8e6 Technologies

8e6 ® Threat Analysis Reporter

USER
GUIDE

Model: TAR

Release 2.0.00 • Manual Version 1.01

THREAT ANALYSIS REPORTER USER GUIDE

CONTENTS

CONTENTS

INTRODUCTORY SECTION

Threat Analysis Reporter

As perimeter security becomes more mature, user-generated Web threats increase and become critical aspects of maintaining networks. Network administrators need tools to monitor these threats so management can enforce corporate Internet usage policies.

8e6's Threat Analysis Reporter (TAR) appliance is designed to offer administrators or management dynamic, real time graphical snapshots of their network's Internet traffic, supported by remediation tools to manage and control user-generated Web threats. Working in conjunction with 8e6's R3000 Internet Filter, TAR interprets end user Internet activity from the R3000's logs and provides data that can be viewed via an easy-to-read dashboard of gauges the administrator can drill down into, thereby identifying the source of the threat.

About this User Guide

The Threat Analysis Reporter User Guide addresses the network administrator designated to configure and manage the TAR server on the network (referred to as the "global administrator" throughout this user guide, since he/she has all rights and permissions on the TAR server), as well as administrators designated to manage user groups on the network (referred to as "group administrators" throughout this user guide).

This user guide is organized into the following sections:

• **Introductory Section** - This section provides general information on how to use this user guide to help you configure the TAR server.

• **Preliminary Setup Section** - This section includes information on creating and maintaining user accounts.

• **Configuration Section** - This section includes information on configuring TAR to alert you to any end user Internet activity not within your organization's Internet usage policies.

• **Administration Section** - This section includes functions for maintaining the TAR server or its database.

• **Technical Support / Product Warranties Section** - This section contains information on technical support and product warranties

• **Appendices** - Appendix A explains how to disable pop-up blocking software installed on a workstation in order to use TAR. Appendix B provides details on setting up and using the System Tray feature for TAR alerts. Appendix C includes information about RAID maintenance and troubleshooting on a TAR "H", "HL", or "SL" server. Appendix D features a glossary of technical terminology used in this user guide.

- **Index** - This section includes an index of subjects and the first page numbers where they appear in this user guide.

How to Use this User Guide

Conventions

The following icons are used throughout this user guide:

NOTE: The "note" icon is followed by italicized text providing additional information about the current subject.

TIP: The "tip" icon is followed by italicized text giving you hints on how to execute a task more efficiently.

WARNING: The "warning" icon is followed by italicized text cautioning you about making entries in the application, executing certain processes or procedures, or the outcome of specified actions.

Terminology

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

- **accordion** - one of at least two or more like objects, stacked on top of each other in a frame or panel, that expands to fill a frame or collapses closed when clicked.
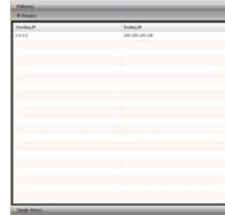
- **alert box** - a pop-up box that informs you about information pertaining to the execution of an action.
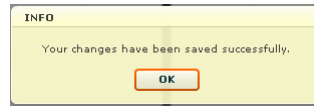
- **button** - an object in a dialog box, alert box, window, or panel that can be clicked with your mouse to execute a command.

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

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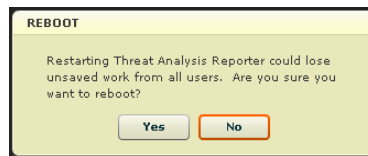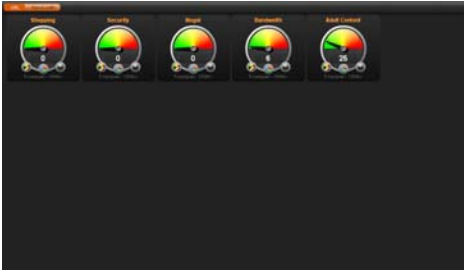
to make one or more entries or selections prior to clicking a button.

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

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

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

- **panel** - the central portion of a screen that is replaced by a different view when clicking a pertinent link or button.

- **pop-up box** or **pop-up window** - a box or window that opens after you click a button in a dialog box, window, or panel. This box or window may display information, or may require you to make one or more entries. Unlike a dialog box, you do not need to choose between options.
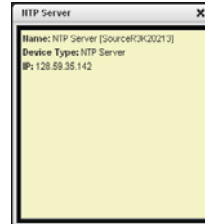
- **pull-down menu** - a field in a dialog box, window, or panel that contains a down arrow to the right. When you click the arrow, a menu of items displays from which you make a selection.
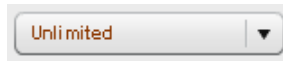
- **re-size button** - positioned between two frames, this button enlarges a frame or makes the frame narrower when clicked and dragged in a specific direction.

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

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

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

- **text box** - an area in a dialog box, window, or screen that accommodates your data entry. A text box is a type of field. (See "field".)

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

Environment Requirements

Workstation Requirements

Minimum system requirements for the administrator include the following:

- Windows XP or later operating system (not compatible with Windows server 2003) running Internet Explorer (IE) 6.0 or later, Firefox 3.0, or the latest version of Google Chrome.

- Macintosh OS X Version 10.5 running Safari 3.1.2, or Firefox 3.0

- Flash plug-in version 9 or later

- Screen resolution set at 1024 x 768 with color quality set at 16 bits

- 256MB RAM

- Pentium III 600 MHz or higher, or equivalent

- Network card and ability to connect to the TAR server and R3000 server

- Email client that can be set up to receive email alerts

- JavaScript enabled

- Java Virtual Machine

- Java Plug-in (use the version specified for the TAR software version)

Network Requirements

- High speed connection from the TAR server to client workstations

- HTTPS connection to 8e6's software update server

- Internet connectivity for downloading Java virtual machine/Flash, if not already installed

Installation Prerequisite

- 8e6 R3000 running software version 2.0.10 or later

NOTE: *The R3000 must be running software version 2.0.10 or later in order to use the time-based lockout feature defined in Chapter 3 of the Configuration Section.*

Getting Started

Initial Setup

To initially set up your TAR server, the administrator installing the unit should follow the instructions in the Quick Start Guide, the booklet packaged with your TAR unit. This guide explains how to perform the initial configuration of the server so that it can be accessed via an IP address on your network.

NOTE: If you do not have the Threat Analysis Reporter Quick Start Guide, contact 8e6 Technologies immediately to have a copy sent to you.

Once the TAR unit is set up on the network, the designated global administrator of the TAR server should be able to access the unit via its URL, using the user name and password registered during Step 1 of the quick start wizard procedures.

Login window

1. From your workstation, launch your browser window.

NOTE: *If pop-up blocking software is installed on the workstation, it must be disabled. Information about disabling pop-up blocking software can be found in Appendix A: Disable Pop-up Blocking Software.*

2. In the **Address** field of the browser window, type in the URL for the TAR server (in which 'x.x.x.x' represents the IP address specified during quick start procedures): ***http://x.x.x.x:8080***—or ***https://x.x.x.x:8443*** for a secure connection.

   This action opens the TAR login window:
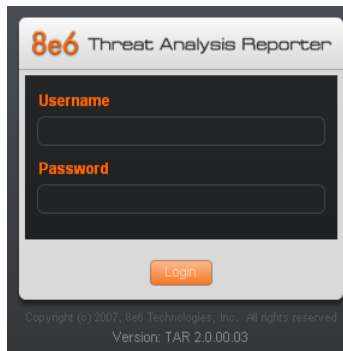
Fig. 1:1-1 TAR Login window

This window serves as a portal for administrators to log into TAR.

NOTE: *In this window, TAR's software version number displays beneath the frame.*

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

Log in

To log in the application:

1. In the **Username** field, type in your username. If you are logging in as the global administrator for the first time, enter the username registered during the quick start wizard procedures. If you are logging in as a group administrator, enter the username set up for you by the global administrator.

2. In the **Password** field, type in your password. If you are logging in as the global administrator for the first time, enter the password registered during the quick start wizard procedures. If you are logging in as a group administrator, enter the password set up for you by the global administrator. This entry displays as a series of asterisks for security purposes.

3. Click the **Login** button to open the application, displaying the URL gauges dashboard in the panel by default. At the top of the screen, on the right side, the Help and Logout buttons display. Tabs for Gauges, Administration, Policy, and Report/Analysis display below, followed by a row of links/buttons pertaining to the selected tab. The URL and Bandwidth buttons display to the left above the panel:

Fig. 1:1-2 Default TAR panel

Navigation toolbar: Tabs and menu topics

The navigation toolbar at the top of the screen consists of tabs and links that let you access panels used for configuring and using the application:

- **Gauges** - click this tab to access links to panels that let you set up and manage URL and bandwidth gauges.

- **Administration** - click this tab to access links to panels that let you set up and maintain administrator profiles and manage the TAR unit.

- **Policy** - click this tab to access links to panels that let you set up and maintain policies used for triggering warnings when gauges approach their upper threshold limits.

- **Report/Analysis** - click this tab to display links and buttons for accessing related applications and Internet usage data on your network.

Help

To open a separate browser window containing the latest User Guide in the PDF format, click the **Help** button at the top of the screen.

Log out

To log out of the application, click the **Logout** button in the upper right corner of the screen. When your session has been terminated, the login window re-displays.

Exit the interface

To exit the interface, click the "X" in the upper right corner of the browser window.

Navigation Tips and Conventions

The following tips and list of conventions will help you navigate the Administrator console:

- **Move a pop-up window** - Click the toolbar of a pop-up window and simultaneously move your mouse to relocate the pop-up window to another area in the current browser window.

- **Scroll up and down, and across a list** - If available, use the scrollbar to the right or along the bottom of a frame or list box to view an entire list.
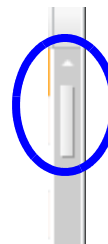
  An extensive list can be viewed in its entirety by clicking the previous and next buttons.

- **Tab to the next field** - Press the Tab key on your keyboard to advance to the next field in a panel.

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

- **Browser Back button, Refresh button** - Clicking either the Back button in the browser window or the Refresh button in your browser will refresh the TAR interface and log you out of the application.

- **Select multiple items in specified windows** - In specified panels, when moving several items from one list box to another, or when deleting several items, the Ctrl and Shift keys can be used to expedite this task.

  - **Ctrl Key** - To select multiple items from a list box, click each item while pressing the Ctrl key on your keyboard.

- **Shift Key** - To select a block of consecutive items from a list box, click the first item, and then press the Shift key on your keyboard while clicking the last item.

  Once the group of items is selected, click the appropriate button to perform the action on the items.

- **Sort records by another column header** - Records can often be sorted by a different column header by clicking the header for that column. This action sorts the records that display in descending order by that column. Clicking the same column header again sorts the records in ascending order by that column.

- **View tooltip information** - To view information about any object that has a circled "i" icon beside it, mouse over the icon to display tooltips that explain how to use that button or field.

- **Return to the gauges dashboard** - To return to the gauges dashboard, click the **Back to Gauges** button located at the top of the screen to the left of the Gauges tab.

PRELIMINARY SETUP SECTION

Introduction

The Preliminary Setup Section of this manual is comprised of three chapters with information on the first steps to take in order to use the TAR application. These steps include setting up user groups, administrator permission groups, and group administrator profiles:

- Chapter 1: User Groups Setup - This chapter explains how to set up user groups—whose Internet activity will be monitored by group administrators.

- Chapter 2: Admin Groups Setup - This chapter explains how to set up permissions so that an administrator in your group will only be able to access areas of the TAR console that you specify.

- Chapter 3: Admins Setup - This chapter explains how to set up a group administrator account.

Chapter 1: User Groups Setup

On a new TAR server, the global administrator should first set up user groups—whose Internet activity will be monitored by group administrators.

A group administrator should set up user groups once he/she is given an account by the global administrator with permissions to access User Groups, as detailed in the next chapters in this section.

1. In the navigation toolbar, click the Administration tab to display topics available to you.

2. Click **User Groups** to display the User Groups panel, which is comprised of the User Groups frame to the left and its Group Members target frame to the right:
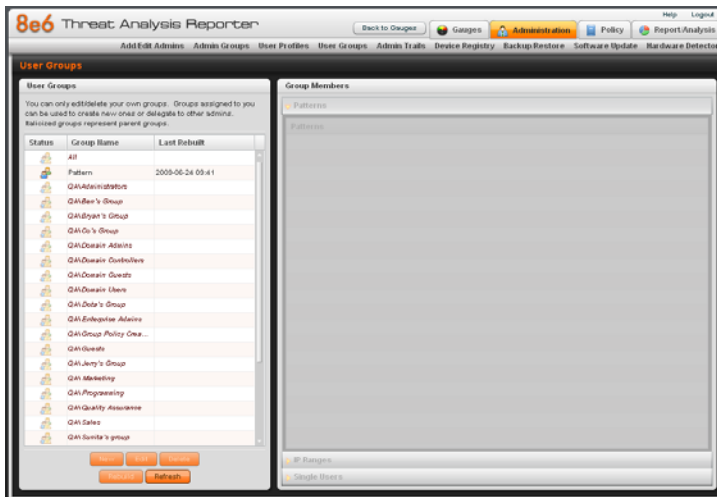
Fig. 2:1-1 User Groups panel

Names of user groups previously added by the administrator display in black text in the User Groups frame. Imported user groups display in italicized brown text. For the global administrator, "All" displays as the first record in the list by default.

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

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

TIP: *Click* **Back to Gauges** *at the top of the screen to re-display the default gauges view.*

NOTES: *This version of TAR will import user groups from a source R3000 using IP group authentication or the following LDAP server types:*

- *Active Directory Mixed Mode*
- *Active Directory Native Mode*
- *Novell eDirectory*
- *SunONE*

Open LDAP usernames will be included in user profiles only if those users generate network traffic.

View User Group Information

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

NOTE: User groups are automatically rebuilt daily.

User group status key

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

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

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

View a list of members in a user group

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

1. Select the user group from the User Groups frame by clicking its Group Name to highlight that record. Based on this selection, the Group Members frame to the right becomes activated along with the following buttons in the section below, based on the status of the user group:

   • If the selected user group is ready to be rebuilt, this action activates all buttons (New, Edit, Delete, Rebuild, Refresh).

   • If the selected user group was not imported and cannot be rebuilt on demand, this action activates the New, Edit, Delete and Refresh buttons.

- If the selected user group was imported and cannot be rebuilt on demand, this action activates the New and Refresh buttons only.

2. Click an accordion in the Group Members frame to open it and view pertinent information:

   - Patterns accordion - view patterns previously set up for that user group.

   - IP Ranges accordion - view Starting IP and Ending IP ranges previously added for that user group.

   - Single Users accordion - view a list of User Names and IP Addresses for individual users previously selected from the Available Users list for that user group.
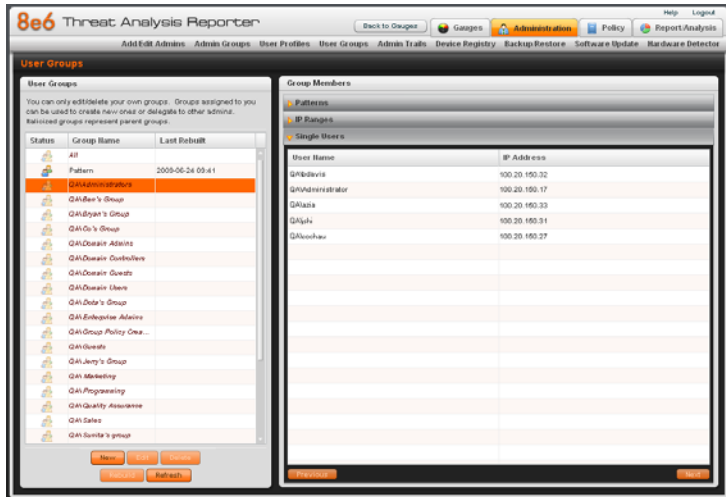
Fig. 2:1-2 View user group information, Single Users accordion

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

For LDAP authentication, the member "IPGROUP" pertains to any end user who has been authenticated but does not yet have a user name associated with his/her IP address.

Add a User Group

To add a new user group:

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

2. Click **New** to display the New User Group panel:

Fig. 2:1-3 New User Group panel

At the top of this panel are the Patterns, IP Ranges, and Single Users checkboxes, and the Group Name field. greyed-out frames corresponding to these checkboxes display below. The only checkboxes that are activated are the ones pertinent to the selected user group.

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

4. Click the checkbox(es) to activate the pertinent corresponding frame(s) below: **Patterns**, **IP Ranges**, **Single Users**.

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

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

Patterns frame

When creating a user group, the Patterns frame is used for adding one or more patterns in order to narrow the list of users to be included in the new group. A pattern consists of a wildcard, or a wildcard plus one or more alphanumeric characters. If any patterns have been inherited from the base group, these display in the Parent Patterns frame and can be added to the new user group.

Add a new pattern

To add a pattern to the new user group:

1. Do one of the following:

    • To add an inherited pattern, select the pattern from the Parent Patterns box to display that pattern in the field below.

    • To add a new pattern, enter the pattern in the field beneath the Parent Patterns box. For example: Enter *200.10.100.3%* to include all IP addresses with "200.10.100.3" as part of the IP address.

2. Click **Add Pattern** to include the pattern in the Assigned Patterns list box below.

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

View users resolved by the pattern

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

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

2. Click **Preview Users** to open the Preview Pattern Users pop-up window that shows the Patterns frame to the left and the Resolved Users frame to the right:
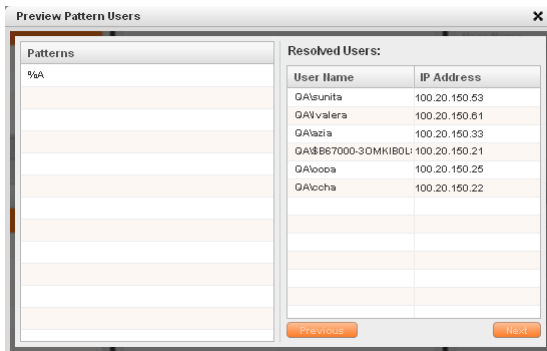
Fig. 2:1-4 Add user group Patterns, Preview Pattern Users

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

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

Remove a pattern

To remove a pattern in the Assigned Patterns list box:

1. In the Patterns frame, select the pattern from the Assigned Patterns list box to highlight it.

2. Click **Remove Pattern** to remove that pattern from the list box.

IP Ranges frame

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

NOTE: If using IP group authentication, parent ranges do not display in this frame unless an IP range was originally set up for this user group's parent user group. To set up the first parent user group to include an IP range, "All" user groups must be used as the base group.
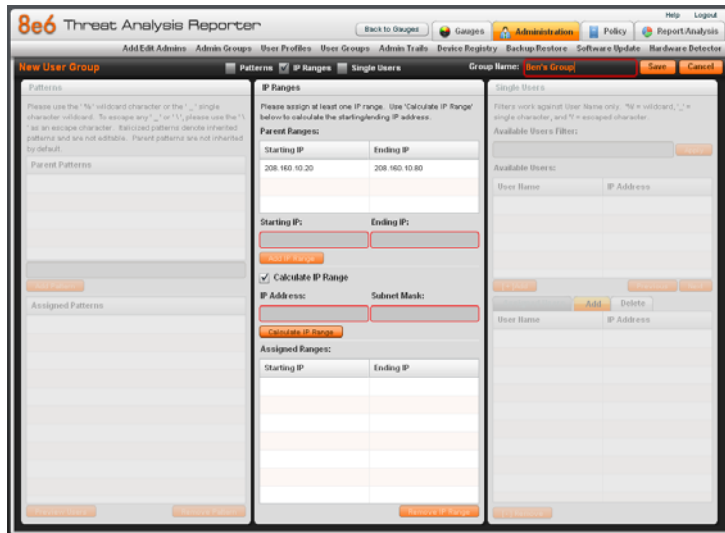
Fig. 2:1-5 Add user group, IP Ranges frame

Specify an IP range

To add an IP address range:

1. Do one of the following:

   • To make a selection from Parent Ranges, click the row in the Parent Ranges box to highlight and select that row, and also to add that Starting IP and Ending IP range in the Starting IP and Ending IP fields below. If necessary, edits can be made to these fields.

   • To add an IP address range without selecting from the Parent Ranges frame:

     a. Enter the **Starting IP** address.

     b. Enter the **Ending IP** address.

   • To calculate an IP address range:

     a. Click the **Calculate IP Range** checkbox to activate the IP Address and Subnet Mask fields below.

     b. Enter the **IP Address**.

     c. Enter the **Netmask** which activates the Calculate Range button.

     d. Click **Calculate IP Range** to display the Starting IP and Ending IP in the fields above.

2. Click **Add IP Range** to include that IP range in the Assigned Ranges list box below:
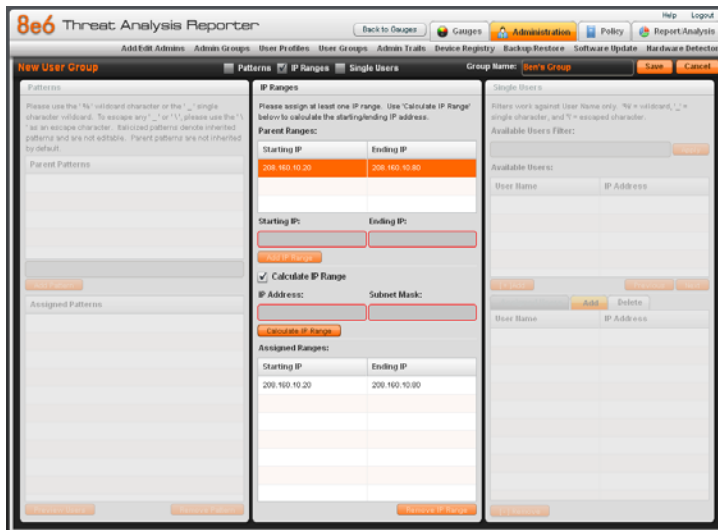
Fig. 2:1-6 Add user group, IP range added

Remove an IP address range

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

1. Click the row to highlight and select it; this action activates the Remove IP Range button below.

2. Click **Remove IP Range** to remove the IP address range from the list box.

Single Users frame

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

NOTE: Only users previously selected from the base user group will be included in the Available Users list.
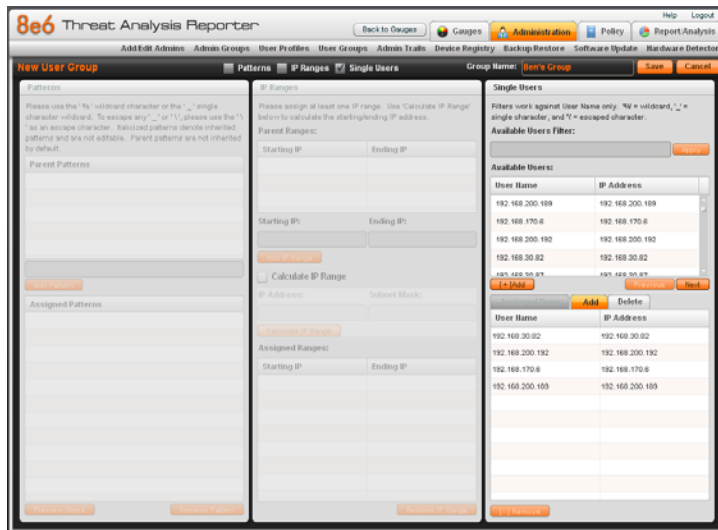
Fig. 2:1-7 Add user group, Single Users frame

Add one or more individual users

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

Use the filter to narrow Available Users results

To use the **Available Users Filter**:

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

2. Click **Apply** to display filtered results in the Available Users box.

Select users to add to the Assigned Users list

To make selections from the Available Users box:

1. Select one or more IPs from the list to highlight the record(s).

2. Click **[+] Add** to include the selected user(s) in the Add Users tab.

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

Remove users from the Add tab

To remove users from this user group:

1. Select the user(s) from the Add tab; this action activates the [-] Remove button:
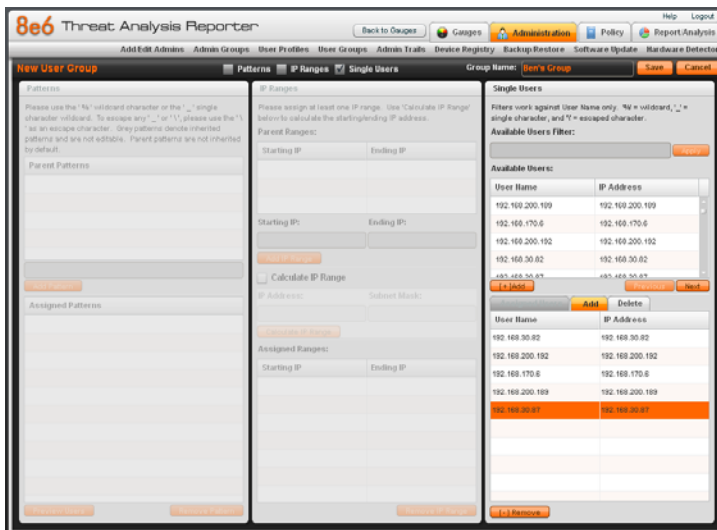
Fig. 2:1-8 Add user group, remove user from Single Users tab

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

Edit a User Group

NOTE: Global and group administrators can only edit user groups they have created, and cannot edit their base groups or imported user groups.

