



8e6® Threat Analysis Reporter

USER GUIDE



Model: TAR

Release 1.3.00 • Manual Version 1.01

THREAT ANALYSIS REPORTER USER GUIDE

© 2009 8e6 Technologies
All rights reserved.

Version 1.01, published January 2009
For software release 1.3.00

Printed in the United States of America

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form without prior written consent from 8e6 Technologies.

Every effort has been made to ensure the accuracy of this document. However, 8e6 Technologies makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. 8e6 Technologies shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. Due to future enhancements and modifications of this product, the information described in this documentation is subject to change without notice.

The latest version of this document can be obtained from
http://www.8e6.com/docs/tar_ug.pdf.

Trademarks

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Part# TAR-UG_v1.01-0901

CONTENTS

- INTRODUCTORY SECTION 1**
 - Threat Analysis Reporter 1**
 - About this User Guide 2**
 - How to Use this User Guide 3**
 - Conventions 3
 - Terminology 4
 - Environment Requirements 7**
 - Workstation Requirements 7
 - Network Requirements 8
 - Installation Prerequisite 8
 - Getting Started 9**
 - Initial Setup 9
 - Login window 10
 - Log in 11
 - Navigation panel menu topics 12
 - Help 12
 - Log out 13
 - Exit the interface 13
 - Navigation Tips and Conventions 14**
- PRELIMINARY SETUP SECTION 16**
 - Introduction 16**
 - Chapter 1: User Groups Setup 17**
 - View User Group Information 19
 - User group status key 19
 - View a list of members in a user group 19
 - Add a User Group 21
 - Patterns tab 22
 - Add a new pattern 22
 - View users resolved by the pattern 23

Remove a pattern.....	23
IP Ranges tab	24
Specify an IP range	25
Remove an IP address range	26
Single User tab	26
Add one or more individual users.....	27
Use the filter to narrow Available Users results	27
Select users to add to the Assigned Users list	27
Remove users from the Add tab	28
Edit a User Group	29
Rebuild the User Group	30
Delete a User Group	31
Chapter 2: Admin Groups Setup	32
Add a Group	33
View an Admin Group's Permissions	34
Edit an Administrator Group	36
Delete an Administrator Group	37
Chapter 3: Admins Setup	38
View Account Info	39
View Account Info	40
Add an Administrator Profile	41
Account Info tab	41
Contact Info tab	42
Groups tab	43
Edit Account Info	44
Change Password	45
User Groups: Add or remove a group	46
Add a group.....	46
Remove a group.....	46
Delete Admin	47
CONFIGURATION SECTION	48
Introduction	48
Chapter 1: Threat Score Setup	49
Anatomy of a Gauge	49
Gauge score methodology	50
View Assigned Threat Score Weights	51

Assign a Threat Score Weight	52
Chapter 2: Custom Gauge Setup, Usage	53
Add a Gauge	54
Add Gauge Information	55
Sync All Categories	56
Select Library Categories	56
Assign User Groups	57
View, edit library components	58
Gauge Components and Activity	60
Types of gauges	60
Read a gauge	61
Modify a Gauge	63
Edit gauge settings	63
Hide, Show a URL Gauge	65
Temporarily hide a URL gauge	65
Save settings for hiding a URL gauge	66
Delete a Gauge	67
View End User Gauge Activity	69
View Overall Ranking	70
View a URL gauge ranking table	71
View a library category gauge ranking table	72
Monitor, Restrict End User Activity	74
View a list of categories accessed by the user	75
View a list of URLs accessed by the user	77
Manually lock out an end user	78
End user workstation lockout	81
Chapter 3: Alerts, Lockout Management	83
Add an Alert	84
Email alert function	85
Configure email alerts	85
Receive email alerts	86
Lockout function	86
Configure automatic lockouts	86
System Tray alert function	87
View, Modify, Delete an Alert	87
View alert settings	88
Modify an alert	89
Delete an alert	90
View the Alert Log	91

Manage the Lockout List	92
View a specified time period of lockouts	93
Unlock a workstation	94
Chapter 4: Analyze Web Usage Trends	95
View URL Trend Reports	96
View all URL dashboard gauge activity	96
View activity for a specified URL gauge	97
Suppress specified scores	98
View scores for a different time period	98
Access Real Time Probe, Web Client	99
Access the R3000 Real Time Probe tool	99
Access the ER Web Client application	99
Chapter 5: View User Category Activity	100
Perform a custom search	100
View a list of Users who accessed a Category	100
View URLs within the accessed category	102
Print the results	103
Access a URL	103
BANDWIDTH MANAGEMENT SECTION	104
Introduction	104
Chapter 1: Monitor Bandwidth Gauges	105
Bandwidth Gauge Components	105
View Bandwidth Gauges	108
View bandwidth usage for a specified protocol	109
View End User Bandwidth Gauge Activity	110
View Overall Ranking for bandwidth	111
View a protocol gauge ranking table	112
View a port gauge ranking table	113
Monitor, Restrict Bandwidth Usage	115
View the end user's port usage in bytes	116
Manually lock out an end user	117
Chapter 2: Modify Bandwidth Gauges	119
Modify Protocol Gauge Settings	119
Edit Port Settings	120

Chapter 3: View Bandwidth Trend Reports	121
View All Bandwidth Gauge Activity	121
View Activity for a Specified Gauge	122
Suppress Criteria of Specified Ports	123
View Criteria for a Different Time Period	123
 ADMINISTRATION SECTION	 124
 Introduction	 124
 Chapter 1: Custom Category Maintenance	 126
View Custom Categories	127
Add a Custom Category	128
Synchronize TAR with the R3000	130
Delete a Custom Category	131
 Chapter 2: View the Master User List	 132
Search the MUL Database	133
View End User Activity	134
Synchronize TAR with the R3000	134
 Chapter 3: View Administrator Activity	 135
Perform a Search on a Specified Activity	136
Search Results	137
 Chapter 4: Maintain the Device Registry	 139
R3000 Device Maintenance	141
View, edit R3000 device criteria	141
Add an R3000 to the registry	142
Delete an R3000 from the registry	142
Threat Analysis Reporter Maintenance	143
View, edit TAR device criteria	143
ER Device Maintenance	145
Add an ER to the registry	145
View, edit ER device criteria	146
Delete ER device	147
View Other Device Criteria	147
View SMTP device criteria	147
View Patch Server device criteria	148
View NTP Server device criteria	148
View Proxy Server device criteria	148

Sync All Devices	149
Chapter 5: Perform Backup, Restoration	150
Execute a Backup on Demand	152
Restore User Settings	153
Restore to Factory Default Settings	154
Chapter 6: Install Software Updates	155
Check for Available Software Updates	155
Apply a Software Update	156
Revert to a Previous Software Installation	157
View Software Installation Details	159
Chapter 7: View Hard Disk Status	160
TECHNICAL SUPPORT / PRODUCT WARRANTIES	162
Technical Support	162
Hours	162
Contact Information	162
Domestic (United States)	162
International	162
E-Mail	162
Office Locations and Phone Numbers	163
8e6 Corporate Headquarters (USA).....	163
8e6 Taiwan.....	163
Support Procedures	164
Product Warranties	165
Standard Warranty	165
Technical Support and Service	166
Extended Warranty (optional)	167
Extended Technical Support and Service	167
APPENDICES SECTION	168
Appendix A	168
Disable Pop-up Blocking Software	168
Yahoo! Toolbar Pop-up Blocker	168
Add the Client to the White List	168
Google Toolbar Pop-up Blocker	170

Add the Client to the White List	170
AdwareSafe Pop-up Blocker	171
Disable Pop-up Blocking	171
Windows XP SP2 Pop-up Blocker	172
Set up Pop-up Blocking	172
Use the Internet Options dialog box.....	172
Use the IE Toolbar	173
Add the Client to the White List	174
Use the IE Toolbar	174
Use the Information Bar	175
Set up the Information Bar.....	175
Access the Client.....	175
Appendix B	177
System Tray Alerts: Setup, Usage	177
LDAP server configuration	177
Create the System Tray logon script.....	177
Assign System Tray logon script to administrators	181
Administrator usage of System Tray	183
Use the TAR Alert icon's menu	183
Status of the TAR Alert icon.....	184
View System Tray alert messages.....	185
Appendix C	186
RAID Maintenance	186
Part 1: Hardware Components	186
Part 2: Server Interface	187
LED indicators in SL and HL units	187
Front control panels on H, SL, and HL units	189
Rear panels on H and HL units	191
Part 3: Troubleshooting	192
Hard drive failure.....	192
Step 1: Review the notification email.....	192
Step 2: Verify the failed drive in the Admin console ...	193
Step 3: Replace the failed hard drive.....	194
Step 4: Rebuild the hard drive	195
Step 5: Contact Technical Support.....	198
Power supply failure.....	198
Step 1: Identify the failed power supply.....	198
Step 2: Unplug the power cord	198
Step 3: Replace the failed power supply	199

- Step 4: Contact Technical Support..... 199
- Fan failure 200
- Identify a fan failure 200
- Appendix D 201**
- Glossary 201
- INDEX 205**

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 Enterprise 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.
- **Bandwidth Management Section** - This section includes information on monitoring and managing inbound and outbound traffic on your network.
- **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.*




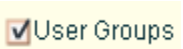
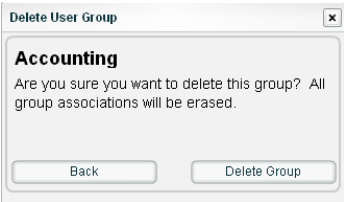

TIP: *The “tip” icon is followed by italicized text giving you hints on how to execute a task more efficiently.*



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.

- **button** - an object in a dialog box, window, or screen that can be clicked with your mouse to execute a command. 
- **checkbox** - a small square in a dialog box, window, or screen used for indicating whether or not you wish to select an option. This object allows you to toggle between two choices. By clicking in this box, a check mark or an “X” is placed, indicating that you selected the option. When this box is not checked, the option is not selected. 
- **dialog box** - a box that opens in response to a command made in a window or screen, 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 screen 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 screen that includes a group of objects such as fields, text boxes, list boxes, buttons, radio buttons, checkboxes, 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 screen that accommodates and/or displays entries of items that can be added or removed.

- **panel** - the top, left, or right section of a screen; the right side which is replaced by a different view when clicking a pertinent 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 screen. 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.

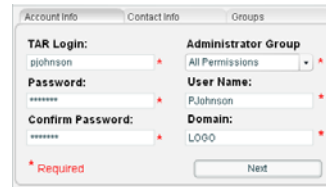
- **pull-down menu** - a field in a dialog box, window, or screen that contains a down arrow to the right. When you click the arrow, a menu of items displays from which you make a selection.



- **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.



- **tab** - one of at least two related pages, each individually labeled and contained within the same window, but only displaying its page in the window when accessed.



- **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** - displays on a screen, and 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 2000 or later operating system (not compatible with Windows server 2003) running Internet Explorer (IE) 6.0 or later, or Firefox 3.0
- Macintosh OS X Version 10.5 running Safari 3.1.2, or Firefox 3.0
- Flash plug-in version 8 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 2.0.00 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 username and password registered during Step 1 of the quick start wizard procedures.

Login window

1. From your workstation, launch Internet Explorer to open an IE 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

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 to 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 **Log In** button to open the application, displaying the URL dashboard gauge view in the right panel by default. The navigation panel displays to the left. In the panel above, the system time and date display (in the HH:MM:SS/MM:DD:YYYY format) beside the Help and Logout buttons:

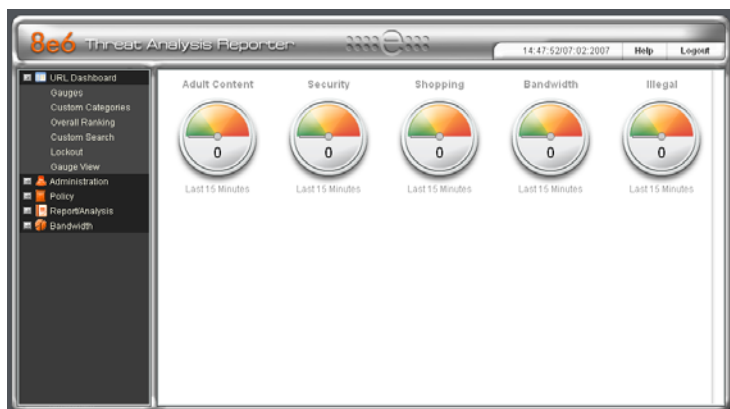


Fig. 1:1-2 Default TAR window

Navigation panel menu topics

The navigation panel at the left of the screen consists of the following menu topics for configuring and using the application:

- **URL Dashboard** - click this topic to access menu options for managing URL gauges that monitor Internet activities which threaten network security, bandwidth usage, and/or end user productivity.
- **Administration** - click this topic to access menu options for setting up and maintaining administrator profiles, and managing the TAR unit.
- **Policy** - click this topic to access menu options for setting up and maintaining policies used for triggering warnings when gauges approach their upper threshold limits.
- **Report/Analysis** - click this topic to access menu options for analyzing Internet usage data.
- **Bandwidth** - click this topic to access menu options for managing bandwidth for protocols used on the network.

Help

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

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.
- **Close all pop-up windows to access another topic** - In order to access another topic from the navigation panel at the left of the screen, all open pop-up windows must first be closed by clicking the “X” in the upper right corner of each 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 back-to-back left and right arrow buttons (circled in the image above) in order to navigate to the previous or next section of the list. In some panels, the <previous and next> buttons display and function in the same manner.

- **Tab to the next field** - Press the Tab key on your keyboard to advance to the next field in a window.
- **Expand, contract a column** - Columns can be expanded or contracted by first

IP	Typ	Severity
202.208.20.3	Lockout	Low
202.208.20.3	Lockout	Medium

mousing over the divider in the column header to display the arrow and double line characters (<-||->). 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 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 windows, 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.

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 panel, click Administration to open that menu.
2. Click User Groups to open the User Groups management panel, which is comprised of the User Groups frame to the left and its target frame to the right:

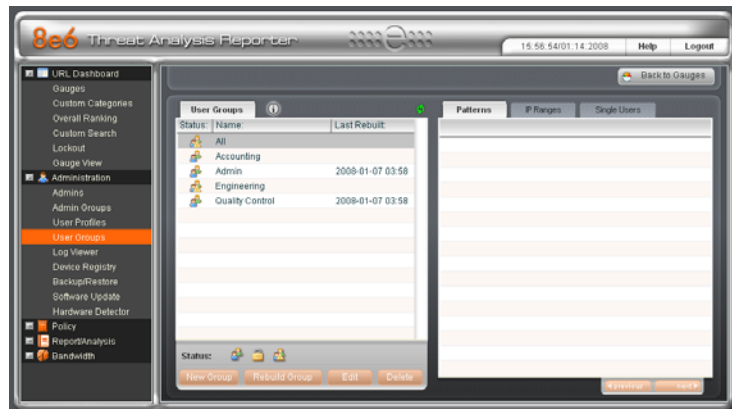


Fig. 2:1-1 User Groups management panel

If any user groups were previously added by the administrator, these display in the User Groups frame in a white- or orange-colored row. Imported user groups display in grey-colored rows. For the global administrator, “All” displays in a grey-colored row 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, or rebuild a user group on demand.



TIPS: Anywhere a grey circled “i” icon appears in a user groups panel, mousing over that icon displays information about entries or actions that can be made in that panel.

Click **Back to Gauges** in the upper right corner of the panel 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 on the Name to highlight the row. Based on this selection, the following occurs:
 - If the selected user group is ready to be rebuilt, this action activates all buttons below (New Group, Rebuild Group, Edit, Delete).
 - If the selected user group was not imported and cannot be rebuilt on demand, this action activates the New Group, Edit, and Delete buttons.
 - If the selected user group was imported and cannot be rebuilt on demand, this action highlights the New Group button only.

2. Click any of the tabs in the frame to the right in order to view pertinent information:
- Patterns tab - view patterns previously set up for that user group.
 - IP Ranges tab - view Starting IP and Ending IP ranges previously added for that user group.
 - Single Users tab - view a list of the individual users previously selected from the Available Users list for that user group.

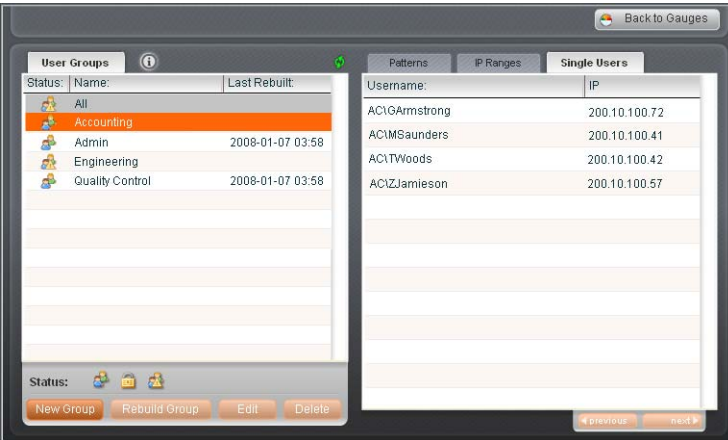


Fig. 2:1-2 View user group information, Single Users tab



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

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

Add a User Group

To add a new user group:

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

Fig. 2:1-3 Add user group, Patterns tab

This panel for adding a user group is comprised of the Group Name field at the top, and the following tabs populated with information from the base group: Patterns, IP Ranges, and Single Users. By default, the Patterns tab displays.

3. Make entries in any of the tabs—as described in the tab sub-sections on the following pages.
4. Enter at least three characters for the **Group Name** to be used for the new user group; this action activates the Save button.



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 management panel.

5. After making entries in the pertinent tabs, click **Save** to save your edits, and to redisplay the main User Groups management panel where the user group you added now displays in the User Groups list box.

Patterns tab

When creating a user group, the Patterns tab 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 a grey-colored row 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 frame to display that pattern in the blank field above.
 - To add a new pattern, enter that pattern in the blank field above. 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 to the right.



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 display the panel that shows the Patterns frame to the left and the Resolved Users frame to the right:

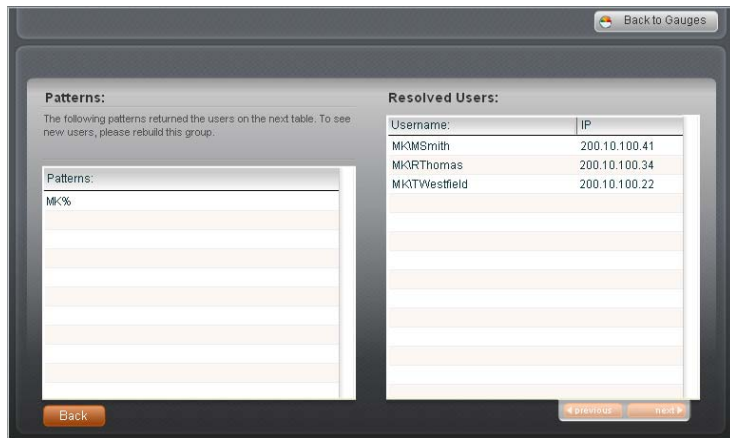


Fig. 2:1-4 Add user group Patterns, Preview Users

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

3. Click the **Back** button to return to the previous panel.

Remove a pattern

To remove a pattern you added:

1. In the Patterns tab, 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 tab

When creating a user group, the IP Ranges tab is used for specifying IP ranges to be used by the new group. The left side of this tab includes fields for entering an IP range or single IP address and netmask. The right side of this tab includes a frame with Parent Ranges. Default Parent Ranges display in a grey-colored row. The Assigned Ranges list box below will include any IP ranges that have been added.



NOTE: *If using IP group authentication, parent ranges do not display in this tab 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.*

The screenshot shows the 'IP Ranges' tab of a user group configuration window. At the top, there is a 'Group Name' field and 'Save' and 'Cancel' buttons. Below this are three tabs: 'Patterns', 'IP Ranges' (selected), and 'Single Users'. A 'Back to Gauges' button is in the top right corner.

The 'IP Ranges' section contains the following elements:

- IP Ranges:** A text area with instructions: "Please type a valid IP range, or you can use the 'Range Calculator' below. Duplicate ranges are not acceptable. The 'From' IP can't be larger than the 'To' IP." Below this are fields for 'Starting IP' and 'Ending IP' with a double-headed arrow between them, and an 'Add IP Range' button.
- Calculate IP Range:** A checkbox labeled 'Calculate IP Range'. Below it are fields for 'IP Address' and 'Netmask', and a 'Calculate Range' button.
- Parent Ranges:** A section titled 'Parent Ranges: Parent ranges are not inherited by default'. It contains a table with 'Starting IP' and 'Ending IP' columns. The first row is highlighted in grey and contains '0.0.0.0' and '255.255.255.255'.
- Assigned Ranges:** A section titled 'Assigned Ranges' containing a table with 'Starting IP' and 'Ending IP' columns. It is currently empty.
- A 'Remove IP Range' button is located at the bottom right of the 'Assigned Ranges' table.

Fig. 2:1-5 Add user group, IP Ranges tab

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 frame 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 at the left of the tab. 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 which activates the IP Address and Netmask fields below.
 - b. Enter the **IP Address**.
 - c. Enter the **Netmask** which activates the Calculate Range button.
 - d. Click **Calculate 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:

Group Name: Save Cancel Back to Gauges

Patterns IP Ranges Single Users

IP Ranges:
Please type a valid IP range, or you can use the "Range Calculator" below. Duplicate ranges are not acceptable. The "From" ip can't be larger than the "To" ip.

Starting IP: 200 10 0 0 Ending IP: 200 10 255 255
Add IP Range

☒ Calculate IP Range
IP Address: 200 10 100 150 Netmask: 255 255 0 0
Calculate Range

Parent Ranges: Parent ranges are not inherited by default.

Starting IP:	Ending IP:
200.10.100.0	255.255.255.255

Assigned Ranges

Starting IP:	Ending IP:
200.10.0.0	200.10.255.255

Remove IP Range

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 User tab

When creating a user group, the Single Users tab is used for adding one or more users to the group. This tab includes a Filter to be used with the Available Users frame that is populated with individual users from the base user group. For each record in the list, the Username/IP address and corresponding IP address display. The frame to the right includes the target Assigned Users, Add, and Delete tabs. The Assigned Users tab displays by default.



