SECURITY REPORTER VIRTUAL INSTALLATION GUIDE

VERSION 3.3.15

Publication Date: 7 August 2014

Legal Notice

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

www.trustwave.com/support/

Trademarks

Part# SR-VIG-140807

Formatting Conventions

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

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

Table of Contents

1 Trustwave SR Virtual Introduction

Thank you for choosing to download and install Trustwave Security Reporter Virtual software. The Security Reporter (SR) from Trustwave consists of the best in breed of Professional Edition reporting software consolidated into one unit, with the capability to generate productivity reports of end user Internet activity from Trustwave Web Filter and/or Trustwave Secure Web Gateway (SWG) appliance(s), and security reports from an SWG.

After the SR software image is installed on your appliance and running as a virtual machine, logs of end user Internet activity from a Web Filter and/or SWG are fed into the 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.

Quick setup procedures to implement the best reporting practices are included in the Best Reporting Practices section of this Guide.

1.1 About this Document

This document is divided into the following sections:

- **Introduction** - This section is comprised of an overview of the SR product and how to use this document
- **Service Information** - This section provides Trustwave contact information
- **Preliminary Setup Procedures** - This section includes instructions on how to prepare your environment for the inclusion of SR Virtual on your network
- **Install and Configure SR Virtual** - This section explains how to install and configure the SR for reporting
- **Best Reporting Practices** - This section includes reporting scenarios and instructions for implementing the best reporting practices to capture a snapshot of end user activity on your network that tells you whether or not policies are being enforced
- **Evaluation Mode** - This section gives information on using the SR in the evaluation mode
- **Appendices** - Appendix A explains how to configure bandwidth monitoring. Appendix B explains how to install the optional Ethernet Tap device on your network for bandwidth monitoring.

- **Index** - An alphabetized list of some topics included in this document

2 Service Information

Any software setup problem that cannot be resolved at your internal organization should be referred to a Trustwave solutions engineer or technical support representative.

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

2.1 Trustwave Technical Support Call Procedures

When calling Trustwave regarding a problem, please provide the representative the following information:

- Your contact information.
- Original order number.
- Description of the problem.
- Network environment in which the virtual appliance hosting SR Virtual software is used.
- State of SR Virtual software before the problem occurred.
- Frequency and repeatability of the problem.
- Can the product continue to operate with this problem?
- Can you identify anything that may have caused the problem?

3 Preliminary Setup Procedures

3.1 Network Requirements

The following items are required for using SR Virtual:

- Host appliance on your network that supports Virtualization Technology
- VMware ESXi 4.1 or 5 server
- VMware ESXi 4.1 or 5 vSphere Client
- SR Virtual product downloaded to your appliance, which includes the following items:
  - SR software image
  - End User License Agreement
  - link to Security Reporter documentation page at Trustwave's Web site: **http://www.trustwave.com/support/sr/documentation.asp**

The following optional devices can be used with SR Virtual:

- One or more attached "NAS" storage devices (e.g. Ethernet connected, SCSI/Fibre Channel connected "SAN")
- An Ethernet Tap device connected to the virtual server for monitoring bandwidth

3.1.1 Server Sizing Recommendations

The virtual host platform should meet the following minimum specifications:

- 64 bit architecture (required for supported ESXi versions)
- Four CPU cores
- 12 GB RAM assigned to the SR virtual appliance.

To determine the appropriate virtual disk size, contact your Account Manager.

If you intend to run more than one VM on the host, be sure to provide enough resource for each VM.

3.2 Download and Install the SR software image

1. Download the SR software image to your appliance from a link on this page:
   http://www.trustwave.com/support/sr/virtual-product-upgrade.asp

Note: Contact your Trustwave account representative or a Trustwave solutions engineer if you need assistance accessing the URL or downloading the SR image. Before installing the software image on your machine, be sure you have reviewed the End User License Agreement.

2. Import the SR software image into the ESXi server..

Caution: Trustwave recommends selecting “Thick provisioned format” for your datastore. See Section 3.3 for important information about selecting “Thin provisioned format”.

3. With the SR powered on, access the vSphere Client’s Console panel and proceed to the next section of this Installation Guide that requires you to set up parameters for the SR to function on the network.

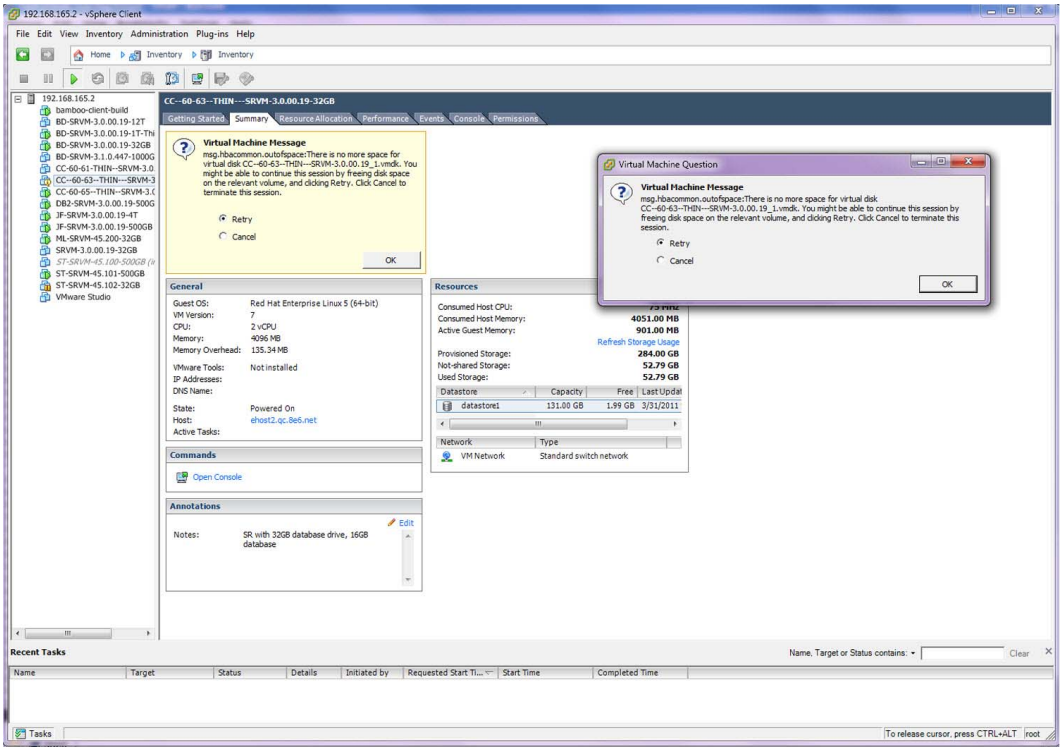
3.3 Important Virtual Machine Message

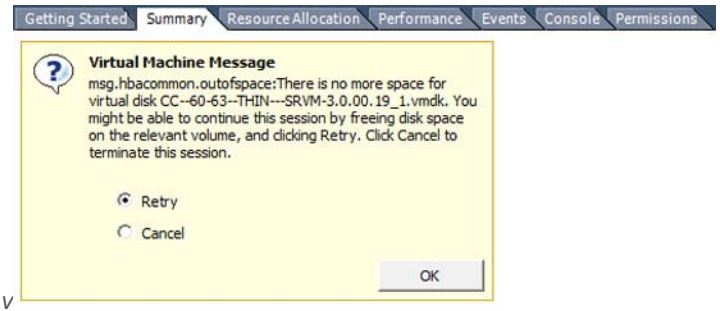
Trustwave recommends selecting “Thick provisioned format” since the system will automatically allocate appropriate disk space to the SR Virtual image and you will not need to monitor the amount of disk space being used by the datastore.

If “Thin provisioned format” is selected, you will need to monitor the amount of disk space available for SR data storage.

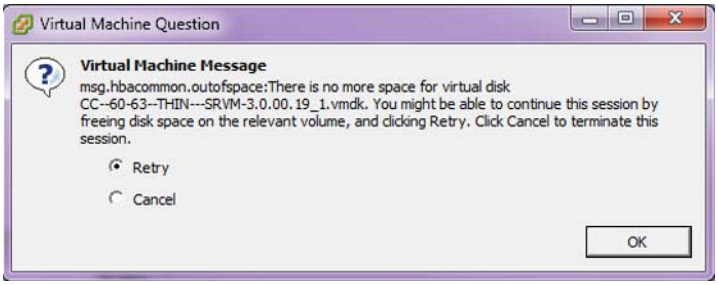
If data storage space runs out, the machine will run out of memory and freeze up, and the following Virtual Machine Message will display in the vSphere Client Console’s Summary tab and in a window: “There is no more space for virtual disk name.vmdk (in which ‘name’ represents the name of the virtual machine). You might be able to continue this session by freeing disk space on the relevant volume, and clicking Retry. Click Cancel to terminate this session.”

The following images illustrate this scenario:





V



To proceed, you will need to free up space on the disk, and then click “Retry” and **OK** to continue.

4 Install and Configure SR Virtual

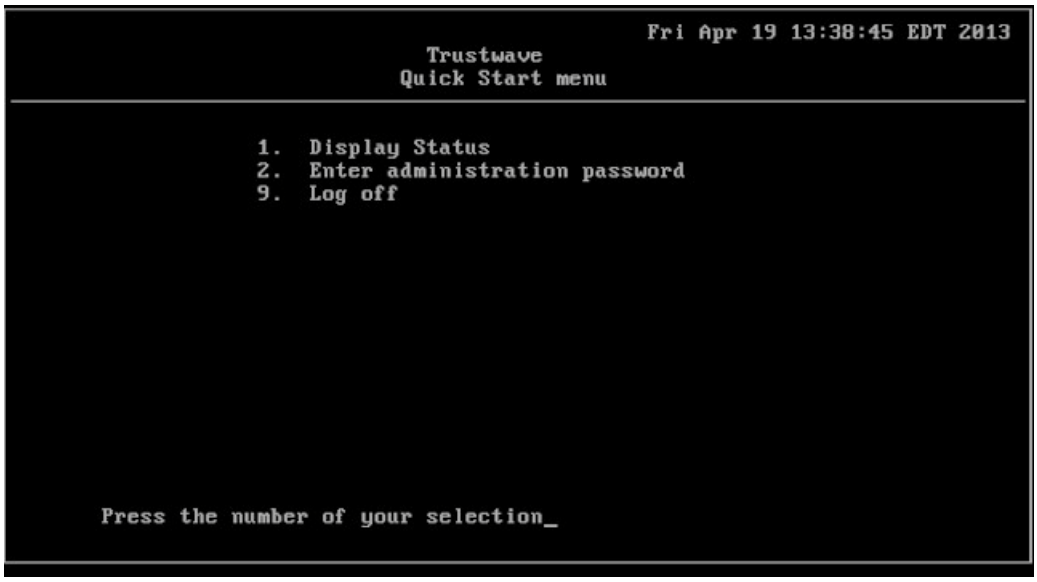
4.1 Quick Start Setup Procedures

4.1.1 Login screen

In the Console panel of the vSphere Client:

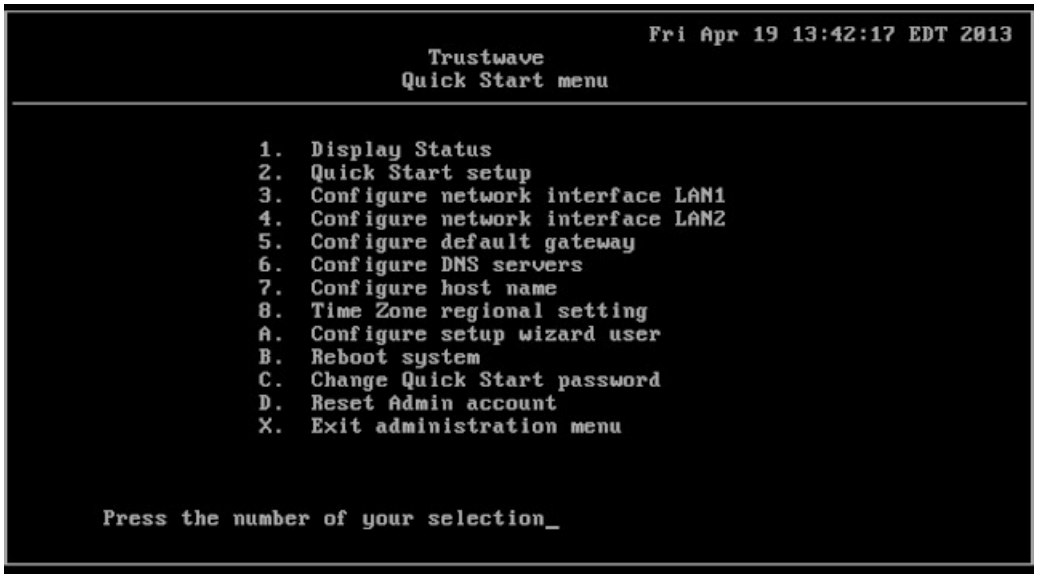
1. At the **login** prompt, type in `menu`.
2. Press the **Enter** key to display the Password prompt.
3. At the **Password** prompt, type in the following: `#s3tup#r3k`
4. Press **Enter** to display the Quick Start menu screen.

4.1.2 Quick Start menu screen



1. At the **Press the number of your selection** prompt, press **2** to select the Quick Start setup process.
2. At the login prompt, re-enter your password: `#s3tup#r3k`
3. Press **Enter** to display the administration menu where you can begin using the Quick Start setup procedures.

4.1.3 Quick Start setup



1. At the **Press the number of your selection** prompt, press **2** to select the “Quick Start setup” process.

   The Quick Start setup process takes you to the following configuration screens to make entries:

   - Configure network interface LAN1
   - Configure network interface LAN2
   - Configure default gateway
   - Configure DNS servers
   - Configure host name
   - Time Zone regional setting
   - Configure setup wizard user.

Note: Please make a note of the LAN 1 and LAN 2 IP address and hostname you assign to the SR server, as well as the username and password you create for logging into the “setup wizard”, as you will need to use this information in later steps of the installation procedure.

2. After making all entries using the Quick Start setup procedures, press **X** to return to the Quick Start menu screen. Or, to verify the status of the SR and review the entries you made using the Quick Start setup, press **1** to view the System Status screen.

Note: To configure an individual screen from the Quick Start menu, press the number or alphabet corresponding to that menu option, as described in the following sub-sections.

4.1.3.1 Configure network interface LAN1

1. From the Quick Start menu, press **3** to go to the Configure Network Interface screen for LAN1.

2. At the **Enter interface LAN1 IP address** prompt, type in the LAN1 IP address and press **Enter**.
3. At the **Enter interface LAN1 netmask** prompt, type in the netmask for the LAN1 IP address and press **Enter**.
4. Press **Y** to confirm, or press any other key to cancel this change.

4.1.3.2 Configure network interface LAN2

1. From the Quick Start menu, press **4** to go to the Configure Network Interface screen for LAN2.
2. At the **Enter interface LAN2 IP address** prompt, type in the LAN2 IP address and press **Enter**.
3. At the **Enter interface LAN2 netmask** prompt, type in the netmask for the LAN2 IP address and press **Enter**.
4. Press **Y** to confirm, or press any other key to cancel this change.

4.1.3.3 Configure default gateway

1. From the Quick Start menu, press **5** to go to the Configure default gateway screen.
2. At the **Enter default gateway IP** prompt, type in the gateway IP address and press **Enter**.
3. Press **Y** to confirm, or press any other key to cancel this change.

4.1.3.4 Configure DNS servers

1. From the Quick Start menu, press **6** to go to the Configure Domain Name Servers screen.
2. At the **Enter first DNS server IP** prompt, type in the IP address of the DNS server to use and press **Enter**.
3. At the **Enter (optional) second DNS server IP** prompt, either type in the IP address of an alternate DNS server to use and press **Enter**, or just press **Enter** to bypass making a second DNS server entry.

4.1.3.5 Configure host name

1. From the Quick Start menu, press **7** to go to the Configure host name screen.
2. At the **Enter host name** prompt, type in the hostname and press **Enter**.
3. Press **Y** to confirm, or press any other key to cancel this change.

4.1.3.6 Time Zone regional setting

1. From the Quick Start menu, press **8** to go to the Time Zone regional configuration screen.
2. Select a region using up-arrow and down-arrow keys. Press **Y** when you have selected the appropriate region, or press **Esc** to cancel this change.

Note: If this server is located in the USA, please select “US” and not “America”.

3. After you select the region, you may be prompted to select the locality within the selected region. Select thefte locality and press **Y** to confirm, or Press **Esc** to cancel the change.

Note: If you are making any change to this menu selection, you must reboot the server to make your settings effective.

4.1.3.7 Configure setup wizard user

1. From the Quick Start menu, press **A** to go to the Configure Wizard user screen.
2. At the **Enter wizard user name** prompt, type in the new username to be used by the global administrator for the SR Wizard user setup process and press **Enter**.

Note: The username ‘admin’ cannot be used since it is already the default username. The default password is ‘testpass’.

3. At the **Enter wizard password** prompt, type in the new password for the username you entered and press **Enter**.

Note: The username and password you enter and save here will be used by the global administrator for Single Sign-On access in the SR user interface.

4. Press **Y** to confirm, or press any other key to cancel this change.

4.1.3.8 Non-Quick Start procedures or settings

The options described below do not pertain to the quick start setup process.

4.1.3.8.1 Reboot system

1. From the Quick Start menu, press **B** to go to the Reboot confirmation screen.
2. At the **Really reboot the system?** prompt, press **Y** to continue, or press any other key to cancel reboot.

4.1.3.8.2 Change Quick Start password

1. From the Quick Start menu, press **C** to go to the Change Administrator Password screen.

Note: This option will change the password used for accessing the Quick Start menu (the default password is `#s3tup#r3k`) but will not change the global administrator’s Single Sign-On password used for accessing the SR user interface via its login window (the default password is ‘testpass’). Option D, “Reset Admin account”, should be used for resetting the SR login password (the default account reset password is ‘reporter1!’) and for unlocking all IP addresses currently locked.

2. At the **Enter the new administrator password** prompt, type in the new password to be used for accessing the Quick Start menu and press **Enter**.
3. At the **Re-enter the new administrator password** prompt, re-type the password you just entered and press **Enter**, or press **Esc** to cancel the change.

4.1.3.8.3 Reset Admin account

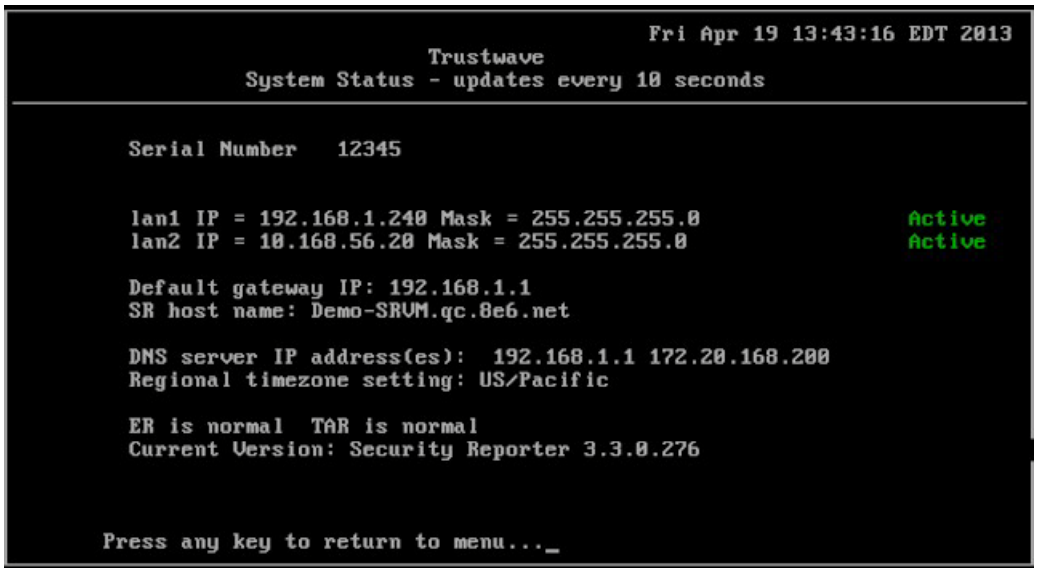
1. From the Quick Start menu, press **D** to go to the Reset admin GUI account confirmation screen that displays the following message:

```
Reset admin account password?  Are you sure?
NOTE: This process will also unlock the admin account and unlock all currently
locked IPs.
```

Caution: This option resets the global administrator's Single Sign-On password to 'reporter1!' and will unlock all IP addresses currently locked.

2. Press **Y** to continue, or press any other key to cancel admin account reset.

4.1.4 System Status screen



The System Status screen contains the following information:

- **Serial Number** (applicable only to SR Appliances)
- **lan1 IP** address and netmask specified in screen 3, and current status ("Active" or "Inactive")
- **lan2 IP** address and netmask specified in screen 4, and current status ("Active" or "Inactive")
- **Default gateway IP** address specified in screen 5 (Configure default gateway)
- **SR host name** specified in screen 7 (Configure host name)
- **DNS server IP address(es)** specified in screen 6 (Configure DNS servers)
- **Regional timezone setting** specified in screen 8 (Time Zone regional setting)
- current status of ER (System Configuration) and TAR (real time reporting) applications

- **Current Version** of software installed

Note: Modifications can be made at any time by returning to the specific screen of the Quick Start setup procedures. To access the System Status screen from the Quick Start setup screen, press **1** and then **Enter**.

4.1.5 Log Off

After completing the Quick Start setup procedures, return to the Quick Start menu screen and press **9** to log out.

Proceed to the next section.

4.2 Connect Peripheral Devices to the Host

Now that your SR network parameters are set, you can physically connect peripheral devices—i.e. Fibre Channel Connected Storage Device and/or Tap device—to the host appliance.

4.2.1 Storage Device Setup (for Attached Storage Units)

If you have a NAS (Fibre Channel Connected Storage Device or “SAN”) that will be used with the SR, you will need to connect it to the host appliance at this point.

4.2.2 Bandwidth Management

If you choose to install an Ethernet Tap for bandwidth monitoring, you will need to connect it to the host appliance at this point. Refer to Appendix A and Appendix B at the end of this document for instructions on how to configure Bandwidth Monitoring and how to connect an Ethernet Tap unit to the host appliance.

Note: In order to monitor bandwidth on the SR, both inbound and outbound traffic must be sent to the SR through use of a port span, tap, or other similar device.

4.3 Access the SR and its Applications Online

Next you will access the SR and its applications online. For this step you will need your network administrator to provide you the following information:

- If using a Web Filter, IP range and netmask of machines on the network that the Security Reporter application will use for monitoring bandwidth on your network
- Web Filter or SWG IP address, and port number to be used between the Web Filter/SWG and SR

4.3.1 Access the SR via its LAN 1 IP Address

1. Launch a supported web browser:
    - Firefox 16
    - Internet Explorer 8 or 9
    - Safari 5 or 6

- Google Chrome 23

2. In the address line of the browser window, enter the URL (web address) of the Security Reporter interface.
   - The URL is like `https://{the LAN 1 IP address}:8443`
   - (HTTPS and port 1443 are used for a secure network connection).
   - For example, if the LAN 1 IP address is 10.10.10.10 type in `https://10.10.10.10:8443`.
3. Click **Go**
   The browser will display a security certificate issue page. This is expected behavior in the Security Reporter setup.
4. Accept the security certificate to proceed to the login page.

Tip: For a full walk-through of accepting certificates in supported browsers, see Appendix C.

