8e6 Technologies

8e6® ProxyBlocker

USER GUIDE

Model: ProxyBlocker

Release 2.1.00 • Manual Version 1.01

8E6 PROXYBLOCKER USER GUIDE

© 2008 8e6 Technologies
All rights reserved.

Version 1.01, published July 2008
To be used with the ProxyBlocker Authentication User Guide version 1.01 for software release 2.1.00

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/pba_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# PBA2.0-UG_v1.01-0807

CONTENTS

APPENDICES SECTION 396

INTRODUCTORY SECTION

8e6 ProxyBlocker

8e6 Technologies' 8e6 ProxyBlocker offers a solution for organizations using an Internet filtering product other than 8e6's R3000 Enterprise Filter. 8e6 ProxyBlocker tracks each user's online activity of Web-based proxies and anonymizers, and can be configured to block specific Web sites or service ports, thereby protecting your organization against lost productivity, network bandwidth issues, and possible legal problems that can result from the misuse of Internet resources.

About this User Guide

The 8e6 ProxyBlocker User Guide primarily addresses the network administrator designated to configure and manage the 8e6 ProxyBlocker server on the network. This administrator is referred to as the "global administrator" throughout this user guide. In part, this user guide also addresses administrators who manage user groups on the network. These administrators are referred to as "group administrators" throughout this user guide. Additional information is provided for administrators of networks that use 8e6 ProxyBlocker with 8e6's Enterprise Reporter (ER) for both filtering and reporting.

See the 8e6 ProxyBlocker Authentication User Guide at http://www.8e6.com/docs/pba_auth_ug.pdf for information on authentication.

This user guide is organized into the following sections:

- **Introductory Section** - This section is comprised of an overview on filtering, Web access logging, and instant messaging and peer-to-peer blocking. This section also

provides information on how to use this user guide to help you configure the ProxyBlocker.

- **Global Administrator Section** - This section includes information for the global administrator—who has all rights and permissions on the ProxyBlocker box—to create group administrator accounts, and to configure the ProxyBlocker for use on the network.
- **Group Administrator Section** - This section includes information for administrators authorized by the global administrator to manage profiles of designated groups and their associated users on the 8e6 ProxyBlocker. Group administrators also have rights to access certain library category functions.
- **Technical Support / Product Warranties Section** - This section contains information on technical support and product warranties
- **Appendices** - Appendix A includes formats and rules used in the filtering profile file. Appendix B provides a list of messages that display when 8e6's executable program "Traveler" is launched and attempts to download updates to the ProxyBlocker server. Appendix C includes information on creating a customized block page. Appendix D provides tips on how to override pop-up windows with pop-up blocker software installed. Appendix E includes information on configuring the ProxyBlocker to work with 8e6's Enterprise Reporter (ER) application. Appendix F includes information about RAID maintenance and troubleshooting on a ProxyBlocker "SL" server. Appendix G 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.*

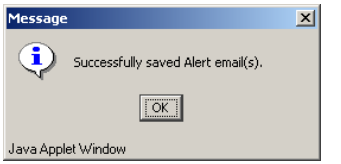
***TIP**: The "tip" icon is followed by italicized text giving you hints on how to execute a task more efficiently.*

***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

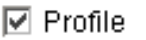
The following terms are used throughout this user guide. Sample images (not to scale) are included for each item.

- **alert box** - a message box that opens in response to an entry you made in a dialog box, window, or screen. This box often contains a button (usually labeled “OK”) for you to click in order to confirm or execute a command.

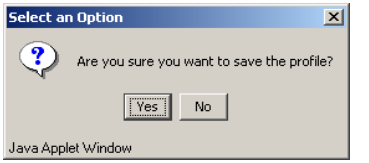


- **button** - an object in a dialog box, window, or screen that can be clicked with your mouse to execute a command.

- **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.



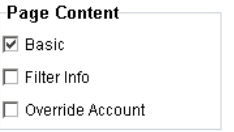
- **dialog box** - a box that opens in response to a command made in a window or screen, and requires your input. You must choose an option by clicking a button (such as “Yes” or “No”, or “Next” or “Cancel”) to execute your command. As dictated by this box, you also might need to make one or more entries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



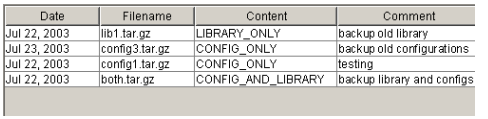
- **field** - an area in a dialog box, window, or screen that either accommodates your data

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, check-boxes, 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.

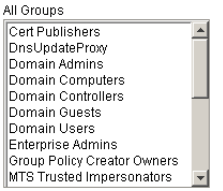


- **grid** - an area in a frame that displays rows and columns of data, as a result of various processes. This data can be reorganized in the Administrator console, by changing the order of the columns.



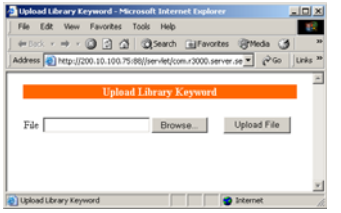
Date	Filename	Content	Comment
Jul 22, 2003	lib1.tar.gz	LIBRARY_ONLY	backup old library
Jul 23, 2003	config3.tar.gz	CONFIG_ONLY	backup old configurations
Jul 22, 2003	config1.tar.gz	CONFIG_ONLY	testing
Jul 22, 2003	both.tar.gz	CONFIG_AND_LIBRARY	backup library and configs

- **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.



- **navigation panel** - the panel that displays at the left of a screen. This panel can contain links that can be clicked to open windows or dialog boxes at the right of the screen. One or more tree lists also can display in this panel. When an item in the tree list is clicked, the tree list opens to reveal items that can be selected.

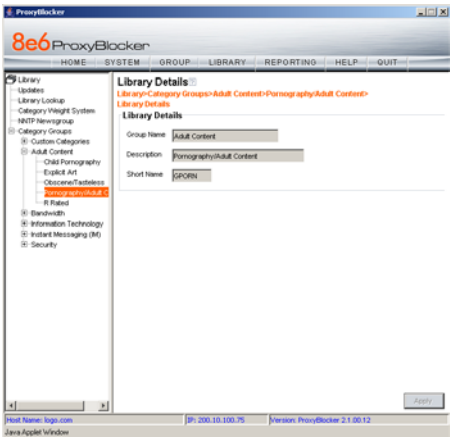
- **pop-up box** or **pop-up window** - a box or window that opens after you click a button in a dialog box, window, or screen. This box or window may display information, or may require you to make one or more entries. Unlike a dialog box, you do not need to choose between options.



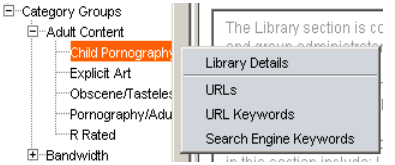
- **pull-down menu** - a field in a dialog box, window, or screen that contains a down-arrow to the right. When you click the arrow, a menu of items displays from which you make a selection.

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

- **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.

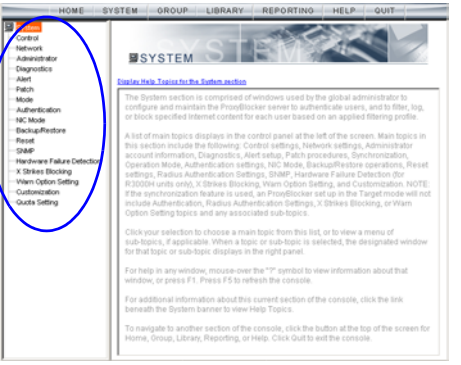


- **sub-topic** - a subset of a main topic that displays as a menu item for the topic. The menu of sub-topics opens when a pertinent topic link in the left panel—the navigation panel—of a screen is clicked. If a sub-topic is selected, the window for that sub-topic displays in the right panel of the screen, or a pop-up window or an alert box opens, as appropriate.

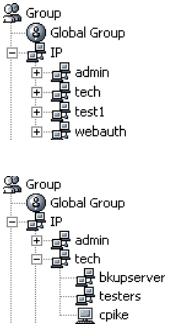


- **text box** - an area in a dialog box, window, or screen that accommodates your data entry. A text box is a type of field. (See “field”.)

- **topic** - a topic displays as a link in the left panel—the navigation panel—of a screen. By clicking the link for a topic, the window for that topic displays in the right panel of the screen, or a menu of sub-topics opens.



- **tree** - a tree displays in the navigation panel of a screen, and is comprised of a hierarchical list of items. An entity associated with a branch of the tree is preceded by a plus (+) sign when the branch is collapsed. By double-clicking the item, a minus (-) sign replaces the plus sign, and any entity within that branch of the tree displays. An item in the tree is selected by clicking it.



- **window** - a window displays on a screen, and can contain frames, fields, text boxes, list boxes, buttons, checkboxes, and radio buttons. A window for a topic or sub-topic displays in the right panel of the screen. Other types of windows include pop-up windows, login windows, or ones from the system such as the Save As or Choose file windows.

Overview

The ProxyBlocker's Administrator console is used by the global administrator—and group administrator, as required—to configure the ProxyBlocker server to perform the following basic functions:

- filter URLs (Web addresses) on the Internet
- log traffic on the Internet

and, if applicable for your organization:

- block instant messaging and peer-to-peer services
- authenticate users via the existing authentication system on the network

***NOTE**: See the 8e6 ProxyBlocker Authentication User Guide at **http://www.8e6.com/docs/pba_auth_ug.pdf** for information on setting up and using authentication.*

To help you become familiar with the ProxyBlocker and how it functions on the network, Chapter 1 of this section of the User Guide provides an overview on filtering. Chapter 2 gives insight into Web site access logging, and instant messaging and peer-to-peer setup procedures. Chapter 3 includes details on getting started, with log in and log out procedures, and tips on navigating the Administrator console.

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 (Windows Vista running IE7)
- Macintosh OS X Version 10.5 running Safari 2.0, Firefox 2.0
- JavaScript enabled
- Java Virtual Machine
- Java Plug-in (use the version specified for the Proxy-Blocker software version)

***NOTE**: 8e6 ProxyBlocker administrators must be set up with software installation privileges in order to install Java used for accessing the interface.*

Network Requirements

- High speed connection from the ProxyBlocker server to the client workstations
- HTTPS connection to 8e6's software update server
- Internet connectivity for downloading Java virtual machine, if not already installed

Chapter 1: Filtering Operations

Invisible Mode

The ProxyBlocker is set up in the invisible mode, indicating that the unit will filter all connections on the Ethernet between client PCs and the Internet, without stopping each IP packet on the same Ethernet segment. The unit will only intercept a session if an inappropriate request was submitted by a client. In this scenario, the ProxyBlocker returns a message to the client and server to deny the request, and a block page displays to deny the client access to the site or service.

Figure 1:1-1 depicts the invisible mode that removes the ProxyBlocker from any inclusion in the network connection path.

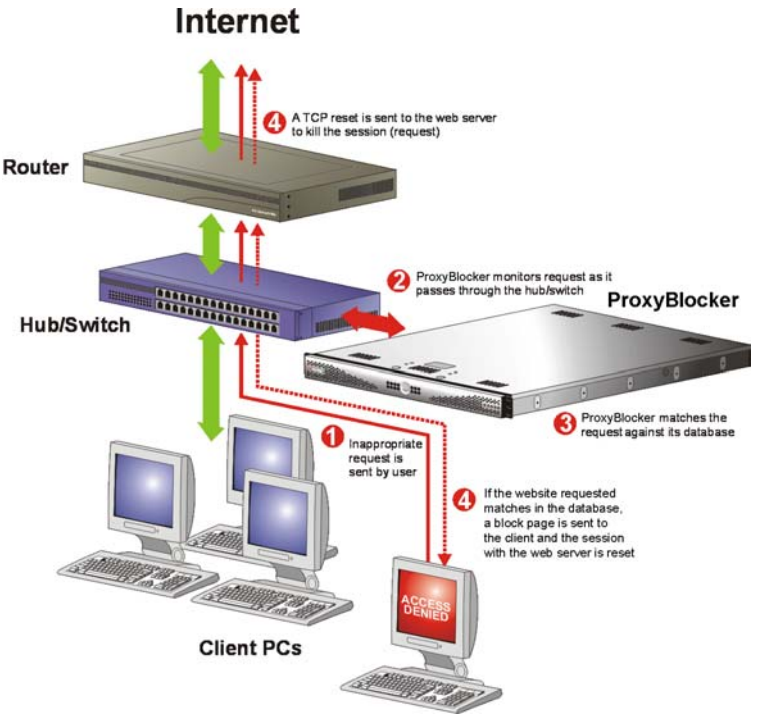


Fig. 1:1-1 Pass-by filtering diagram

When users (Client PCs) make Internet requests, the traffic flows (1) through the network path without interruption. The ProxyBlocker captures the request as the user's request (2) leaves the network. The ProxyBlocker then determines the action (3) to either block or pass the request. If the ProxyBlocker determines to block the user's request, a block message (4) is sent to the user plus a terminate message (4) is sent to the Internet server.

In the invisible mode, the ProxyBlocker performs as a standalone server that can be connected to any network environment.

Group Types

After the operational filtering mode is configured on the ProxyBlocker, the group type(s) that will be used on the ProxyBlocker must be set up so that filtering can take place.

In the Group section of the Administrator console, group types are structured in a tree format in the navigation panel. The global administrator can access the Global Group and IP groups in the tree. The group administrator can only access the designated IP group to be maintained.

***NOTE**: If authentication is enabled, the global administrator can also access the NT and LDAP branches of the tree.*

Global Group

The first group that must be set up is the global group, represented in the tree structure by the global icon  . The filtering profile created for the global group represents the default profile to be used by all groups that do not have a filtering profile, and all users who do not belong to a group.

IP Groups

The IP group type is represented in the tree by the IP icon . A master IP group is comprised of sub-group members and/or individual IP members .

The global administrator adds master IP groups, adds and maintains override accounts at the global level, and establishes and maintains the minimum filtering level.

The group administrator of a master IP group adds sub-group and individual IP members, override account, time profiles and exception URLs, and maintains filtering profiles of all members in the master IP group.