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

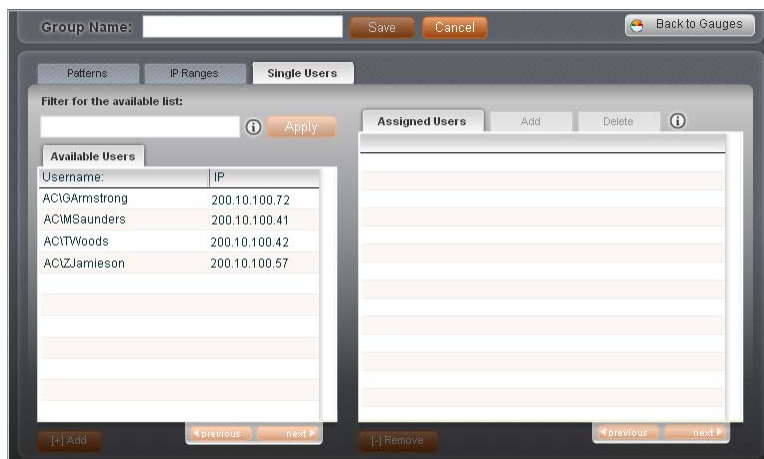


Fig. 2:1-7 Add user group, Single Users tab

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 filter.

Use the filter to narrow Available Users results

To use the available user list 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 frame.

Select users to add to the Assigned Users list

To make selections from the Available Users frame:

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 that now displays to the right.

 **NOTE:** Users added to the Add tab will still be listed in the Available Users list.

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:

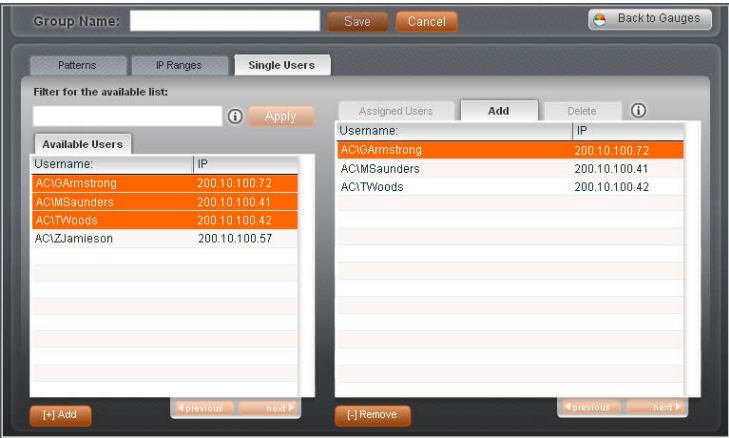


Fig. 2:1-8 Add user group, remove user from Single Users tab

- 2. Click **[-] Remove** button 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 management panel, select the user group from the list in the User Groups frame.
2. Click **Edit** to display the first tab in the user groups panel with settings made in it for that user group—i.e. if the Patterns tab had a setting made in it, that tab displays; if the Single Users tab was the only tab with settings made in it, that tab displays.
3. Make any of these edits in a tab or field:
 - Click a tab to access it, and then make any necessary modifications:
 - Patterns tab - add or remove a pattern.
 - IP Ranges tab - add or remove an IP address range.
 - Single Users tab - add or remove one or more users.



NOTE: When editing the Single Users tab, 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 main User Groups management panel.

Rebuild the User Group

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

1. In the main User Groups management panel, select the user group to be rebuilt.
2. Click **Rebuild Group** to change the user group's status to rebuilt, to make the screen turn hazy, and to open the Rebuild Started! alert box with the message: "Your group rebuild has started. This action might take a few minutes".
3. Click **OK** to close the alert box, and to make the screen reappear as normal.
4. After a few minutes, click the green reload icon above the User Groups frame to refresh the status of the rebuilt user group. Note in the User Groups frame, 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 main User Groups management panel, select the user group from the User Groups list.
2. Click **Delete** to turn the screen hazy, and to open the Delete dialog box with the message: "Do you really want to delete this 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 Cancel to close the dialog box and to return to the main User Groups management panel.*

3. Click **OK** 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 panel, click Admin Groups to open the Group Management pop-up window:

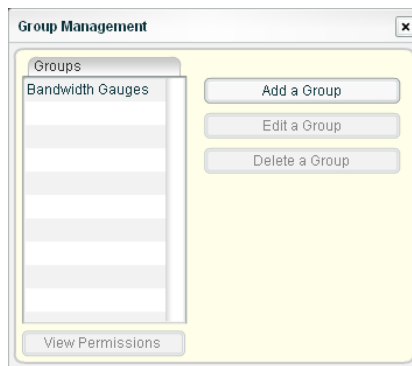


Fig. 2:2-1 Group Management

Groups previously set up display in the Groups frame.

From this pop-up window, 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. Click **Add a Group** to open the Add a new Group pop-up window:

Fig. 2:2-2 Add a new Group

2. 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. By default, “Gauges” is selected and therefore greyed-out. This indicates the administrator to be added will be able to view and modify gauge content. Click the appropriate checkbox(es) to specify the type of access the administrator will be granted on the TAR console or its related devices:
 - User Profiles - manage a list of end users’ logged events
 - Admins - manage group administrator profiles
 - Backup/Restore - perform a backup and/or restoration on the TAR server
 - Admin Groups - manage administrator groups
 - User Groups - manage user groups

- Alerts - manage alerts that indicate if gauges are close to—or have reached—their established upper thresholds
- 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
- Reporter - access the ER application to generate reports on end user Internet activity
- Bandwidth Gauges - monitor and manage bandwidth gauges for inbound and outbound traffic



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

4. Click **Submit** to close both pop-up windows. The Group Name you just entered will appear in the Groups frame the next time you open the Group Management pop-up window.

View an Admin Group's Permissions

1. In the Group Management pop-up window, click the name of the administrator group to highlight the group name and to activate all buttons:

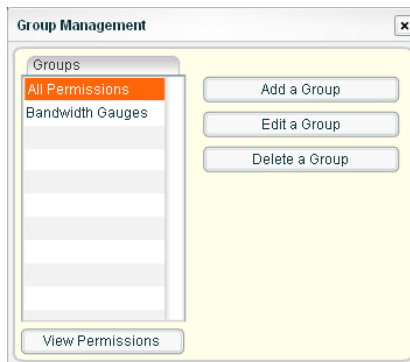


Fig. 2:2-3 Group Management, selection

2. Click **View Permissions** to open the Permissions Viewer pop-up window:

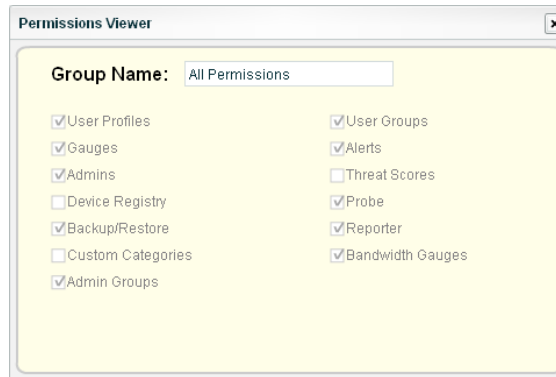


Fig. 2:2-4 Permissions Viewer

3. Note the available features in this pop-up window. In addition to the selections mentioned in the Add a Group sub-section, the following administrator functions are listed:

- 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, and devices connected to TAR
- Custom Categories - maintain the list of custom library categories to be used by gauges, and synchronize the source R3000's custom categories with TAR
- Threat Scores - manage the severity levels for library categories

These permissions are reserved for the global administrator and cannot be assigned to group administrators.

4. Click the “X” in the upper right corner of the Permissions Viewer pop-up window to close it.

Edit an Administrator Group

1. In the Group Management pop-up window, click the name of the administrator group to highlight the group name and to activate all buttons (see Fig. 2:2-3).
2. Click **Edit a Group** to open the Edit Group pop-up window:

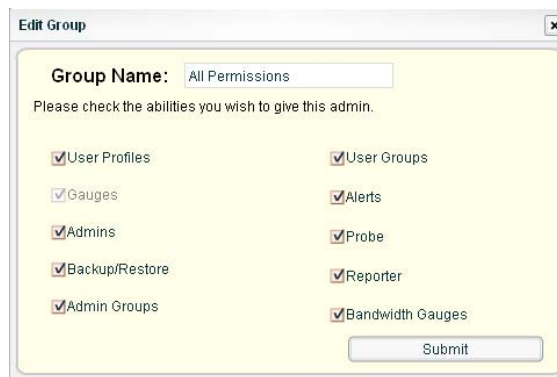


Fig. 2:2-5 Edit Group

3. Perform any of the following actions:
 - Modify the Group Name
 - Add functions to be monitored by the administrator
 - Remove functions to be monitored by the administrator
4. Click **Submit** to close the Edit Group and Group Management pop-up windows.

Delete an Administrator Group

1. In the Group Management pop-up window, click the name of the administrator group to highlight the group name and to activate all buttons (see Fig. 2:2-3).
2. Click **Delete a Group** to open the Delete Group dialog box:

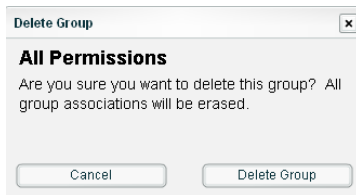


Fig. 2:2-6 Delete Group

3. Click **Delete Group** to remove the administrator group. This action closes the dialog box and the Group Management pop-up window.



NOTE: Clicking *Cancel* closes the dialog box without removing the administrator group, and returns you to the Group Management pop-up window.

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.

1. In the navigation panel, click Admins to open the Admin System pop-up window:

Fig. 2:3-1 Admin System

At the left side of this window, the Active Users frame displays TAR Login IDs of administrator accounts previously set up in this window.



NOTE: In addition to seeing account IDs he/she set up in this window, 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.

From this pop-up window, you view account information for an existing administrator, add a group administrator

profile using the Add new Administrator wizard, and modify or delete a group administrator profile, as necessary.

2. After performing the intended actions in this window, click the “X” in the upper right corner of the window to close it.

View Account Info

In the Active Users frame, click the TAR Login ID of the administrator to display that user’s account information in the Account Info frame:

The screenshot shows the 'Admin System' window with the 'Account Info' tab selected. On the left, the 'Active Users' list contains 'jsmith', 'pjohnson' (highlighted), and 'tjones'. Below this list are 'Add New Admin' and 'Delete Admin' buttons. The main area displays the account details for 'pjohnson':

- Employee Name:** Phil Johnson *
- TAR Login:** pjohnson *
- Administrator Group:** All Permissions (dropdown) *
- Work Phone:** 714 282 6111 *
- Home Phone:** (empty field)
- Email:** pjohnson@logo.com *
- Location:** (empty field)
- LDAP Username:** pjohnson
- Domain:** LOGO
- Comments:** (empty text area)
- User Groups:** Accounting (list box)

Buttons include 'Change Password' (next to TAR Login), 'Add group' and 'Remove' (next to User Groups), and a 'Save' button at the bottom right.

Fig. 2:3-2 Admin System, Active Users selection

View Account Info

The following entries saved for the administrator's account display in the Account Info frame: Employee Name, Work Phone, Email address, TAR Login, User Groups.

Additionally, if any of the following optional entries were saved for the administrator's account, these also display: Home Phone, Location information, LDAP Username, Domain, Comments.



NOTES: *By default, the Administrator Group pull-down menu displays the first alphanumeric entry in the list—this does not reflect the selection saved for the group administrator's profile.*

The global administrator profile that was created during the quick start wizard hardware installation process displays at minimum the TAR Login ID and Email address. For this profile, the Administrator Group field does not display and the User Groups list box is empty, since this administrative account receives email alerts about maintaining the TAR unit, and does not manage user groups.

Add an Administrator Profile

Use the Add new Administrator wizard to add a group administrator profile.

Account Info tab

1. Click **Add New Admin** to open the Add new Administrator pop-up window:

The screenshot shows a 'Add new Administrator' dialog box with the 'Account Info' tab selected. The form contains the following fields and values:

- TAR Login:** pjohnson *
- Password:** ***** *
- Confirm Password:** ***** *
- Administrator Group:** All Permissions *
- LDAP Username:** pjohnson
- Domain:** LOGO

A red asterisk and the text '* Required' are shown at the bottom left. A 'Next' button is located at the bottom right.

Fig. 2:3-3 Add new Administrator, Account Info

2. Type in the **TAR Login** ID the group administrator will use to access the TAR interface.
3. 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.
4. Select the **Administrator Group** (previously set up in the Admins Group menu option) from the available choices in the pull-down menu.
5. If the administrator has an Active Directory LDAP account, username, and domain, type in the alphanumeric group administrator's **LDAP Username** exactly as set up on the Active Directory domain in which he/she is registered.

6. If an entry was made in the LDAP Username field, type in the exact characters for the LDAP Active Directory **Domain** name in which the group administrator is registered.



NOTE: If the group administrator will be using the System Tray feature—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 Username 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.)

7. Click **Next** to go to the Contact Info tab.

Contact Info tab



TIP: Click **Back** at the bottom left of this tab if you need to return to the Account Info tab.

1. Type in the group administrator’s **Employee Name**.

The screenshot shows a dialog box titled "Add new Administrator" with a close button (X) in the top right corner. It has three tabs: "Account Info", "Contact Info" (which is selected), and "Groups". The "Contact Info" tab contains the following fields:

- Employee Name:** A text box containing "Phil Johnson" with a red asterisk to its right.
- Work Phone:** A text box containing "714 123 4567" with a red asterisk to its right.
- Home Phone:** An empty text box.
- Email:** A text box containing "pjohnson@logo.com" with a red asterisk to its right.
- Location:** An empty text box.
- Comments:** A large empty text area.

At the bottom of the dialog box are two buttons: "Back" on the left and "Next" on the right.

Fig. 2:3-4 Add new Administrator, Contact Info

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

3. Optional: Type in the group administrator's **Home Phone** number without entering any special characters.
4. Type in the group administrator's **Email** address.
5. Optional: Type in identifying information about the group administrator's physical office **Location**.
6. Optional: Type in any **Comments** to be associated with the group administrator's account.
7. Click **Next** to go to the Groups tab.

Groups tab



TIP: Click **Back** at the bottom left of this tab if you need to return to the **Contact Info** tab.

In the Group tab you select the user group(s) to be monitored by the group administrator.

Fig. 2:3-5 Add new Administrator, Groups

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



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

3. After selecting each user group to be assigned to the group administrator, click **Submit** to close the Add new Administrator pop-up window and to return to the Admin System pop-up window. Note that the Active Users frame now includes the group administrator's TAR Login ID.

Edit Account Info

1. In the activated Account Info frame:
 - The following information can be modified or updated: Employee Name, TAR Login ID, Administrator Group selection, Work Phone number, Email address, LDAP Username or Domain name—the latter two fields are available if using LDAP.
 - The following information can be added, modified, or deleted: Home Phone number, Location information, Comments.
 - The following actions can also be performed: Change (TAR Login) Password, Add (a user) group, or Remove (a user) group.



TIP: See the *Change Password and User Groups: Add or remove a group sub-sections* for information on updating passwords and user group selections.

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

Change Password

1. In the activated Account Info frame, click Change Password to open the Change Password pop-up window:

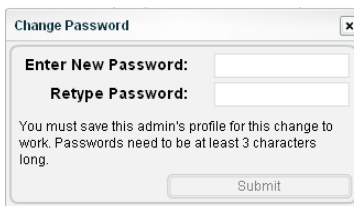
A screenshot of a 'Change Password' dialog box. The dialog has a title bar with the text 'Change Password' and a close button (X). Inside, there are two text input fields: the first is labeled 'Enter New Password:' and the second is labeled 'Retype Password:'. Below these fields, there is a note: 'You must save this admin's profile for this change to work. Passwords need to be at least 3 characters long.' At the bottom right of the dialog is a 'Submit' button.

Fig. 2:3-6 Change Password

2. Type the new password in the **Enter New Password** field, and the **Retype Password** field. These entries display as asterisks for security purposes.
3. Click **Submit** to close the Change Password pop-up window and to activate the new password.



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.

User Groups: Add or remove a group

Add a group

1. In the User Groups section of the activated Account Info frame, click **Add group** to open the Add new user group pop-up window:

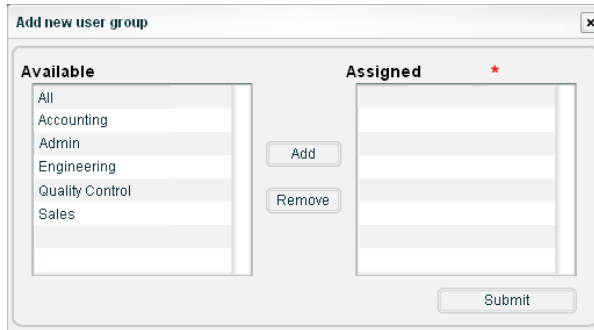


Fig. 2:3-7 Add new user group

2. Select the user group(s) from the Available list, and then click **Add** to include the user group(s) in the Assigned list box.



NOTE: A user group added to the Assigned list box can be removed, but at least one user group must be included in the Assigned list box in order to save your entries.

3. After adding the user group(s) to the Assigned list box, click **Submit** to close the Add new user group pop-up window, and to display the added group(s) in the User Groups list box of the Admin System pop-up window.

Remove a group

1. In the User Groups section of the activated Account Info frame, select the user group in the list box to highlight it.
2. Click **Remove** to remove the user group from the list box.
3. Click **Save** to save your edits.

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 System pop-up window, select the TAR Login ID of the group administrator from the Active Users frame.
2. Click **Delete Admin** to open the Delete Administrator dialog box:

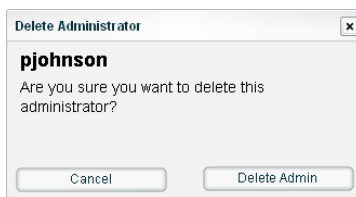


Fig. 2:3-8 Delete Administrator



TIP: Clicking **Cancel** closes the dialog box without removing the group administrator profile, and returns you to the Admin System pop-up window.

3. Click **Delete Admin** to close the dialog box and to remove the group administrator profile.

CONFIGURATION SECTION

Introduction

The Configuration Section of this user guide is comprised of five 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: Threat Score Setup - This chapter explains how the global administrator assigns a threat score “weight” to each library category on the source (primary) R3000 connected to this TAR server. A threat score is a component that influences gauge movement.
- 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 Web Usage Trends - This chapter explains how URL trend reports 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: View User Category Activity - This chapter explains how to perform a custom search on Internet/network activity performed by a specified user or within a specified category.

Chapter 1: Threat Score Setup

After setting up group administrators with access to the TAR server, the global administrator should assign a threat score “weight” to each library category on the source R3000 connected to TAR. A threat score is a component that influences gauge movement.

Anatomy of a Gauge

Understanding the anatomy of a gauge will help you determine the threat score to assign a library category affecting that gauge.

The illustration below depicts a URL dashboard gauge and a library category gauge:

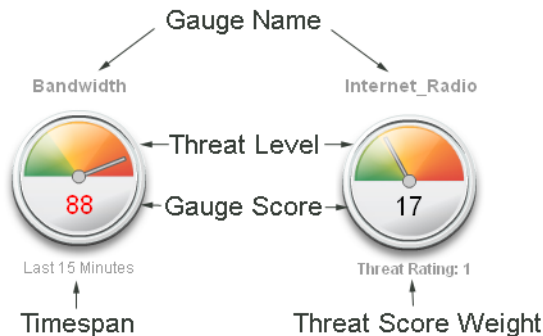


Fig. 3:1-1 URL dashboard gauge anatomy

The name of the gauge displays above the gauge icon. The timespan for the gauge’s activity displays beneath the URL dashboard gauge icon, while the threat score weight displays beneath the library category gauge icon.

The gauge itself is comprised of three colored sections above: One of the sections in which the gauge’s dial is positioned. The bottom section of the gauge contains its numerical score.

Gauge score methodology

The numerical score displayed inside the URL dashboard gauge icon is based upon: The library categories included in the gauge, the threat score assigned to each library category, and the total score of all end users assigned to a specific gauge. The score is calculated as follows: Page count, plus blocked object count, multiplied by the threat score assigned to the library category.

For example: A group administrator sets up a custom gauge labeled “Unacceptable Material” that includes the following library categories: Pornography/Adult Content, Child Pornography, and Shopping. Pornography/Adult Content and Child Pornography have been assigned a threat score of “3” and Shopping has been assigned a threat score of “2”. Bob, Larry, and Sue are included as members to monitor in the custom gauge. In this example, Bob accesses a Web page categorized as Pornography, and Sue goes to a Web page categorized as Shopping. As a result of these end users’ activity, the gauge shows a “score” of “5” (score of “3” for Bob plus a score of “2” for Sue).

View Assigned Threat Score Weights

1. In the navigation panel, click Policy to open that menu.
2. Click Threat Score to open the Scoring Weight Editor pop-up window:

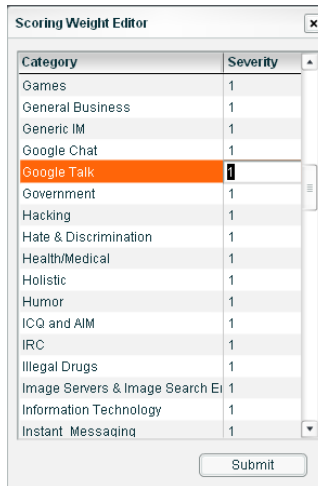


Fig. 3:1-2 Scoring Weight Editor

All library categories set up on the source R3000 connected to this TAR server display in the Category list. By default, each Category is assigned a Severity threat score weight of “1”, indicating a “low” threat.



NOTE: In order to reduce complexity, it is recommended that first time users of TAR should leave all threat score weights at “1”.

3. After performing the intended actions in this window, click the “X” in the upper right corner of the window to close it.