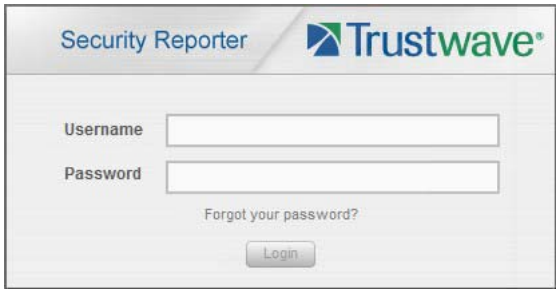
If the security issue page does not display in your browser, verify the following:

- The SR is powered on.
- Can the administrator workstation normally connect to the Internet?
- Is the administrator workstation able to ping the SR's LAN 1 IP address? (To ping the SR using the Command Prompt in Windows XP, Vista, and 7, go to Start | All Programs | Accessories | Command Prompt, type in `Ping` and the IP address using the x.x.x.x format—in which each 'x' represents an octet—and then press **Enter**.)
- If pinging the IP address of the SR is unsuccessful, try restarting the network service or rebooting the SR.
- If still unsuccessful, contact a Trustwave solutions engineer or technical support representative.

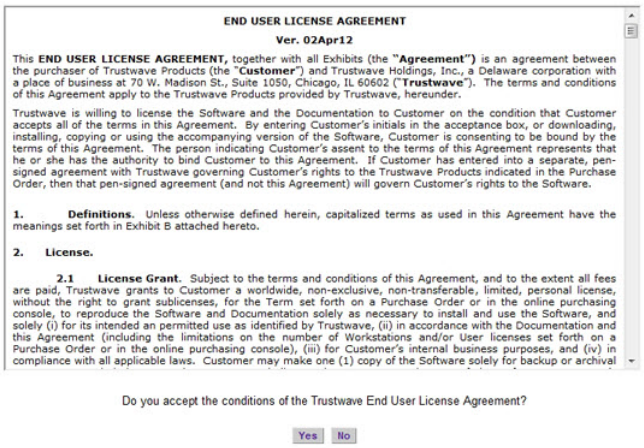
Note: On a newly installed unit, reports will remain inaccessible until logs are transferred to the SR and the database is built.

4.3.2 Accept the End User License Agreement

1. In the Security Reporter login window, enter your **Username** and **Password**, and then click **Login** to proceed:



You may be prompted to accept a security exception for the SR application, after which the EULA Agreement dialog box opens:



2. After reading the End User License Agreement, click **Yes** to accept the EULA, close the EULA Agreement dialog box, and open the Security Reporter Wizard Login window.

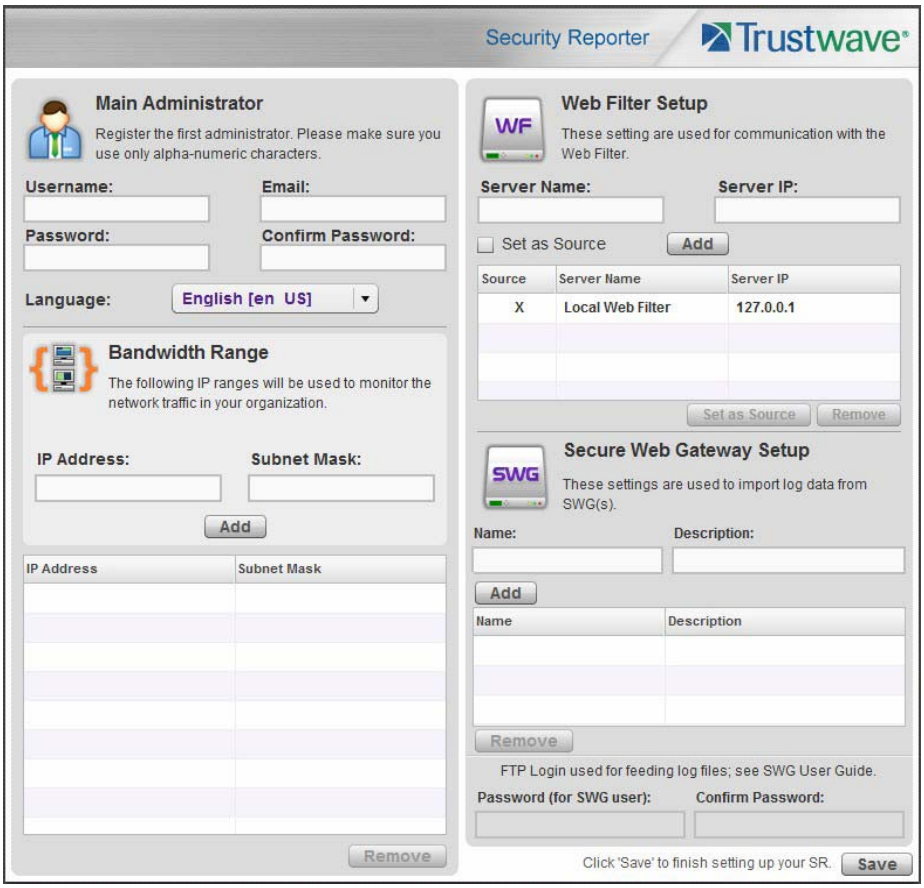
   Proceed to Log in to the Security Reporter Wizard.

4.3.3 Log in to the Security Reporter Wizard

1. In the **Username** field of the Login window, type in the username specified in the Configure setup wizard user screen of the Quick Start Setup Procedures:

2. In the **Password** field, type in the password specified in the wizard screen.
3. Click **Login** to close the login window and to go to the Security Reporter wizard screen.

4.3.4 Use the SR Wizard to Specify Application Settings



At minimum, the Main Administrator section must be populated and saved. The following section(s) should be populated for the type of Web-access logging device(s) to be used with this SR, if you have the necessary data at this time:

- Bandwidth Range and Web Filter Setup sections, if using one or more Web Filters with this SR.
- Secure Web Gateway Setup section, if using one or more SWG policy servers with this SR.

Note: If the Web Filter or Secure Web Gateway sections are not populated at this time, the required information will need to be provided in the Device Registry panel of the user interface before the SR can function on your network.

4.3.4.1 Enter Main Administrator Criteria

1. Enter the **Username** the global administrator will use when logging into the Security Reporter. The global administrator has the highest level of permissions in all user applications in SR.
2. Enter the **Email** address of the global administrator, who will be notified via email regarding system alerts.
3. Enter the **Password** to be used with that username, and enter the same password again in the **Confirm Password** field.

4. 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.

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

4.3.4.2 For Web Filters: Go to Bandwidth Range and Web Filter Setup

Note: Bandwidth Range and Web Filter Setup entries are pertinent only to Web Filters to be used with this SR. If one or more Web Filters will be used with this SR, these entries are not required during this Wizard setup process, but if not entered during this process, must be configured in the device registry in order to use the SR on your network.

4.3.4.2.1 Enter Bandwidth Range

1. Enter the bandwidth **IP Address** range the Security Reporter will monitor.
2. Enter the **Subnet Mask** for the bandwidth IP range to be monitored, using the dotted decimals notation format.
3. Click **Add** to include your entries in the list box below.

Note: Additional bandwidth ranges can be included by following steps A through C again. To remove a bandwidth range, select the IP Address from the list box and then click **Remove**.

4.3.4.2.2 Enter Web Filter Setup Criteria

1. Enter the **Server Name** of the Web Filter to be used with the Security Reporter, which is any name you wish to associate with that Web Filter.
2. Enter the **Server IP** address of the Web Filter server to be used with the Security Reporter.
3. Click the “Set as Source” check box if this Web Filter will be designated the primary Web Filter to be associated with the Security Reporter. Otherwise, leave the check box blank.
4. Click **Add** to include your entries in the list box below.

Notes:

- Additional Web Filters can be included by following steps A through D again.
- The Source Web Filter is designated by an “X” in the Source column of the list box.
- To specify a Source Web Filter server from available entries in the list box, select the Server Name and then click Set as Source.
- To remove a Web Filter server from the list, select the Server Name from the list box and then click Remove.

4.3.4.3 For SWGs: Go to Secure Web Gateway Setup

Note: Secure Web Gateway Setup entries only apply if you plan to use this SR to provide reporting for one or more SWG Policy Servers. SWG entries are not required during this Wizard setup process. You can enter them later in the device registry.

1. In the Secure Web Gateway Setup section, type in the **Name** and/or **Description** for the SWG.
2. 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**.

3. Type in the **Password (for SWG user)** and type this same password again in the **Confirm Password** field. The password entered here will be used by all SWG Policy Servers set up in the Device Registry panel to provide security when the SWGs 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.

4.3.4.4 Save settings

Click **Save** at the bottom right of the screen to save your settings and to go to the login window of the Security Reporter user interface (see Step 4).

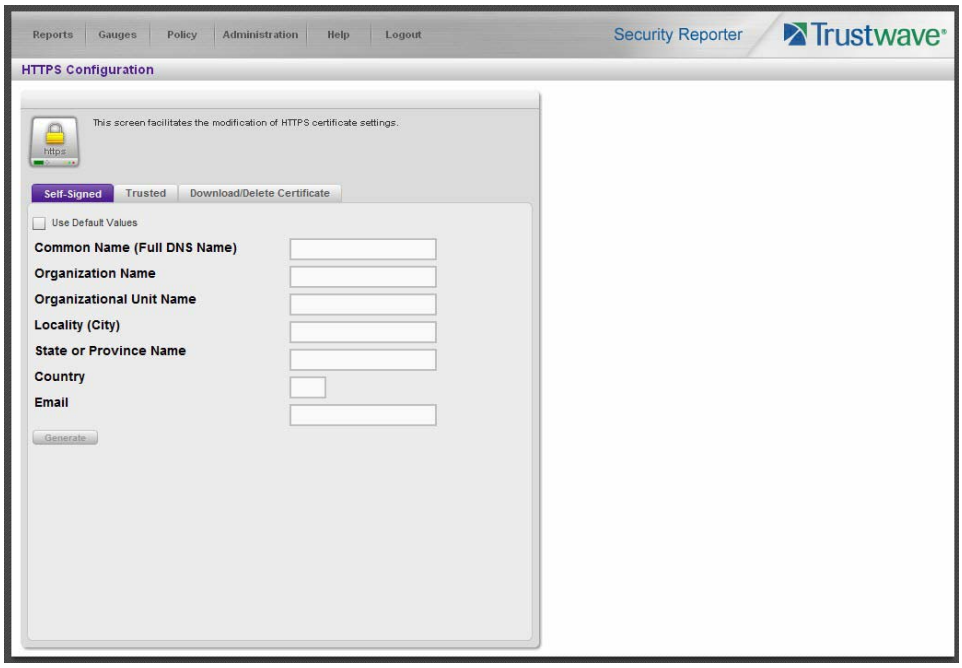
4.4 Generate SSL Certificate

4.4.1 Generate a Self-Signed Certficate for the SR

This step requires you to generate a self-signed certificate so your browser will recognize the SR as an accepted application.

1. In the Security Reporter login window, type in the **Username** and **Password** set up during the SR wizard.
2. Click **Login** to access the Report Manager application.

3. Go to the navigation menu bar at the top of the screen and select Administration | HTTPS Configuration to display the HTTPS Configuration screen:



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.

4. Do the following:
   - click the check box corresponding to **Use Default Values** to grey-out the tab, or
   - make entries in these fields:
     - **Common Name (Full DNS Name)** - hostname of the server, such as `logo.com`.
     - **Organization Name** - Name of your organization, such as `Logo`.
     - **Organizational Unit Name** - Name of your department, such as `Administration`.
     - **Locality (City)** - Name of your organization's city or principality, such as `Orange`.
     - **State or Province Name** - Full name of your state or province, such as `California`.
     - **Country** - Two-character code for your country, such as `US`.
     - **Email** - Your email address.
5. Click **Create** to generate the SSL certificate to be stored on the SR, and to restart the Report Manager. Thereafter, 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: Although the Security Reporter login window may re-display right away, the service will take a few minutes before it starts up again.

If using a Firefox, Safari, or Chrome browser, proceed to Section 4.5.

If using an IE browser, continue to IE Security Certificate Installation Procedures.

4.4.2 IE Security Certificate Installation Procedures

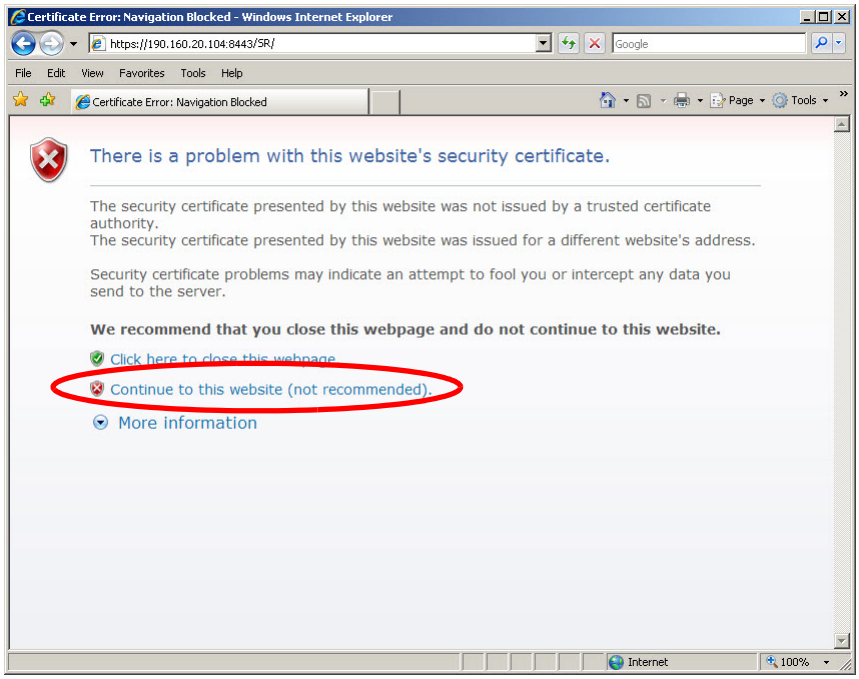
4.4.2.1 Accept the Security Certificate in IE

Go to the appropriate sub-section if using the following Windows operating system and IE browser:

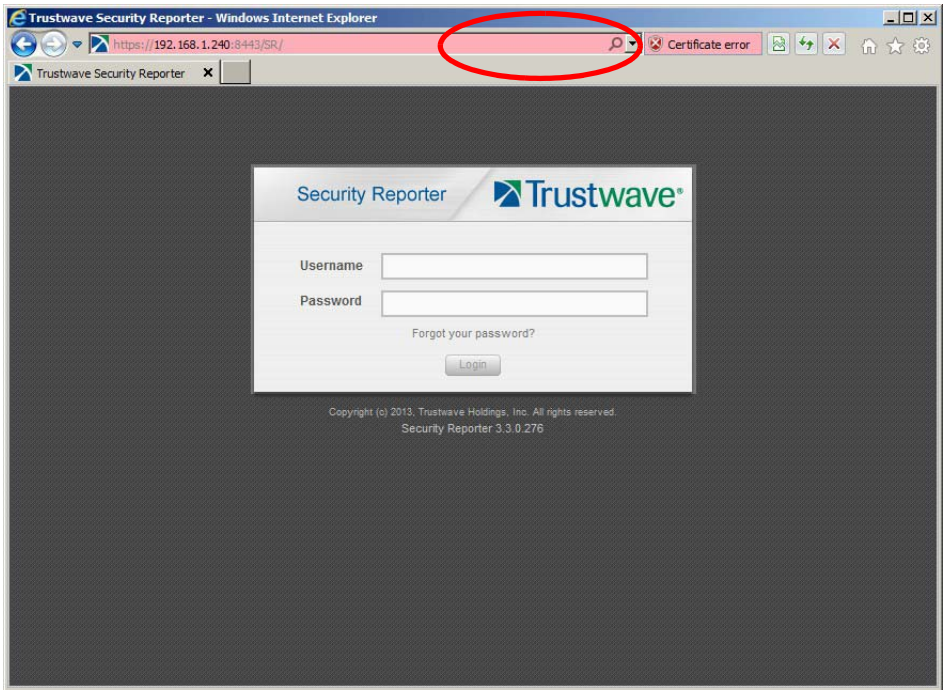
- Windows XP or Vista with IE 8 or 9
- Windows 7 with IE 8 or 9

4.4.2.1.1 Windows XP or Vista with IE 8 or 9

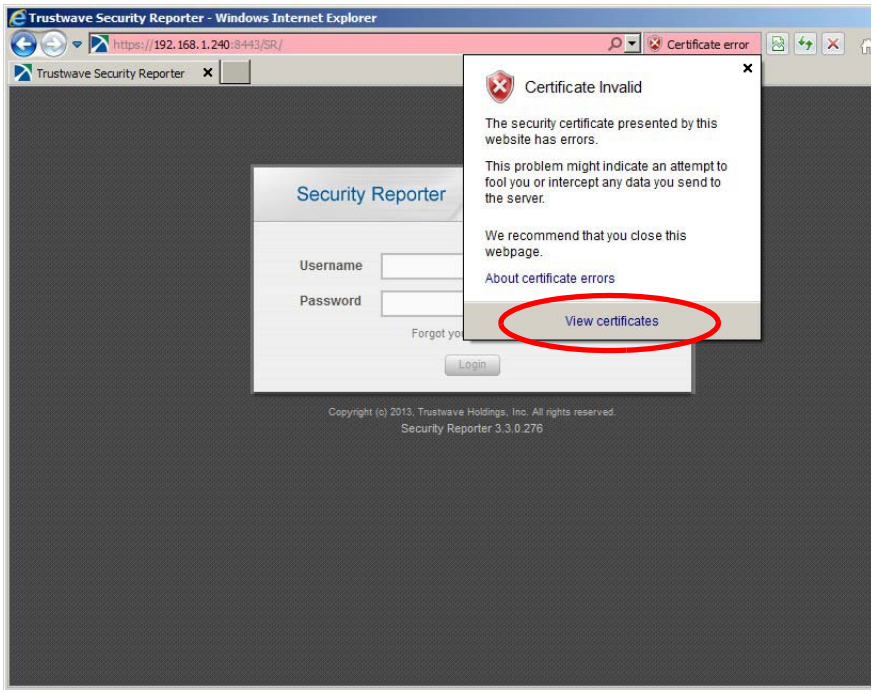
1. If using an IE 8 or 9 browser on a Windows XP or Vista machine, in the page “There is a problem with this website's security certificate.”, click **Continue to this website (not recommended)**:



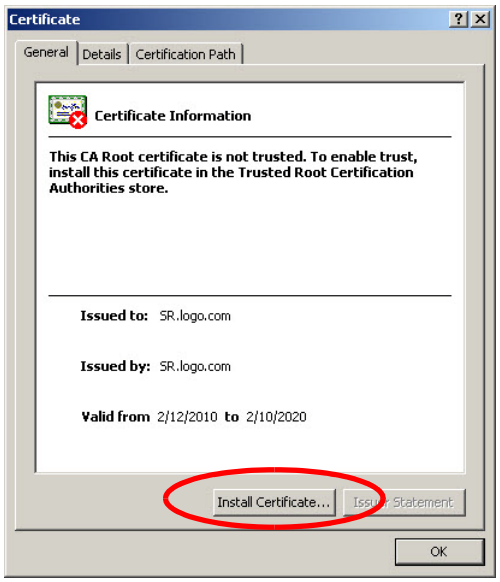
Selecting this option displays the SR Welcome window with the address field and the Certificate Error button to the right of the field shaded a reddish color:



2. Click **Certificate Error** to open the Certificate Invalid box:

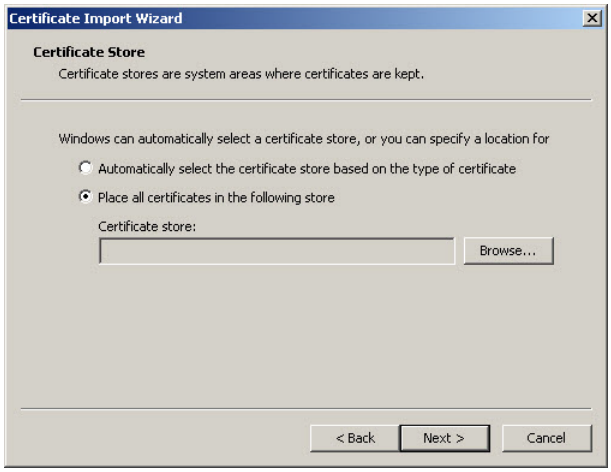


3. Click **View certificates** to open the Certificate window that includes the hostname you assigned to the SR:



4. Click **Install Certificate...** to launch the Certificate Import Wizard:

5. Click **Next >** to display the Certificate Store page:

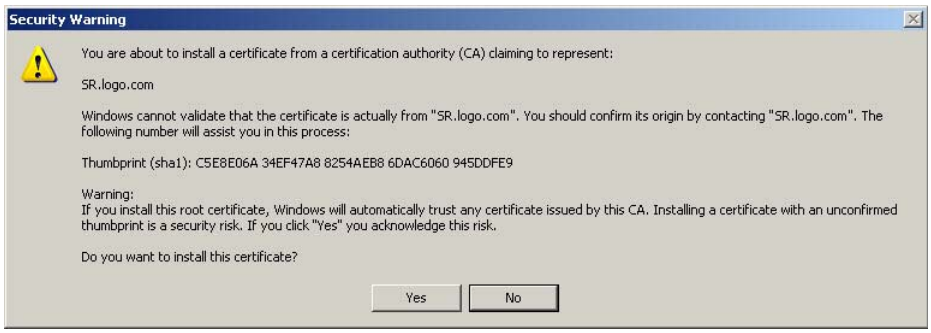


6. Choose the option “Place all certificates in the following store” and then click **Browse...** to open the Select Certificate Store box:

7. Choose “Trusted Root Certification Authorities” and then click **OK** to close the box.

8. Click **Next >** to display the last page of the wizard:

9. Click **Finish** to close the wizard and to open the Security Warning dialog box asking if you wish to install the certificate:



10. Click **Yes** to install the certificate and to close the dialog box. When the certificate is installed, the alert window opens to inform you the certificate installation process has been completed.
11. Click **OK** to close the alert box, and then close the Certificate window.

Now that the security certificate is installed, you will need to map the SR's IP address to its hostname. Proceed to Map the SR's IP Address to the Server's Hostname.

4.4.2.1.2 Windows 7 with IE 8 or 9

1. If using an IE 8 or 9 browser on a Windows 7 machine, in the page "There is a problem with this website's security certificate.", click **Continue to this website (not recommended)**.
2. From the toolbar, select Tools | Internet Options to open the Internet Options box.
3. Select the Security tab, click **Trusted sites**, and then click **Sites** to open the Trusted sites box.
4. In the Trusted sites box, confirm the URL displayed in the field matches the IP address of the SR, and then click **Add** and **Close**.
5. Click **OK** to close the Internet Options box.
6. Refresh the current Web page by pressing the **F5** key on your keyboard.
7. Follow steps a to k documented in Windows XP or Vista with IE 8 or 9:
    a. When the security issue page re-displays with the message: "There is a problem with this website's security certificate.", click **Continue to this website (not recommended)** (see Figure A1). Choosing this option displays the SR Welcome window with the address field and the Certificate Error button to the right of the field shaded a reddish color (see Figure A2).
    b. Click **Certificate Error** to open the Certificate Invalid box (see Figure B).
    c. Click **View certificates** to open the Certificate window that includes the hostname you assigned to the SR (see Figure C).
    d. Click **Install Certificate...** to launch the Certificate Import Wizard (see Figure D).
    e. Click **Next >** to display the Certificate Store page (see Figure E).
    f. Choose the option "Place all certificates in the following store" and then click **Browse...** to open the Select Certificate Store box (see Figure F).

g. Choose “Trusted Root Certification Authorities” and then click **OK** to close the box.

h. Click **Next >** to display the last page of the wizard (see Figure G).

i. Click **Finish** to close the wizard and to open the Security Warning dialog box asking if you wish to install the certificate (see Figure H).

j. Click **Yes** to install the certificate and to close the dialog box. When the certificate is installed, the alert window opens to inform you the certificate installation process has been completed (see Figure I).