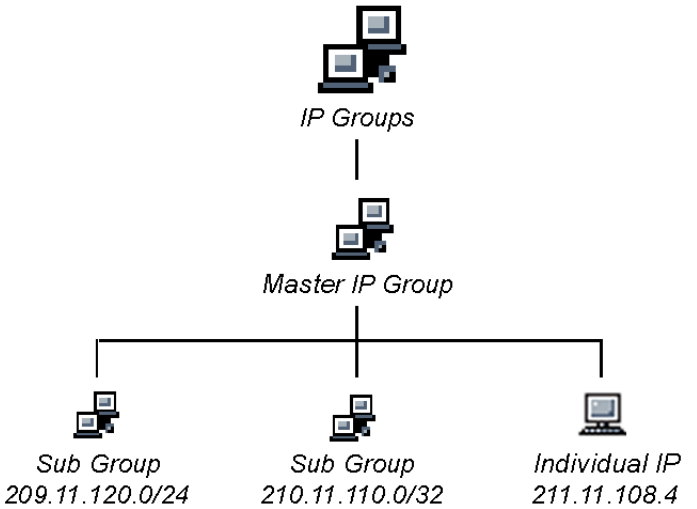


Fig. 1:1-2 IP diagram with a sample master IP group and its members

Filtering Profile Types

A filtering profile is used by all users who are set up to be filtered on the network. This profile consists of rules that dictate whether a user has access to a specified Web site or service on the Internet.

The following types of filtering profiles can be created, based on the set up in the tree menu of the Group section of the console:

Global Group

- **global filtering profile** - the default filtering profile positioned at the base of the hierarchical tree structure, used by end users who do not belong to a group.

IP group (master group)

- **master group filtering profile** - used by end users who belong to the master group.
- **master time profile** - used by master group users at a specified time.

IP group member

- **sub-group filtering profile** - used by a sub-group member.
- **individual filtering profile** - used by an individual IP group member.
- **time profile** - used by a sub-group/individual IP group member at a specified time.

Other filtering profiles

- **authentication profile** - used by NT and/or LDAP group members.

***NOTE**: For information about authentication filtering profiles, see the 8e6 ProxyBlocker Authentication User Guide.*

- **override account profile** - set up in either the global group section or the master group section of the console.
- **lock profile** - set up under X Strikes Blocking in the Filter Options section of the profile.

Static Filtering Profiles

Static filtering profiles are based on fixed IP addresses and include profiles for master IP groups and their members.

Master IP Group Filtering Profile

The master IP group filtering profile is created by the global administrator and is maintained by the group administrator. This filtering profile is used by members of the group—including sub-group and individual IP group members—and is customized to allow/deny users access to URLs, or warn users about accessing specified URLs, to redirect users to another URL instead of having a block page display, and to specify usage of appropriate filter options.

IP Sub-Group Filtering Profile

An IP sub-group filtering profile is created by the group administrator. This filtering profile applies to end users in an IP sub-group and is customized for sub-group members.

Individual IP Member Filtering Profile

An individual IP member filtering profile is created by the group administrator.This filtering profile applies to a specified end user in a master IP group.

Active Filtering Profiles

Active filtering profiles include the global group profile, override account profile, time profile, and lock profile.

***NOTE**: For information about authentication filtering profiles, see the 8e6 ProxyBlocker Authentication User Guide.*

Global Filtering Profile

The global filtering profile is created by the global administrator. This profile is used as the default filtering profile. The global filtering profile consists of a customized profile that contains a list of library categories to block, open, add to a white list, or assign a warn setting, and service ports that are configured to be blocked. A URL can be specified for use instead of the standard block page when users attempt to access material set up to be blocked. Various filter options can be enabled.

Override Account Profile

If any user needs access to a specified URL that is set up to be blocked, the global administrator or group administrator can create an override account for that user. This account grants the user access to areas set up to be blocked on the Internet.

Time Profile

A time profile is a customized filtering profile set up to be effective at a specified time period for designated users.

Lock Profile

This filtering profile blocks the end user from Internet access for a set period of time, if the end user's profile has the X Strikes Blocking filter option enabled and he/she has received the maximum number of strikes for inappropriate Internet usage.

Filtering Profile Components

Filtering profiles are comprised of the following components:

- **library categories** - used when creating a rule, minimum filtering level, or filtering profile for the global group or any entity
- **service ports** - used when setting up filter segments on the network, creating the global group (default) filtering profile, or establishing the minimum filtering level
- **rules** - specify which library categories should be blocked, left open (a set number of minutes in which that category remains open can be defined), assigned a warn setting, or white listed
- **filter options** - specify which features will be enabled: X Strikes Blocking, Google/Yahoo!/Ask.com/AOL Safe Search Enforcement, Search Engine Keyword Filter Control, URL Keyword Filter Control
- **minimum filtering level** - takes precedence over filtering profiles of entities who are using a filtering profile other than the global (default) filtering profile
- **filter settings** - used by service ports, filtering profiles, rules, and the minimum filtering level to indicate whether users should be granted or denied access to specified Internet content

Library Categories

A library category contains a list of Web site addresses and keywords for search engines and URLs that have been set up to be blocked or white listed. Library categories are used when creating a rule, the minimum filtering level, or a filtering profile.

8e6 Supplied Categories

8e6 furnishes a collection of library categories, grouped under the heading “Category Groups” (excluding the “Custom Categories” group). Updates to these categories are provided by 8e6 on an ongoing basis, and administrators also can add or delete individual URLs within a specified library category.

Custom Categories

Custom library categories can be added by either global or group administrators. As with 8e6 supplied categories, additions and deletions can be made within a custom category. However, unlike 8e6 supplied categories, a custom category can be deleted.

***NOTE**: 8e6 cannot provide updates to custom categories. Maintaining the list of URLs and keywords is the responsibility of the global or group administrator.*

Service Ports

Service ports are used when setting up filter segments on the network (the range of IP addresses/netmasks to be detected by the ProxyBlocker), the global (default) filtering profile, and the minimum filtering level.

When setting up the range of IP addresses/netmasks to be detected, service ports can be set up to be open (ignored). When creating the global filtering profile and the minimum filtering level, service ports can be set up to be blocked or filtered.

Examples of service ports that can be set up include File Transfer Protocol (FTP), Hyper Text Transfer Protocol (HTTP), Network News Transfer Protocol (NNTP), Secured HTTP Transmission (HTTPS), and Secure Shell (SSH).

Rules

A rule is comprised of library categories to block, leave open, assign a warn setting, or include in a white list. Access to an open library category can be restricted to a set number of minutes. Each rule that is created by the global administrator is assigned a number. A rule is selected when creating a filtering profile for an entity.

Minimum Filtering Level

The minimum filtering level consists of library categories set up at the global level to be blocked or opened, and service ports set up to be blocked or filtered. If the minimum filtering level is created, it applies to all users in IP groups, and takes precedence over filtering settings made for group and user filtering profiles.

The minimum filtering level does not apply to any user who does not belong to a group, and to groups that do not have a filtering profile established.

***NOTE**: If the minimum filtering level is not set up, global (default) filtering settings will apply instead.*

If an override account is established at the IP group level for a member of a master IP group, filtering settings made for that end user will override the minimum filtering level if the global administrator sets the option to allow the minimum filtering level to be bypassed. An override account established at the global group level will automatically bypass the minimum filtering level.

Filter Settings

Categories and service ports use the following settings to specify how filtering will be executed:

- **block** - if a category or a service port is given a block setting, users will be denied access to the URL set up as “blocked”
- **open** - if a category or the filter segment detected on the network is given an open (pass) setting, users will be allowed access to the URL set up as “opened”

***NOTE**: Using the quota feature, access to an open category can be restricted to a defined number of minutes.*

- **always allowed** - if a category is given an always allowed setting, the category is included in the user’s white list and takes precedence over blocked categories
- **warn** - If a category is given a warn setting, a warning page displays for the end user to warn him/her that accessing the intended URL may be against established policies and to proceed at his/her own risk
- **filter** - if a service port is given a filter setting, that port will use filter settings created for library categories (block or open settings) to determine whether users should be denied or allowed access to that port

- **ignore** - if the filter segment detected on the network has a service port set up to be ignored, that service port will be bypassed

Filtering Rules

Filtering Levels Applied

1. The global (default) filtering profile applies to any user who does not belong to a master IP group.
2. If the minimum filtering level is defined, it applies to all master IP groups and members assigned filtering profiles. The minimum filtering level combines with the user's profile to guarantee that categories blocked in the minimum filtering level are blocked in the user's profile.
3. For master IP group members:
   a. A master IP group filtering profile takes precedence over the global profile.
   b. A master IP group time profile takes precedence over the master IP group profile.
4. For IP sub-group members:
   a. An IP sub-group filtering profile takes precedence over the master IP group's time profile.
   b. An IP sub-group time profile takes precedence over the IP sub-group profile.
5. For individual IP members:
   a. An individual IP member filtering profile takes precedence over the IP sub-group's time profile.
   b. An individual IP member time profile takes precedence over the individual IP member profile.
6. An authentication (NT/LDAP) profile takes precedence over an individual IP member's time profile.

7. An override account profile takes precedence over an authentication profile. This account may override the minimum filtering level—if the override account was set up in the master IP group tree, and the global administrator allows override accounts to bypass the minimum filtering level, or if the override account was set up in the global group tree.

***NOTE**: An override account set up in the master group section of the console takes precedence over an override account set up in the global group section of the console.*

8. A lock profile takes precedence over all filtering profiles. This profile is set up under Filter Options, by enabling the X Strikes Blocking feature.

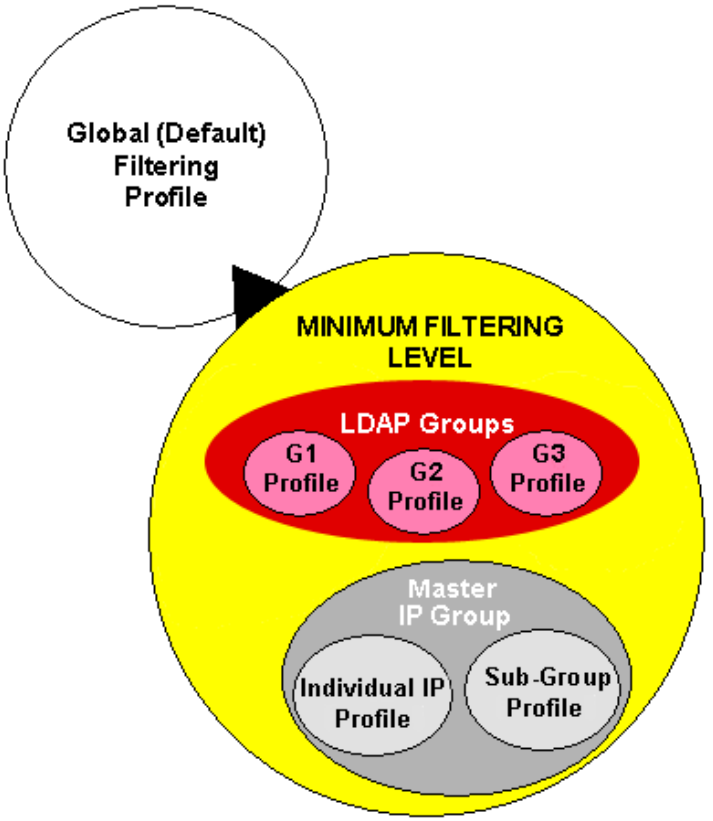


Fig. 1:1-3 Sample filtering hierarchy diagram

Chapter 2: Logging and Blocking

Web Access Logging

One of the primary functions of the ProxyBlocker is to log the activity of users on the Internet. Information captured in the log can be transferred to a reporting appliance, to be viewed on a PC monitor or output to a printer.

8e6 recommends using the Enterprise Reporter (ER) for generating reports. When the ER server is connected to the ProxyBlocker server, log files from the ProxyBlocker are transferred to the ER server where they are “normalized” and then inserted into a MySQL database. The ER client reporting application accesses that database to generate queries and reports.

***NOTE**: See Appendix E: Configuring the ProxyBlocker for ER Reporting for information on configuring the ProxyBlocker and ER.*

Instant Messaging, Peer-to-Peer Blocking

The ProxyBlocker has options for blocking and/or logging the use of Instant Messaging and Peer-to-Peer services, and makes use of Intelligent Footprint Technology (IFT) for greatly increasing management and control of these popular—yet potentially harmful—applications. This section explains how to set up and use IM and P2P.

How IM and P2P Blocking Works

IM Blocking

Instant Messaging (IM) involves direct connections between workstations either locally or across the Internet. Using this feature of the ProxyBlocker, groups and/or individual client machines can be set up to block the use of IM services specified in the library category.

When the IM module is loaded on the server, the Proxy-Blocker compares packets on the network with IM libraries stored on the ProxyBlocker server. If a match is found, the ProxyBlocker checks the user's profile to see whether the user's connection to the IM service should be blocked, and then performs the appropriate action.

***WARNING**: The following items are known issues pertaining to the IM module:*

- *IM can only block by destination IP address if network traffic is being tunneled, sent through a Virtual Private Network (VPN), or encrypted.*
- *IM will not be blocked if a client-side VPN is set up to proxy traffic through a remote IP address outside the connection protected by the ProxyBlocker.*
- *Some versions of the AOL client create a network interface that send a network connection through a UDP proxy server, which prevents blocking IM.*

P2P Blocking

Peer-to-Peer (P2P) involves communication between computing devices—desktops, servers, and other smart devices—that are linked directly to each other. Using this feature of the ProxyBlocker, groups and/or individual client machines can be set up to block the use of P2P services specified in the library category.

When the P2P module is loaded on the server, the Proxy-Blocker compares packets on the network with the P2P library stored on the ProxyBlocker server. If a match is found, the ProxyBlocker checks the user's profile to see whether the user's connection to the P2P service should be blocked, and then performs the appropriate action.

Setting up IM and P2P

IM and P2P are set up in the System and Library sections of the Administrator console.

1. In the System section, activate Pattern Blocking in the Filter window.
2. In the Library section, note the services set up to be blocked, as defined at: **http://www.8e6.com/pbahelp/files/1system_im_block.html**.

***NOTE**: Please contact an 8e6 technical support representative or a solutions engineer if access is needed to one or more P2P services blocked by 8e6's supplied library category for P2P.*

3. In the Manual Update to 8e6 Supplied Categories window (accessible via Library > Updates > Manual Update), IM pattern files can be updated on demand.

Using IM and P2P

To solely log IM and/or P2P user activity, the Pattern Blocking setting needs to be enabled in the Filter window.

To additionally block specified groups and/or users from using components and features of IM and/or P2P, settings need to be made in the Group section of the Administrator console.

If applying 8e6's supplied IM and/or P2P library category to an entity's profile, all IM and/or P2P services included in that category will be blocked.