To edit a user group:

1. From the main User Groups panel, select the user group from the list in the User Groups frame.

2. Click **Edit** to display the User Group panel showing activated frames—i.e. if the Patterns frame had settings made in it, that frame is activated; if the Single Users frame was the only frame with settings made in it, that frame is activated. Any frame without settings made in it displays greyed-out.

3. Make any of these edits:

   • To make entries in a frame that is not yet activated, click the available checkbox to activate that frame: **Patterns**, **IP Ranges**, **Single Users**.

   • Make any of these edits in a frame:

     • Patterns frame - add or remove a pattern.

     • IP Ranges frame - add or remove an IP address range.

     • Single Users frame - add or remove one or more users.

NOTE: When editing the Single Users frame, users who are added display in the Add tab, and users who are removed display in the Delete tab.

   • If necessary, edit the name of the user group in the **Group Name** field.

4. Click **Save** to save your edits and to return to the User Groups panel.

Rebuild the User Group

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

1. In the User Groups panel, select the user group to be rebuilt.

2. Click **Rebuild** to initiate the rebuild process for that user group.

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

Delete a User Group

NOTES: A user group can only be deleted by the administrator who added it. A base group cannot be deleted.

To delete a user group:

1. In the User Groups panel, select the user group from the User Groups list.

2. Click **Delete** to open the Confirm dialog box with the message: "Are you sure you want to delete this user group?"

WARNING: If the user group to be deleted has been delegated to an administrator, that user group will be removed from that administrator's User Groups list as well as your User Groups list.

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

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

Chapter 2: Admin Groups Setup

Once you have set up user groups, you are ready to create a set of management permissions, so that a group administrator you set up will only be able to access areas of the TAR console that you specify.

This function is available to a group administrator only if permissions were granted by the administrator who set up his/her account, as detailed in this chapter and in Chapter 3.

In the navigation toolbar, with the Administration tab selected, click **Admin Groups** to open the Admin Groups panel, comprised of the Admin Groups frame to the left and the Group Privileges frame to the right:
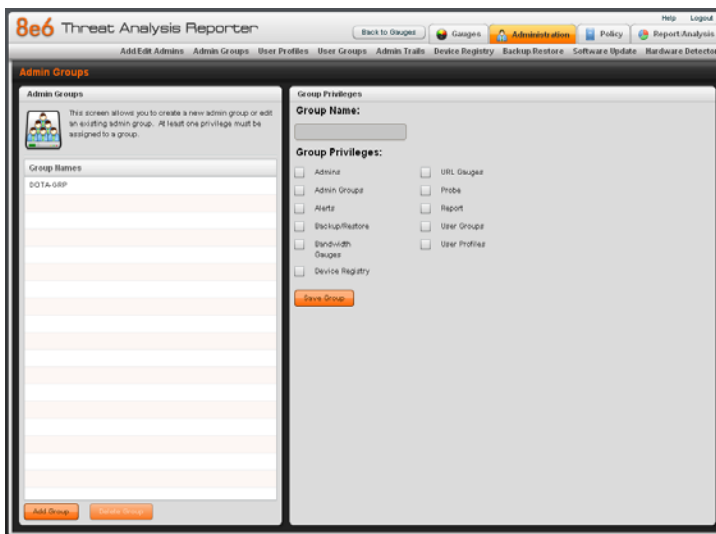
Fig. 2:2-1 Admin Groups panel

Administrator groups previously set up display in the Group Names list box in the Admin Groups frame.

In this panel, you can add an administrator group, view information for an existing administrator group, and modify or delete that group, as necessary.

Add a Group

1. At the bottom of the Admin Groups frame, Click **Add Group**.

2. At the top of the Group Privileges frame, type in up to 32 characters for the **Group Name**.

💡 *TIP: You may want to name the group for the type of permissions to be assigned. This will distinguish the name from other names, such as those set up for user groups.*

3. In the Group Privileges section, click the appropriate checkbox(es) to specify the type of access the administrator group will be granted on the TAR console or its related devices:
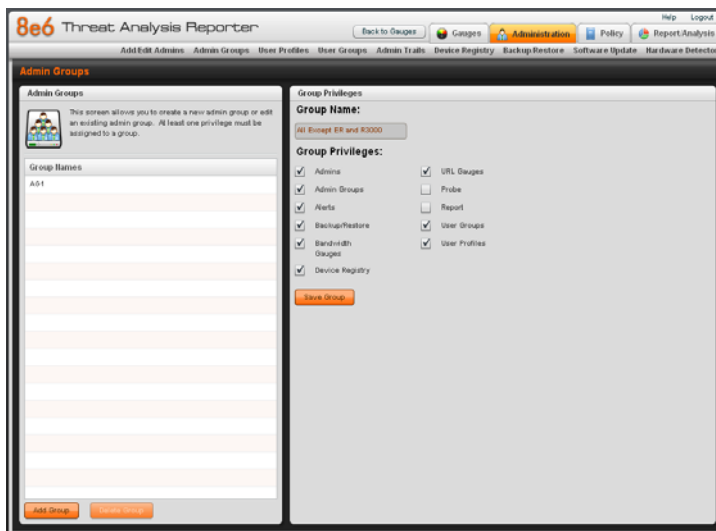
Fig. 2:2-2 Add a new Group

- **Admins** - Manage group administrator profiles.
- **Admin Groups** - Manage administrator groups.
- **Alerts** - Manage alerts that indicate if gauges are close to—or have reached—their established upper thresholds.

- **Backup/Restore** - Perform a backup and/or restoration on the TAR server.
- **Bandwidth Gauges** - Monitor and manage bandwidth gauges for inbound and outbound traffic.
- **Device Registry** - Edit settings for an R3000, ER, or TAR (a bandwidth IP address range for TAR can also be added or removed); add another R3000, or add an ER (if the latter was not previously added); view information about devices connected to the TAR server; or synchronize—with TAR—the source R3000's supplied library category updates, custom categories, user group information, and devices connected to TAR.
- **URL Gauges** - Monitor and manage URL gauges.
- **Probe** - Access the R3000 application's Real Time Probe feature that lets you monitor end user Internet usage in real time to verify whether the Internet is being used appropriately.
- **Report** - Access the ER application to generate reports on end user Internet activity.
- **User Groups** - Manage user groups.
- **User Profiles** - Manage a list of end users' logged events.

TIP: To remove a checkmark from any active checkbox containing a checkmark, click the checkbox.

4. Click **Save Group** to save your entries and to add the new administrator group name in the Group Names list box.

View, Edit an Admin Group's Permissions

View Admin Group settings

In the Admin Groups frame, click the name of the administrator group to highlight the group name, activate all buttons, and to populate the Group Privileges frame with previously-saved settings:
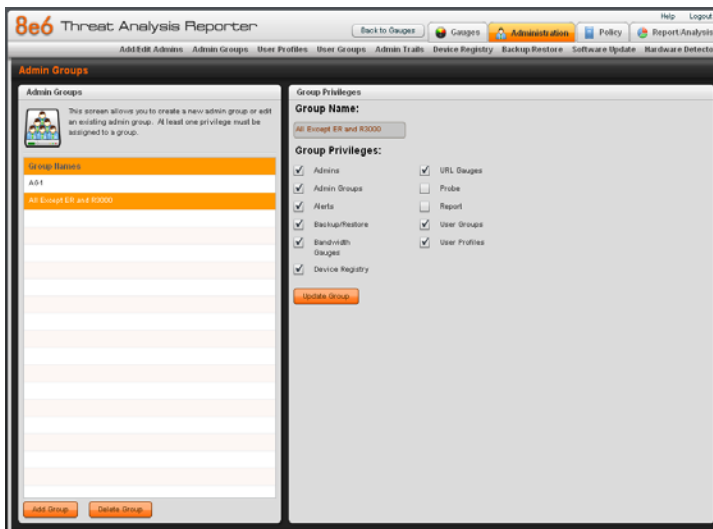
Fig. 2:2-3 Admin Groups group selections

With the Group Privileges frame populated, you can now make edits as described in the following sub-section.

Edit Admin Group settings

1. In the Group Privileges frame, perform any of the following actions:

   • Modify the **Group Name**

   • Add functions to be monitored by the administrator group

   • Remove functions to be monitored by the administrator group

2. Click **Update Group** to save your settings and to clear all selections in the Group Privileges frame.

Delete an Administrator Group

1. In the Group Names list box, click the name of the administrator group to highlight the group name, activate all buttons, and to populate the Group Privileges frame with previously-saved settings.

2. Click **Delete Group** to open the Confirm dialog box with the message: "Are you sure you want to delete this admin group?"

3. Click **Yes** to close the dialog box and to remove the administrator group from the Group Names list box.

NOTE: Clicking Cancel closes the dialog box without removing the administrator group.

Chapter 3: Admins Setup

After permission sets have been created, profiles of group administrators can be set up to monitor user groups.

This function is available to a group administrator only if permissions were granted by the administrator who set up his/her account, as detailed in Chapter 2 and in this chapter.

In the navigation toolbar, with the Administration tab selected, click **Add/Edit Admins** to display the Add/Edit Admins panel:

Fig. 2:3-1 Add/Edit Admins panel

At the left side of this panel, the Admin Names list box in the Admins frame displays TAR Login IDs of administrator accounts previously set up in this panel.

NOTE: In addition to seeing account IDs set up and saved in this panel, a global administrator will also see the TAR Login ID established during the quick start wizard hardware installation process. A group administrator will only see administrator profiles he/she added.

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

Add an Administrator Profile

1. At the bottom of the Admins frame, click **Add Admin** to clear and reset the Admin Detail frame.

2. In the Admin Detail frame, make the following entries or selections as appropriate:
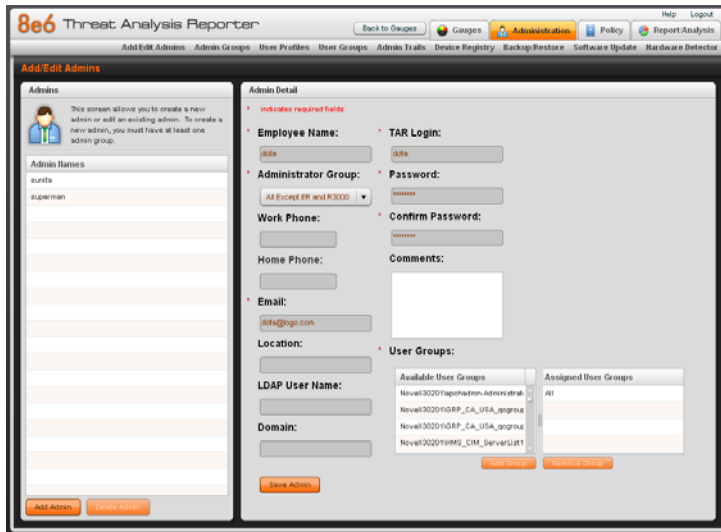
Fig. 2:3-2 New administrator information entered but not yet saved

- Type in the group administrator's **Employee Name**.
- Select the **Administrator Group** (previously set up in the Admins Group panel) from the available choices in the pull-down menu.

- Optional: Type in the group administrator's **Work Phone** number, without entering special characters such as parentheses ( ), a hyphen (-), a period (.), or a left slash (/).

- Optional: Type in the group administrator's **Home Phone** number without entering any special characters.

- Type in the group administrator's **Email** address.

- Optional: Type in identifying information about the group administrator's physical office **Location**.

- Optional: If the administrator has an Active Directory LDAP account, user name, and domain, type in the alphanumeric group administrator's **LDAP User Name** exactly as set up on the Active Directory domain in which he/she is registered.

- Optional: If an entry was made in the LDAP User Name field, type in the exact characters for the LDAP Active Directory **Domain** name in which the group administrator is registered.

NOTE: If the group administrator will be using the System Tray feature—that triggers an alert in his/her System Tray if an end user's Internet usage has reached the upper threshold established for a gauge's alert—the LDAP User Name and Domain entered in these fields should be the same as the login ID and password the group administrator uses to authenticate on his/her workstation. (See Configuration Section, Chapter 3: Alerts, Lockout Management and Appendix B: System Tray Alerts: Setup, Usage for details on setting up and using the System Tray feature.)

- Type in the **TAR Login** ID the group administrator will use to access the TAR interface. This entry will display in the Admin Names list when the record is saved.

- Type in the **Password** the group administrator will use in conjunction with the TAR Login ID, and enter that same password again in the **Confirm Password** field. These entries display as asterisks for security purposes.

- Optional: Type in any **Comments** to be associated with the group administrator's account.

3. In the User Groups section, select the user group(s) to be monitored by the group administrator:

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

- Click **Add Group** to include the user group(s) in the Assigned User Groups list box.

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

4. After selecting each user group to be assigned to the group administrator, click **Save Admin** to add the TAR Login ID for the new administrator to the Admin Names list box.

View, Edit Admin Detail

View Admin Details

In the Admin Names list box, select the administrator's TAR Login ID to populate that user's account information in the Admin Detail frame:

Fig. 2:3-3 Add/Edit Admins, Admin Names selection

NOTE: *The global administrator profile that was created during the quick start wizard hardware installation process displays at minimum the TAR Login ID, Email address, asterisks in the Password and Confirm Password fields, and, in the Assigned User Groups list box, all user groups that would be available in the Available User Groups box. For this profile, the Employee Name and Administrator Group field do not display since this administrative account does not manage user groups, but does receive email alerts about maintaining the TAR unit.*

Edit Account Info

1. In the populated Admin Detail frame:

   • The following information can be updated: Employee Name, Administrator Group selection, Email address, TAR Login ID, Password and Confirm Password entries, and User Groups selections.

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

2. After making any modifications, click **Update Admin** to save your edits.

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

Delete Admin

NOTE: The global administrator account established during the quick start hardware installation process can be modified but cannot be deleted.

1. In the Admin Names list box, select the group administrator's TAR Login ID.

2. Click **Delete Admin** to open the Confirm dialog box with the message: "Are you sure you want to delete this admin?"

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

3. Click **Yes** to close the dialog box and to remove the administrator's TAR Login ID from the list.

CONFIGURATION SECTION

Introduction

The Configuration Section of this user guide is comprised of four chapters with information on configuring and using TAR to immediately alert you to any end user Internet activity not within your organization's Internet usage policies:

- Chapter 1: Gauge Components - This chapter describes the types of gauges, the components of a gauge, how to read a gauge, and how to perform shortcuts using gauges.

- Chapter 2: Custom Gauge Setup, Usage - This chapter explains how gauges are configured and monitored.

- Chapter 3: Alerts, Lockout Management - This chapter explains how alerts are set up and used, and how to manage end user lockouts.

- Chapter 4: Analyze Usage Trends - This chapter explains how trend charts are used for assessing end user Internet/network activity. For additional or historical information about end user Internet usage trends, the R3000's Real Time Probe interface—and the ER's Web Client reporting application, if the ER server is installed and connected to the source R3000—can be accessed from the TAR interface.

- Chapter 5: Identify Users, Threats - This chapter explains how to perform a custom search on Internet/network usage by a specified user, or for a specified threat or threat group.

Chapter 1: Gauge Components

Types of Gauges

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

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

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

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

Anatomy of a Gauge

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

The illustration below depicts a URL gauge and a bandwidth gauge and some of their components:
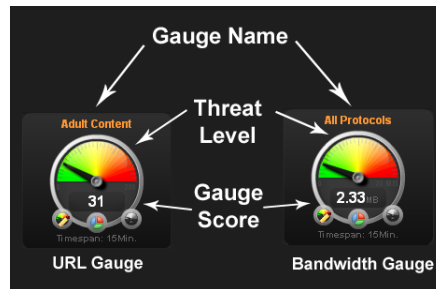
Fig. 3:1-1 URL and bandwidth gauge anatomy

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

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

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

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

• URL gauge - score includes the total number of end user hits (page count plus blocked object count) for all library categories the gauge monitors.

• Bandwidth gauge - score includes the total number of bytes (KB, MB, GB) of inbound/outbound end user traffic for all protocols/ports the gauge monitors.

How to Read a Gauge

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

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

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

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

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

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

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

Bandwidth Gauge Components

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

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

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

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

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

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

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

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

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

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

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

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

- **1214** - TCP/UDP port for Kazaa, Morpheous, Grokster, etc.
- **4662** - TCP/UDP port for eMule, eDonkey, etc.
- **4665** - TCP/UDP port for eDonkey 2000
- **6346** - TCP/UDP port for Gnutella file sharing (Frost-Wire, LimeWire, BearShare, etc.)
- **6347** - TCP/UDP port for Gnutella
- **6699** - UDP port for Napster
- **6881** - TCP/UDP port for BitTorrent

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

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

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

Gauge Usage Shortcuts

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

- **View Gauge Ranking** - Clicking a gauge or right-clicking a gauge and selecting this topic from the menu displays the Gauge Ranking panel. The table in this panel contains a list of library categories/protocols/ports that comprise the gauge, along with the list of current users driving the gauge's score. (See View End User Gauge Activity in Chapter 2 of the Configuration Section.)

- **Edit Gauge** - Clicking the left icon at the bottom of a gauge—or right-clicking a gauge and then selecting this menu topic—displays the panel that lets you edit the gauge's components. This is a shortcut to use instead of going to the Add/Edit Gauges panel, selecting the gauge, and then clicking Edit Gauge. (See Modify a Gauge in Chapter 2 of the Configuration Section.)

- **Hide Gauge** - Clicking the right icon at the bottom of a gauge—or right-clicking a gauge and then selecting this menu topic—lets you remove the gauge from the dashboard. This is a shortcut to use instead of going to the Gauge View tab, selecting the gauge from the list, and then clicking the Hide Gauge icon. (See Hide, Disable, Delete, Rearrange Gauges in Chapter 2 of the Configuration Section.)

- **Trend Charts** - Clicking the middle icon at the bottom of a gauge—or right-clicking a gauge and then selecting this menu topic—displays a Trend Chart for this particular gauge that lets you
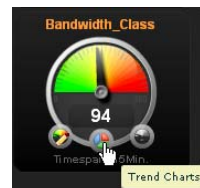
analyze the gauge's activity. (See View Trend Charts in Chapter 4 of the Configuration Section.)

- **Disable Gauge** - Right-clicking a gauge and then selecting this menu topic lets you disable a gauge. This is a shortcut to use instead of going to the Gauge View tab, selecting the gauge from the list, and then clicking the Disable Gauge icon. (See Hide, Disable, Delete, Rearrange Gauges in Chapter 2 of the Configuration Section.)

- **Delete Gauge** - Right-clicking a gauge and then selecting this menu topic lets you delete a gauge. This is a shortcut to use instead of going to the Gauge View tab, selecting the gauge from the list, and then clicking the Delete Gauge icon. (See Hide, Disable, Delete, Rearrange Gauges in Chapter 2 of the Configuration Section.)

Chapter 2: Custom Gauge Setup, Usage

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

Any of the functions described in this chapter are only available to a group administrator if permissions were granted by the administrator who set up his/her account, as detailed in Preliminary Setup Section.

1. In the navigation toolbar, with the Gauges tab selected, click **Add/Edit Gauges** to open the Add/Edit Gauges panel:
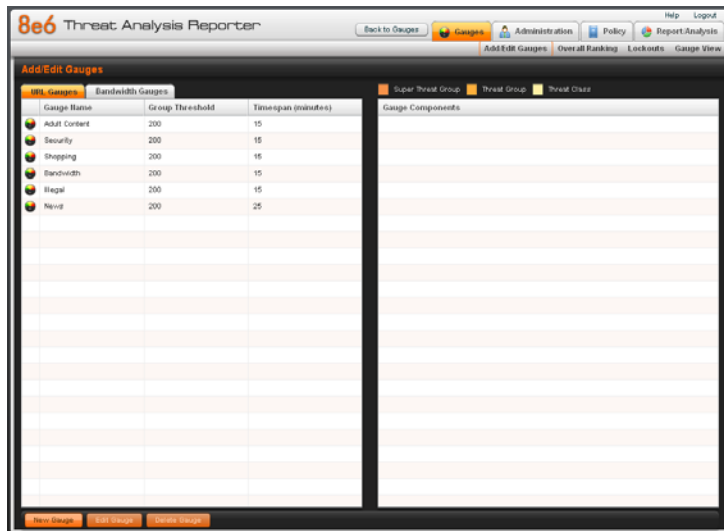
Fig. 3:2-1 Add/Edit Gauges panel

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

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

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

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

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

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

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

3. Select a Gauge Name to display a list of its library categories/protocols/ports in the Gauge Components frame:
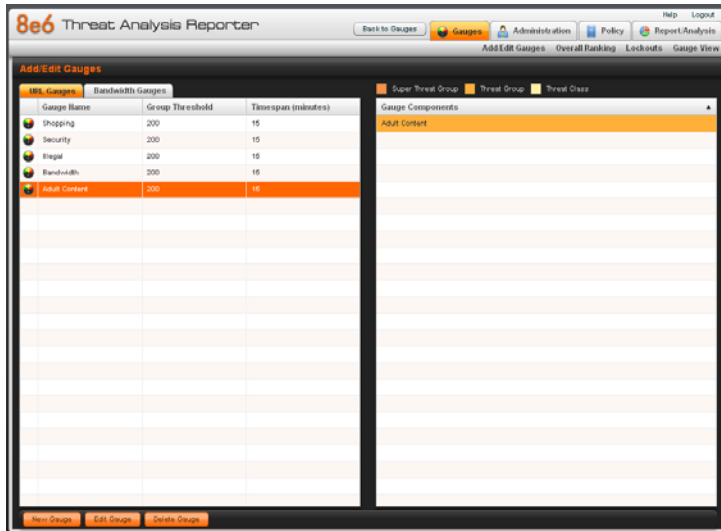
Fig. 3:2-2 Gauge Components frame populated

Add a Gauge

In the Add/Edit Gauge panel, click **New Gauge** to display Gauge panel:
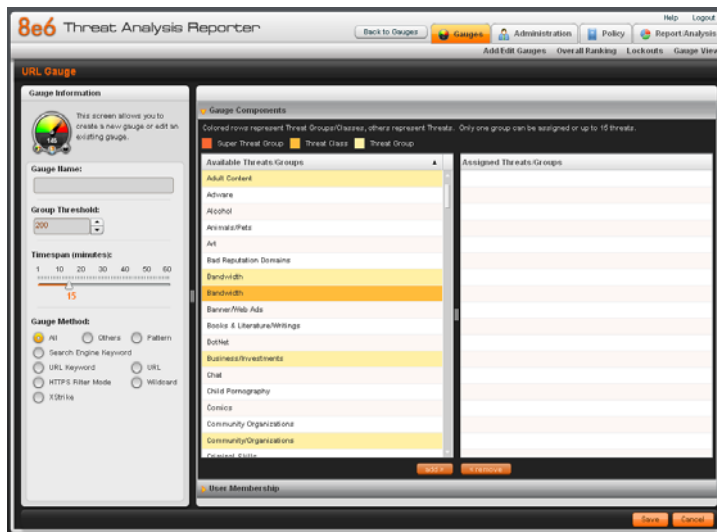
Fig. 3:2-3 Add a new gauge

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

When adding a new gauge, do the following:

• Name the gauge, and specify group threshold limits, timespan values, and the method(s) to be used by the gauge (see Specify Gauge Information).