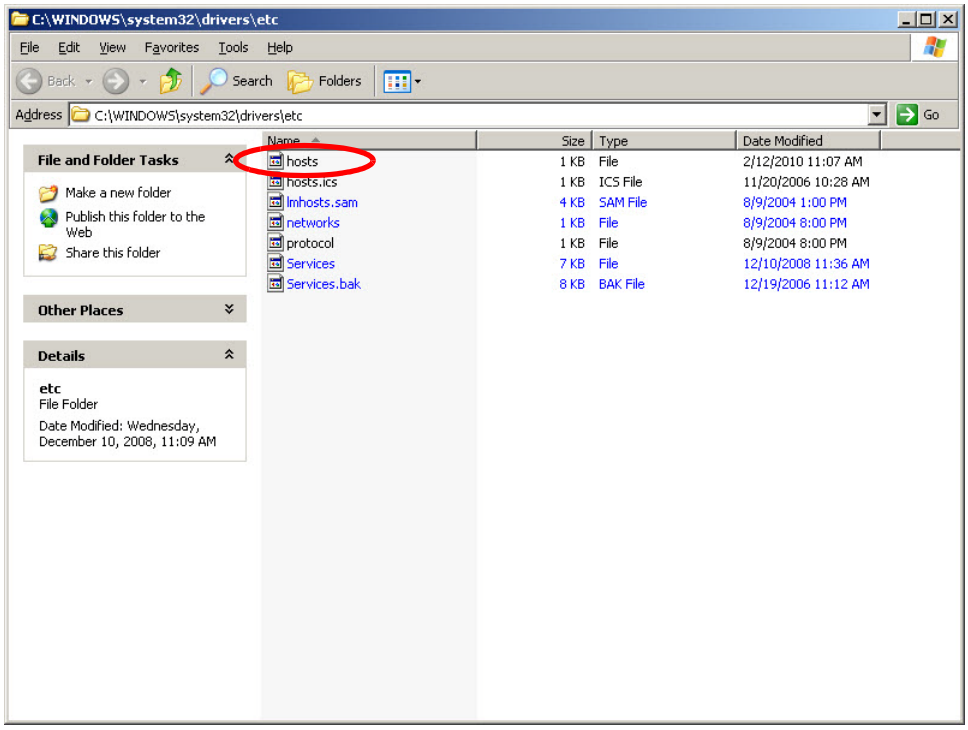
k. Click **OK** to close the alert box, and then close the Certificate window.

8. From the toolbar of your browser, select Tools | Internet Options to open the Internet Options box.
9. Select the Security tab, click **Trusted sites**, and then click **Sites** to open the Trusted sites box.
10. Select the URL you just added, click **Remove**, and then click **Close**.

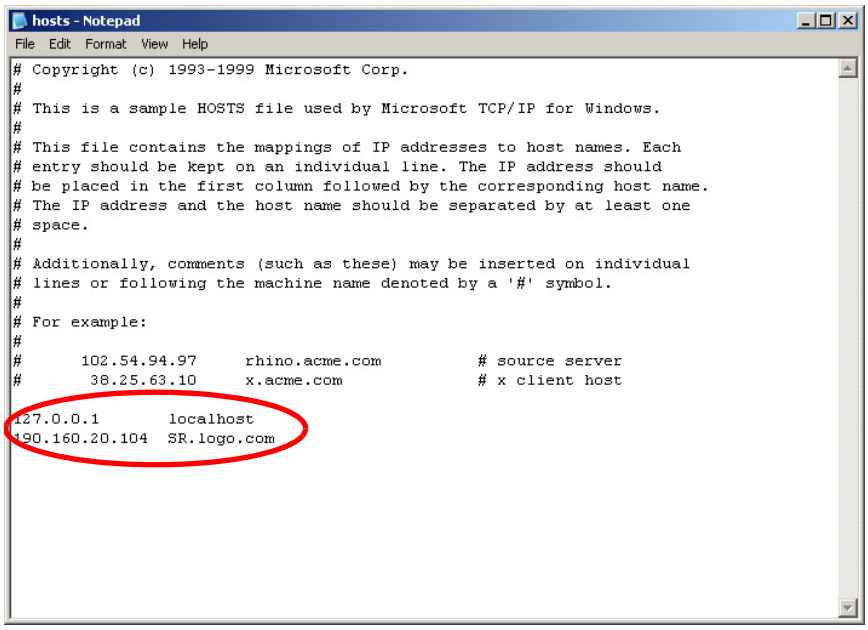
Now that the security certificate is installed, you will need to map the SR’s IP address to its hostname. Proceed to Map the SR’s IP Address to the Server’s Hostname.

4.4.2.2 Map the SR’s IP Address to the Server’s Hostname

1. From your workstation, launch Windows Explorer and enter `C:\WINDOWS\system32\drivers\etc` in the Address field to open the folder where the hosts file is located:

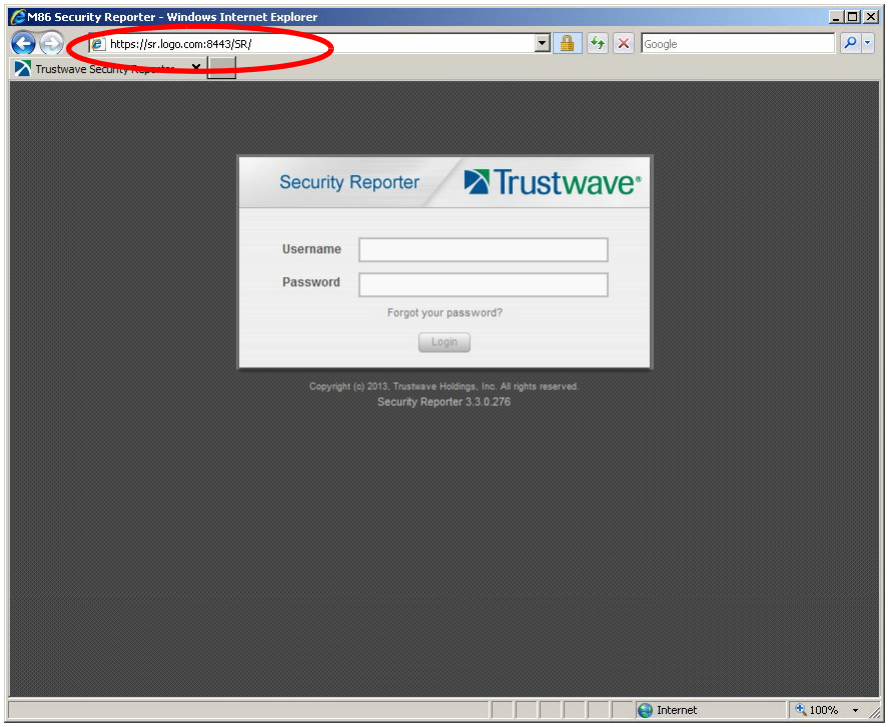


2. Double-click “hosts” to open a window asking which program you wish to use to open the file. Double-click “Notepad” or “TextPad” to launch the hosts file using that selected program:



3. Enter a line in the hosts file with the SR’s IP address and its hostname—the latter entered during the Configure host name screen of the Quick Start Setup Procedures—and then save and close the file.

4. In the address field of your newly opened IE browser, from now on you will need to use the SR’s hostname instead of its IP address—that is `https://hostname:8443/SR/` would be used instead of `https://x.x.x.x:8443/SR/`. Click **Go** to open the SR Welcome window:

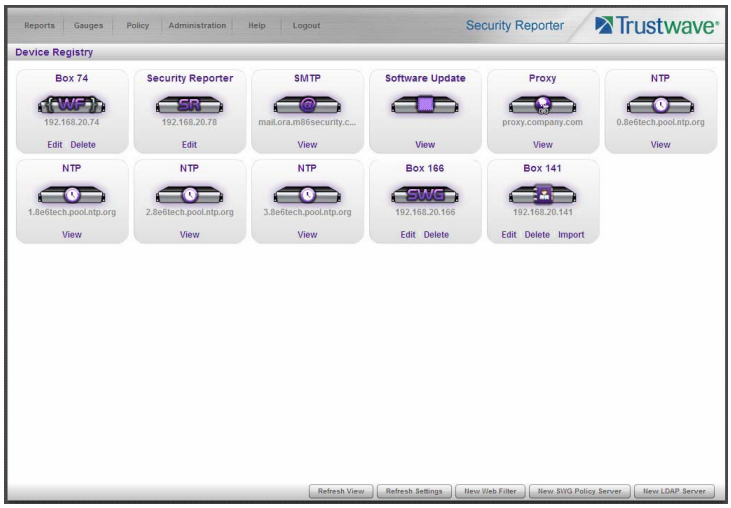


Proceed to the next section.

4.5 Add Web Filter, SWG to Device Registry

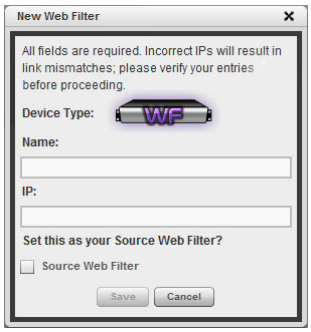
Before you begin configuring the Web Filter and/or SWG to send logs to the SR, you will need to add the Web Filter/SWG in the SR's Device Registry panel if the device(s) was/were not added during the SR Wizard installation process in Step 3.

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



4.5.1 Add a Web Filter Device

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.
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.

4.5.2 Add an SWG Device

1. At the bottom of the Device Registry panel, click **New SWG Policy Server** 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 to enter this information in the SWG to allow the SWG to transfer logs to this SR. The Path consists of the IP address of the SR, and a unique number for each configured SWG policy server.

2. Enter a **Name** for the device and/or a **Description** for the device.
3. If this is the first SWG you have entered and you did not previously enter a common password for the SWG, enter the **Password** and 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.

All SWG devices use the common password that you configured in the Secure Web Gateway Setup section of the SR Wizard (or in the Add SWG dialog described above, if you did not configure it in the SR wizard). To change this password if required, edit any configured SWG device and click **Change Common Password**.

4.6 Set up Web Filter, SWG Log Transfers

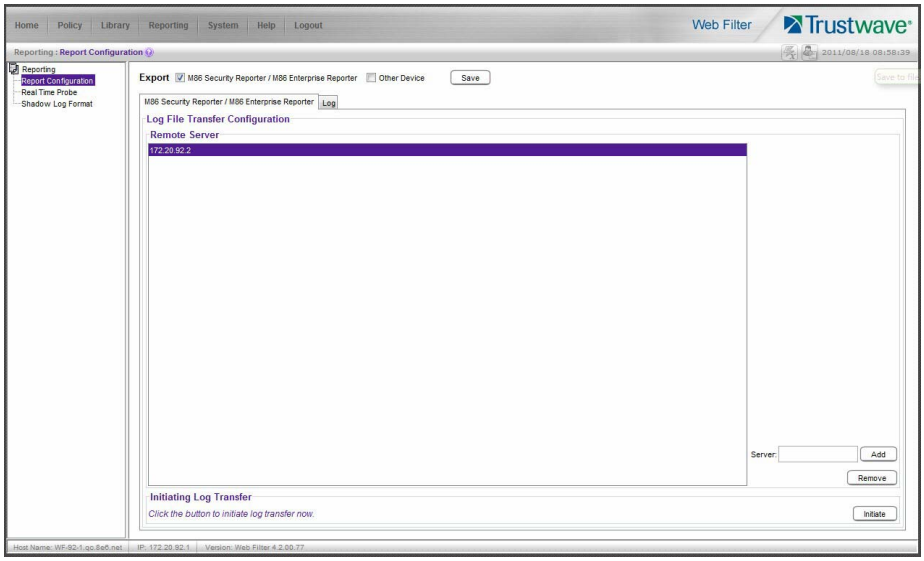
This step can be performed any time during SR setup, but must be completed in order for the SR to receive logs from the Web Filter and/or SWG.

4.6.1 Web Filter Setup

4.6.1.1 Web Filter Configuration

1. Access the user interface of the Web Filter.
2. Choose the **Reporting** link at the top of the screen to display the Reporting section of the Administrator console.

3. From the navigation panel at the left of the screen, choose **Report Configuration** to display the Report Configuration window.
4. Select **M86 Security Reporter / M86 Enterprise Reporter** to display the M86 Security Reporter / M86 Enterprise Reporter tab:



5. In the **Server** field, enter the LAN 1 IP address you assigned to your SR, and then click **Add** to include this IP address in the Remote Server list box.
6. Click **Save**. Your Web Filter is now set to transfer its log files to your SR via HTTPS.

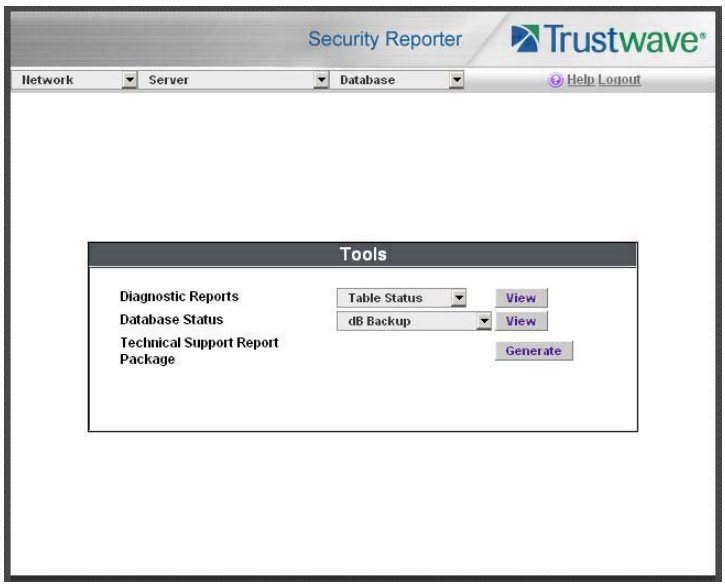
Note: It is recommended you wait for 1 - 2 hours after the initial installation so sufficient data is available for viewing.

4.6.1.2 Web Filter Log Transfer Verification

You can see if log files have transferred by following these steps in the SR:

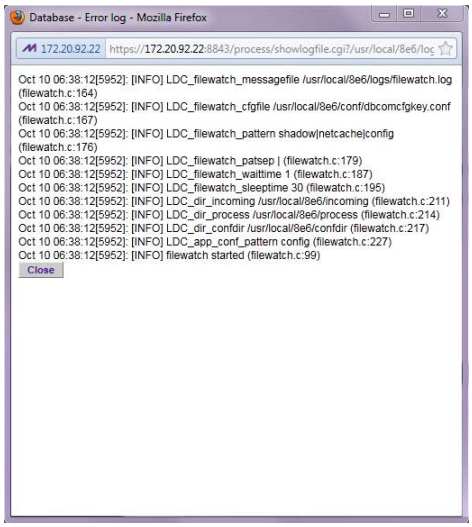
1. Access the System Configuration administrator console.

2. Go to the Database pull-down menu and choose **Tools** to display the Tools screen:



3. From the **Database Status** menu, select **File Watch Log**.

4. Click **View** to open the Database log:

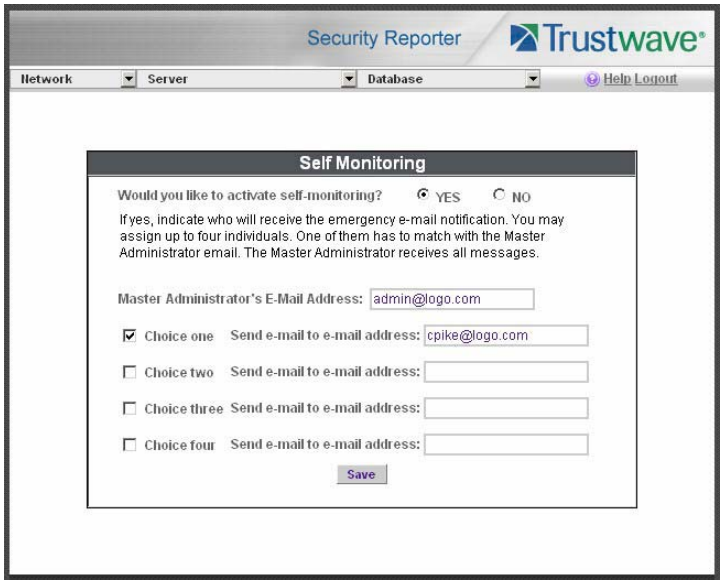


The transfer is working if you see an entry that includes the date and time for incoming shadow logs. The transfer should occur every hour. Once you see an entry, reporting information will be available one hour after the timestamp of the import listing.

4.6.1.3 Set Self-Monitoring

1. In the SR Report Manager navigation toolbar, select Administration | System Configuration to display the Server Status panel screen of the System Configuration administrator console.

2. From the Server pull-down menu, choose **Self-Monitoring** to display the Self Monitoring screen:



3. Choose **YES** to activate monitoring.
4. Enter the **Master Administrator's E-Mail Address**.
5. Click **Choice one** and enter an e-mail address of an individual in your organization that you would like notified if the SR detects any problems when processing data. This can be the same e-mail address entered in the previous field. Enter up to four e-mail addresses.
6. Click **Save**.

4.6.2 SWG Setup

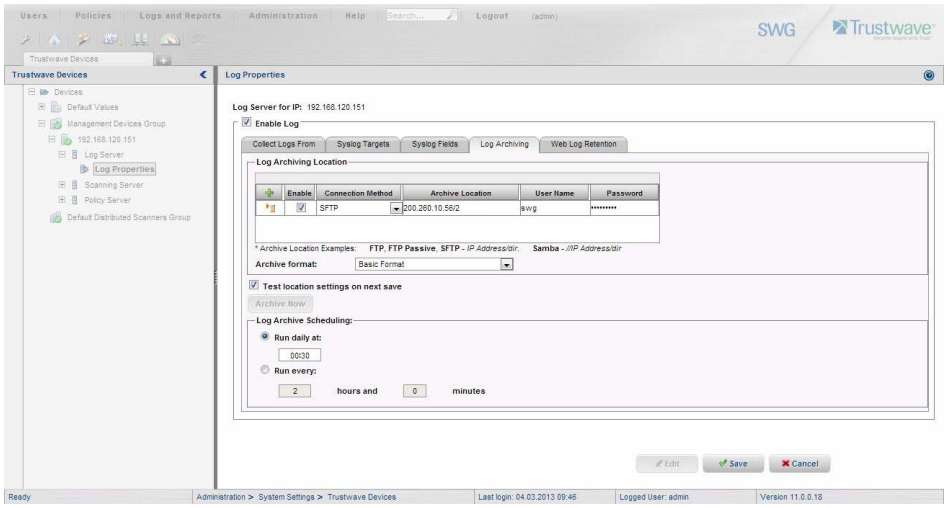
Setup instructions differ depending on the SWG software version to be used with the SR (10.0 or 9.2.5).

4.6.2.1 SWG Configuration for Software Version 10.0 or above

4.6.2.1.1 Configure SWG to Send Logs to the SR

1. Access the SWG user interface (Management Console).
2. Navigate to Administration | System Settings | Trustwave Devices.
    - Depending on the SWG version this page could also be named M86 Devices or SWG Devices.
3. In the Devices tree, find the SWG's IP address and drill down to Log Server | Log Properties.

4. In the Log Properties panel, click the **Log Archiving** tab:



5. Click **Edit** to activate the elements in this tab.

6. In Log Archiving Location, click the '**+**' (plus character) in the table header to add a new row in the table, and specify the following criteria to the right of the check mark in the Enable column:

   - **Connection Method:** Select "SFTP" from the pull-down menu.
   - **Archive Location:** Type in the path information that you noted when setting up this SWG in the SR Device Registry. The Path will be the IP address of this SR, a slash character (/) and an integer. Do not include the leading //. For example: `200.260.10.56/2`.
   - **User Name**: Type in the SWG's Username from the Device Registry, which is `swg` (in lower case characters).
   - **Password**: Type in the password you entered for the SWG in the Device Registry.

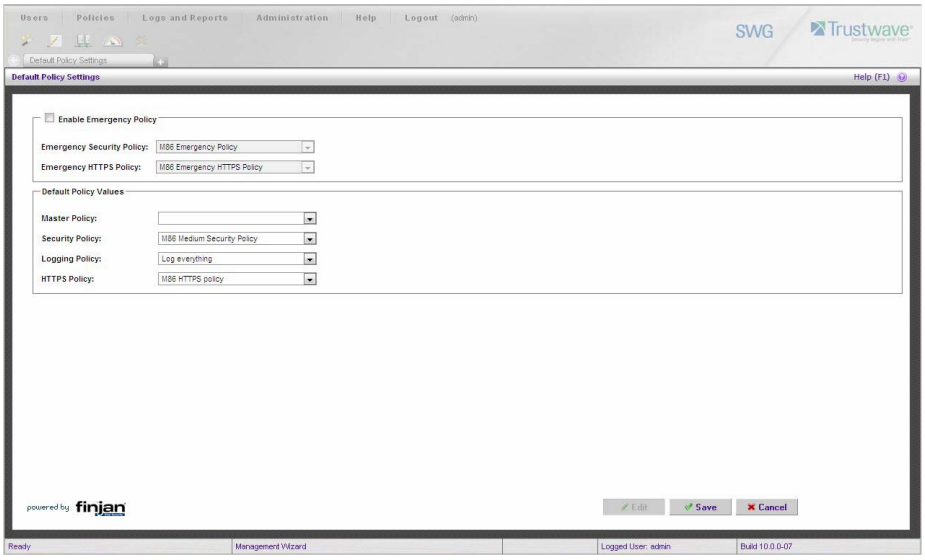
Note: Be sure "Extended Format" is selected for Archive format, and Log Archive Scheduling specifies the correct interval you wish to use for sending logs from the SWG to the SR.

7. Click **Save** to save your settings.

4.6.2.1.2 Policy Settings

1. Navigate to Policies | Default Policy Settings and verify if the settings in Enable Emergency Policy and Default Policy Values are the ones you wish to use for sending logs to the SR.

2. To modify any settings, click **Edit** to activate all elements in this panel:



3. Make your selections from the pull-down menu(s).
4. Click **Save** to save your edit(s).

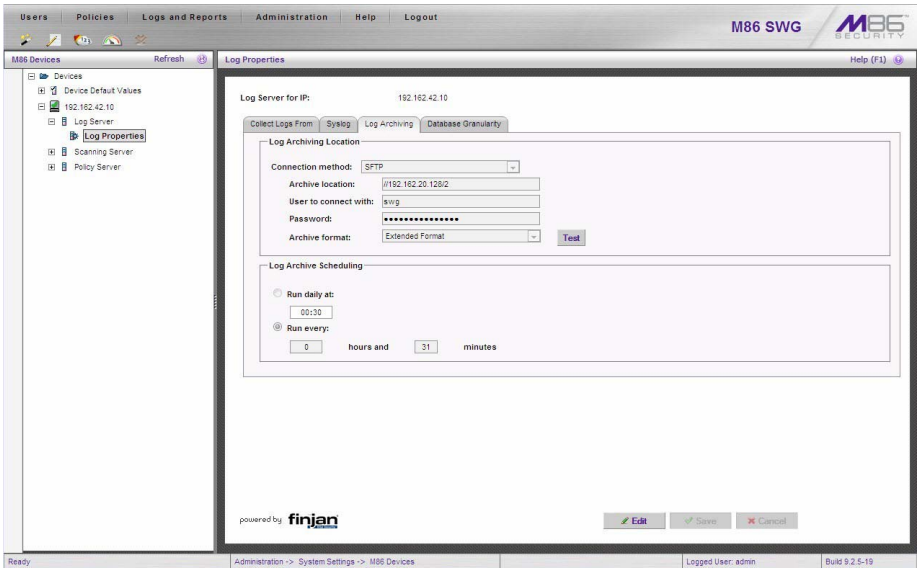
4.6.2.2 SWG Configuration for Software Version 9.2.5

Caution: This version of SWG has reached End of Life. You should upgrade to a newer version.