***NOTE**: If IM and/or P2P was set up to be blocked while a user's IM and/or P2P session was in progress, the user will not be blocked from using that service until he/she logs off the server and back on again.*

Block IM, P2P for All Users

Block IM for All Users

To block IM for all users on the network:

- the Pattern Blocking option in the Filter window must be activated
- the global filtering profile must have ***both*** CHAT and specified individual Instant Messaging library categories (such as IMGEN, IMGCHAT, IMGTALK, ICQAIM, IMMSN, IMMYSP, and/or IMYAHOO) set up to be blocked
- the minimum filtering level profile must have ***both*** CHAT and specified individual Instant Messaging library categories set up to be blocked.

Block P2P for All Users

To block P2P for all users on the network:

- the Pattern Blocking option in the Filter window must be activated
- the global filtering profile must have the PR2PR library category set up to be blocked
- the minimum filtering level profile must have the PR2PR library category set up to be blocked.

Block Specified Entities from Using IM, P2P

Block IM for a Specific Entity

To block IM for a specified group or user:

- the Pattern Blocking option in the Filter window must be activated
- the CHAT and specified individual Instant Messaging library categories must ***both*** be set up to be blocked for that entity
- the global filtering profile should ***not*** have IM blocked, unless blocking all IM traffic with the Range to Detect feature is desired
- the minimum filtering level profile should ***not*** have IM blocked, unless blocking all IM traffic with the Range to Detect feature is desired.

Block P2P for a Specific Entity

To block P2P for a specified group or user:

- the Pattern Blocking option in the Filter window must be activated
- the PR2PR library category must be set up to be blocked for that entity
- the global filtering profile should ***not*** have P2P blocked, unless blocking all P2P traffic with the Range to Detect feature is desired
- the minimum filtering level profile should ***not*** have P2P blocked, unless blocking all P2P traffic with the Range to Detect feature is desired.

Chapter 3: Getting Started

Initial Setup

To initially set up your ProxyBlocker server, follow the instructions in the Quick Start Guide, the booklet packaged with your ProxyBlocker 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 ProxyBlocker Quick Start Guide, contact 8e6 Technologies immediately to have a copy sent to you.*

Using the Administrator Console

Log On

1. Launch a browser window supported by the Proxy-Blocker.
2. In the address line of the browser window, type in the ProxyBlocker server's IP address appended by the following port number:
   - ":88" for an HTTP address
   - ":1443" for an HTTPS address

   For example, if your IP address is 210.10.131.34, type in **http://210.10.131.34:88** or **https://210.10.131.34:1443**.
3. Click **Go** to open the ProxyBlocker Introductory Window:

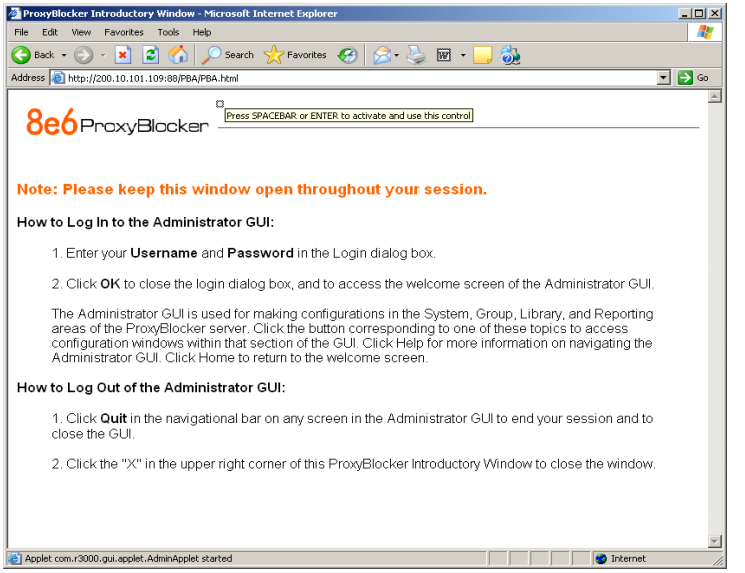


Fig. 1:3-1 ProxyBlocker Introductory Window

***NOTE**: The ProxyBlocker Introductory Window must be left open throughout your session. This window displays minimized when the Login dialog box opens.*

4. When the Login dialog box opens, enter your **Username** and **Password**:

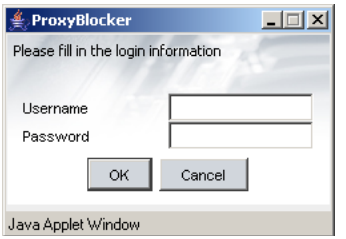


Fig. 1:3-2 Login dialog box

***TIP**: The default Username is **admin** and the Password is **user3**. To change this username and password, go to the Administrator window (see the Administrator window of the System screen in the Global Administrator Section) and create a global administrator account.*

***NOTE**: See Chapter 1: System screen in the Global Administrator Section for information on logging into the ProxyBlocker interface if your password has expired.*

5. Click **OK** to close the login dialog box and to access the welcome screen of the Administrator console:

Fig. 1:3-3 Welcome screen

On this screen, the ProxyBlocker Version Number displays in the Product frame, and dates for the Last Patch Update and Last Library Update display in the ProxyBlocker Status frame.

The following information displays at the bottom of the Administrator console: Host Name, LAN IP address used for sending block pages, and software Version number.

Last Library Update message

If it has been more than seven days since the ProxyBlocker last received updates to library categories, upon logging into the Administrator console a pop-up dialog box opens and displays the following message: ”Libraries were last updated more than 7 days ago. Do you want to update your libraries now?” Click either Yes or No to perform the following actions:

- **Yes** - clicking this button closes the dialog box and opens an alert box indicating that it will take a few minutes to perform the library update. Click **OK** to close the alert box and to execute the command to update the libraries. After the libraries are updated, today’s date will appear as the Last Library Update on the welcome screen.

***NOTE**: Refer to the Library screen’s Manual Update to 8e6 Supplied Categories window—in the Global Group Section—for information about updating library categories on demand.*

- **No** - clicking this button closes the dialog box and displays the welcome screen with the Last Library Update and the following message below in orange colored text: “Libraries were last updated 7 days ago. Please use the Weekly Update option”:

Fig. 1:3-4 Welcome screen, Last Library Update text

Click the checkbox “Do not show “Old Library Warning” dialog box in future” to disable the Last Library Update message pop-up box. After the libraries are updated, the welcome screen will appear as in Fig. 1:3:3 with today’s date as the Last Library Update in black text.

Navigation Tips

Access Main Sections

The Administrator console is organized into six sections, each accessible by clicking the corresponding button in the navigational bar at the top of the screen:

- **Home** - clicking this button displays the welcome screen of the Administrator console.
- **System** - clicking this button displays the main screen for the System section. This section is comprised of windows used by the global administrator for configuring and maintaining the server to authenticate users, and to filter or block specified Internet content for each user based on the applied filtering profile.
- **Group** - clicking this button displays the main screen for the Group section. Windows in the Group section are used for creating and managing master IP groups, sub-groups, and individual IP filtering profiles, or for setting up NT/LDAP domains, groups, and individual users, and their filtering profiles.
- **Library** - clicking this button displays the main screen for the Library section. Library section windows are used for adding and maintaining library categories. Library categories are used when creating or modifying a filtering profile.
- **Reporting** - clicking this button displays the main screen for the Reporting section. The Reporting section contains windows used for configuring reports on users' Internet activities.

- **Help** - clicking this button displays the Help screen. This screen includes navigational tips and a link to the PDF copy of this User Guide:

Fig. 1:3-5 Help screen

Help Features

Help features provide information about how to use windows in the Administrator console. Such features include help topics and tooltips.

Access Help Topics

Each of the main section screens contains a link beneath the banner. When that link is clicked, a separate browser window opens with Help Topics for that section:

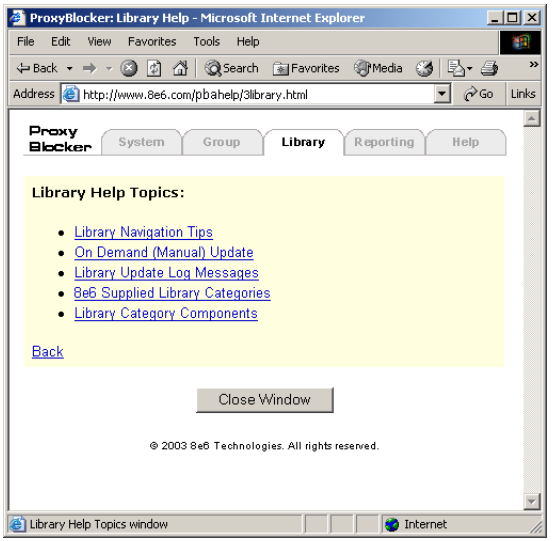


Fig. 1:3-6 Help Topics window

1. Click a link to go to a specified topic.
2. To view Help Topics for another section, click the tab for that section: System, Group, Library, Reporting, or Help.
3. Click **Close Window** to close the Help Topics window.

Tooltips

In any window that features the icon, additional information about that window can be obtained by hovering over that icon with your mouse, or by pressing the **F1** key on your keyboard.

- **Hover Display**

  The yellow tooltip box displays when you hover over the icon with your mouse:

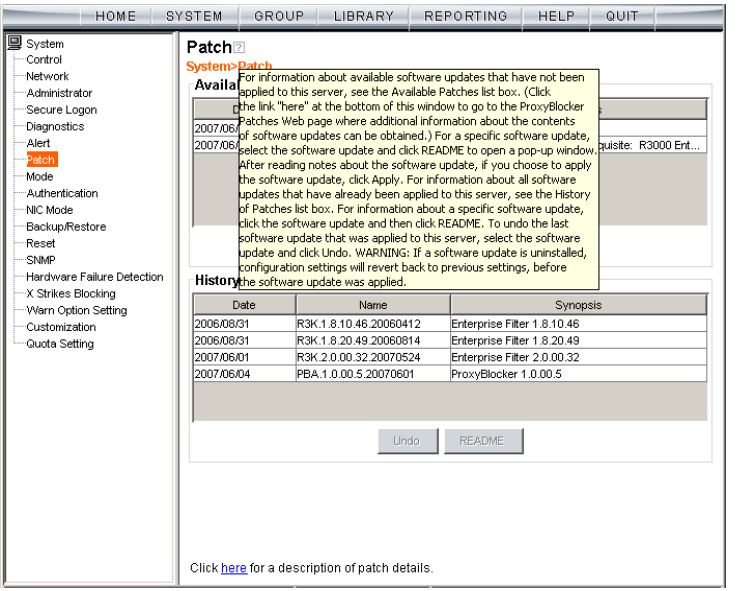


Fig. 1:3-7 Tooltip mouseover effect

To close the tooltip box, move the mouse away from the icon.

- **Help pop-up box**

  The Help pop-up box opens when you press the **F1** key on your keyboard:

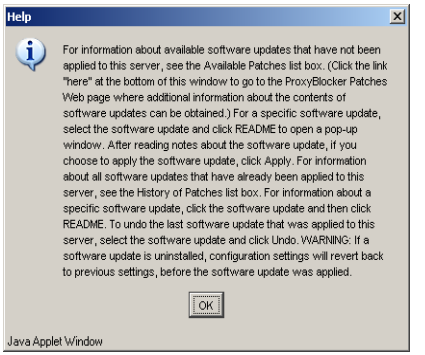


Fig. 1:3-8 Help pop-up box

  Click **OK** to close the pop-up box.

Screen and Window Navigation

All screens are divided into two panels: a navigation panel to the left, and a window in the panel to the right. Windows display in response to a selection made in the navigation panel.

In the Administrator console, screens and windows use different navigation formats, based on the contents of a given screen or window. Screens can contain topic links and sub-topic menus, and/or tree lists with topics and sub-topic menus. Windows can contain tabs that function as sub-windows.

Topic Links

In System, Library, and Reporting screens, the navigation panel contains topic links. By clicking a topic link, the window for that topic displays in the right panel:

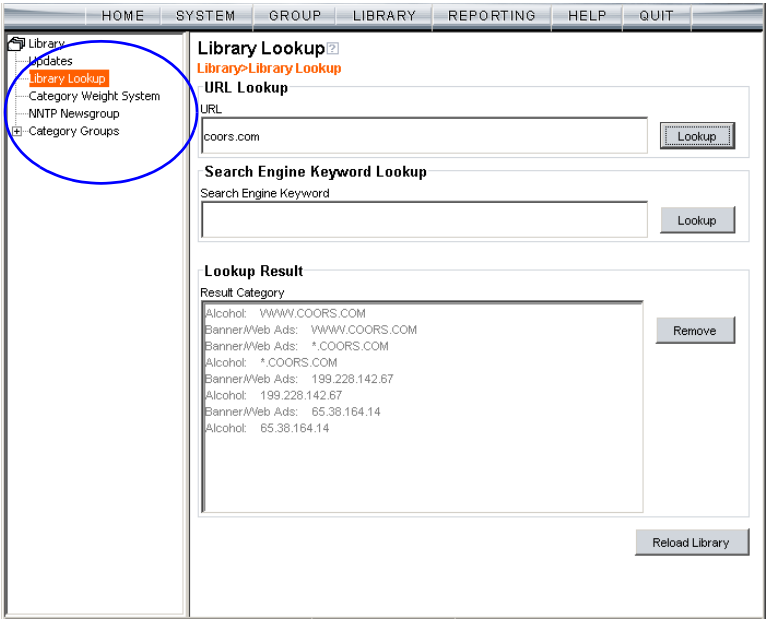


Fig. 1:3-9 Selected topic and its corresponding window

Select Sub-topics

Some topics in System and Library screens consist of more than one window. For these topics, clicking a topic link opens a menu of sub-topics:

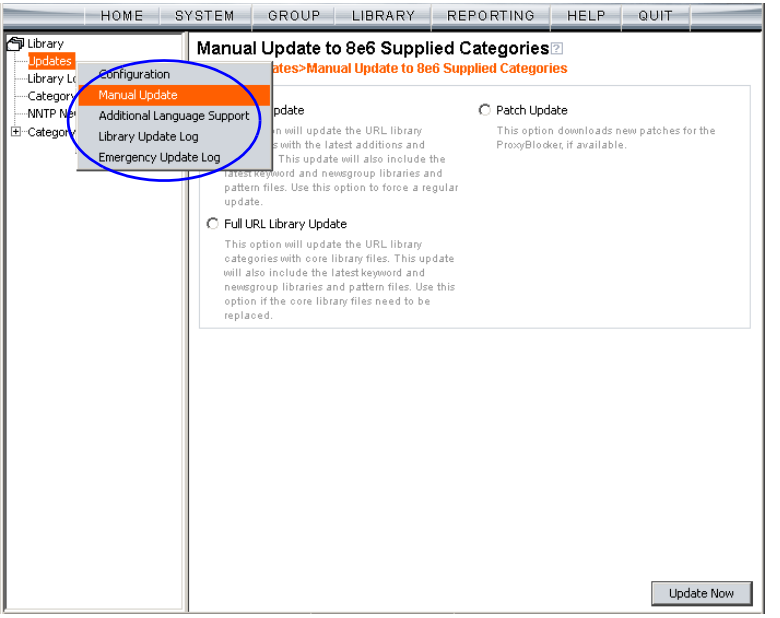


Fig. 1:3-10 Sub-topics menu

When a sub-topic from this menu is selected, the window for that sub-topic displays in the right panel of the screen.

