting each unique minute of Web time as one minute. Using this algorithm, an end user could never have more than 24 hours of Web time within a given 24-hour period.

Note: The Time Usage Reports option does not display if the Time Usage feature is disabled in the System Configuration administrator console. Refer to the Optional Features screen sub-section of the System Configuration Section of this user guide for information about enabling or disabling the Time Usage feature.

In the navigation toolbar, hover over the Reports menu link and select **Time Usage** to display the Time Usage Reports panel:



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 choosing this option, the Date Scope field displays "Yesterday" and yesterday's date.
   - **Show User Group** - If choosing this option, select the user group from the User Group Selection list box below. The Date Scope field displays "Yesterday" and yesterday's date.
   - **Show Specific User** - If choosing this option, enter the username—or a portion of the username with the '%' wildcard—in the Specific User 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 choosing 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 choosing this option, make a selection from the **Date Scope** field to display the date range for that time period: Yesterday, Last Week, Last Month, 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 - 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

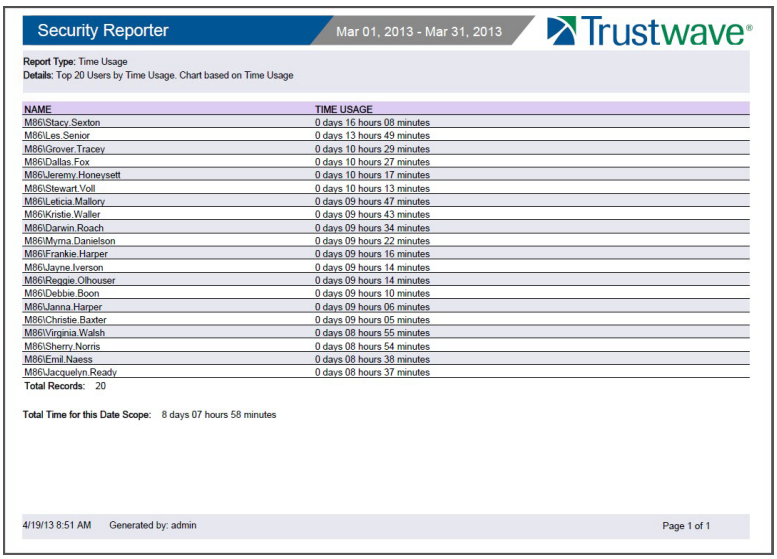
The header of the generated Time Usage report includes the date range, Report Type, and Details criteria.

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 Mar 01, 2013 - Mar 31, 2013 Trustwave

Report Type: Time Usage
Details: Top 20 Users by Time Usage. Chart based on Time Usage

NAME	TIME USAGE
M86\Stacy.Sexton	0 days 16 hours 08 minutes
M86\Les.Senior	0 days 13 hours 49 minutes
M86\Grover.Tracey	0 days 10 hours 29 minutes
M86\Dallas.Fox	0 days 10 hours 27 minutes
M86\Jeremy.Honeysett	0 days 10 hours 17 minutes
M86\Stewart.Voll	0 days 10 hours 13 minutes
M86\Leticia.Mallory	0 days 09 hours 47 minutes
M86\Kristie.Waller	0 days 09 hours 43 minutes
M86\Darwin.Roach	0 days 09 hours 34 minutes
M86\Myrna.Danielson	0 days 09 hours 22 minutes
M86\Frankie.Harper	0 days 09 hours 16 minutes
M86\Jayne.Iverson	0 days 09 hours 14 minutes
M86\Reggie.Olhouser	0 days 09 hours 14 minutes
M86\Debbie.Boon	0 days 09 hours 10 minutes
M86\Janna.Harper	0 days 09 hours 06 minutes
M86\Christie.Baxter	0 days 09 hours 05 minutes
M86\Virginia.Walsh	0 days 08 hours 55 minutes
M86\Sherry.Norris	0 days 08 hours 54 minutes
M86\Emil.Naess	0 days 08 hours 38 minutes
M86\Jacquelyn.Ready	0 days 08 hours 37 minutes

Total Records: 20

Total Time for this Date Scope: 8 days 07 hours 58 minutes

4/19/13 8:51 AM Generated by: admin Page 1 of 1

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:

12:00:01 www.trustwave.com
12:00:10 www.abc.com
12:01:00 www.trustwave.com
12:02:04 www.whitepages.com
12:05:58 www.yellowpages.com
12:05:58 www.yellowpages.com/714.jsp
12:05:59 www.yellowpages.com/phone_number.gif
12:07:03 www.google.com
12:07:33 www.yahoo.com
12:08:23 www.news.com
12:08:30 www.usatoday.com
12:08:59 www.usatoday.com/usa.gif
12:09:00 www.usatoday.com/ca.gif
12:09:01 www.yahoo.com
12:09:02 http://200.100.10.65:88
12:09:03 www.abc.com
12:09:04 www.nbc.com

The total for this end user is based on a nine-minute time span that includes 17 entries in the log, and seven unique minute entries: 00, 01, 02, 05, 07, 08, and 09.

5 Real Time Reports Section

5.1 Introduction

This section of the user guide provides instructions to administrators on how to utilize data from Web Filter logs for monitoring end user Internet and network activity in real time.

- Gauge Components - Section 5.2 describes the types of gauges, the components of a gauge, how to read a gauge, and how to perform shortcuts using gauges.
- Custom Gauge Setup, Usage - Section 5.3 explains how gauges are configured and monitored.
- Alerts, Lockout Management - Section 5.4 explains how alerts are set up and used, and how to manage end user lockouts.
- Analyze Usage Trends - Section 5.5 explains how trend charts are used for assessing end user Internet/network activity.
- Identify Users, Categories - Section 5.6 explains how to perform a custom search on Internet/network usage by a specified user, or for a specified category or category group.

These features are disabled by default. To enable or disable these features, use the Security Reporter Maintenance feature in the Device Registry. For more information, see Section 3.3.4.3.

Caution: Real-time Reporting consumes significant processing power and other resources. Data processing will be slower, and generation of Productivity and Security reports will be less responsive, if Real-time Reporting is enabled.

5.2 Gauge Components

5.2.1 Types of Gauges

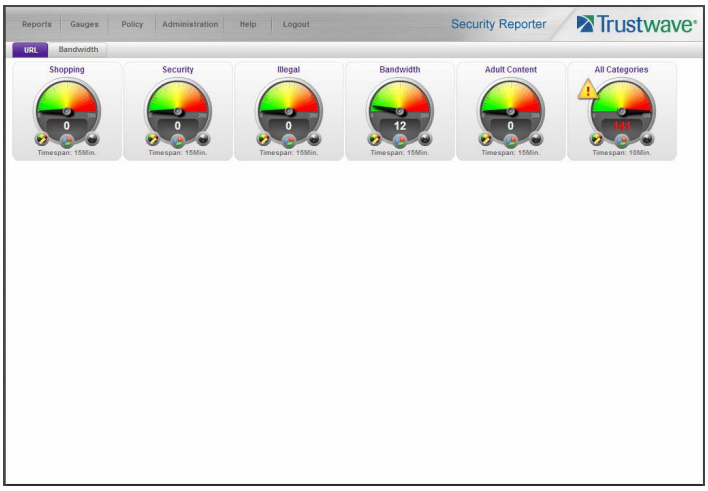
There are two types of gauges that are used for monitoring user activity on the network: URL gauges and bandwidth gauges.

Either gauge type is referred to as a "gauge group" if it is comprised of a group of library categories or protocol(s)/port numbers.

5.2.1.1 URL gauges

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

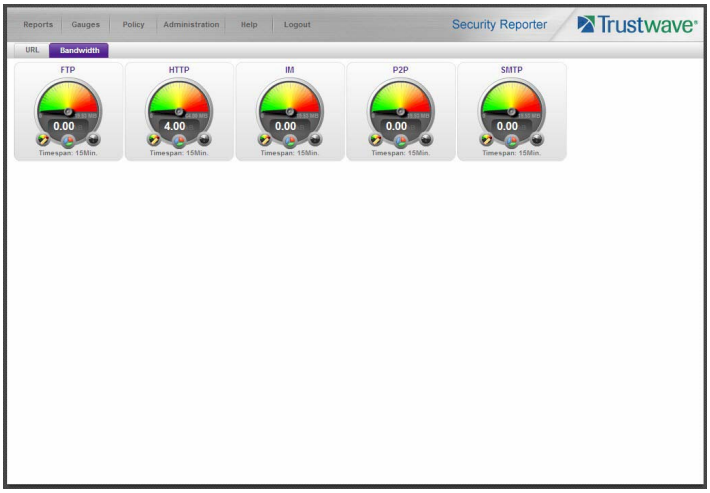
When clicking **Gauges** in the navigation toolbar, the URL gauges Dashboard panel displays showing overall activity in URL gauges:



5.2.1.2 Bandwidth gauges

A bandwidth gauge is comprised of protocols/port numbers and monitors a targeted user group's inbound/outbound network traffic generated for specified protocols/port numbers.

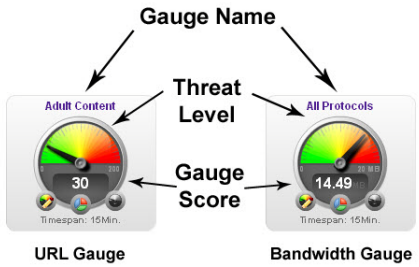
With the URL gauges Dashboard displayed, click the Bandwidth tab—located beside the URL tab—to display the Bandwidth gauges Dashboard panel showing overall activity in bandwidth gauges:



5.2.2 Anatomy of a Gauge

Understanding the anatomy of a gauge will help you better configure and maintain gauges to monitor network threats.

The illustration below depicts a URL gauge and a bandwidth gauge and some of their components:



Gauge Name: The name of the gauge displays above the gauge icon.

Timespan: The Timespan for the gauge's activity displays beneath the gauge icon.

Threat Level: The top portion of the gauge is comprised of three colored sections, one in which the gauge's dial is positioned: green (safe) section, yellow (warning) section, or red (network threat) section. This position of the dial represents the current threat level for the gauge.

Gauge Score: The bottom portion of the gauge contains a numerical score, based on the Timespan, activity of end users assigned to the gauge, and type of gauge:

- URL gauge - score includes the total number of end user hits (page count plus blocked object count) for all library categories the gauge monitors.
- Bandwidth gauge - score includes the total number of bytes (kB, MB, GB) of inbound/outbound end user traffic for all protocols/ports the gauge monitors.

5.2.3 How to Read a Gauge

Gauges become active when end users access URLs/ports included in that gauge. Activity is depicted by the position of the dial within one of three sections in the gauge—green, yellow, or red—and by the gauge's score.

The score will always reflect activity from the most recent past number of specified minutes set up in the Timespan, unless gauge settings were manually changed and saved, at which point the gauge is reset.

If the threat for a gauge is currently low or medium, the score displays in white text.

The image to the right shows a URL gauge with its score displayed in white text and the dial positioned in the green section of the gauge, indicating there is no immediate threat for the library categories in this gauge group.

If the threat level for a gauge is high (exceeding 66 percent of the ceiling established for a gauge), the score displays in red text with a flashing yellow triangle containing a red exclamation point. However, if the score drops below 66 percent within the Timespan set up for the gauge, the text changes from red to solid white again.

The image to the right shows a URL gauge that has exceeded its threshold limit. The source of the threat can be investigated by drilling down into the gauge. It may be that one or more library categories within the gauge currently have a high score, and that one or more end users are responsible for this threat.

For bandwidth gauges, if the total byte score reaches the threshold limit, the score displays in red text and the triangle flashes.

5.2.4 Bandwidth Gauge Components

Incoming/outgoing bandwidth gauges include the following gauges and ports (TCP and/or UDP) to monitor:

- **HTTP** - Hyper Text Transfer Protocol gauge monitors the protocol used for transferring files via the World Wide Web or an intranet.

  This protocol gauge is comprised of gauges for monitoring the following ports by default:

  - **80** - HTTP TCP port used for transferring and listening
  - **443** - HTTPS TCP/UDP port used for encrypted transmission over TLS/SSL
  - **8080** - HTTP Alternate (http-alt) TCP port used under the following conditions: when running a second Web server on the same machine (the other is using port 80), as a Web proxy and caching server, or when running a Web server as a non-root user. This port is used for Tomcat.

- **FTP** - File Transfer Protocol gauge monitors the protocol used for transferring files from one computer to another on the Internet or an intranet.

  This protocol gauge is comprised of gauges for monitoring the following ports by default:

  - **20** - FTP TCP/UDP data port for file transfer
  - **21** - FTP TCP/UDP control (command) port for file transfer

- **SMTP** - Simple Mail Transfer Protocol gauge monitors the protocol used for transferring email messages from one server to another.

  This protocol gauge is comprised of gauges for monitoring the following ports by default:

  - **25** - SMTP TCP/UDP port used for email routing between mail server email messages
  - **110** - POP3 (Post Office Protocol version 3) TCP port used for sending/retrieving email messages

- **P2P** - Peer-to-Peer gauge monitors the protocol used for communication between computing devices—desktops, servers, and other smart devices—that are linked directly to each other.

  This protocol gauge is comprised of gauges for monitoring the following ports by default:

  - **1214** - TCP/UDP port for Kazaa, Morpheous, Grokster, etc.
  - **4662** - TCP/UDP port for eMule, eDonkey, etc.
  - **4665** - TCP/UDP port for eDonkey 2000
  - **6346** - TCP/UDP port for Gnutella file sharing (FrostWire, LimeWire, BearShare, etc.)

- **6347** - TCP/UDP port for Gnutella
- **6699** - UDP port for Napster
- **6881** - TCP/UDP port for BitTorrent

- **IM** - Instant Messaging gauge monitors the protocol used for direct connections between workstations either locally or across the Internet.

  This protocol gauge is comprised of gauges for monitoring the following ports by default:

  - **1863** - TCP/UDP port for MSN Messenger
  - **5050** - TCP/UDP port for Yahoo! Messenger
  - **5190** - TCP/UDP port for ICQ and AOL Instant Messenger (AIM)
  - **5222** - TCP/UDP port for Google Talk, XMPP/Jabber client connection

5.2.5 Gauge Usage Shortcuts

The following shortcut actions can be performed in the gauges dashboard:

- **View Gauge Ranking** - Clicking a gauge or right-clicking a gauge and selecting this topic from the menu displays the Gauge Ranking panel. The table in this panel contains a list of library categories/protocols/ports that comprise the gauge, along with the list of current users driving the gauge's score. (See View End User Gauge Activity.)

•**Edit Gauge** - Clicking the left icon at the bottom of a gauge—or right-clicking a gauge and then selecting this menu topic—displays the panel that lets you edit the gauge's components. This is a shortcut to use instead of going to the Add/Edit Gauges panel, selecting the gauge, and then clicking Edit Gauge. (See Modify a Gauge.)

•**Hide Gauge** - Clicking the right icon at the bottom of a gauge—or right-clicking a gauge and then selecting this menu topic—lets you remove the gauge from the dashboard. This is a shortcut to use instead of going to Dashboard Settings, selecting the gauge from the list, and then clicking the Hide Gauge icon. (See Hide, Disable, Delete, Rearrange Gauges.)

•**Trend Charts** - Clicking the middle icon at the bottom of a gauge—or right-clicking a gauge and then selecting this menu topic—displays a Trend Chart for this particular gauge that lets you analyze the gauge's activity. (See View Trend Charts.)