4.6.2.2.1 Configure SWG to Send Logs to the SR

1. Access the SWG user interface.
2. Navigate to Administration | System Settings | M86 Devices.
3. In the Devices tree, find the SWG's IP address and drill down to Log Server | Log Properties.

4. In the Log Properties panel, click the **Log Archiving** tab:



5. Click **Edit** to activate the elements in this tab.

6. In Log Archiving Location, be sure the following is specified:

   - **Connection Method**: “SFTP” is selected from the pull-down menu.
   - **Archive Location**: Type in the path information that you noted when setting up this SWG in the SR Device Registry. The Path will be a double backslash(//), the IP address of this SR, a slash character (/) and an integer. For example: `//200.260.10.56/2` for an SR with that IP address.
   - **Password**: The password you entered for the SWG in the Device Registry.
   - **Archive Format**: “Extended” is selected from the pull-down menu.

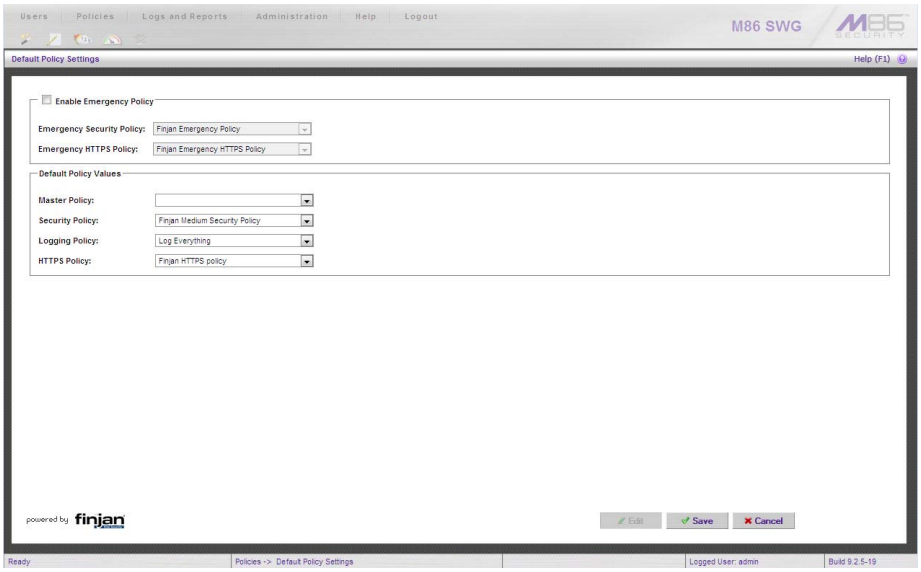
Note: Be sure Log Archive Scheduling specifies the correct interval you wish to use for sending logs from the SWG to the SR.

7. Click **Save** to save your settings.

4.6.2.2.2 Policy Settings

1. Navigate to Policies | Default Policy Settings and verify if the settings in Enable Emergency Policy and Default Policy Values are the ones you wish to use for sending logs to the SR.

2. To modify any settings, click **Edit** to activate all elements in this panel:



3. Make your selections from the pull-down menu(s).
4. Click **Save** to save your edit(s).

4.7 Single Sign-On Access, Default Username/Password

4.7.1 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

4.7.2 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

Application	Username	Password
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.

4.8 Next Steps

Congratulations; you have completed the SR installation procedures. Now that the SR server is set up on your network you will need to be sure the Web-access logging device you are using is sending log files to the SR database. Once the SR database is populated—this generally takes a full day—the Report Manager can be used for generating reports.

Initially, you will only be able to report on IP addresses. To implement user names in SR reports using a Web Filter, please consult the System Configuration Section of the Security Reporter User Guide. Refer to the Reports Section, Real Time Reports Section, and Security Reports Section of the Security Reporter User Guide for information on generating reports.

For real time and security reports, the next step is to set up user groups or administrator groups. For real time reports, you will set up and configure gauges thereafter.

Obtain the latest Security Reporter User Guide at http://www.trustwave.com/support/sr/documentation.asp .

Note: If you cannot view reports, or if your specific environment is not covered in the Security Reporter User Guide, contact a Trustwave solutions engineer or technical support representative..

Caution: If you cannot view reports, or if your specific environment is not covered in the Security Reporter User Guide, contact a Trustwave solutions engineer or technical support representative.

5 Best Reporting Practices

This Best Reporting Practices section is provided to help you get started using the Report Manager user interface. The main areas of focus in this section are productivity and security reporting, and real time reporting.

In the Productivity and Security Reports Usage Scenarios sub-section you will learn how to:

- access Summary Reports to obtain a high level snapshot of end user Internet activity
- use Drill Down Reports to conduct an investigation of specific Internet activity
- modify a report view
- generate a report view grouped by two sets of criteria
- generate a summary report view and a detail report view
- create a new report view
- export a report view to an output format
- save a report
- schedule a report to run on a regular basis to capture Internet activity at set intervals of time
- create a Custom Category Group
- generate a summary report and a detail report for a custom category group
- create a custom User Group
- generate a summary report and a detail report for a single user group

Note: The SR must collect data for a full day in order to generate Summary Reports. To use Drill Down Reports, the SR must collect data for a couple of hours. Therefore, it would be best to wait a day after the SR has been installed and fully operational before beginning any of the exercises described in the Productivity Reports Usage Scenarios sub-section.

- In the Real Time Reports Usage Scenarios sub-section you will learn how to:
- navigate panels to access tools for configuring the Report Manager
- drill down into a dashboard gauge to target sources of unusually high Internet activity
- create a gauge that will monitor a user group’s Internet activity
- set up an email alert for notification of potential Internet usage threats on the network

5.1 Productivity and Security Reports Usage Scenarios

This collection of productivity and security reporting scenarios is designed to help you use the Report Manager to create typical snapshots of end user Internet activity. Each scenario is followed by setup information. Please consult the “How to” section in the index of the Security Reporter User Guide for pages

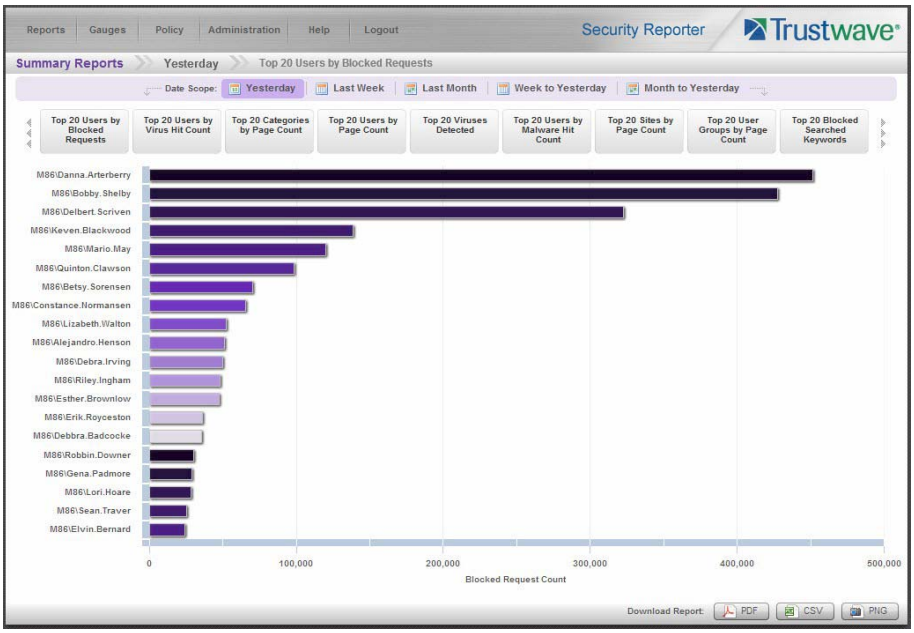
containing detailed, step-by-step instructions on configuring and/or using the tools and features described in that scenario.

5.1.1 Summary Report and Drill Down Report exercise

In this exercise you will learn how to use Summary Reports to obtain a high level overview of end user activity, and then use Drill Down Reports to obtain more detailed information on specific user activity. You will also learn that there are two basic types of Drill Down Reports (summary and detail), and various types of reports you can generate for each of these two basic drill down report types.

5.1.1.1 Use Summary Reports for a high level activity overview

From the navigation menu, select Reports | Summary to display yesterday's "Top 20 Users by Blocked Requests" Summary Report containing pre-generated data. Since the data has already been captured from the previous day, the report loads quickly in your browser:



In the dashboard that displays near the top of the panel, you can click any thumbnail to view the related Summary Report. For example, the Top 20 Categories by Page Count report shows the categories that were most frequently visited by users yesterday.

Note: Click the left or right arrow in the dashboard to view additional thumbnails.

In the Security Reporter *Administrator Guide* index, see:

- How to: generate a Summary Report

5.1.1.2 Further investigate using a Summary Drill Down Report

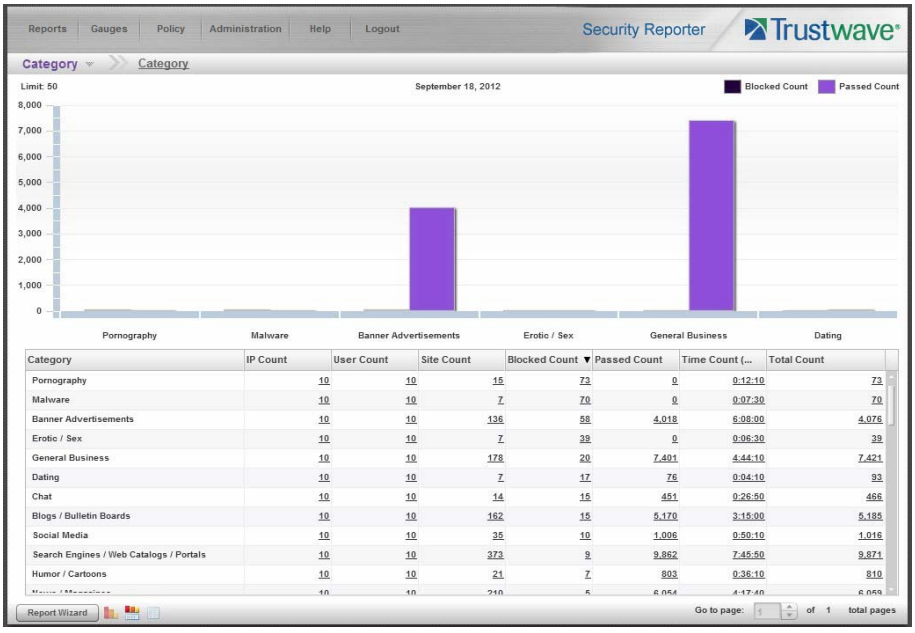
Now you will use a Drill Down Report to find out which user(s) are visiting sites in the category you've targeted for investigation.

From the navigation menu, go to Reports | Drill Down | Category to display the generated Summary Drill Down Report view, ranking categories in order by the most blocked requests.

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 a link to the Report Wizard, used for modifying the current report view, downloading, emailing, saving, and/or re-running the report:



Note that the drill down report view has been generated for today's activity by default.

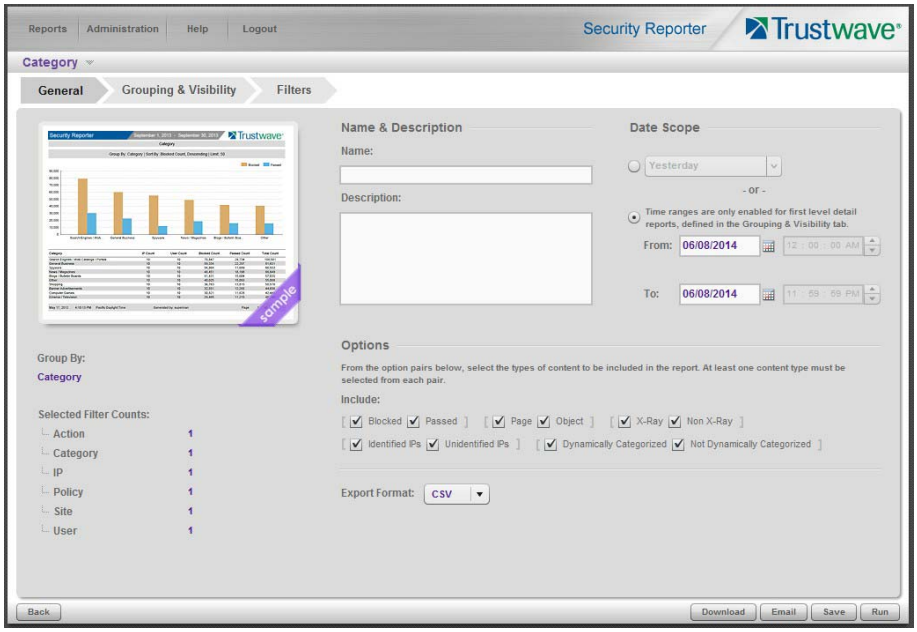
To continue this investigation using data from yesterday's Summary Report, you must create a new report from this current report view by first changing the date scope.

In the Security Reporter *Administrator Guide* index, see:

- How to: generate a Drill Down Report

5.1.1.3 Create a new report using yesterday's date scope

1. At the bottom left of the Summary Drill Down Report view, click **Report Wizard** to open the Report Wizard for the Category type of report:



   The Report Wizard is comprised of three tabs used for specifying reporting criteria: General, Grouping & Visibility, and Filters. The bottom right of the panel includes the Download, Email, Save, and Run buttons.

   For this exercise, we will only use the default General tab.

2. By default, "Today" is selected as the **Date Scope**. Choose "Yesterday" from this menu.

3. Click **Run** to accept your selection. The regenerated Category report now displays yesterday's data in the Summary Drill Down Report view.

In the Security Reporter *Administrator Guide* index, see:

- How to: create a new report from the current report view

5.1.1.4 Create a report grouped by two report types

1. To continue this exercise, select the record for the category you wish to further investigate.

Note: If necessary, scroll down to view the entire list of categories in the report view.

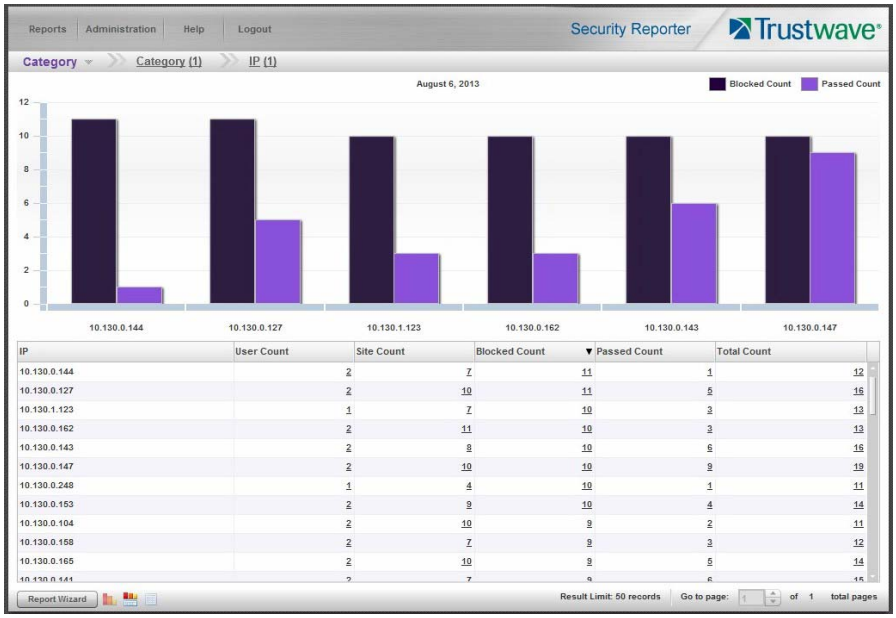
2. Now, to find out who is visiting sites in this category, you will need to identify the user(s).

   Since there are two sets of criteria you need for this exercise, you must drill down into the selected category and also specify that you wish to view user IP addresses, thereby creating a report view grouped by two report types.

Note the Count columns to the right of the Category column, each with clickable links.

Note: The Bandwidth column displays with GB or MB statistics if using a SWG only with this SR.

Click the **IP Count** link corresponding to the targeted category:



After executing the last command, note that user IP addresses now display in the first column of the report view instead of categories.

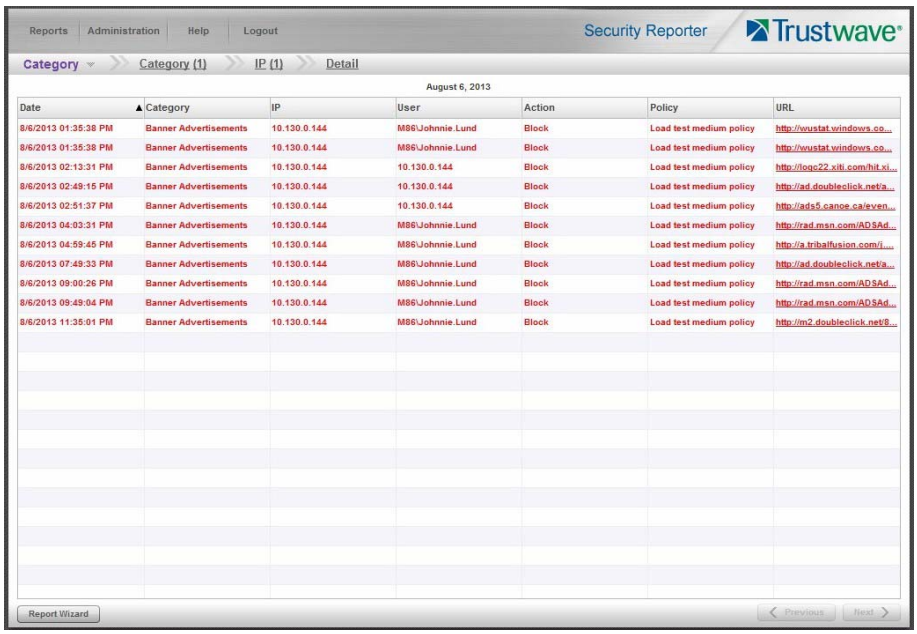
In the Security Reporter *Administrator Guide* index, see:

- How to: use count columns and links

For the last step of this exercise, you will select a user from the current Summary Drill Down Report view and then drill down further to see which URLs that user visited, thereby creating a Detail Drill Down Report view.

5.1.1.5 Create a Detail Drill Down Report to obtain a list of URLs

1. To investigate the activity of a specific user listed in the current Summary Drill Down Report view, select that user's record and then click the hyperlink in the Blocked Count, Passed Count, or Total Count column to show results in the Detail Drill Down Report view that now displays:



   Note that the Detail Drill Down Report view contains columns of information pertaining to the user's machine and setup on the network, sites visited, categorized URLs, and clickable links to access pages the user viewed. Records for blocked user requests display in red text.

2. In this report view, click any URL link to open the page for that URL.

In the Security Reporter *Administrator Guide* index, see:

- How to: create a detail Blocked Count report from a summary report

You have now learned how to access Summary Reports and to use Drill Down Reports to conduct an investigation. You have also learned how to change the date scope of a Drill Down Report to create a new report, generate a report view grouped by two report types, and drill down into the current summary report view to create a detail report view.

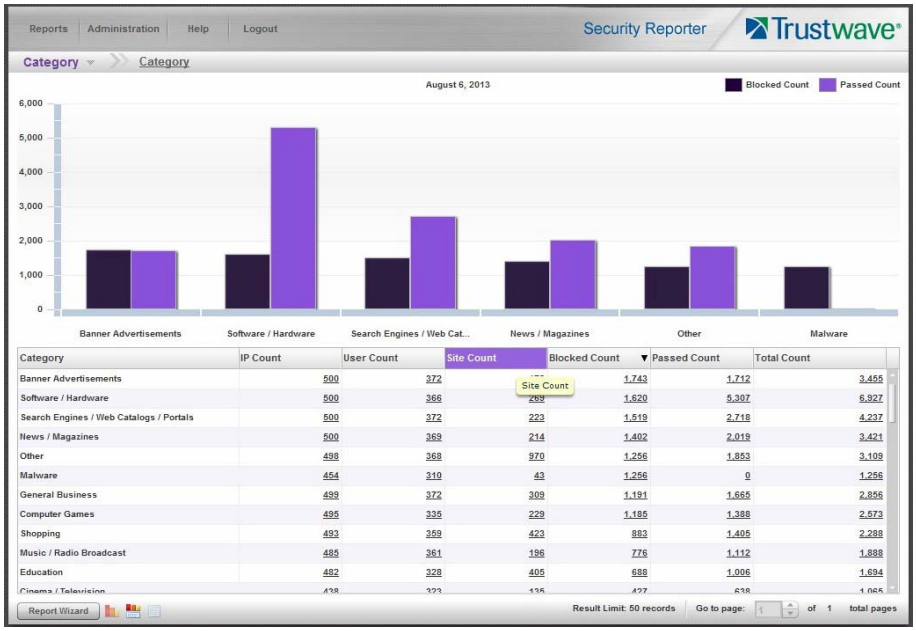
These tools and other tools can be used separately or combined to create many different types of reports to fulfill different purposes.

5.1.2 'Group By' Report and Export Report exercise

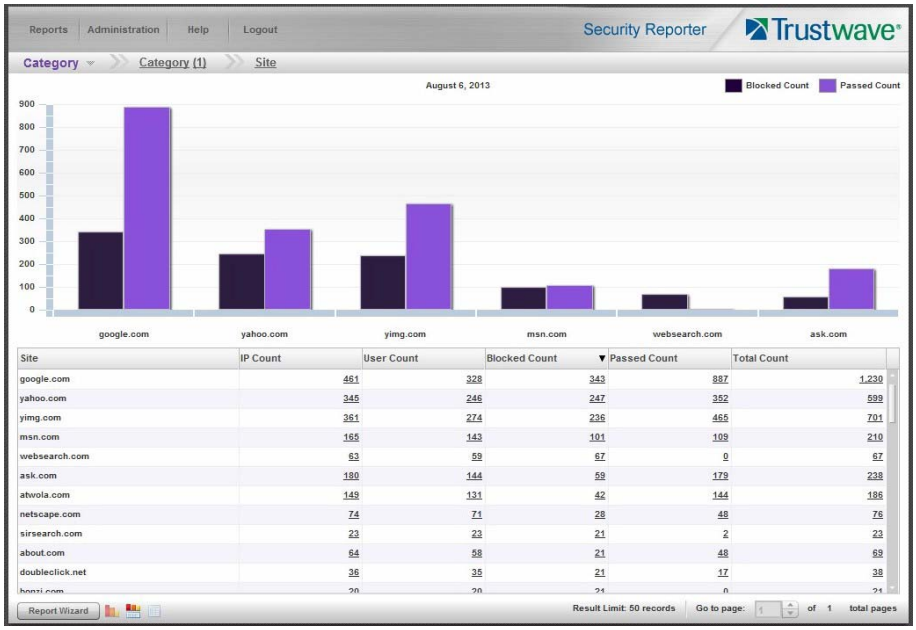
In this exercise you will learn how to display only the top 10 records of a summary drill down 'group by' report view, export that report view in the PDF output format, and then view the results of the generated PDF file.