• Select the library categories/protocols/ports for the gauge to monitor (see Define Gauge Components).

• Assign user groups whose end users' Internet/network activity will be monitored by the gauge (see Assign User Groups).

Specify Gauge Information

In the Gauge Information frame:

1. Type in at least two characters for the **Gauge Name** using upper and/or lowercase alphanumeric characters, and spaces, if desired.

2. Specify the **Group Threshold** ceiling of gauge activity. The default and recommended value is *200* for a URL gauge and *20 MB* for a bandwidth gauge. This ceiling can be adjusted after using TAR for awhile and evaluating activity levels at your organization.

   To modify information in this field, type a specific value in the pre-populated field, and/or use the up/down arrow buttons to increment/decrement the current byte value by one. Make a selection from the pull-down menu if you need to change the byte unit (kB, MB, GB).

3. Use the slider tool to specify the **Timespan (minutes)** for tracking gauge activity (1 - 60 minutes). The default and recommended value is *15* minutes. The timespan will always keep pace with the current time period, so that if a timespan of 15 minutes is specified, the gauge will always reflect the most recent end user activity from the past 15 minutes.

4. If necessary, specify a different **Gauge Method** to be used for tracking gauge activity:

   • For a URL gauge - **All** (default), **Others** (all gauge methods, not including Keywords or URLs), **Pattern**, **Search Engine Keyword**, **URL Keyword**, **URL**, **HTTPS Filter Mode**, **Wildcard**, **XStrike**.

   • For a bandwidth gauge - **Inbound, Outbound**, **Both** (default).

NOTE: If the selected gauge method is "Search Engine Keyword" or "URL Keyword", Filter Options for end user profiles on the source R3000 used with TAR must have "Search Engine Keyword Filter Control" or "URL Keyword Filter Control" enabled.

Define Gauge Components

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

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

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

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

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

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

2. Click **add >** (for URL gauges) or **add port >** (for bandwidth gauges) to move the selection(s) to the Assigned Threats/Groups list box.

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

Assign user groups

To assign user groups to be monitored by the gauge:

1. Click the User Membership accordion to open it and to display a list of Available User Groups in the list to the left:
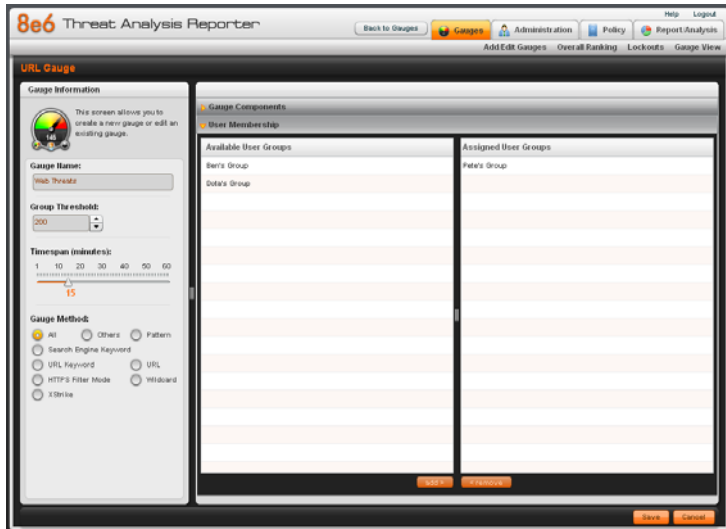
Fig. 3:2-4 User Membership accordion opened

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

2. From the Available User Groups list, select the user group to highlight it.

3. Click **add >** to move the user group to the Assigned User Groups list box.

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

Save gauge settings

After adding users, click **Save** to return to the Add/Edit Gauges panel that now includes the name of the gauge you just added:
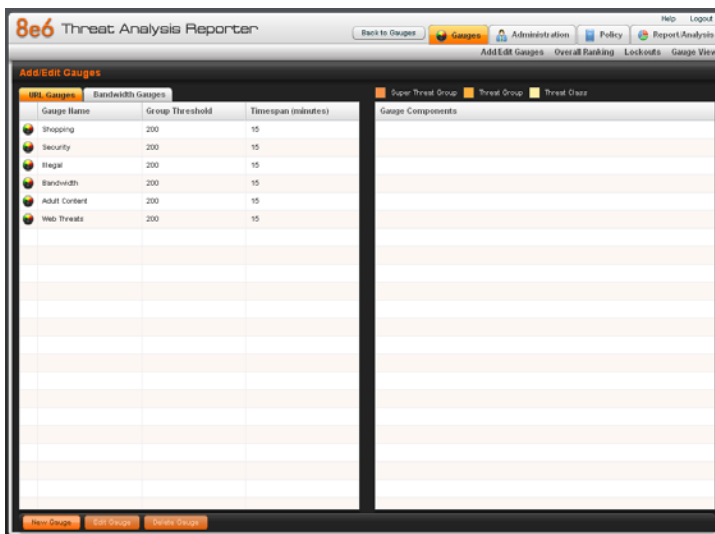
Fig. 3:2-5 New gauge added

Modify a Gauge

Edit gauge settings

1. In the Add/Edit Gauge panel, click the URL Gauges or Bandwidth Gauges tab.

2. Select the gauge from the list to activate all buttons below and populate the Gauge Components frame to the right:
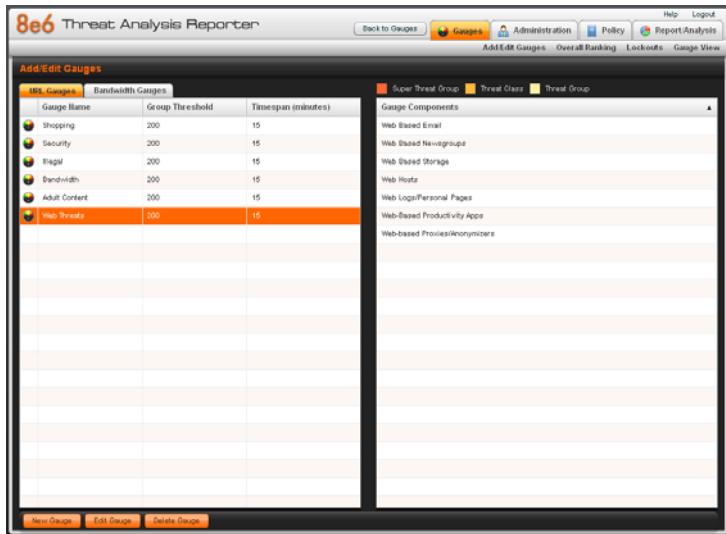
Fig. 3:2-6 Select the gauge to be edited

3. Click **Edit Gauge** to display the URL Gauge or Bandwidth Gauge panel showing the Gauge Information frame to the left and the Gauge Components frame to the right, populated with settings previously saved for the gauge:
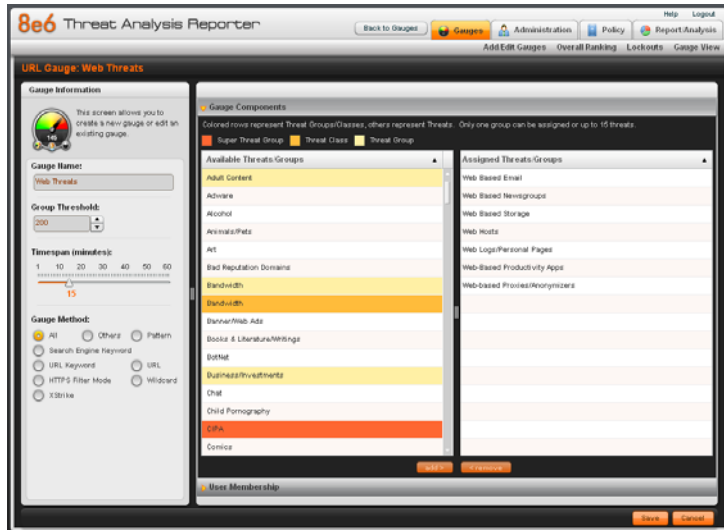
Fig. 3:2-7 Edit gauge settings

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

4. Edit any of the following criteria, as necessary:

   - Gauge Information - Gauge Name, Group Threshold, Timespan in minutes, Gauge Method (see Specify Gauge Information).

   - Gauge Components (see Define Gauge Components).

   - User Membership (see Assign user groups).

5. Click **Save** to save your edits and return to the Add/Edit Gauges panel.

Hide, Disable, Delete, Rearrange Gauges

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

TIP: In addition to the instructions provided in this sub-section, gauges can be hidden, disabled, and deleted from the gauges dashboard by right-clicking the gauge to display its menu, and then choosing the appropriate topic. See Gauge Usage Shortcuts in Chapter 1 of the Configuration Section.

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

1. In the navigation toolbar, with the Gauges tab selected, click **Gauge View** to display the Gauge View panel:
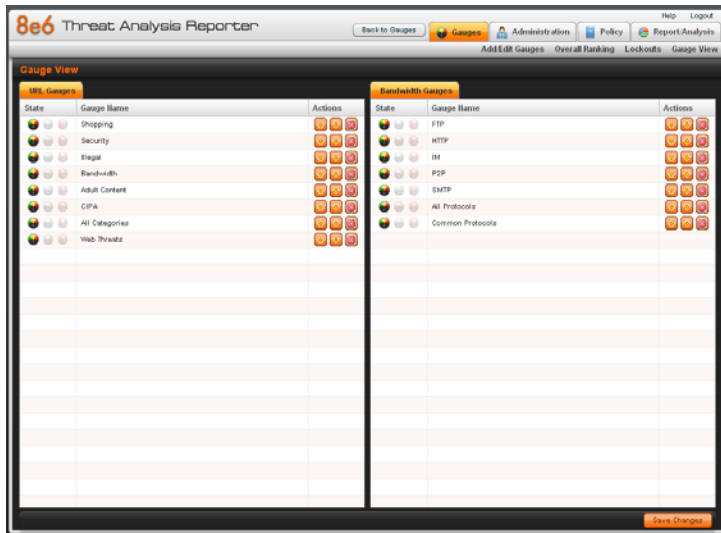
Fig. 3:2-8 Gauge View panel

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

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

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

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

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

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

• Gauge Name - The name given to the gauge.

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

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

Hide a gauge

To hide a gauge from displaying in the dashboard:

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

2. In the State column, click the icon in the second column (Hide Gauge) to change the gauge's status to "hidden."

Disable a gauge

To disable a gauge:

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

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

Show a gauge

To re-display a gauge in the dashboard again:

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

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

Rearrange the gauge display in the dashboard

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

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

2. In the Actions column, perform any of the following actions:

- Click the "up" arrow icon in the first column to move the Gauge Name up one row in this tab, and one position forward in the dashboard.
- Click the "down" arrow icon in the second column to move the Gauge Name down one row in this tab, and one position backward in the dashboard.

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

Delete a gauge

To delete a gauge:

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

2. In the Actions column, click the "X" icon in the far right column to open the Confirm dialogue box with the message: "Deleting this gauge will remove all alerts that are associated with this gauge. Are you sure you want to delete this gauge?"

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

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

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

View End User Gauge Activity

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

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

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

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

View Overall Ranking

1. In the navigation toolbar, with the Gauges tab selected, click **Overall Ranking** to open the Overall Ranking panel:
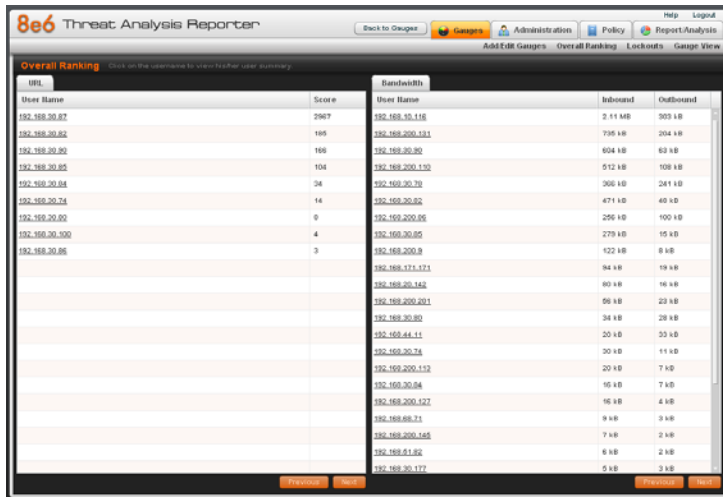
Fig. 3:2-9 Overall Ranking panel

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

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

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

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

View a Gauge Ranking table

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

Fig. 3:2-10 Gauge Ranking table

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

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

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

• Access the User Summary panel by clicking the **User Name** (see Monitor, Restrict End User Activity: View User Summary data). In the User Summary panel, you can view URLs visited by the end user and lock out that user from accessing designated areas of the Internet/network.

• Access the Threat View User panel by clicking a user's score for a gauge (see Monitor, Restrict End User Activity: Access the Threat View User panel). In the Threat View User panel, you view current details for the gauge.

Monitor, Restrict End User Activity

View User Summary data

The User Summary panel contains the following frames:

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

- Gauge Readings frame to the right that includes the URL Gauges and Bandwidth Gauges tabs, each showing the Gauge Name and end user's Total score for each gauge in the dashboard.
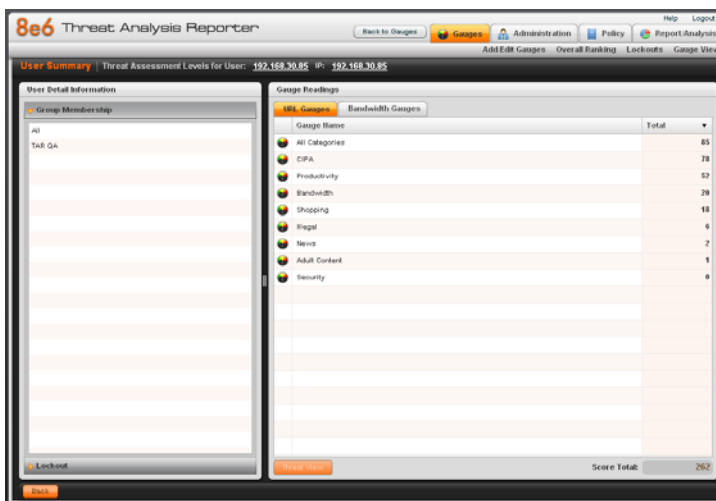
Fig. 3:2-11 User Summary panel

In this panel you can perform the following actions:

- Access the Threat View User panel to see which of the gauge's library categories/ports the end user accessed and the score (see Access the Threat View User panel).

- Access the Lockout option to lock out the end user from specified Internet/network privileges (see Manually lock out an end user).

Access the Threat View User panel

1. In the User Summary panel, make sure the appropriate tab (URL Gauges or Bandwidth Gauges) is selected, then click a Gauge Name with a score to activate the Threat View button.

2. Click **Threat View** to display the Threat View User panel which includes criteria that is based on the type of gauges to be viewed (URL or bandwidth).

URL Gauges tab selection

For URL gauges, the Threat View User panel displays the Threats frames to the left, showing a list of current library category Threats and the Total score of each threat for that end user. The target URLs frame displays to the right.

1. Select a Threat from the list, which populates the URLs frame with URLs accessed by that end user for that threat:

Fig. 3:2-12 Threat View User panel for URL Gauges tab selection

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

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

Bandwidth Gauges tab selection

For Bandwidth gauges, the Threat View User panel contains the Threats frame showing the Ports column and corresponding Inbound/Outbound bandwidth usage by the end user for that port, and the combined Total inbound and outbound bandwidth usage by the end user for that port:
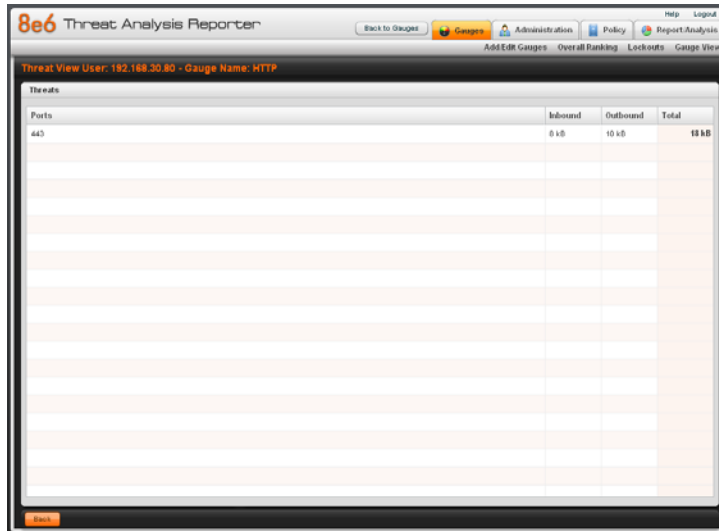
Fig. 3:2-13 Threat View User panel for Bandwidth Gauges tab selection

Manually lock out an end user

1. In the User Summary panel, in the User Detail Summary frame, click the Lockout accordion to open it:
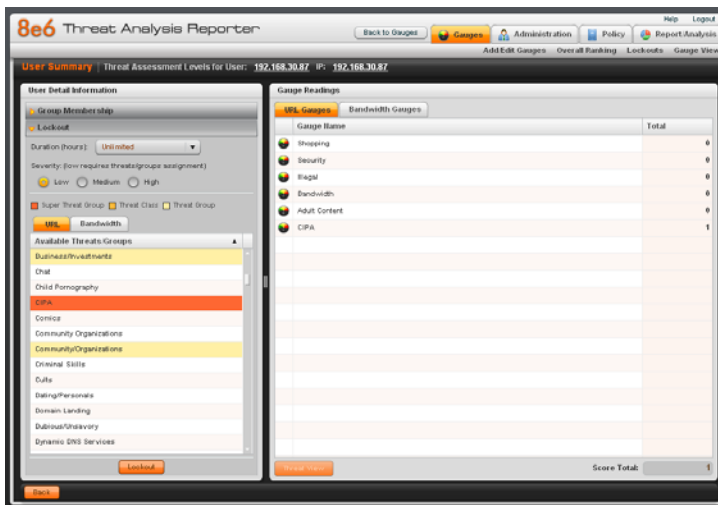
Fig. 3:2-14 User Summary panel, Lockout accordion expanded

2. Specify the **Duration** of the lockout from the choices in the pull-down menu (Unlimited, Half Hour, 1, 1-1/2 ... 8).

NOTES: If "Unlimited" is selected, the end user remains locked out of the specified areas on the Internet/network until the administrator unlocks his/her workstation. To "unlock" the end user, go to the Gauges > Lockouts panel. For information on this feature, see Chapter 3: Alerts, Lockout Management.

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

   • **Low** - This selection lets you choose which library categories/ports the end user will not be able to access (see Low severity lockout).

   • **Medium** - This selection locks out the end user from Internet access (see Medium and High severity lockout).

- **High** - This selection locks out the end user from all network access (see Medium and High severity lockout).

4. After performing the additional steps based on the chosen lockout Severity level, click **Lockout** at the bottom of the frame to open the Info alert box with the message: "This user has been locked out."

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

Low severity lockout

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

- If using the URL tab, choose the library category/categories from the list. Up to 15 categories or one threat group/class can be added.

- If using the Bandwidth tab, make a selection from the protocols in the list.

  You can also enter a port number in the **Port Number** field, or modify the value in that field by clicking the up/down arrows to increment/decrement the current value by one, and then click **add port >** to include the port number in the Assigned Threats/Groups frame. Up to 15 port numbers can be added.

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

Medium and High severity lockout

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

End user workstation lockout

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

Low severity URL lockout

In a low severity URL lockout, when an end user attains the User Threshold established for a gauge, and that end user attempts to access a URL for a library category set up to be monitored by that gauge, the following lockout page displays for the end user:
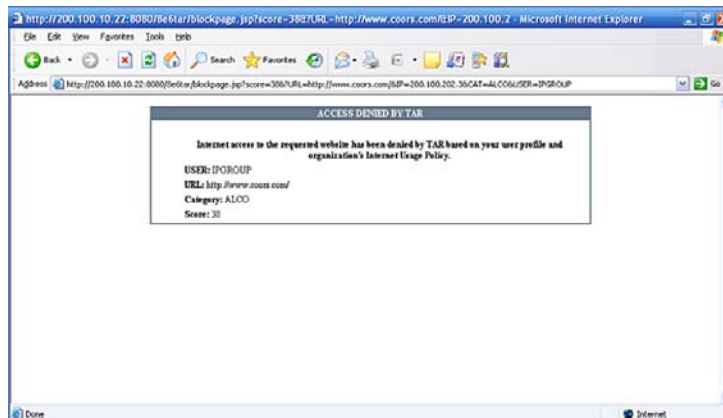
Fig. 3:2-15 Low severity URL lockout page

This page contains the following information: header "ACCESS DENIED BY TAR", USER name/IP address, the URL that was denied access, Category in which the URL resides, and the end user's Score.