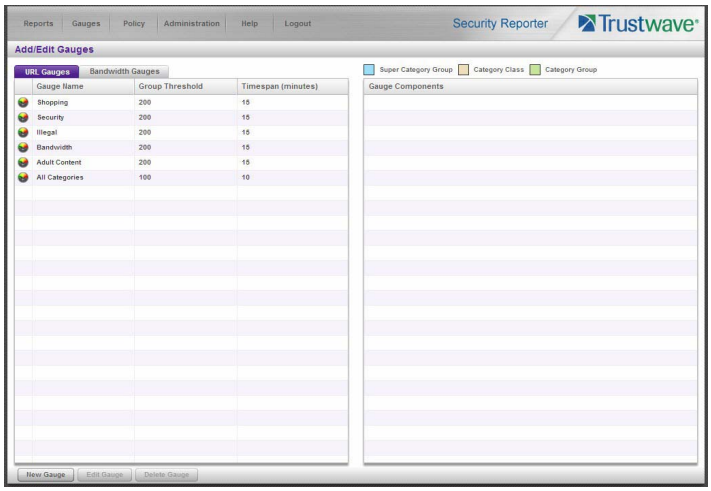
•**Disable Gauge** - Right-clicking a gauge and then selecting this menu topic lets you disable a gauge. This is a shortcut to use instead of going to Dashboard Settings, selecting the gauge from the list, and then clicking the Disable Gauge icon. (See Hide, Disable, Delete, Rearrange Gauges)

- **Delete Gauge** - Right-clicking a gauge and then selecting this menu topic lets you delete a gauge. This is a shortcut to use instead of going to Dashboard Settings, selecting the gauge from the list, and then clicking the Delete Gauge icon. (See Hide, Disable, Delete, Rearrange Gauges.)

5.3 Custom Gauge Setup, Usage

Once an account for the group administrator is set up, he/she can begin setting up gauges for monitoring end users' Internet activity.

1. In the navigation toolbar, hover over the Gauges menu link and select **Add/Edit Gauges** to open the Add/Edit Gauges panel:



   By default, a sub-panel containing the URL Gauges and Bandwidth Gauges tabs displays to the left, and the empty, target Gauge Components sub-panel displays to the right.

2. Do the following to view the contents in the tab to be used:

   - Click **URL Gauges** if this tab currently does not display. By default, this tab includes the following list of Gauge Names: Shopping, Security, Illegal, Bandwidth, Adult Content.

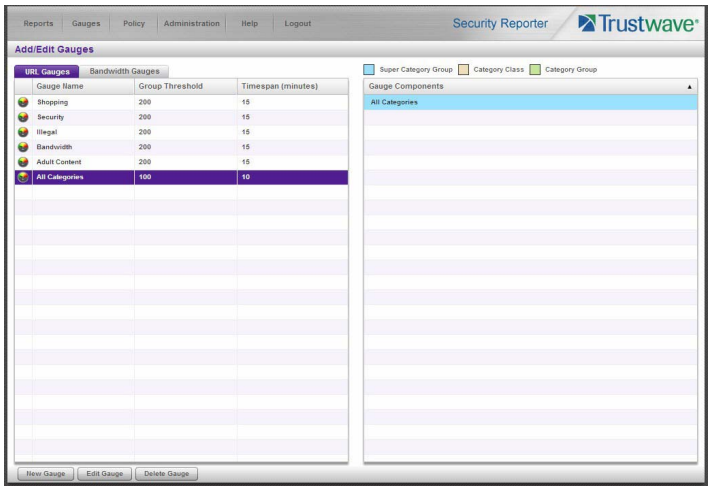
     For each Gauge Name in this list, the following information displays: Group Threshold (*200*), Timespan (minutes)—*15* by default.

   - Click **Bandwidth Gauges** to view the contents of this tab. By default, this tab includes the following list of Gauge Names: FTP, HTTP, IM, P2P, SMTP.

     For each Gauge Name in this list, the following information displays: Group Threshold (*20 MB*), Timespan (minutes)—*15* by default.

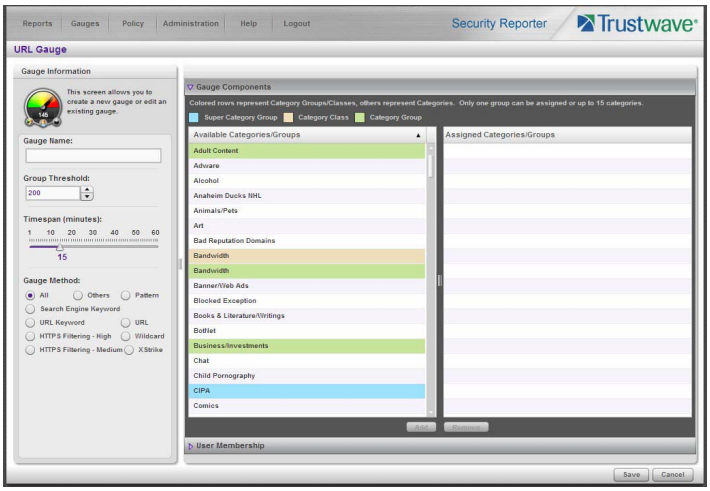
Note: Up to five bandwidth gauges can be used at a time. If a different bandwidth gauge is needed, one of the default bandwidth gauges must be deleted before a new bandwidth gauge can be added.

3. Select a Gauge Name to display a list of its library categories/protocols/ports in the Gauge Components sub-panel:



5.3.1 Add a Gauge

In the Add/Edit Gauge panel, click **New Gauge** to display URL Gauge panel:



This panel includes the Gauge Information sub-panel to the left and accordions for Gauge Components and User Membership to the right.

When adding a new gauge, do the following:

- Name the gauge, and specify group threshold limits, timespan values, and the method(s) to be used by the gauge (see Specify Gauge Information).
- Select the library categories/protocols/ports for the gauge to monitor (see Define Gauge Components).
- Assign user groups whose end users' Internet/network activity will be monitored by the gauge (see Assign User Groups).

5.3.1.1 Specify Gauge Information

In the Gauge Information sub-panel:

1. Type in at least two characters for the **Gauge Name** using upper and/or lowercase alphanumeric characters, and spaces, if desired.
2. Specify the **Group Threshold** ceiling of gauge activity. The default and recommended value is 200 for a URL gauge and 20 MB for a bandwidth gauge. This ceiling can be adjusted after using SR for awhile and evaluating activity levels at your organization.

   To modify information in this field, type a specific value in the pre-populated field, and/or use the up/down arrow buttons to increment/decrement the current byte value by one. Make a selection from the pull-down menu if you need to change the byte unit (kB, MB, GB).
3. Use the slider tool to specify the **Timespan (minutes)** for tracking gauge activity (1 - 60 minutes). The default and recommended value is 15 minutes. The timespan will always keep pace with the current time period, so that if a timespan of 15 minutes is specified, the gauge will always reflect the most recent end user activity from the past 15 minutes.
4. If necessary, specify a different **Gauge Method** to be used for tracking gauge activity:
   - For a URL gauge - **All** (default), **Others** (all gauge methods, not including Keywords or URLs), **Pattern**, **Search Engine Keyword**, **URL Keyword**, **URL**, **HTTPS Filtering - High**, **HTTPS Filtering - Medium**, **Wildcard**, **X Strike**.
   - For a bandwidth gauge - **Inbound, Outbound**, **Both** (default).

Note: If the selected gauge method is "Search Engine Keyword" or "URL Keyword", Filter Options for end user profiles on the source Web Filter used with this SR must have "Search Engine Keyword Filter Control" or "URL Keyword Filter Control" enabled.

5.3.1.2 Define Gauge Components

Next, specify which library categories/protocols/ports the gauge will use for monitoring end user activity.

Note: At least one library category/protocol/port must be selected when creating a gauge. The maximum number of library categories/ports that can be selected/added is 15.

1. From the Available Categories/Groups list in the Gauge Components accordion, select an available Category Group/Class or library categories/ports the end user should not access.

   For bandwidth gauges, to modify criteria in the **Port Number** field, type a specific value in the pre-populated field, and/or use the up/down arrow buttons to increment/decrement the current value by one.

Note: For a global administrator, Available Categories/Groups include All Categories and CIPA selections for URL gauges, and All Protocols and Common Protocols selections for bandwidth gauges, if these selections are not currently in use by another gauge. Common Protocols include: FTP, HTTP, IM, P2P, and SMTP.

Even though a group administrator does not have the Common Protocols bandwidth selection available when creating a gauge, this Super Category Group is available to him/her via the User Summary Panel. Thus, he/she will have the ability to lock out all users (assigned to him/her) who are currently using FTP, HTTP, IM, P2P and SMTP protocols. (See Monitor, Restrict End User Activity.)

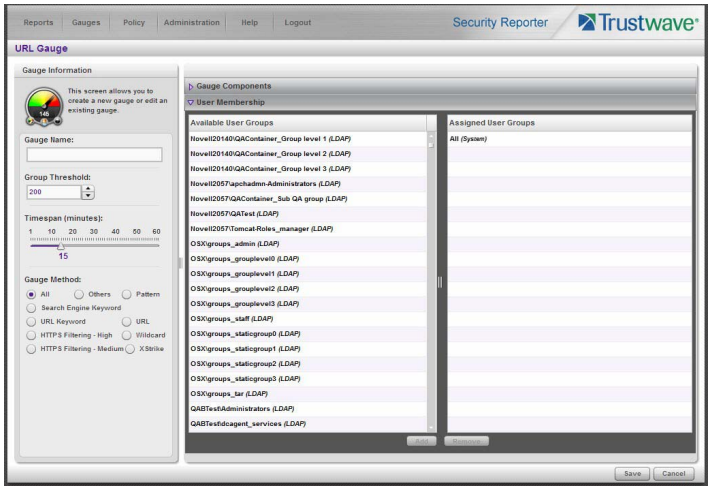
2. Click **Add** (for URL gauges) or **Add Port** (for bandwidth gauges) to move the selection(s) to the Assigned Categories/Groups list box.

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

5.3.1.3 Assign user groups

To assign user groups to be monitored by the gauge:

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



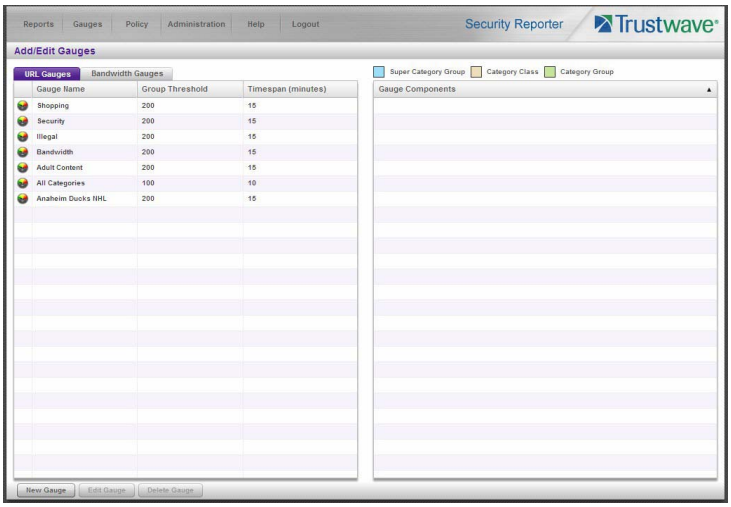
Note: The base group displays in the Assigned list box by default but can be removed. This group consists of all end users whose network activities are set up to be monitored by the designated group administrator.

2. From the Available User Groups list, select the user group to highlight it.
3. Click **Add** to move the user group to the Assigned User Groups list box.

Tip: To remove a user group from the Assigned User Groups list box, click the user group to highlight it, and then click Remove to move the group back to the Available User Groups list.

5.3.1.4 Save gauge settings

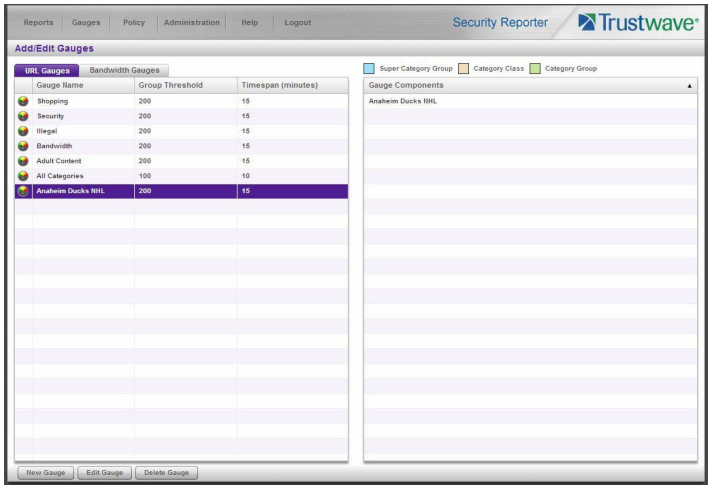
After adding users, click **Save** to return to the Add/Edit Gauges panel that now includes the name of the gauge you just added:



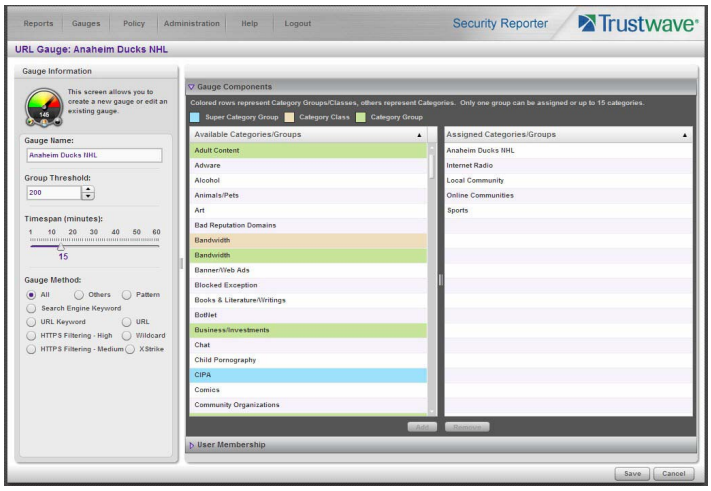
5.3.2 Modify a Gauge

5.3.2.1 Edit gauge settings

1. In the Add/Edit Gauge panel, click the URL Gauges or Bandwidth Gauges tab.
2. Select the gauge from the list to activate all buttons below and populate the Gauge Components sub-panel to the right:



3. Click **Edit Gauge** to display the URL Gauge or Bandwidth Gauge panel showing the Gauge Information sub-panel to the left and the Gauge Components sub-panel to the right, populated with settings previously saved for the gauge:



Tip: This panel is also accessible from the gauges dashboard by clicking the Edit Gauge icon at the bottom left of the gauge.

4. Edit any of the following criteria, as necessary:
   - Gauge Information - Gauge Name, Group Threshold, Timespan in minutes, Gauge Method (see Specify Gauge Information).
   - Gauge Components (see Define Gauge Components).
   - User Membership (see Assign user groups).
5. Click **Save** to save your edits and return to the Add/Edit Gauges panel.

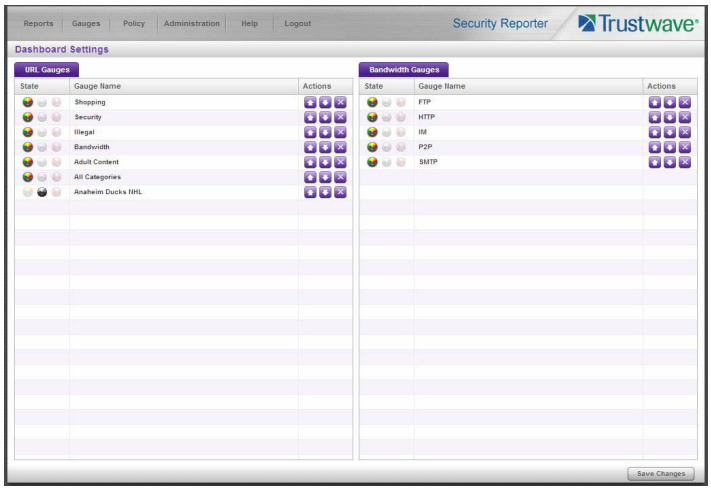
5.3.3 Hide, Disable, Delete, Rearrange Gauges

If you want to view certain gauges in the dashboard, options are available to hide, disable, or delete a specified gauge. You can also manipulate the order in which gauges display in the dashboard.