Navigate a Tree List

Tree lists are included in the navigation panel of Group and Library screens.

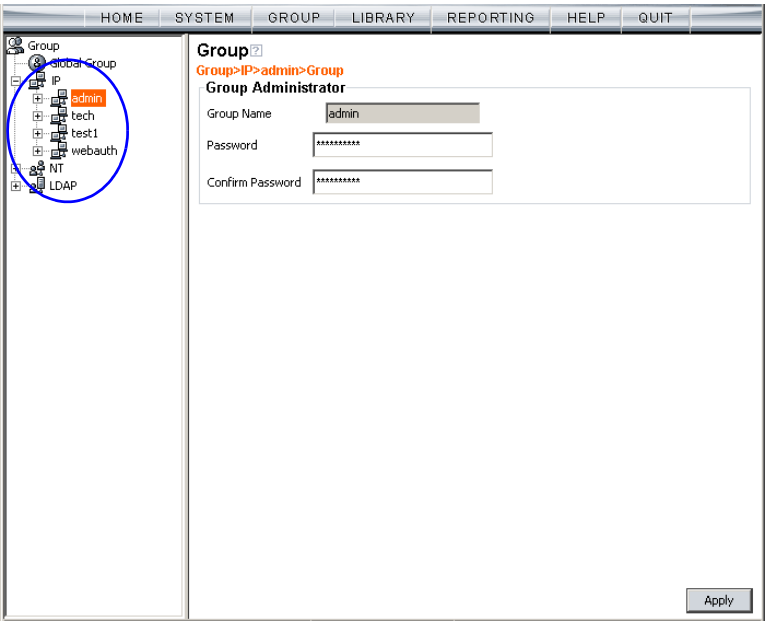


Fig. 1:3-11 Tree menu

A tree is comprised of a hierarchical list of items. An entity associated with a branch of the tree is preceded by a plus (+) sign, when that branch of the tree is collapsed.

By double-clicking the entity, a minus (-) sign replaces the plus sign, and all branches within that branch of the tree display.

An item in the tree is selected by clicking it.

Tree List Topics and Sub-topics

Group and Library tree lists possess a menu of topics and sub-topics.

Topics in the tree list display by default when the tree is opened. Examples of tree list topics are circled in Fig. 1:4-12.

When a tree list topic is selected and clicked, a menu of sub-topics opens:

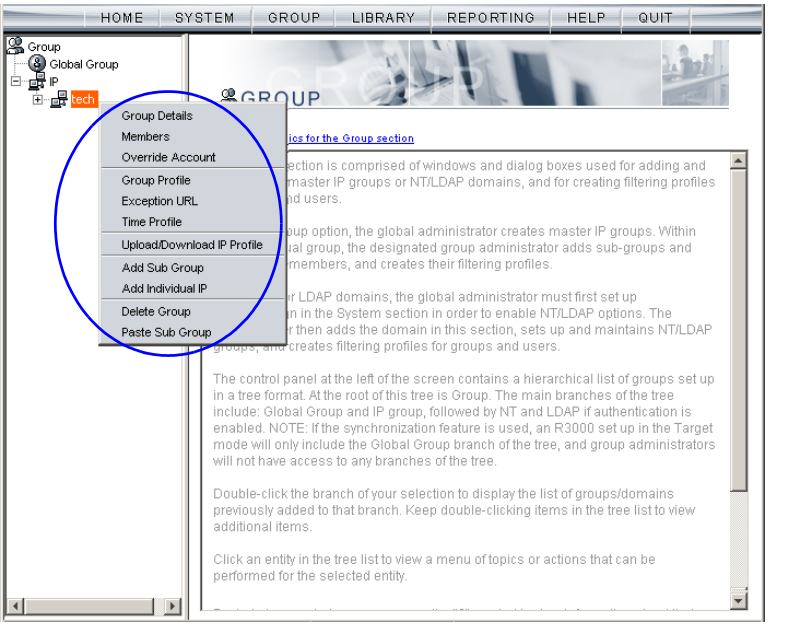


Fig. 1:3-12 Tree list topics and sub-topics

Clicking a sub-topic displays the corresponding window in the right panel, or opens a pop-up window or alert box, as appropriate.

Navigate a Window with Tabs

In each section of the console, there are windows with tabs.

When selecting a window with tabs from the navigation panel, the main tab for that window displays. Entries made in a tab must be saved on that tab, if the tab includes the Apply button.

***NOTE**: In the Time Profile and Override Account pop-up windows, entries are saved at the bottom of the window.*

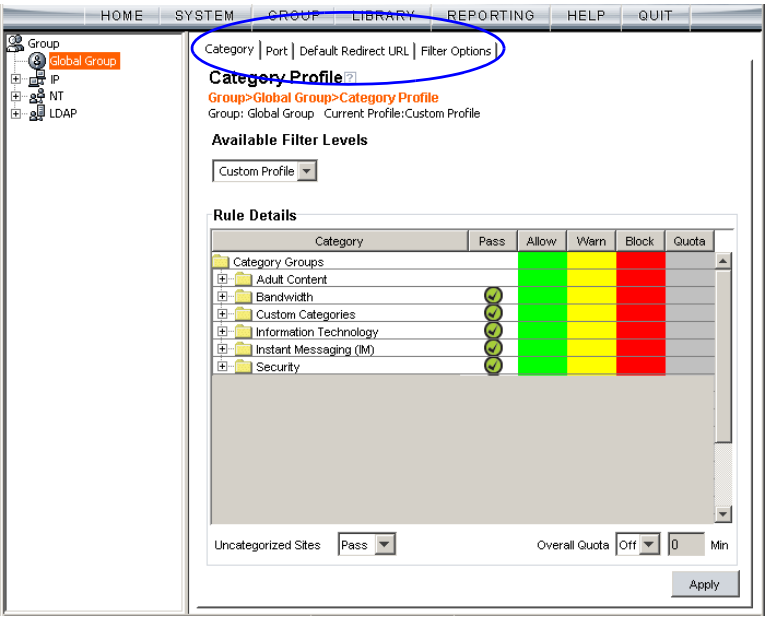


Fig. 1:3-13 Window with tabs

Console Tips and Shortcuts

The following list of tips and shortcuts is provided to help you use windows in the Administrator console with greater efficiency.

Navigation Path

The navigation path displays at the top of each window:

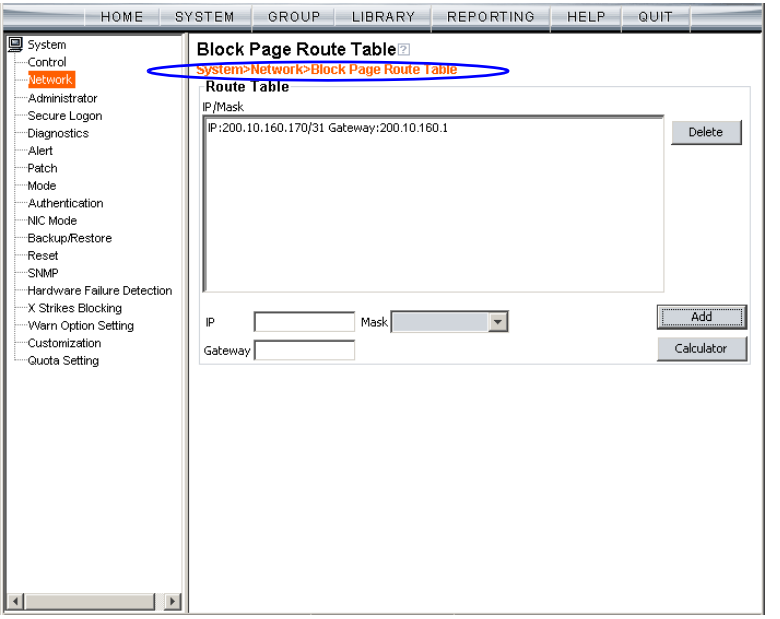


Fig. 1:3-14 Navigation path

This path reminds you of your location in the console. The entire path shows the screen name, followed by the topic name, and sub-topic name if applicable.

Refresh the Console

Press **F5** on your keyboard to refresh the Administrator console. This feature is useful in the event that more than one browser window is open simultaneously for the same ProxyBlocker server.

Select Multiple Items

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 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.

Copy and Paste Text

To save time when making duplicate data entries, text previously keyed into the GUI can be copied and pasted into other fields without needing to key in the same text again.

- **Copy command**

  Copy text by using the cursor to highlight text, and then pressing the **Ctrl** and **C** keys on the keyboard.

- **Paste command**

  Text that was just copied from a field can be pasted into another field that is either blank or populated with text.

- To paste text into an empty field, place the cursor in the field and then press the **Ctrl** and **V** keys.
- To copy over existing text, highlight text currently in the field and then press the **Ctrl** and **V** keys.

Calculate IP Ranges without Overlaps

The Calculator button displays on windows in which IP ranges are entered. These windows include: Block Page Route Table window from the System section, and Range to Detect and Members windows from the Group section.

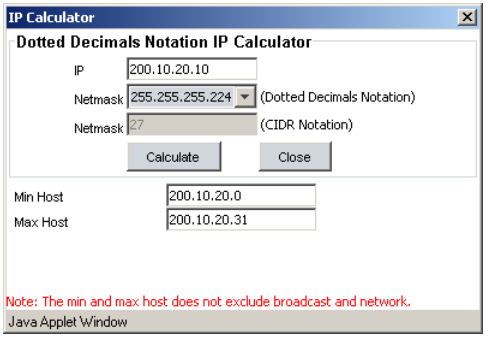


Fig. 1:3-15 IP Calculator pop-up window

This window is used to view and/or calculate the minimum and maximum range for an IP address.

1. Click **Calculator** to open the IP Calculator pop-up window.
   - If the IP address field in the window on the console is already populated, note the IP Calculator pop-up window displays the IP address, default Netmask in both the Dotted Decimals Notation (e.g. “255.255.255.248”) and CIDR Notation (e.g. “29”) format, Min Host, and Max Host IP addresses.

- If the IP address field in the window on the console is empty, in this pop-up window enter the **IP** address, specify the Dotted Decimals Notation **Netmask**, and then click **Calculate** to display the Min Host and Max Host IP addresses.

***TIP**: If necessary, make a different IP address entry and Netmask selection, and then click **Calculate** to display different Min Host and Max Host results.*

2. After making a note of the information in this pop-up window, click **Close** to close the IP Calculator.

Log Off

To log off the Administrator console:

1. Click the **Quit** button in the navigational panel at the top of the screen. This action opens the Quit dialog box:

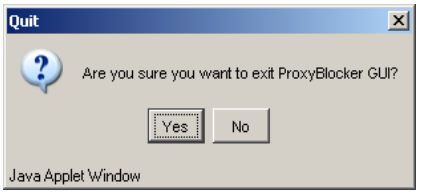


Fig. 1:3-16 Quit dialog box

2. Click **Yes** to close the Administrator console.
3. Click the "X" in the upper right corner of the ProxyBlocker Introductory Window to close it.

***WARNING:** If you need to turn off the server, see the ShutDown window of the System screen in the Global Administrator Section.*

GLOBAL ADMINISTRATOR SECTION

Introduction

The Global Administrator Section of this user guide is comprised of four chapters, based on the layout of the Administrator console. This section is used by the authorized global administrator of the ProxyBlocker for configuring and maintaining the ProxyBlocker server.

The global administrator is responsible for integrating the server into the existing network, and providing the server a high-speed connection to remote client workstations and to a reporting application, if pertinent. To attain this objective, the global administrator performs the following tasks:

- provides a suitable environment for the server, including:
  - Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) link to the current logging device
  - power connection protected by an Uninterruptible Power Supply (UPS)
  - high speed access to the server by authorized client workstations
- adds group administrators
- sets up administrators for receiving automatic alerts
- updates the server with software supplied by 8e6
- analyzes server statistics
- utilizes diagnostics for monitoring the server status to ensure optimum functioning of the server
- configures the server for authenticating users
- adds and maintains filtering categories
- adds and maintains filtering profiles of entities

Chapter 1: System screen

The System screen is comprised of windows used for configuring and maintaining the server to authenticate users, and to filter, log, or block specified Internet content for each user based on an applied filtering profile.

Fig. 2:1-1 System screen

A list of main topics displays in the navigation panel at the left of the screen. Main topics in this section include the following: Control settings, Network settings, Administrator account information, Secure Logon, Diagnostics, Alert contacts, Patch, operation Mode, Authentication settings (see the 8e6 ProxyBlocker Authentication User Guide for information about this topic), NIC Mode, Backup/Restore operations, Reset settings, SNMP, Hardware Failure Detection, X Strikes Blocking, Warn Option Setting, Customization, and Quota Setting.

Click your selection to choose a main topic from this list, or to view a menu of sub-topics, if applicable. When a topic or sub-topic is selected, the designated window for that topic or sub-topic displays in the right panel.

Control

Control includes options for controlling basic ProxyBlocker server functions. Click the Control link to view a menu of sub-topics: Filter, Block Page Authentication, ShutDown, and Reboot.