Medium severity URL and bandwidth lockout

In a medium severity URL or bandwidth lockout, when an end user attains the User Threshold established for a gauge, and that end user attempts to access a threat category/port or threat group set up to be monitored by that gauge, the following lockout page displays for the end user:
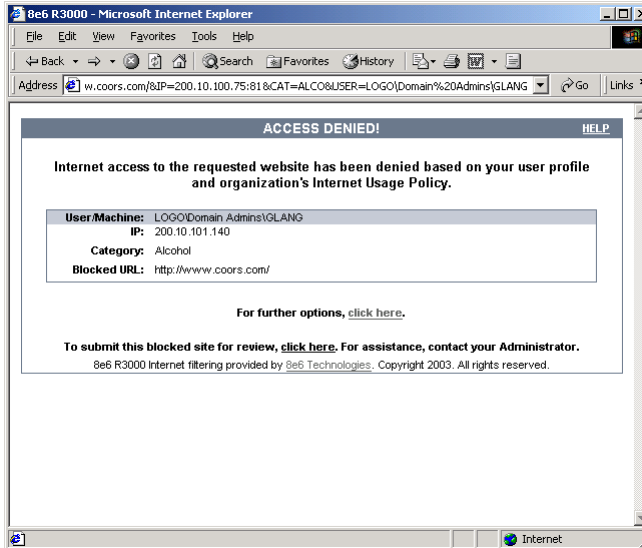
Fig. 3:2-16 Medium severity lockout page

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

By default, the following standard links are included in the block page: HELP; 8e6 Technologies; For further options, click here; To submit this blocked site for review, click here.

NOTE: Please refer to the R3000 User Guide for information about fields in the block page and how to use them.

Low/high bandwidth, high severity URL lockout

In a low severity bandwidth or high severity URL or band-width lockout, when an end user attains the User Threshold established for a gauge, and that end user attempts to access a URL for a threat category/port or threat group set up to be monitored by that gauge, the following lockout page displays for the end user:
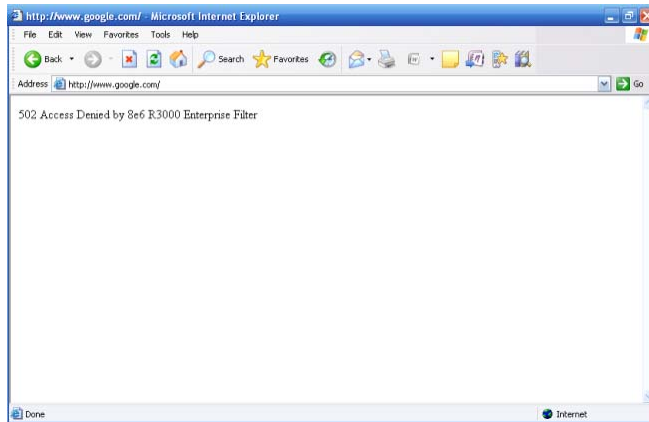
Fig. 3:2-17 Low severity bandwidth, high severity lockout page

This page contains the following information: "502 Access Denied by 8e6 R3000 Enterprise Filter".

Chapter 3: Alerts, Lockout Management

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

These functions are available to a group administrator only if permissions were granted by the administrator who set up his/her account, as detailed in Chapters 2 and 3 of the Preliminary Setup Section.

1. In the navigation toolbar, with the Policy tab selected, click **Alerts** to open the Alerts panel:
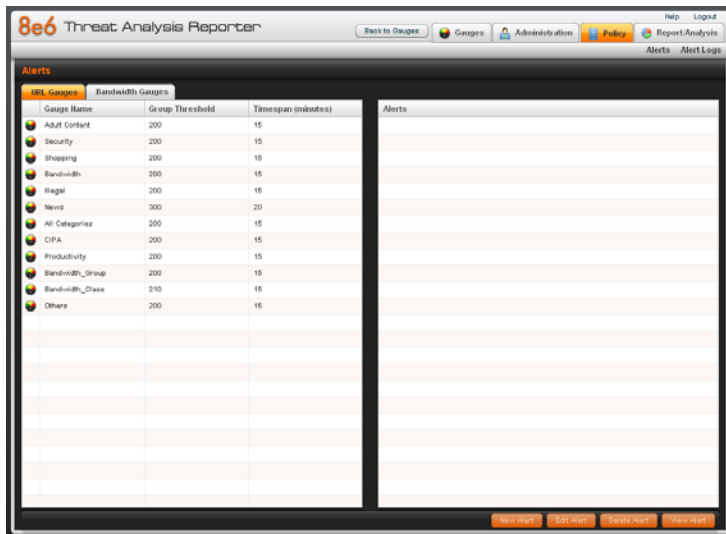
Fig. 3:3-1 Alerts panel

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

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

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

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

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

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

Add an Alert

1. From the left frame, select the gauge for which an alert will be created; this action activates the New Alert button.

2. Click **New Alert** to open the panel for that gauge:
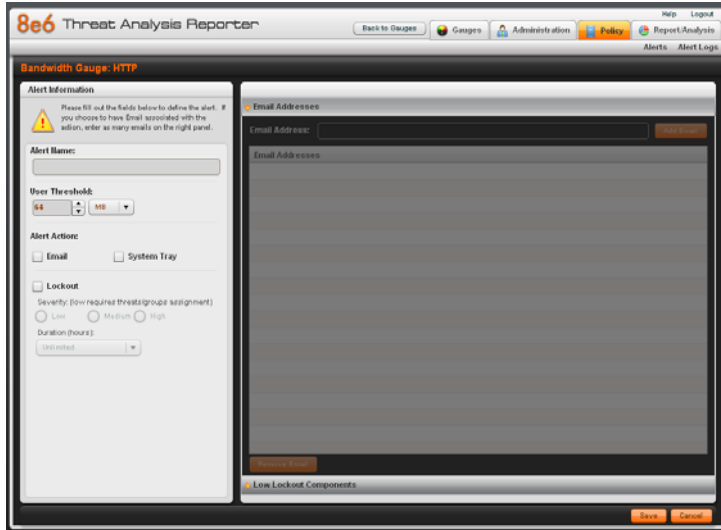
Fig. 3:3-2 Add a new Alert

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

3. In the Alert Information frame, type in the **Alert Name** to be used for the alert that will be delivered to the group administrator.

4. Specify the **User Threshold** ceiling of gauge activity that will trigger the alert.

NOTE: An alert is triggered for any end user whose current score for a gauge matches the designated threshold limit. (See How to Read a Gauge in Chapter 1 of this section for information on how scoring is defined.)

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

   • **Email** - An email alert notifies a group administrator via email if an end user has reached the threshold limit set up in a gauge alert.

   • **System Tray** - A TAR Alert message notifies a group administrator via his/her workstation's System Tray if an end user has reached the threshold limit set up in a gauge alert.

   • **Lockout** - The Lockout function locks out an end user from Internet/network access if he/she reaches the threshold limit set up in a gauge alert.

NOTE: The System Tray alert feature is only available for an administrator with an Active Directory LDAP account, user name, and domain, and is not available if using IP groups.

6. After making all entries in this panel, click **Save** to save your entries and to activate your alert.

Email alert function

Configure email alerts

To set up the email alert function:

1. In the Alert Action section of the Alert Information frame, click the checkbox corresponding to **Email** to open the Email Addresses accordion in the target frame to the right.

2. Type in the **Email Address**.

3. Click **Add Email** to include the address in the Email Addresses list box.

   Follow steps 2 and 3 for each email address to be sent an alert.

TIP: To remove an email address from the list box, select the email address and then click Remove Email. Click Submit to save your settings.

Receive email alerts

If an alert is triggered, an email message is sent to the mailbox address(es) specified. This message includes the following information:

- Subject: Alert triggered by user (user name/IP address).

- Body of message: User (user name/IP address) has triggered the (Alert Name) alert with a threshold of 'X' (in which "X" represents the alert threshold) on the (gauge name) gauge.

  Beneath this information, the date and time (YYYY-MM-DD HH:MM:SS), and clickable URL display for each URL accessed by the user that triggered this alert.

System Tray alert function

If using LDAP with an Active Directory user name, account, and domain, to set up the feature for System Tray alerts, click the checkbox corresponding to **System Tray** and follow the instructions in Appendix B: System Tray Alerts: Setup, Usage.

NOTE: In order to use this feature, the LDAP User Name and Domain set up in the administrator's profile account (see Chapter 3 in the Preliminary Setup Section) must be the same ones he/she uses when logging into his/her workstation.

Lockout function

To set up the lockout function:

1. Click the checkbox corresponding to **Lockout** to activate the Severity and Duration (hours) fields.

2. Specify the **Severity** of the end users' lockout:

   • **Low** - Choosing this option opens the Low Lockout Components accordion containing the Available Threats/Groups and Assigned Threats/Groups frames.

   Select the library category/categories or protocol(s) the end user should not access.

   For bandwidth gauges, to specify a port number the user should not access, type a specific value in the **Port Number** field, and/or use the up/down arrow buttons to increment/decrement the current value by one.

   Click **add >** (for URL gauges) or **add port >** (for bandwidth gauges) to move the selection(s) to the Assigned Threats/Groups list box.

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

   • **Medium** - Choosing this option will lock out an end user from Internet access if he/she reaches the threshold limit set up for the gauge.

   • **High** - Choosing this option will lock out an end user from network access if he/she reaches the threshold limit set up for the gauge.

3. Specify the **Duration (hours)** of the end users' lockout: Unlimited, Half Hour, 1, 1-1/2 ... 8.

   NOTE: If "Unlimited" is specified, the end user will remain locked out from Internet/network access until the group administrator unlocks his/her workstation using the Gauges > Lockouts panel.

> **TIP**: After making your selections, click **Save** to save your settings.

View, Modify, Delete an Alert

1. In the Alerts panel, select the URL Gauges or Bandwidth Gauges tab.

2. Select the gauge for which an alert will be viewed and/or modified. This action populates the Alerts frame list box with any existing alerts created for that gauge.

3. Select the alert to be viewed or modified by clicking on it to highlight it; this action activates all buttons below the Alerts frame (Add Alert, Edit Alert, Delete Alert, View Alert):
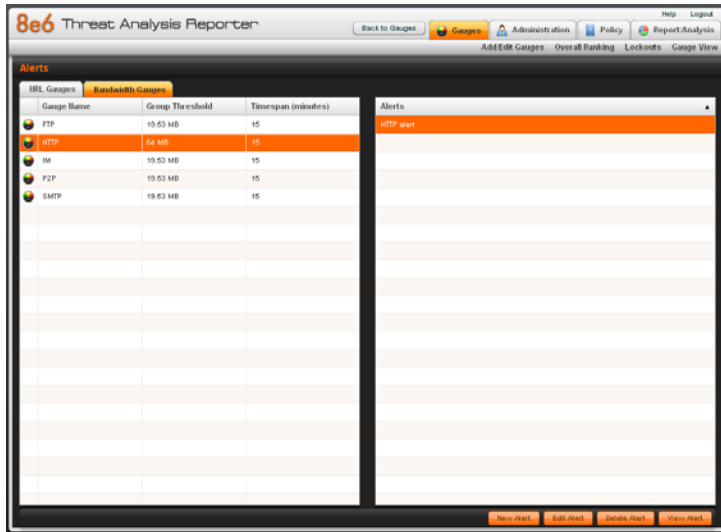
Fig. 3:3-3 Alert added

View alert settings

1. Beneath the Alerts frame, click **View Alert** to open the alert viewer pop-up window:

Fig. 3:3-4 View an alert

The following information displays to the left of this window:

- User Threshold amount
- Alert Action criteria (yes/no): Email, System Tray
- Lockout (yes/no)
- Severity (Low, Medium, High)
- Duration (hours)

To the right of this window, the Email Addresses and Low Lockout Components accordions display. Click an accordion to expand it, and view the contents—if any—within that accordion.

NOTE: The System Tray alert feature is only available if using Active Directory LDAP, and is not available if using IP groups.

2. Click the "X" in the upper right corner of the alert viewer pop-up window to close it.

Modify an alert

1. In the Alerts panel, click the URL Gauges or Bandwidth Gauges tab.

2. Select the gauge from the list to populate the Alerts frame with alerts for that gauge, and to activate all buttons beneath the frame.

3. Click **Edit Alert** to open the edit Alert panel:
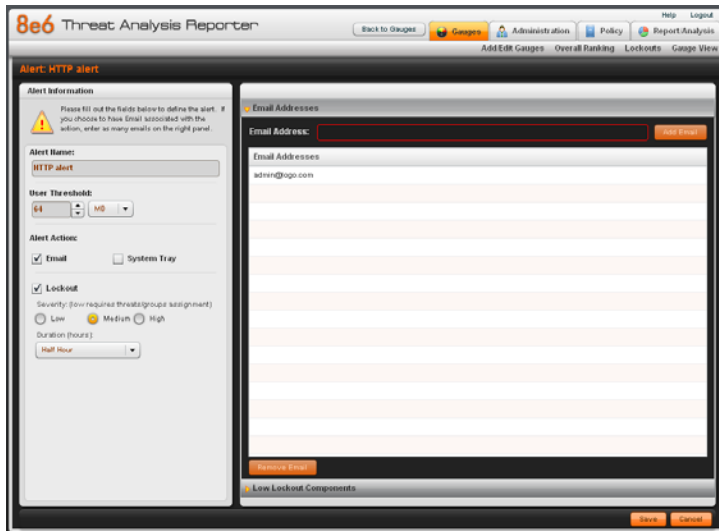
Fig. 3:3-5 Edit an alert

4. The following items can be edited:

- Alert Name
- User Threshold
- Alert Action selections: Email, System Tray—the latter is only functional for Active Directory LDAP—and Lockout
- Lockout Severity selection (Low, Medium, High)
- Duration (hours) selection
- Email Addresses
- Low Lockout Components

5. Click **Save** to save your edits, and to return to the main Alerts panel.

Delete an alert

1. In the Alerts panel, click the URL Gauges or Bandwidth Gauges tab.

2. Select the gauge from the list to populate the Alerts frame with alerts for that gauge, and to activate all buttons beneath the frame.

3. Click **Delete Alert** to open the Confirm dialog box with the message: "Are you sure you want to delete this alert?"

NOTE: Clicking No closes the dialog box without removing the alert, and returns you to the main Alerts panel.

4. Click **Yes** to close the Confirm dialog box and to remove the alert from the list.

View the Alert Log

After alerts are sent to an administrator, a list of alert activity is available for viewing in the Alert Logs panel.

1. In the navigation toolbar, with the Policy tab selected, click **Alert Logs** to open the Alert Logs panel.

2. Select the URL Gauges or Bandwidth Gauges tab to display its contents:
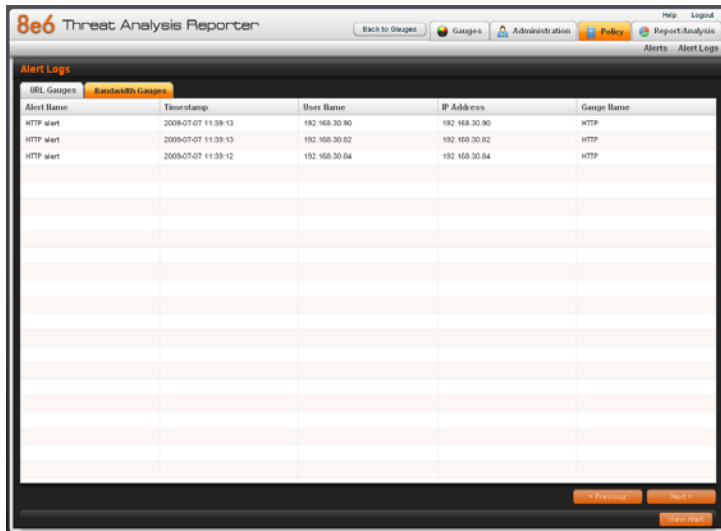
Fig. 3:3-6 Alert Logs panel

The alert log contains a list of alert records for the most recent 24-hour time period. Each record displays in a separate row. For each row in the list, the following information displays: Alert Name, Timestamp (using the YYYY-MM-DD HH:MM:SS military time format), User Name (or IP address), IP Address, Gauge Name.

NOTE: If an alert was deleted during the most recent 24-hour time period, any records associated with that alert will be removed from the alert log.

3. To view details on an alert, select the alert record in the list to highlight it.

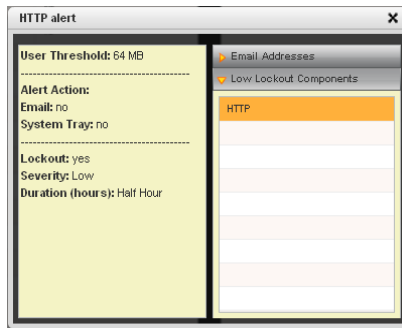4. Click **View Alert** to open the alert viewer pop-up window:
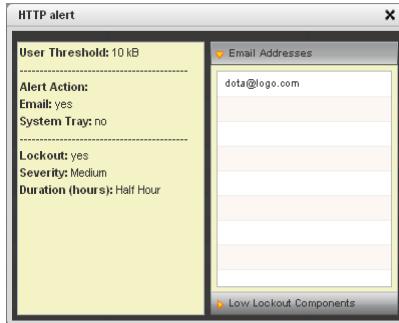
Fig. 3:3-7 View an alert

The following information displays to the left of this window:

- User Threshold amount
- Alert Action criteria (yes/no): Email, System Tray
- Lockout (yes/no)
- Severity (Low, Medium, High)
- Duration (hours)

To the right of this window, the Email Addresses and Low Lockout Components accordions display. Click an accordion to expand it, and view the contents—if any—within that accordion.

5. Click the "X" in the upper right corner of alert viewer pop-up window to close it.

Manage the Lockout List

An end user who is manually or automatically locked out for an "Unlimited" period of time—from accessing designated content on the Internet or using the network—can only have his/her workstation unlocked by an administrator.

To view the current lockout list:

1. In the navigation toolbar, with the Gauges tab selected, click **Lockouts** to open the Lockouts panel.

2. Select the URL Gauges or Bandwidth Gauges tab to display its contents:
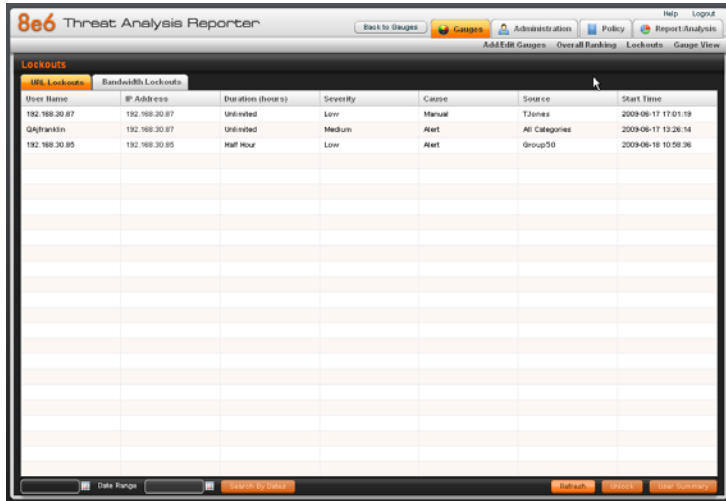
Fig. 3:3-8 View Lockouts

The lockout list contains records for all end users currently locked out of the Internet/network. Each end user's record displays in a separate row. For each row in the list, the following information displays: User Name (or IP address); IP address; Duration (hours); Severity of the lockout (Low, Medium, High); Cause of the lockout (Manual, Automatic); Source of the lockout (user name of the administrator who locked out the end user in a

Manual lockout, or name of the alert in an Automatic lockout); Start Time for the alert (using the YYYY-MM-DD HH:MM:SS format).

View a specified time period of lockouts

If the lockout list is populated with many records, using the Date Range feature will only show you records within the range of dates you specify.

1. At the **Date Range** field, click the 🔲 calendar icon located to the right of the first date field; this action opens the larger calendar for the current month, with today's date highlighted:

💡 *TIP: To view the calendar for the previous month, click the left arrow at the top left of the box. To view the calendar for the next month, click the right arrow at the top right of the box.*

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

3. At the **Date Range** field, click the 🔲 calendar icon located to the right of the second date field; this action opens the larger calendar for the current month, with today's date highlighted.

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

5. Click **Search By Dates** to display records for only the selected dates.

TIP: Click Refresh to clear all records returned by the search query, and to display the default records (all lockout records) in the panel.

Unlock workstations

1. In the populated Lockouts panel, click each record to highlight it.

2. Click **Unlock** to unlock the end user(s) and to remove the record(s) from the list.

NOTE: By unlocking an end user's workstation, all records in this list pertaining to that end user are removed from the list.

Access User Summary details

1. To access details about an end user's online activity, first click the user's record to highlight it.

2. Next, click **User Summary** to display the User Summary panel where you can monitor that end user's online activity and lock him/her out of designated areas of the Internet/network. (See Monitor, Restrict End User Activity in Chapter 2 of the Configuration Section for details about using the User Summary panel.)

Chapter 4: Analyze Usage Trends

When analyzing end user Internet usage trends, trend charts help you configure gauges and alerts so you can focus on current traffic areas most affecting the network.

If more information is required in your analysis, the R3000's Real Time Probe tool—or the Enterprise Reporter's Web Client, if the ER server is installed and connected to your R3000—can be accessed via the TAR interface so you can generate customized reports to run for a time period of your specifications.

These functions are available to a group administrator only if permissions were granted by the administrator who set up his/her account, as detailed in Chapters 2 and 3 of the Preliminary Setup Section.

View Trend Charts

There are three basic types of trend charts that can be generated on demand to show total gauge score averages for a specified, limited time period:

- Pie trend chart for an individual URL or bandwidth gauge

- Pie trend chart for all collective URL or bandwidth gauges

- Line chart showing details for a pie chart

View activity for an individual gauge

To view activity for any individual URL or bandwidth gauge:

1. If the gauges dashboard does not currently display, click **Back to Gauges** in the navigation toolbar.

2. Be sure the dashboard of your choice (URL or Bandwidth gauges) displays. If not, click the URL or Bandwidth button above the dashboard to display the dashboard of your choice.

3. Find the gauge for which the trend chart will be generated, and then click the Trend Charts icon at the bottom middle of that gauge:

This action of clicking the Trend Charts icon displays the Gauge Trend Chart panel:
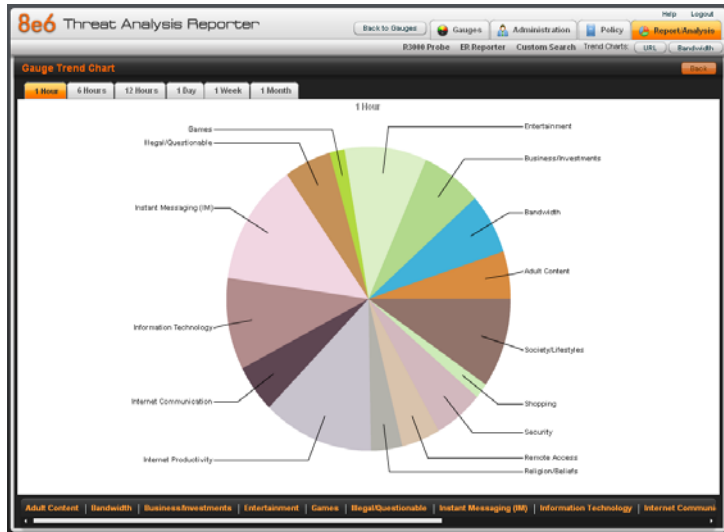
Fig. 3:4-1 Pie trend chart for an individual URL gauge

The pie trend chart that displays in the middle of this panel includes the following information:

- For a URL gauge - By default, each slice of the pie represents the percentage of end user hits in a library category during the last hour; the total for all categories in that gauge equaling 100 percent.