Tip: In addition to the instructions provided in this sub-section, gauges can be hidden, disabled, and deleted from the gauges dashboard by right-clicking the gauge to display its menu, and then choosing the appropriate topic. See Gauge Usage Shortcuts.

Note: If a global administrator hides or disables a gauge, this will not affect the dashboard view for a group administrator who has been assigned to monitor this gauge.

1. In the navigation toolbar, hover over the Gauges menu link and select **Dashboard Settings** to display the Dashboard Settings panel:



This panel shows the URL Gauges tab to the left and the Bandwidth Gauges tab to the right. In each of these tabs, a list of gauges displays with the following information:

- State - A gauge icon displays in one of three columns to indicate the current status of the gauge, with the other two columns greyed-out:

  (visible) - This icon in the first column indicates the gauge displays in the dashboard.

  (hidden) - This icon in the second column indicates the gauge does not display in the dashboard.

  (disabled) - This icon in the third column indicates the gauge does not display in the dashboard. This gauge most likely has not been deleted because it will be used on a later occasion.

Note: Statistics for gauges that are hidden or disabled will not be included in trend reports.

- Gauge Name - The name given to the gauge.
- Actions - Icons display for performing any one of the following actions on the gauge as necessary: Move the gauge up or down in the current list in order to change the position in which that gauge displays the dashboard, or delete the gauge.

2. After making all necessary Dashboard Settings modifications—hide, disable, show, rearrange, or delete a gauge—defined in the following sub-sections, click **Save Changes** to save your edits.

5.3.3.1 Hide a gauge

To hide a gauge from displaying in the dashboard:

1. Select the gauge in the URL Gauges or Bandwidth Gauges tab.
2. In the State column, click the icon in the second column (Hide Gauge) to change the gauge's status to "hidden."

5.3.3.2 Disable a gauge

To disable a gauge:

1. Select the gauge in the URL Gauges or Bandwidth Gauges tab.

2. In the State column, click the icon in the third column (Disable Gauge) to change the gauge's status to "disabled."

5.3.3.3 Show a gauge

To re-display a gauge in the dashboard again:

1. Select the gauge in the URL Gauges or Bandwidth Gauges tab.
2. In the State column, click the icon in the first column (Show Gauge) to change the gauge's status to "show."

5.3.3.4 Rearrange the gauge display in the dashboard

To rearrange the order in which gauges display in the dashboard:

1. Select the gauge in the URL Gauges or Bandwidth Gauges tab.
2. In the Actions column, perform any of the following actions:
   - Click the "up" arrow icon in the first column to move the Gauge Name up one row in this tab, and one position forward in the dashboard.
   - Click the "down" arrow icon in the second column to move the Gauge Name down one row in this tab, and one position backward in the dashboard.

Tip: These actions can be performed multiple times in order to move the gauge to the desired position in the dashboard.

5.3.3.5 Delete a gauge

To delete a gauge:

1. Select the gauge in the URL Gauges or Bandwidth Gauges tab.
2. In the Actions column, click the "X" icon in the far right column to open the Confirm dialogue box with a message informing you that deleting the gauge will remove all alerts associated with the gauge, and asking if you wish to proceed.

Note: Deleting a gauge also deletes any associated alerts set up for that gauge.

Tip: Clicking Cancel closes the dialog box without removing the gauge.

3. Click **Yes** to close the dialog box and to remove both the Gauge Name from the tab and the gauge from the dashboard.

5.3.4 View End User Gauge Activity

There are two types of gauge activity you will want to view and monitor:

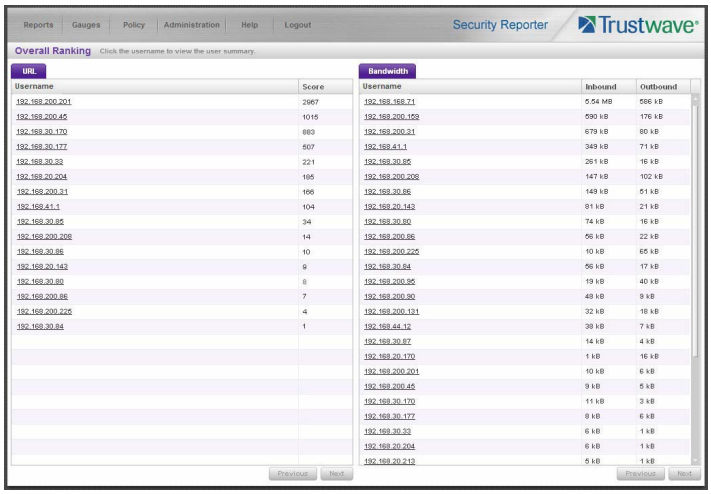
- Overall Ranking - Use this option for a snapshot of end user activity for all gauges, ranked in order by the highest to lowest end user score.

- Gauge Ranking - Use this option for a snapshot of a specific gauge's end user activity, ranked in order by the highest to lowest end user score.

Either option lets you drill down and view information on a specific end user's activity, and lets you lock out the end user, if necessary.

5.3.4.1 View Overall Ranking

1. In the navigation toolbar, hover over the Gauges menu link and select **Overall Ranking** to open the Overall Ranking panel:



   The URL sub-panel displays to the left and the Bandwidth sub-panel displays to the right, containing the User Name (or IP address) and Score for each user currently affecting one or more gauges.

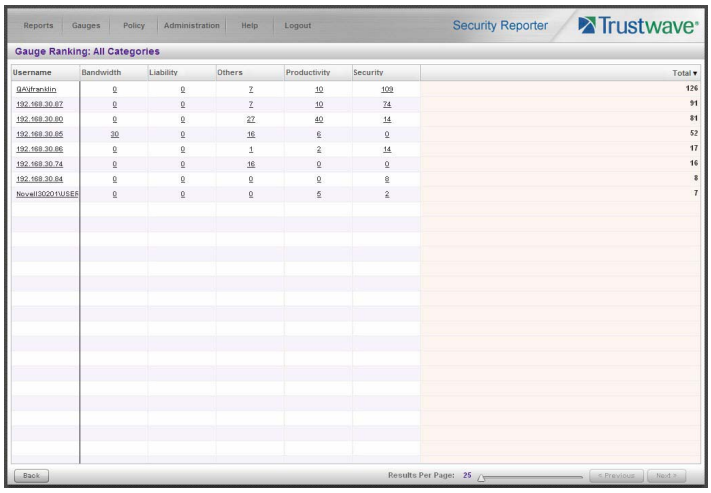
   In the URL tab, this Score includes the number of hits the user made in library categories. In the Bandwidth tab, this score includes the end user's byte total for Inbound/Outbound protocols/ports.

2. To drill down and view additional information about an end user's activity, click the **Username** in the appropriate tab to access the User Summary panel (see Monitor, Restrict End User Activity).

3. In the User Summary panel, you can view URLs visited by the end user and lock out that user from accessing designated areas of the Internet/network.

5.3.4.2 View a Gauge Ranking table

1. In the gauges dashboard, click a gauge to open the Gauge Ranking panel:



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

This panel includes rows of records for each end user who is affecting the gauge. For each record in the list, the following information displays: Username (or IP address), gauge name and end user score, and the end user's Total score for all gauges he/she affected. End users are ranked in descending order by their Total score.

2. Perform one of two drill-down actions from here:

   - Access the User Summary panel by clicking the **Username** (see Monitor, Restrict End User Activity: View User Summary data). In the User Summary panel, you can view URLs visited by the end user and lock out that user from accessing designated areas of the Internet/network.
   - Access the Category View User panel by clicking a user's score for a gauge (see Monitor, Restrict End User Activity: Access the Category View User panel). In the Category View User panel, you view current details for the gauge.

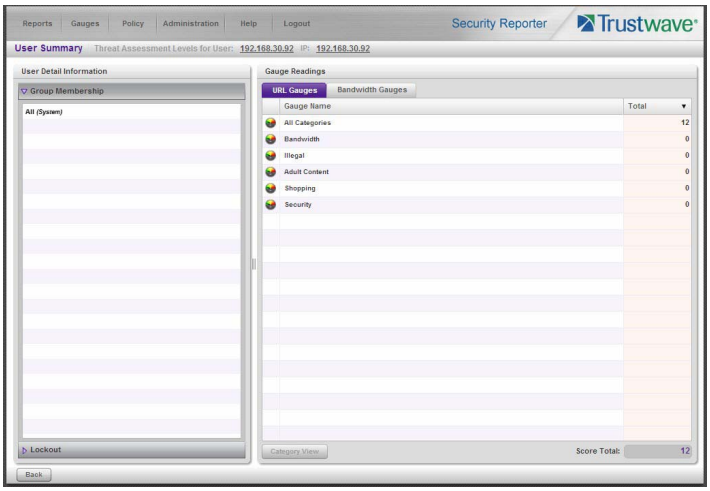
5.3.5 Monitor, Restrict End User Activity

5.3.5.1 View User Summary data

The User Summary panel contains the following sub-panels:

- User Detail Information sub-panel to the left that includes the Group Membership and Lockout accordions. The Group Membership accordion is expanded by default and displays a list of groups in which the end user belongs.

- Gauge Readings sub-panel to the right that includes the URL Gauges and Bandwidth Gauges tabs, each showing the Gauge Name and end user's Total score for each gauge in the dashboard.



In this panel you can perform the following actions:

- Access the Category View User panel to see which of the gauge's library categories/ports the end user accessed and the score (see Access the Category View User panel).
- Access the Lockout option to lock out the end user from specified Internet/network privileges (see Manually lock out an end user).

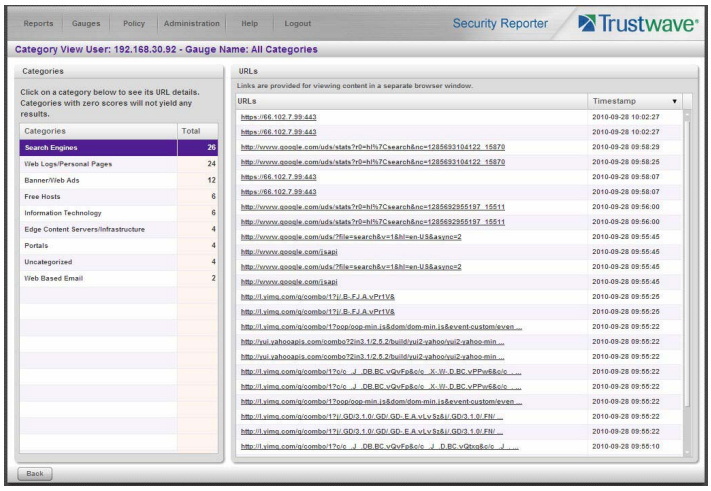
5.3.5.2 Access the Category View User panel

1. In the User Summary panel, make sure the appropriate tab (URL Gauges or Bandwidth Gauges) is selected, then click a Gauge Name with a score to activate the Category View button.
2. Click **Category View** to display the Category View User panel which includes criteria that is based on the type of gauges to be viewed (URL or bandwidth).

5.3.5.2.1 URL Gauges tab selection

For URL gauges, the Category View User panel displays the Categories sub-panel to the left, showing a list of current library categories that were accessed and the Total score of each category for that end user. The target URLs sub-panel displays to the right.

1. Select a category from the list, which populates the URLs sub-panel with URLs accessed by that end user for that category:

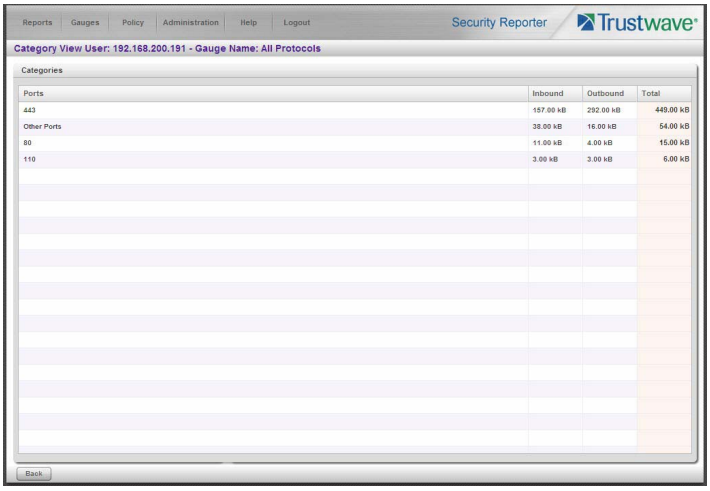


For each URL included in the list, the Timestamp displays using military time in the YYYY-MM-DD HH:MM:SS format.

2. Click a URL from the list to open a separate browser window or tab displaying the contents of that URL.

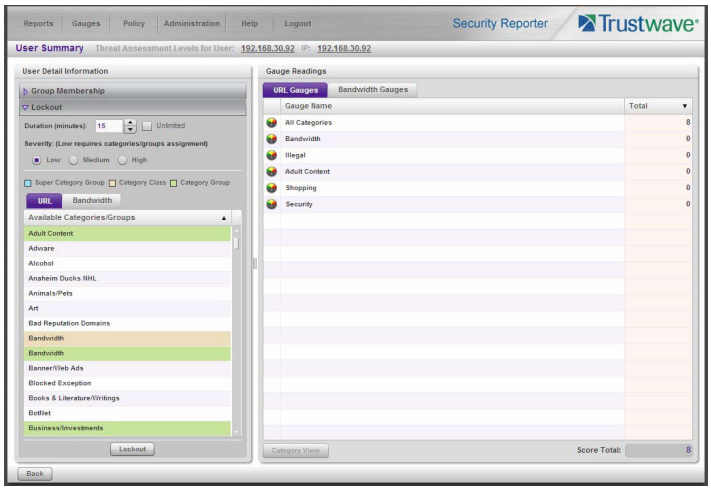
5.3.6 Bandwidth Gauges tab selection

For Bandwidth gauges, the Category View User panel contains the Categories sub-panel showing the Ports column and corresponding Inbound/Outbound bandwidth usage by the end user for that port, and the combined Total inbound and outbound bandwidth usage by the end user for that port:



5.3.6.1 Manually lock out an end user

1. In the User Summary panel, in the User Detail Information sub-panel, click the Lockout accordion to open it:



2. Specify the **Duration** (minutes) of the lockout (the default is "15" minutes), or click the "Unlimited" check box.

Note: If "Unlimited" is selected, the end user remains locked out of the specified areas on the Internet/network until the administrator unlocks his/her workstation. To "unlock" the end user, go to the Gauges | Lockouts panel. For information on this feature, see Alerts, Lockout Management.

3. Specify the **Severity** of the lockout from the radio button choices:

   - **Low** - This selection lets you choose which library categories/ports the end user will not be able to access (see Low severity lockout).
   - **Medium** - This selection locks out the end user from access to the World Wide Web (see Medium and High severity lockout).
   - **High** - This selection locks out the end user from all network access via a TCP connection (see Medium and High severity lockout).

4. After performing the additional steps based on the chosen lockout Severity level, click **Lockout** at the bottom of the sub-panel to open the Info alert box with a message informing you that the user has been locked out.

5. Click **OK** to close the alert box and to lock out the user from the designated library categories/ports for the specified duration of time.

5.3.6.1.1 Low severity lockout

If a "Low" Severity lockout was selected, the Available Categories/Groups box displays. Do the following:

- If using the URL tab, choose the library category/categories from the list. Up to 15 categories or one category group/class can be added.
- If using the Bandwidth tab, make a selection from the protocols in the list.

  You can also enter a port number in the **Port Number** field, or modify the value in that field by clicking the up/down arrows to increment/decrement the current value by one, and then click **Add Port** to

include the port number in the Assigned Categories/Groups sub-panel. Up to 15 port numbers can be added.

Note: In the Available Categories/Groups box, a global administrator will not see the "All Categories" selection for URL gauges, nor see the "All Protocols" selection available for bandwidth gauges. In order to lock out end users using either of these selections, a "Medium" severity lockout should be used.