Assign a Threat Score Weight

1. Click the Category to highlight it.
2. Click in the Severity column to make the field editable.
3. One of the following entries can be made:
 - Enter **1** to assign a low threat score for the least dangerous sites, such as those in the News category
 - Enter **2** to assign a medium threat score for mid-level threats, such as Shopping or Sports categories
 - Enter **3** to assign a high threat score for the most dangerous sites, such as those in the Child Pornography category
4. After modifying all threat scores, click **Submit**.

Chapter 2: Custom Gauge Setup, Usage

With threat score weights established, a group administrator can begin setting up gauges for monitoring end users' Internet activity.

1. In the navigation panel, go to the URL Dashboard and click Gauges to open the Gauge Management pop-up window:

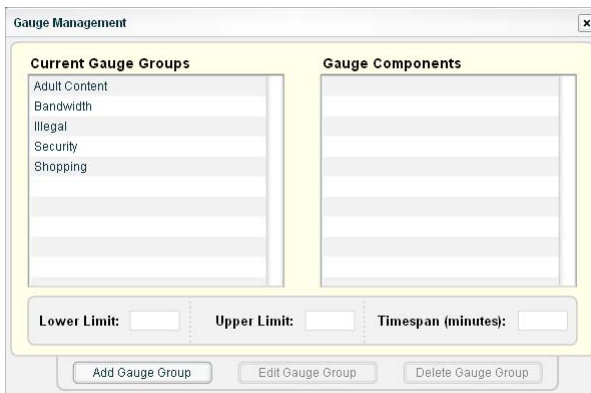


Fig. 3:2-1 Gauge Management

By default, the Current Gauge Groups include: Adult Content, Bandwidth, Illegal, Security, Shopping.

2. In the Current Gauge Groups list box, click the gauge name to display a list of library categories and threshold criteria set up for that gauge:

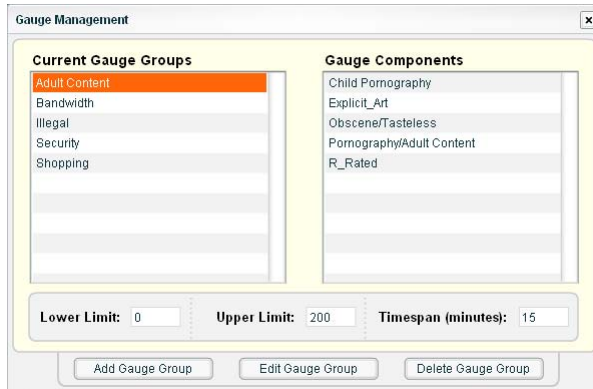


Fig. 3:2-2 Gauge Management, Gauge Components

3. To exit this window, click the “X” in the upper right corner of the window to close it.

Add a Gauge

In the Gauge Management window, click **Add Gauge Group** to open the Add a new Gauge Group pop-up window:

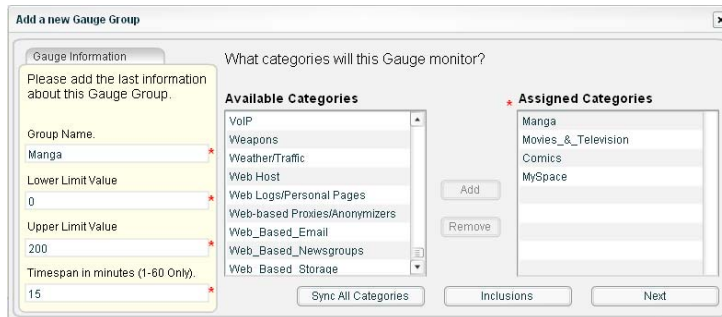


Fig. 3:2-3 Add a new Gauge Group

When adding a gauge group, you need to do the following:

- Name the gauge, and specify limit and timespan values
- Synchronize all library categories from the source R3000 with the TAR unit
- Select library categories for the gauge to monitor
- Assign user groups whose end users' Internet/network activity will be monitored by the gauge
- Verify limit values for library categories included in the gauge, and specify the library category method(s) to be used by the gauge

Add Gauge Information

In the Gauge Information box:

1. Type in at least four characters for the **Gauge Name** using upper and/or lowercase alphanumeric characters, and spaces, if desired.
2. Type in the **Lower Limit Value** of the floor for any gauge activity. The recommended value is **0** (zero).
3. Type in the **Upper Limit Value** of the ceiling for gauge activity. The recommended value is **200**. This can be adjusted after using TAR for awhile and evaluating activity levels at your organization.
4. Type in the **Timespan in minutes (1-60 Only)** for tracking gauge activity; usually **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.

Sync All Categories

To synchronize 8e6 supplied library category updates and custom libraries from the source R3000 to this TAR unit, click **Sync All Categories**.

Select Library Categories

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



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

1. From the Available Categories list, select one or more library categories.
2. Click **Add** to move the selection(s) to the Assigned Categories list box.



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

Assign User Groups

To assign user groups to be monitored by the gauge:

1. Click **Inclusions** to open the Assign Groups pop-up window:

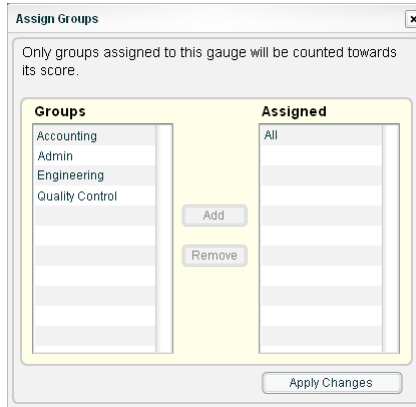


Fig. 3:2-4 Assign Groups



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



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

4. After adding groups, click **Apply Changes** to close the Assign Groups pop-up window, and to return to the Add a new Gauge Group pop-up window.

- Click **Next** to open the second Add a new Gauge Group pop-up window that includes information about the components of the gauge.

View, edit library components

In the second Add a new Gauge Group pop-up window, view and edit settings for any library category set up for the gauge:

	Lower Limit	Upper Limit
Manga	0	200
Movies_ & _Television	0	200
Comics	0	200
MySpace	0	200

Set a gauge method: All

Next

Fig. 3:2-5 Add a new Gauge Group, gauge components

- The floor and ceiling threshold settings that were established for the gauge group display in the Lower/Upper Limit fields of each library category. These values can be edited, as necessary.
- If necessary, make a selection from the **Set a gauge method** pull-down menu to change the end user Internet usage method(s) for determining gauge activity: All (default), Keyword, URL, Others (passed categories).



NOTE: If the selected gauge method is "Keyword" or "URL", 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.

3. Click **Next** to close the Add a new Gauge Group windows and to display the new gauge in the URL dashboard gauge view:

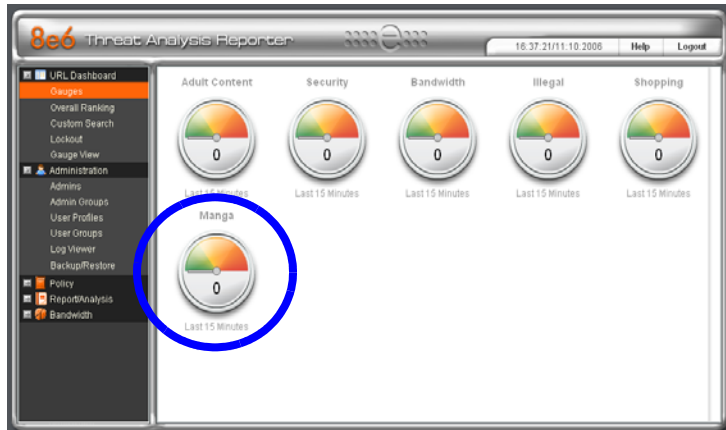


Fig. 3:2-6 New Gauge Group added

Gauge Components and Activity

Types of gauges

There are four types of gauges: URL dashboard gauges, library category gauges, protocol bandwidth gauges, and port gauges.

Gauges that display in the URL dashboard are comprised of library categories. Library category gauges display in a pop-up window for the URL dashboard gauge.

Inbound/Outbound protocol bandwidth gauges are comprised of ports. Port gauges display in the a pop-up window for the protocol bandwidth gauge. (See Bandwidth Management Section.)

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 the gauge—green (safe) section, yellow (warning) section, or red (network threat) section—and by a numerical “score” displayed in the middle of the gauge icon. This score is based upon the type of Internet activity, threat score, timespan, and upper and lower thresholds established for the gauge.

The score displayed in the middle of the gauge icon 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 black text. If the threat for a gauge is high (exceeding 66 percent of the ceiling established for a gauge group or gauges contained within the group), the score displays in flashing red text. However, if the score drops below 66 percent within the timespan set up for the gauge, the text changes from blinking red to solid black again.

If a gauge group (“parent” gauge) displays flashing red text while its dial is positioned in the green or yellow sections, this is indicative that the dial on at least one “child” gauge contained within the gauge group is currently positioned in the red section.

The image to the right shows the URL dashboard’s Bandwidth gauge, comprised of several library category gauges. Note the timespan for gauge activity displays beneath the gauge icon. In this example, the hit score displays flashing in red and the dial is positioned in the red section of the gauge, currently indicating a high threat score for this gauge. 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.

Inbound/Outbound protocol bandwidth gauges also display the timespan for gauge activity beneath the gauge icon. However, unlike URL dashboard gauges, instead of displaying the total hit score in the middle of the icon, protocol bandwidth gauges display the total byte score. As with URL dashboard gauges, the score in the middle of the icon displays in flashing red text if activity registers in the upper threshold limit established for the gauge. (See Bandwidth Management Section.)

The image to the right shows a gauge for the Internet_Radio library category in the URL dashboard's Bandwidth gauge. Note the Threat Rating displays beneath the gauge icon. In this example, the text displays in black and the dial is positioned in the green section of the gauge, indicating that there is no immediate threat for this library category. If a high threat score displays for any library category, the source of the threat can be investigated by drilling down into the gauge.



Modify a Gauge

Edit gauge settings

To edit an existing gauge, click Gauges in the navigation panel to open the Gauge Management pop-up window:

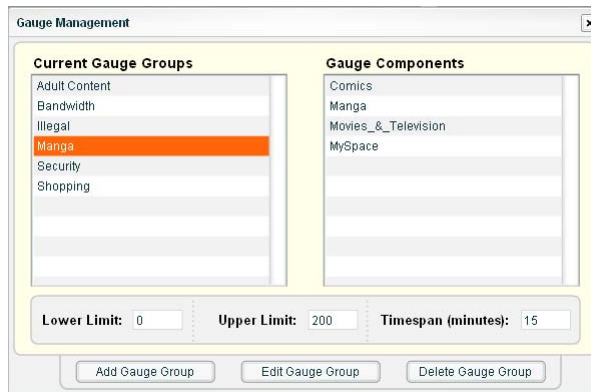


Fig. 3:2-7 Group Management, edit gauge

1. In the Current Gauge Groups list box, select the gauge to be edited. This action highlights the gauge name and populates the Gauge Components box with a list of library categories set up to be monitored by that gauge.
2. Click the **Edit Gauge Group** button to open the Edit Gauge Group pop-up window:

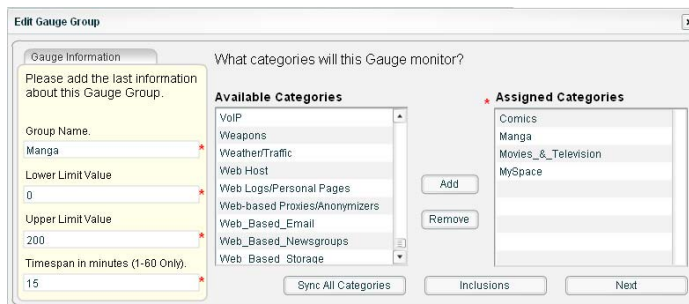


Fig. 3:2-8 Edit Gauge Group



TIP: The Edit Gauge Group pop-up window is also accessible by right-clicking a URL dashboard gauge, and then selecting Edit Gauge Group from the pop-up menu (see Fig. 3:2-12).

3. Edit any of the following criteria, as necessary:
 - Gauge Information - Gauge Name, Lower/Upper Limit Value(s), Timespan in minutes (see Add Gauge Information)
 - Assigned Categories (see Select Library Categories)
 - Assigned Groups (see Assign User Groups)
4. Click **Next** to go to the second Edit Gauge Group pop-up window:

	Lower Limit	Upper Limit
Comics	0	200
Manga	0	200
Movies_&Television	0	200
MySpace	0	200

Set a gauge method: All

Save Changes

Fig. 3:2-9 Edit a Gauge Group, gauge components

5. Edit any of the following criteria, as necessary:
 - Lower/Upper Limit fields for gauge activity in each library category
 - Internet usage method for the gauge.
6. Click **Save Changes** to close the Edit Gauge Group windows and to return to the URL dashboard gauges panel.



NOTE: When saving your edits, the gauge hits and score are reset to zero (“0”).

Hide, Show a URL Gauge

If you only want to view certain URL gauges and their associated library categories, options are available to hide specified URL gauges.

Temporarily hide a URL gauge

To hide a URL gauge for the current session only:

1. In the URL dashboard, right-click the gauge to open its pop-up menu (see Fig. 3:2-12).
2. Select Hide Gauge to remove the URL gauge from the current view.



NOTE: Using this option, any gauges hidden during this session will reappear in the next session.

Save settings for hiding a URL gauge

To permanently hide a URL dashboard gauge:

1. Click Gauge View in the URL Dashboard section of the navigation panel to open the Edit Gauge Visibility pop-up window:

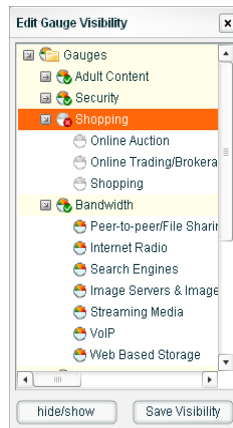



Fig. 3:2-10 Edit Gauge Visibility

This window includes a list of URL gauges, each preceded by a gauge icon. Gauges that are currently visible in the URL dashboard include a green circle with a checkmark in the lower right corner of the gauge icon. Gauges that are currently hidden from view include a red circle with an X in the lower right corner of the gauge icon.




TIP: To view the library categories included in a URL gauge, click the URL gauge name to open the tree. Click the gauge name again to close the list of library categories.

2. Select the URL gauge to be hidden.
3. Click the **hide/show** button to change the icon from the green circle with a checkmark to a red circle with an X. This action also removes the URL dashboard gauge from the current view.

 **TIP:** To redisplay the URL dashboard gauge in the current view, select the gauge and click the hide/show button again.

4. Click **Save Visibility** to save your settings. These settings will remain the next time you log into the TAR server.

 **NOTE:** Gauges that are hidden will not display in trend reports (see View URL Trend Reports in Chapter 4: Analyze Web Usage Trends).

Delete a Gauge

1. To delete a gauge, begin by either selecting the gauge from the dashboard, or by using the navigation panel:
 - If you select the gauge from the dashboard:

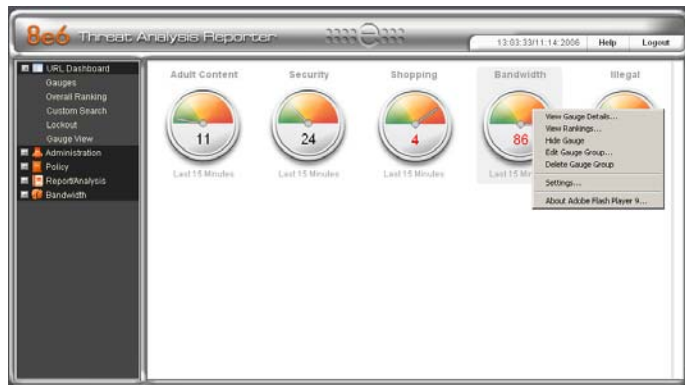


Fig. 3:2-11 Gauge pop-up menu

- a. In the gauges view, right-click the gauge to open its pop-up menu (see Fig. 3:2-11).
 - b. Select Delete Gauge Group to open the Delete Gauge dialog box (see Fig. 3:2-12).
- If you select the gauge using the navigation panel:
 - a. Click Gauges in the navigation panel to open the Gauge Management pop-up window (see Fig. 3:2-7).

- b. In the Current Gauge Groups list, select the gauge to be deleted. This action highlights the gauge name and populates the Gauge Components list box with library categories set up to be monitored by that gauge.
- c. Click the **Delete Gauge Group** button to open the Delete Gauge dialog box (see Fig. 3:2-12).



TIP: Clicking Cancel in the Delete Gauge dialog box closes the dialog box without removing the gauge, and returns you to the Gauge Management pop-up window.

2. Click **Delete Gauge** to remove the gauge:

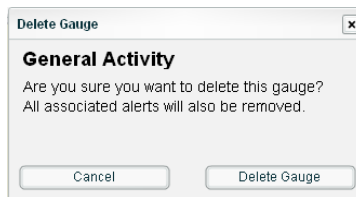


Fig. 3:2-12 Edit Gauge Group

This action closes the dialog box and returns you to the URL dashboard, removing any associated alerts.

View End User Gauge Activity

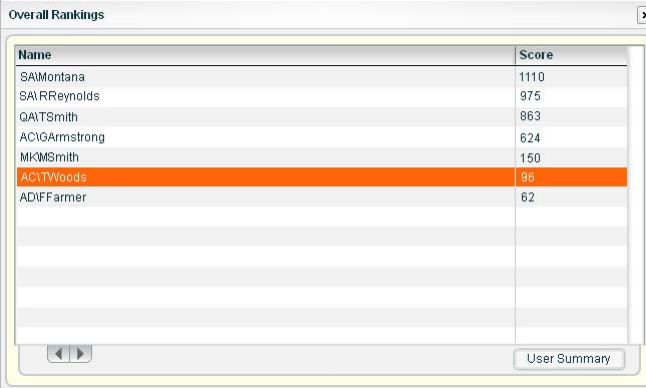
There are several ways to access information on end user gauge activity:

- Overall end user gauge activity - For a snapshot of all current gauge activity ranked in order by the highest to lowest end user score, use the Overall Ranking option (see View Overall Ranking). This option also lets you drill down and view information on gauges affected by a specified end user.
- End user activity by URL gauge - For a snapshot of a URL gauge's current activity ranked in order by the highest to lowest end user score, use the Ranking Table option (see View a URL gauge ranking table).
- End user activity by library category gauge - For a snapshot of a library category gauge's current activity ranked in order by the highest to lowest end user score, use the library category ranking table option (see View a library category ranking table).

View Overall Ranking

To view details about current gauge activity for all end users affecting gauges:

1. In the URL Dashboard section of the navigation panel, click Overall Ranking to open the Overall Rankings pop-up window:



The image shows a pop-up window titled "Overall Rankings" with a close button (X) in the top right corner. Inside the window is a table with two columns: "Name" and "Score". The table lists several users and their corresponding scores, sorted in descending order. The user "ACITWoods" is highlighted with an orange background. At the bottom right of the window is a button labeled "User Summary".

Name	Score
SAIMontana	1110
SAIRReynolds	975
QAITSmith	863
ACIGArmstrong	624
MKMSmith	150
ACITWoods	96
ADVFFarmer	62

Fig. 3:2-13 Overall Rankings

This window includes rows of records for each end user who is currently affecting one or more gauge. For each record in the list, the following information displays: Name (username/IP address), and corresponding Score. End users are ranked in descending order by their score.

2. To drill down and view additional information about an end user's activity, click the Name to highlight it.
3. Click **User Summary** to open the Individual User View pop-up window (see Fig. 3:2-17), and perform any of the actions described for this window (see Monitor, Restrict End User Activity).
4. Click the "X" in the upper right corner of this pop-up window to close it.

View a URL gauge ranking table

To view details about a specified URL gauge's current activity:

1. Right-click the URL dashboard gauge to open its pop-up menu (see Fig. 3:2-12).
2. Choose View Rankings to open the URL gauge's ranking table pop-up window:



Name	Score
MKMSaunders	85
ACITWoods	28
QATSmith	22
SAIReynolds	1

Fig. 3:2-14 URL gauge ranking table

This window includes rows of records for each end user who is affecting this URL gauge. For each record in the list, the following information displays: Name (username/IP address), and corresponding Score. End users are ranked in descending order by their score.



NOTE: The URL gauge's ranking table pop-up window is also accessible via the following options:

- Double-clicking a URL dashboard gauge to open the URL gauge's pop-up window, and then clicking the Ranking Table button.
- Right-clicking a URL dashboard gauge, selecting View Gauge Details from the pop-up menu (see Fig. 3:2-12) to open the URL gauge's pop-up window, and then clicking the Ranking Table button.

3. To drill down and view additional information about an end user's activity, click the Name to highlight it.
4. Click **User Summary** to open the Individual User View pop-up window (see Fig. 3:2-17), and perform any of the actions described for this window (see Monitor, Restrict End User Activity).
5. Click the "X" in the upper right corner of this pop-up window to close it.

View a library category gauge ranking table

To view details about a specified library category gauge's current activity:

1. Right-click the URL dashboard gauge to open its pop-up menu (see Fig. 3:2-12).
2. Choose View Gauge Details to open a pop-up window displaying library category gauges comprising the URL dashboard gauge:

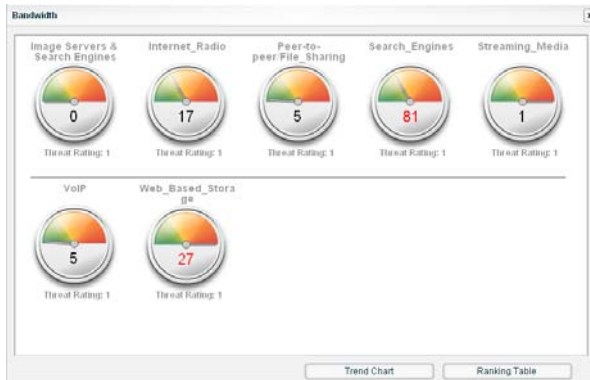
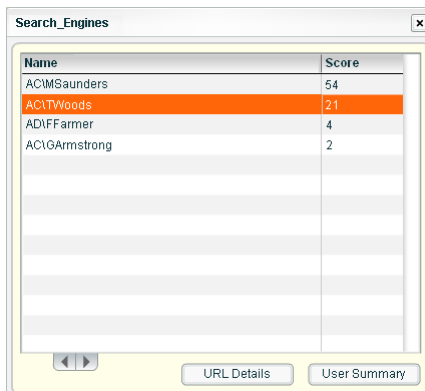


Fig. 3:2-15 Gauge pop-up window



NOTE: The total of all library category gauge scores equals the score of the URL dashboard gauge.