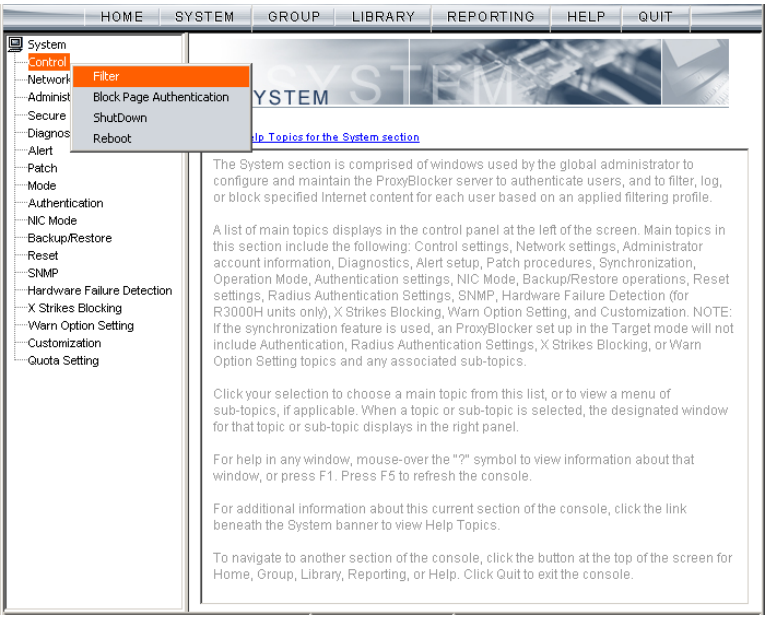


Fig. 2:1-2 System screen, Control menu

Filter window

The Filter window displays when Filter is selected from the Control menu. This window is used for specifying network filtering preferences on this server.

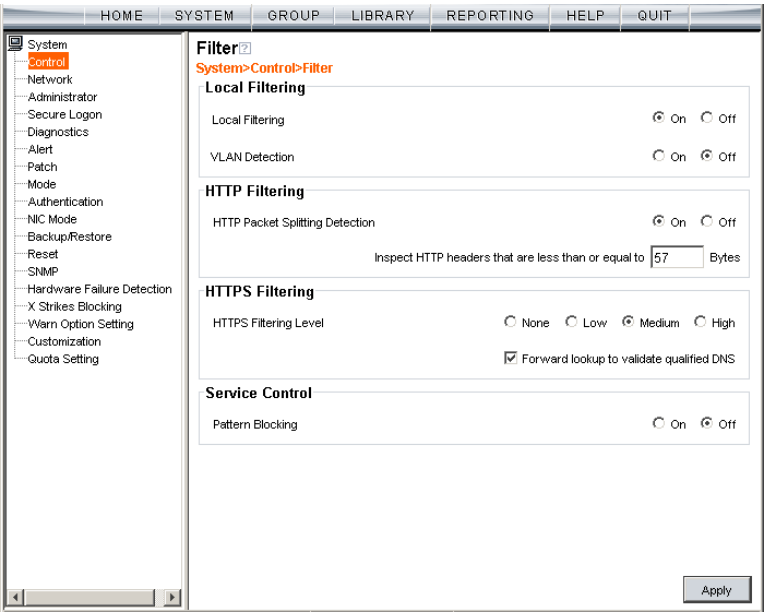


Fig. 2:1-3 Filter window

Local Filtering is used for specifying whether this server being configured will filter traffic on the network. If enabling the HTTP Filtering feature that automatically detects a split packet, HTTP headers less than or equal to the number of bytes specified will be inspected. HTTPS Filtering lets you set the level of filtering for HTTPS sites on ProxyBlockers set up in the Stand Alone or Source mode. In the Service Control frame, enabling Pattern Blocking will log IM and P2P end user activity, and block end users from using clients such as Google Web Accelerator and proxy patterns that bypass filtering (see **http://www.8e6.com/pbahelp/**

files/1system_proxy_block .html for a list of proxy pattern types set up to be blocked).

***TIP**: See the Introductory Section for overviews on IM and P2P (Chapter 2: Logging and Blocking).*

Local Filtering

In the Local Filtering frame, indicate the function of this server being configured, in regards to filtering the network. The default setting has **Local Filtering** "On" and **VLAN Detection** "Off".

Disable Local Filtering Options

If you have multiple ProxyBlocker servers on the network, you may wish to disable local filtering on the source server and use the server primarily for authenticating users who log on the network. This frees up resources on the server.

To disable **Local Filtering** and/or **VLAN Detection**, click the "Off" radio button(s).

Enable Local Filtering Options

To enable **Local Filtering**, click "On". The server will filter the specified Range to Detect on the network.

To enable the detection of VLAN traffic on the network, at **VLAN Detection**, click "On".

***NOTE**: After making all entries in this window, click **Apply**.*

HTTP Filtering

In the HTTP Filtering frame, enable or disable the feature that automatically detects a split HTTP packet.

Enable HTTP Packet Splitting Detection

By default, the feature that automatically detects a split HTTP packet is disabled.

1. Click “On” to enable **HTTP Packet Splitting Detection**; this action displays a field below the radio buttons.
2. In the **Inspect HTTP headers that are less than or equal to ___ Bytes** field, by default *48* displays for the number of bytes. This entry can be modified to specify a different number of bytes for HTTP header inspection.

Disable HTTP Packet Splitting Detection

To disable automatic detection of a split HTTP packet, click “Off.” This action removes the field below the radio buttons.

***NOTE**: After making all entries in this window, click **Apply**.*

HTTPS Filtering

Specify your preference for filtering HTTPS sites in the HTTPS Filtering frame. Select from the following settings for the **HTTPS Filtering Level**:

- "None" - if you do not want the ProxyBlocker to filter HTTPS sites
- "Low" - if you want the ProxyBlocker to filter HTTPS sites without having the ProxyBlocker communicate with IP addresses or hostnames of HTTPS servers
- "Medium" - if you want the ProxyBlocker to communicate with HTTPS servers in order to get the URL from the certificate for URL validation only (this is the default setting)

  If "Medium" is selected, by default the option is enabled for forwarding the DNS lookup in order to validate the hostname in the certificate
- "High" - if you want the ProxyBlocker to communicate with HTTPS servers to obtain the certificate with a very strict validation of the return URL

  If "High" is selected, by default the option is enabled for a library lookup to overrule the DNS validation of the hostname in the certificate.

***WARNING**: If using the "High" setting, end users may be blocked from accessing acceptable Web sites if the host names of these sites do not match their generated certificates. To allow users access to acceptable HTTPS sites, the IP addresses and corresponding URLs of these sites should be included in a custom library category that is allowed to pass. (See the Custom Categories sub-section in Chapter 3: Library screen for information on maintaining the ALLOW and PASS custom library categories. See Global Group Profile window and Minimum Filtering Level window in Chapter 2: Group screen from the Global Administrator Section for information on allowing a library category to pass.)*

***NOTE**: After making all entries in this window, click **Apply**.*

Service Control

In the Service Control frame, indicate whether or not Pattern Blocking with be enabled or disabled.

Enable Pattern Blocking

By default, **Pattern Blocking** is disabled. Click “On” to block the usage of clients such as Google Web Accelerator and various proxy pattern types on end user workstations that bypass filtering, and to log IM and P2P activity of end users once IM and P2P pattern files are downloaded on demand via the Manual Update to 8e6 Supplied Categories window.

***NOTE**: See **http://www.8e6.com/pbahelp/files/1system_proxy_block.html** for a list of proxy pattern types that are set up to be blocked.*

***TIPS**: To block specified users from accessing proxy patterns, the 8e6 supplied “PROXY” library category (Web-based Proxies/ Anonymizers) must be applied to the group or user's filtering profile. Or, to block all users from accessing these proxy patterns, the global filtering profile and minimum filtering level must have the “PROXY” library category set up to be blocked.*

To block specified users from accessing IM services, specified Instant Messaging 8e6 supplied library categories (such as “IMGEN”, “IMGCHAT”, “IMGTALK”, “ICQAIM”, “IMMSN”, “IMMYSP”, and/or “IMYAHOO”) must be applied to the group or user's filtering profile. Or, to block all users from accessing IM services, the global filtering profile and minimum filtering level must have appropriate Instant Messaging library categories set up to be blocked.

Additionally, to block specified users from accessing P2P services, the 8e6 supplied “PR2PR” library category must be applied to the group or user’s filtering profile. Or, to block all users from accessing P2P services, the global filtering profile and minimum filtering level must have the “PR2PR” library category set up to be blocked.

Disable Pattern Blocking

Click “Off” to disable **Pattern Blocking**.

***NOTE**: After making all entries in this window, click **Apply**.*

Block Page Authentication window

The Block Page Authentication window displays when Block Page Authentication is selected from the Control menu. This feature is used for entering criteria the ProxyBlocker server will use when validating a user's account. Information entered/selected in this window is used by the block page that displays when an end user attempts to access a site or service that is set up to be blocked.

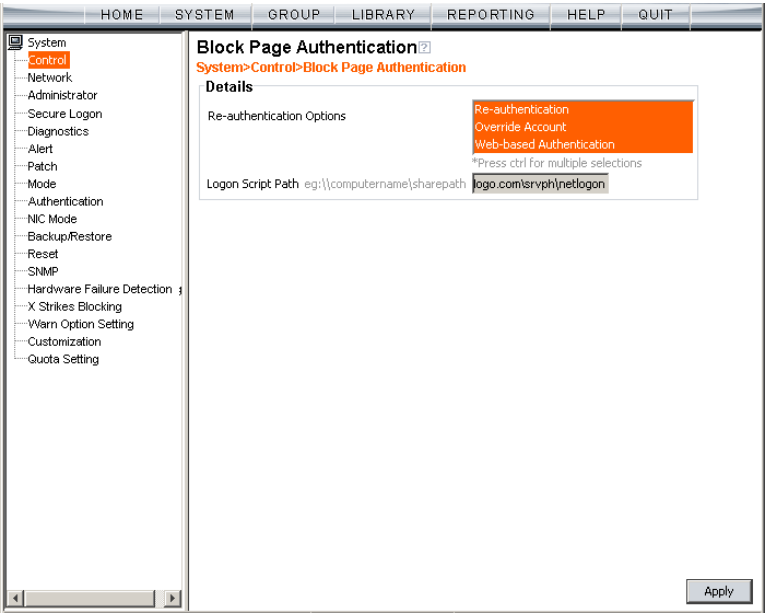


Fig. 2:1-4 Block Page Authentication window

***NOTE**: See the Block Page Customization window and Common Customization window in this chapter for information on customizing the 8e6 block page. See Appendix C: Create a Custom Block Page for information on creating a customized block page using your own design.*

Enter, Edit Block Page Options

***NOTE**: If you are not using authentication, and/or if your users do not have override accounts set up, you do not need to select any option at the Re-authentication Options field.*

1. In the **Re-authentication Options** field of the Details frame, all block page options are selected by default, except for Web-based Authentication. Choose from the following options by clicking your selection:
   - **Web-based Authentication** - select this option if using Web authentication with time-based profiles or persistent login connections for NT or LDAP authentication methods.
   - **Re-authentication** - select this option for the re-authentication option. The user can restore his/her profile and NET USE connection by clicking an icon in a window to run a NET USE script.
   - **Override Account** - select this option if any user has an Override Account, allowing him/her to access URLs set up to be blocked at the global or IP group level.

***NOTE**: Details about the Web-based Authentication option can be found in the 8e6 ProxyBlocker Authentication User Guide.*

***TIP**: Multiple options can be selected by clicking each option while pressing the Ctrl key on your keyboard.*

***NOTE**: For more information about the Override Account option, see information on the following windows in this user guide:*

- *Global Administrator Section: Override Account window and Bypass Option window for the global group*
- *Group Administrator Section: Override Account window for IP groups, and Exception URL window for IP groups.*

2. If the Re-authentication option was selected, in the **Logon Script Path** field, *PDCSHARE**scripts* displays by default. In this field, enter the path of the logon script that the ProxyBlocker will use when re-authenticating users on the network, in the event that a user's machine loses its connection with the server, or if the server is rebooted. This format requires the entry of two back-slashes, the authentication server's computer name (or computer IP address) in capital letters, a backslash, and name of the share path.
3. Click **Apply** to apply your settings.

Block page

When a user attempts to access Internet content set up to be blocked, the block page displays on the user's screen:

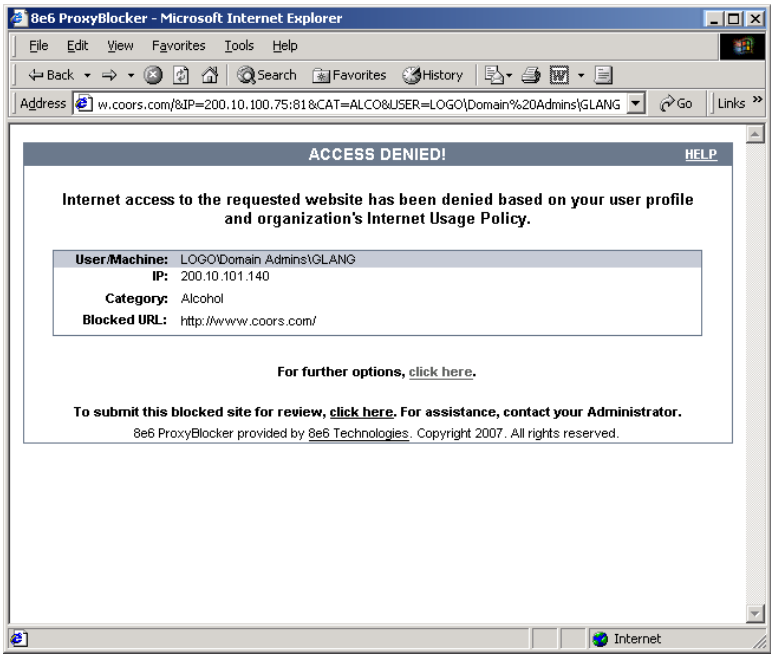


Fig. 2:1-5 Sample Block Page

By default, the following data displays in the User/Machine frame of the block page:

- **User/Machine** field - The username displays for the NT/LDAP user. This field is blank for the IP group user.
- **IP** field - The user's IP address displays.
- **Category** field - The name of the library category that blocked the user's access to the URL displays. If the content the user attempted to access is blocked by an Exception URL, "Exception" displays instead of the library category name.

- **Blocked URL** field - The URL the user attempted to access displays.

By default, the following standard links are included in the block page:

- **HELP** - Clicking this link takes the user to 8e6's Technical Support page that explains why access to the site or service may have been denied.
- **8e6 Technologies** - Clicking this link takes the user to 8e6's Web site.

By default, these links are included in the block page under the following conditions:

- **For further options, click here.** - This phrase and link is included if any option was selected at the Re-authentication Options field. Clicking this link takes the user to the Options window, described in the Options page subsection that follows.
- **To submit this blocked site for review, click here.** - This phrase and link is included if an email address was entered in the Submission Email Address field in the Common Customization window. Clicking this link launches the user's default email client. In the composition window, the email address from the Submission Email Address field populates the "To" field. The user's message is submitted to the global administrator.