5.3.6.1.2 Medium and High severity lockout

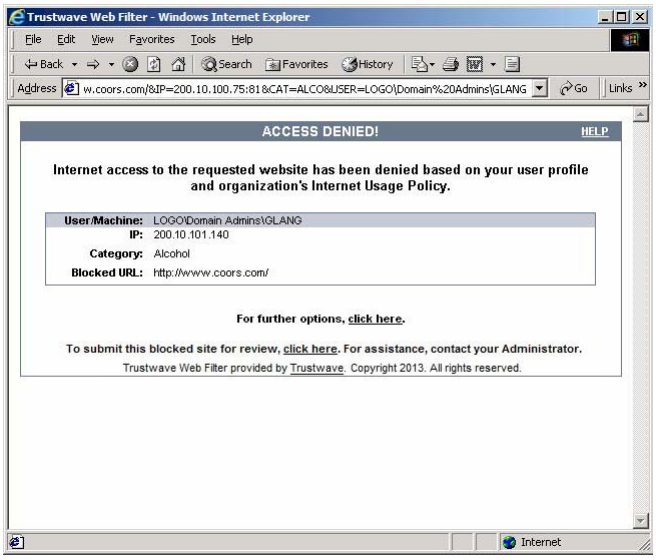
If a "Medium" or "High" Severity lockout was selected, the **Type** field displays. Click either "Medium" or "High" to select that lockout level.

5.3.6.1.3 End user workstation lockout

There are two different scenarios that can occur for end users when they are locked out, based on the severity of the lockout (low, medium, or high), and the gauge type (URL or bandwidth).

Low severity URL, medium URL/bandwidth lockout

In a low or medium severity URL lockout, or a medium severity bandwidth type lockout, when an end user attains the User Threshold established for a gauge, and that end user attempts to access a category/port or category group set up to be monitored by that gauge, the following lockout page displays for the end user.



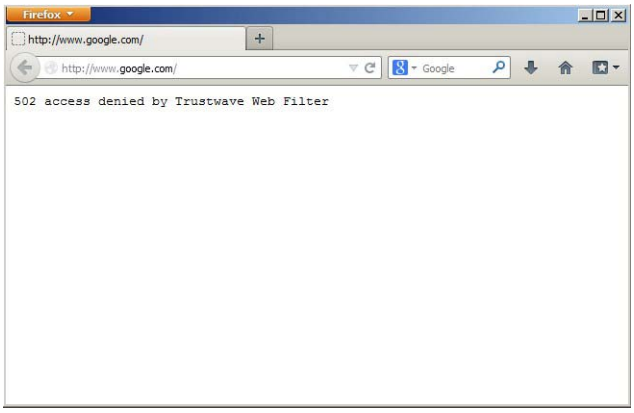
This page contains the following information: header "ACCESS DENIED!", User/Machine name for an LDAP user (blank for an IP group user), user's IP address, library Category in which the URL resides, and the Blocked URL the user attempted to access.

By default, the following standard links are included in the block page: HELP; Trustwave; For further options, click here; To submit this blocked site for review, click here.

Note: Please refer to the Global Administrator Section of the Trustwave Web Filter User Guide or Trustwave IR Web Filter User Guide for information about fields in the block page and how to use them.

High severity URL, low/high bandwidth lockout

In a high severity URL lockout, or a low or high severity bandwidth type lockout, when an end user attains the User Threshold established for a gauge, and that end user attempts to access a URL for a threat category/port or category group set up to be monitored by that gauge, the following lockout page displays for the end user:



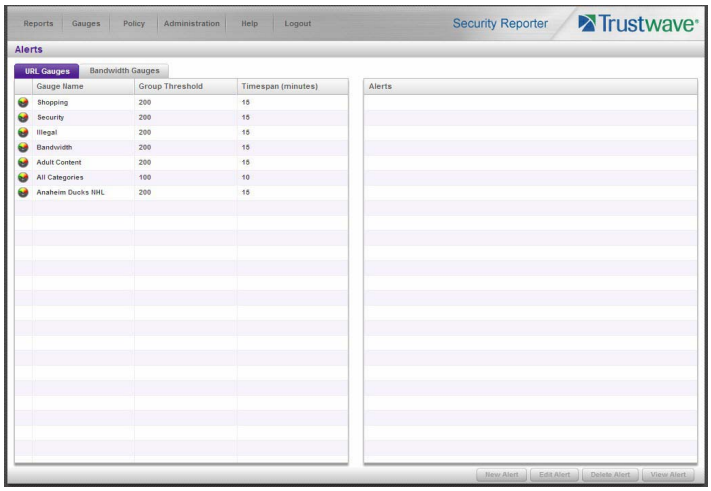
This page contains the following information: "502 Access Denied by Trustwave Web Filter".

5.4 Alerts, Lockout Management

After setting up gauges for monitoring end user Internet activity, notifications for Internet abuse should be set up in the form of policy alerts. These messages inform the administrator when an end user has triggered an alert for having reached the threshold limit established for a gauge. If the end user was locked out of Internet/network for an indefinite time period as a result of his/her Internet activity, the administrator can determine when to unlock that end user's workstation.

These functions are available to global administrators only.

1. In the navigation toolbar, hover over the Policy menu link and select **Alerts** to open the Alerts panel:



   This panel includes a sub-panel to the left that contains the URL Gauges and Bandwidth Gauges tabs, and the empty, target Alerts sub-panel to the right.

2. Do the following to view the contents in the tab to be used:

   - Click **URL Gauges** if this tab currently does not display. By default, this tab includes the following list of Gauge Names: Shopping, Security, Illegal, Bandwidth, Adult Content.

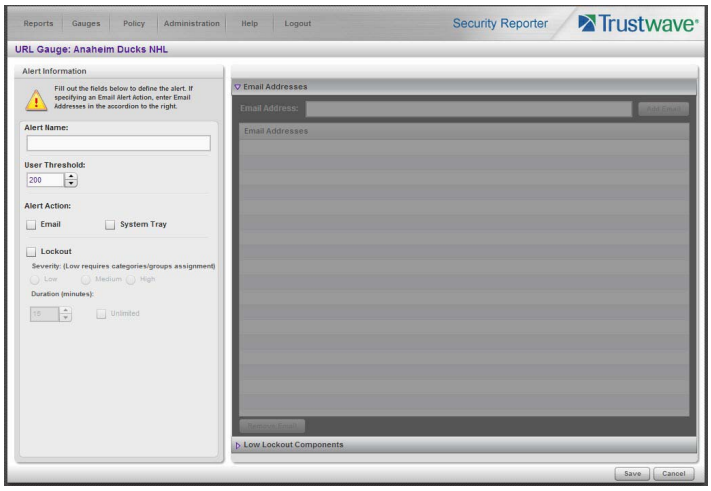
     For each Gauge Name in this list, the following information displays: Group Threshold (200), Timespan (minutes)—15 by default.

   - Click **Bandwidth Gauges** to view the contents of this tab. By default, this tab includes the following list of Gauge Names: FTP, HTTP, IM, P2P, SMTP.

     For each Gauge Name in this list, the following information displays: Group Threshold (20 MB—64 MB for "HTTP"), Timespan (minutes)—15 by default.

5.4.1 Add an Alert

1. From the left sub-panel, select the gauge for which an alert will be created; this action activates the New Alert button.
2. Click **New Alert** to open the panel for that gauge:



   In this panel, the Alert Information sub-panel displays to the left and the greyed-out target panel displays to the right containing the Email Addresses and Low Lockout Components accordions.

3. In the Alert Information sub-panel, type in the **Alert Name** to be used for the alert that will be delivered to the group administrator.
4. Specify the **User Threshold** ceiling of gauge activity that will trigger the alert.

Note: An alert is triggered for any end user whose current score for a gauge matches the designated threshold limit. (See How to Read a Gauge for information on how scoring is defined.)

5. In the Alert Action section, specify the mode(s) to use when an alert is triggered:

   - **Email** - An email alert notifies a group administrator via email if an end user has reached the threshold limit set up in a gauge alert.

- **System Tray** - An SR Alert message notifies a group administrator via his/her workstation's System Tray if an end user has reached the threshold limit set up in a gauge alert.
- **Lockout** - The Lockout function locks out an end user from Internet/network access if he/she reaches the threshold limit set up in a gauge alert.

Note: The System Tray alert feature is only available for an administrator with an Active Directory LDAP account, user name, and domain, and is not available if using IP groups.

6. After making all entries in this panel, click **Save** to save your entries and to activate your alert.

5.4.1.1 Email alert function

5.4.1.1.1 Configure email alerts

To set up the email alert function:

1. In the Alert Action section of the Alert Information sub-panel, click the check box corresponding to **Email** to open the Email Addresses accordion in the target sub-panel to the right.
2. Type in the **Email Address**.
3. Click **Add Email** to include the address in the Email Addresses list box.

   Follow steps 2 and 3 for each email address to be sent an alert.

Tip: To remove an email address from the list box, select the email address and then click Remove Email. Click Submit to save your settings.

5.4.1.1.2 Receive email alerts

If an alert is triggered, an email message is sent to the mailbox address(es) specified. This message includes the following information:

- Subject: Alert triggered by user (username/IP address).
- Body of message: User (username/IP address) has triggered the (Alert Name) alert with a threshold of 'X' (in which "X" represents the alert threshold) on the (gauge name) gauge.

  Beneath this information, the date and time (YYYY-MM-DD HH:MM:SS), and clickable URL display for each URL accessed by the user that triggered this alert.

5.4.1.2 System Tray alert function

If using LDAP with an Active Directory user name, account, and domain, to set up the feature for System Tray alerts, click the check box corresponding to **System Tray** and follow the instructions in Appendix D: System Tray Alerts: Setup, Usage.

Note: In order to use this feature, the LDAP User Name and Domain set up in the administrator's profile account must be the same ones he/she uses when logging into his/her workstation.

5.4.1.3 Lockout function

To set up the lockout function:

1. Click the check box corresponding to **Lockout** to activate the Severity and Duration (minutes) fields.

2. Specify the **Severity** of the end users' lockout:

   - **Low** - Choosing this option opens the Low Lockout Components accordion containing the Available Categories/Groups and Assigned Categories/Groups sub-panels.

     Select the library category/categories or protocol(s) the end user should not access.

     For bandwidth gauges, to specify a port number the user should not access, type a specific value in the **Port Number** field, and/or use the up/down arrow buttons to increment/decrement the current value by one.

     Click **Add** (for URL gauges) or **Add Port** (for bandwidth gauges) to move the selection(s) to the Assigned Categories/Groups list box.

Tip: To remove one or more library categories/ports from the Assigned Categories/Groups list box, make your selection(s), and then click <remove to move the selection(s) back to the Available Categories/Groups list.

   - **Medium** - Choosing this option will lock out an end user from World Wide Web access if he/she reaches the threshold limit set up for the gauge.
   - **High** - Choosing this option will lock out an end user from network access via a TCP connection if he/she reaches the threshold limit set up for the gauge.

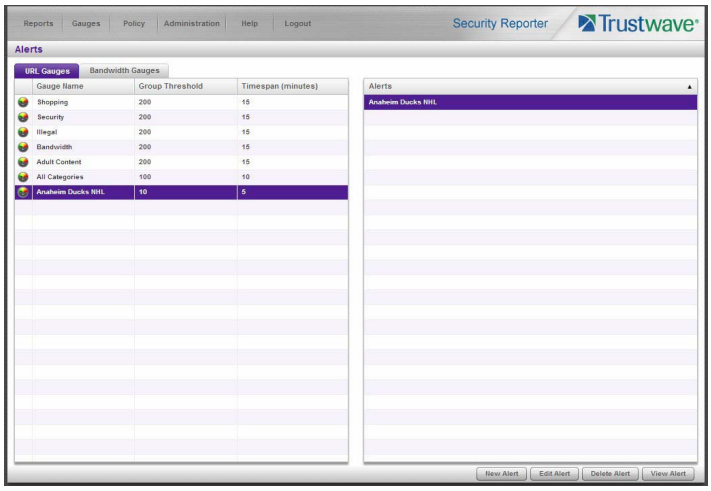
3. Specify the **Duration** (minutes) of the lockout (the default is "15" minutes), or click the "Unlimited" check box.

Note: If "Unlimited" is specified, the end user will remain locked out from Internet/network access until the group administrator unlocks his/her workstation using the Gauges | Lockouts panel.

Tip: After making your selections, click **Save** to save your settings.

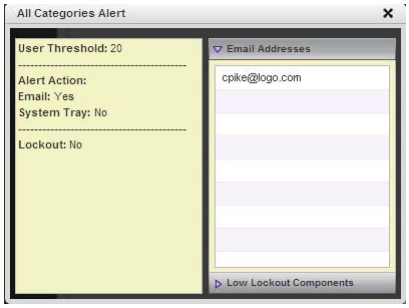
5.4.2 View, Modify, Delete an Alert

1. In the Alerts panel, select the URL Gauges or Bandwidth Gauges tab.
2. Select the gauge for which an alert will be viewed and/or modified. This action populates the Alerts sub-panel list box with any existing alerts created for that gauge.
3. Select the alert to be viewed or modified by clicking on it to highlight it; this action activates all buttons below the Alerts sub-panel (Add Alert, Edit Alert, Delete Alert, View Alert):



5.4.2.1 View alert settings

1. Beneath the Alerts sub-panel, click **View Alert** to open the alert viewer window:



The following information displays to the left of this window:

- User Threshold amount
- Alert Action criteria (Yes/No): Email, System Tray
- Lockout (Yes/No)

If a Lockout was set up for the alert, the following information displays below "Lockout":

- Severity (Low, Medium, High)
- Duration (minutes)

To the right of this window, the Email Addresses and Low Lockout Components accordions display. Click an accordion to expand it, and view the contents—if any—within that accordion.

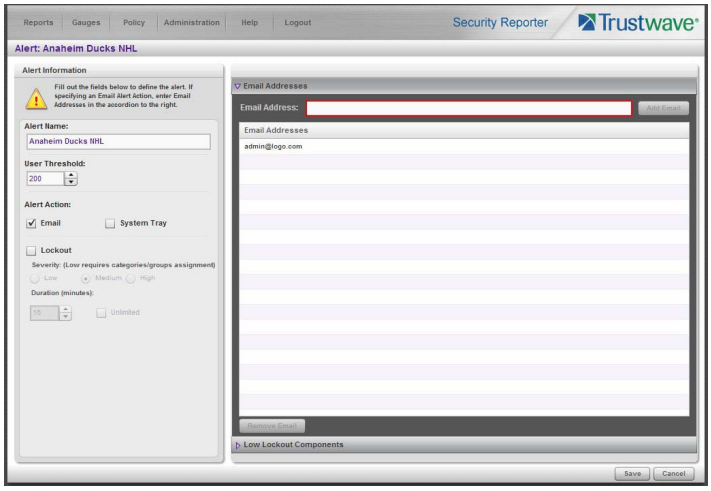
Note: The System Tray alert feature is only available if using Active Directory LDAP, and is not available if using IP groups.

2. Click the "X" in the upper right corner of the alert viewer window to close it.

5.4.2.2 Modify an alert

1. In the Alerts panel, click the URL Gauges or Bandwidth Gauges tab.

2. Select the gauge from the list to populate the Alerts sub-panel with alerts for that gauge, and to activate all buttons beneath the sub-panel.
3. Click **Edit Alert** to open the edit Alert panel:



4. The following items can be edited:
   - Alert Name
   - User Threshold
   - Alert Action selections: Email, System Tray—the latter is only functional for Active Directory LDAP—and Lockout
   - Lockout Severity selection (Low, Medium, High)
   - Duration (minutes) selection
   - Email Addresses
   - Low Lockout Components
5. Click **Save** to save your edits, and to return to the main Alerts panel.