- For a Bandwidth gauge - By default, each slice of the pie represents the percentage of end user traffic for a port during the last hour; the total for all ports in that gauge equaling 100 percent.

The top and bottom sections of this panel contain tabs.

Information about all actions that can be performed in this panel appears in the Navigate a trend chart sub-section.

View overall gauge activity

1. In the navigation toolbar, with the Report/Analysis tab selected, go to the Trend Charts option.

2. Click either the **URL** or **Bandwidth** button to display the Overall Trend Chart panel for the specified gauge type (URL or Bandwidth):
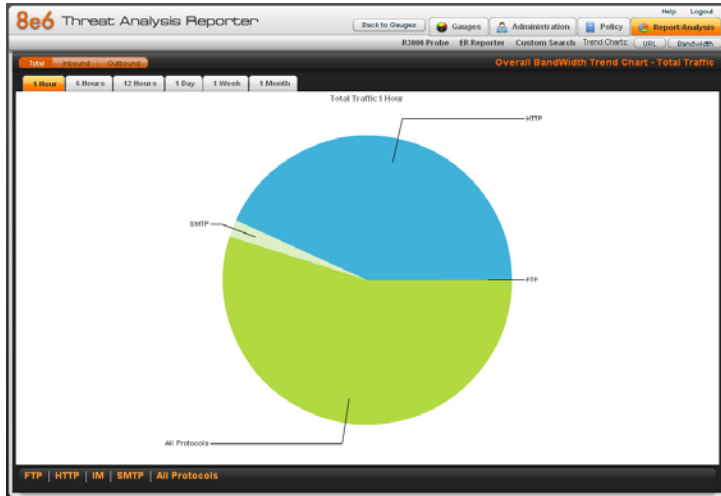
Fig. 3:4-2 Overall Bandwidth Trend Chart, Total Traffic

The pie trend chart that displays in the middle of this panel includes the following information:

- For URL gauges - By default, each slice of the pie represents that URL gauge's percentage of end user scores during the last hour; the total for all URL gauges in the dashboard equaling 100 percent.

- For Bandwidth gauges - By default, each slice of the pie represents that bandwidth gauge's percentage of end user traffic during the last hour; the total for all bandwidth gauges in the dashboard equaling 100 percent.

The top and bottom sections of this panel contains tabs. For the bandwidth trend chart, buttons display above this panel.

Information about all actions that can be performed in this panel appears in the Navigate a trend chart sub-section.

Navigate a trend chart

The following actions can be performed in this panel:

- View gauge activity for a different time period (1 Hour, 6 Hours, 12 Hours, 1 Day, 1 Week, 1 Month)

- Analyze gauge activity in a pie chart

- Analyze gauge activity in a line chart

- View Inbound, Outbound bandwidth gauge activity

- Print a trend chart from an IE browser window

View gauge activity for a different time period

To view a pie chart showing activity for a different time period of gauge activity, click the appropriate tab above the pie chart diagram:

- **1 Hour** - This selection displays the gauge URL/byte average score in 10 minute increments for the past 60-minute time period

- **6 Hours** - This selection displays the gauge URL/byte average score in 30 minute increments for the past six-hour time period

- **12 Hours** - This selection displays the gauge URL/byte average score in one hour increments for the past 12-hour time period

- **1 Day** - This selection displays the gauge URL/byte average score in one hour increments for the past 24-hour time period

- **1 Week** - This selection displays the gauge URL/byte average score in 12 hour increments for the past seven-day time period

- **1 Month** - This selection displays the gauge URL/byte average score in one-day increments for the past month's time period

Once you've selected the time period you wish to view, you can analyze the activity for that gauge (see Analyze gauge activity in a pie chart), and drill down into a slice of the pie to view a line chart for that given time period (see Analyze gauge activity in a line chart).

Analyze gauge activity in a pie chart

Once a pie chart displays in the panel, its pieces can be analyzed by mousing over that slice of the pie chart:
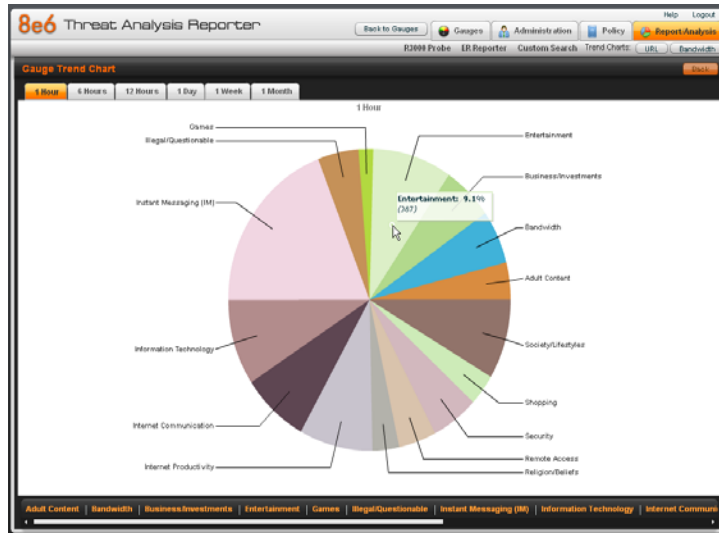

Fig. 3:4-3 Pie Gauge Trend Chart slice

The following information displays for that pie slice: gauge component name, percentage of that pie slice (based on a total of 100 percent for all pie slices), and total end user score for that pie slice.

That slice of the pie can be further analyzed by drilling down into it (see Analyze gauge activity in a line chart).

Analyze gauge activity in a line chart

1. To view a line chart showing activity for a slice of the pie chart, do either of the following:

   • Click that slice of the pie chart

   • Click the specified tab beneath the pie chart

   Either action displays the line Trend Chart:
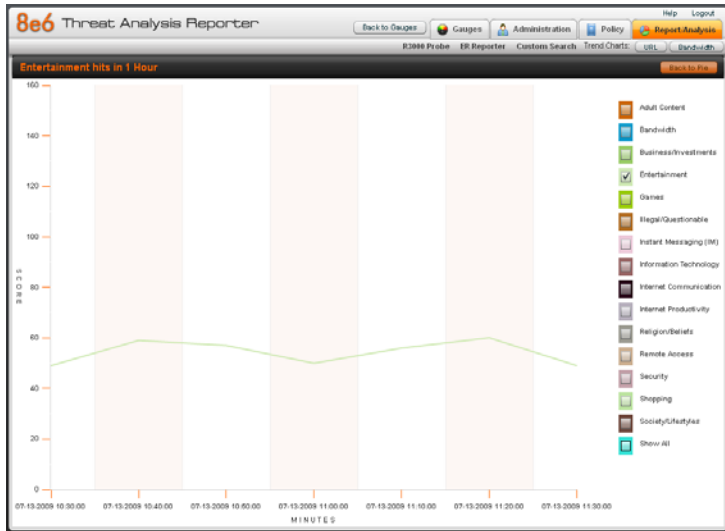
Fig. 3:4-4 Drill into a pie slice to display a line Trend Chart

By default, this chart contains the following information: linear depiction of the total end user SCORE in fixed time increments (using the MM-DD-YYYY HH:MM:SS format) for MINUTES included in the specified time period for the gauge component, and the checkbox populated for the selected library category/protocol/port.

NOTE: See View gauge activity for a different time period for a definition of MINUTES included in the current chart.

2. Perform any of the following actions in this chart:

- To include other gauge component activity in this line chart, click the checkboxes corresponding to the gauge names.

TIP: *Click a populated checkbox to remove the check mark and the line showing activity for that gauge.*

- To view information about a specific point in the line chart, mouse over that point in the chart:
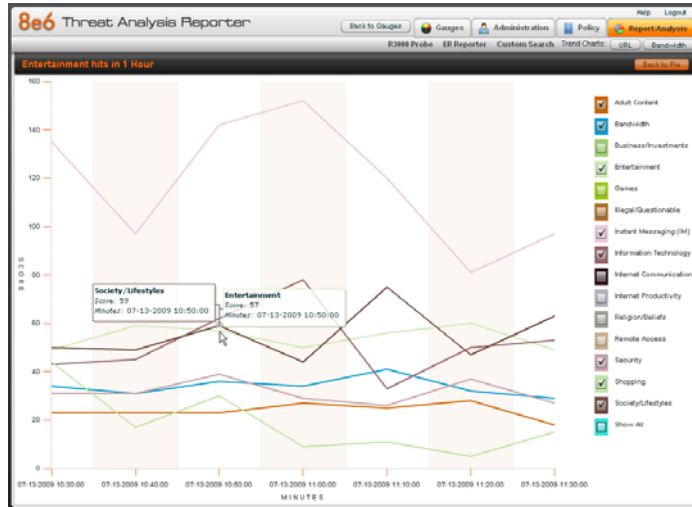
Fig. 3:4-5 Line Trend Chart data

If the chart includes more than one line, and more than one point is located in the area of the mouse pointer, a separate box appears for each point in that section of the chart.

Each box includes the following information: gauge component name, Score for that point, and Minutes for that fixed time increment (using the MM-DD-YYYY HH:MM:SS format).

- To return to the pie chart, click **Back to Pie** in the upper right portion of the panel.

- To print this trend chart, if using an IE browser, see Print a trend chart from an IE browser window.

View In/Outbound bandwidth gauge activity

To view either Inbound or Outbound activity in an Overall Bandwidth Trend Chart, click the **Inbound** or **Outbound** above the pie chart to the right of the Total button.

Print a trend chart from an IE browser window

A trend chart can be printed from an IE browser window by using the browser window's toolbar and going to **File > Print** and proceeding with the print commands.

Access Real Time Probe, Web Client

R3000 Real Time Probe reports can be generated to obtain more information about end user Internet usage trends. If an ER server is connected to the R3000, ER Web Client reports can be generated for viewing historical Internet usage trend data.

Access the R3000 Real Time Probe tool

In the navigation toolbar, with the Report/Analysis tab selected, click **R3000 Probe** to launch the login window of the R3000 Real Time Probe interface.

NOTE: See the Reporting screen chapter from the Global Administrator Section of the R3000 User Guide for information on configuring and using Real Time Probes.

Access the ER Web Client application

In the navigation toolbar, with the Report/Analysis tab selected, click **ER Reporter** to launch the login window of the ER Web Client application.

Chapter 5: Identify Users, Threats

If there are certain end users who are generating excessive, unwanted traffic on the network, or if some library categories containing URLs against your organization's policies are persistently being frequented, you can target offending entities by performing a custom search to identify which users, URLs, and port are being accessed.

Perform a Custom Search

In the navigation toolbar, with the Report/Analysis tab selected, click **Custom Search** to display the Custom Search panel:
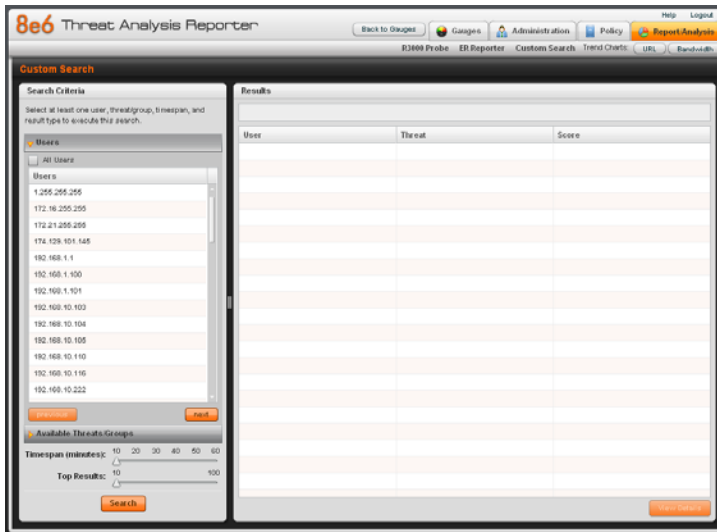

Fig. 3:5-1 Custom Search, Users accordion opened

This panel displays the Search Criteria frame to the left with the open Users accordion and closed Available Threats/ Groups accordion, Timespan and Top Results sliders, Search button; and to the right, the empty Results target frame.

Specify Search Criteria

1. In the **Users** accordion, do one of the following:

   - To identify users with the highest scores - Click the **All Users** checkbox to select all users in the list and to grey-out the list.

   - To identify the activities of a specific user - Select the user name/IP address from the list to highlight it.

2. Click the Available Threats/Groups accordion to open it.

3. Select either the **URL Threats** or **Bandwidth Threats** tab to display its list of library categories/protocols, and do either of the following:

   - To identify library categories or protocols with the highest scores - Select a category group or protocol that includes as many of categories/ports as possible.

   - To identify activities for a specific threat class/group - Select that threat class or group.

     For bandwidth gauges, to query activities for a specific port number, click the **Port Number** checkbox to activate the port field and to deactivate the listed bandwidth protocol selections. Type a specific value in the pre-populated field, and/or use the up/down arrow buttons to increment/decrement the current value by one.

4. Use the **Timespan (Minutes)** slider to specify the time period in which the threat(s)/group(s) were accessed: last 10, 20, 30, 40, 50, 60 minutes.

5. If a user selection other than "All Users" was specified in the Users accordion, the **Top Results** slide becomes activated and you can make a selection for the maximum number of records to return in the results for that user: top 10, 20, 30, 40, 50, 60, 70, 80, 90, 100 records.

6. Click **Search** to display records returned by the query in the Results frame at the right side of the panel:
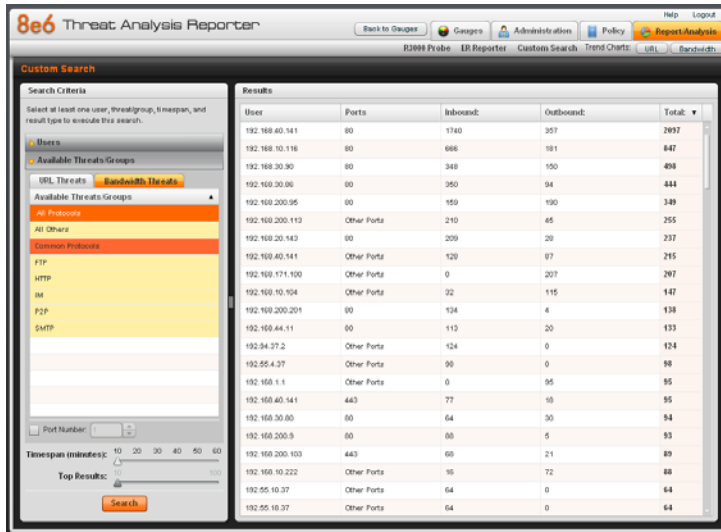
Fig. 3:5-2 Custom Search results for Bandwidth Threats

For each record in the table, the following information displays:

- For a URL search - User (user name/IP address), Threat name, and the end user's total Score for that record.

- For a bandwidth search - User (user name/IP address), Ports number, Inbound score, Outbound score, and the end user's Total score for that record.

For a URL search, you can drill down even further by selecting a user's record and then viewing the URLs that user accessed (see View URLs within the accessed category).

View URLs within the accessed category

In the Results frame, do the following to view a specific URL:

1. Click the User name/IP address to highlight that user's record and to activate the View Details button.

2. Click **View Details** to display a list of URLs and corresponding Timestamp (using the YYYY-MM-DD HH:MM:SS format) for each URL in the library category accessed by the end user within the specified time period:

Fig. 3:5-3 List of URLs visited by the user

💡 *TIP*: *Click Back to results to return to the previous page where you can perform another query.*

You can now print the results displayed in this window if using an IE browser window, or access another selected URL.

ADMINISTRATION SECTION

Introduction

The Administration Section of this user guide is comprised of six chapters with instructions on maintaining the TAR server or its database.

NOTES: *As part of the maintenance procedures, the TAR server will dispatch an email message to the global administrator—whose email address was supplied during the TAR Wizard installation procedures—if there is any potential system error on TAR.*

See Appendix C for information about using the Hardware Detector panel to troubleshoot RAID on a TAR "SL", "HL", or "H" server.

- Chapter 1: View the User Profiles List - This chapter explains the options for viewing end user information comprising the User Profiles list.

- Chapter 2: View Administrator Activity - This chapter explains how to view activity performed on TAR by the global or group administrators.

- Chapter 3: Maintain the Device Registry - This chapter provides information on viewing TAR's registry of associated devices; synchronizing TAR with the source R3000, and adding, editing or deleting a non-source R3000 or an ER device.

- Chapter 4: Perform Backup, Restoration - This chapter explains how to perform a backup on the TAR server, and how to restore user configuration settings saved in a previous backup to the server.

- Chapter 5: Install Software Updates - This chapter explains how the global administrator installs software updates on the TAR server.

- Chapter 6: View Hard Disk Status - This chapter explains how to view the current hardware drive status on a TAR-SL, HL, or H server with RAID technology.

Chapter 1: View the User Profiles List

The User Profiles panel contains the list of users that is created when TAR first communicates with the source R3000. This list is used for verifying that the list of active end users on the source R3000 matches the list of end users on the TAR server. If there are any discrepancies, synchronization can be forced between the two servers (see Chapter 4: Maintain the Device Registry).

The User Profiles panel is available to a group administrator only if permissions were granted by the administrator who set up his/her account, as detailed in Chapters 2 and 3 of the Preliminary Setup Section.

In the navigation toolbar, with the Administration tab selected, click **User Profiles** to display the User Profiles panel:
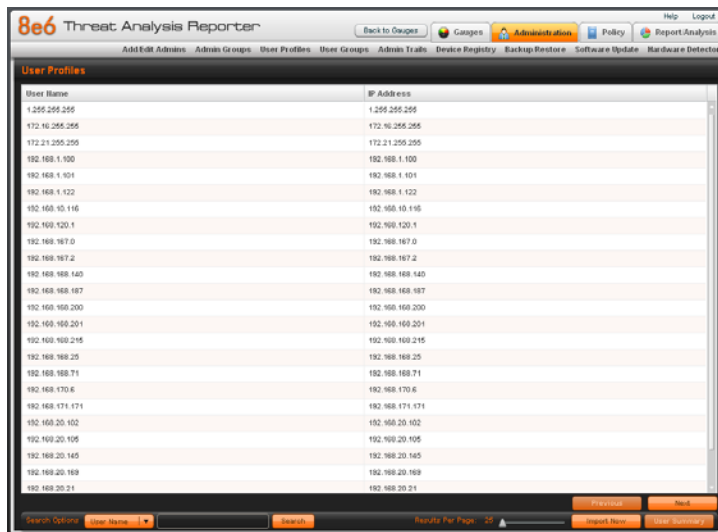
Fig. 4:1-1 View User Profiles list

By default, this panel is comprised of rows of end user records, sorted in ascending order by User Name (IP

address). For each user name in the list, the corresponding end user IP Address displays.

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

Search the User Database

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

   • **User Name** - This selection performs a search by an end user's user name.

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

2. Make an entry in the blank field to the right:

   • If User Name was selected, enter a user name

   • If IP Address was selected, enter an IP address.

3. Click **Search** to display a record that matches your criteria.

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

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

View End User Activity

1. To drill down and view additional information about an end user's activity, select the user's record to highlight it.

2. Click **User Summary** to open the User Summary panel, and perform any of the actions described for this panel (see Monitor, Restrict End User Activity in the Configuration Section, Chapter 2: Custom Gauge Setup, Usage).

Chapter 2: View Administrator Activity

The Admin Trails panel is used for viewing the most recent administrative activity performed on TAR.

In the navigation toolbar, with the Administration tab selected, click **Admin Trails** to display the Admin Trails panel:
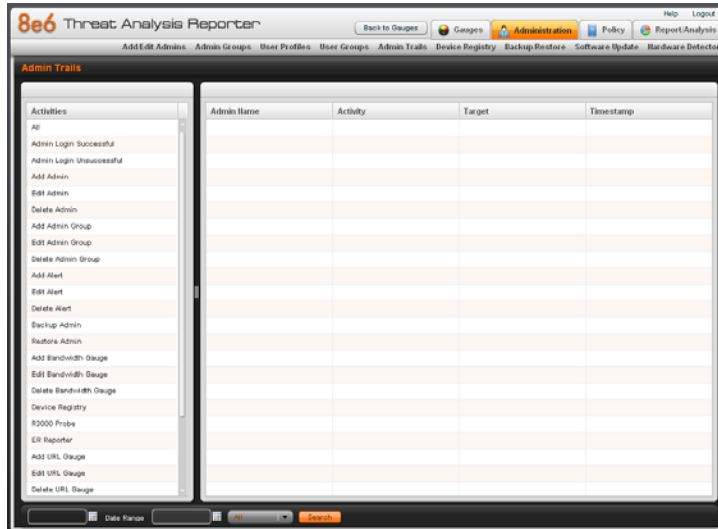
Fig. 4:2-1 Admin Trails panel

The Activity frame displays to the left and the empty target frame displays to the right. Below these frames is the Date Range field, the administrator user names menu, and Search button.

Perform a Search on a Specified Activity

To perform a search on a specified activity:

1. Select the type of Activity from available choices in the list: All, Admin Login Successful, Admin Login Unsuccessful, Add Admin, Edit Admin, Delete Admin, Add Admin Group, Edit Admin Group, Delete Admin Group, Backup Admin, Restore Admin, Add Alert, Edit Alert, Delete Alert, Add Bandwidth Gauge, Edit Bandwidth Gauge, Delete Bandwidth Gauge, Device Registry, R3000 Probe, ER Reporter, Add URL Gauge, Edit URL Gauge, Delete URL Gauge, Add User Group, Edit User Group, Delete User Group, User Profiles.

NOTE: The Activity list will only display activity types performed on TAR within the past 30 days.

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

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

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

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

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

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

7. Click **Search** to display the specified records for the selected dates in the Results list:
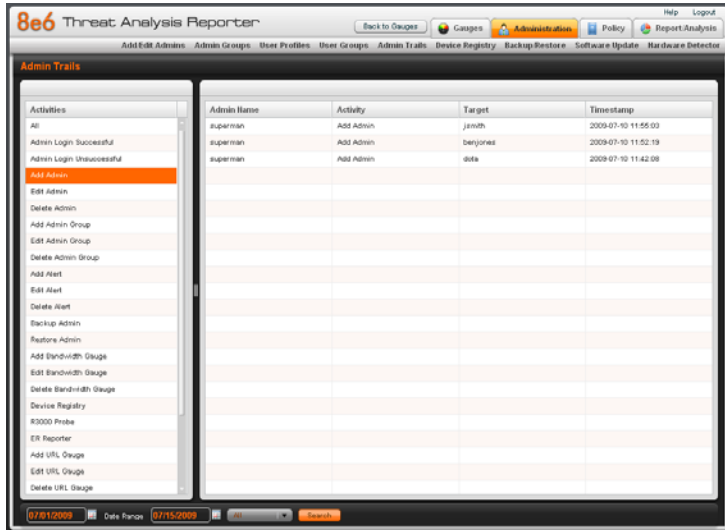
Fig. 4:2-2 Admin Trails results

Search results

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

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

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

• administrator name for Add/Edit/Delete Admin

• group name for Add/Edit/Delete Admin Group

• alert name for Add/Edit/Delete Alert

• gauge name for Add/Edit/Delete URL/Bandwidth Gauge.