Options page

The Options page displays when the user clicks the following link in the block page: **For further options, click here.**

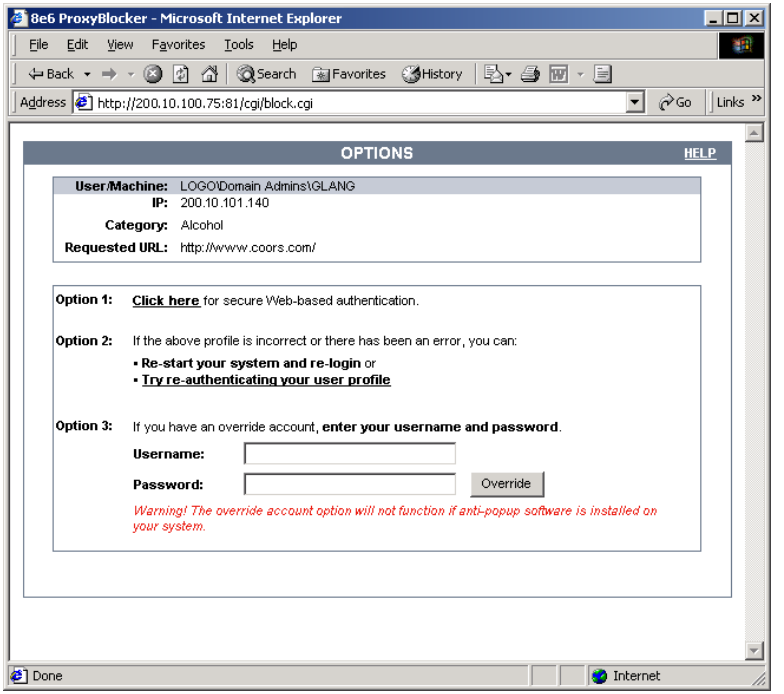


Fig. 2:1-6 Options page

The following items previously described for the Block page display in the upper half of the Options page:

- **HELP** link
- User/Machine frame contents

The frame beneath the User/Machine frame includes information for options (1, 2, and/or 3) based on settings made in this window and the Common Customization window.

***NOTE**: Information about Option 1 is included in the 8e6 Proxy-Blocker Authentication User Guide.*

Option 2

The following phrase/link displays, based on options selected at the Re-authentication Options field:

- **Re-start your system and re-login** - This phrase displays for Option 2, whether or not either of the other Re-authentication Options (Re-authentication, or Web-based Authentication) was selected. If the user believes he/she was incorrectly blocked from a specified site or service, he/she should re-start his/her machine and log back in.
- **Try re-authenticating your user profile** - This link displays if "Re-authentication" was selected at the Re-authentication Options field, and an entry was made in the Logon Script Path field. When the user clicks this link, a window opens:

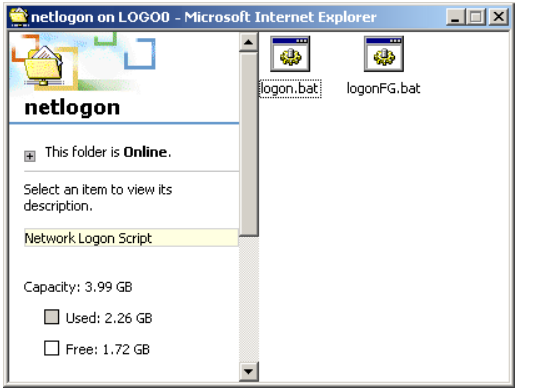


Fig. 2:1-7 Re-authentication option

The user should click the **logon.bat** icon to run a script that will re-authenticate his/her profile on the network.

Option 3

Option 3 is included in the Options page, if “Override Account” was selected at the Re-authentication Options field.

This option is used by any user who has an override account set up for him/her by the global group administrator or the group administrator. An override account allows the user to access Internet content blocked at the global or IP group level.

The user should enter his/her **Username** and **Password**, and then click **Override** to open the Profile Control pop-up window:

Fig. 2:1-8 Profile Control pop-up window

This pop-up window must be left open throughout the user’s session in order for the user to be able to access blocked Internet content.

***NOTES**: See Profile Control window for information on customizing the content in the Profile Control pop-up window. See Appendix D: Override Pop-up Blockers for information on how a user with an override account can authenticate if a pop-up blocker is installed on his/her workstation.*

ShutDown window

The ShutDown window displays when ShutDown is selected from the Control menu. This window is used for powering off the server.

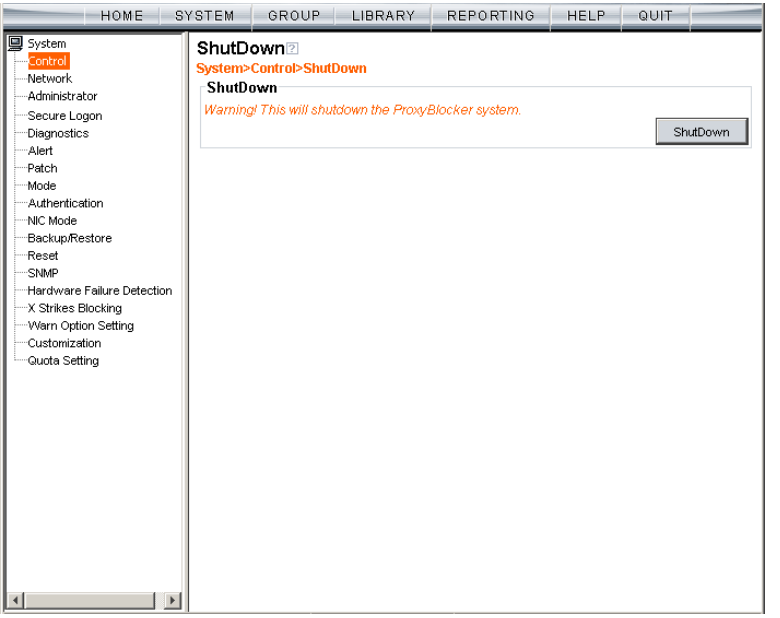


Fig. 2:1-9 ShutDown window

Shut Down the Server

In the ShutDown frame, click **ShutDown** to power off the server. To restart the server, the ProxyBlocker console needs to be re-accessed.

Reboot window

The Reboot window displays when Reboot is selected from the Control menu. This window is used for reconnecting the server on the network.

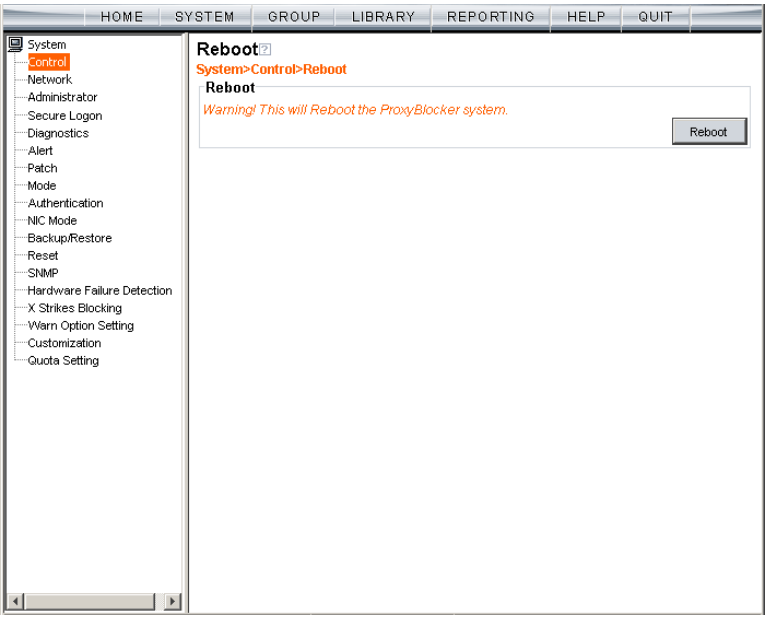


Fig. 2:1-10 Reboot window

Reboot the Server

1. In the Reboot frame, click **Reboot** to open the Reboot ProxyBlocker Enterprise Filter dialog box:

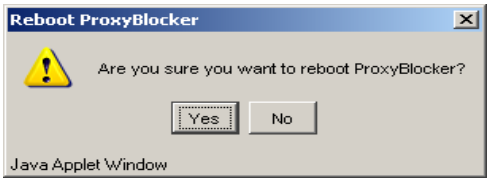


Fig. 2:1-11 Reboot ProxyBlocker dialog box

2. Click **Yes** to close the dialog box and to launch the Server Status message box, informing you that the server is now disconnected:

Fig. 2:1-12 Server Status: disconnect message

When the Server Status box closes, the ProxyBlocker status message box opens and informs you that the server is rebooting itself, and how much time has elapsed since this process began:

Fig. 2:1-13 ProxyBlocker status message box

After the server is rebooted, the ProxyBlocker status message box closes, and the ProxyBlocker ready alert box opens:

Fig. 2:1-14 ProxyBlocker ready alert box

The Server connected alert box also opens, informing you that the server is connected, and that you must restart the server:

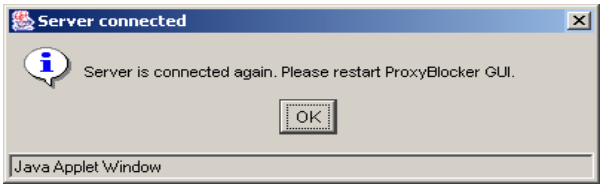


Fig. 2:1-15 Server connected alert box

3. Click **OK** to close the ProxyBlocker ready alert box.
4. Click **OK** to close the Server connected alert box.
5. You must now re-access the ProxyBlocker console.

Network

Network includes options for configuring the ProxyBlocker server on the network. Click the Network link to view a menu of sub-topics: LAN Settings, NTP Servers, Regional Setting, and Block Page Route Table.

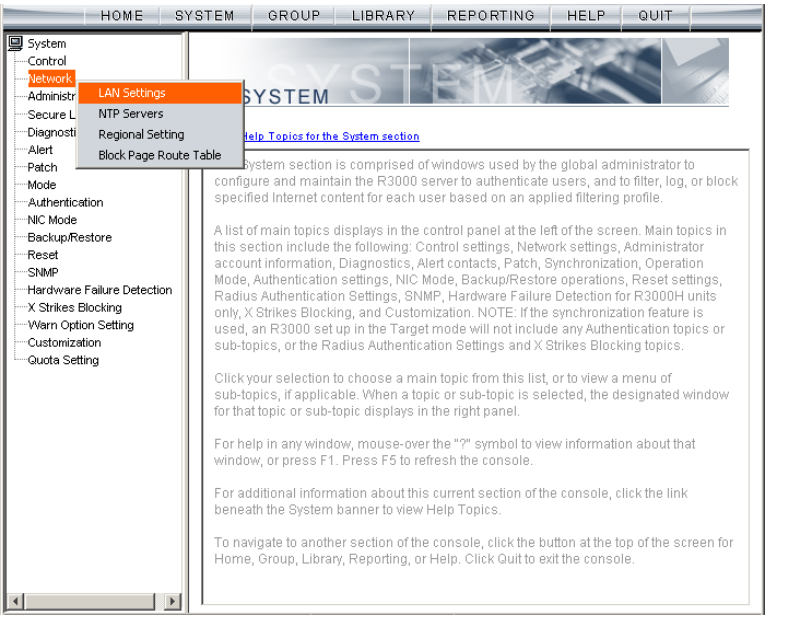


Fig. 2:1-16 System screen, Network menu

LAN Settings window

The LAN Settings window displays when LAN Settings is selected from the Network menu. This window is used for configuring network connection settings for the Proxy-Blocker.

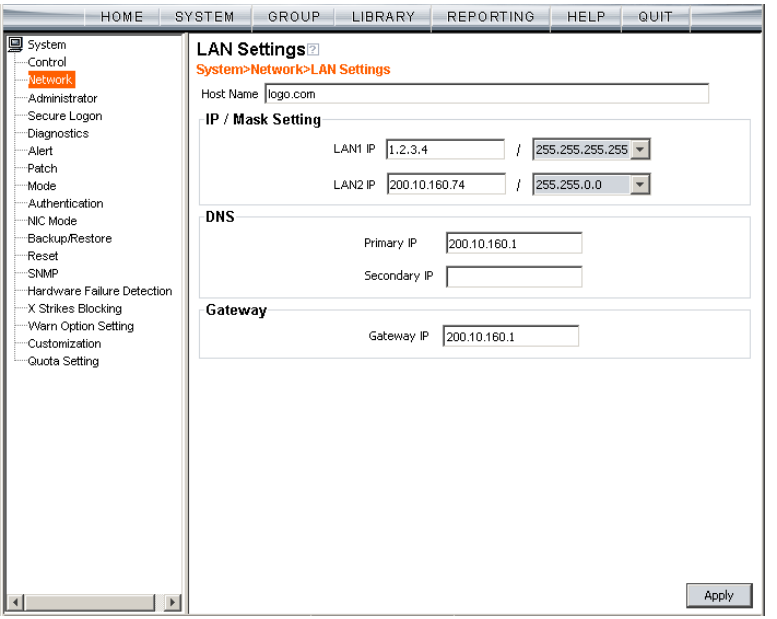


Fig. 2:1-17 LAN Settings window

Specify LAN Settings

1. In the **Host Name** field, enter up to 50 alphanumeric characters for the name of the host for this server, such as **pba.LOGO.com**.
2. Specify the following information, as necessary:
   - In the **LAN1 IP** field of the IP/Mask Setting frame, the default LAN 1 IP address is *1.2.3.3*. Enter the IP address and select the corresponding subnet mask of the LAN1 network interface card to be used on the network.
   - In the **LAN2 IP** field, the default LAN 2 IP address is *1.2.3.4*. Enter the IP address and select the corresponding subnet mask of the LAN2 network interface card to be used on the network.

***TIP**: Be sure to place the LAN1 and LAN2 IP addresses in different subnets.*

   - In the **Primary IP** field of the DNS frame, the default IP address is *4.2.2.1*. Enter the IP address of the first DNS server to be used for resolving the IP address of the authentication server with the machine name of that server.
   - In the **Secondary IP** field of the DNS frame, the default IP address is *4.2.2.2*. Enter the IP address of the second DNS server to be used for resolving the IP address of the authentication server with the machine name of that server.
   - In the **Gateway IP** field of the Gateway frame, the default IP address is *1.2.3.1*. Enter the IP address of the default router to be used for the entire network segment.
3. Click **Apply** to apply your settings.