5.4.2.3 Delete an alert

1. In the Alerts panel, click the URL Gauges or Bandwidth Gauges tab.
2. Select the gauge from the list to populate the Alerts sub-panel with alerts for that gauge, and to activate all buttons beneath the sub-panel.
3. Click **Delete Alert** to open the Confirm dialog box with a message asking if you want to delete the alert.

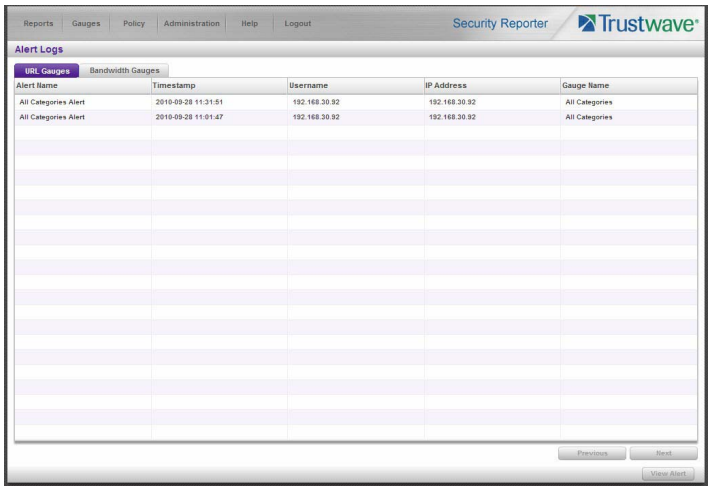
Note: Clicking No closes the dialog box without removing the alert, and returns you to the main Alerts panel.

4. Click **Yes** to close the Confirm dialog box and to remove the alert from the list.

5.4.3 View the Alert Log

After alerts are sent to an administrator, a list of alert activity is available for viewing in the Alert Logs panel.

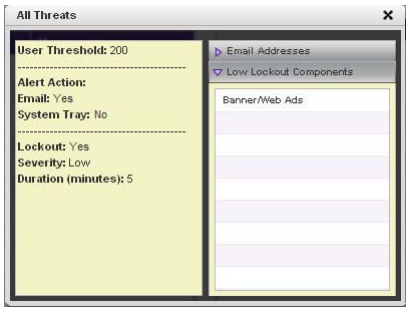
1. In the navigation toolbar, hover over the Policy menu link and select **Alert Logs** to open the Alert Logs panel.
2. Select the URL Gauges or Bandwidth Gauges tab to display its contents:



The alert log contains a list of alert records for the most recent 24-hour time period. Each record displays in a separate row. For each row in the list, the following information displays: Alert Name, Timestamp (using the YYYY-MM-DD HH:MM:SS military time format), Username (or IP address), IP Address, Gauge Name.

Note: If an alert was deleted during the most recent 24-hour time period, any records associated with that alert will be removed from the alert log.

3. To view details on an alert, select the alert record in the list to highlight it.
4. Click **View Alert** to open the alert viewer window:



The following information displays to the left of this window:

- User Threshold amount
- Alert Action criteria (Yes/No): Email, System Tray
- Lockout (Yes/No)

If a Lockout was set up for the alert, the following information displays below "Lockout":

- Severity (Low, Medium, High)
- Duration (minutes)

To the right of this window, the Email Addresses and Low Lockout Components accordions display. Click an accordion to expand it, and view the contents—if any—within that accordion.

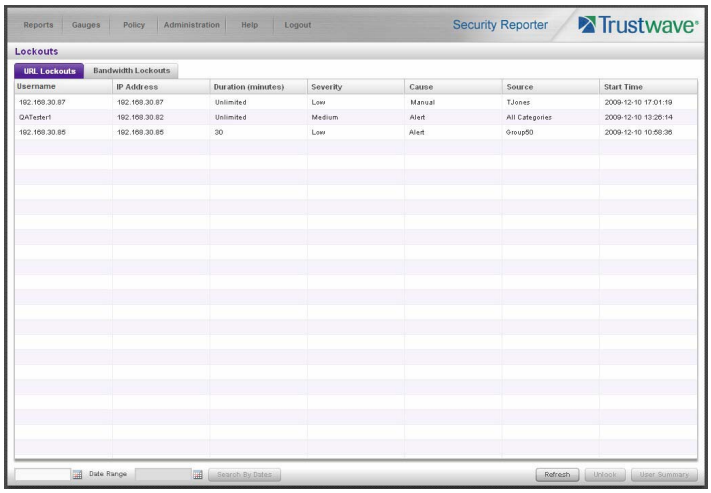
5. Click the "X" in the upper right corner of alert viewer window to close it.

5.4.4 Manage the Lockout List

An end user who is manually or automatically locked out for an "Unlimited" period of time—from accessing designated content on the Internet or using the network—can only have his/her workstation unlocked by an administrator.

To view the current lockout list:

1. In the navigation toolbar, hover over the Gauges menu link and select **Lockouts** to open the Lockouts panel.
2. Select the URL Gauges or Bandwidth Gauges tab to display its contents:

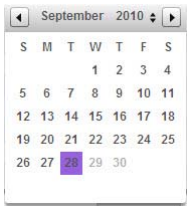


The lockout list contains records for all end users currently locked out of the Internet/network. Each end user's record displays in a separate row. For each row in the list, the following information displays: Username (or IP address); IP address; Duration (minutes); Severity of the lockout (Low, Medium, High); Cause of the lockout (Manual, Automatic); Source of the lockout (username of the administrator who locked out the end user in a Manual lockout, or name of the alert in an Automatic lockout); Start Time for the alert (using the YYYY-MM-DD HH:MM:SS format).

5.4.4.1 View a specified time period of lockouts

If the lockout list is populated with many records, using the Date Range feature will only show you records within the range of dates you specify.

1. At the **Date Range** field, click the calendar icon located to the right of the first date field; this action opens the larger calendar for the current month, with today's date highlighted:



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

2. Click the starting date to select it and to close the calendar pop-up window. This action populates the field with the selected date.
3. At the **Date Range** field, click the calendar icon located to the right of the second date field; this action opens the larger calendar for the current month, with today's date highlighted.
4. Click the ending date to select it and to close the calendar pop-up window. This action populates the field with the selected date.
5. Click **Search By Dates** to display records for only the selected dates.

Tip: Click Refresh to clear all records returned by the search query, and to display the default records (all lockout records) in the panel.

5.4.4.2 Unlock workstations

1. In the populated Lockouts panel, click each record to highlight it.
2. Click **Unlock** to unlock the end user(s) and to remove the record(s) from the list.

Note: By unlocking an end user's workstation, all records in this list pertaining to that end user are removed from the list.

5.4.4.3 Access User Summary details

1. To access details about an end user's online activity, first click the user's record to highlight it.
2. Next, click **User Summary** to display the User Summary panel where you can monitor that end user's online activity and lock him/her out of designated areas of the Internet/network. (See Monitor, Restrict End User Activity for details about using the User Summary panel.)

5.5 Analyze Usage Trends

When analyzing end user Internet usage trends, trend charts help you configure gauges and alerts so you can focus on current traffic areas most affecting the network.

If more information is required in your analysis, the Web Filter application, Report Manager tools, and System Configuration administrator console should be consulted so you can generate customized reports to run for a time period of your specifications.

5.5.1 View Trend Charts

There are three basic types of trend charts that can be generated on demand to show total gauge score averages for a specified, limited time period:

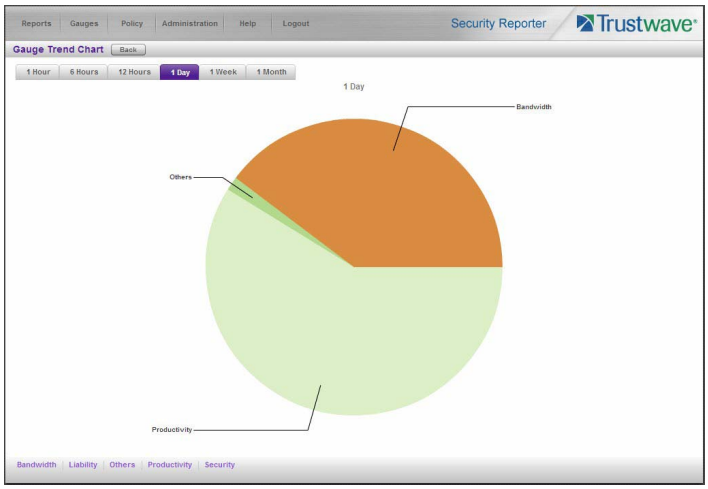
- Pie trend chart for an individual URL or bandwidth gauge
- Pie trend chart for all collective URL or bandwidth gauges
- Line chart showing details for a pie chart

5.5.1.1 View activity for an individual gauge

To view activity for any individual URL or bandwidth gauge:

1. If the gauges dashboard does not currently display, choose **Dashboard** from the Gauges menu in the navigation toolbar.
2. Be sure the dashboard of your choice (URL or Bandwidth gauges) displays. If not, click the URL or Bandwidth button above the dashboard to display the dashboard of your choice.
3. Find the gauge for which the trend chart will be generated, and then click the Trend Charts icon at the bottom middle of that gauge:

This action of clicking the Trend Charts icon displays the Gauge Trend Chart panel:



The pie trend chart that displays in the middle of this panel includes the following information:

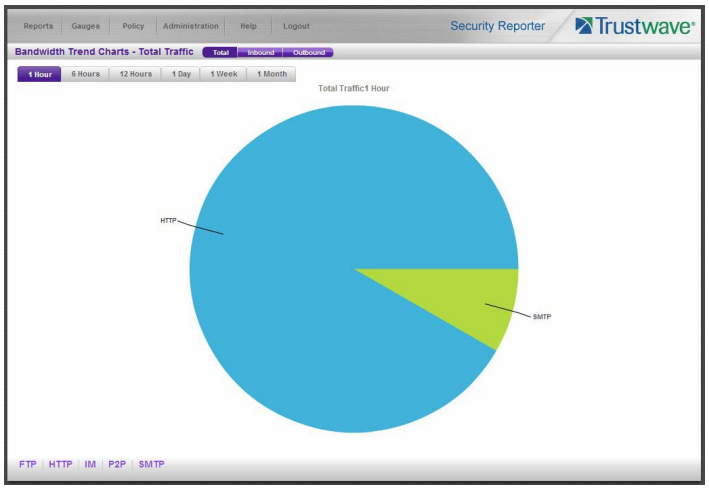
- For a URL gauge - By default, each slice of the pie represents the percentage of end user hits in a library category during the last hour; the total for all categories in that gauge equaling 100 percent.
- For a Bandwidth gauge - By default, each slice of the pie represents the percentage of end user traffic for a port during the last hour; the total for all ports in that gauge equaling 100 percent.

The top and bottom sections of this panel contain tabs.

Information about all actions that can be performed in this panel appears in the Navigate a trend chart sub-section.

5.5.1.2 View overall URL or bandwidth gauge activity

1. In the navigation toolbar, hover over the Reports menu link and select either the **URL Trend Charts** to display the URL Trend Charts panel, or select **Bandwidth Trend Charts** to display the Bandwidth Trend Charts panel:



The pie trend chart that displays in the middle of this panel includes the following information:

- For URL gauges - By default, each slice of the pie represents that URL gauge's percentage of end user scores during the last hour; the total for all URL gauges in the dashboard equaling 100 percent.
- For Bandwidth gauges - By default, each slice of the pie represents that bandwidth gauge's percentage of end user traffic during the last hour; the total for all bandwidth gauges in the dashboard equaling 100 percent.

The top and bottom sections of this panel contains tabs. For the bandwidth trend chart, buttons display above this panel.

Information about all actions that can be performed in this panel appears in the Navigate a trend chart sub-section.

5.5.1.3 Navigate a trend chart

The following actions can be performed in this panel:

- View gauge activity for a different time period (1 Hour, 6 Hours, 12 Hours, 1 Day, 1 Week, 1 Month)

- Analyze gauge activity in a pie chart
- Analyze gauge activity in a line chart
- View Inbound, Outbound bandwidth gauge activity
- Print a trend chart from an IE browser window

5.5.1.3.1 View gauge activity for a different time period

To view a pie chart showing activity for a different time period of gauge activity, click the appropriate tab above the pie chart diagram:

- **1 Hour** - This selection displays the gauge URL/byte average score in 10 minute increments for the past 60-minute time period
- **6 Hours** - This selection displays the gauge URL/byte average score in 30 minute increments for the past six-hour time period
- **12 Hours** - This selection displays the gauge URL/byte average score in one hour increments for the past 12-hour time period
- **1 Day** - This selection displays the gauge URL/byte average score in one hour increments for the past 24-hour time period
- **1 Week** - This selection displays the gauge URL/byte average score in 12 hour increments for the past seven-day time period
- **1 Month** - This selection displays the gauge URL/byte average score in one-day increments for the past month's time period

Once you've selected the time period you wish to view, you can analyze the activity for that gauge (see Analyze gauge activity in a pie chart), and drill down into a slice of the pie to view a line chart for that given time period (see Analyze gauge activity in a line chart).

5.5.1.3.2 Analyze gauge activity in a pie chart

Once a pie chart displays in the panel, its pieces can be analyzed by hovering over that slice of the pie chart.

The following information displays for that pie slice: gauge component name, percentage of that pie slice (based on a total of 100 percent for all pie slices), and total end user score for that pie slice.

That slice of the pie can be further analyzed by drilling down into it (see Analyze gauge activity in a line chart).

5.5.1.3.3 Analyze gauge activity in a line chart

1. To view a line chart showing activity for a slice of the pie chart, do either of the following:
   - Click that slice of the pie chart
   - Click the specified tab beneath the pie chart

   Either action displays the line Trend Chart:

By default, this chart contains the following information: linear depiction of the total end user SCORE in fixed time increments (using the MM-DD-YYYY HH:MM:SS format) for MINUTES or HOURS included in the specified time period for the gauge component, and the check box populated for the selected library category/protocol/port.

Note: See View gauge activity for a different time period for a definition of MINUTES or HOURS included in the current chart.

2. Perform any of the following actions in this chart:

- To include other gauge component activity in this line chart, click the check boxes corresponding to the gauge names.

Tip: Click a populated check box to remove the check mark and the line showing activity for that gauge.

- To view information about a specific point in the line chart, hover over that point in the chart:

  If the chart includes more than one line, and more than one point is located in the area of the hover pointer, a separate box appears for each point in that section of the chart.

  Each box includes the following information: gauge component name, Score for that point, and Minutes or Hours for that fixed time increment (using the MM-DD-YYYY HH:MM:SS format).

- To return to the pie chart, click **Back to Pie** in the upper right portion of the panel.
- To print this trend chart, if using an IE browser, see Print a trend chart from an IE browser window.

5.5.1.3.4 View In/Outbound bandwidth gauge activity

By default, the total inbound and outbound bandwidth activity is included in the overall Bandwidth Trend Chart. To view only Inbound or Outbound activity, click the **Inbound** or **Outbound** button above the pie chart, to the right of the Total button.

5.5.1.3.5 Print a trend chart from an IE browser window

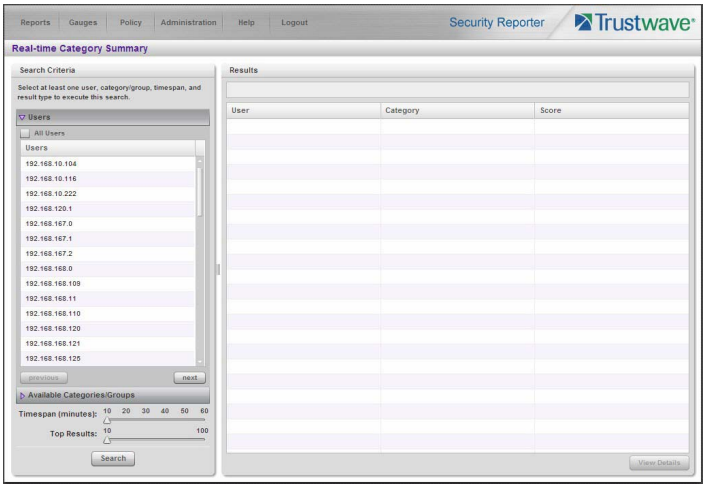
A trend chart can be printed from an IE browser window by using the browser window's toolbar and going to File | Print and proceeding with the print commands.