Chapter 3: Maintain the Device Registry

TAR's device registry is used by the global administrator to view information about devices connected to the TAR unit, synchronize TAR with user groups and libraries from the source R3000, edit 8e6 appliance criteria, and add or delete an R3000 or ER.

in the navigation toolbar, with the Administration tab selected, click **Device Registry** to display the Device Registry panel:
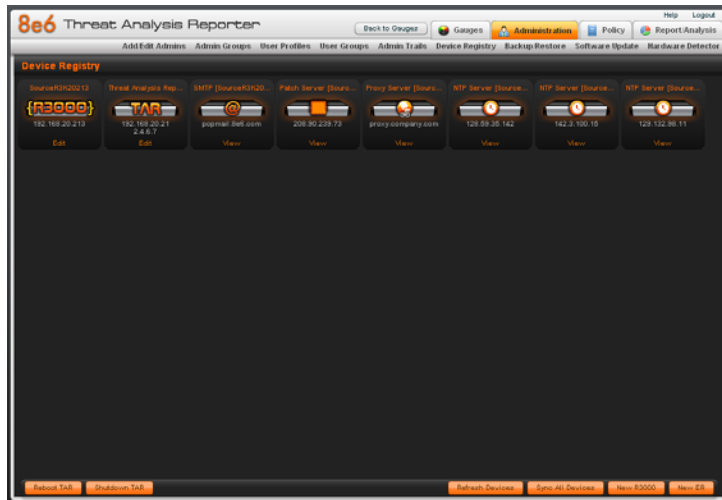
Fig. 4:3-1 Device Registry

This panel is comprised of images representing devices set up to communicate with TAR. Each device's image includes at least one link describing the action(s) that can be performed on that device: View, Edit, Delete.

At the bottom of the panel the following buttons display:

• **Reboot TAR** - Click this button to restart the TAR server.

• **Shutdown TAR** - Click this button to shut down the TAR server.

- **Refresh Devices** - Click this button if any image representing a device does not properly display in the interface.

- **Sync All Devices** - Click this button to synchronize R3000 library Categories, Source R3000 Devices, and/or User Groups.

- **New R3000** - Click this button to add another R3000 to the device registry.

- **New ER** - Click this button to add an ER server to the device registry—if an ER device is connected to the source R3000.

Restart the TAR server

1. Click **Reboot TAR** to open the REBOOT dialog box with the following message: "Restarting Threat Analysis Reporter could lose unsaved work from all users. Are you sure you want to reboot?"

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

2. Click **Yes** to proceed with that action.

Shut down the TAR server

1. Click **Shutdown TAR** to open the SHUTDOWN dialog box with the following message: "Shutting down Threat Analysis Reporter could lose unsaved work from all users. Are you sure you want to shutdown?"

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

2. Click **Yes** to proceed with that action.

R3000 Device Maintenance

View, edit R3000 device criteria

1. Go to the image of the R3000 server in the Device Registry panel, and then click **Edit** to open the R3000 pop-up window:

Fig. 4:3-2 R3000 pop-up window

The Device Type (R3000) displays and cannot be edited.

2. Edit any of the following:

- **Name** - Name of the server.
- **IP** - IP address of the server.
- **Source R3000** - If populated, this checkbox displays greyed-out. If this checkbox is not populated and the R3000 will now be the source R3000, click in the checkbox to place a check mark here.

💡 *TIP: Click **Cancel** to close this pop-up window.*

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

Add an R3000 to the device registry

1. At the bottom of the Device Registry panel, click **New R3000** to open the New R3000 pop-up window:
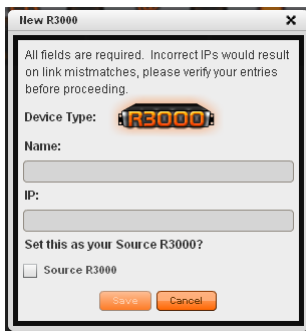
Fig. 4:3-3 New R3000 pop-up window

2. Type in the server **Name**.

3. Type in the **IP** address of the server.

4. If this R3000 will be the source server, click the **Source R3000** checkbox.

*TIP: Click **Cancel** to close this pop-up window.*

5. Click **Save** to save and process your information, and to return to the Device Registry panel where a square representing the R3000 device you added now displays.

Delete an R3000 from the device registry

1. Go to the image of the R3000 server in the Device Registry panel and click **Delete** to open the CONFIRM dialog box with the message: "Are you sure you want to delete this device?"

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

2. Click **Yes** to delete the R3000 device from the registry, and to remove the square representing that R3000 from the Device Registry panel.

TIP: A source R3000 cannot be deleted. If the current source R3000 needs to be replaced, please use the edit function to specify a different R3000 as the source server before deleting the R3000 currently designated as the source server.

Threat Analysis Reporter Maintenance

View TAR device criteria

Go to the image of the TAR server in the Device Registry panel, and then click **Edit** to open the Threat Analysis Reporter pop-up window:
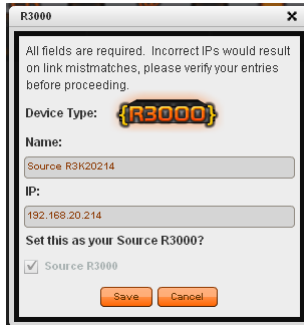

Fig. 4:3-4 Threat Analysis Reporter pop-up window

The following displays at the left side of this window: Device Type (TAR), Name of the server (Threat Analysis Reporter), and LAN1 and LAN2 IP address(es) entered during the quick start wizard process.

The following displays at the right side of this window: Bandwidth Range IP Address and Subnet Mask fields, and buttons for adding or removing a range of IP addresses the TAR server will monitor for network traffic. Any IP Address and Subnet Mask previously entered in this window displays in the list box.

Add, remove a bandwidth range

1. Do the following in the Bandwidth Range section:

   - To add a bandwidth IP address range:

     a. Type in the **IP Address**.

     b. Type in the **Subnet Mask**.

     c. Click **Add** to add the bandwidth IP range in the list box.

   - To remove a bandwidth IP address range:

     a. Select the IP address range from the list box; this action activates the Remove button.

     b. Click **Remove** to remove the IP address range.

*TIP: Click **Cancel** to close the pop-up window without saving your entries.*

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

ER Device Maintenance

If an ER is connected to the source R3000 server, this ER device should be added in the Device Registry.

Add an ER to the device registry

1. Click the **New ER** button to open the Enterprise Reporter pop-up window:
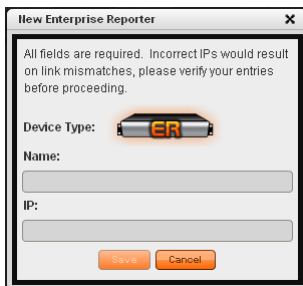
Fig. 4:3-5 Enterprise Reporter window, add

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

2. Type in the **Name** of the server.

3. Type in the **IP** address of the server.

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

4. Click **Save** to save your entries, and to return to the Device Registry panel where an image representing the ER device now displays.

NOTE: *Once the ER is added, the New ER button is greyed-out. Criteria for this ER can be edited, and the ER can be deleted from the Device Registry.*

View, edit ER device criteria

1. Go to the image of the ER server in the Device Registry panel, and then click **Edit** to open the Enterprise Reporter pop-up window:
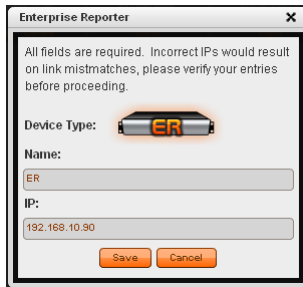
Fig. 4:3-6 Enterprise Reporter window, edit

The Device Type (Enterprise Reporter) displays and cannot be edited.

2. Edit any of the following:

   - **Name** - Name of the server.
   - **IP** - IP address of the server.

*TIP: Click **Cancel** to close this pop-up window.*

3. Click **Save** to save your edits, and to close the pop-up window.

Delete the ER device from the registry

1. Go to the image of the ER server in the Device Registry panel and click **Delete** to open the CONFIRM dialog box with the message: "Are you sure you want to delete this device?"

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

2. Click **Yes** to delete the ER device from the registry, and to remove the square representing that ER from the Device Registry panel. This action also activates the New ER button.

View Other Device Criteria

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

View SMTP device criteria

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

SMTP Server

Name: SMTP [R3K20213]
Device Type: SMTP Server
IP: popmail.logo.com
Port: 25
Username:
Password:
Authentication: false
Queue Size: 50

Fig. 4:3-7 SMTP window

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

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

View Patch Server device criteria

1. Go to the image of the Patch Server in the Device Registry panel and click **View** to open the Patch Server pop-up window. The foll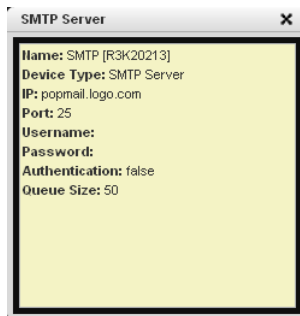owing information displays: Name of server, Device Type (Patch Server), IP address, Username (if applicable), Password (if applicable, asterisks display), HTTPS ("on" or "off"), Transfer Mode ("active" or "passive").

2. Click **Close** to close this pop-up window.

View NTP Server device criteria

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

2. Click **Close** to close this pop-up window.

View Proxy Server device criteria

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

2. Click **Close** to close this pop-up window.

Sync All Devices

A forced synchronization should be performed on the TAR unit if any of the source R3000's related devices listed in the Device Registry are updated.

1. Click **Sync All Devices** to open the Sync All Devices pop-up window:
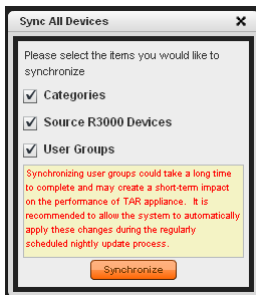
Fig. 4:3-8 Sync All Devices

2. Check the checkbox(es) pertaining to information to be synchronized between the R3000 and TAR devices, and to activate the Synchronize button:

   • **Categories** - Make this selection to synchronize 8e6 supplied library category updates and custom library categories from the source R3000 to TAR.

   • **Source R3000 Devices** - Make this selection to synchronize information from all devices tied to the source R3000 server (SMTP server, patch server, proxy server, NTP server) to TAR.

   • **User Groups** - Make this selection to synchronize LDAP user group information on the source R3000 to TAR.

TIP: *Click the "X" in the upper right corner of this pop-up window to close it.*

WARNING: *The User Groups synchronization process may be lengthy and thus may create an impact on TAR's performance.*

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

Chapter 4: Perform Backup, Restoration

The Backup/Restore panel is used for reviewing the automatic backup file list, backing up gauge configuration settings to the TAR server, or restoring such settings saved from a previous backup to the TAR server.

NOTE: Backup and restoration files include settings pertinent to the administrator who configured the gauges, and do not include other administrators' configuration settings.

These features are available to a group administrator only if permissions were granted by the administrator who set up his/her account, as detailed in Chapters 2 and 3 of the Preliminary Setup Section.

This panel is also used by the global administrator to reset the server to factory default settings, if necessary.

In the navigation toolbar, with the Administration tab selected, click **Backup/Restore** to display the Backup/Restore panel:
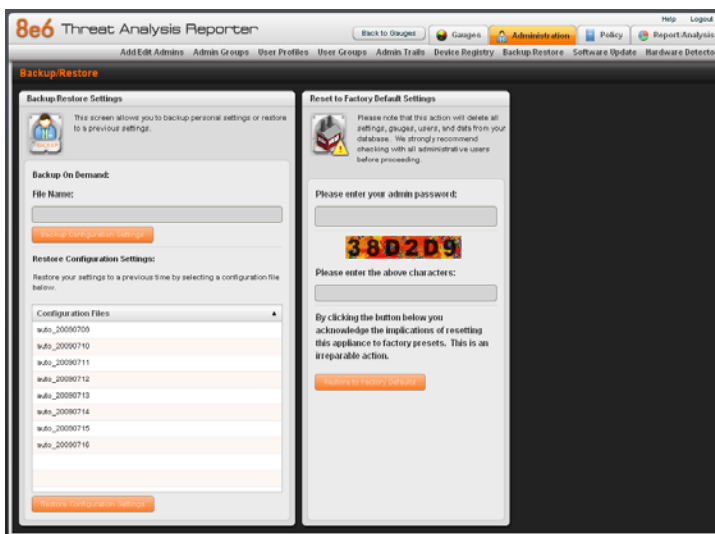

Fig. 4:4-1 Backup/Restore panel

This panel includes the Backup/Restore Settings frame to the left with the Backup On Demand and Restore Configuration Settings sections.

In the Restore Configuration Settings section, the Configuration Files box includes a list of the eight most recent automatic backup files, and any backup files created on demand by the administrator.

By default, TAR performs an automatic backup each morning at 2:00 a.m. Automatic backup files display with the characters "auto_" and use the YYYYMMDD format. For example: ***auto_20090716*** displays for an automatic backup executed on July 16, 2009.

NOTE*: In the event that TAR should fail, please contact 8e6 Technical Support to restore TAR with the most recent backup.*

The Reset to Factory Default Settings frame displays to the right for the global administrator only. By using the elements in this frame, all gauges, alerts, user lists, administrator profiles, data and logs stored on the TAR server will be deleted.

Execute a Backup on Demand

On demand backups ensure user settings saved in these files are retained on the server indefinitely.

1. In the Backup On Demand section of the Backup/ Restore Settings panel, enter the **File Name** for the backup file to activate the Backup Configuration Settings button:
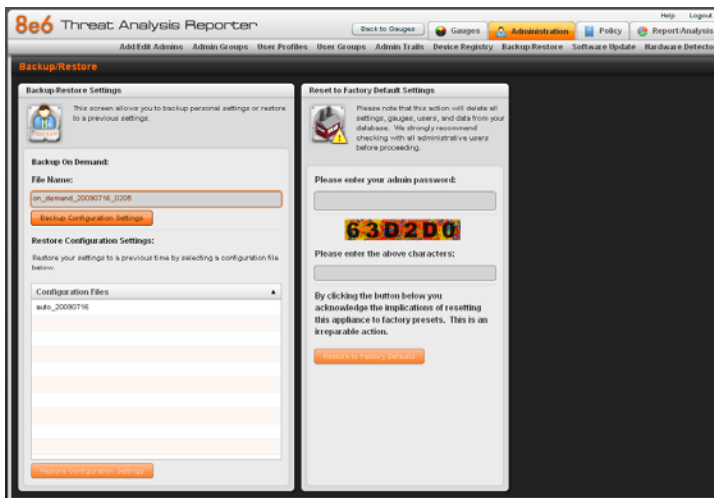
Fig. 4:4-2 Backup on demand

💡 **TIP**: *Spaces cannot be entered in this field, but numerals, upper- and lowercase characters, and the underscore (_) character can be used.*

2. Click **Backup Personal Data** to back up current user settings saved in the interface. Upon successfully executing the file backup, the file name is added to the Configuration Files list in the Restore Configuration Settings section, and the INFO alert box opens with the message: "Your settings were successfully backed up."

3. Click **OK** to close the alert box.

Restore User Settings

1. In the Restore Configuration Settings section of the Backup/Restore Settings panel, from the Configuration Files box, select the file to be restored by clicking on it to highlight it:

Fig. 4:4-3 Restore Personal Settings

2. Click **Restore Configuration Settings** to restore settings from the selected file. Upon successfully executing the file restoration, the INFO alert box opens with the following message: "Your settings were success-fully restored."
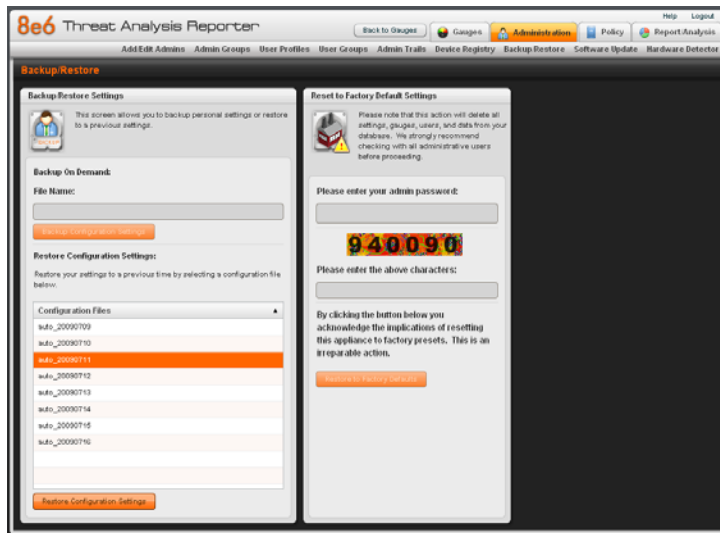
3. Click **OK** to close the alert box.

Restore to Factory Default Settings

If a TAR server needs to be purged of all existing data, a global administrator can restore the unit back to factory default settings.

⚠ *WARNING: When using this option, all settings made to the unit—including administrator, group, and gauge configuration—will be purged, and administrator and group settings cannot be restored.*

Reset to Factory Default Settings frame

1. In the Reset to Factory Default Settings panel, **Please enter your admin password** that was created during the TAR Wizard installation process.

2. Beneath the security characters, **Please enter the above characters**:
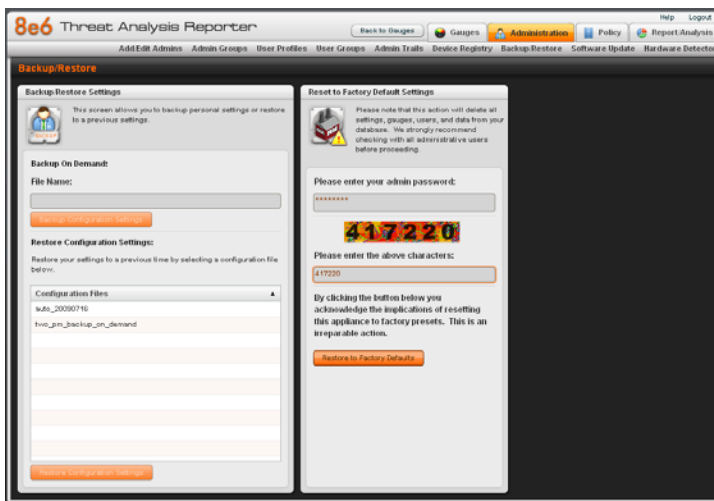

Fig. 4:4-4 Reset to Factory Default Settings frame

3. Click **Restore to Factory Defaults** to reset the TAR server and to display the TAR End User License Agreement screen:

Fig. 4:4-5 End User License Agreement

4. After reading the contents of the EULA, click **Yes** to accept it and to go to the Wizard Login window:
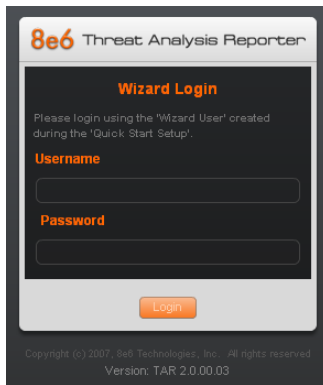
Fig. 4:4-6 Wizard Login window

Wizard Login window

1. In the Wizard Login window (see Fig. 4:4-6), type in the **Username** created during the quick start installation Wizard process.

2. Type in the **Password** created for the Username during the quick start installation Wizard process.

3. Click **Login** to display the Wizard screen:

Fig. 4:4-7 Wizard screen

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

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

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

6. In the R3000 Setup section, type in the **Server Name** and **Server IP** address, indicate if this R3000 will be **Set as Source**, and then click **Add** to include the server criteria in the list box below.

💡 *TIPS: To add another R3000, follow the instructions in step 6 above. To remove an R3000 from the list box, select it and then click **Remove**. To make an R3000 the Source server—if no R3000 in the list has yet been specified as the Source server— select the R3000 from the list box and then click **Set as Source**.*

7. In the section that asks: Do you have an Enterprise Reporter? click the radio button corresponding to "Yes" or "No".

   If "Yes" was selected, enter the **Server Name** and **Server IP** address of the ER server connected to the Source R3000 server:
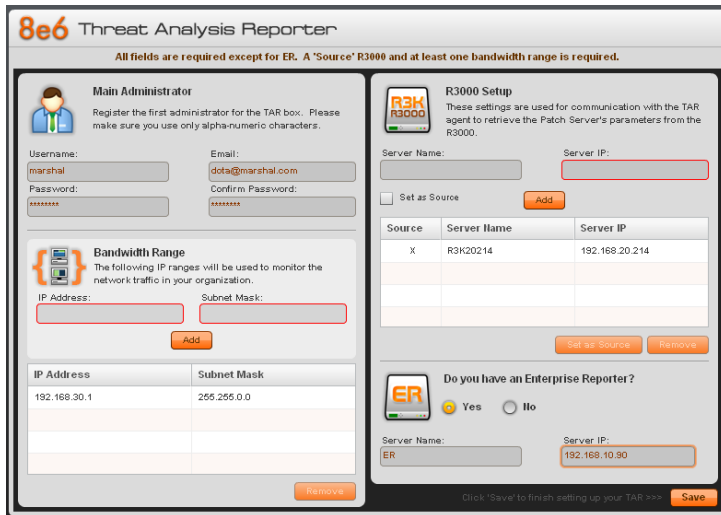
Fig. 4:4-8 Wizard screen with field entries made

8. Click **Save** to save your entries and to go to the TAR login window (see Fig. 1:1-1).

Chapter 5: Install Software Updates

This chapter explains how the global administrator installs software updates on the TAR server.

By default, the TAR server waits to receive software updates each hour via Traveler, 8e6's executable program. If a new software update is available, it is downloaded to TAR and an email message is dispatched to the global administrator whose email address was supplied during the TAR Wizard installation procedures. This email informs the administrator of the software release version that is ready for installation.

In the navigation toolbar, with the Administration tab selected, click **Software Update** to display the Software Update panel:
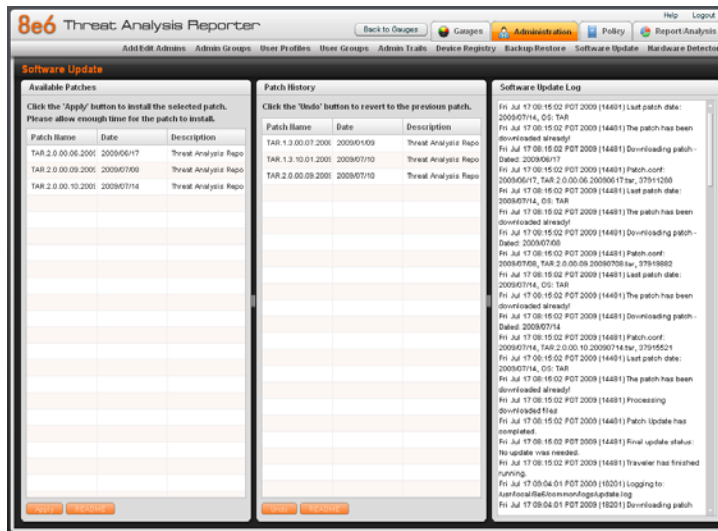
Fig. 4:5-1 Software Update panel

This panel contains three frames: Available Patches, Patch History, and Software Update Log.

The Available Patches frame lists available software updates, with each selection in the list showing the Patch

Name, Date (using the YYYY/MM/DD format), and Description.