- Click the library category gauge to open its pop-up window:



The screenshot shows a window titled "Search_Engines" with a close button (X) in the top right corner. Inside the window is a table with two columns: "Name" and "Score". The table contains the following data:

Name	Score
ACIMSaunders	54
ACTWoods	21
ADIFFarmer	4
ACIGArmstrong	2

Below the table, there are two buttons: "URL Details" and "User Summary".

Fig. 3:2-16 Library category gauge ranking table

This window includes rows of records for each end user who is affecting this library category gauge. For each record in the list, the following information displays: Name (username/IP address), and corresponding Score. End users are ranked in descending order by their score.



NOTE: The library gauge's ranking table pop-up window is also accessible by double-clicking a URL dashboard gauge to open the URL gauge's pop-up window, and then clicking a library category gauge.

- To drill down and view additional information about an end user's activity, click the Name to highlight it. This action activates the two buttons in this window:
 - URL Details** - click this button to open the View Details pop-up window (see Fig. 3:2-19), and perform the actions described in this window (see View a list of URLs accessed by the user).
 - User Summary** - click this button to open the Individual User View pop-up window (see Fig. 3:2-17), and perform any of the actions described for this window (see Monitor, Restrict End User Activity).

5. After performing the intended actions in this window, click the “X” in the upper right corner of this window to close it.

Monitor, Restrict End User Activity

The Individual User View window lets you view/restrict an end user’s use of the Internet/network.

1. From any of the user ranking windows, with the end user’s record selected, click **User Summary** to open the Individual User View pop-up window:

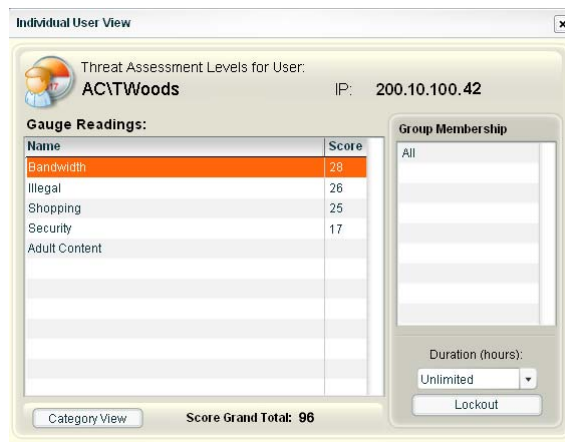


Fig. 3:2-17 Individual User View

This window contains Gauge Readings for each URL gauge Name, ranked in descending order by the end user’s Score for the corresponding gauge. The user-name/IP address and end user’s IP display above. At the right side of this window, the Group Membership to which the user belongs displays above the Duration (hours) pull-down menu and the Lockout button. At the bottom of the window, the Category View button displays to the left of the Score Grand Total for all of the end user’s gauge readings.



TIP: To sort the list in descending order by either Name or Score, click the column header. To sort the list in ascending order, click the column header again.

2. After performing the intended actions in this window, click the “X” in the upper right corner of this window to close it.

View a list of categories accessed by the user

To view a list of categories the end user accessed:

1. In the Individual User View pop-up window (see Fig. 3:2-17), select the Name of the URL dashboard gauge to highlight it.
2. Click **Category View** to open the View by Hits pop-up window:

Category	Hits	Score
Search_Engines	21	21
VoIP	0	0
Streaming_Media	0	0
Web_Based_Storage	0	0
Peer-to-peer/File_Sharing	0	0
Internet_Radio	0	0
Image Servers & Search E	0	0

URL Details

Fig. 3:2-18 View by Hits

A list of each library Category gauge and its corresponding Hits and Score for the URL dashboard gauge displays in this window.

3. Select a library category gauge to highlight it.
4. Click **URL Details** to open the View Details pop-up window (see Fig. 3:2-19) that displays a list of URLs


accessed by the end user within that category (see View a list of URLs accessed by the user).

5. After performing the intended actions in this window, click the “X” in the upper right corner of this window to close it.

View a list of URLs accessed by the user

There are two ways to access the View Details window that contains a list of URLs the end user viewed within a specified category:

- by selecting the library Category, and then clicking the **URL Details** button in the View by Hits pop-up window (see Fig. 3:2-18)
- or
- by selecting the Name (username/IP address), and then clicking the **URL Details** button in the Library category gauge pop-up window (see Fig. 3:2-16)



URL	Timestamp
http://203.89.237.80/	2008-03-02 15:22:12
http://203.89.237.80/	2008-03-02 15:22:07
http://203.89.237.80/siteinclude/default.asp?CentreID=&CentreName=&unlock=§ion=C	2008-03-02 15:22:02
http://203.89.237.80/siteinclude/flashDetect.asp?CentreID=&CentreName=&unlock=§ion=C	2008-03-02 15:22:02
http://203.89.237.80/	2008-03-02 15:22:02
http://203.89.237.80/siteinclude/default.asp?CentreID=&CentreName=&unlock=§ion=C	2008-03-02 15:21:57
http://203.89.237.80/siteinclude/flashDetect.asp?CentreID=&CentreName=&unlock=§ion=C	2008-03-02 15:21:57
http://203.89.237.80/	2008-03-02 15:21:57
http://203.89.237.80/siteinclude/default.asp?CentreID=&CentreName=&unlock=§ion=C	2008-03-02 15:21:17
http://203.89.237.80/siteinclude/flashDetect.asp?CentreID=&CentreName=&unlock=§ion=C	2008-03-02 15:21:17
http://203.89.237.80/	2008-03-02 15:21:17
http://203.89.237.80/siteinclude/default.asp?CentreID=&CentreName=&unlock=§ion=C	2008-03-02 15:21:12
http://203.89.237.80/siteinclude/flashDetect.asp?CentreID=&CentreName=&unlock=§ion=C	2008-03-02 15:21:12

Open URL

Fig. 3:2-19 View Details

In the View Details window, a list of each URL and corresponding Timestamp displays (using military time in the YYYY-MM-DD HH:MM:SS format) for each URL accessed in that library category.



NOTE: Drill Down Reports in the Enterprise Reporter Web Client should be used to obtain a list of clickable URLs. The ER Web Client is accessible by going to the navigation panel and selecting Report/Analysis > ER Reporter.

1. If a URL in the list is linked to a page or object, select the URL in the list, and then click **Open URL** to open the page/object in a separate browser window.
2. After performing the intended actions in this window, click the “X” in the upper right corner of this window to close it.

Manually lock out an end user

To prevent the end user from accessing specified URLs, the Internet, or the entire network:

1. In the Individual User View pop-up window (see Fig. 3:2-17), select the Name of the URL dashboard gauge to highlight it.
2. Specify the **Duration (hours)** for the lockout by making a selection from the pull-down menu (Unlimited, Half Hour, 1, 1-1/2 ... 8).



NOTE: If “Unlimited” is selected, the end user remains locked out of the specified areas on the Internet/network until the administrator unlocks his/her workstation. To “unlock” the end user, go to the Lockout window in the URL Dashboard section of the navigation panel. For information on this feature, see Chapter 3: Alerts, Lockout Management.

3. Click **Lockout** to open the Lockout dialog box:



Fig. 3:2-20 Lockout



TIP: Click No to close this dialog box without locking out the user.

4. Specify the **Severity** of the lockout from the choices in the pull-down menu:

- Low - this selection lets you choose which library category's contents the end user will not be able to access
 - Medium - this selection locks out the end user from Internet access
 - High - this selection locks out the end user from all network access
5. Click **Yes** to proceed.
- If a "Low" severity was selected, clicking **Yes** opens the Lockout by Categories pop-up window:

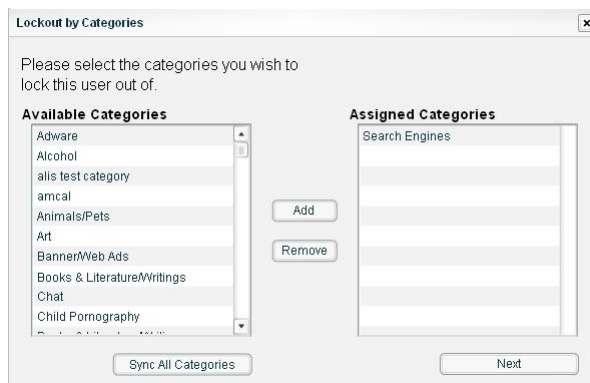


Fig. 3:2-21 Lockout by Categories

- From the Available Categories list, select the available library category containing URLs the end user should not access.
- Click **Add** to move the library category to the Assigned Categories list box.



TIPS: To remove a library category from the Assigned Categories list box, click the library category to highlight it, and then click **Remove** to move the category back to the Available Categories list.

Click **Sync All Categories** after custom library categories have been added to the list, in order to force synchronization between the R3000 and the TAR unit.

- c. After adding all library categories, click **Next** to open the alert box stating: “The user has been locked out.”
- d. Click the “X” in the upper right corner of the box to close it.
- If a “Medium” or “High” severity was selected:
 - a. Clicking **Yes** in the Lockout dialog box opens the the alert box stating: “The user has been locked out.”
 - b. Click the “X” in the upper right corner of the box to close it.

End user workstation lockdown

The following scenario occurs for the end user when he/she is locked out:

- Low severity lockdown - In this scenario, after attaining the designated score established for a gauge, when the end user attempts to access a URL for a library category set up to be monitored by that gauge, the following lockdown page displays for the end user:

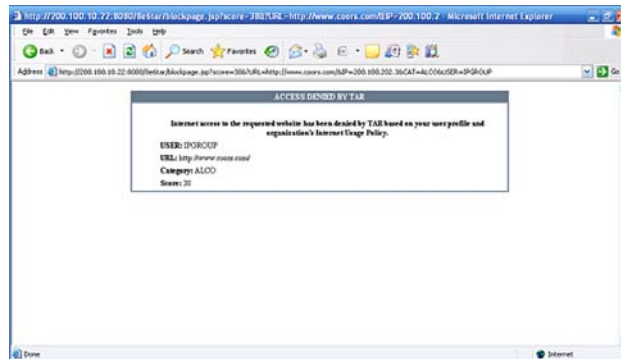


Fig. 3:2-22 Low severity lockdown page

This page contains the following information: message “Access Denied by TAR”, USER name/IP address, URL denied access, Category in which the URL resides, and end user’s Score.

- Medium severity lockdown - In this scenario, after attaining the designated score established for a gauge, when the end user attempts to access any URL, the following lockdown page displays for the end user:

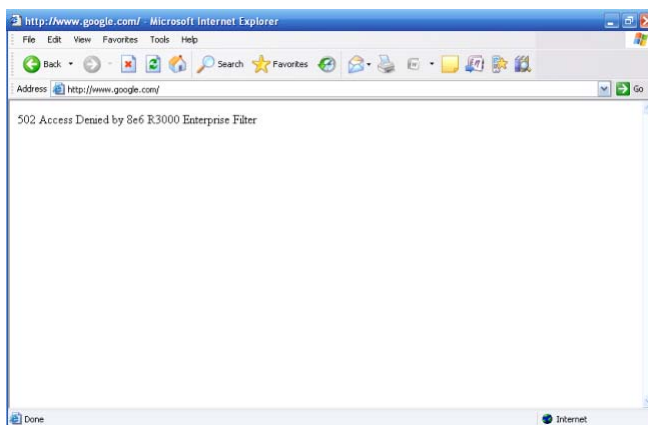


Fig. 3:2-23 Medium severity lockout page

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

- High severity lockout - In this scenario, after attaining the designated score established for a gauge, the end user will be unable to access the organization’s network.

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.

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 Chapters 2 and 3 of the Preliminary Setup Section.

1. In the navigation panel, click Policy to open that menu.
2. Click Alerts to open the Alert Manager pop-up window:

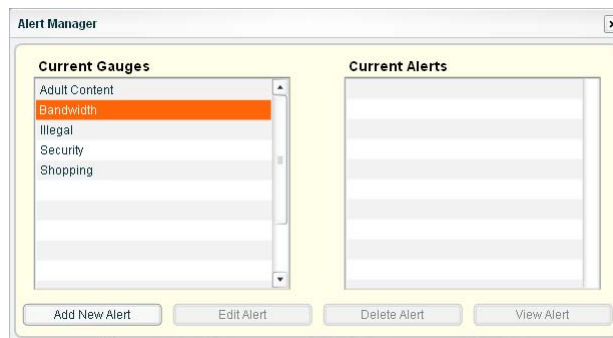


Fig. 3:3-1 Alert Manager

3. After performing the intended actions in this window, click the "X" in the upper right corner of the pop-up window to close it.

Add an Alert

1. In the Current Gauges box, click the gauge for which an alert will be created (see Fig. 3:3-1).
2. Click **Add New Alert** to open the Add a new Alert pop-up window:

Fig. 3:3-2 Add a new Alert

3. Type in the **Alert Name** to be used for the alert that will be delivered to the group administrator.
4. In the **Threshold** field, enter the number for the threshold limit 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 Gauge score methodology in Chapter 1 of this section for information on how scoring is defined.)

5. In the Alert Action portion of the window, 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.
- 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.
- 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.



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

6. After making all entries in this window, click **Submit** to save your entries and to close the Add a new Alert pop-up window.

Email alert function

Configure email alerts

To set up the email alert function:

1. Click the checkbox corresponding to “Email” to display the Email Addresses list box, and associated field and buttons to the upper right of this window.
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 (username/IP address).
- Body of message: User (username/IP address) has triggered the (Alert Name) alert with a threshold of 'X' (in which "X" represents the alert threshold) on the (URL dashboard 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.

Lockout function

Configure automatic lockouts

To set up the lockout function:

1. Click the checkbox corresponding to "Lockout" to display the Severity and Duration (hours) pull-down menus at the right side of this window.
2. Specify the **Severity** of the end users' lockout:
 - Low - choosing this option opens the Lockout by Categories pop-up window (see Chapter 3: Custom Gauge Setup, Usage - Fig. 3:2-15). Specify the library category containing URLs the end user should not access.
 - 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 Lockout window.



TIP: After making your selections, click Submit to save your settings.

System Tray alert function

If using LDAP with an Active Directory username, 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 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.

View, Modify, Delete an Alert

1. In the Alert Manager pop-up window's Current Gauges box, select the gauge for which an alert will be viewed and/or modified:

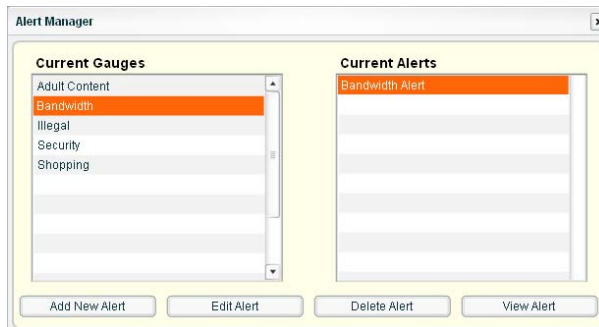


Fig. 3:3-3 Alert Manager

This action populates the Current Alerts box with any existing alerts created for that gauge.

2. Select the alert to be viewed or modified by clicking on it to highlight it.

View alert settings

1. In the Alert Manager pop-up window, click **View Alert** to open the Alert Viewer pop-up window:

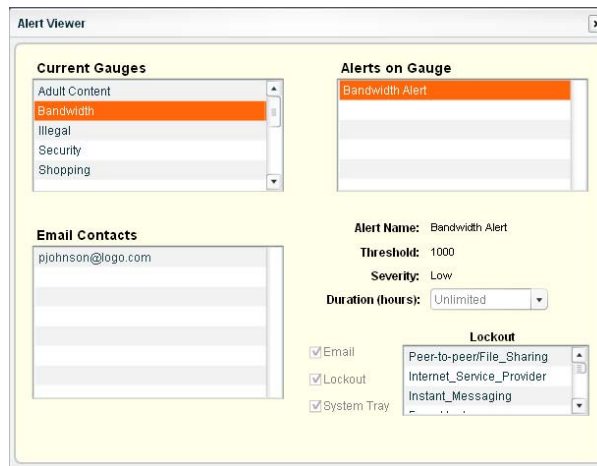


Fig. 3:3-4 Alert Viewer

The Alert Name, Threshold, Severity, and Duration (hours) display, along with any options specified in the Add a new Alert or Edit an Alert pop-up window. These options include Email Contacts; checkbox(es) for Email, Lockout, and/or System Tray features, and Lockout Categories, if a Low Severity was specified.



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 this pop-up window to close it.

Modify an alert

1. In the Alert Manager pop-up window, click **Edit Alert** to open the Edit an Alert pop-up window:

Please fill out the fields below to define the alert. If you choose to have Email associated with the action, enter as many email addresses as required.

Current Gauge

- Adult Content
- Bandwidth**
- Illegal
- Security
- Shopping

Email Addresses

- pjohnson@logo.com

Alert Action

☒ Email

☒ Lockout

☒ System Tray

Severity: Low

Duration (hours): Unlimited

Threshold: 500

Alert Name: Bandwidth Alert

Remove Email Add Email

Categories

Submit

Fig. 3:3-5 Edit an Alert

2. The following items can be edited:
 - Alert Name
 - Threshold
 - Alert Action selections: Email, Lockout, System Tray—the latter is only functional for Active Directory LDAP
 - Email Addresses
 - Severity selection
 - Duration (hours) selection
3. Click **Submit** to save your edits, and to close the Edit an Alert pop-up window.

Delete an alert

1. In the Alert Manager pop-up window, click **Delete Alert** to open the Delete Alert dialog box:

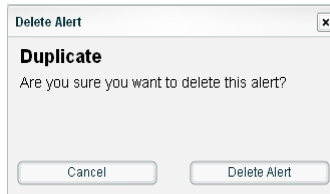


Fig. 3:3-6 Delete Alert

2. Click **Delete Alert** to close the Delete Alert dialog box and to remove the alert from the Current Alerts box.



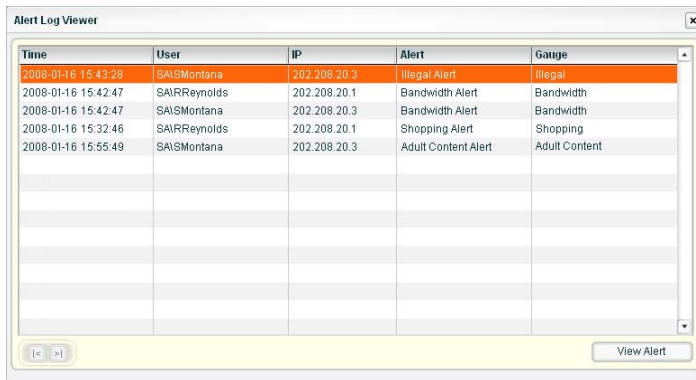
NOTE: Clicking *Cancel* closes the dialog box without removing the alert, and returns you to the Alert Manager pop-up window.

View the Alert Log

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

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 Chapters 2 and 3 of the Preliminary Setup Section.

1. In the Policy menu, click Alert Log to open the Alert Log Viewer pop-up window:



The screenshot shows a window titled "Alert Log Viewer" with a table of alert records. The table has five columns: Time, User, IP, Alert, and Gauge. The first row is highlighted in orange. Below the table are navigation buttons: "< >" and "View Alert".

Time	User	IP	Alert	Gauge
2008-01-16 15:43:28	SA\SMontana	202.208.20.3	Illegal Alert	Illegal
2008-01-16 15:42:47	SA\RRenolds	202.208.20.1	Bandwidth Alert	Bandwidth
2008-01-16 15:42:47	SA\SMontana	202.208.20.3	Bandwidth Alert	Bandwidth
2008-01-16 15:32:46	SA\RRenolds	202.208.20.1	Shopping Alert	Shopping
2008-01-16 15:55:49	SA\SMontana	202.208.20.3	Adult Content Alert	Adult Content

Fig. 3:3-7 Alert Log Viewer

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: Time the alert was sent (using the YYYY-MM-DD HH:MM:SS military time format), User (username/IP address), IP address, Alert name, Gauge name.



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

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

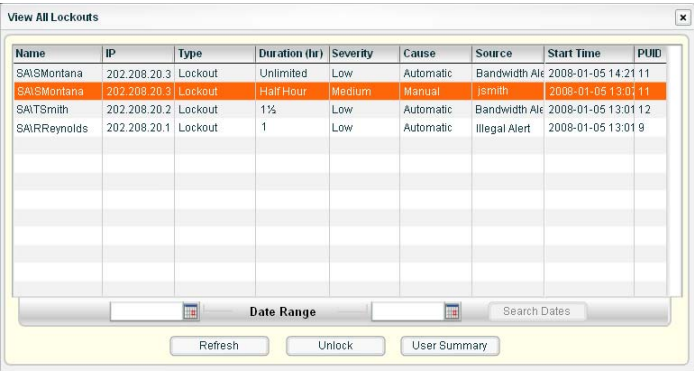
- 3. Click View Alert to open the Alert Viewer pop-up window (see Fig. 3:3-4).
- 4. Click the “X” in the upper right corner of Alert Viewer and Alert Log Viewer pop-up windows to close them.

Manage the Lockout List

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

To view the current lockout list:

- 1. Go to the navigation panel and select URL Dashboard.
- 2. Click Lockout to open the View All Lockouts pop-up window:



The screenshot shows a window titled "View All Lockouts" with a close button (X) in the top right corner. Inside the window is a table with the following data:

Name	IP	Type	Duration (hr)	Severity	Cause	Source	Start Time	PUID
SAISMontana	202.208.20.3	Lockout	Unlimited	Low	Automatic	Bandwidth Alc	2008-01-05 14:21 11	
SAISMontana	202.208.20.3	Lockout	Half Hour	Medium	Manual	jsmith	2008-01-05 13:01 11	
SAITSmith	202.208.20.2	Lockout	1½	Low	Automatic	Bandwidth Alc	2008-01-05 13:01 12	
SAIRReynolds	202.208.20.1	Lockout	1	Low	Automatic	Illegal Alert	2008-01-05 13:01 9	

Below the table, there is a "Date Range" section with two calendar icons and a "Search Dates" button. At the bottom of the window are three buttons: "Refresh", "Unlock", and "User Summary".