5.6 Identify Users, Categories

If there are certain end users who are generating excessive, unwanted traffic on the network, or if some library categories containing URLs against your organization's policies are persistently being frequented, you can target offending entities by performing a custom search to identify which users, URLs, and port are being accessed.

5.6.1 Perform a Custom Search

In the navigation toolbar, hover over the Reports menu link and select **Real-time Category Summary** to display the Real-time Category Summary panel:



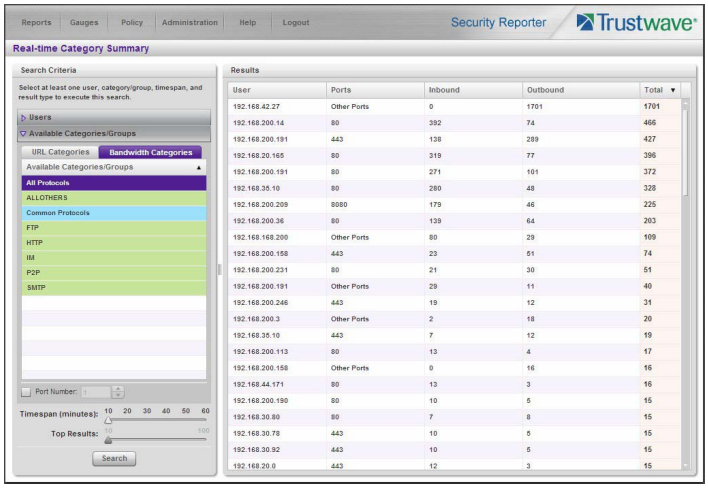
This panel displays the Search Criteria sub-panel to the left with the open Users accordion and closed Available Categories/Groups accordion, Timespan and Top Results sliders, Search button; and to the right, the empty Results target sub-panel.

5.6.1.1 Specify Search Criteria

1. In the **Users** accordion, do one of the following:
   - To identify users with the highest scores - Click the **All Users** check box to select all users in the list and to grey-out the list.
   - To identify the activities of a specific user - Select the user name/IP address from the list to highlight it.
2. Click the Available Categories/Groups accordion to open it.
3. Select either the **URL Categories** or **Bandwidth Categories** tab to display its list of library categories/protocols, and do either of the following:
   - To identify library categories or protocols with the highest scores - Select a category group or protocol that includes as many of categories/ports as possible.
   - To identify activities for a specific class/group - Select that class or group.

For bandwidth gauges, to query activities for a specific port number, click the **Port Number** check box to activate the port field and to deactivate the listed bandwidth protocol selections. Type a specific value in the pre-populated field, and/or use the up/down arrow buttons to increment/decrement the current value by one.

4. Use the **Timespan (Minutes)** slider to specify the time period in which the threat(s)/group(s) were accessed: last 10, 20, 30, 40, 50, 60 minutes.
5. If a user selection other than "All Users" was specified in the Users accordion, the **Top Results** slide becomes activated and you can make a selection for the maximum number of records to return in the results for that user: top 10, 20, 30, 40, 50, 60, 70, 80, 90, 100 records.
6. Click **Search** to display records returned by the query in the Results sub-panel at the right side of the panel:



For each record in the table, the following information displays:

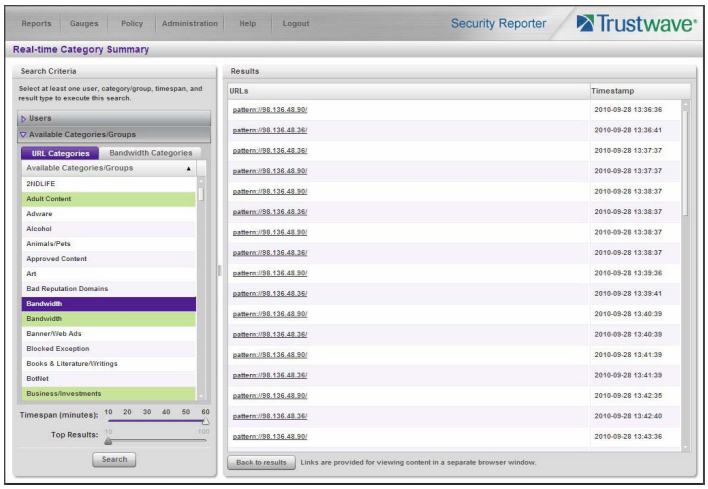
- For a URL search - User (user name/IP address), Category name, and the end user's total Score for that record.
- For a bandwidth search - User (user name/IP address), Ports number, Inbound score, Outbound score, and the end user's Total score for that record.

For a URL search, you can drill down even further by selecting a user's record and then viewing the URLs that user accessed (see View URLs within the accessed category).

5.6.1.1.1 View URLs within the accessed category

In the Results sub-panel, do the following to view a specific URL:

1. Click the User name/IP address to highlight that user's record and to activate the View Details button.
2. Click **View Details** to display a list of URLs and corresponding Timestamp (using the YYYY-MM-DD HH:MM:SS format) for each URL in the library category accessed by the end user within the specified time period:



Tip: Click Back to results to return to the previous page where you can perform another query.

You can now print the results displayed in this window if using an IE browser window, or access another selected URL.

Appendices

Appendix A: Disable Pop-up Blocking Software

An administrator with pop-up blocking software installed on his/her workstation will need to disable pop-up blocking in order to use the System Configuration console.

This appendix provides instructions on how to disable pop-up blocking software for the supported browser types (Internet Explorer, Firefox, Chrome, and Safari) and the following products: Yahoo! Toolbar, Google Toolbar, AdwareSafe, and Windows XP Service Pack 2 (SP2).

A.1 Browser Pop-up Blockers

A.1.1 Internet Explorer 8.0

In the Internet Explorer toolbar, navigate to Tools | Pop-up Blocker.

If you wish to disable all pop-up blocking, be sure the Turn Off Pop-up Blocker selection is enabled.

If you wish to block all pop-ups except those from URLs you choose to whitelist, enable Turn On Pop-up Blocker and then navigate to Pop-up Blocker Settings, adding the SR's URL in the Allowed sites list box.

A.1.2 Mozilla Firefox 6.0

1. In the Firefox toolbar, 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.1.3 Google Chrome 13.0

1. In the Chrome toolbar, navigate to the 'wrench' icon | Options | Under the Hood tab.
2. Click Content settings... | Pop-ups.
3. Choose either:
   - Allow all sites to show pop-ups

   or

   - Do not allow any site to show pop-ups (recommended) | Manage exceptions..., adding the SR's URL to the Pop-up Exceptions box.

A.1.4 Safari 5.1

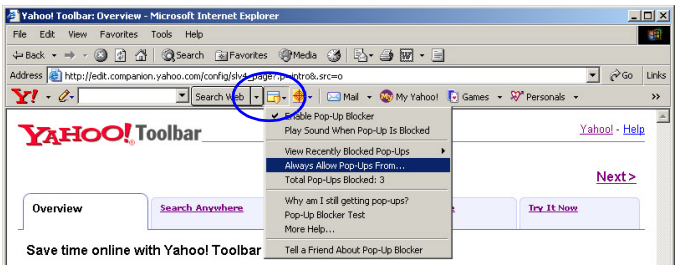
In the Safari toolbar, navigate to the Safari menu and de-select "Block Pop-Up Windows" to disable pop-up blocking.

A.2 Yahoo! Toolbar Pop-up Blocker

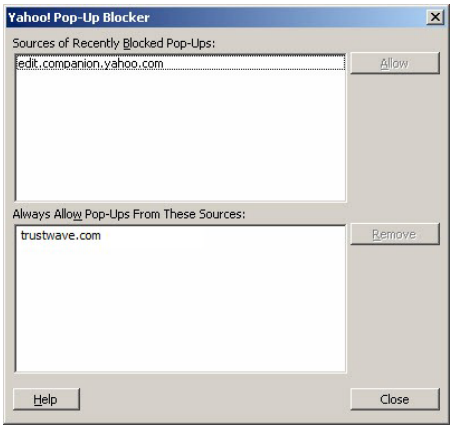
A.2.1 Add the Client to the White List

If the Client was previously blocked by the Yahoo! Toolbar, it can be moved from the black list and added to the white list so that it will always be allowed to pass. To do this:

1. Go to the Yahoo! Toolbar and click the pop-up icon to open the pop-up menu:



2. Choose Always Allow Pop-Ups From to open the Yahoo! Pop-Up Blocker dialog box:

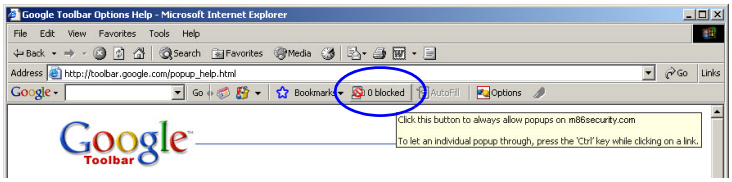


3. Select the source from the Sources of Recently Blocked Pop-Ups list box to activate the Allow button.
4. Click **Allow** to move the selected source to the Always Allow Pop-Ups From These Sources list box.
5. Click **Close** to save your changes and to close the dialog box.

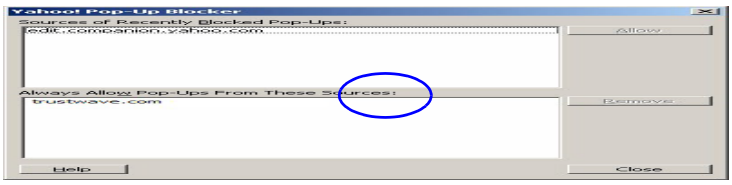
A.3 Google Toolbar Pop-up Blocker

A.3.1 Add the Client to the White List

To add the Client to the white list so that it will always be allowed to pass, go to the Google Toolbar and click the Pop-up blocker button:



Clicking this icon toggles to the Pop-ups okay button, adding the Client to your white list:



A.4 AdwareSafe Pop-up Blocker

A.4.1 Disable Pop-up Blocking

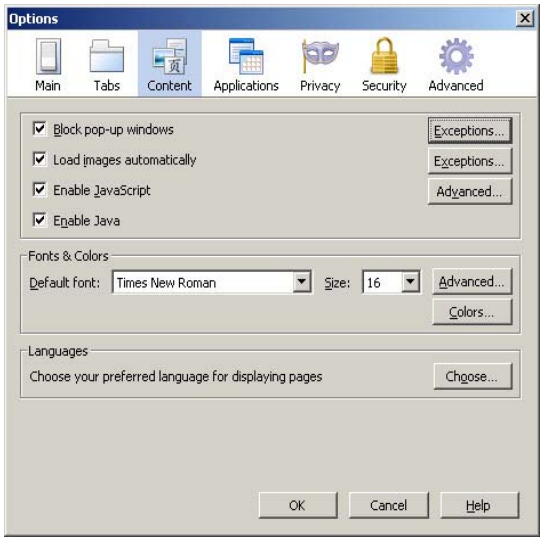
AdwareSafe's SearchSafe toolbar lets you toggle between enabling pop-up blocking (# popups blocked) and disabling pop-up blocking (Popup protection off) by clicking the pop-up icon.

1. In the IE browser, go to the SearchSafe toolbar and click the icon for # popups blocked to toggle to Popup protection off. This action turns off pop-up blocking.
2. After you are finished using the Client, go back to the SearchSafe toolbar and click the icon for Popup protection off to toggle back to # popups blocked. This action turns on pop-up blocking again.

A.5 Mozilla Firefox Pop-up Blocker

A.5.1 Add the Client to the White List

1. From the Firefox browser, go to the toolbar and select Tools | Options to open the Options dialog box.
2. Click the Content tab at the top of this box to open the Content section:



3. With the "Block pop-up windows" check box checked, click the **Exceptions...** button at right to open the Allowed Sites - Pop-ups box:

4. Enter the **Address of the web site** to let the client pass.
5. Click **Allow** to add the URL to the list box section below.
6. Click **Close** to close the Allowed Sites - Pop-ups box.
7. Click **OK** to close the Options dialog box.

A.6 Windows XP SP2 Pop-up Blocker

This sub-section provides information on setting up pop-up blocking and disabling pop-up blocking in Windows XP SP2.

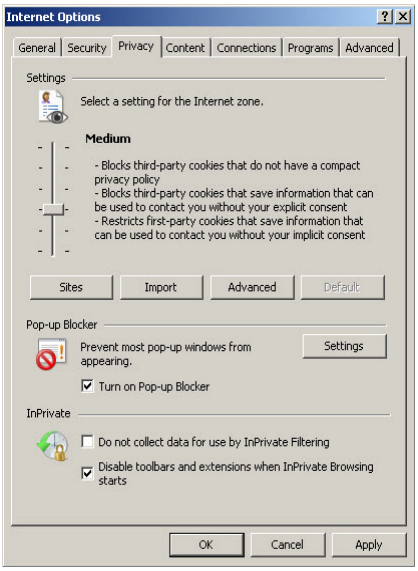
A.6.1 Set up Pop-up Blocking

There are two ways to enable the pop-up blocking feature in the IE browser.

A.6.1.1 Use the Internet Options dialog box

1. From the IE browser, go to the toolbar and select Tools | Internet Options to open the Internet Options dialog box.

2. Click the Privacy tab:

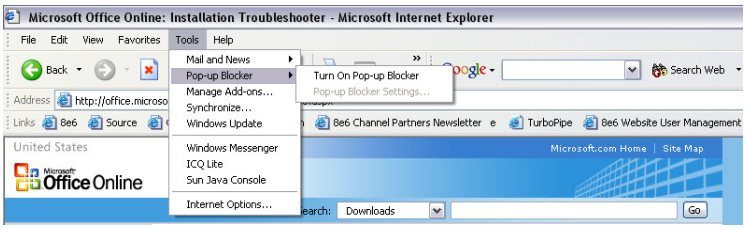


3. In the Pop-up Blocker frame, check “Turn on Pop-up Blocker”.

4. Click **Apply** and then click **OK** to close the dialog box.

A.6.1.2 Use the IE Toolbar

In the IE browser, go to the toolbar and select Tools | Pop-up Blocker | Turn On Pop-up Blocker:



When you click Turn On Pop-up Blocker, this menu selection changes to Turn Off Pop-up Blocker and activates the Pop-up Blocker Settings menu item.

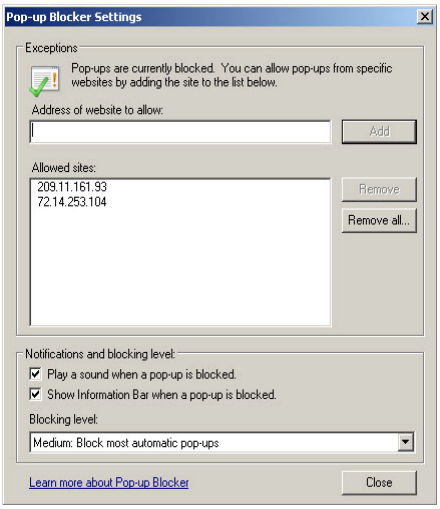
You can toggle between the On and Off settings to enable or disable pop-up blocking.

A.6.2 Add the Client to the White List

There are two ways to disable pop-up blocking for the Client and to add the Client to your white list.

A.6.2.1 Use the IE Toolbar

1. With pop-up blocking enabled, go to the toolbar and select Tools | Pop-up Blocker | Pop-up Blocker Settings to open the Pop-up Blocker Settings dialog box:



2. Enter the **Address of website to allow**, and click **Add** to include this address in the Allowed sites list box. Click **Close** to close the dialog box. The Client has now been added to your white list.

A.6.2.2 Use the Information Bar

With pop-up blocking enabled, the Information Bar can be set up and used for viewing information about blocked pop-ups or allowing pop-ups from a specified site.