The Patch History frame lists patches previously applied to this server, with each selection in the list showing the Patch Name, Date the software update was applied (using the YYYY/MM/DD format), and Description.

The Software Update Log includes a list of Traveler software update activity for this server.

Apply a Software Update

1. If a software update is available in the Available Patches frame, click the software update to select and highlight it.

2. Click **Apply** to open the two boxes: Readme pop-up box and CONFIRM dialog box.

3. After reading about the software release, click the "X" in the upper right corner of the Readme pop-up box to close it.
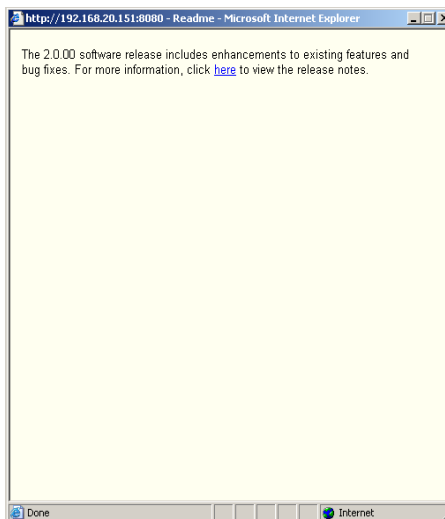
Fig. 4:5-2 Readme file

4. In the CONFIRM dialog box, the following message displays: "Are you sure you want to apply patch xxx?" (in which 'xxx' represents the software update name).

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

5. Click **Yes** to proceed with the software update application and to close the dialog box.

6. Wait five minutes for the software update to be automatically applied to the server, and then launch a new browser window.

7. Clear the browser's cache.

8. Log back in to TAR using the login window.

NOTE: See View Software Installation Details to determine whether the software was successfully applied.

Revert to a Previous Software Installation

NOTE: Only the most recently applied software update can be uninstalled, unless the Description for the software update specifies that the upgrade cannot be uninstalled.

WARNING: If a software update is uninstalled, configuration settings will revert to the previous settings, before the software update was applied.

To restore the previous software version on the server:

1. Go to the Patch History frame and select the software update to be unapplied:

2. Click **Undo**.

3. Launch a new browser window.

4. Clear the browser's cache.

5. Log back in to TAR using the login window.

Chapter 6: View Hard Disk Status

This chapter explains how the global administrator views the hard disk status on a TAR-SL, TAR-HL, or TAR-H server with RAID.

In the navigation toolbar, with the Administration tab selected, click **Hardware Detector** to display the Hardware Detector panel:
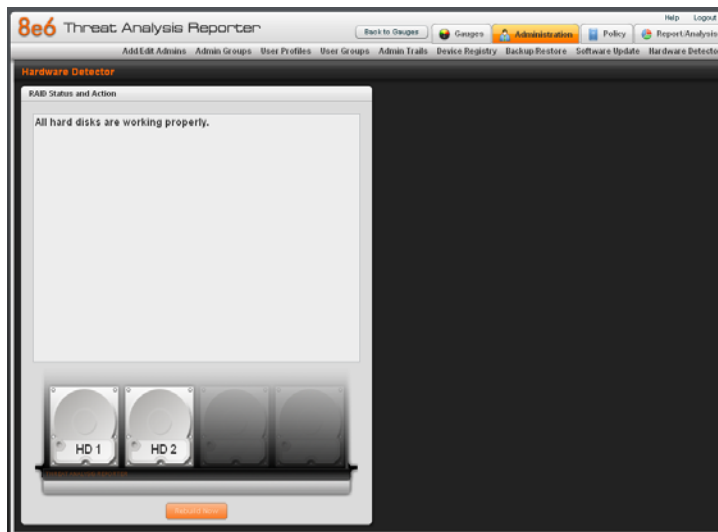
Fig. 4:6-1 Hardware Detector, hard disks OK

NOTE*: If the TAR server is a TAR-S or TAR-MSA unit, when clicking Hardware Detector, the Result alert window opens with the following message: "This is not a RAID box." Click **OK** to close the alert box.*

This panel contains the RAID Status and Action frame with an image showing two hard drives inside the chassis, labeled "HD 1" and "HD 2". If no hard disk failure has been detected on this server, the following message displays at the top of the frame: "All hard disks are working properly."

RAID Failure Detection

If a hard disk failure has been detected, the affected hard drive image displays in red with the message "FAIL," and the Rebuild button displays at the bottom of the window in place of the status message:

Fig. 4:6-2 Hardware Detector, hard disk failure

See Appendix C: RAID Maintenance for information on troubleshooting RAID, and replacing and rebuilding the hard drive.

TECHNICAL SUPPORT / PRODUCT WARRANTIES

Technical Support

For technical support, visit 8e6 Technologies's Technical Support Web page at **http://www.m86security.com/ support/**, or contact us by phone, by email, or in writing.

Hours

Regular office hours are from Monday through Friday, 8 a.m. to 5 p.m. PST.

After hours support is available for emergency issues only. Requests for assistance are routed to a senior-level technician through our forwarding service.

Contact Information

Domestic (United States)

1. Call **1-888-786-7999**
2. Select *option 3*

International

1. Call **+1-714-282-6111**
2. Select *option 3*

E-Mail

For non-emergency assistance, email us at **support@m86security.com**

Office Locations and Phone Numbers

8e6 Corporate Headquarters (USA)

828 West Taft Avenue
Orange, CA 92865-4232
USA

Local	:	714.282.6111
Fax	:	714.282.6116
Domestic US	:	1.888.786.7999
International	:	+1.714.282.6111

8e6 Taiwan

7 Fl., No. 1, Sec. 2, Ren-Ai Rd.
Taipei 10055
Taiwan, R.O.C.

Taipei Local	:	2397-0300
Fax	:	2397-0306
Domestic Taiwan	:	02-2397-0300
International	:	886-2-2397-0300

Support Procedures

When you contact our technical support department:

- You will be greeted by a technical professional who will request the details of the problem and attempt to resolve the issue directly.

- If your issue needs to be escalated, you will be given a ticket number for reference, and a senior-level technician will contact you to resolve the issue.

- If your issue requires immediate attention, such as your network traffic being affected or all blocked sites being passed, you will be contacted by a senior-level technician within one hour.

- Your trouble ticket will not be closed until your permission is confirmed.

Product Warranties

Standard Warranty

8e6 Technologies warrants the medium on which the 8e6 product is provided to be free from defects in material and workmanship under normal use for period of one year (the "Warranty Period") from the date of delivery. This standard Warranty Period applies to both new and refurbished equipment for a period of one year from the delivery date. 8e6 Technologies' entire liability and customer's exclusive remedy if the medium is defective shall be the replacement of the hardware equipment or software provided by 8e6 Technologies.

8e6 Technologies warrants that the 8e6 product(s) do(es) not infringe on any third party copyrights or patents. This warranty shall not apply to the extent that infringement is based on any misuse or modification of the hardware equipment or software provided. This warranty does not apply if the infringement is based in whole or in part on the customer's modification of the hardware equipment or software.

8e6 Technologies specifically disclaims all express warranties except those made herein and all implied warranties; including without limitation, the implied warranties of merchantability and fitness for a particular purpose. Without limitation, 8e6 Technologies specifically disclaims any warranty related to the performance(s) of the 8e6 product(s). Warranty service will be performed during 8e6 Technologies' regular business hours at 8e6 Technologies' facility.

Technical Support and Service

8e6 Technologies will provide initial installation support and technical support for up to 90 days following installation. 8e6 Technologies provides after-hour emergency support to 8e6 server customers. An after hours technician can be reached by voice line.

Technical support information:

Online: http://www.m86security.com/support/

Toll Free: 888-786-7999, *press 3*

Telephone: 1+714-282-6111, *press 3*

E-mail: support@m86security.com

Have the following information ready before calling technical support:

Product Description: _____

Purchase Date: _____

Extended warranty purchased: _____

Plan # _____

Reseller or Distributor contact: _____

Customer contact: _____

Extended Warranty (optional)

The extended warranty applies to hardware and software of the product(s) except any misuse or modification of the product(s), or product(s) located outside of the United States. The extended warranty does not include new product upgrades. Hardware parts will be furnished as necessary to maintain the proper operational condition of the product(s). If parts are discontinued from production during the Warranty Period, immediate replacement product(s) or hardware parts will be available for exchange with defective parts from 8e6 Technologies' local reseller or distributor.

Extended Technical Support and Service

Extended technical support is available to customers under a Technical Support Agreement. Contact 8e6 Technologies during normal business hours, 8 a.m. to 5 p.m. PST, at (888) 786-7999, or if outside the United States, call 1+(714) 282-6111.

APPENDICES SECTION

Appendix A

Disable Pop-up Blocking Software

An administrator with pop-up blocking software installed on his/her workstation will need to disable pop-up blocking in order to use the TAR console.

This appendix provides instructions on how to disable pop-up blocking software for the following products: Yahoo! Toolbar, Google Toolbar, AdwareSafe, and Windows XP Service Pack 2 (SP2).

Yahoo! Toolbar Pop-up Blocker

Add the Client to the White List

If the Client was previously blocked by the Yahoo! Toolbar, it can be moved from the black list and added to the white list so that it will always be allowed to pass. To do this:
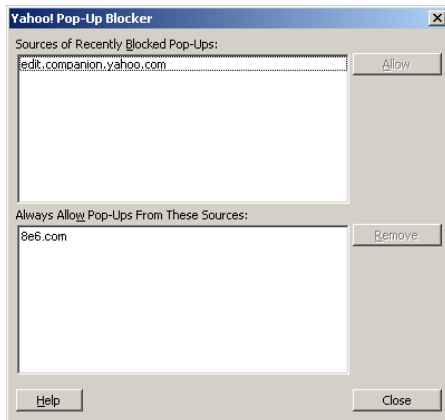
1. Go to the Yahoo! Toolbar and click the pop-up icon to open the pop-up menu:
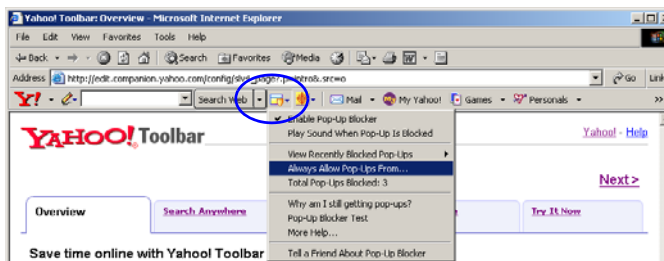
Fig. A-1 Select menu option Always Allow Pop-Ups From

2. Choose Always Allow Pop-Ups From to open the Yahoo! Pop-Up Blocker dialog box:

Fig. A-2 Allow pop-ups from source

3. Select the source from the Sources of Recently Blocked Pop-Ups list box to activate the Allow button.

4. Click **Allow** to move the selected source to the Always Allow Pop-Ups From These Sources list box.

5. Click **Close** to save your changes and to close the dialog box.

Google Toolbar Pop-up Blocker

Add the Client to the White List

To add the Client to the white list so that it will always be allowed to pass, go to the Google Toolbar and click the # blocked icon:
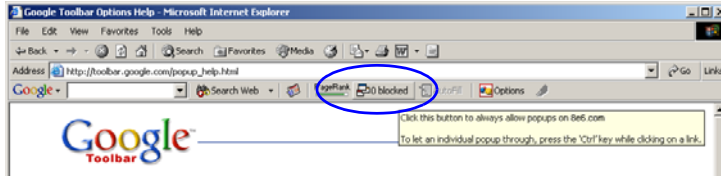

Fig. A-3 # blocked icon enabled

Clicking this icon toggles to the Site pop-ups allowed icon, adding the Client to your white list:
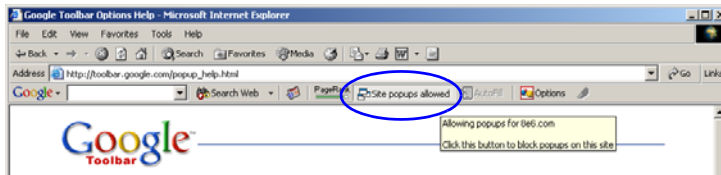

Fig. A-4 Site pop-ups allowed icon enabled

AdwareSafe Pop-up Blocker

Disable Pop-up Blocking

AdwareSafe's SearchSafe toolbar lets you toggle between enabling pop-up blocking (# popups blocked) and disabling pop-up blocking (Popup protection off) by clicking the pop-up icon.

1. In the IE browser, go to the SearchSafe toolbar and click the icon for # popups blocked to toggle to Popup protection off. This action turns off pop-up blocking.

2. After you are finished using the Client, go back to the SearchSafe toolbar and click the icon for Popup protection off to toggle back to # popups blocked. This action turns on pop-up blocking again.

Windows XP SP2 Pop-up Blocker

This sub-section provides information on setting up pop-up blocking and disabling pop-up blocking in Windows XP SP2.

Set up Pop-up Blocking

There are two ways to enable the pop-up blocking feature in the IE browser.

Use the Internet Options dialog box

1. From the IE browser, go to the toolbar and select **Tools > Internet Options** to open the Internet Options dialog box.
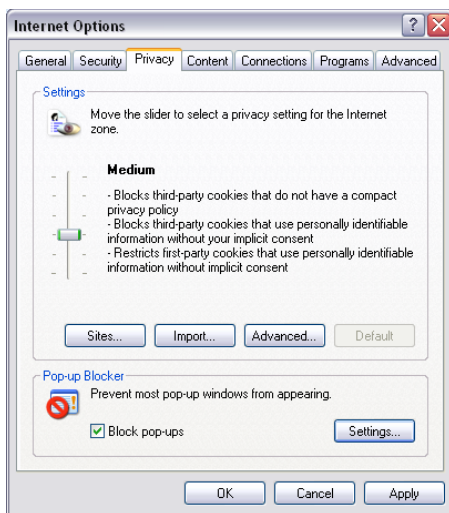
2. Click the Privacy tab:

Fig. A-5 Enable pop-up blocking

3. In the Pop-up Blocker frame, check "Block pop-ups".

4. Click **Apply** and then click **OK** to close the dialog box.

Use the IE Toolbar

In the IE browser, go to the toolbar and select **Tools > Pop-up Blocker > Turn On Pop-up Blocker**:
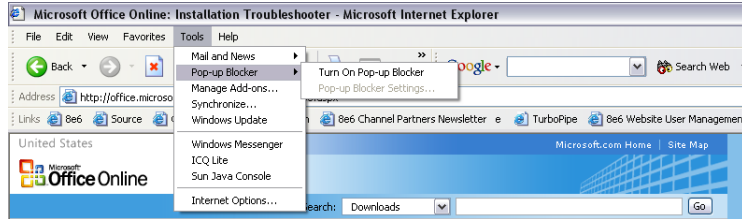
Fig. A-6 Toolbar setup

When you click Turn On Pop-up Blocker, this menu selection changes to Turn Off Pop-up Blocker and activates the Pop-up Blocker Settings menu item.

You can toggle between the On and Off settings to enable or disable pop-up blocking.

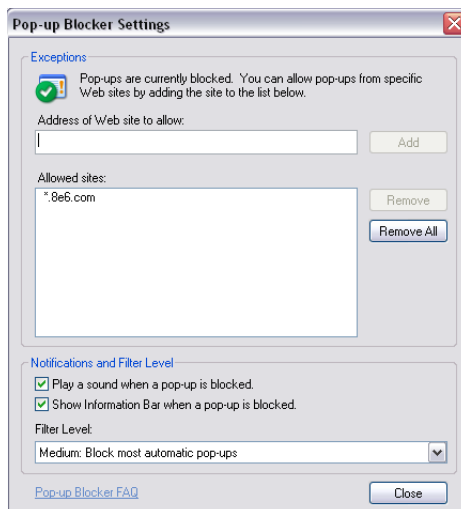## Add the Client to the White List

There are two ways to disable pop-up blocking for the Client and to add the Client to your white list.

Use the IE Toolbar

1. With pop-up blocking enabled, go to the toolbar and select **Tools > Pop-up Blocker > Pop-up Blocker Settings** to open the Pop-up Blocker Settings dialog box:

Fig. A-7 Pop-up Blocker Settings

2. Enter the **Address of Web site to allow**, and click **Add** to include this address in the Allowed sites list box. Click **Close** to close the dialog box. The Client has now been added to your white list.

Use the Information Bar

With pop-up blocking enabled, the Information Bar can be set up and used for viewing information about blocked pop-ups or allowing pop-ups from a specified site.

Set up the Information Bar

1. Go to the toolbar and select **Tools > Pop-up Blocker > Pop-up Blocker Settings** to open the Pop-up Blocker Settings dialog box (see Fig. A-7).

2. In the Notifications and Filter Level frame, click the checkbox for "Show Information Bar when a pop-up is blocked."

3. Click **Close** to close the dialog box.

Access the Client

1. Click the Information Bar for settings options:

Fig. A-8 Information Bar menu options
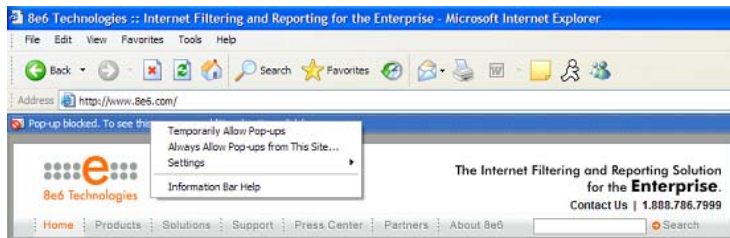
2. Select Always Allow Pop-ups from This Site—this action opens the Allow pop-ups from this site? dialog box:
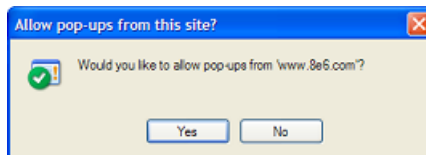

Fig. A-9 Allow pop-ups dialog box

3. Click **Yes** to add the Client to your white list and to close the dialog box.

NOTE: To view your white list, go to the Pop-up Blocker Settings dialog box (see Fig. A-7) and see the entries in the Allowed sites list box.

Appendix B

System Tray Alerts: Setup, Usage

This appendix explains how to set up and use the feature for System Tray alerts. A TAR Alert is triggered in an administrator's System Tray if an end user's Internet usage has reached the upper threshold established for a gauge set up by that administrator.

This feature is only available to administrators using an LDAP username, account, and domain, and is not available if using IP groups authentication.

NOTE: In order to use this feature, the LDAP Username and Domain set up in the administrator's profile account (see Chapter 3 in the Preliminary Setup Section) must be the same ones he/she uses when logging into his/her workstation.

LDAP server configuration

Create the System Tray logon script

Before administrators can use the TAR Alert feature, an administrator with permissions on the LDAP server must first create a logon script on the LDAP server for authenticating administrators.

1. From the taskbar of the LDAP server, go to: **Start > Run** to open the Run dialog box:
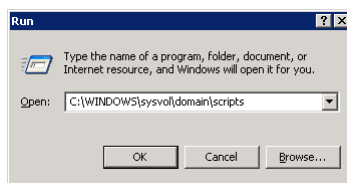

Fig. B-1 Run dialog box

2. In the Run dialog box, type in the path to the scripts folder: **C:\WINDOWS\sysvol\domain\scripts**.

3. Click **OK** to open the scripts folder:
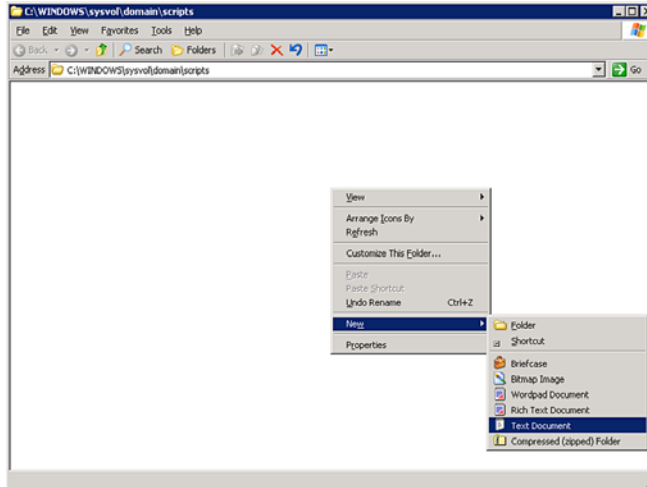
Fig. B-2   C:\WINDOWS\sysvol\domain\scripts window

4. Right-click in this Windows folder to open the pop-up menu.

5. Select **New > Text Document** to launch a New Text Document:
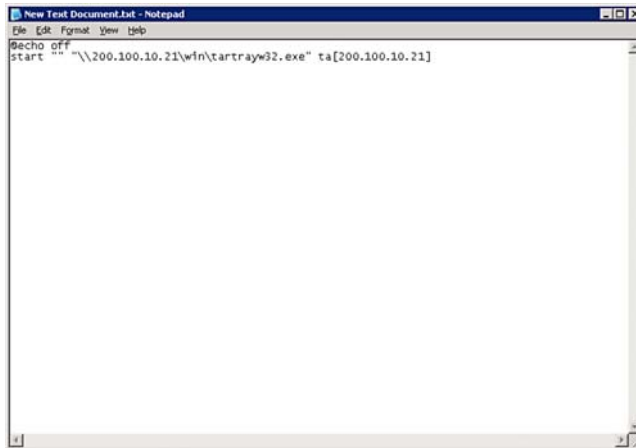
Fig. B-3 New Text Document

6. Type the following text in the blank document file:

@echo off
start "" "\\X.X.X.X\win\tartrayw32.exe" ta[X.X.X.X]

in which "X.X.X.X" represents the IP address of the TAR server, and "\win\tartrayw32.exe" refers to the location of the TAR Alert executable file on the TAR server.

7. Go to: **File > Save As** to open the Save As window:

Fig. B-4 Save As dialog box

8. In the **File name** field, type in the name for the file using the "filename.bat" format. For example: *tartray21.bat*.

NOTE: Be sure that the Save as type field has "All Files" selected.

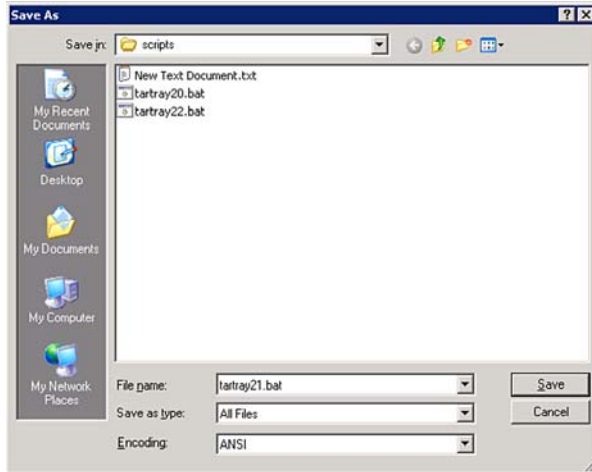9. Click **Save** to save your file and to close the window.

Assign System Tray logon script to administrators

With the ".bat" file created, the administrator with permissions on the LDAP server can now begin to assign the System Tray logon script to as many administrators as needed.