5.1.2.1 Drill down to view the most blocked sites in a category

1. From the top panel, go to Reports | Drill Down | Category to generate a Summary Drill Down Report view, ranking categories in order by the most blocked to the least blocked:



2. To find out which sites were blocked in a category, target the category and then click the **Site Count** link corresponding to that category to create a report view grouped by two report types:



Note that URLs/IP addresses of blocked sites in the category now display in the first column of the modified report view, instead of category names.

In the Security Reporter *Administrator Guide* index, see:

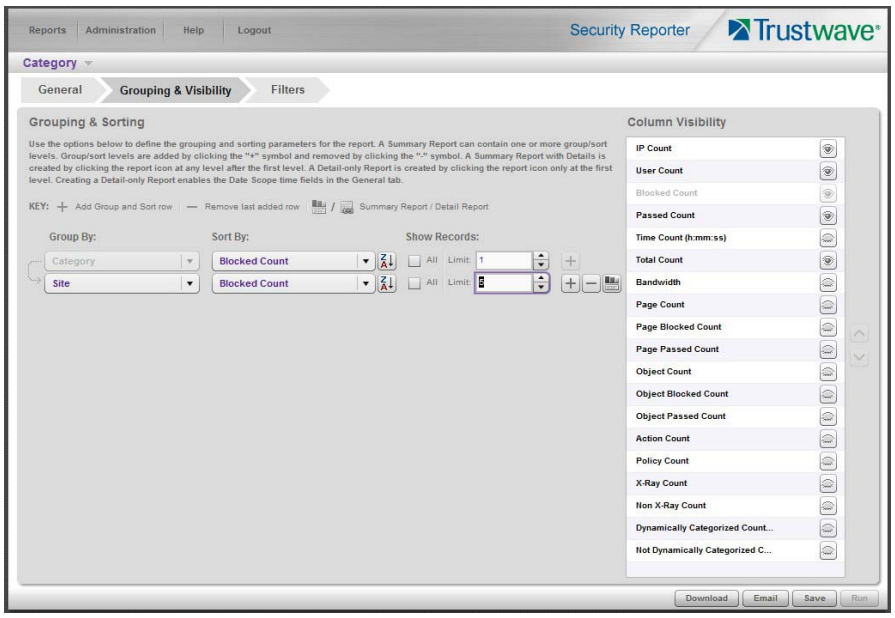
- How to: generate a Drill Down Report
- How to: use count columns and links

5.1.2.2 Export a report for the top five site records

1. Now, to only display the top five blocked sites in the top category, navigate to **Report Wizard.**
2. On the General tab, choose an **Export format** of “PDF”.

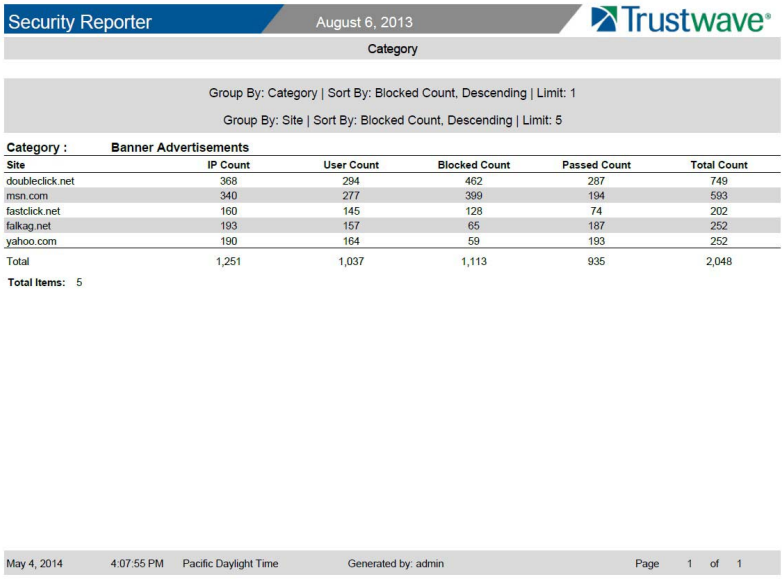
Note: The default export format is CSV because production reports with large amounts of data are most efficiently generated in this format.

3. Click the Grouping & Visibility tab:



4. In the Group & Sort by section, for **Show Records**, type in `1` for the record Limit.
5. Click the “+” symbol to add the next level to the report, and select **Group by** “Site”.
6. Under **Show Records**, type in a Limit of `5` records.

7. Click **Download** to begin the exportation process using the PDF export format. When the exportation process has been completed, the PDF file opens in a separate browser window:



Security Reporter August 6, 2013 Trustwave

Category

Group By: Category | Sort By: Blocked Count, Descending | Limit: 1

Group By: Site | Sort By: Blocked Count, Descending | Limit: 5

Category : **Banner Advertisements**

Site	IP Count	User Count	Blocked Count	Passed Count	Total Count
doubleclick.net	368	294	462	287	749
msn.com	340	277	399	194	593
fastclick.net	160	145	128	74	202
falkag.net	193	157	65	187	252
yahoo.com	190	164	59	193	252
Total	1,251	1,037	1,113	935	2,048

Total Items: 5

May 4, 2014 4:07:55 PM Pacific Daylight Time Generated by: admin Page 1 of 1

The generated PDF file for the report includes a list of the top 5 Sites records for the selected category, as well as the following counts for each record in the report: IP Count, User Count, Blocked Count, Passed Count, and Total Count. The Total and Total items display at the end of the report.

In the Security Reporter *Administrator Guide* index, see:

- How to: display only a specified number of records
- How to: export a report
- How to: print or save an exported report

You have now learned how to modify a Summary Drill Down Report view grouped by two report types to include only the top 5 records, and then export that content for viewing in the PDF format.

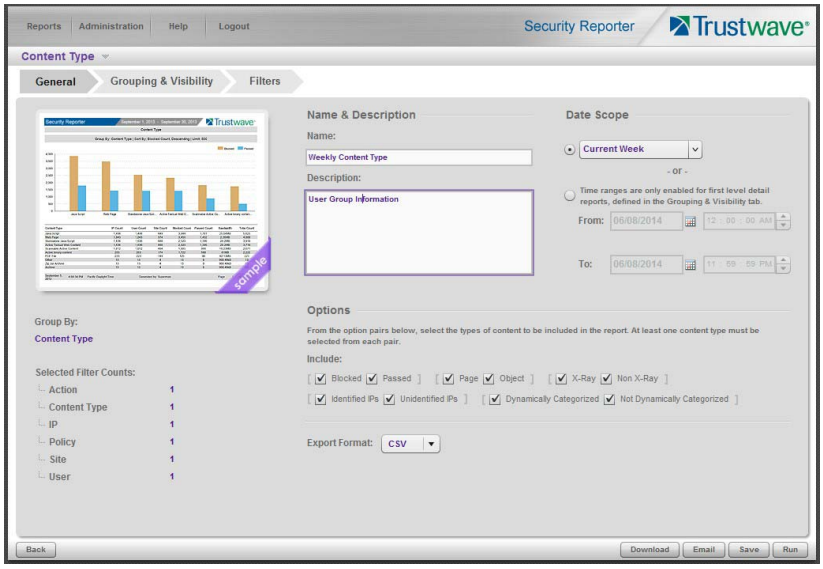
Variations of this exercise can be performed to generate and export countless reports using criteria of your specifications.

5.1.3 Save and schedule a report exercise

In this exercise you will learn how to save report view criteria, and then create a schedule for running a report on a regular basis using that criteria. While a Summary Drill Down Report is used in this exercise, these steps also apply to a Detail Drill Down Report.

5.1.3.1 Save a report

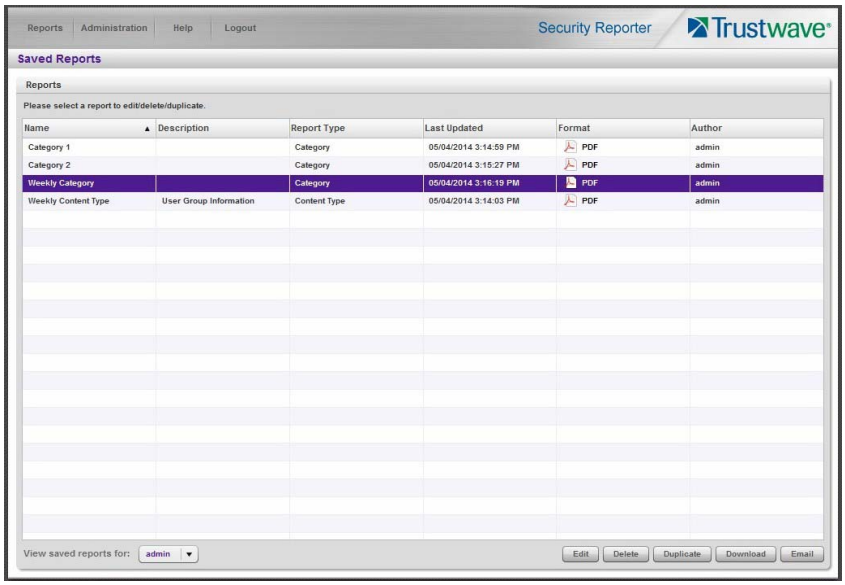
1. To use specific criteria for a report you wish to run again, navigate to Report Wizard and configure settings in the tabs:



In order to save the report settings, you must at least enter a **Name** for the report in the General tab.

2. Click **Save** at the bottom of the panel to save the report.

Note: Saved reports can be edited at any time. These reports are accessed by going to Reports | Saved, and then choosing the report from the **Reports list**:



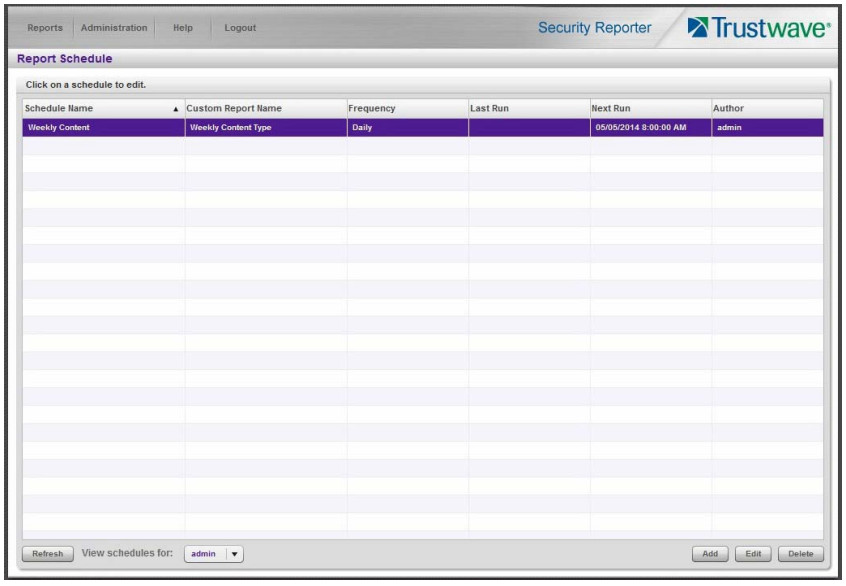
In the Security Reporter *Administrator Guide* index, see:

- How to: save a Drill Down report
- How to: edit a saved Drill Down report

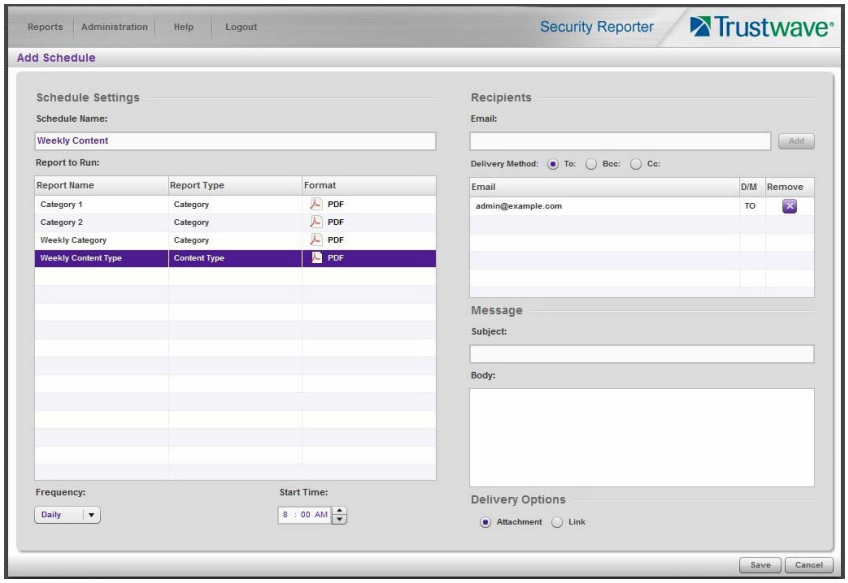
5.1.3.2 Schedule a recurring time for the report to run

Now that you've saved the report, you can schedule a time for the report to run.

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

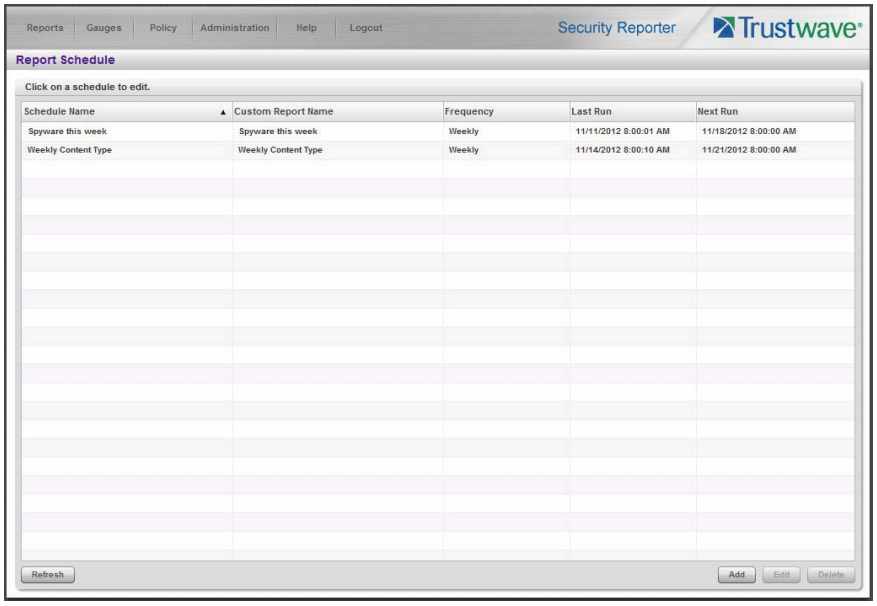


2. Click **Add** to go to the Add Schedule panel:



3. Enter a **Schedule Name**, select the **Report to Run**, and specify the run **Frequency** (Daily, Weekly, Monthly, Once) and pertinent criteria.

4. Click **Save** to save your settings and add the schedule to the Report Schedule panel list.



In the Security Reporter *Administrator Guide* index, see:

- How to: schedule a Drill Down report to run

You have now learned how to save a report and schedule the report to run at a designated time.

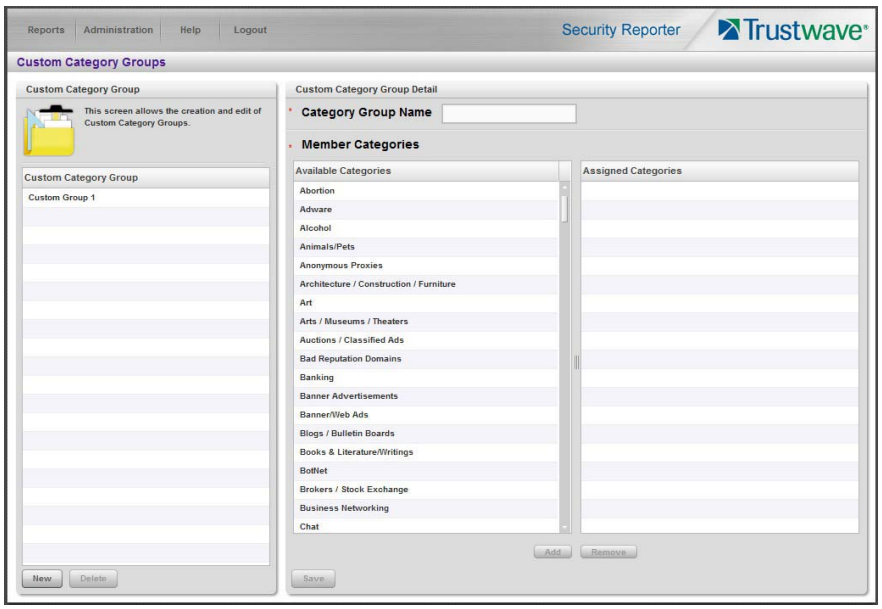
Reports created for a variety of purposes can be scheduled to run on different dates and times to capture records of specified user activity as necessary.

5.1.4 Create a Custom Category Group and generate reports

After you've run a few summary and detail reports for the top visited categories, you might want to generate reports targeting specified categories only. To do so, you must first create a Custom Category Group.

5.1.4.1 Create a Custom Category Group

1. To create a Custom Category Group, choose Administration | Custom Category Groups from the navigation menu:



2. Type in the **Category Group Name** to be used.
3. Specify whether the **Service Type** for reporting is "URL" or "Bandwidth"; if "Bandwidth" is selected, this action affects the Member Categories section below:
   - For a URL Service Type: Choose the Available Categories and click **Add** to include each category in the Assigned Categories list box.
   - For a Bandwidth Service Type: Specify the Port Number(s) and click **Add Port** to include each port in the Assigned Ports list box.
4. Click **Save** to save your settings and to display the name of the group you added in the Custom Category Group list box.

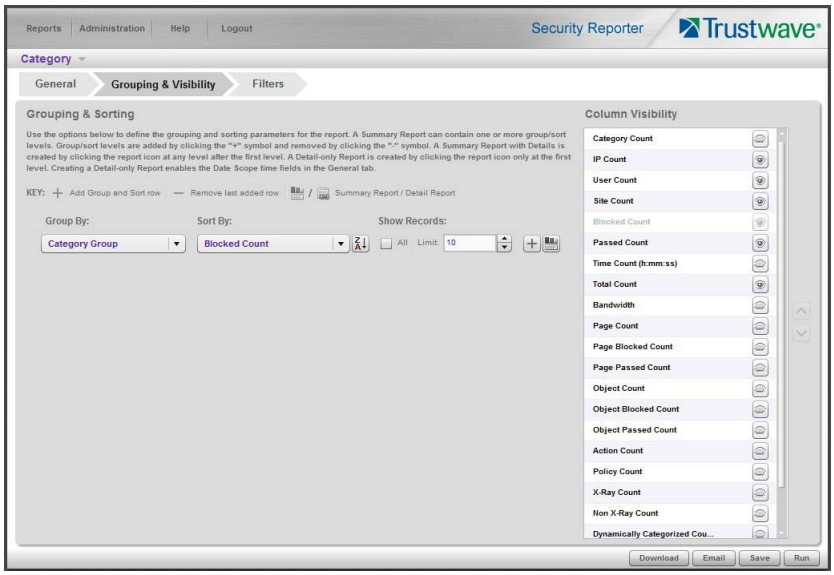
In the Security Reporter *Administrator Guide* index, see:

- How to: add a Custom Category Group

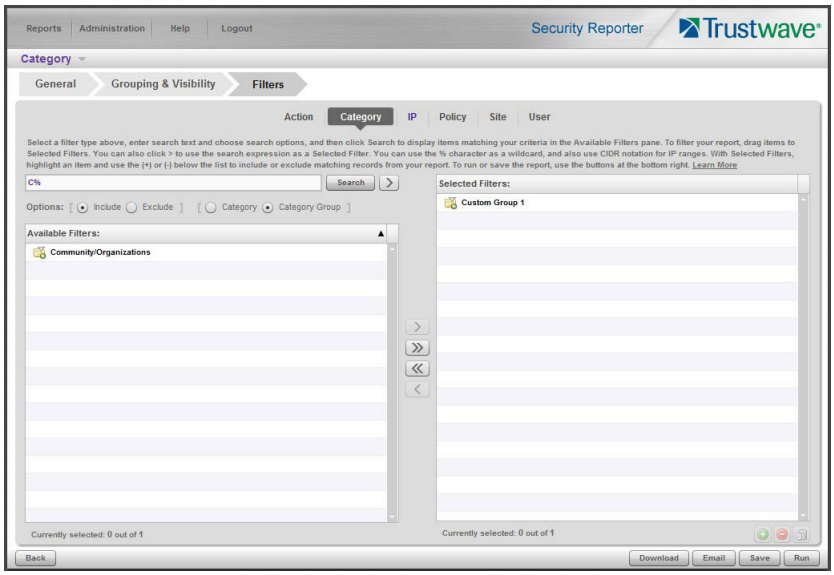
5.1.4.2 Run a report for a specified Custom Category Group

1. To create a report for the Custom Category Group you created, choose Reports | Drill Down | Report Wizard from the navigation menu.

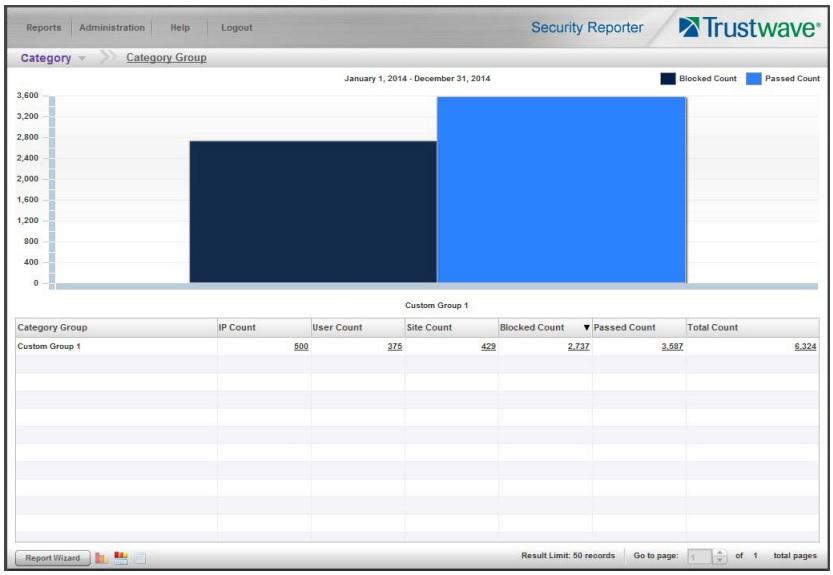
2. Specify reporting criteria in the General tab.
3. In the Grouping & Visibility tab, specify the report will **Group By** “Category Group”:



4. In the Filters tab, select the Category Group filter and search for the custom category group you created:



5. After adding the custom category to the Selected Filters list box, click **Run** to begin generating the report view. The finished report view displays in the Drill Down report panel:



In the Security Reporter *Administrator Guide* index, see:

- How to: generate a Custom Category Group report

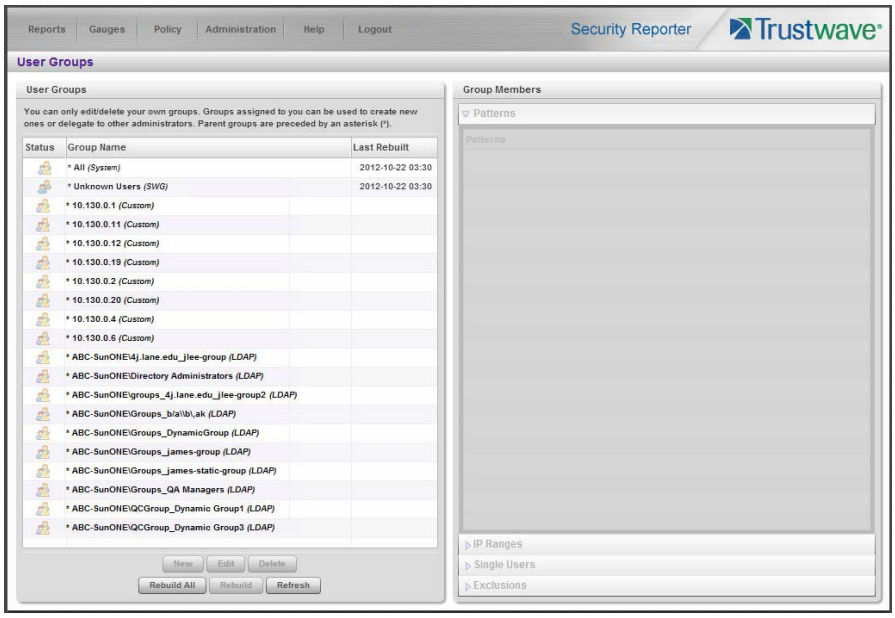
5.1.5 Create a custom User Group and generate reports

In addition to running reports for various custom category groups, you might want to create one or more custom user groups and run reports for these user groups.