***NOTE**: Whenever modifications are made in this window, the server must be restarted in order for the changes to take effect.*

NTP Servers window

The NTP Servers window displays when NTP Servers is selected from the Network menu. This window is used for specifying IP addresses of servers running Network Time Protocol (NTP) software. NTP is a time synchronization system for computer clocks throughout the Internet. The ProxyBlocker will use the actual time from a clock at a specified IP address.

***NOTE**: The System Time displays beneath the Details frame, using the YYYY/MM/DD HH:MM:SS Coordinated Universal Time (UTC) format for the current time zone.*

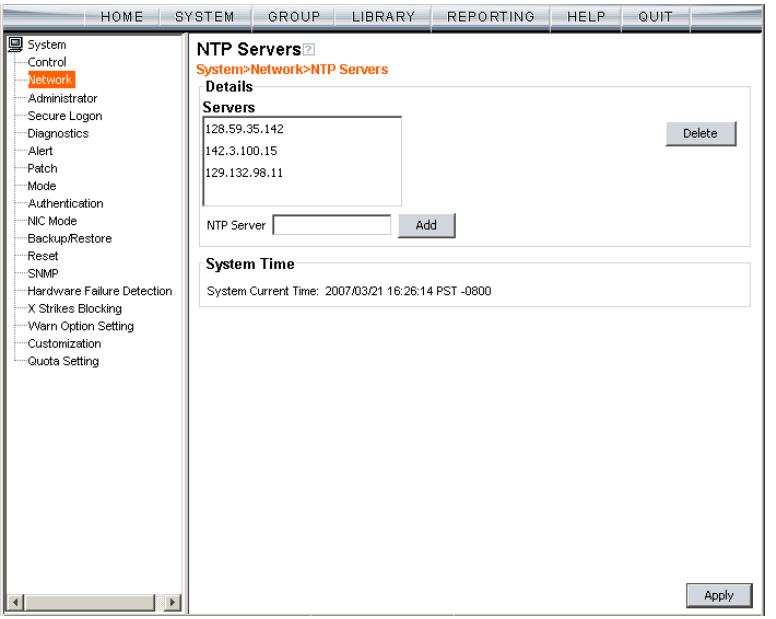


Fig. 2:1-18 NTP Servers window

Specify Network Time Protocol Servers

In the Details frame, three NTP server IP addresses display by default in the Servers list box. These IP addresses are: *128.59.35.142*, *142.3.100.15*, and *129.132.98.11*.

***NOTE**: Any IP address following the first entry in the Servers list box is only used in the event that the ProxyBlocker cannot access the primary time NTP server specified. IP addresses are used in the order in which they display in the list box.*

Add an NTP Server

To add an NTP server:

1. Enter the IP address in the **NTP Server** field.
2. Click **Add** to include this IP address in the Servers list box.
3. Click **Apply** to apply your settings.

Remove an NTP Server

To remove an NTP server:

1. Select the IP address from the Servers list box.
2. Click **Delete**.
3. Click **Apply** to apply your settings.

***WARNING**: If using the ProxyBlocker with the 8e6 Technologies Enterprise Reporter unit, be sure the ER unit is connected to the same NTP servers as the ProxyBlocker.*

Regional Setting window

The Regional Setting window displays when Regional Setting is selected from the Network menu. This window is used for specifying the time zone to be used by the Proxy-Blocker and the language set type, if necessary.

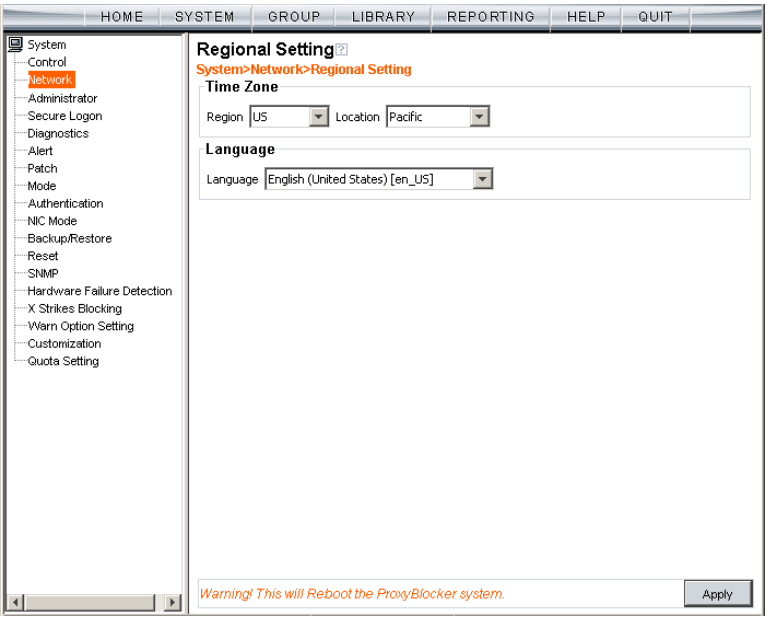


Fig. 2:1-19 Regional Setting window

Specify the Time Zone, Language Set

In the Details frame, the Region “US” and the Location “Pacific” display by default. To change these settings:

1. At the **Region** pull-down menu, select your country from the available choices.
2. At the **Location** pull-down menu, select the time zone for the specified region.

   If necessary, select a language set from the **Language** pull-down menu to specify that you wish to display that text in the console.
3. Click **Apply** to apply your settings, and to reboot the ProxyBlocker.

***WARNING**: If using the ProxyBlocker with an 8e6 Technologies Enterprise Reporter unit, be sure each ProxyBlocker used by the ER is set up in the same time zone as the ER. These “like” settings ensure consistency when tracking the logging times of all users on the network.*

Block Page Route Table window

The Block Page Route Table window displays when Block Page Route Table is selected from the Network menu. This window is used for building and maintaining a list of destination based routers the server will use for communicating with other segments of the network. You need to set up a route table only if your local network is interconnected with another network, and if users' client machines are not being served block pages when appropriate.

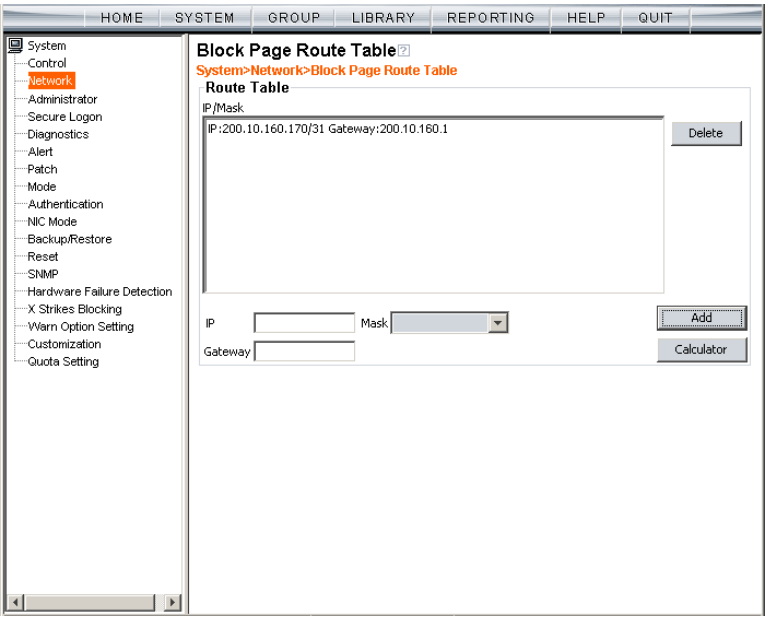


Fig. 2:1-20 Block Page Route Table window

***NOTE**: See the Block Page Authentication window for information on setting up block pages.*

Add a Router

In the Route Table frame:

1. Enter the **IP** address.
2. Select the network subnet **Mask** from the pull-down menu.
3. In the **Gateway** field, enter the IP address of the portal to which packets will be transferred to and from the Internet.

***TIP**: Click **Calculator** to open the IP Calculator pop-up window. Use this calculator to calculate IP ranges without any overlaps.*

4. Click **Add** to include your entries in the IP/Mask list box.

***NOTE**: Follow steps 1-4 for each router you wish to include in the routing table.*

Remove a Router

To remove one or more routers from the IP/Mask list box:

1. Select the router(s) from the list box.
2. Click **Delete**.

Administrator

Administrator window

The Administrator window displays when Administrator is selected from the navigation panel. This window is used for adding and maintaining global administrator (Admin) and group administrator (Sub Admin) accounts. A Sub Admin manages NT or LDAP entities and their filtering profiles.

***NOTE**: See the Group Details window in Chapter 1: Group screen of the Group Administrator Section for information on setting up and maintaining accounts for IP group administrators. See the 8e6 ProxyBlocker Authentication User Guide for more information on setting up and maintaining NT and LDAP Sub Admin group administrator accounts.*

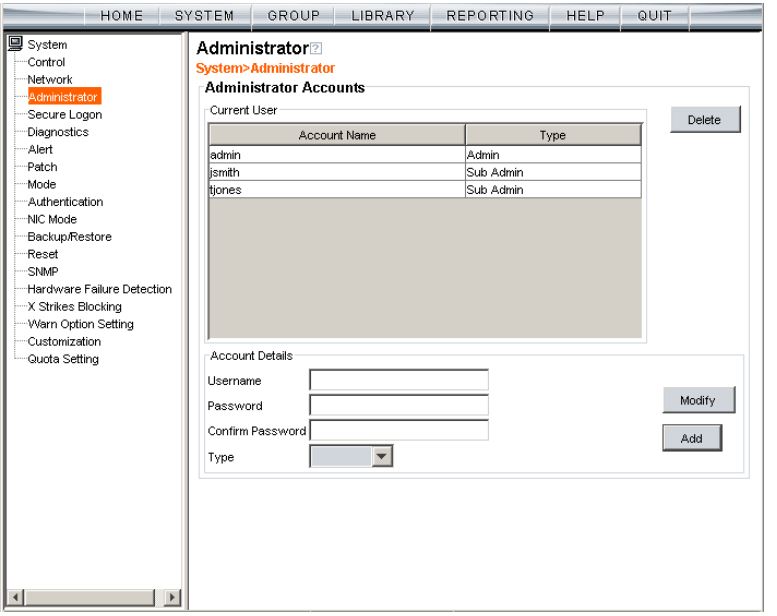


Fig. 2:1-21 Administrator window

***TIP**: The default Username is **admin** and the Password is **user3**. 8e6 recommends that you retain this default account and password in the event that the ProxyBlocker unit cannot be accessed. An authorized 8e6 Technologies technical representative may need to use this username and password when troubleshooting the unit.*

***WARNING**: Always be sure that at least one account is listed in this window at all times.*

View Administrator Accounts

The Current User list box includes the Account Name and corresponding account Type (“Admin” or “Sub Admin”) for each active global administrator or NT/LDAP group administrator previously set up in this window.

Add an Administrator Account

To add a global or NT/LDAP group administrator account:

1. In the Account Details frame, enter the username in the **Username** field.
2. In the **Password** field, enter eight to 20 characters—including at least one alpha character, one numeric character, and one special character. The password is case sensitive.
3. Make the same entry again in the **Confirm Password** field.
4. Select “Admin” or “Sub Admin” from the **Type** pull-down menu.
5. Click **Add** to include the username and account type in the Current User list box.

Edit an Administrator Account

To change an administrator's password and/or account type:

1. Select the username from the Current User list box; this action populates the Account Details frame with data.
2. In the **Password** field, enter eight to 20 characters for a new password—including at least one alpha character, one numeric character, and one special character. The password is case sensitive.
3. Enter the same new password again in the **Confirm Password** field.

   If the administrator's account type needs to be changed, select the appropriate account type from the **Type** pull-down menu ("Admin" for global administrator or "Sub Admin" for NT/LDAP group administrator).
4. Click **Modify** to apply your settings.

***NOTE**: A username cannot be modified, but can be deleted and added again.*

Delete an Administrator Account

To delete an administrator account:

1. Select the username from the Current User list box.
2. Click **Delete** to remove the account.

Secure Logon

Secure Logon includes options for setting user passwords to expire after a designated number of days, and/or locking out users from the ProxyBlocker after unsuccessfully attempting to log in for the specified number of attempts within the defined timespan. Click the Secure Logon link to view a menu of sub-topics: Logon Settings, and Logon Management.

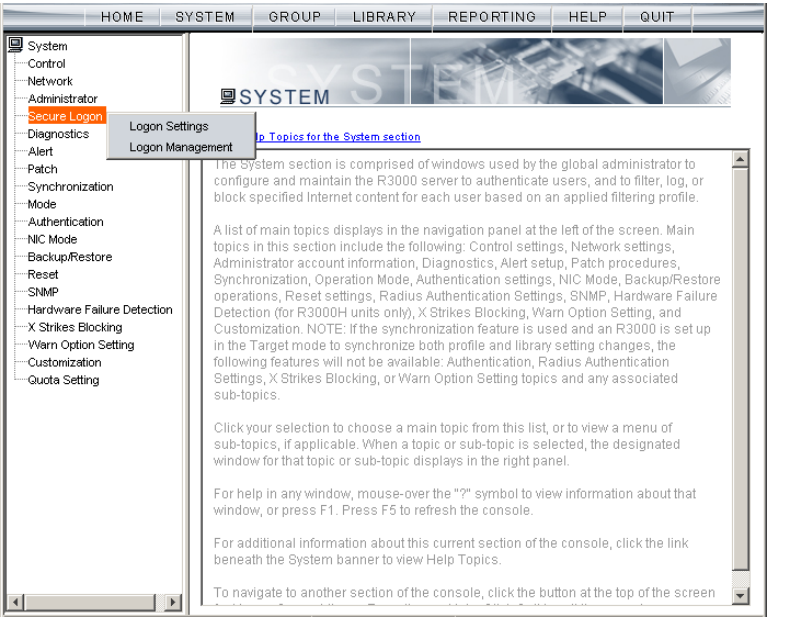


Fig. 2:1-22 System screen, Secure Logon window

Logon Settings window

The Logon Settings window displays when Logon Settings is selected from the Secure Logon menu. This window is used for enabling the password expiration feature that lets you define the number of days a password will be valid before a new password must be used. This window also lets you enable the feature for locking out a user from the interface by username and/or IP address if an incorrect password is entered for a specified number of times within a defined timespan.