Fig. 3:3-8 View All 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: Name (user-name/IP address); IP address; Type of activity (Lockout); Duration (hr); Severity of the lockout (Low, Medium, High); Cause of the lockout (Manual, Automatic); Source

of the lockout (username of the administrator who locked out the end user in a Manual lockout, or name of the alert in an Automatic lockout); Start Time for the alert (using the HH:MM:SS/MM:DD:YYYY format); PUID (Personal User IDentification assigned by TAR to the end user).

3. After performing the intended actions in this window, click the “X” in the upper right corner of the pop-up window to close it.

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. 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.

2. 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.

3. Click the  calendar icon on the right to open 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 to the left of the calendar icon with the selected date.
5. Click **Search 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 window.

6. Click the “X” in the upper right corner of the pop-up window to close it.

Unlock a workstation

1. In the View All Lockouts pop-up window, click the record to highlight it.
2. Click **Unlock** to unlock the end user(s) and to remove the record(s) from the window.



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

Chapter 4: Analyze Web Usage Trends

When analyzing end user Internet usage trends, URL trend reports 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 URL Trend Reports

There are two types of URL trend reports that can be generated on demand to show total gauge score averages for a specified, limited time period: All Visible Gauges trend chart, and specified URL dashboard gauge trend chart.

View all URL dashboard gauge activity

1. In the navigation panel, click Report/Analysis to open that menu.
2. Click Trend Chart to open the All Visible Gauges trend chart:

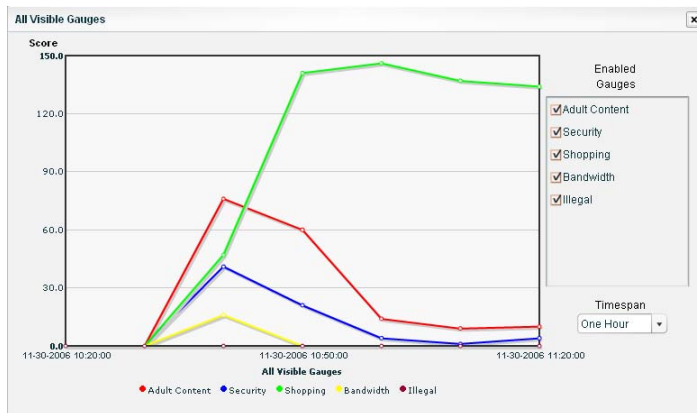


Fig. 3:4-1 All Visible Gauges trend chart

By default, this chart contains the following information: graphical depiction of last hour's end user Score for all visible URL dashboard gauges; fixed time increments (using the MM-DD-YYYY HH:MM:SS format); all Enabled Gauges selected; Timespan pull-down menu, and a color-coded key listing All Visible Gauges.



NOTE: A URL dashboard gauge is made invisible or visible via settings in the Gauge View window (see *Hide, Show a URL Gauge* in Chapter 3: Custom Gauge Setup, Usage).

3. After you have viewed the information in this chart, click the “X” in the upper right corner of the window to close it.

View activity for a specified URL gauge

1. In the URL dashboard gauge view, double-click the gauge to open a pop-up window displaying library category gauges comprising the URL dashboard gauge (see Fig. 3:2-15).
2. Click Trend Chart to open the Trend Chart for that URL dashboard gauge:

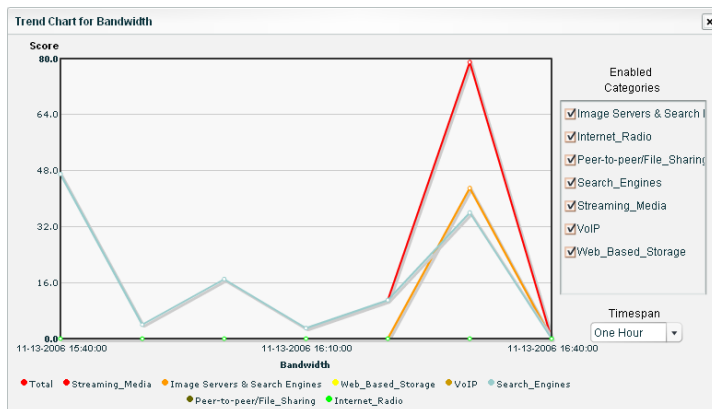


Fig. 3:4-2 Trend Chart for selected URL dashboard gauge

By default, this chart contains the following information: graphical depiction of last hour's end user Score for that URL gauge; fixed time increments (using the MM-DD-YYYY HH:MM:SS format); all library categories (Enabled Categories) selected; Timespan pull-down menu, and a color-coded key listing all library categories for that gauge.

3. After you have viewed the information in this chart, click the “X” in the upper right corner of the window to close it.

Suppress specified scores

To view only specified gauge scores in the chart, click the checkbox corresponding to the gauge to suppress graphical information for that gauge from displaying in the chart. To re-enable displaying information for that gauge, click the checkbox again.

View scores for a different time period

To view a different time period of gauge score averages, make a selection from the **Timespan** pull-down menu:

- One Hour - this selection displays gauge score averages in 10 minute increments for the past 60-minute time period
- Six Hours - this selection displays gauge score averages in 30 minute increments for the past six-hour time period
- Twelve Hours - this selection displays gauge score averages in one hour increments for the past 12-hour time period
- One Day - this selection displays gauge score averages in one hour increments for the past 24-hour time period
- One Week - this selection displays gauge score averages in one-day increments for the past seven-day time period
- One Month - this selection displays gauge score averages in one-day increments for the past month's time period

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

1. In the navigation panel, click Report/Analysis to open that menu.
2. 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

1. In the navigation panel, click Report/Analysis to open that menu.
2. Click ER Reporter to launch the login window of the ER Web Client application.

Chapter 5: View User Category Activity

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 URLs being accessed in such library categories.

Perform a custom search

View a list of Users who accessed a Category

To view a list of end users who accessed a specified library category:

1. In the navigation panel, go to URL Dashboard and click Custom Search to open the Custom Search pop-up window:

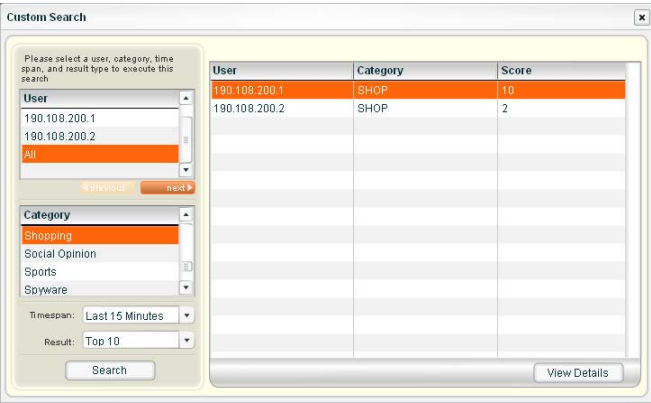


Fig. 3:5-1 Custom Search

2. In the **User** box, select the username/IP address to highlight it, or choose “All.”
3. In the **Category** box, select the library category to highlight it.

4. Make a selection from the **Timespan** pull-down menu for the time period in which URLs within the category were accessed: Last 15 Minutes, Last 30 Minutes, Last 45 Minutes, Last Hour.
5. If “All” was selected in the User field, the **Result** field becomes activated. Make a selection for the maximum number of users’ records to return in the results: Top 10, Top 20, Top 50, Top 100.
6. Click **Search** to display any records returned by the query in the table at the right side of the window (see Fig. 3:5-1). For each record in the table, the following information displays: User (username/IP address), Category name, and the user’s total Score for that category.
7. After performing the intended actions in this window, click the “X” in the upper right corner of the pop-up window to close it.

View URLs within the accessed category

To find out which URLs an end user accessed within the library category:

1. Click the User to highlight his/her record. This action activates the View Details button.
2. Click **View Details** to display a list of records showing the Timestamp (using the YYYY-MM-DD HH:MM:SS format) and corresponding URL for each URL in the library category the end user visited within the specified time period:

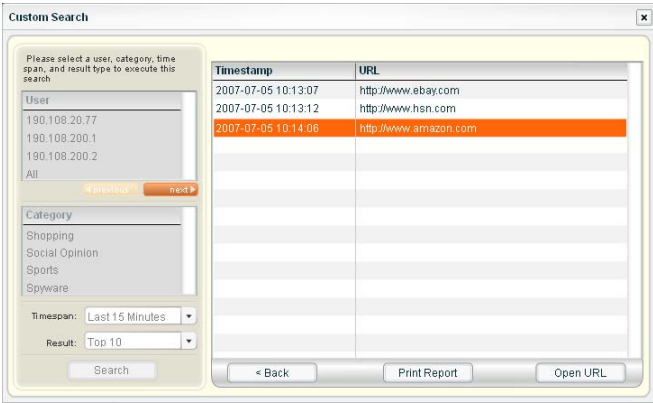


Fig. 3:5-2 List of URLs visited by the user



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

You can now print the results displayed in this window or access a selected URL.

3. After performing the intended actions in this window, click the “X” in the upper right corner of the pop-up window to close it.

Print the results

To print the results displayed in this window:

1. Click any record to highlight it and to activate the Print Report button.
2. Click **Print Report** to open the Print dialog box where you specify criteria for printing the report.
3. After performing the intended actions in this window, click the “X” in the upper right corner of this window to close it.

Access a URL

1. If a URL in the list is linked to a page or object, select the URL in the list, and then click **Open URL** to open the page/object in a separate browser window.
2. After performing the intended actions in this window, click the “X” in the upper right corner of this window to close it.

BANDWIDTH MANAGEMENT SECTION

Introduction

Whereas the URL dashboard Bandwidth gauge monitors end user Internet activity by the number of URL hits, gauges in the Bandwidth section of the interface monitor incoming and outgoing end user bandwidth traffic by the number of bytes.

The Bandwidth Management Section of this user guide is comprised of three chapters with information on monitoring inbound and outbound traffic, adjusting bandwidth gauge settings, and using reports for analyzing network traffic data in order to more effectively manage your resources.

- Chapter 1: Monitor Bandwidth Gauges - This chapter explains how bandwidth gauges are used for monitoring inbound and outbound traffic.
- Chapter 2: Modify Bandwidth Gauges - This chapter explains how to modify bandwidth gauge settings so you are alerted only when needed to safeguard your network.
- Chapter 3: View Bandwidth Trend Reports - This chapter explains how to analyze data in bandwidth trend reports.

Chapter 1: Monitor Bandwidth Gauges

Bandwidth gauges work similarly to URL dashboard gauges, except these gauges solely monitor inbound or outbound network traffic. Viewing bandwidth gauge activity of end users helps target areas that are slowing down or endangering the network.

There are two types of bandwidth gauges: bandwidth gauges that monitor incoming/outgoing bandwidth for specified protocols (HTTP, FTP, SMTP, P2P, IM), and bandwidth gauges that monitor incoming/outgoing bandwidth for specified port numbers within a given protocol. The latter type of bandwidth gauge is a subset of the former type of bandwidth gauge.



NOTE: *Unlike URL dashboard gauges, protocol bandwidth gauges cannot be added to—or removed from—the interface. However, protocol port numbers can be changed based on end user utilization in your organization. (See Chapter 2, Edit Port Settings for information on changing port numbers to be monitored.)*

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

View Bandwidth Gauges

1. In the navigation panel, click Bandwidth to open its menu.
2. Click either Inbound or Outbound to open the View Incoming/Outgoing Bandwidth Gauge pop-up window:

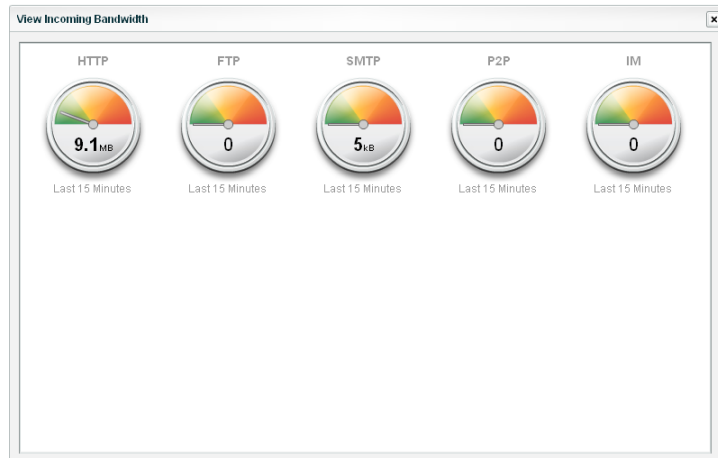


Fig. 4:1-1 View Incoming Bandwidth

The total score in bytes (KB, MB, GB) displays in each of the following gauge icons: HTTP, FTP, SMTP, P2P, IM. The timespan for gauge activity displays beneath each gauge icon.

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

View bandwidth usage for a specified protocol

1. In the View Incoming/Outgoing Bandwidth gauge pop-up window, right-click the bandwidth protocol gauge to open its pop-up menu:

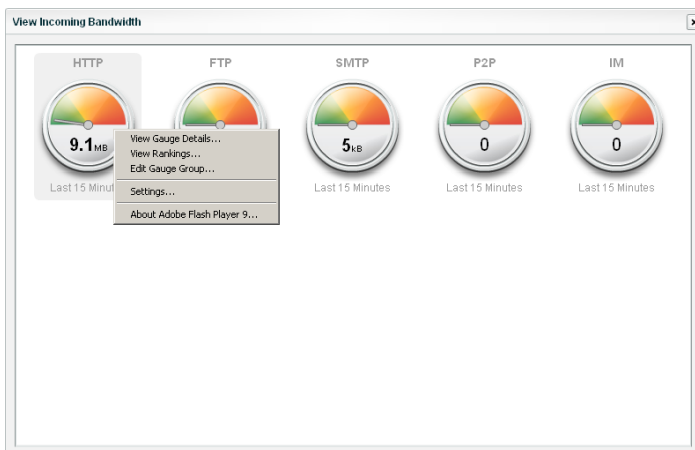


Fig. 4:1-2 Bandwidth gauge pop-up menu

2. Select View Gauge Details to open the protocol gauge's pop-up window containing port gauges:

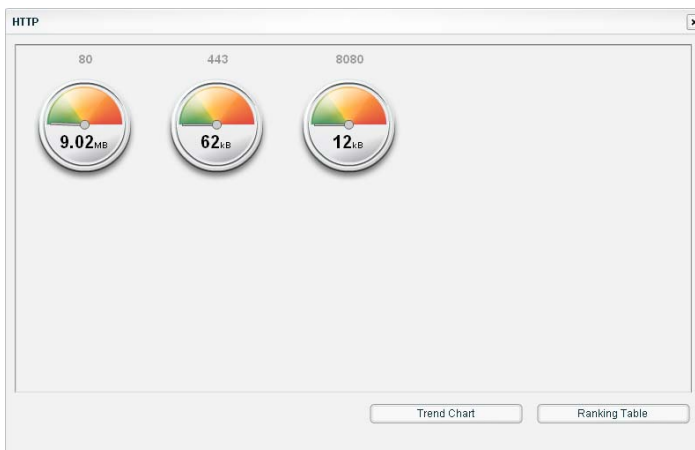


Fig. 4:1-3 Protocol gauge pop-up window

The total score in bytes (KB, MB, GB) displays in each of the port icons. The total number of bytes for all ports in this window equals the total number of bytes for the bandwidth protocol.



TIP: The protocol gauge's pop-up window is also accessible by double-clicking the protocol gauge in the View Incoming/Outgoing Bandwidth pop-up window.

View End User Bandwidth Gauge Activity

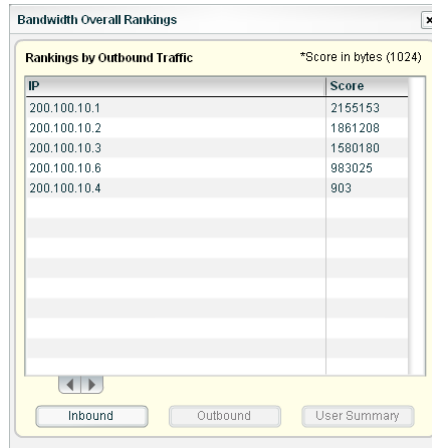
There are several ways to access information on end user bandwidth gauge activity:

- Overall end user bandwidth gauge activity - For a snapshot of all current bandwidth gauge activity ranked in order by the highest to lowest end user score, use the Overall Ranking option (see View Overall Ranking for bandwidth). This option also lets you drill down and view information on bandwidth gauges affected by a specified end user.
- End user activity by protocol gauge - For a snapshot of a protocol gauge's current activity ranked in order by the highest to lowest end user score, use the Ranking Table option (see View a protocol gauge ranking table).
- End user activity by port gauge - For a snapshot of a port gauge's current activity ranked in order by the highest to lowest end user score, use the port ranking table option (see View a port gauge ranking table).

View Overall Ranking for bandwidth

To view details about current bandwidth gauge activity for all end users affecting bandwidth gauges:

1. In the Bandwidth section of the navigation panel, click Overall Ranking to open the Overall Rankings pop-up window:



IP	Score
200.100.10.1	2155153
200.100.10.2	1961208
200.100.10.3	1580180
200.100.10.6	983025
200.100.10.4	903

Fig. 4:1-4 Bandwidth Overall Rankings

By default, this window includes rows of records for each end user who is currently affecting one or more bandwidth gauge for Outbound traffic. For each record in the list, the following information displays: user IP address, and corresponding Score in bytes. End users are ranked in descending order by their byte score.



NOTE: To view current bandwidth gauge activity for incoming traffic, click **Inbound**.

2. To drill down and view additional information about an end user's activity, click the IP address to highlight it.
3. Click **User Summary** to open the Individual User View pop-up window (see Fig. 4:1-7), and perform any of the

actions described for this window (see Monitor, Restrict Bandwidth Usage).

- 4. Click the “X” in the upper right corner of this pop-up window to close it.

View a protocol gauge ranking table

To view details about a specified bandwidth protocol gauge’s current activity:

- 1. Right-click the bandwidth gauge to open its pop-up menu (see Fig. 4:1-2).
- 2. Choose View Rankings to open the bandwidth protocol gauge’s ranking table pop-up window:

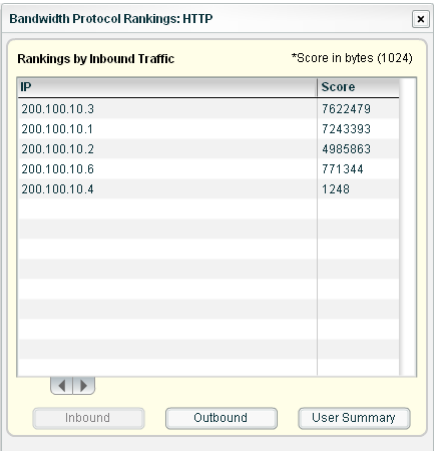



Fig. 4:1-5 Bandwidth Protocol Rankings

By default, this window includes rows of records for each end user who is affecting this protocol gauge. For each record in the list, the following information displays: user IP address, and corresponding Score in bytes. End users are ranked in descending order by their byte score.

 **TIP:** To view current protocol gauge activity for outbound end user traffic, click Outbound; for inbound traffic, click Inbound.



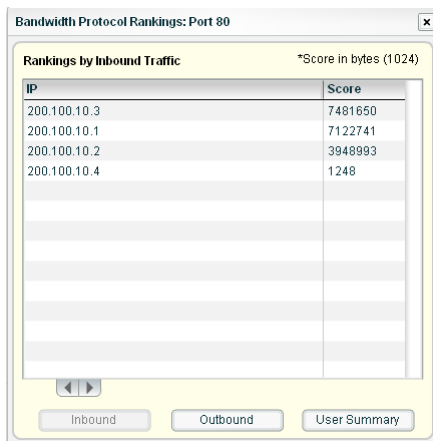
NOTE: *The protocol gauge's ranking table pop-up window is also accessible by right-clicking a protocol gauge, selecting View Gauge Details from the pop-up menu (see Fig. 4:1-2), and then clicking the Ranking Table button in the pop-up window.*

3. To drill down and view additional information about an end user's activity, click the IP address to highlight it.
4. Click **User Summary** to open the Individual User View pop-up window (see Fig. 4:1-7), and perform any of the actions described for this window (see Monitor, Restrict Bandwidth Usage).
5. Click the "X" in the upper right corner of this pop-up window to close it.

View a port gauge ranking table

To view details about a specified port gauge's current activity:

1. Right-click the bandwidth gauge to open its pop-up menu (see Fig. 4:1-2).
2. Select View Gauge Details to open the protocol gauge's pop-up window containing port gauges (see Fig. 4:1-3).
3. Click the port gauge to open its pop-up window:



Bandwidth Protocol Rankings: Port 80

Rankings by Inbound Traffic *Score in bytes (1024)

IP	Score
200.100.10.3	7481650
200.100.10.1	7122741
200.100.10.2	3948993
200.100.10.4	1248

Navigation buttons: Inbound, Outbound, User Summary

Fig. 4:1-6 Port gauge ranking table

By default, this window includes rows of records for each end user who is affecting this port gauge. For each record in the list, the following information displays: user IP address, and corresponding Score in bytes. End users are ranked in descending order by their byte score.



TIP: To view current port gauge activity for outbound end user traffic, click *Outbound*; for inbound traffic, click *Inbound*.

4. To drill down and view additional information about an end user's activity, click the IP address to highlight it.
5. Click **User Summary** to open the Individual User View pop-up window (see Fig. 4:1-7), and perform any of the actions described for this window (see Monitor, Restrict Bandwidth Usage).
6. Click the "X" in the upper right corner of this pop-up window to close it.