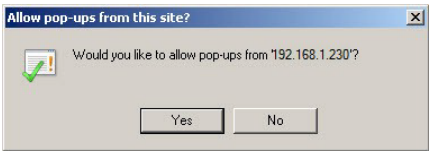
To set up the Information bar:

1. Go to the toolbar and select Tools | Pop-up Blocker | Pop-up Blocker Settings to open the Pop-up Blocker Settings dialog box.
2. In the Notifications and Filter Level frame, click the check box for "Show Information Bar when a pop-up is blocked."
3. Click **Close** to close the dialog box.

To access the Client:

1. Click the Information Bar for settings options:

2. Select Always Allow Pop-ups from This Site—this action opens the Allow pop-ups from this site? dialog box:



3. Click **Yes** to add the Client to your white list and to close the dialog box.

Note: To view your white list, go to the Pop-up Blocker Settings dialog box and see the entries in the Allowed sites list box.

Appendix B: RAID and Hardware Maintenance

This appendix is divided into three parts: Hardware Components, Server Interface, and Troubleshooting—in the event of a failure in one of the drives, power supplies, or fans.

Note: As part of the ongoing maintenance procedure for your RAID server, 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: If 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

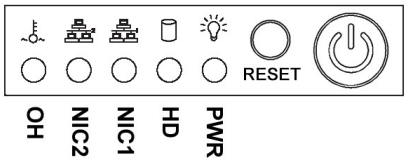
B.2.1 Front Control Panel on a 300 model

The keypad on the front of the server is used for performing basic server functions.

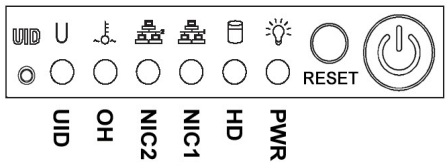
- **Boot up** - Depress and hold the checkmark key for 3 seconds.
- **Reboot** - Depress and hold the checkmark key for 10 seconds.
- **Shut down** - Depress and hold the 'X' key for 10 seconds.

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.

B.3.1.2 Verify the failed drive in the Admin console

The Hardware Failure Detection screen in the System Configuration console is accessible via the **Server | Hardware Failure Detection** menu selection:

Figure 7: Hardware Failure Detection screen, 300 model

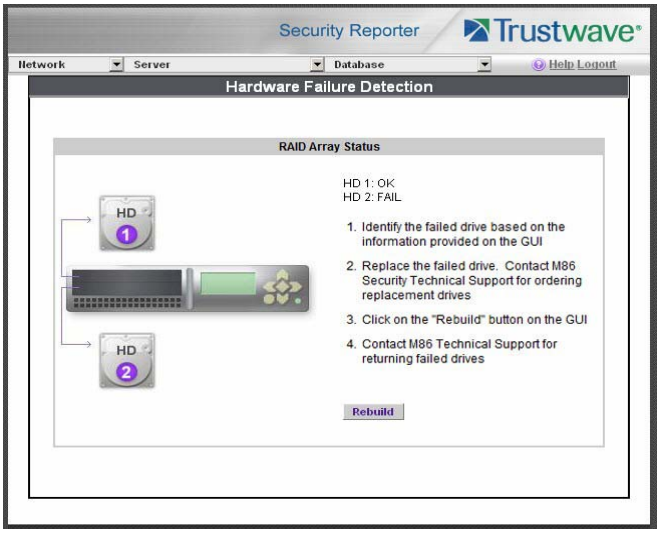


Figure 8: Hardware Failure Detection window, 500, 700, 730 model

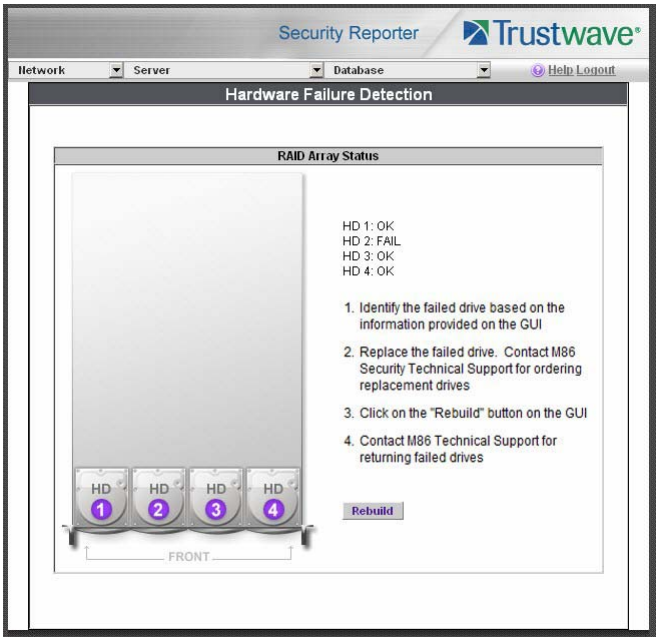


Figure 9: Hardware Failure Detection screen, 505 IBM model

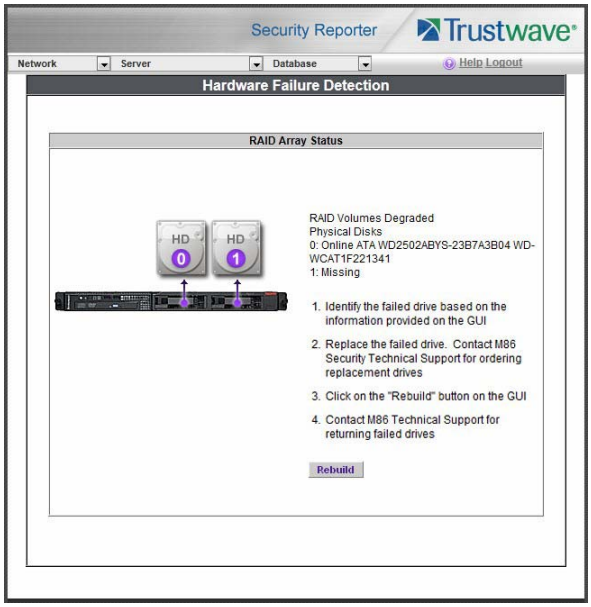
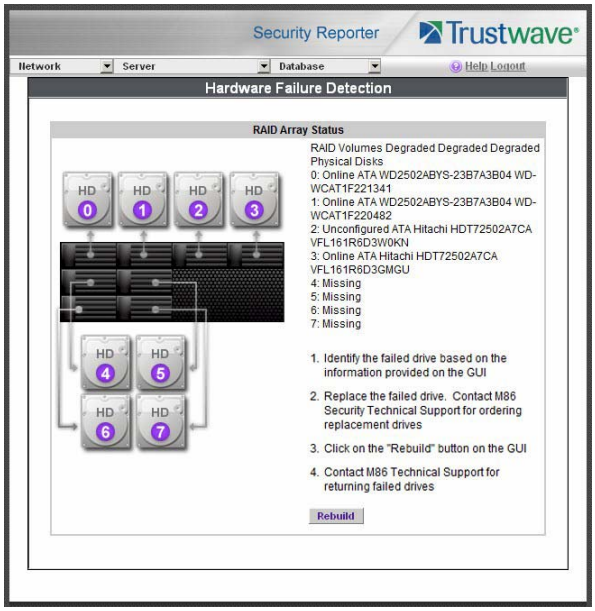


Figure 10: Hardware Failure Detection screen, 705 or 735 IBM model



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.

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.

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.

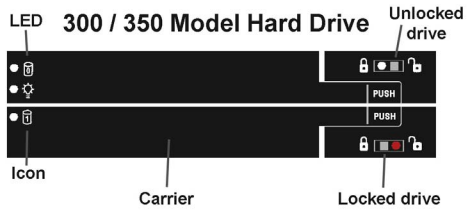
Before taking any action in this window, replace the drive.

B.3.1.3 Replace the failed hard drive

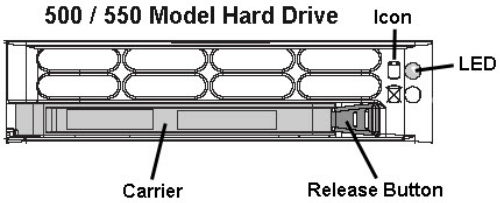
After verifying the failed hard drive in the Administrator console, go to the server to replace the drive.

Drive replacement on Equus SR models 300, 500, 700, 730

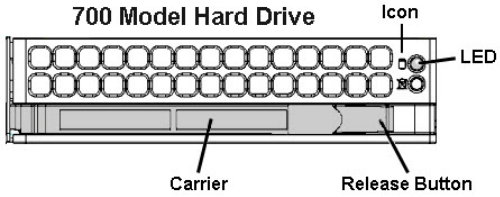
On a 300 model, be sure the carrier is unlocked, then press the section on the carrier handle labeled PUSH to release the carrier handle. On a 500, 700, or 730 model, press the red release button to release the carrier handle.



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.3.1.4.

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.3.1.4 .

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.3.1.4 Rebuild the hard drive

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.

Drive rebuild 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.3.1.5 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.

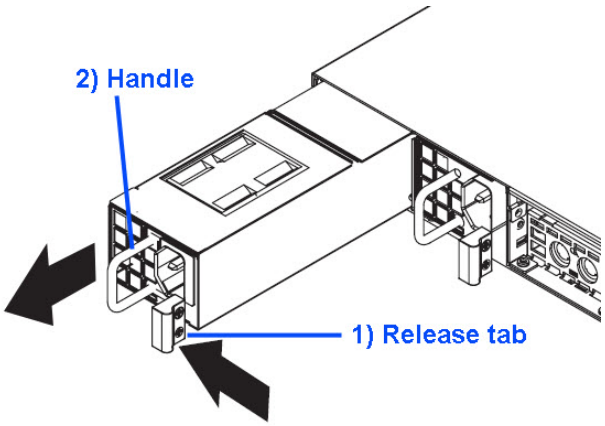
Caution: Be sure the correct failed power supply has been identified. Removing the wrong power supply will cause the system to crash.

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.

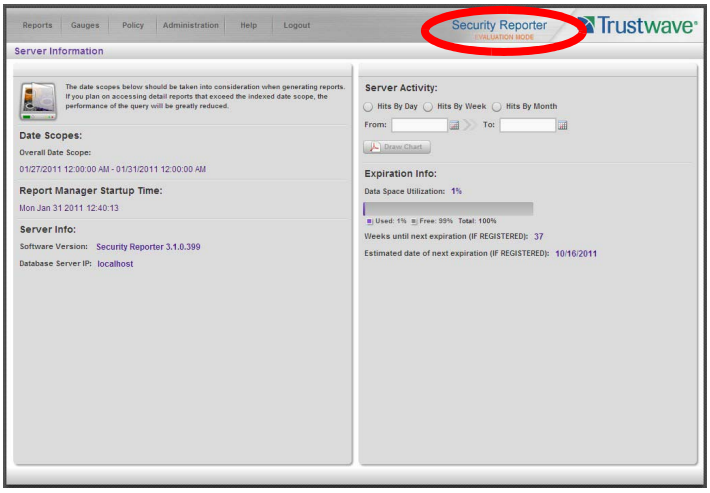
A steady red LED (on and not flashing) on a 500, 700, or 730 model indicates an overheating condition, which may be caused by cables obstructing the airflow in the system or the ambient room temperature being too warm. Check the routing of the cables and make sure all fans are present and operating normally. 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. This appendix explains how to use the SR in evaluation mode, and how to register the SR to function in registered mode.

C.1 Report Manager Banner

In evaluation mode, the Report Manager banner displays 'EVALUATION MODE' beneath the Security Reporter name/link:

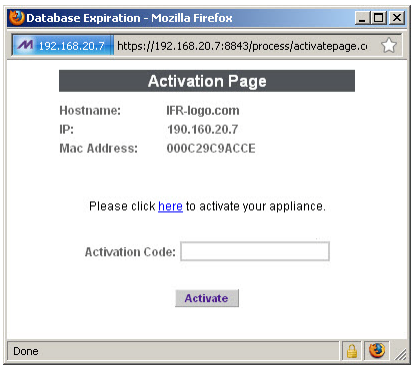


Hover over the '**EVALUATION MODE**' link to display a definition of 'Evaluation Mode'. Click this link to launch the SR Server Status screen of the System Configuration administrator console and Status pop-up box as described in the next sub-section.

Note: The System Configuration administrator console is only available to global administrators.

C.2 System Configuration Console

For an SR unit currently in evaluation mode, whenever the Server | Server Status screen is accessed, the SR Status pop-up box opens:



The SR will store data for the period specified in the pop-up box: "EVALUATION MODE - MAX DATA STORAGE 'X' DAYS"—in which 'X' represents the maximum number of days in the SR's data storage scope available to view during the evaluation period.

You have the option to either use the SR in the evaluation mode, or change the evaluation mode in one of two ways—by extending the evaluation period, or by registering the SR so that it can be used in the registered mode.

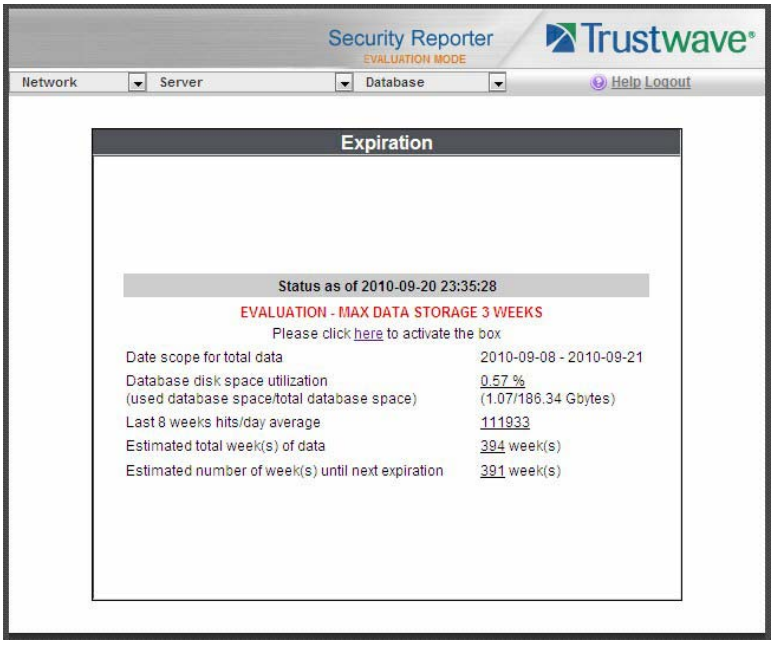
Note: The message: "EVALUATION MODE - MAX DATA STORAGE 'X' WEEKS" also displays at the top of the Expiration screen in the System Configuration console. Refer to the Expiration screen sub-section in the System Configuration Section for more information about data storage and expiration.

C.2.1 Use the Server in the Evaluation Mode

To use the unit in evaluation mode, click the "X" in the upper right corner of the SR Status pop-up box to close it.

C.2.1.1 Expiration screen

When navigating to Database | Expiration, the Expiration screen displays additional information in evaluation mode:



The following message displays beneath the Status bar: "EVALUATION – MAX DATA STORAGE 'X' WEEKS" (in which 'X' represents the maximum number of weeks in the SR's data storage scope available to view). This message is followed by a line stating: "Please click here to activate the box."

Clicking the link "here" is used for activating the SR to function in registered mode.

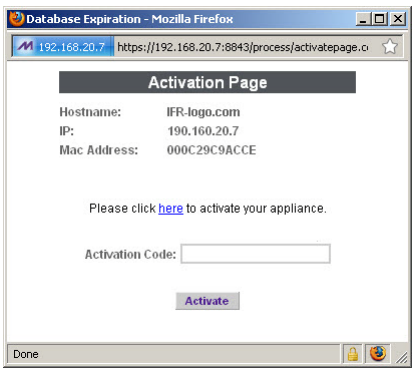
Note: The Status date and time and EVALUATION message do not display on a newly installed server, or a server that has just been reset to factory default settings. (See Reset to Factory Defaults panel in the Report Manager Administration Section for information about resetting the server to factory default settings.)