1. From the taskbar of the LDAP server, go to: **Start > Programs > Administrative Tools > Active Directory Users and Computers** to open the Active Directory Users and Computers folder:
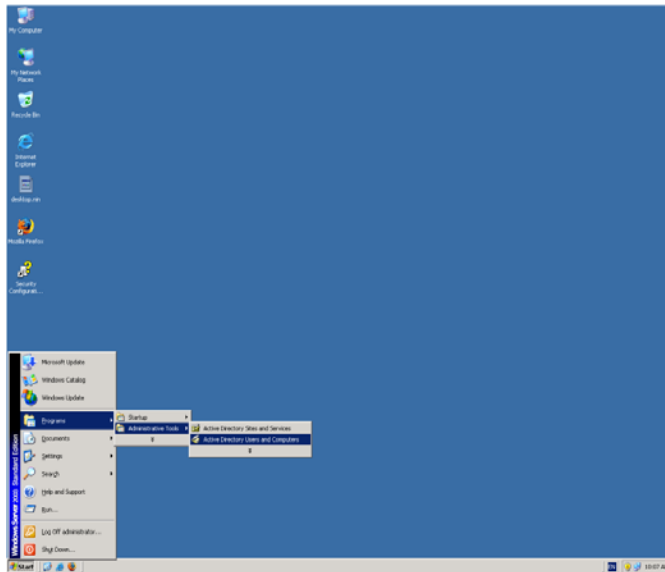
Fig. B-5 Programs > Administrative Tools > Active Directory Users

2. In the Active Directory Users and Computers folder, double-click the administrator's Name in the Users list to open the Properties dialog box for his/her profile:
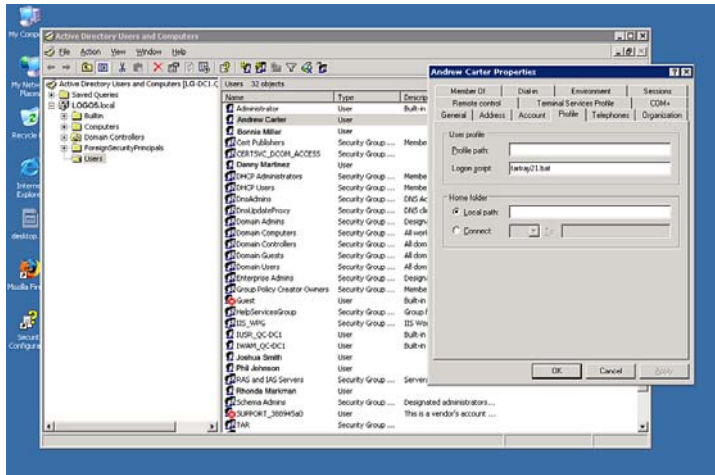
Fig. B-5 Properties dialog box, Active Directory Users folder

3. In the Properties dialog box, click the Profile tab to display its contents.

4. In the **Login script** field, type in the ".bat" filename. For example: *tartray21.bat*.

5. Click **Apply** to save your entry.

6. Click **OK** to close the dialog box.

7. Click the "X" in the upper right corner of the folder to close the window.

Administrator usage of System Tray

Once the System Tray logon script has been added to the administrator's profile, when the administrator logs on his/her workstation, the TAR Alert icon (pictured to the far left in the image below) automatically loads in his/her System Tray:

 NOTE: The TAR Alert icon will not load in the System Tray if the TAR server is not actively running.

Use the TAR Alert icon's menu

When right-clicking the TAR Alert icon, the following pop-up menu items display:

- Tar Admin Interface - clicking this menu selection launches a browser window containing the TAR Administrator Interface's login window.

- Reconnect - clicking this menu selection re-establishes the TAR Alert icon's connection to the TAR server, resetting the status of the TAR Alert icon to the standard setting.

- Exit - clicking this menu selection removes the TAR Alert icon from the System Tray.

Status of the TAR Alert icon

If there are no alerts for any gauges set up by the administrator, the following message displays when mousing over the standard TAR Alert icon: "Connected. No Alerts."

However, if an alert is triggered, the TAR Alert icon changes in appearance from the standard gauge to a yellow gauge (pictured to the far left in the image below):

The following message appears briefly above the yellow gauge: "New 8e6 TAR Alert!" The following message displays whenever mousing over this icon: "New 8e6 TAR Alert".

If more than one alert is triggered for the administrator, the message reads: "New 8e6 TAR Alert! (X Total)", in which "X" represents the total number of new alerts. The following message displays whenever mousing over this icon: "X New 8e6 TAR Alerts", in which "X" represents the total number of new alerts.

View System Tray alert messages

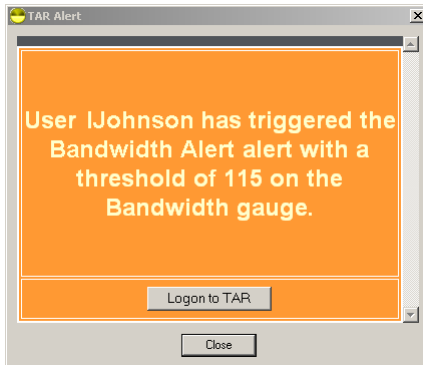1. Double-click the yellow TAR Alert icon to open the TAR
   Alert box:

Fig. B-6 TAR Alert

This box contains the following message: "User (user-
name/IP address) has triggered the (Alert Name) alert
with a threshold of X (in which "X" represents the alert
threshold) on the (URL dashboard gauge name) gauge."

The Logon to TAR button displays beneath this
message, followed by the Close button.

If more than one alert was triggered, the alert box
includes the following message and button to the right of
the Close button: "X more alerts" (in which "X" represents
the number of additional alerts), and the Next >> button.

2. Click **Logon to TAR** to launch the TAR login window (see
   Fig. 1:1-1).

If there are additional alerts, click **Next >>** to view the
next TAR Alert. Each time the Next >> button is clicked,
the number of remaining alerts to be viewed decreases
by one. The Next >> button no longer displays after the
last alert is viewed.

3. Click **Close** to close the TAR Alert box.

Appendix C

RAID Maintenance

This appendix pertains to TAR "H", "SL", and "HL" servers and is divided into three parts: Hardware Components, Server Interface, and Troubleshooting—in the event of a failure in one of the drives, power supplies, or fans.

NOTE: As part of the ongoing maintenance procedure for your RAID server, 8e6 recommends that you always have a spare drive and spare power supply on hand.

Contact 8e6 Technical Support for replacement hard drives and power supplies.

Part 1: Hardware Components

The TAR "H", "SL", and "HL" RAID server contains two hard drives, two power supplies, and five sets of dual cooling fans (10 in total). These components are depicted in the diagram below:

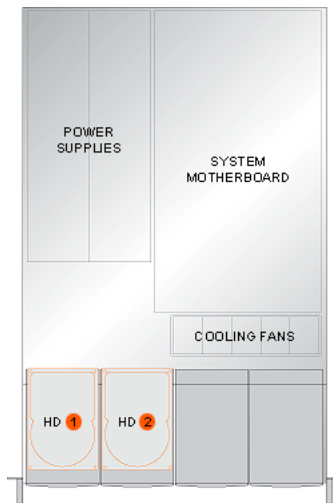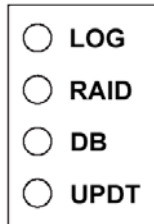*Fig. C-1 TAR RAID Server components*

Part 2: Server Interface

LED indicators in SL and HL units

On an "SL" and "HL" unit, the following LED indicators for software and hardware status monitoring display on the left side of the front panel:

- LOG = Log Download Status

- RAID = Hard Drive Status

- DB = Database Status

- UPDT = Software Update Status

LED Indicator Chart

Below is a chart of LED indicators in the "SL" and "HL" unit:

LED Indicator	Color	Condition	Description
LOG	Green	On	Downloading a log
	--	Off	No log download detected
RAID	Green	On	RAID mode enabled and running
	--	Off	RAID mode is inactive
	Red	On	Hard drive fault or failure
DB	Green	On	Database is active
	Red	On	Database in inactive
UPDT	Amber	On	Software update detected
	--	Off	No software update detected

Front control panels on H, SL, and HL units

Control panel buttons, icons, and LED indicators display on the right side of the front panel. The buttons let you perform a function on the unit, while an LED indicator corresponding to an icon alerts you to the status of that feature on the unit.
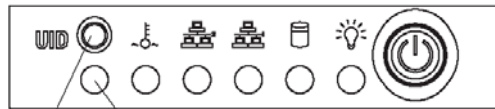
"H" chassis front panel
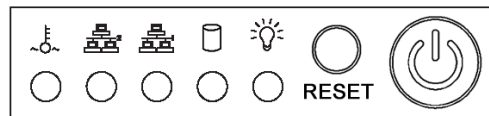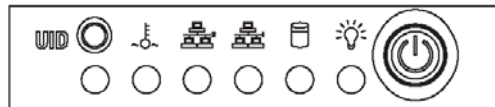
"SL" chassis front panel

"HL" chassis front panel

The buttons and LED indicators for the depicted icons function as follows:

UID (button) – On an "H" or "HL" server, when the UID button is pressed, a steady blue LED displays on both the front and rear of the chassis (see also Rear of chassis). These indicators are used for easy location of the chassis in a large stack configuration. The LED remains on until the button is pressed a second time.

Overheat/Fan Fail (icon) – This LED is unlit unless the chassis is overheated. A flashing red LED indicates a fan failure. A steady red LED (on and not flashing) indicates an overheating condition, which may be caused by cables obstructing the airflow in the system or the ambient room temperature being too warm.

NIC2 (icon) – A flashing green LED indicates network activity on LAN2. The LED is a steady green with link connectivity, and unlit if there with no link connectivity.

NIC1 (icon) – A flashing green LED indicates network activity on LAN1. The LED is a steady green with link connectivity, and unlit if there with no link connectivity.

HDD (icon) – In addition to displaying in the control panel, this icon also displays on the front panel on each hard drive carrier. Hard drive activity is indicated by a green LED on an "H" or "HL" server, and by an amber LED on an "SL" server. An unlit LED on a drive carrier may indicate a hard drive failure. (See Hard drive failure in the Troubleshooting sub-section for information on detecting a hard drive failure and resolving this problem.)

Power (icon) – The LED is unlit when the server is turned off. A steady green LED indicates power is being supplied to the unit's power supplies. (See also Rear of chassis.) (See Power supply failure in the Troubleshooting sub-section for information on detecting a power supply failure and resolving this problem.)

Power (button) – When the power button is pressed, the main power to the server is turned on. When the power button is pressed again, the main power to the server is removed but standby power is still supplied to the server.

Rear panels on H and HL units

UID (LED indicator) – On the rear of the "H" or "HL" chassis, to the left of the power supplies, a steady blue UID LED indicator displays when the UID button on the control panel is pressed. This LED remains lit until the UID button is pressed again.

VGA Port   **Button/LED**
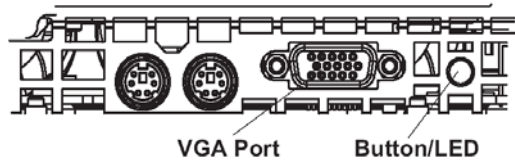
Power Supplies (LED indicators) – The power supplies are located at the right on the rear of the chassis. An LED indicator is located above each of the power plugs. (See Power supply failure in the Troubleshooting sub-section for information on detecting a power supply failure and resolving this problem.)
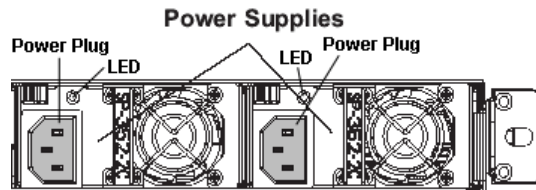
Part 3: Troubleshooting

The text in this section explains how the server alerts the administrator to a failed component, and what to do in the event of a failure.

Hard drive failure

Step 1: Review the notification email

If a hard drive fails, a notification email is sent to the administrator of the server. This email identifies the failed hard drive by its number (HD 1 or HD 2). Upon receiving this alert, the administrator should verify the status of the drives by first going to the Hardware Detector panel in the Administrator console.

⚠ **WARNING**: *Do not attempt to remove any of the drives from the unit at this time. Verification of the failed drive should first be made in the Administrator console before proceeding, as data on the server will be lost in the event that the wrong drive is removed from the unit.*

Step 2: Verify the failed drive in the Admin console

The Hardware Detector panel in the Administrator console is accessible via the **Administration > Hardware Detector** menu selection:

Fig. C-2 Hardware Detector panel, failed hard drive detected

The Hardware Detector panel displays the current RAID Array Status for the two hard drives (HD 1 and HD 2).

Normally, when both hard drives are functioning without failure, no text displays above the hard drive number.

However, if a hard drive has failed, the image of the drive displays with a yellow triangle containing a red exclamation point, and the message "FAIL" above the hard drive number.

Before taking any action in this panel, proceed to Step 3.

Step 3: Replace the failed hard drive

After verifying the failed hard drive in the Administrator console, go to the server to replace the drive.
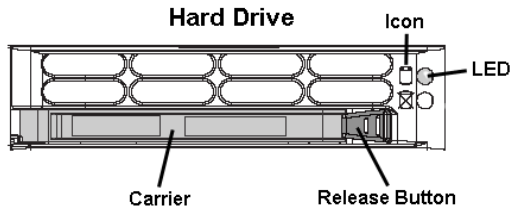
Press the red release button to release the handle on the carrier, and then extend the handle fully and pull the carrier out towards you. Replace the failed drive with your spare replacement drive.
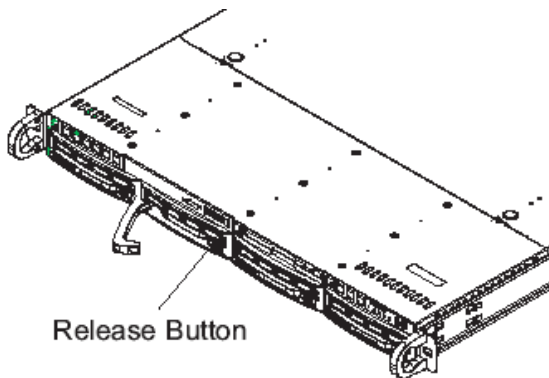
NOTE: Contact Technical Support if you have any questions about replacing a failed hard drive.

Step 4: Rebuild the hard drive

A. Once the failed hard drive has been replaced, return to the Hardware Detector panel in the Administrator console, and click **Rebuild Now** to open the Results alert box:
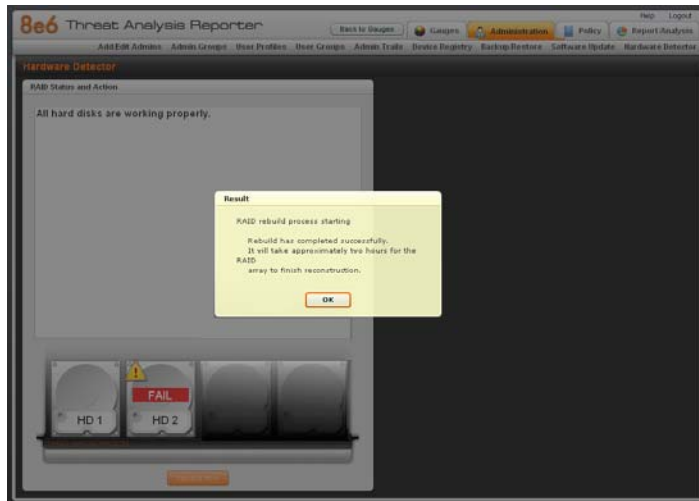
Fig. C-3 Hardware Detector panel, initiate Rebuild process

The Results alert box displays the following messages if the RAID rebuild proceeds as expected: "RAID rebuild process starting. Rebuild has completed successfully. It will take approximately two hours for the RAID array to finish reconstruction."

B. Click **OK** to close the Results alert box and to continue with the RAID array reconstruction process.

⚠ *WARNING: When the RAID array reconstruction process begins, the Administrator console will close and the hard drive will become inaccessible.*

Step 5: Contact Technical Support

Contact Technical Support to order a new replacement hard drive and for instructions on returning your failed hard drive to 8e6.

Power supply failure

Step 1: Identify the failed power supply

The administrator of the server is alerted to a power supply failure on the chassis by an audible alarm and an amber power supply LED—or an unlit LED—on the front and rear of the chassis.

NOTE*: A steady amber power supply LED also may indicate a disconnected or loose power supply cord. Verify that the power supply cord is plugged in completely before removing a power supply.*

WARNING*: Be sure the correct failed power supply has been identified. Removing the wrong power supply will cause the system to crash.*

Step 2: Unplug the power cord

To prevent electrical shock to yourself and damage to the unit, unplug the power cord from the failed power supply.

Step 3: Replace the failed power supply

Remove the failed power supply by locating the red release tab (1) and pushing it to the right (2), then lifting the curved metal handle and pulling the power supply module towards you (3).
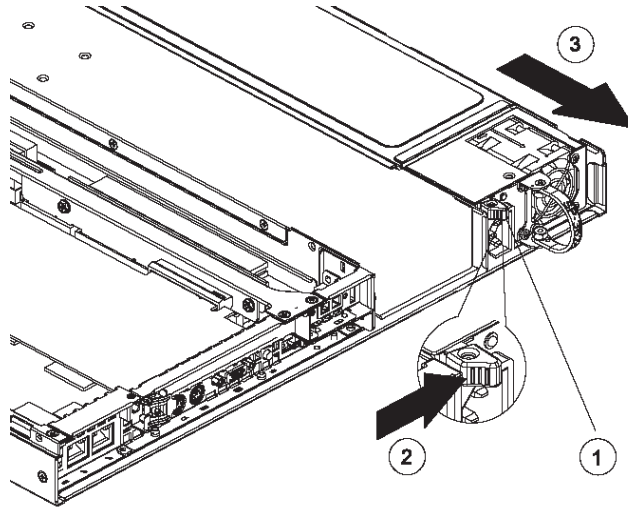
Note that an audible alarm sounds and the LED is unlit when the power supply is disengaged. Replace the failed power supply with your spare replacement power supply. The alarm will turn off and the LED will be a steady green when the replacement power supply is securely locked in place.

Step 4: Contact Technical Support

Contact Technical Support to order a new replacement power supply and for instructions on returning your failed power supply to 8e6.

Fan failure

Identify a fan failure

A flashing red LED indicates a fan failure. If this displays on your unit, contact Technical Support for an RMA (Return Merchandise Authorization) number and for instructions on returning the unit to 8e6.

A steady red LED (on and not flashing) indicates an over-heating condition, which may be caused by cables obstructing the airflow in the system or the ambient room temperature being too warm. Check the routing of the cables and make sure all fans are present and operating normally. The LED will remain steady as long as the over-heating condition exists.

Appendix D

Glossary

This glossary includes definitions for terminology used in this user guide.

base group - A user group consisting of end users whose network activities are monitored by the designated group administrator(s). Only the creator of the base group can modify the base group, delegate the base group to another group administrator, or delete the base group.

custom category - A unique library category on the R3000 that includes URLs, URL keywords, and/or search engine keywords to be blocked. In TAR, global administrators can create and manage custom library categories and sync them to the source R3000.

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

global administrator - An authorized administrator of the network who maintains all aspects of TAR. The global administrator configures TAR, sets up user groups, administrator groups and group administrators, and performs routine maintenance on the server.

group administrator - An authorized administrator of TAR who maintains user group, administrator groups, group administrator profiles, and gauges.

HTTP - Hyper Text Transfer Protocol is used for transferring files via the World Wide Web or an intranet.

instant messaging - IM involves direct connections between workstations either locally or across the Internet.

library category - A list of URLs, URL keywords, and search engine keywords set up to be blocked.

LDAP - One of two authentication method protocols that can be used with TAR. Lightweight Directory Access Protocol (LDAP) is a directory service protocol based on entries (Distinguished Names). The other authentication method that can be used with TAR is IP groups.

peer-to-peer - P2P involves communication between computing devices—desktops, servers, and other smart devices—that are linked directly to each other.

protocol - A type of format for transmitting data between two devices. LDAP and SMB are types of authentication method protocols.

Real Time Probe - On the R3000, this tool is used for monitoring the Internet activity of specified users in real time. The report generated by the probe lets the administrator know whether end users are using the Internet appropriately.

search engine - A program that searches Web pages for specified keywords and returns a list of the pages or services where the keywords were found.

SMTP - Simple Mail Transfer Protocol is used for transferring email messages between servers.

synchronization - A process by which two or more machines run in parallel to each other. User filtering profiles, library configurations, and devices connected to the source R3000 can be set up to be synchronized between the source R3000 and TAR.

TCP - An abbreviation for Transmission Control Protocol, one of the core protocols of the Internet protocol suite. Using TCP, applications on networked hosts can create connections to one another, over which streams of data can be exchanged.

Traveler - 8e6's executable program that downloads updates to TAR at a scheduled time.

UDP - An abbreviation for User Data Protocol, one of the core protocols of the Internet protocol suite. Using UDP, programs on networked computers can send short messages (sometimes known as datagrams) to one another.

URL - An abbreviation for Uniform Resource Locator, the global address of Web pages and other resources on the Internet. A URL is comprised of two parts. The first part of the address specifies which protocol to use (such as "http"). The second part specifies the IP address or the domain name where the resource is located (such as "203.15.47.23" or "8e6.com").

INDEX

A

accordion, terminology *4*
alert box, terminology *4*
alert log *86*
alert messages *76*

B

Back to Gauges button *15*
backup *129*
bandwidth *34*
    gauge *44*
base group *21*, *56*
    definition *179*
button, terminology *4*
byte score *46*

C

checkbox, terminology *4*
Ctrl key *14*
custom category
    definition *179*
custom search *102*

D

delete a gauge *60*
device registry *115*
dialog box, terminology *4*
disable a gauge *60*
disable pop-up blockers *148*

E

Enterprise Reporter *34*
environment requirements *8*
ER *34*, *43*, *91*, *101*, *106*

expand or contract a column *14*

F

field, terminology *5*
Firefox *8*
Flash plug-in *8*
frame, terminology *5*
FTP *47*
    definition *179*

G

gauge
    restore configuration settings *129*
global administrator *2*
    definition *179*
group administrator *2*
    definition *179*

H

H server *166*
hide a gauge *60*
HL server *166*
How to
    access the Add/Edit Gauges panel *51*
    add a new alert *78*
    add a new gauge *53*
    drill down into a gauge *65*
    navigate the interface *13*, *14*
    set up email alert notifications *79*
    view an email alert *80*
    view end user gauge activity *64*
    view URLs a user visited *64*
HTTP *47*
    definition *179*
HTTPS *9*

I

IM *48*

P

P2P *48*
    definition *180*
panel, terminology *5*
peer-to-peer
    definition *180*
pop-up blocking, disable *148*
pop-up box/window, terminology *6*
Product Warranties section *145*
protocol
    bandwidth gauge *44*
    definition *180*
pull-down menu, terminology *6*

Q

quick start
    installation procedures *11*, *37*, *41*, *106*, *120*, *137*
Quick Start Guide *10*

R

R3000 *1*, *8*, *9*, *34*, *91*, *101*, *106*, *108*, *115*
    end user lockout *81*
RAID *140*
Real Time Probe *180*
rearrange the gauge display *60*
recovery procedures *130*
requirements
    environment *8*
resize button, terminology *6*

S

Safari *8*
screen, terminology *6*
search engine
    definition *180*
Shift key *15*
SL server *166*
slider, terminology *6*