Monitor, Restrict Bandwidth Usage

The Individual User View window lets you view/restrict an end user's bandwidth usage.

1. From any of the user ranking windows, with the user-name/IP address selected, click **User Summary** to open the Individual User View pop-up window:

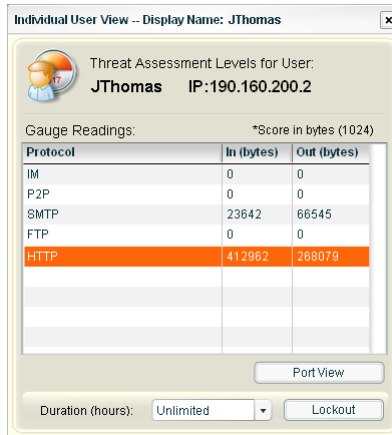


Fig. 4:1-7 Individual User View

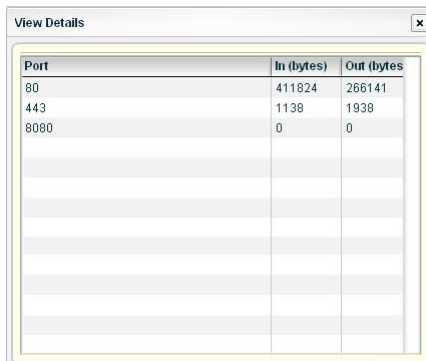
The Threat Assessment Levels for the username/IP address display in this window, including Gauge Readings for each bandwidth gauge Protocol, with the end user's corresponding score in bytes for Inbound and Outbound bandwidth traffic. This window also includes the Duration (hours) pull-down menu, and Port View and Lockout buttons.

2. After performing all intended actions in this window, click the "X" in the upper right corner of the pop-up window to close it.

View the end user's port usage in bytes

To monitor an end user's bandwidth port traffic:

1. In the Individual User View pop-up window (see Fig. 4:1-7), select the protocol gauge to highlight it.
2. Click **Port View** to open the View Details pop-up window:



The screenshot shows a window titled "View Details" with a close button (X) in the top right corner. Inside the window is a table with three columns: "Port", "In (bytes)", and "Out (bytes)". The table contains three rows of data: Port 80 with 411824 In bytes and 266141 Out bytes; Port 443 with 1138 In bytes and 1938 Out bytes; and Port 8080 with 0 In bytes and 0 Out bytes. There are several empty rows below the data.

Port	In (bytes)	Out (bytes)
80	411824	266141
443	1138	1938
8080	0	0

Fig. 4:1-8 View Details

This window contains Port numbers and the end user's corresponding score in bytes for Inbound and Outbound bandwidth traffic.

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

Manually lock out an end user

To prevent the end user from accessing specified URLs that result in too much bandwidth usage:

1. In the Individual User View pop-up window (see Fig. 4:1-7), select the name of the Protocol to highlight it.
2. Specify the **Duration (hours)** for the lockout by making a selection from the pull-down menu (Unlimited, Half Hour, 1, 1-1/2 ... 8).



NOTE: If “Unlimited” is selected, the end user remains locked out of the specified areas on the Internet/network until the administrator unlocks his/her workstation. To “unlock” the end user, go to the Lockout window in the URL Dashboard section of the navigation panel. For information on this feature, see Chapter 3: Alerts, Lockout Management in the Configuration Section.

3. Click **Lockout** to open the Lockout dialog box (see Fig. 3:2-20).



TIP: Click No to close this dialog box without locking out the user.

4. Specify the **Severity** of the lockout from the choices in the pull-down menu:
 - Low - this selection lets you choose which library category’s contents the end user will not be able to access
 - Medium - this selection locks out the end user from Internet access
 - High - this selection locks out the end user from all network access
5. Click **Yes** to proceed.
 - If a “Low” severity was selected, clicking **Yes** opens the Lockout by Categories pop-up window (see Fig. 3:2-21).

- a. From the Available Categories list box, select the available library category containing URLs the end user should not access.
- b. Click **Add** to move the library category to the Assigned Categories list box.



TIPS: To remove a library category from the Assigned Categories list box, click the library category to highlight it, and then click *Remove* to move the category back to the Available Categories list box.

Click Sync All Categories after custom library categories have been added to the list, in order to force synchronization between the R3000 and the TAR unit.

- c. After adding all library categories, click **Next** to open the alert box stating: “The user has been locked out.”
 - d. Click the “X” in the upper right corner of the box to close it.
- If a “Medium” or “High” severity was selected:
 - a. Clicking **Yes** in the Lockout dialog box opens the the alert box stating: “The user has been locked out.”
 - b. Click the “X” in the upper right corner of the box to close it.



NOTE: See *End user workstation lockout* in Chapter 2 of the Configuration Section for information on what occurs on the end user’s workstation when he/she is locked out.

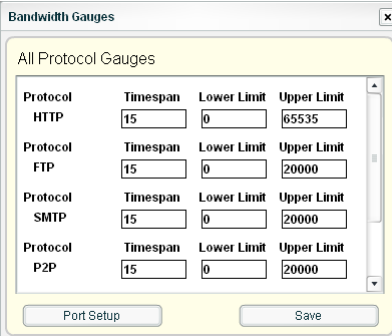
Chapter 2: Modify Bandwidth Gauges

While bandwidth protocol gauges cannot be added or removed, their timespan and threshold limits can be modified, along with their associated port numbers.

This function to modify bandwidth protocol gauges 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.

Modify Protocol Gauge Settings

1. To modify a bandwidth protocol gauge's settings, click Gauges in the Bandwidth section of the navigation panel to open the Bandwidth Gauges pop-up window for All Protocol Gauges:



The screenshot shows a window titled "Bandwidth Gauges" with a close button (X) in the top right corner. Inside the window, there is a section labeled "All Protocol Gauges" containing a table with four rows of protocol settings. Each row has four columns: "Protocol", "Timespan", "Lower Limit", and "Upper Limit". The protocols listed are HTTP, FTP, SMTP, and P2P. The "Timespan" for all protocols is set to 15. The "Lower Limit" for all protocols is set to 0. The "Upper Limit" for HTTP is 65535, and for FTP, SMTP, and P2P, it is 20000. Below the table, there are two buttons: "Port Setup" and "Save".

Protocol	Timespan	Lower Limit	Upper Limit
HTTP	15	0	65535
FTP	15	0	20000
SMTP	15	0	20000
P2P	15	0	20000

Fig. 4:2-1 Bandwidth Gauges

This window includes the Timespan and threshold fields for each Protocol gauge (HTTP, FTP, SMTP, P2P, IM).

2. Modify any of the following information:
 - Timespan - the default is 15 minutes
 - Lower Limit - the default lower threshold is "0" (zero)

- Upper Limit - the default upper threshold for HTTP is 65535, and 20000 for all other protocols
3. If you do not need to modify any port settings, click **Save** to save your edits and to close the Bandwidth Gauges pop-up window.

Edit Port Settings

1. To change a protocol gauge's port settings, in the Bandwidth Gauges pop-up window (see Fig. 4:2-1), click **Port Setup** to open the Port Setup pop-up window for Custom Port Setup:

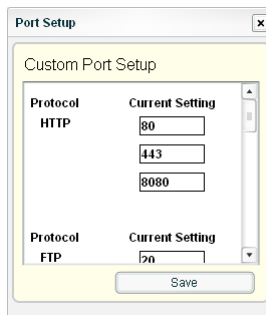


Fig. 4:2-2 Port Setup

This window contains Current Setting fields for each Protocol port.

2. To use a different port number other than one currently displayed in this window, enter a valid port number for the Protocol.
3. Click **Save** to save your edits and to close the Port Setup pop-up window.
4. Click **Save** to retain your settings and to close the Bandwidth Gauges pop-up window.

Chapter 3: View Bandwidth Trend Reports

Similarly to URL trend reports, bandwidth trend reports help you further configure bandwidth gauges and alerts so you can focus on traffic areas that most affect the network.

There are two types of bandwidth trend reports that can be generated on demand to show total gauge score averages for a specified, limited time period: All Bandwidth Gauges trend chart, and the specified bandwidth protocol gauge trend chart.

View All Bandwidth Gauge Activity

1. In the navigation panel, click Bandwidth to open that menu.
2. Click **Trend Chart** to open the All Bandwidth Gauges trend chart:

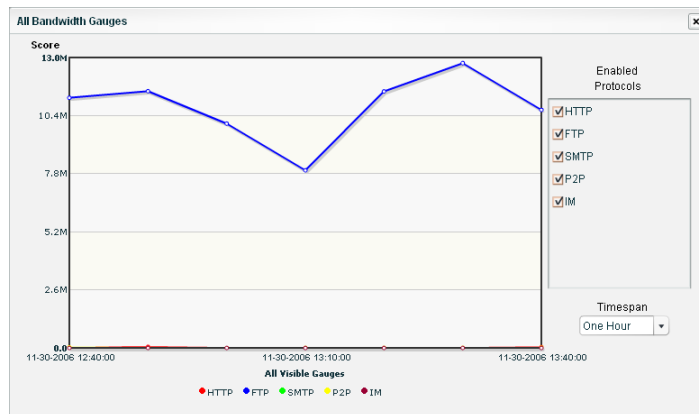


Fig. 4:3-1 All Bandwidth Gauges

By default, this chart contains the following information: graphical depiction of last hour's end user Score for all bandwidth gauges (HTTP, FTP, SMTP, P2P, IM); fixed time increments (using the MM-DD-YYYY HH:MM:SS format); all Enabled Protocols selected; Timespan pull-

down menu, and a color-coded key listing All Visible Gauges.

3. After you have viewed the information in this chart, click the “X” in the upper right corner of the window to close it.

View Activity for a Specified Gauge

1. In the Bandwidth section of the navigation panel, choose either Inbound or Outbound to open the View Incoming/Outgoing Bandwidth pop-up window (see Fig. 4:1-1).
2. Double-click a bandwidth protocol gauge to open a pop-up window displaying port gauges comprising that protocol gauge (see Fig. 4:1-3).
3. Click **Trend Chart** to open the Trend Chart for that protocol gauge:

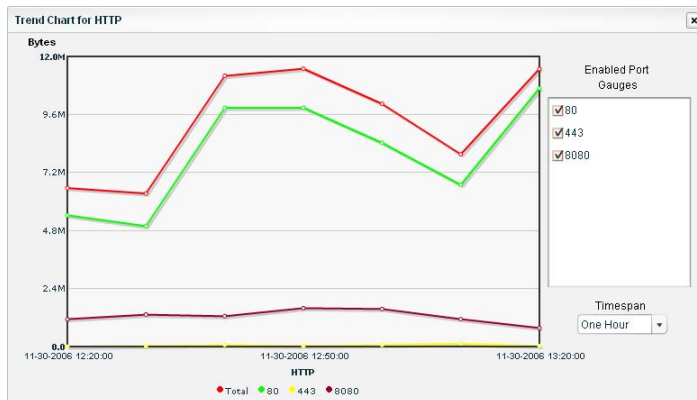


Fig. 4:3-2 Trend Chart for selected protocol gauge

By default, this chart contains the following information: graphical depiction of last hour's end user score in Bytes for ports comprising that protocol gauge; fixed time increments (using the MM-DD-YYYY HH:MM:SS format); all ports (Enabled Port Gauges) selected; Timespan pull-down menu, and a color-coded key listing all ports for that protocol gauge.

4. After you have viewed the information in this chart, click the “X” in the upper right corner of the window to close it.

Suppress Criteria of Specified Ports

To view only specified port criteria in the chart, click the checkbox corresponding to a port name/number to suppress that port’s graphical information from displaying in the chart. To re-enable displaying information for that port, click the checkbox again.

View Criteria for a Different Time Period

To view a different time period of byte averages, make a selection from the **Timespan** pull-down menu:

- One Hour - this selection displays byte averages in 10 minute increments for the past 60-minute time period
- Six Hours - this selection displays byte averages in 30 minute increments for the past six-hour time period
- Twelve Hours - this selection displays byte averages in one hour increments for the past 12-hour time period
- One Day - this selection displays byte averages in one hour increments for the past 24-hour time period
- One Week - this selection displays byte averages in one-day increments for the past seven-day time period
- One Month - this selection displays byte averages in one-day increments for the past month’s time period

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 window to troubleshoot RAID on a TAR “SL”, “HL”, or “H” server.

- Chapter 1: Custom Category Maintenance - This chapter explains how the global administrator maintains criteria for Custom Categories set up on the source R3000 connected to this TAR server.
- Chapter 2: View the Master User List - This chapter explains the options for viewing end user information comprising the Master User List.
- Chapter 3: View Administrator Activity - This chapter explains how to use the Log Viewer to view activity performed on TAR by the global or group administrators.
- Chapter 4: Maintain the Device Registry - This chapter provides information to the global administrator 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 5: 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 6: Install Software Updates - This chapter explains how the global administrator installs software updates on the TAR server.
- Chapter 7: 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: Custom Category Maintenance

The Custom Categories window is used by the global administrator to manage criteria for Custom Categories set up on the source R3000 connected to this TAR server.

1. In the navigation panel, go to URL Dashboard and click Custom Categories to open the Custom Categories pop-up window:

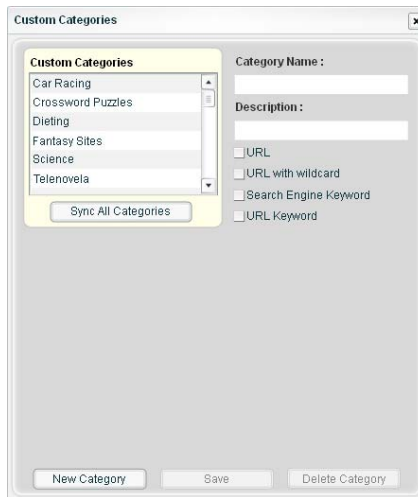


Fig. 5:1-1 Custom Categories

From this window, details about custom categories can be viewed, custom categories can be added or deleted, and synchronization between the source R3000 and this TAR unit can be executed on demand.

2. After performing the intended actions in this window, click the “X” in the upper right corner of the pop-up window to close it.

View Custom Categories

To view details about a custom category:

1. Select the custom category from the Custom Categories frame, which populates fields, checkbox(es), and tab(s), and activates the Delete Category button:

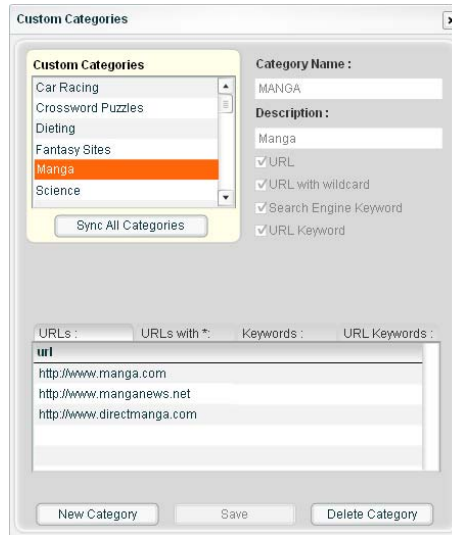


Fig. 5:1-2 View Custom Category details

To the right of the Custom Categories frame, the Category Name, Description, and the checkbox(es) corresponding to the tab(s) configured for this custom category display: URL, URL with wildcard, Search Engine Keyword, and URL Keyword.

2. Click an available tab (URLs, URLs with *, Keyword, URL Keywords) to view URLs or keywords entered in that tab.

Add a Custom Category

1. Click **New Category**.
2. Enter up to seven characters for the **Category Name**. This entry automatically displays in uppercase characters.
3. Enter the **Description** for the category.
4. Click in any of the checkboxes to display the corresponding elements below:

Fig. 5:1-3 New custom category

- URL - clicking this checkbox displays the URL field, and “URLs” tab below.
- URL with wildcard - clicking this checkbox displays the URL with Wildcard (*) field, and “URLs with *” tab below.
- Search Engine Keyword - clicking this checkbox displays the Search Engine Keyword field, and “Keywords” tab below.

- URL Keyword - clicking this checkbox displays the URL Keyword field, and “URL Keywords” tab below.
5. Make the following entries, based on the checkbox selection(s):

- **URL** - type in the URL, and then click **Add** to include the entry in the “URLs” tab.



TIP: If a protocol prefix is not entered, “http://” automatically will precede the entry when Add is clicked and the entry is added to the URLs list below.

- **URL with Wildcard (*)** - type in the wildcard after the “*.” displayed in the text box, and then click **Add** to include the entry in the “URLs with *” tab.



TIP: The minimum number of levels that can be entered is three (e.g. *.yahoo.com) and the maximum number of levels is six (e.g. *.mail.attachments.message.yahoo.com).

- **Search Engine Keyword** - type in up to 64 alphanumeric characters (including spaces), and then click **Add** to include the entry in the “Keywords” tab.
- **URL Keyword** - type in up to 64 alphanumeric characters, and then click **Add** to include the entry in the “URL Keywords” tab.



TIP: Prior to saving your entries, an addition made to any tab can be deleted. Click the last entry made in the tab, and then click **Delete Selection**.

6. After making all entries, click **Save** to refresh the window and to display the name of the newly added category in the Custom Categories frame.

When a custom category is added in TAR, the new category also is added in the Custom Categories list on the source R3000.



NOTE: The maximum number of Custom Categories that can be added in the TAR interface is 131.

Synchronize TAR with the R3000

Custom library category synchronization automatically takes place each hour. During this process, the following occurs:

- new custom categories that were added in the source R3000 are added to TAR
- new custom categories that were added in TAR are added to the source R3000
- custom category additions/deletions that were made in the source R3000 are executed in TAR
- custom category additions/deletions that were made in TAR are executed in the source R3000
- custom library categories that were removed in the source R3000 are removed from TAR
- custom library categories that were removed in TAR are removed from the source R3000.

If you need to force synchronization between the source R3000 and TAR, click **Sync All Categories**.

Delete a Custom Category

1. Click a custom category in the Custom Categories list to highlight it.
2. Click **Delete Category** to open the Delete Custom Category dialog box:

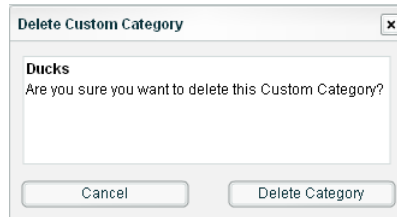


Fig. 5:1-4 Delete custom category



TIP: Click **Cancel** to close the dialog box and to return to the Custom Categories window.

3. Click **Delete Category** to close the dialog box and to remove the category from the Custom Categories list. This action also removes the category from the Custom Categories list on the source R3000 connected to this TAR server.

Chapter 2: View the Master User List

The View Master List window contains the Master User List 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.

The View Master List window 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.

1. In the navigation panel, click Administration to open that menu.
2. Click User Profiles to open the View Master User List pop-up window:

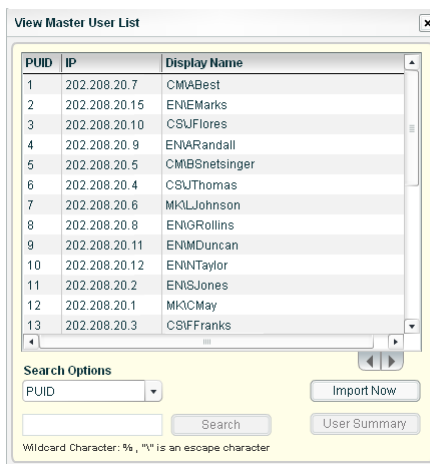


Fig. 5:2-1 View Master User List

By default, this window is comprised of rows of end user ID records, sorted in ascending order by Personal User Identification number (PUID) assigned to end users by TAR. For each PUID in the list, the following displays:

corresponding end user IP address, and Display Name (username/IP address).

3. After performing the intended actions in this window, click the “X” in the upper right corner of the pop-up window to close it.

Search the MUL Database

1. Make a selection from the **Search Options** pull-down menu to specify the type of user search to perform:
 - PUID - this selection performs a search by end user Personal User IDs
 - IP - this selection performs a search by end user IP addresses
 - Display Name - this selection performs a search by end user usernames/IP addresses



TIP: *To narrow your search criteria, make an entry in the wildcard field by entering the beginning characters to be included in the search, followed by the “%” (percent) character. For example, to include only IP addresses beginning with 200, enter **200%** in this field.*

2. Click **Search** to display records from the search that match your criteria.

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 Individual User View pop-up window (see Fig. 3:2-17), and perform any of the actions described for this window (see Monitor, Restrict End User Activity in the Configuration Section, Chapter 2: Custom Gauge Setup, Usage).

Synchronize TAR with the R3000

If changes were made to the user list on the LDAP server or on the source R3000, click **Import Now** to force synchronization between the servers. This action re-displays all current records in the Master User List.

Chapter 3: View Administrator Activity

The Log Viewer window is used for viewing the most recent administrative activity performed on TAR by the global or group administrators, for a period of time up to the past 30 days.

1. In the navigation panel, click Administration to open that menu.
2. Click Log Viewer to open the Log Viewer pop-up window:



Fig. 5:3-1 Log Viewer

3. After performing the intended actions in this window, click the "X" in the upper right corner of the window to close it.


Perform a Search on a Specified Activity

To perform a search on a specified activity:

1. Select the type of activity from the Log Headings list: All, Invalid Authentication (TAR was busy and unable to respond to a valid login request), Log In Attempt (incorrect Admin Name or Password entered), Successful Log In, MUL (Master User List) Fetch, Add New Group, Add New Administrator, Add Admin Detail, Admin Group Edit, User Group Edit, Update Admin Info, Password Change, Delete Admin, Delete Group.




NOTE: The Log Headings 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. Click **Search** to display the specified records for the selected dates in the Results box.



TIP: To narrow your search criteria, make an entry in the Search by Admin Name field, and then click Search again.

Search Results

When populated with rows of records, the Results box includes the following columns: AdminName (entry from the Admin Name field in the login window); activity Type [Invalid Authentication, Log In Attempt, Successful Log In, Add New Group, Add New Administrator, Add Admin Detail, MUL Fetch, Update Admin Info, Admin Group Edit, User Group Edit, Password Change, Delete Admin, Delete Group]; Target (administrator group name or group administrator name, if applicable), and Time [using the Mon (abbreviated month name) DD, YYYY HH:MM:SS AM/PM format].