C.2.2 Change the Evaluation Mode

After the designated evaluation period has expired, you may extend your evaluation period, or register the unit and use it in the registered mode. There are two ways to change the evaluation mode from the System Configuration console:

- in the SR Status pop-up box, click **Change Evaluation Mode**
- in the Evaluation screen, click the link ("here") in the message at the top of the screen: "Please click here to activate the box".

By clicking the button or link, the Activation Page pop-up box opens:



C.2.2.1 Activation Page

1. In the Activation Page pop-up box, the **Hostname** of the Server, **IP** address, and **Mac Address** (Media Access Control address) display.
2. In the message "Please click here to activate your appliance.", click the link '**here**' to open the Product Activation page at the 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**. After Trustwave obtains your information, a technical support representative will issue you an activation code.
5. 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 extending the evaluation period for the unit, the following message displays: "It is now in evaluation mode ('X' days)!" in which 'X' represents the number of days in the new evaluation period.
   - If registering the unit, the following message displays: "Your box has been activated!"
7. Click the 'X' in the upper right corner to close the Activation Page pop-up box.

Appendix D: System Tray Alerts: Setup, Usage

This appendix explains how to set up and use the feature for System Tray alerts. This feature is available when real time reporting is enabled.

Caution: Real time reporting is disabled by default, and use of the feature is deprecated, because it seriously affects performance of report generation. For more information about real time reporting, see section 5.

An SR Alert is triggered in an administrator's System Tray if an end user's Internet usage has reached the upper threshold established for a gauge set up by that administrator.

This feature is only available to administrators using an LDAP username, account, and domain, and is not available if using IP groups authentication.

Note: In order to use this feature, the LDAP Username and Domain set up in the administrator's profile account (see Admin Profiles panel from the Report Manager Administrator Section) must be the same one he/she uses when logging into his/her workstation.

D.1 LDAP server configuration

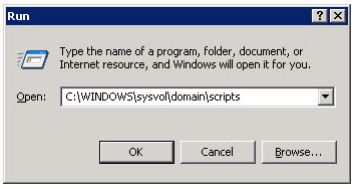
D.1.1 Create the System Tray logon script

Before administrators can use the System Tray Alert feature, an administrator with permissions on the LDAP server must first create a logon script on the LDAP server for authenticating administrators.

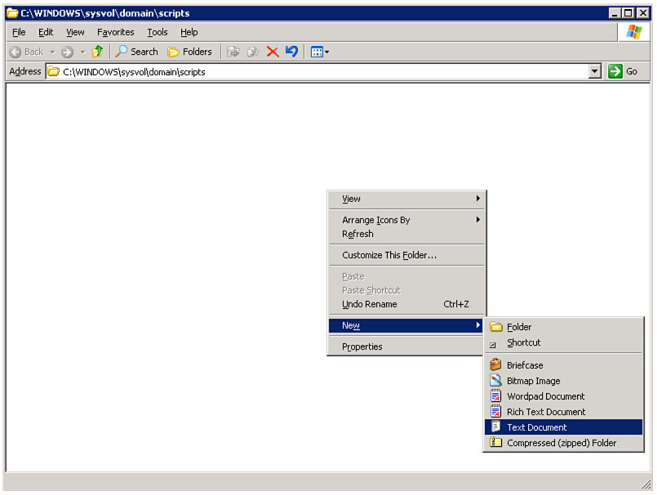
1. From the SR GUI menu, click Policy > Alert Application to download the tray application (`srtrayw32.exe`).
2. Save this application in a network share location that can be accessed from all administrator workstations.

Note: You could also direct administrators to copy and run the file from their local workstations.

3. From the taskbar of the LDAP server, go to: Start | Run to open the Run dialog box:

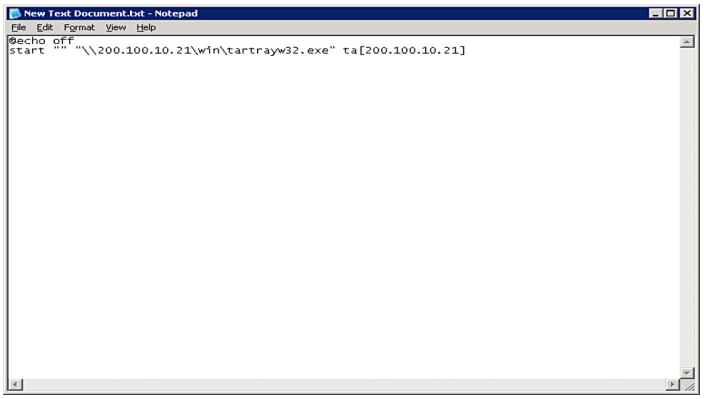


4. In the Run dialog box, type in the path to the scripts folder: `C:\WINDOWS\sysvol\domain\scripts`.
5. Click **OK** to open the scripts folder:



6. Right-click in this Windows folder to open the pop-up menu.

7. Select New | Text Document to launch a New Text Document:



8. Type the following text in the blank document file:

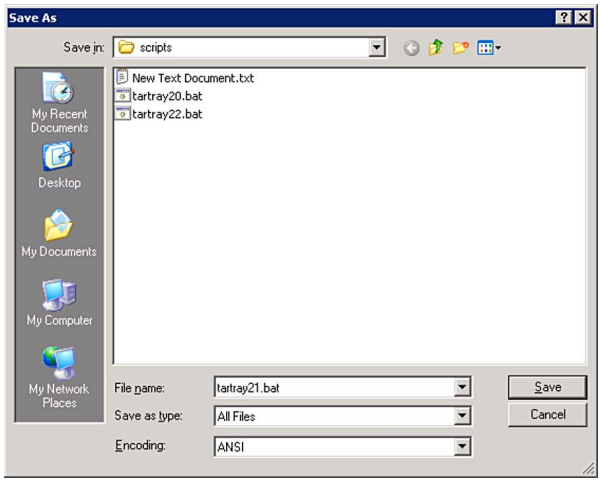
   ```
   @echo off

   start “” “\\{server}\{path}\srtrayw32.exe” ta[{SR IP}]
   ```

   where \\{server}\{path} is the full CIFS name (Windows network share name) of the network share where the SR Tray Alert executable file srtrayw32.exe is located, and {SR IP} is the IP address of the SR server.

Note: { } braces indicate variables and should NOT be entered in your file. [ ] braces are part of the syntax and MUST be entered in your file. See the above screenshot for an example.

9. Go to: File | Save As to open the Save As window:



10. In the **File name** field, type in the name for the file using the “filename.bat” format. For example: `srtray21.bat`.

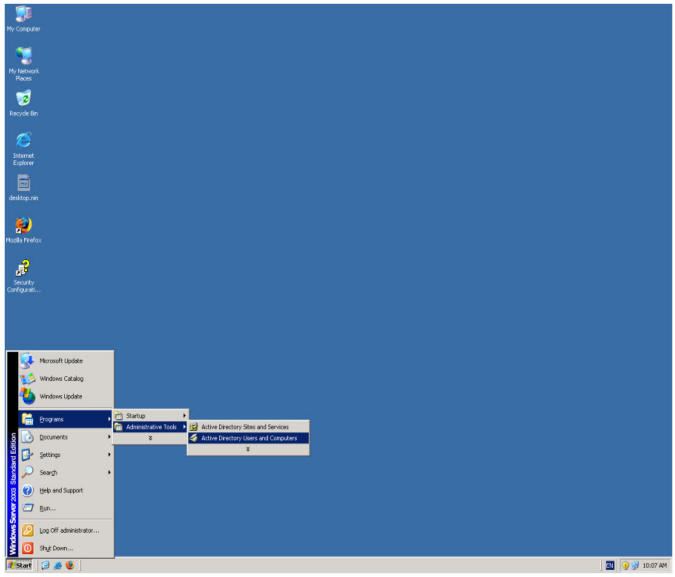
Note: Be sure that the Save as type field has “All Files” selected.

11. Click **Save** to save your file and to close the window.

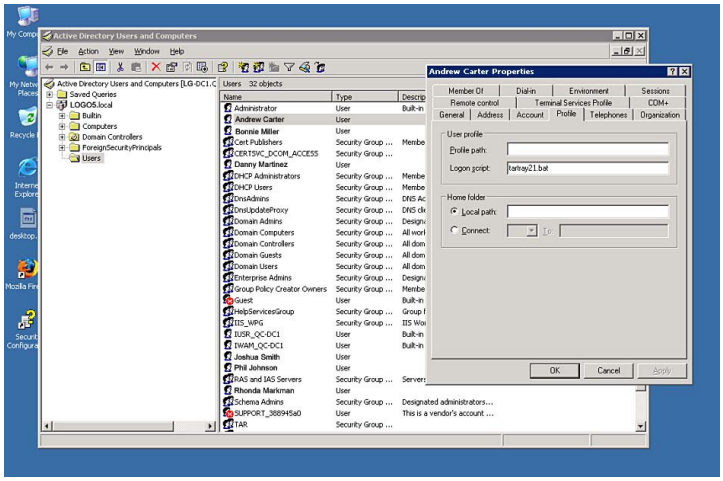
D.1.2 Assign System Tray logon script to administrators

With the ".bat" file created, the administrator with permissions on the LDAP server can now begin to assign the System Tray logon script to as many administrators as needed.

1. From the taskbar of the LDAP server, go to: Start | Programs | Administrative Tools | Active Directory Users and Computers to open the Active Directory Users and Computers folder:



2. In the Active Directory Users and Computers folder, double-click the administrator's Name in the Users list to open the Properties dialog box for his/her profile:



3. In the Properties dialog box, click the Profile tab to display its contents.
4. In the **Login script** field, type in the ".bat" filename. For example: `srtray21.bat`.
5. Click **Apply** to save your entry.
6. Click **OK** to close the dialog box.

7. Click the "X" in the upper right corner of the folder to close the window.

D.2 Administrator usage of System Tray

Once the System Tray logon script has been added to the administrator's profile, when the administrator logs on his/her workstation, the System Tray Alert icon (pictured to the far left in the image below) automatically loads in his/her System Tray:

Note: The System Tray Alert icon will not load in the System Tray if the SR server is not actively running.

D.2.1 Use the System Tray Alert icon's menu

When right-clicking the System Tray Alert icon, the following pop-up menu items display:

- SR Admin Interface - clicking this menu selection launches a browser window containing the SR user interface's login window.
- Reconnect - clicking this menu selection re-establishes the System Tray Alert icon's connection to the SR server, resetting the status of the System Tray Alert icon to the standard setting.
- Exit - clicking this menu selection removes the System Tray Alert icon from the System Tray.

D.2.2 Status of the System Tray Alert icon

If there are no alerts for any gauges set up by the administrator, the following message displays when hovering over the standard System Tray Alert icon: "Connected. No Alerts."

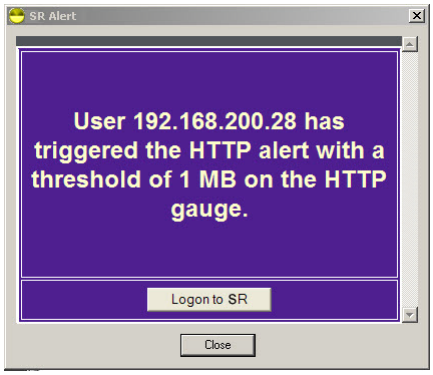
However, if an alert is triggered, the System Tray Alert icon changes in appearance from the standard gauge to a yellow gauge (pictured to the far left in the image below):

The new SR Alert! message appears briefly above the yellow gauge, and the new SR Alert message displays whenever hovering over this icon.

If more than one alert is triggered for the administrator, the new SR Alert! message includes "(X Total)", in which "X" represents the total number of new alerts. The "X" new SR Alerts message displays whenever hovering over this icon, in which "X" represents the total number of new alerts.

D.2.3 View System Tray alert messages

1. Double-click the SR Tray Alert notification icon to open the SR Alert box:



   This box contains the following message: "User (username/IP address) has triggered the (Alert Name) alert with a threshold of X (in which "X" represents the alert threshold) on the (URL dashboard gauge name) gauge."

   The Logon to SR button displays beneath this message, followed by the Close button.

   If more than one alert was triggered, the alert box includes the following message and button to the right of the Close button: "X more alerts" (in which "X" represents the number of additional alerts), and the Next >> button.

2. Click **Logon to SR** to launch the SR login window.

   If there are additional alerts, click **Next >>** to view the next SR Alert. Each time the Next >> button is clicked, the number of remaining alerts to be viewed decreases by one. The Next >> button no longer displays after the last alert is viewed.

3. Click **Close** to close the SR Alert box.

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, group administrator profiles, and gauges.

group by report type
A report that includes two or more sets of report type criteria, such as User/Sites or Category/IPs or Category/Site/Users.

hit count
the number of pages and/or objects end users access as the result of entering URLs in a browser window.

HTTP
Hyper Text Transfer Protocol is used for transferring files via the World Wide Web or an intranet.

instant messaging
IM involves direct connections between workstations either locally or across the Internet.

library category
A list of URLs, URL keywords, and search engine keywords set up to be blocked.

LDAP
One of two authentication method protocols that can be used with the SR. Lightweight Directory Access Protocol (LDAP) is a directory service protocol based on entries (Distinguished Names). The other authentication method that can be used with the SR is IP groups.

object count
The number of objects end users access on a Web page, including images, graphics, multimedia items, and text items. The number of objects on a page is generally higher than the number of pages a user visits.

page count
The number of Web pages end users access, which can exceed the number of objects per page in categories that use a lot of pop-up ads (porn, gambling, and other related sites). A user may visit only one site, but visit 20 pages on that site if the page has pop-up ads or banner ads that link to other pages.

peer-to-peer
P2P involves communication between computing devices—desktops, servers, and other smart devices—that are linked directly to each other.

protocol
A type of format for transmitting data between two devices. LDAP is a type of authentication method protocol.

search engine
A program that searches Web pages for specified keywords and returns a list of the pages or services where the keywords were found.

SMTP
Simple Mail Transfer Protocol is used for transferring email messages between servers.

summary drill down report
One of two types of basic reports—the other report type being a "detail drill down report"—that provides a synopsis of end user Internet activity for the specified time period.

synchronization
A process by which two or more machines run in parallel to each other. User filtering profiles and library configurations on the source Web Filter can be set up to be synchronized between the source Web Filter and the SR.

TCP
An abbreviation for Transmission Control Protocol, one of the core protocols of the Internet protocol suite. Using TCP, applications on networked hosts can create connections to one another, over which streams of data can be exchanged.

time count
The amount of time end users spend on a given Web page, including the number of times that page is refreshed by either the user or a banner ad.

Time Usage Report count
The amount of time end users spend on the Internet, based on the Time Usage algorithm. For each user, the number of seconds from the log is dropped, and any unique minute within a given hour counts as one minute.

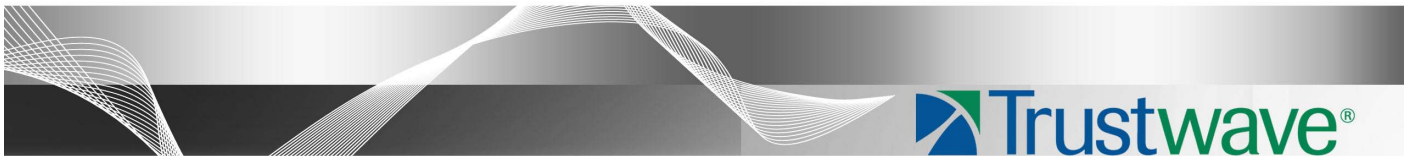
Traveler
Trustwave's executable program that downloads updates to the SR at a scheduled time.

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 SS, such as Trustwave Web Filter or Trustwave Secure Web Gateway (SWG).

Index



About Trustwave®

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