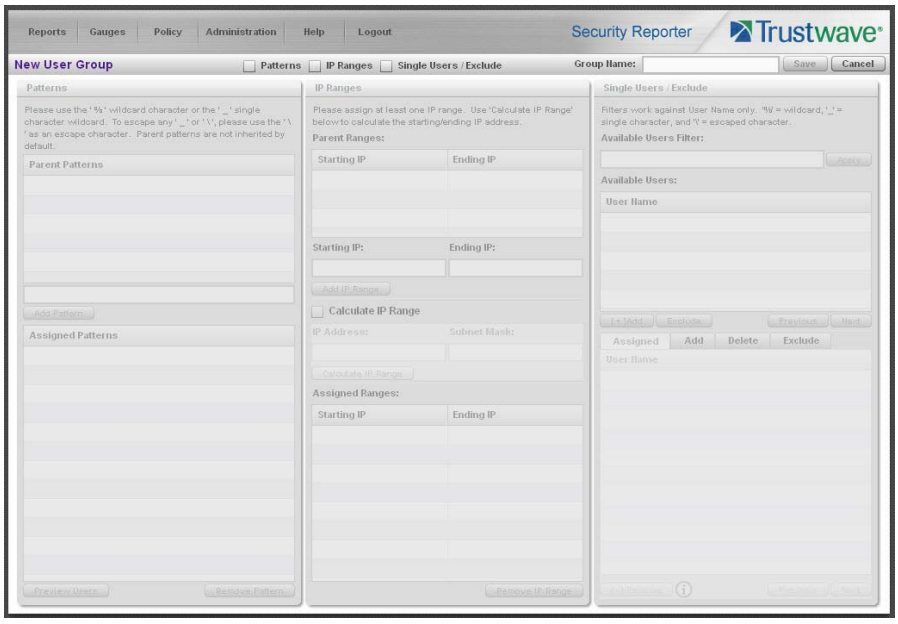
Note: In order to generate reports for a custom user group, the user group must be created a day in advance, since the list of users is updated each day automatically based on group definitions and latest usage data.

5.1.5.1 Create a custom User Group

1. To create a user group, navigate to Administration | User Groups:



2. Choose an existing user group from the User Groups list and then click **New** to display the New User Groups panel:



3. Type in the **Group Name** and check the box(es) corresponding to “Patterns”, “IP Ranges”, and/or “Single Users/Exclude” to activate the section(s) below. For this example, select “IP Ranges”.

4. Specify criteria for the group. In this example, enter an IP address within the range of the parent group.

5. Click **Save** to save your settings and to return to the User Groups panel. Note the group you added now displays in the User Groups list.

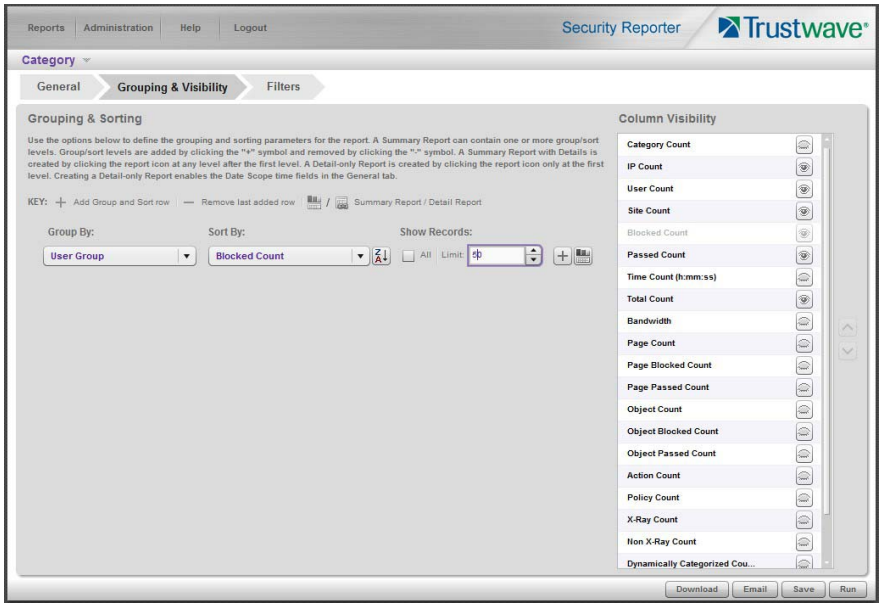
In the Security Reporter *Administrator Guide* index, see:

- How to: add a user group

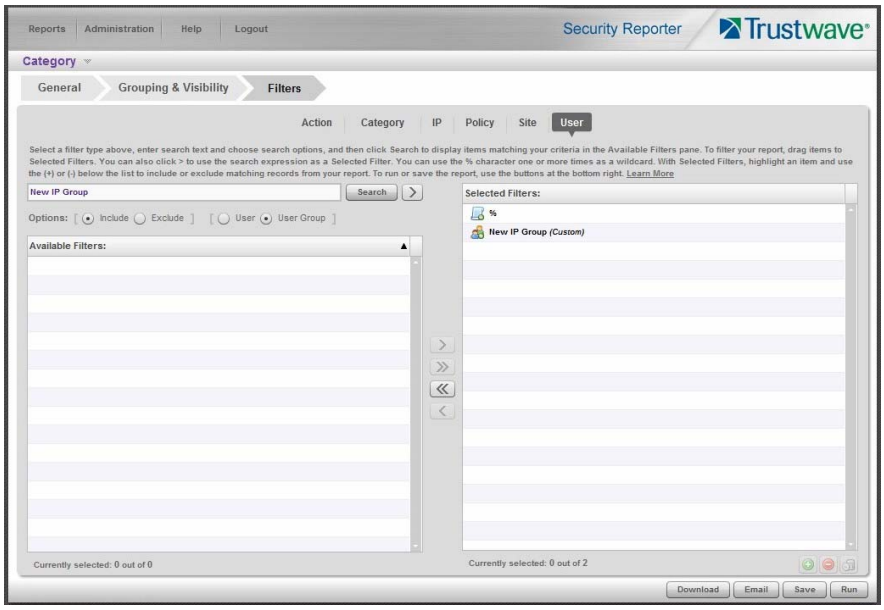
5.1.5.2 Generate a report for a custom User Group

Once the custom User Group is recognized by the SR (on the following day), reports can be generated.

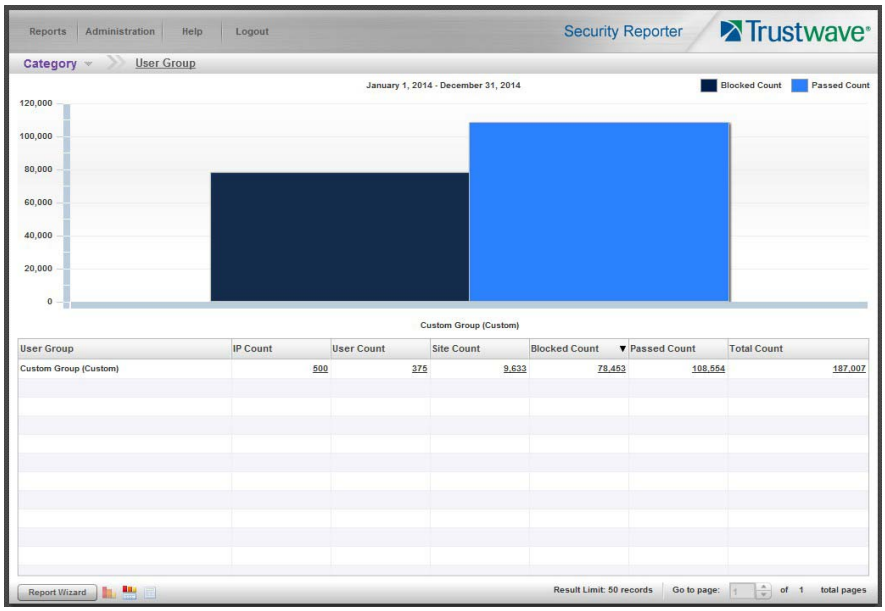
1. To generate a summary or detail report for a custom User Group, navigate to Reports | Drill Down | Report Wizard, and click the Grouping & Visibility tab.
2. Choose “User Group” from the menu:



3. In the Filters tab, select User, and choose the User Group option. Search for the user group you created, and then add it in the Selected Filters list box:



4. Click **Run** to begin generating the report view. The finished report view displays in the Drill Down report panel:



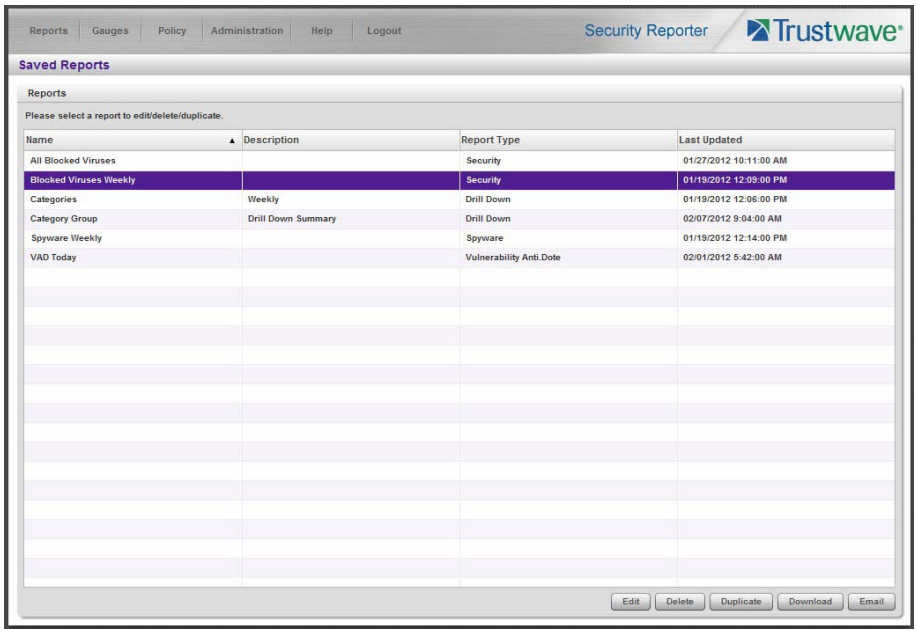
In the Security Reporter *Administrator Guide* index, see:

- How to: use the Report Wizard to generate a User Group report

5.1.5.3 Access the Saved Reports panel

A saved Drill Down report can be edited any time as follows:

1. Navigate to Reports | Saved.
2. Select the report name from the list:



3. Click **Edit** to go to the Report Wizard panel where the report can be updated and saved.

In the Security Reporter *Administrator Guide* index, see:

- How to: access saved Drill Down reports

5.2 Real Time Reports Usage Scenarios

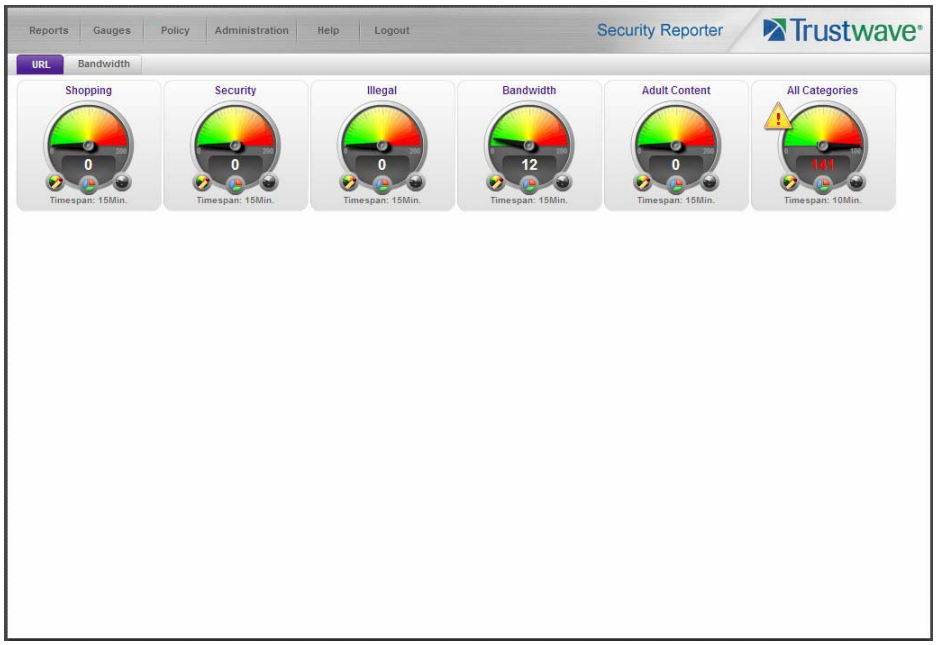
This collection of setup and usage scenarios is designed to help you understand and use basic tools in the console for enforcing your Internet usage policy. Each scenario is followed by console setup information. Please consult the “How to” section in the index of the Security Reporter User Guide for pages containing detailed, step-by-step instructions on configuring and/or using the tools and features described in that scenario.

5.2.1 Screen navigation exercise

This exercise will familiarize you with the four sections of the user interface and inform you where to go to customize the application to perform a specified task or function.

5.2.1.1 Navigate panels in the Gauges section

The URL Gauges Dashboard displays by default when you select Gauges in the navigation toolbar:



Each URL gauge contains a number that represents its current score. This score is derived by activity within that gauge, based on the activities of end users who visited URLs listed in library categories that comprise the gauge.

To view bandwidth gauge activity, click the Bandwidth tab above the URL gauges dashboard to display the bandwidth gauges dashboard. The score for each bandwidth gauge represents the number of bytes of end user bandwidth traffic in ports or protocols that comprise the gauge.

Click any of the topic links from the Gauges menu to display panels used for viewing/configuring URL/bandwidth gauges and/or gauge activity:

- **Dashboard** - view current gauge activity
- **Overall Ranking** - view details about current gauge activity for all end users affecting gauges
- **Lockouts** - prevent the end user from accessing specified URLs, the Internet, or the entire network
- **Add/Edit Gauges** - create and maintain gauges used for monitoring end users' Internet activity
- **Dashboard Settings** - customize the view to only show certain gauges

5.2.1.2 Navigate panels in the Policy section

Click the Policy link to display its menu. Click any of the menu topics to display panels used for establishing policies for high threat level threshold management:

- **Alert Logs** - view a list of alert records for the most recent 24-hour time period

- **Alerts** - manage alerts that indicate if gauges are close to—or have reached—their established upper thresholds

In the Security Reporter *Administrator Guide* index, see:

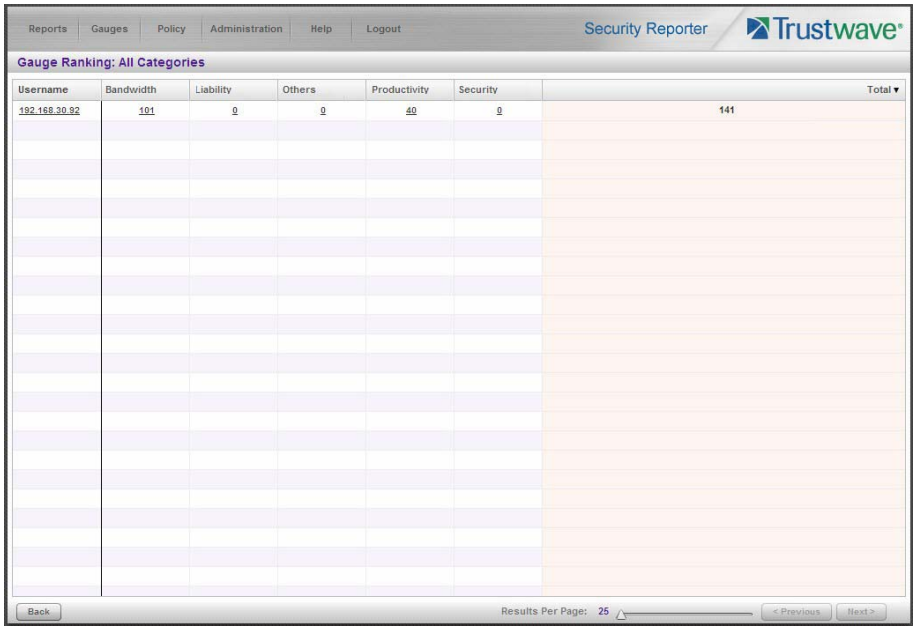
- How to: use Gauges and Policy menu selections

5.2.2 Drill down into a gauge exercise

This exercise will teach you how to drill down into a URL gauge to conduct an investigation on abnormally high Internet activity in a particular filtering category, in order to find out which individuals are driving that gauge's score, and which URLs they are visiting.

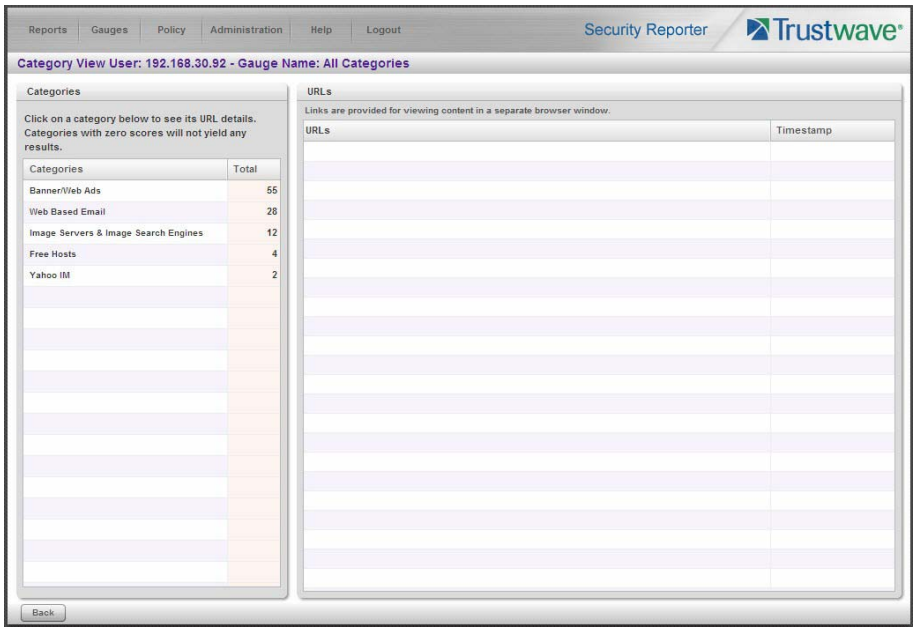
5.2.2.1 Select the gauge with the highest score

1. In the URL dashboard, select the gauge with the highest score and click it to open the Gauge Ranking table showing columns with names of library categories that comprise the gauge, and rows of end user records with activity in one or more of these library categories:



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

2. Find the library category with the highest score, and click that score to open the Category View User panel:



Note the left side of this panel is populated with rows of records for Categories affected by the selected end user.

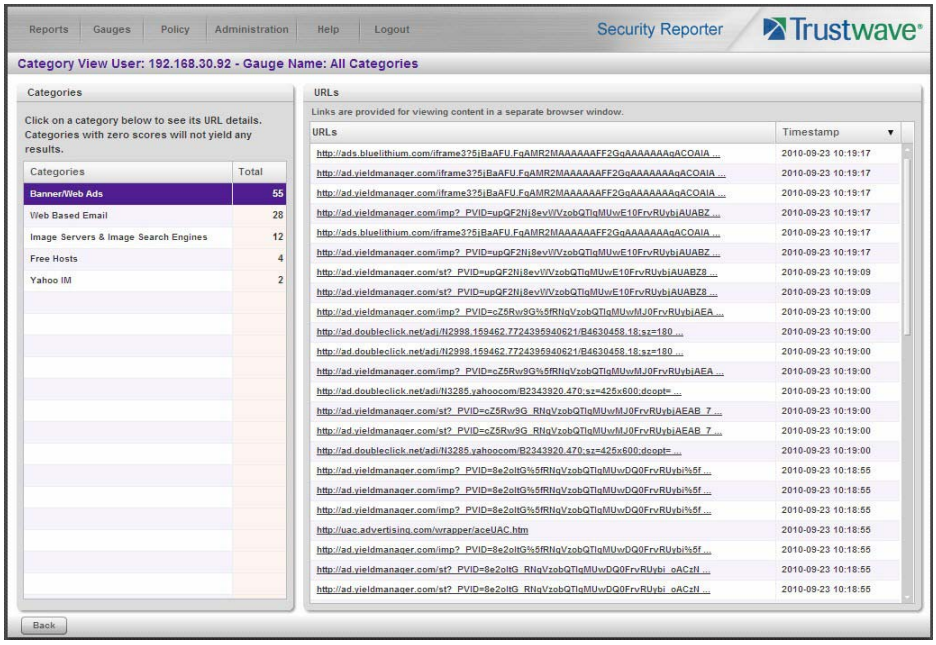
Now that you've identified the user affecting the highest scoring gauge, next you will investigate the activity of the user driving that gauge's score.