The information that displays in these columns differs depending on the Type of search performed, and if an administrator name was specified in the Search by Admin Name field.

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

- Add New Group - the Target column for this selection displays the group administrator name added in the Group Management window
- Add New Administrator - the Target column for this selection displays the group administrator name added in the Admin System window
- Add Admin Detail - the Target column for this selection displays the group administrator name for the entity who had profile information added in the Admin System window
- Update Admin Info - the Target column for this selection displays the group administrator name of the entity whose profile was updated in the Admin System window
- Admin Group Edit - the Target column for this selection displays the group administrator name of the entity who

edited an administrator group via the Group Management window

- User Group Edit - the Target column for this selection displays the group administrator name of the entity who edited a user group via the User Groups management panel
- Password Change - the Target column for this selection displays the group administrator name of the entity whose password was modified in the Admin System window
- Delete Admin - the Target column for this selection displays the group administrator name for the entity whose profile was deleted from the Admin System window
- Delete Group - the Target column for this selection displays the group administrator name for the entity whose group was deleted via the Group Management window

Chapter 4: 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.

1. In the navigation panel, click Administration to open that menu.
2. Click Device Registry to display the Device Registry panel:



Fig. 5:4-1 Device Registry

At the top of the panel the following buttons display:

- **Sync All Devices** - click to open a pop-up window that lets you specify which types of items to synchronize
- **New R3000** - click to open a panel that lets you add another R3000
- **New ER** - click to open a panel that lets you add an ER—if an ER device is connected to the source R3000
- **Back to Gauges** - click to re-display the default gauges view

In the middle of the panel, each device communicating with TAR is represented by a square with a picture of a chassis, labeled with an icon indicating the type of device, the device's IP address, and at least one button for an action that can be performed for that device: View, Edit, Delete.

At the bottom of the panel, the following labels, icons, and buttons display:

- R3000 - Enterprise Internet Filter server
- ER - Enterprise Reporter server
- TAR - Threat Analysis Reporter server
- envelope icon - SMTP Server
- globe with link icon - Proxy Server
- clock icon - NTP Server
- asterisk icon - Source R3000 server
- patch icon - Patch Server
- **Refresh Devices** - click this button if any square representing a device does not properly display in the interface.
- **Previous** - click this button (if activated) to view the previous page of devices.
- **Next** - click this button (if activated) to view the next page of devices.



TIP: Click **Back to Gauges** in the upper right corner of the panel to re-display the default gauges view.

R3000 Device Maintenance

The actions in this sub-section are initiated from the main Device Registry panel, in the square representing the R3000 device.

View, edit R3000 device criteria

1. Click **Edit** to display the R3000 panel:

Fig. 5:4-2 R3000 panel

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

2. Edit any of the following:
 - **Name** - the 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 panel and to return to the main Device Registry panel.

3. Click **Save** to save your edits, and to return to the main Device Registry panel.

Add an R3000 to the registry

1. Click **New R3000** to display the R3000 panel (see Fig. 5:4-2).
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 panel and to return to the main Device Registry panel.

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

Delete an R3000 from the registry

Click **Delete** to delete an R3000 device from the registry, and to remove the square representing that R3000 from the main 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

The actions in this sub-section are initiated from the main Device Registry panel, in the square representing the TAR device that is connected to the source R3000 device.

View, edit TAR device criteria

1. Click **Edit** to display the Threat Analysis Reporter panel:

The screenshot shows the 'Threat Analysis Reporter' panel. At the top, there are buttons: 'Sync All Devices', 'New R3000', 'New ER', and 'Back to Gauges'. The panel title is 'Threat Analysis Reporter'. Below the title, a message states: 'Please Add/Remove any bandwidth ranges you would like to use. The rest of the fields on this form are not editable.'

On the left side, there are fields for 'Device Type' (set to 'TAR'), 'Name' (set to 'Threat Analysis Reporter'), and 'IP: LAN1' (set to '202.208.20.21'). There are 'Save' and 'Cancel' buttons at the bottom left.

On the right side, there are fields for 'Bandwidth IP:' and 'Bandwidth Netmask:'. Below these is a table with two columns: 'Bandwidth IP:' and 'Bandwidth Netmask:'. The table contains two rows of data: '202.208.200.1' and '255.255.255.0', and '202.208.200.77' and '255.255.255.255'. There is an '+ Add Range' button above the table and a '- Remove Range' button at the bottom right.

Fig. 5:4-3 Threat Analysis Reporter panel

On the left side of this panel, the Device Type (TAR), Name of the server (Threat Analysis Reporter), and IP address(es) entered during the quick start wizard process display and cannot be edited.

On the right side of this panel, fields and buttons for adding or removing a bandwidth IP range display. Any Bandwidth IP range and Bandwidth Netmask previously entered in this panel displays in the list box.

2. For bandwidth criteria:
 - To add a bandwidth IP address range:
 - a. Type in the **Bandwidth IP** address.
 - b. Type in the **Bandwidth Netmask**.
 - c. Click **[+] Add Range** to add the bandwidth IP range in the list box.
 - To remove a bandwidth IP address range:
 - a. Select the record for the IP range from the list box.
 - b. Click **[-] Remove Range**.
3. After making edits in this panel, click **Save** to save your entries and to return to the previous panel.

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 registry

1. Click the **New ER** button to display the ER panel:


Fig. 5:4-4 Enterprise Reporter panel, add device

The Device Type (Enterprise Reporter) 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 panel and to return to the main Device Registry panel.

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

 **NOTE:** Once the ER is added, the New ER button no longer displays. Criteria for this ER can be edited, and the ER can be deleted from the Device Registry.

View, edit ER device criteria

The actions in this sub-section are initiated from the main Device Registry panel, in the square representing the ER device.

1. Click **Edit** to display the ER panel:



Fig. 5:4-5 ER panel, edit

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

2. Edit any of the following:
 - **Name** - the name of the server.
 - **IP** - IP address of the server.



TIP: Click **Cancel** to close this panel and to return to the main Device Registry panel.

3. Click **Save** to save your edits, and to return to the main Device Registry panel.

Delete ER device

The actions in this sub-section are initiated from the main Device Registry panel, in the square representing the ER device.

Click **Delete** to delete the ER device from the registry, and to remove the square representing that ER box from the main Device Registry panel. This action also adds the New ER button to the top of the panel.

View Other Device Criteria

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

View SMTP device criteria

1. Click **View** to open the SMTP pop-up window:



Fig. 5:4-6 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 **Close** to close this pop-up window.

View Patch Server device criteria

1. Click **View** to open the Patch Server pop-up window. The following 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. 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. 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, Proxy Switch ("on" or "off"), Username (if applicable), Password (if applicable, asterisks display), Port number.
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** to open the Sync All Devices pop-up window:

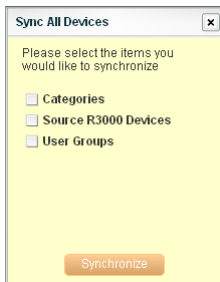


Fig. 5:4-7 Sync All Devices

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 sync 8e6 supplied library category updates and custom library categories from the source R3000 to TAR.
 - Source R3000 Devices - Make this selection to sync 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 sync LDAP user group information on the source R3000 to TAR.



WARNING: The User Groups synchronization process may be lengthy and thus may create an impact on the performance of TAR.

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

Chapter 5: Perform Backup, Restoration

This Backup/Restore window is used for backing up gauge configuration settings to the TAR server, or restoring such settings saved from a previous backup to the TAR server.

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 Chapters 2 and 3 of the Preliminary Setup Section. Backup and restoration files include settings pertinent to the administrator who configured the gauges, and do not include other administrator's configuration settings.

By default, TAR performs an automatic backup each morning at 2:00 a.m., storing up to seven days of automatic backup files.



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

1. In the navigation panel, click Administration to open that menu.
2. Click Backup/Restore to open the Backup And Restore pop-up window:

Backup And Restore

Backup user configuration

Backup on demand:

File Name :

Backup Personal Data

Restore to Factory Defaults

Restore user configuration

Restore your settings to a previous time by selecting a restoration file

Restoration File :

- auto: 1128 020001 2006
- auto: 1130 020001 2006
- M2New102306
- auto: 1123 020001 2006
- auto: 1124 020000 2006

Restore Personal Settings

Fig. 5:5-1 Backup And Restore

This window is comprised of the Backup user configuration frame and the Restore user configuration frame.

In the Restore user configuration frame, the Restoration File box includes a list of up to seven of the most recent automatic backup files, and any backup files created on demand by the administrator.

Automatic backup files display in the following format: auto date (in the MD format), time (in the HHMMSS format), and year (in the YYYY format). For example: **auto 123 020001 2007** displays for an automatic backup executed on December 3, 2007 at 2:00:01 (2:00 a.m. and one second).

3. After performing the intended actions in this window, click the “X” in the upper right corner of the window to close it.

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 window, enter the **File Name** for the backup file to activate the Backup Personal Data button:

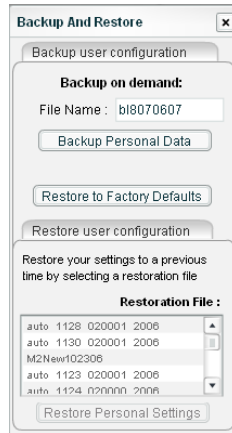


Fig. 5:5-2 Backup on demand

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 Restoration File list, and a pop-up box opens displaying the following message: "The operation was successful."
3. Click the "X" in the upper right corner of the message box to close it.

Restore User Settings

1. From the Restoration File box, select the file to be restored by clicking on it to highlight it:

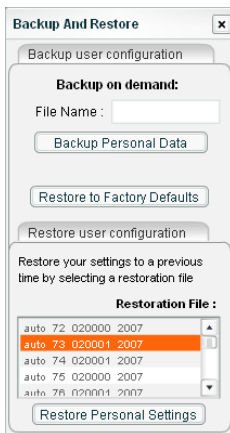


Fig. 5:5-3 Restore Personal Settings

2. Click **Restore Personal Settings** to restore user settings from the selected file. Upon successfully executing the file restoration, a pop-up box opens displaying the following message: “The operation was successful.”
3. Click the “X” in the upper right corner of the message box to close it.

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.

1. Click **Restore to Factory Defaults** to display the Backup/Restore Global Data frame to the right of the Backup user configuration frame:

The screenshot shows a dialog box titled "Backup And Restore" with a close button (X) in the top right corner. It has two tabs: "Backup user configuration" and "Backup/Restore Global Data". The "Backup/Restore Global Data" tab is selected and contains the following elements:

- A warning icon (yellow triangle with exclamation mark) and text: "Please note that this action will delete all settings, gauges, users, and data from your database. We strongly recommend checking with all administrative users before proceeding."
- A confirmation code displayed in a stylized font: **4BEB7A5**.
- A text prompt: "Please retype the above characters:" followed by a text input field containing "4BEB7A5".
- A text prompt: "Please retype your admin password:" followed by a password input field with masked characters "*****".
- A disclaimer: "By clicking the button below you acknowledge the implications of resetting this appliance to factory presets. This is an irreparable action."
- A button labeled "Restore to Factory Defaults".

The "Backup user configuration" tab is also visible and contains:

- A section "Backup on demand:" with a "File Name:" label and an empty text field, and a "Backup Personal Data" button.
- A "Restore to Factory Defaults" button.
- A section "Restore user configuration" with text: "Restore your settings to a previous time by selecting a restoration file".
- A "Restoration File:" section with a list box containing several file names (e.g., "auto_1128_020001_2006", "auto_1130_020001_2006", "M2New102306", "auto_1123_020001_2006", "auto_1124_020001_2006") and a "Restore Personal Settings" button.

Fig. 5:5-4 Restore to Factory Defaults

2. In the first field in this frame, type in the eight case-sensitive alphanumeric characters exactly as displayed above.
3. In the field below, type in your administrator password—used when logging into the TAR interface—to activate the Restore to Factory Defaults button.
4. Click **Restore to Factory Defaults** to delete all information on the TAR unit and to restore factory default settings.

Chapter 6: 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.

Check for Available Software Updates

To check the console for available software updates:

1. In the navigation panel, click Administration to open that menu.
2. Click Software Update to open the Software Update window:

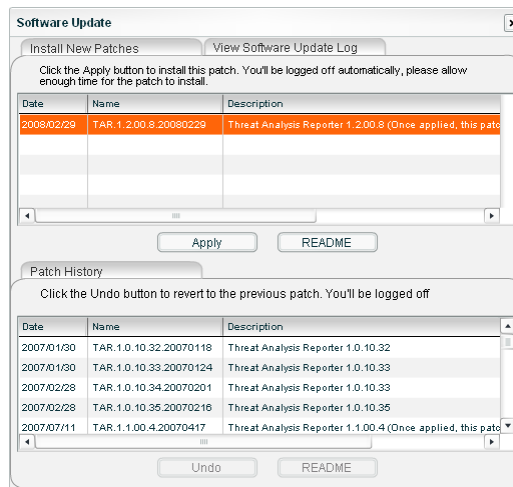


Fig. 5:6-1 Software Update, Install New Patches

This window displays any available software updates in the table at the top of the Install New Patches tab. Any updates previously applied display in the Patch History frame below.

3. After performing the intended actions in this window, click the “X” in the upper right corner of this window to close it.

Apply a Software Update

If a software update is available:

1. In the Install New Patches tab, click the software update listed in the table to select and highlight it (see Fig. 5:6-1).
2. Click **README** to open a pop-up box containing information about the software release:

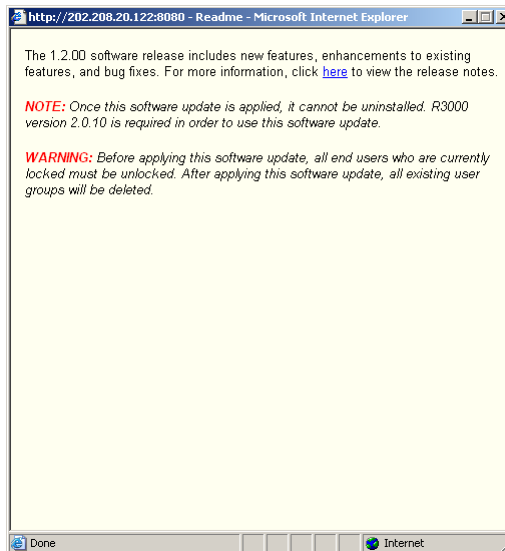


Fig. 5:6-2 Readme file

3. After reading the contents of the software release, click the “X” in the upper right corner to close the pop-up box.

- Click **Apply** to open a dialog box confirming that you wish to apply the software release:

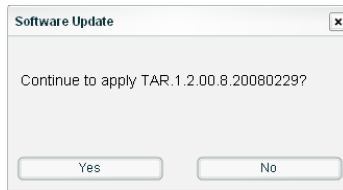


Fig. 5:6-3 Apply dialog box

- Click **Yes** to close the dialog box and to begin the software update application process.
- Wait five minutes for the software update to be automatically applied to the server, and then launch a new browser window.
- Clear the browser's cache.
- 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:

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

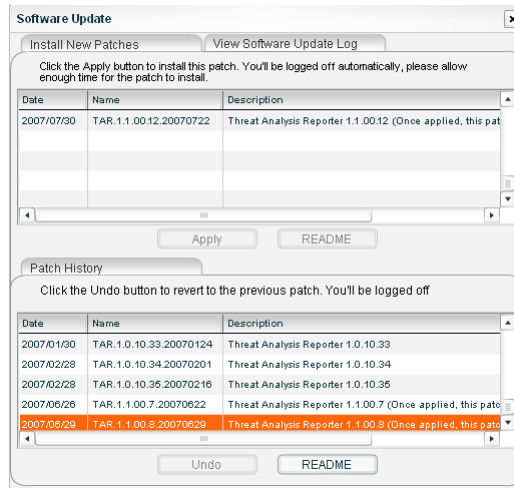


Fig. 5:6-4 Software Update, Patch History

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.

View Software Installation Details

To view information about the software installation:

1. Click the View Software Update Log tab to display information about the software update recently applied to the server:

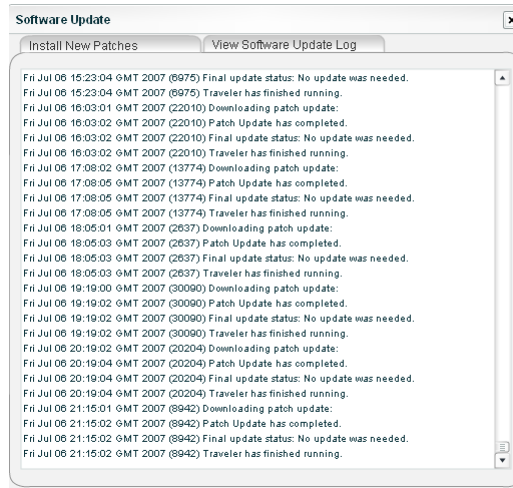


Fig. 5:6-5 Software Update, View Software Update Log

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

Chapter 7: 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.

1. In the navigation panel, click Administration to open that menu.
2. Click Hardware Detector to open the Hardware Detector window:

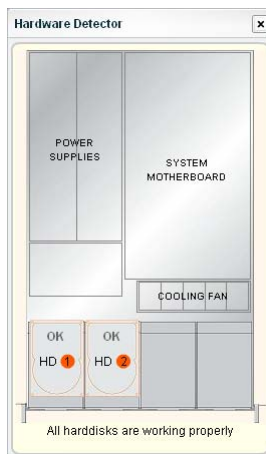


Fig. 5:6-6 Hardware Detector, hard disks OK



NOTE: If the TAR server is a TAR-S or TAR-MSA unit, when clicking Hardware Detector, the following message displays in a pop-up box: "This is not a RAID box!" Click the "X" in the upper right corner to close the pop-up box.

If no hard disk failure has been detected on the TAR server with RAID, the status of each hard drive displays as "OK" and the following message displays at the bottom of the window: "All harddisks are working properly."

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:

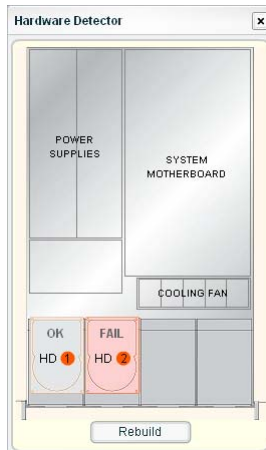


Fig. 5:6-7 Hardware Detector, hard disk failure

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.8e6.com/support.html>, 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@8e6.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.8e6.com/support.html>

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

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

E-mail: support@8e6.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:

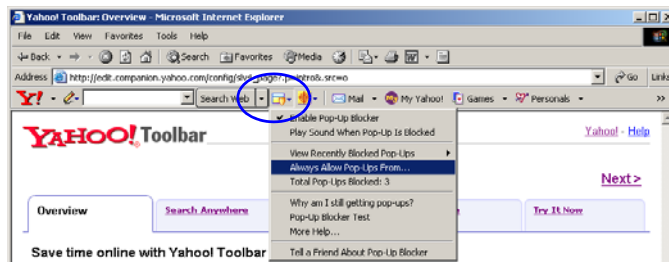


Fig. A-1 Select menu option Always Allow Pop-Ups From

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

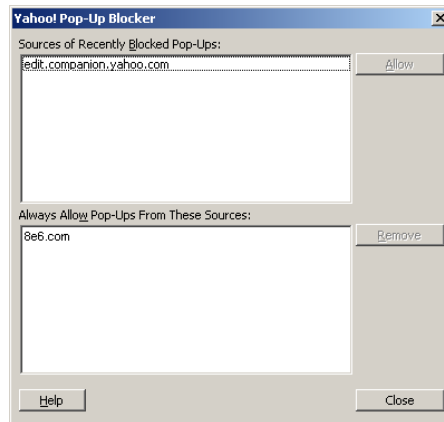


Fig. A-2 Allow pop-ups from source

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:

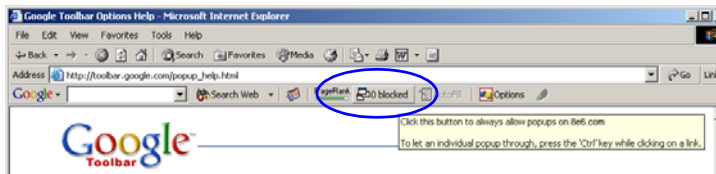


Fig. A-3 # blocked icon enabled

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

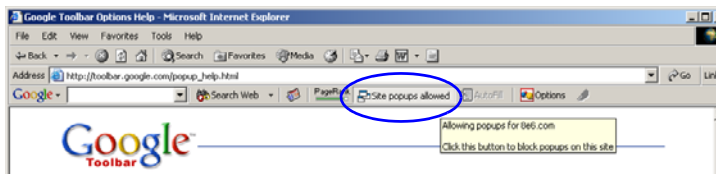


Fig. A-4 Site pop-ups allowed icon enabled

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:

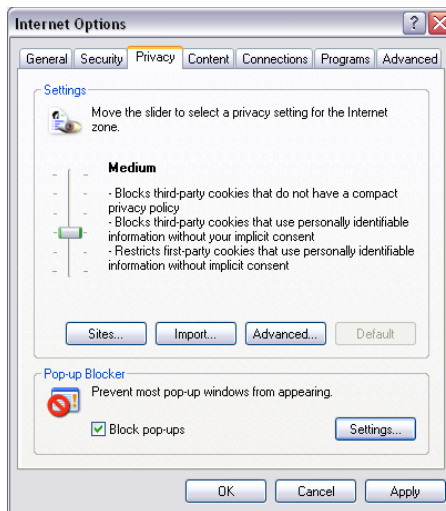


Fig. A-5 Enable pop-up blocking

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**:

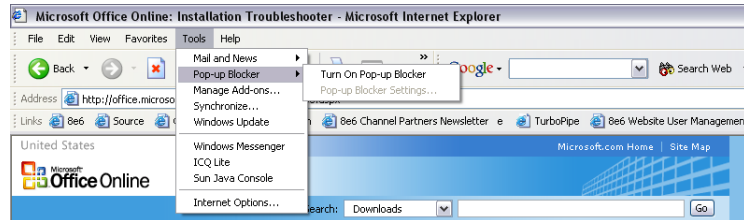


Fig. A-6 Toolbar setup

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:

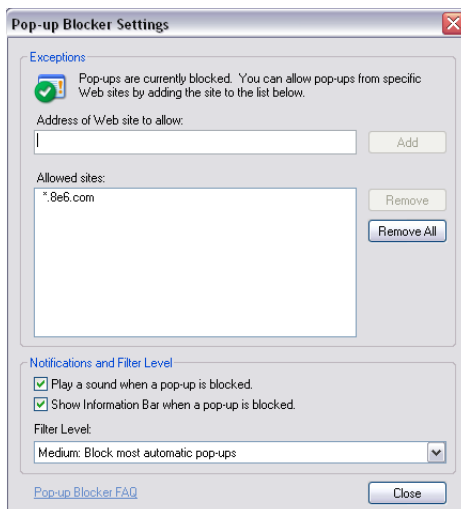


Fig. A-7 Pop-up Blocker Settings

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:

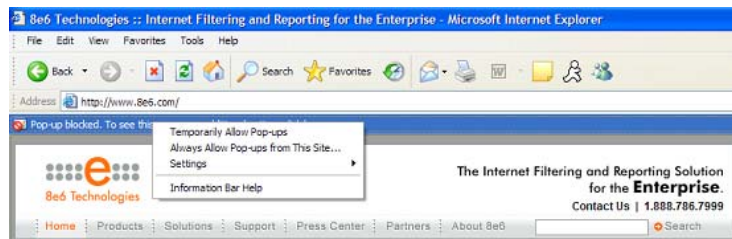


Fig. A-8 Information Bar menu options

2. Select **Always Allow Pop-ups from This Site**—this action opens the Allow pop-ups from this site? dialog box:

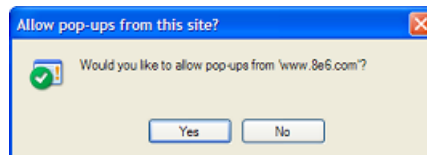


Fig. A-9 Allow pop-ups dialog box

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:

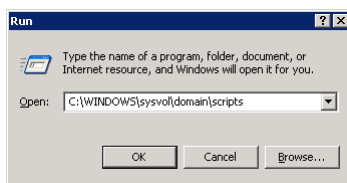


Fig. B-1 Run dialog box

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:

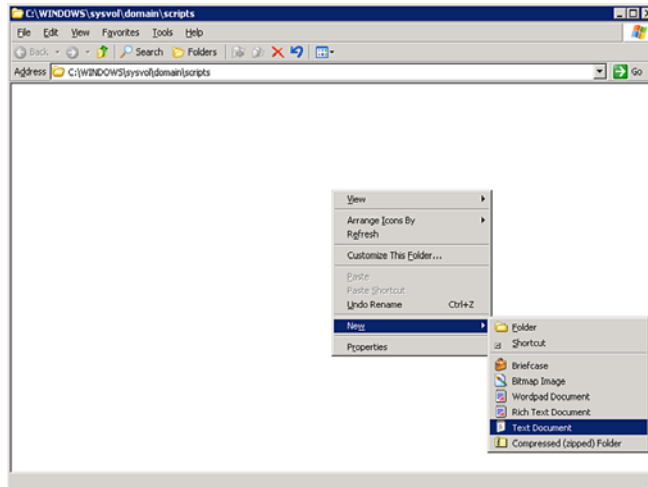


Fig. B-2 C:\WINDOWS\sysvol\domain\scripts window

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

5. Select **New > Text Document** to launch a New Text Document:

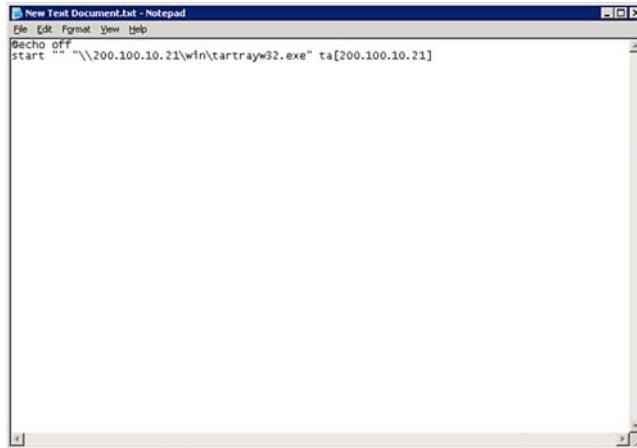


Fig. B-3 New Text Document

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:

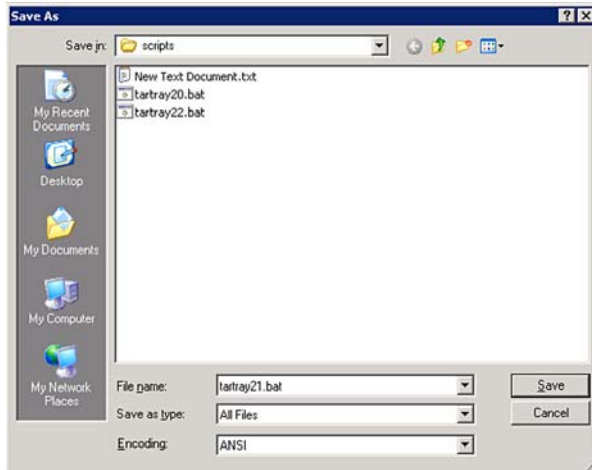


Fig. B-4 Save As dialog box

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:

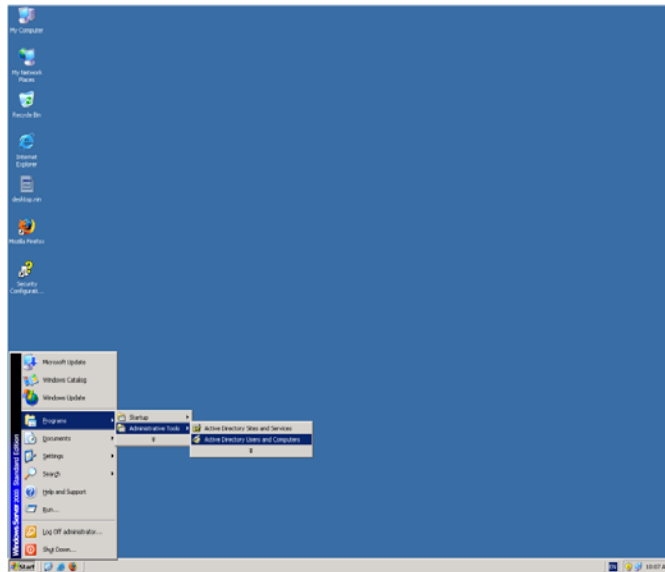


Fig. B-5 Programs > Administrative Tools > Active Directory Users

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:

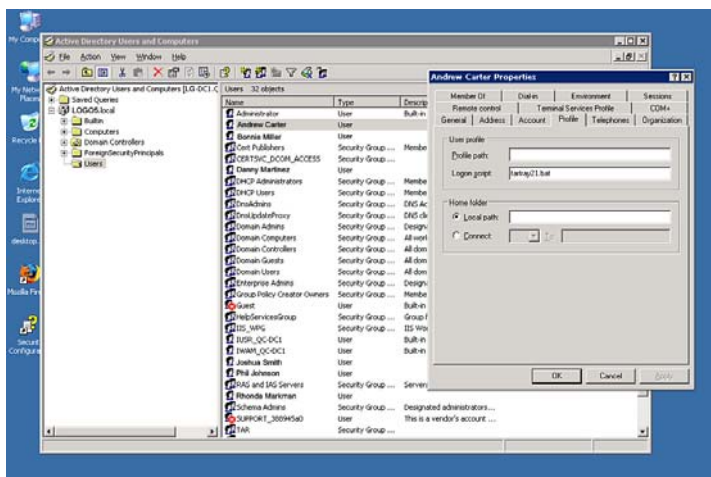


Fig. B-5 Properties dialog box, Active Directory Users folder

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:

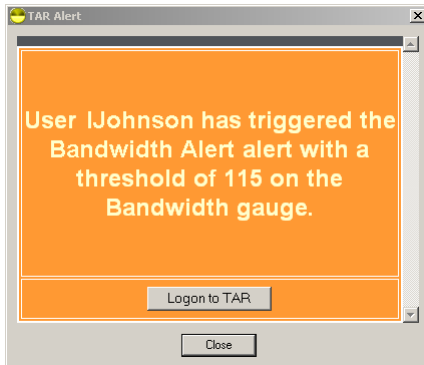


Fig. B-6 TAR Alert

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:

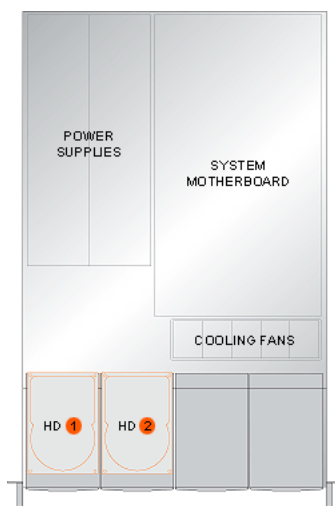
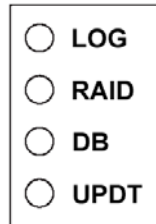


Fig. C-1 TAR RAID Server components

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

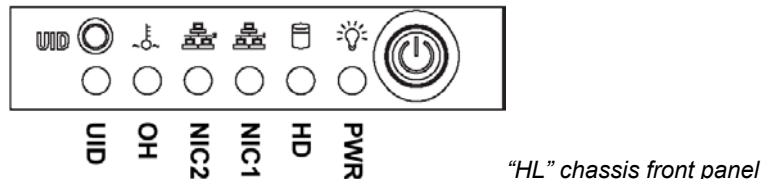
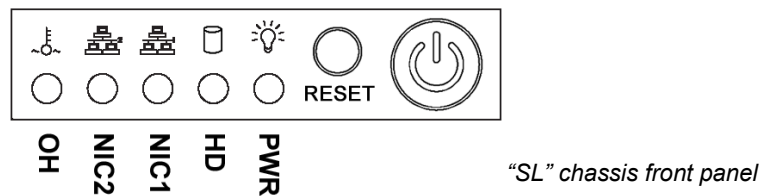
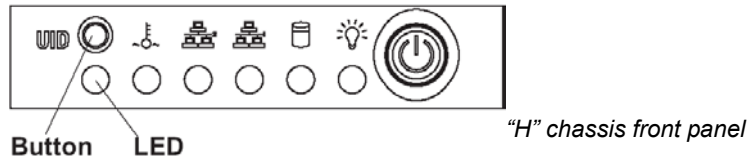
LED Indicator Chart

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.



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.)



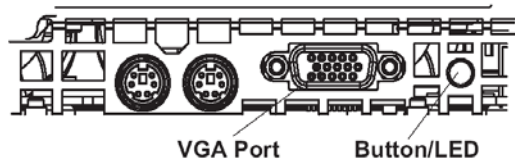
Power (icon) – The LED is unlit when the server is turned off. A steady green LED indicates power is being supplied to the unit's power supplies. (See also Rear of chassis.) (See Power supply failure in the Troubleshooting sub-section for information on detecting a power supply failure and resolving this problem.)



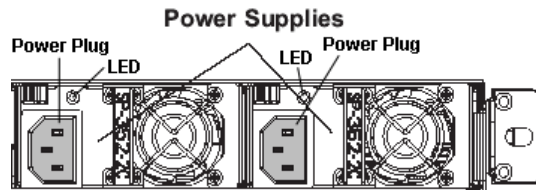
Power (button) – When the power button is pressed, the main power to the server is turned on. When the power button is pressed again, the main power to the server is removed but standby power is still supplied to the server.

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.



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 window 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 window in the Administrator console is accessible via the **Administration > Hardware Detector** menu selection:

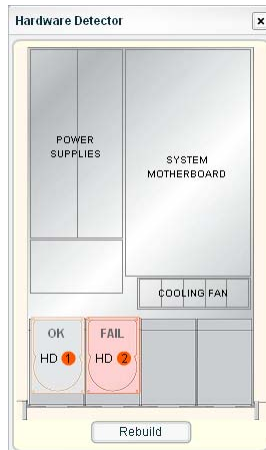


Fig. C-2 Hardware Detector window

The Hardware Detector window displays the current RAID Array Status for the two hard drives (HD 1 and HD 2).

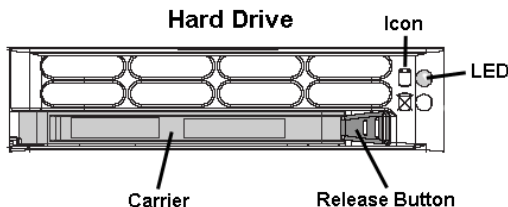
Normally, when both hard drives are functioning without failure, the text "OK" displays above the hard drive number, and no other text displays in the diagram.

However, if a hard drive has failed, the image of the drive displays in red and the message "FAIL" displays above the hard drive number.

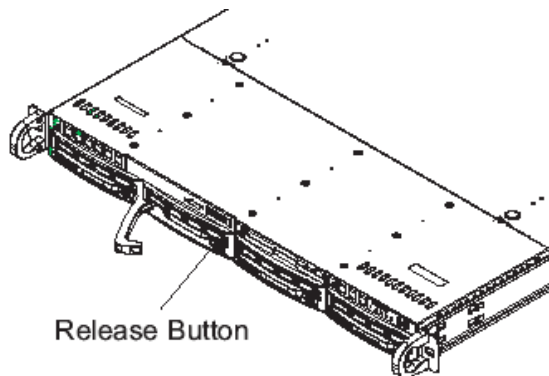
Before taking any action in this window, proceed to Step 3.

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 window in the Administrator console, and click **Rebuild** to display instructions on how to proceed with the rebuild process:

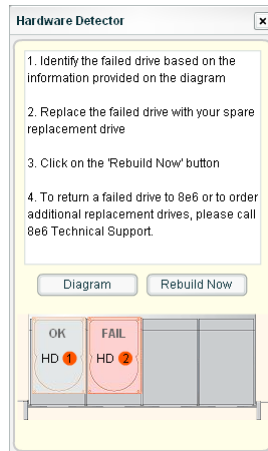


Fig. C-3 Hardware Detector window, step 2

- B. Click **Diagram** to return to the previous display (see Fig. C-2) or click **Rebuild Now** to initiate the process for rebuilding the hard drive:

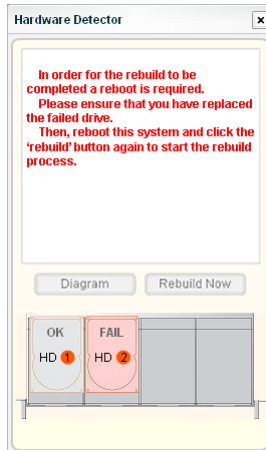


Fig. C-4 Hardware Detector window, step 3

- C. Return to the chassis. Push the Power button in and hold it down for five seconds, and then release it to reboot the unit.
- D. Log back into the Administrator console, and navigate to **Administration > Hardware Detector** window that still displays the failed image (see Fig. C-2).
- E. Click **Rebuild** again to redisplay the instructional page of the wizard (see Fig. C-3).
- F. Click **Rebuild Now** again to initiate the drive rebuild process, and to display a message stating that after the hard drive is rebuilt, it will take a couple of hours for the RAID array to finish the reconstruction process:

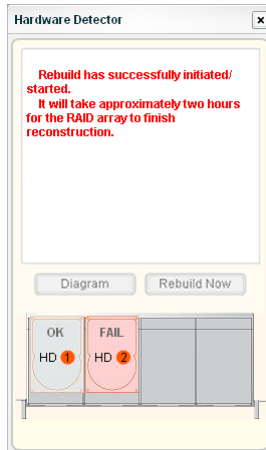


Fig. C-5 Hardware Detector window, step 4

During this process, a message might display indicating that the server has timed out.

- G. If you log back into the Administrator console and navigate to **Administration > Hardware Detector** window, note that the failed hard drive now displays an “OK” status even though the rebuild process has been initiated and is running in the background:

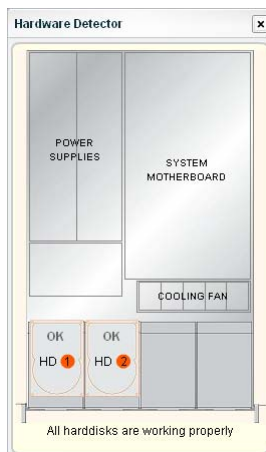


Fig. C-6 Hardware Detector window, rebuild steps completed



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.



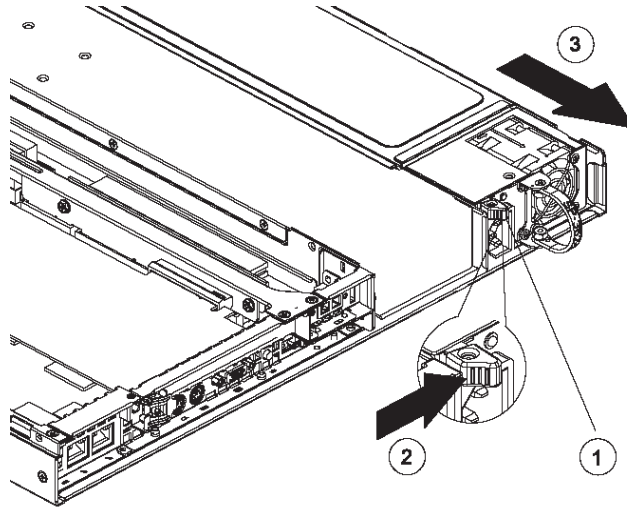
WARNING: Be sure the correct failed power supply has been identified. Removing the wrong power supply will cause the system to crash.

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 overheating condition, which may be caused by cables obstructing the airflow in the system or the ambient room temperature being too warm. Check the routing of the cables and make sure all fans are present and operating normally. The LED will remain steady as long as the overheating condition exists.

Appendix 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

- alert log 91
- alert messages 83

B

- backup 150
- bandwidth 34
 - gauge 60
 - gauge monitoring 104
 - reading gauges 61
 - traffic monitoring 104
- base group 21, 57
 - definition 201
- button, terminology 4
- byte score 62, 111, 123

C

- checkbox, terminology 4
- Ctrl key 15
- custom category 126
 - definition 201
- custom search 100

D

- device registry 139
- dialog box, terminology 4
- disable pop-up blockers 168

E

- Enterprise Reporter 35
- Enterprise Reporter Web Client 77
- environment requirements 7
- ER 34, 48, 95, 99, 124

F

- field, terminology 4
- Firefox 7
- Flash plug-in 7
- frame, terminology 5
- FTP 106
 - definition 201

G

- gauge
 - components 60
 - restore configuration settings 150
 - scoring methodology 50
 - types 60
- global administrator 2
 - definition 201
- group administrator 2
 - definition 201

H

- H server 186
- hit score 61, 75, 104
- HL server 186
- How to
 - access the Alert Manager window 83
 - access the Gauge Management window 53
 - add a new alert 84
 - add a new gauge 54
 - add a new gauge in the dashboard 59
 - drill down into a gauge 72
 - navigate the interface 12, 14
 - set up email alert notifications 85
 - view an email alert 86
 - view end user gauge activity 73, 74
 - view URLs a user visited 73, 77
- HTTP 105
 - definition 201
- HTTPS 8

I

- IM 107
- inbound
 - traffic monitoring 104
- install software update 155
- installation prerequisite 8
- instant messaging
 - definition 201
- Internet Explorer 7, 10, 171
- IP group
 - authentication method 177
- IPGROUP 20

J

- Java virtual machine 8

K

- keyword
 - dashboard gauge method 58

L

- LDAP 20, 177
 - definition 202
 - server types supported 18
- LED indicators 187
- library categories
 - definition 201
- list box, terminology 5
- lockout 42, 74, 83, 115
 - automatic 86
 - end user workstation 81
 - function 85
 - list management 92
 - manual 78
 - unlock workstation 94
- log
 - into TAR 11
 - out of TAR 13

M

- Macintosh 7
- Master User List 132

N

- network requirements 8

O

- outbound
 - traffic monitoring 104

P

- P2P 106
 - definition 202
- panel, terminology 5
- peer-to-peer
 - definition 202
- pop-up blocking, disable 168
- pop-up box/window, terminology 5
- port
 - gauge 60
 - number 105
- Product Warranties section 165
- protocol
 - bandwidth gauge 60, 105
 - definition 202
- pull-down menu, terminology 6

Q

- quick start
 - installation procedures 10, 38, 40, 124, 143, 155
- Quick Start Guide 9

R

- R3000 1, 7, 8, 34, 35, 48, 49, 95, 99, 124, 126, 130, 132, 139
 - end user lockout 86, 117

- RAID 160
- Real Time Probe 202
- recovery procedures 150
- requirements
 - environment 7

S

- Safari 7
- screen, terminology 6
- search engine
 - definition 202
- search engine keyword
 - in custom category 128
- Shift key 15
- SL server 186
- SMTP 106
 - definition 202
- software updates 155
- synchronization
 - custom category update 79, 118
 - definition 202
 - Master User List update 132
 - update device registry 139
- system requirements 7
- System Tray 177

T

- tab, terminology 6
- TCP 105
 - definition 202
- technical support 162
- text box, terminology 6
- threat score 51, 61
 - assign weight 52
- timespan 55, 61, 64, 96, 108, 121
- Traveler 155
 - definition 202

U

- UDP 105
 - definition 203
- URL 9, 10
 - category details 77
 - custom category 128
 - dashboard gauge method 58
 - lock out user from bandwidth usage 117
 - lock out users from access 79, 86, 92
 - trend reports 95
 - trend reports for bandwidth usage 121
 - with wildcard in custom category 128
- URL Keyword
 - custom category 129
- URL, definition 203

W

- window, terminology 6
- wizard 9, 11, 39
- workstation requirements 7