In the Security Reporter *Administrator Guide* index, see:

- How to: drill down into a gauge

5.2.2.2 Investigate a user's activity in a specified gauge

1. To find out which URLs the top end user visited in the high-scoring library category, select the category with the highest score and then click it to display a list of URLs the user visited in the right side of this panel:



2. Choose a URL you wish to view, and then click it to open a separate browser window accessing that URL.

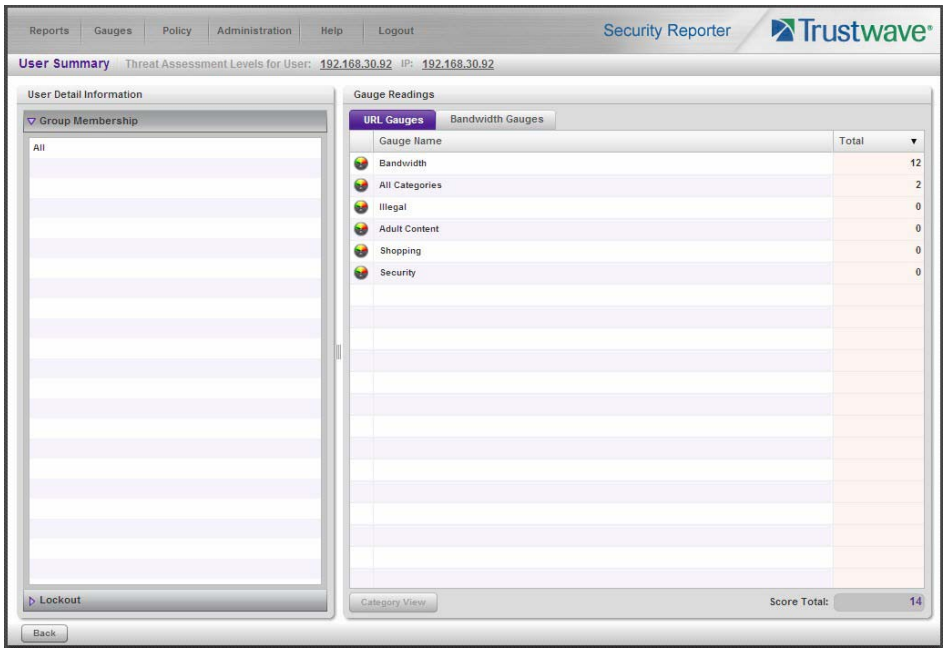
   After investigating one or more URLs in the list, you may wish to find out which other gauges that same user is currently affecting.

In the Security Reporter *Administrator Guide* index, see:

- How to: view URLs a user visited

5.2.2.3 Investigate the user's Internet activity in other gauges

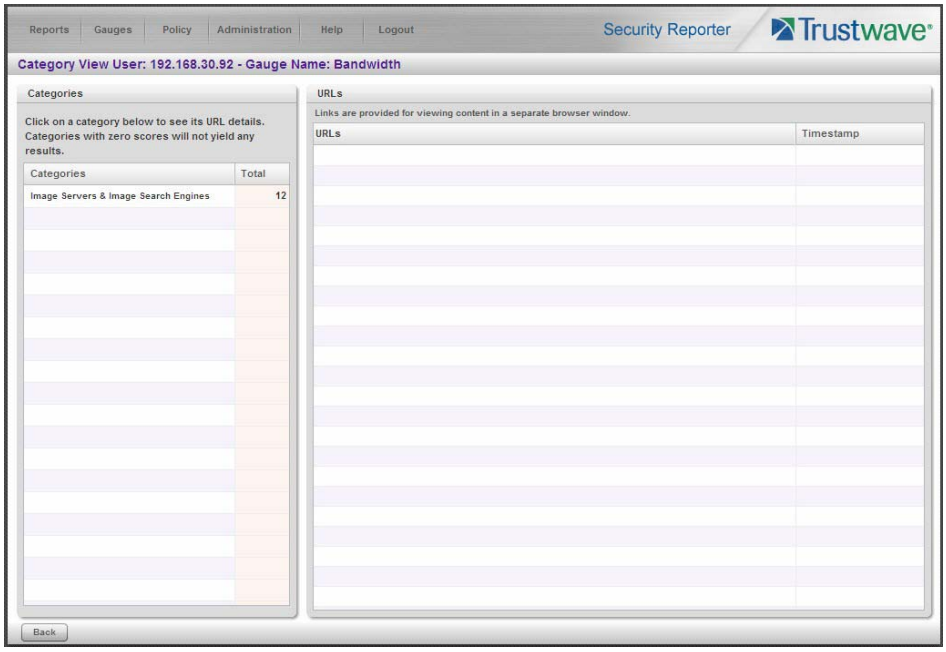
1. To find out which other gauges the same user is currently affecting, return to the Gauge Ranking table by going to the lower left corner of the Category View User panel and clicking the **Back** button. In the Username column, click that user's link to display the User Summary panel for that user:



   Note Gauge Readings to the right with the Total score for each Gauge Name listed.

2. Select a Gauge Name to investigate, which activates the Category View button below.

3. Click **Category View** to display the Category View User panel:



4. To find out which URLs the user is viewing in a particular library category, choose the category from the list, and then click the URL in the URLs list.

In the Security Reporter *Administrator Guide* index, see:

- How to: view end user gauge activity

You have just learned how to drill down into a gauge to conduct an investigation on identifying the source of unusually high Internet activity. The steps in this exercise demonstrated how to investigate gauge scores in order to find out which end users are driving the score in one or more gauges, and how to view URLs visited by the user.

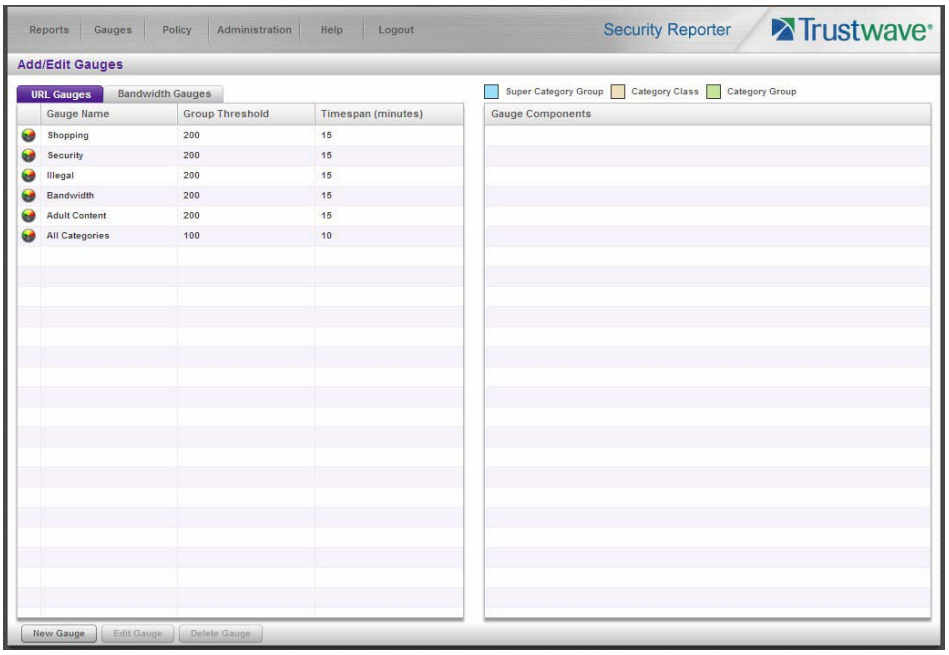
When you become accustomed to using the gauges on a regular basis to conduct these types of investigations, you will eventually want to explore other tools in the interface to restrict or lock out offending users from accessing certain library categories.

5.2.3 Create a gauge exercise

This exercise will teach you how to create a URL gauge to be used for monitoring a user group's Internet activity in specified filtering categories.

5.2.3.1 Access the Add/Edit Gauges panel

From the Gauges menu, select Add/Edit Gauges to open the Add/Edit Gauges panel:



Note that this panel contains the current Gauge Name list at the left side.

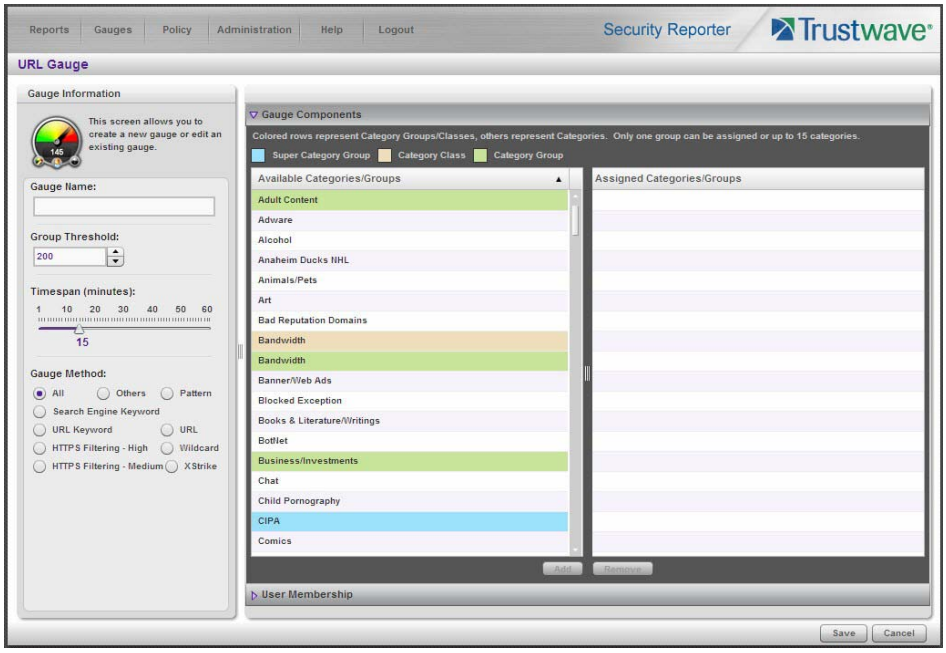
Next, you will specify that you wish to create a new gauge.

In the Security Reporter *Administrator Guide* index, see:

- How to: access the Add/Edit Gauges panel

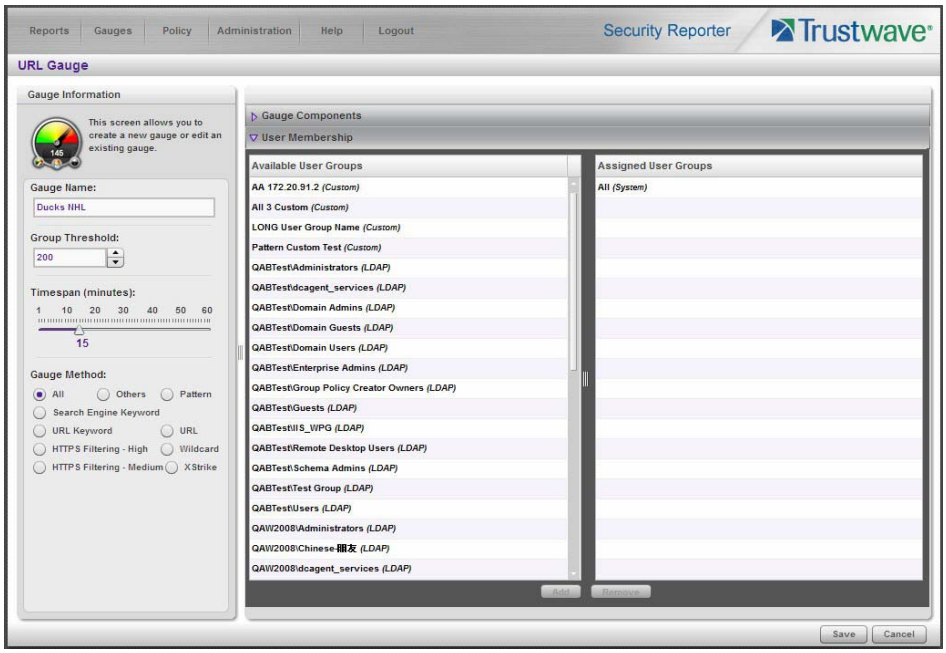
5.2.3.2 Add a URL Gauge

1. Click **New Gauge** at the bottom left of the panel to open the URL Gauge panel:



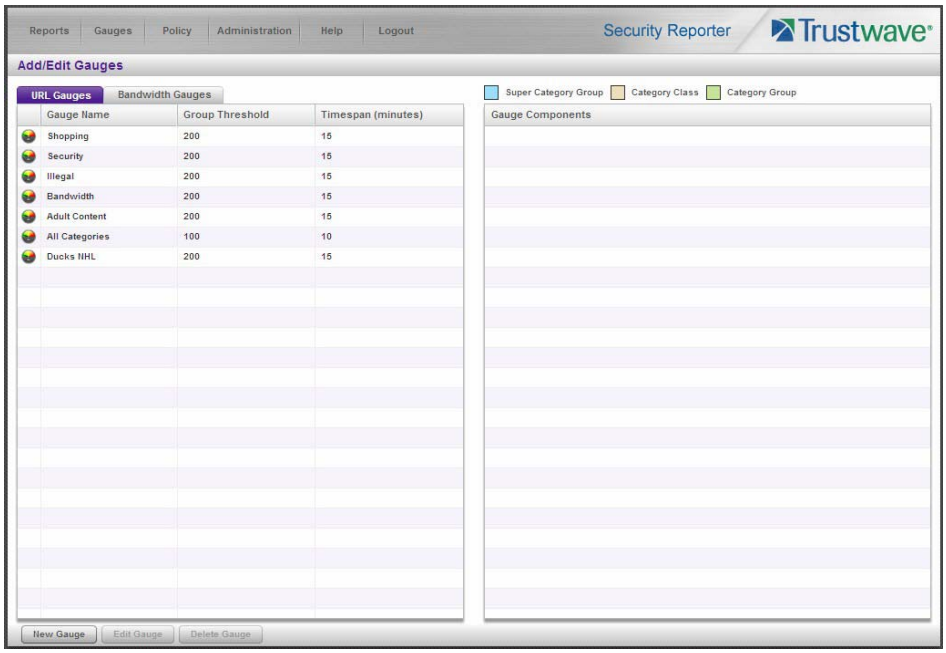
2. In Gauge Information to the left, specify the following information as necessary:
   a. **Gauge Name** you wish to use and display for this gauge; this entry must be at least two characters in length.
   b. **Group Threshold** for the ceiling of gauge activity. For this exercise we will use the default and recommended value, which is 200 for a URL gauge.
   c. **Timespan (minutes)** for tracking gauge activity (1 - 60 minutes). For this exercise we will use the default and recommended value, which is 15 minutes.
   d. **Gauge Method** to be used for tracking gauge activity. For this exercise we will use the default “All” gauge method, so you do not need to make any selection from the drop-down menu. The selected “All” method considers all methods users can use to access URLs in library categories included in the gauge.
3. In the Available Categories/Groups list to the right, select one Category Class/Group, or up to 15 library categories by clicking each one while pressing the **Ctrl** key on your keyboard. When you have made your selection(s) for the gauge to monitor, click the **Add** button to move the choice(s) to the Assigned Categories/Groups list box.

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



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

7. After adding user groups, click **Save** at the bottom right of the panel to return to the Add/Edit Gauges panel that now includes the name of the gauge you just added:



In the Security Reporter *Administrator Guide* index, see:

- How to: add new a gauge

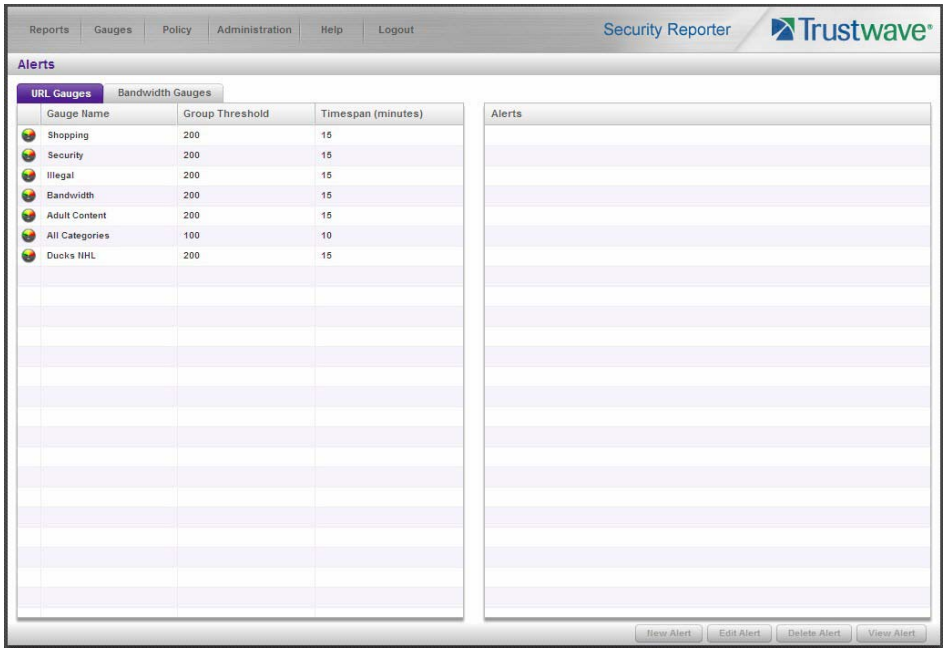
Now that you know the basics of creating a gauge, you will soon be able to create and use gauges to monitor various groups of users who frequent URLs in library categories you wish to restrict, and deal in real time with Internet usage issues that endanger your network and/or consume an excessive amount of bandwidth resources.

5.2.4 Create an email alert exercise

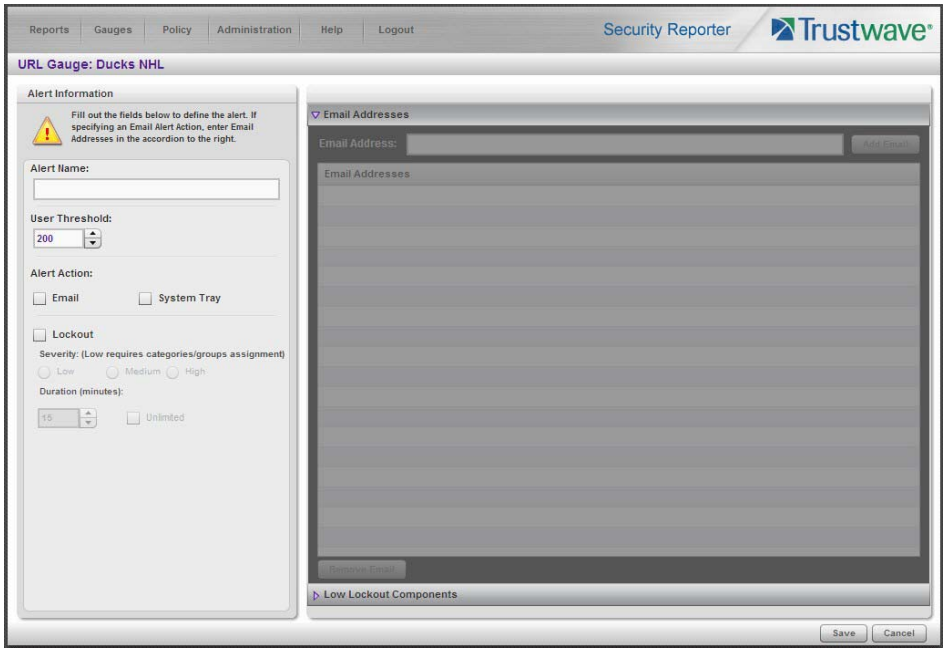
This exercise will teach you how to set up an email alert so you will be notified when a gauge reaches the high end of its established threshold.

5.2.4.1 Add a new alert

1. From the Policy menu, select Alerts to open the Alerts panel:



2. Select the gauge for which an alert will be created; this action activates the New Alert button.
3. Click **New Alert** to open a panel that displays Alert Information to the left and the greyed-out target panel to the right containing the Email Addresses and Low Lockout Components accordions:



4. Type in the **Alert Name** to be used for the alert that will be delivered to the group administrator.

5. Specify the **User Threshold** ceiling of gauge activity that will trigger the alert. The default and recommended value is 200 for a URL gauge.
6. Specify the **Alert Action** method(s) to be used for alert notifications:
   - **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.

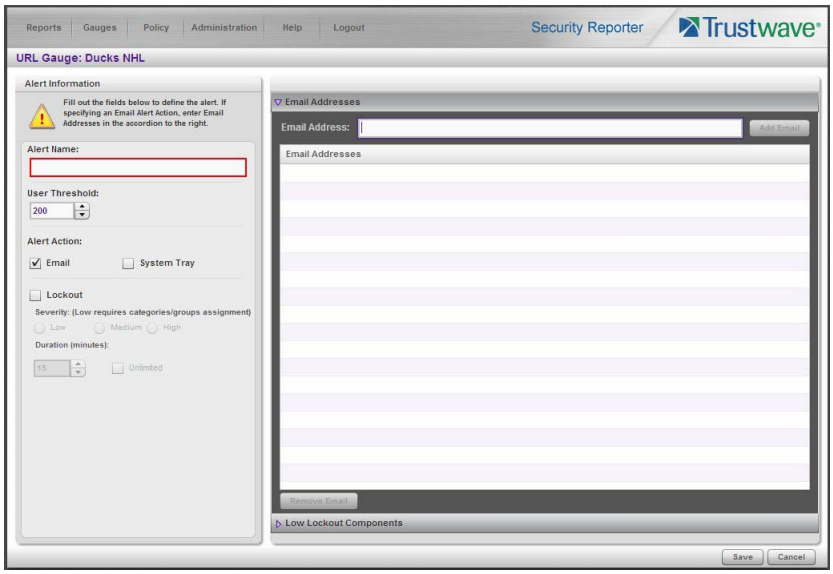
   For this exercise, however, you will only want to select Email, as described in the next step.

In the Security Reporter *Administrator Guide* index, see:

- How to: add a new alert

5.2.4.2 Select Email Alert Action

1. In the Alert Action section, choose the "Email" alert notification option.



   Note that this action opens and activates the Email Addresses accordion at the right side of the panel.
2. In the **Email Address** field, type in the email address to which the alert will be sent, and then click **Add Email** to include the email address in the list box above.
3. Click **Save** at the bottom right of the panel to save your entries and to display the Alerts panel.

   Next you will learn what to expect when an email alert is sent to your mailbox.

In the Security Reporter *Administrator Guide* index, see:

- How to: set up email alert notifications

5.2.4.3 Receiving an email alert

When an end user's activity in a gauge reaches the threshold limit established for an alert, it triggers an alert notification. If the email alert option was selected, an email is sent to the email address that was specified.

The email alert identifies the end user who triggered the alert, and includes a list of URLs the user visited, along with the date and time each URL was accessed. Clicking any of the URLs in the email opens a browser window containing the contents of that URL.

In the Security Reporter *Administrator Guide* index, see:

- How to: view an email alert

Now that you know how to create an email alert for a gauge, you will quickly identify users who are misusing their Internet access privileges, giving you knowledge about policy violations in real time so you can immediately take action to protect your resources.

6 Using the SR in the Evaluation Mode

Evaluation mode pertains to the state of an SR in which a maximum of three weeks of data is available to view on the server.

When evaluating the SR in evaluation mode, the Report Manager user interface and Expiration screen from the System Configuration administrator console display differently than they do in registered (standard) mode.

Note: See the System Configuration Section and Report Manager Administration Section of the Security Reporter User Guide for information about using panels/screens in registered mode.

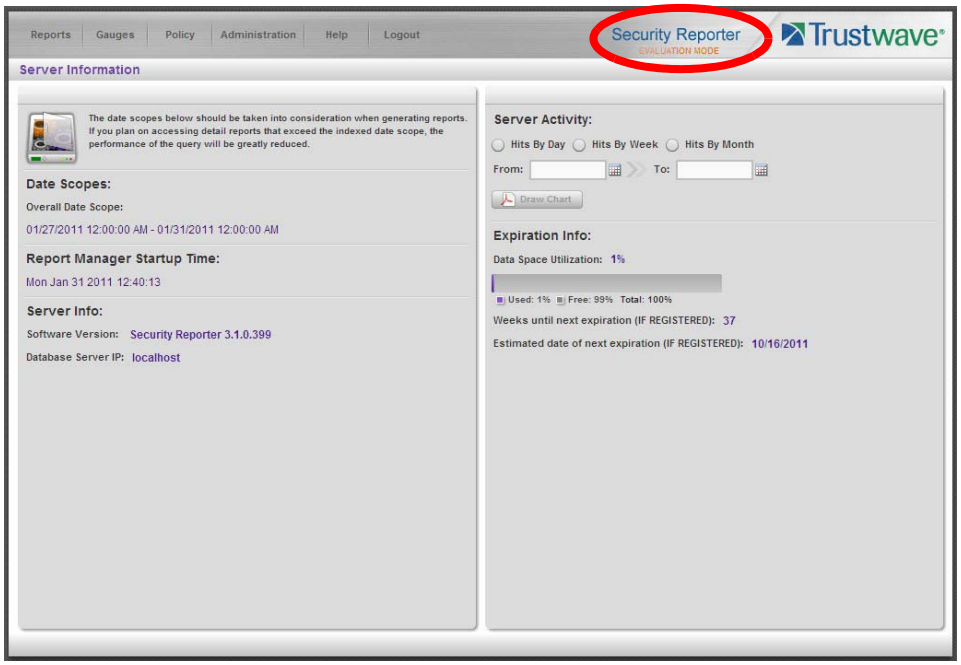
6.1 Report Manager

In evaluation mode, the Report Manager banner displays ‘EVALUATION MODE’ beneath the Security Reporter name/link as shown in the sample panel below.

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 (see more about the pop-up box on the next page).

6.1.1 Server Information Panel

Information about the server’s status can be viewed in the Server Information panel (shown below). The Expiration Info section at the bottom right of the panel displays the amount of data space allocated to the SR and used by the SR, as well as data expiration criteria calculated for this SR, if activated in registered mode.

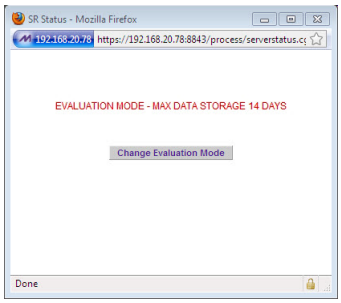


6.2 System Configuration

Note: See Appendix C: Evaluation Mode in the Security Reporter User Guide for information about changing the SR's mode from evaluation to registered.

6.2.1 Evaluation Mode Pop-Up

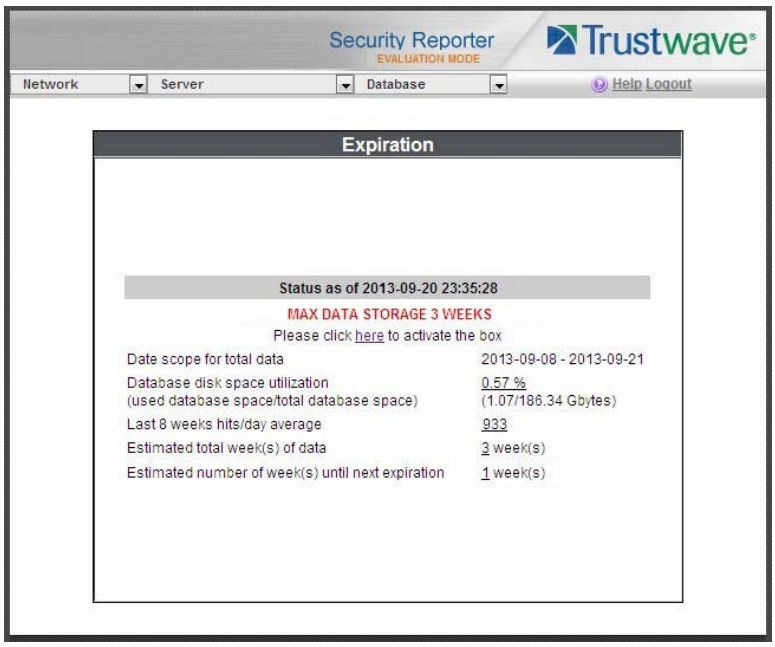
In evaluation mode, the SR Status pop-up box opens when accessing the System Configuration administrator console:



Until the SR is in registered mode, this pop-up box will continue to open whenever accessing the System Status screen of the System Configuration administrator console.

6.2.2 Expiration screen

In evaluation mode, the Expiration screen includes the following message beneath the Status bar: "EVALUATION – MAX DATA STORAGE 'X' WEEKS" (in which 'X' represents the maximum number of weeks available to view in the SR's data storage scope).



Appendices

Appendix A: Bandwidth Monitoring

A.1 Initial Setup on the ESXi Server

1. Plug in a network cable from the switch used for Bandwidth monitoring to an empty NIC on the ESXi server.
2. On the ESXi server, open the vSphere client and select the host machine.
3. Select the Configuration tab and choose **Add Networking...** to open the Add Network Wizard window. For each step, do the following:
   a. Connection Type: Select “Virtual Machine”, then click **Next >**.
   b. Network Access: Select “Create a virtual switch”—the virtual NIC should be automatically selected—then click **Next >**.
   c. Connection Settings: Enter the **Network Label**, then click **Next >**.
   d. Summary: Review the settings, then click **Finish** to close the Wizard window.
4. In the Configuration tab, choose **Properties...** for the Virtual Switch that will monitor Bandwidth traffic; this action opens the vSwitch Properties window. Do the following:
   a. In the Ports tab, select **vSwitch**, then click **Edit...** to open the second vSwitch Properties window.
   b. Select the Security tab, then set the **Promiscuous Mode** to “Accept”, and then click **OK** to close the Properties window.
5. Click **Close** to close the first vSwitch Properties window.

A.2 Steps to Set Up the VM to Use Bandwidth Monitoring

1. Open the vSphere client, then Login to the ESXi server.
2. Select the Virtual Machine to use for Bandwidth monitoring.
3. Select the Summary tab, then choose **Edit Settings** to open the Virtual Machine Properties window.
4. In the Hardware tab, select “Network adapter 2”.
5. In the Network Connection frame, for **Network Label** choose the network that was created for Bandwidth monitoring.
6. Click **OK** to close the Virtual Machine Properties window.

Appendix B: Optional Ethernet Tap Installation

This appendix pertains to the optional installation of the Ethernet Tap unit for bandwidth monitoring.

Note: In order to monitor bandwidth on the SR, both inbound and outbound traffic must be sent to the SR through use of a port span, tap, or other similar device.

B.1 Preliminary Setup Procedures

The instructions in this section pertain to the use of a NetOptics 10/100BaseT Tap that can be purchased from Trustwave.

B.2 Unpack the Ethernet Tap Unit from the Box

Open the NetOptics Ethernet Tap box and verify that all accessories are included. Save all packing materials in the event that the unit needs to be returned to Trustwave.

The NetOptics box should contain the following items:

- 1 NetOptics 10/100BaseT Tap
- 2 power supply units
- 2 AC power cords
- 2 crossover cables
- 2 straight through cables
- 1 installation guide

B.3 Other Required Installation Items

In addition to the contents of the NetOptics box, you will need the following item to install the Ethernet Tap unit:

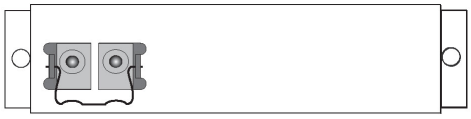
- 1 standard CAT-5E cable

Inspect the box for damage. If the contents appear damaged, file a damage claim with the carrier immediately.

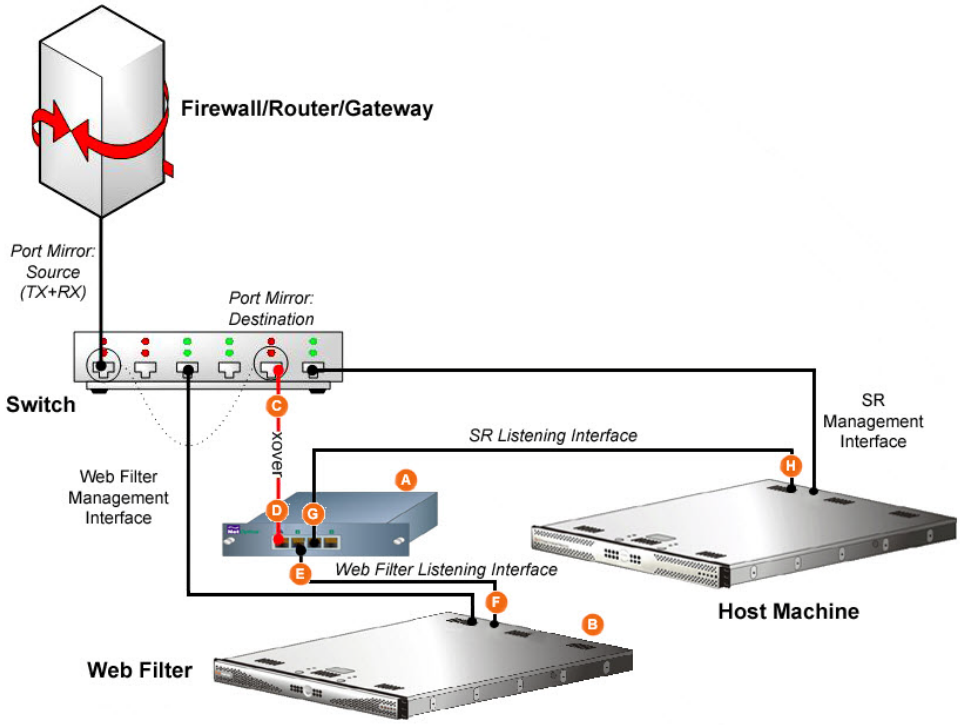
B.4 Install the Ethernet Tap Unit

The procedures outlined in this step require the use of a CAT-5E cable.

1. Provide power to the Ethernet Tap by connecting both power cords from the unit to the power source.



2. If a designated source Web Filter (to be used with the Security Reporter) is already installed on the network, disconnect the cable that connects this Web Filter to the switch.

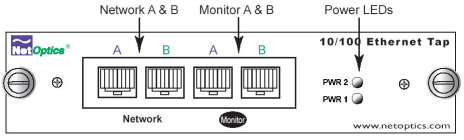


   If the designated Web Filter has not yet been installed, disregard this sub-step and proceed to the next step.

3. Using a crossover cable, connect one end to the Switch's port configured to be the destination port of the Port Mirror.

   If adding the host machine to an existing installation, this port would be the port that was originally occupied by the listening interface of the Web Filter.

4. Connect the other end of the crossover cable to the Ethernet Tap's Network A port.



5. Using a straight through cable, connect one end to the Ethernet Tap's Network B port.
6. Connect the other end of the straight through cable to the listening interface of the Web Filter.
7. Using the second straight through cable, connect one end to the Ethernet Tap's Monitor A port.
8. Connect the other end of the second straight through cable to the host machine's listening interface.

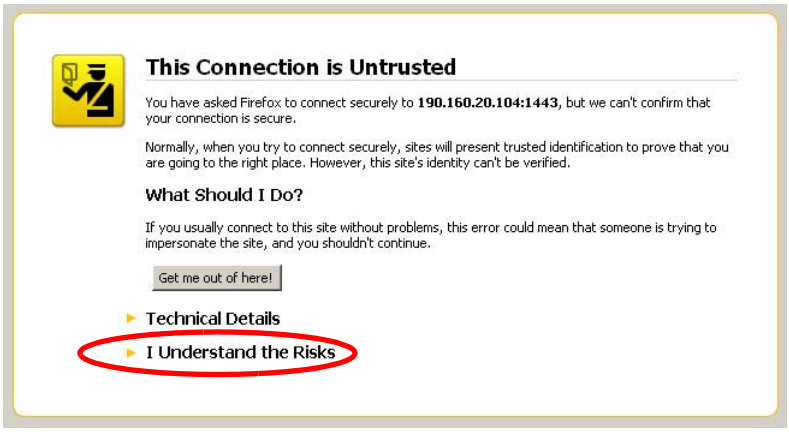
After completing the steps in this Appendix, continue with SR configuration.

Appendix C: Accepting Security Certificates

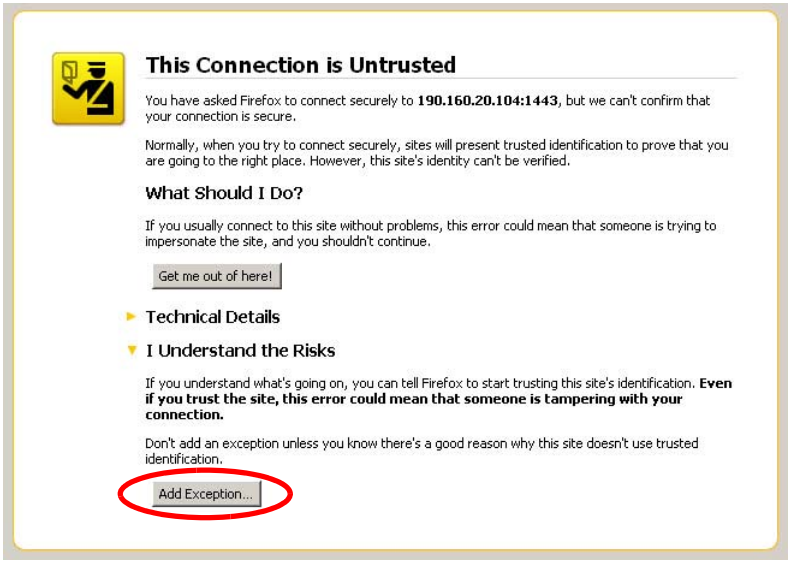
When you connect to the SR, you may need to accept a security certificate exception. This is a normal behavior for the certificate used by this product. This appendix provides detailed walk-throughs of the procedure in several supported web browsers.

C.1 Accept the Security Certificate in Firefox

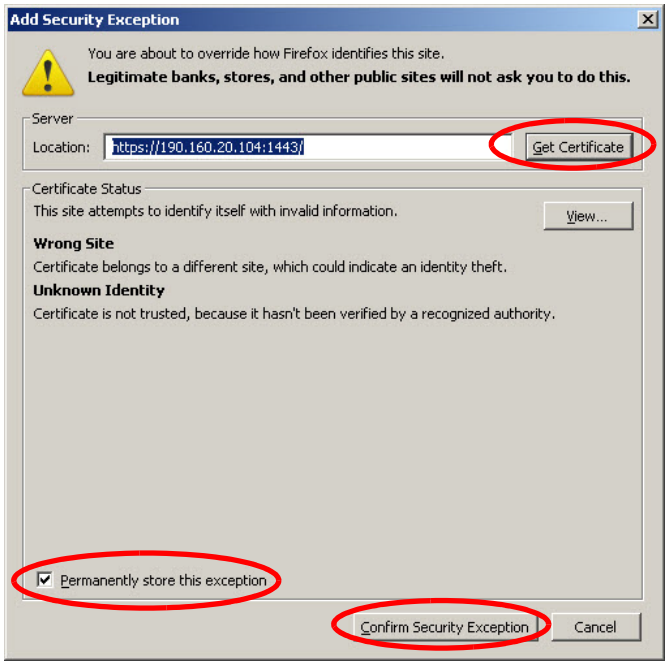
1. If using a Firefox browser, in the page "This Connection is Untrusted," click the option **I Understand the Risks**:



2. In the next set of instructions that display, click **Add Exception...**:

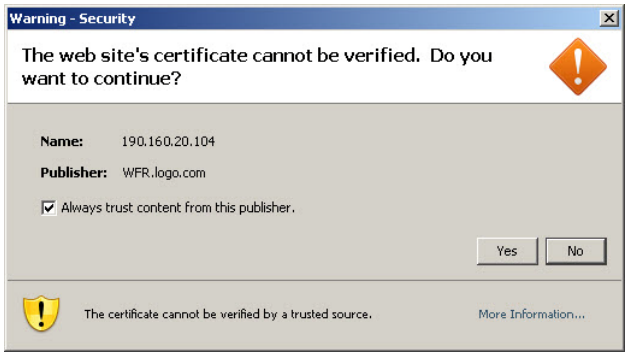


3. Clicking Add Exception opens the Add Security Exception window:

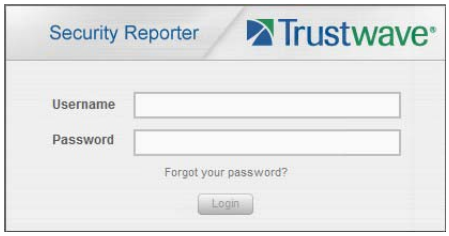


4. In the Add Security Exception window, click **Get Certificate** and wait a few seconds until the security certificate is obtained by the server.

5. With the check box **Permanently store this exception** selected, click **Confirm Security Exception** to open the Security warning dialog box:

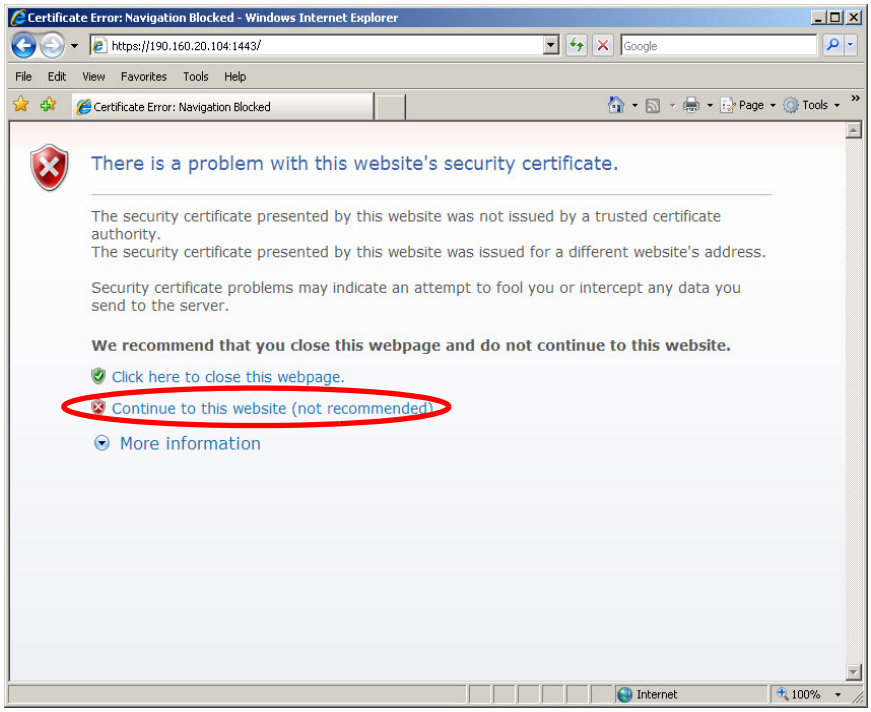


6. With the check box “Always trust content from this publisher.” populated, click **Yes** to close the Security warning dialog box and to access the login window of the SR user interface:

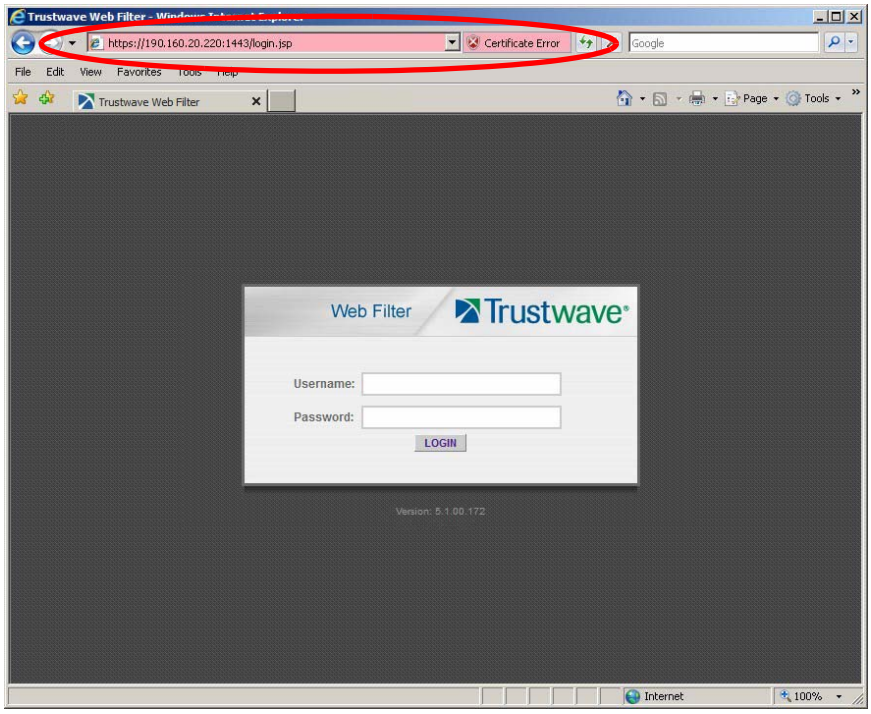


C.2 Temporarily Accept the Security Certificate in IE

If using an IE browser, in the page “There is a problem with this website's security certificate.”, click **Continue to this website (not recommended)**:



Selecting this option displays the SR login page with the address field and the Certificate Error button to the right of the field shaded a reddish color:



C.3 Accept the Security Certificate in Safari

If using a Safari browser, the window explaining “Safari can't verify the identity of the website...” opens:

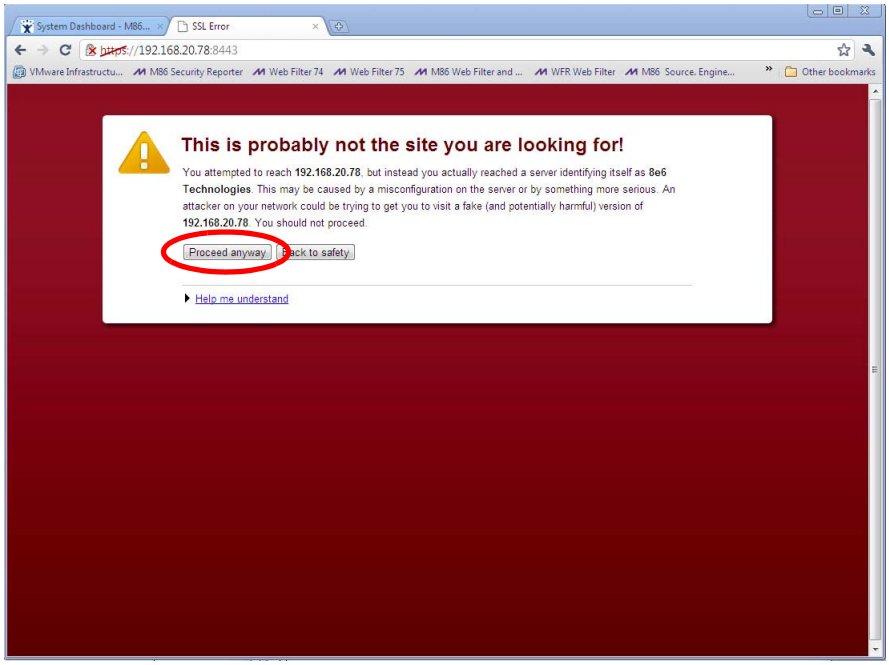
1. Click **Show Certificate** to open the certificate information box at the bottom of this window:

2. Click the “Always trust...” check box and then click **Continue**:

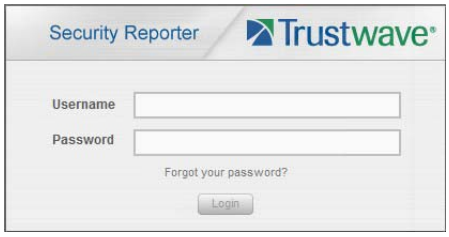
3. You will be prompted to enter your password in order to install the certificate.

C.4 Accept the Security Certificate in Chrome

If using a Chrome browser, in the page “This is probably not the site you are looking for!” click the button **Proceed anyway**:



4. Clicking this button launches the SR login window:



Note: With Chrome, you must follow this procedure every time you connect to SR.

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.