***NOTE**: This window displays only on servers set up in the Standalone or Source mode.*

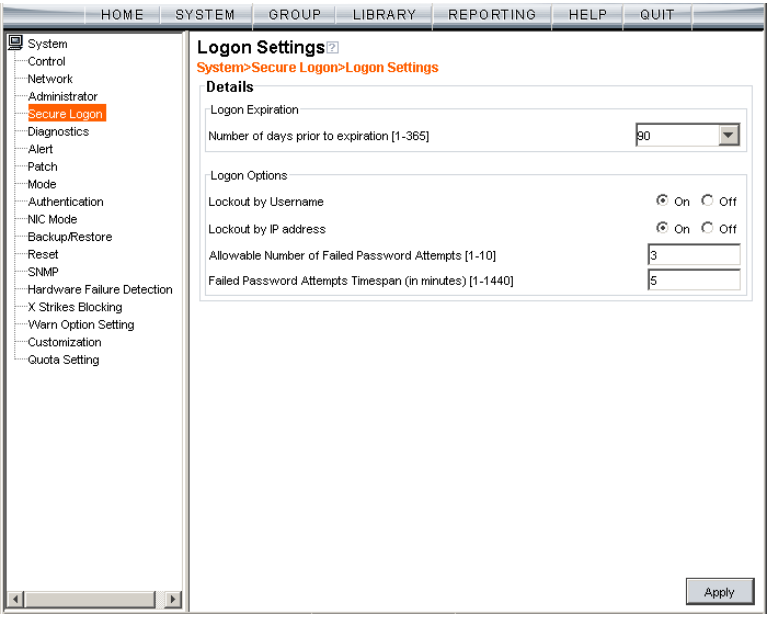


Fig. 2:1-23 Logon Settings window

Enable, Disable Password Expiration

In the Logon Expiration frame, at the **Number of days prior to expiration [1-365]** field, specify the number of days logon passwords will be effective by doing one of the following:

- select from available choices (1, 30, 90, 365, Never Expired)
- make an entry for the number of days until passwords expire.

***NOTE**: If a user's password has expired, when he/she enters his/her username and password in the Login dialog box and clicks OK, a different login dialog box opens:*

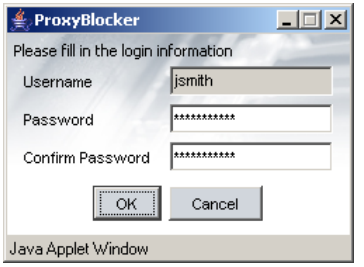


Fig. 2:1-24 New password entry

This dialog box displays his/her Username and prompts him/her to enter a new password in the Password and Confirm Password fields. Upon clicking OK, the ProxyBlocker interface opens.

Enable, Disable Account Lockout

1. In the Logon Options frame, enable any of the following options:
   - At the **Lockout by Username** field, click the radio button corresponding to either of the following options:
     - **On** - Choose this option to lock out the user by username if the incorrect password is entered—for the number of times specified in the Allowable Number of Failed Password Attempts [1-10] field—within the interval defined in the Failed Password Attempts Timespan (in minutes) [1-1440] field.
     - **Off** - Choose this option if the user will not be locked out by username after entering the incorrect password.
   - At the **Lockout by IP address** field, click the radio button corresponding to either of the following options:
     - **On** - Choose this option to lock out the user by IP address if the incorrect password is entered—for the number of times specified in the Allowable Number of Failed Password Attempts [1-10] field—within the interval defined in the Failed Password Attempts Timespan (in minutes) [1-1440] field.
     - **Off** - Choose this option if the user will not be locked out by IP address after entering the incorrect password.
   - At the **Allowable Number of Failed Password Attempts [1-10]** field—with the Lockout by Username and/or Lockout by IP address option(s) enabled—enter the number of times a user can enter an incorrect password during the interval defined in the Failed Password Attempts Timespan (in minutes) [1-1440] field before being locked out of the ProxyBlocker.

- At the **Failed Password Attempts Timespan (in minutes) [1-1440]** field—with the Lockout by Username and/or Lockout by IP address option(s) enabled—enter the number of minutes that defines the interval in which a user can enter an incorrect password—as specified in the Allowable Number of Failed Password Attempts [1-10] field—before being locked out of the ProxyBlocker.

***NOTE**: If the number of failed attempts is 3 and the number of minutes in the timespan is 10, if any user (one or more) enters an incorrect password for that same username within the 10-minute timespan, a lockout would be made for that username on the third unsuccessful attempt. However, if the third failed login attempt is made outside of the 10-minute timespan, there would be no lock out for that username. In a similar scenario for an IP address (using the same timespan and designated number of failed login attempts), if any user (one or more) enters an incorrect password for any username (one or more) using that same machine, a lockout would be made for that machine's IP address on the third unsuccessful login attempt. But there would be no lockout for that IP address if the third failed attempt was made outside of the 10-minute timespan.*

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

Logon Management

The Logon Management window displays when Logon Management is selected from the Secure Logon menu. This window is used for viewing the status of user accounts—including the date passwords will expire, and which user-names/IP addresses are currently locked out of the Proxy-Blocker interface—and for unlocking usernames and IPs currently locked out of the ProxyBlocker. If the user account is a global (Admin) or NT/LDAP group administrator (Sub Admin) account, the areas of interface accessible to that administrator can be viewed.

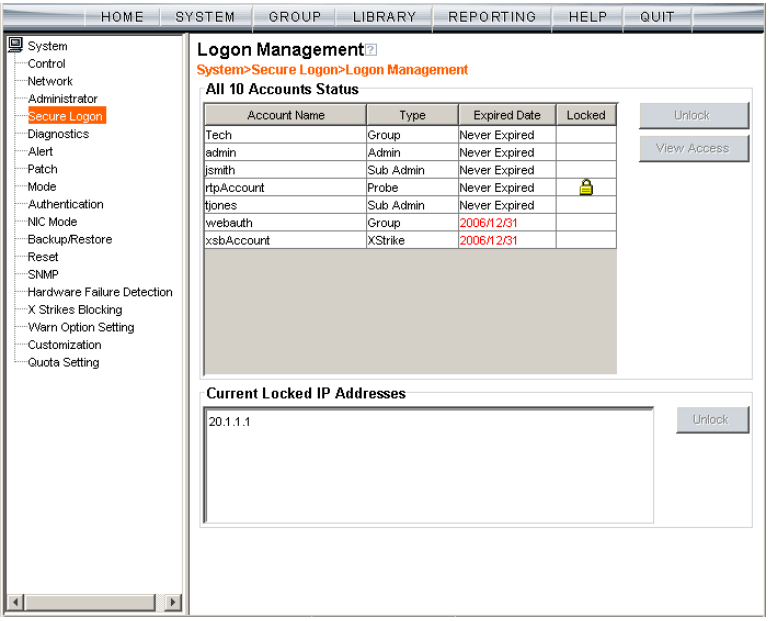


Fig. 2:1-25 Logon Management window

***NOTE**: An account/IP address becomes locked if the Lockout by Username/IP address feature is enabled in the Logon Settings window, and a user is unable to log into the Administrator console due to a password expiration, or having met the specified number of failed password attempts within the designated timespan.*

View User Account Status, Unlock Username

View Account Status

The All Accounts Status frame displays password statuses of current login accounts set up in this ProxyBlocker being configured, including:

- Account Name - username
- Type of account:
  - Admin - global administrator account set up in the Administrator window
  - Sub Admin - NT/LDAP group administrator account set up in the Administrator window
  - Group - IP group administrator account set up in the IP branch of the Group tree
  - Probe - Real Time Probe account set up in the Real Time Probes Logon Accounts window
  - XStrike - X Strikes Blocking account set up in the X Strikes Blocking Logon Accounts window
- Expired Date (either Never Expired or a date using the YYYY-MM-DD format, based on the configuration in the Logon Settings window at the time the password was saved in that window)
- lock symbol if the account is currently locked.

***TIP**: This list can be resorted by clicking a specified column header.*

Unlock a Username

To unlock a username:

1. Select the Account Name from the All Accounts Status frame by clicking on it to highlight it.
2. Click **Unlock** to open the dialog box asking if you wish to proceed with this action.

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

3. Click **Yes** to display the alert box indicating the account was unlocked.
4. Click **OK** to close the alert box, and to remove the locked symbol from the Locked column for the row corresponding to the username.

View Locked IP Address, Unlock IP Address

View Locked IPs

The Current Locked IP Addresses frame displays any IP address currently locked.

Unlock an IP Address

To unlock the IP address of a machine:

1. In the Current Locked IP Addresses frame, click the IP address to highlight it.
2. Click **Unlock** to open the dialog box, asking if you wish to unlock the IP address.

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

3. Click **Yes** to display the alert box indicating the IP address was unlocked.
4. Click **OK** to close the alert box, and to remove the IP address from the list.

View Admin, Sub Admin Interface Access

To view the areas of the interface accessible by a global or NT/LDAP group administrator:

1. Select the Admin or Sub Admin username from the list.
2. Click **View Access** to open the Assign Access View pop-up window:

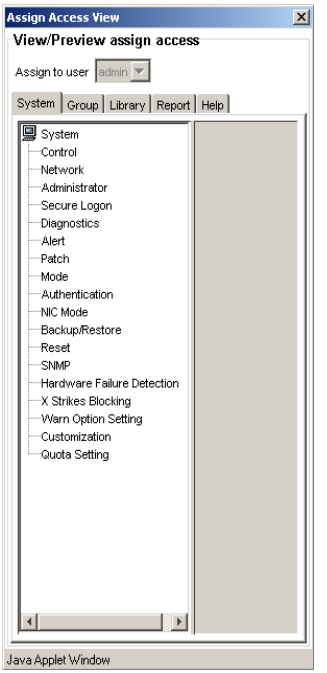


Fig. 2:1-26 Assign Access View

3. The View/Preview assign access frame displays the username in the greyed-out “Assign to user” field.

   Click any of the available tabs (System, Group, Library, Report, Help) to view menu topics, sub-topics, and branches of trees available to that administrator.

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

Diagnostics

Diagnostics includes options for setting up or running processes for maintaining the server. Click the Diagnostics link to view a menu of sub-topics: System Command, View Log File, Troubleshooting Mode, Active Profile Lookup, and Admin Audit Trail.

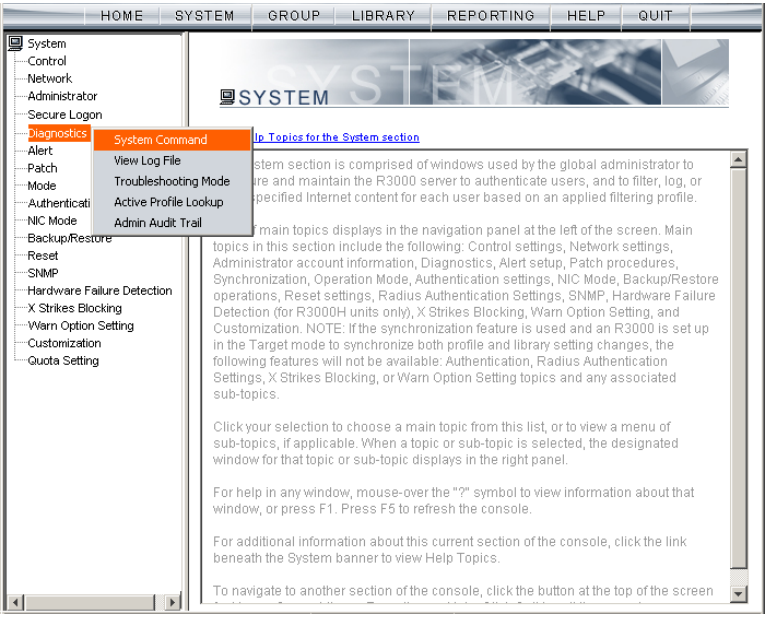


Fig. 2:1-27 System screen, Diagnostics menu

System Command window

The System Command window displays when System Command is selected from the Diagnostics menu. This window is used for viewing server statistics and for performing diagnostic tests on the server.

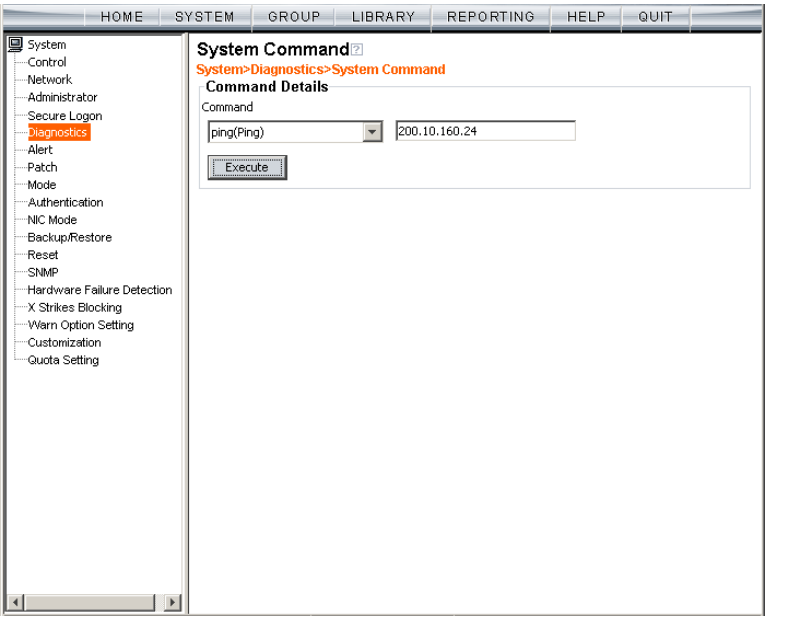


Fig. 2:1-28 System Command window

WARNING: *Diagnostics tools utilize system resources, impacting the ProxyBlocker's performance.*

Perform a Diagnostic Test, View Data

1. Select a diagnostic tool from the **Command** pull-down menu: ping(Ping), traceroute(Trace Route), ps(Process list), top(TOP CPU processes), ifconfig(NIC configuration), netstat(active connections), netstat(routing table), free(current memory usage), iostat(CPU usage), sar(system performance), recent logins, uptime(system uptime), df(disk usage), and dmesg(print kernel ring buffer).

***NOTE**: See Command Selections for a list of commands and their functions.*

   If “Ping” or “Trace Route” was selected from the pull-down menu, a blank field displays to the right and must be populated.

2. Click **Execute** to open a pop-up window containing the query results:

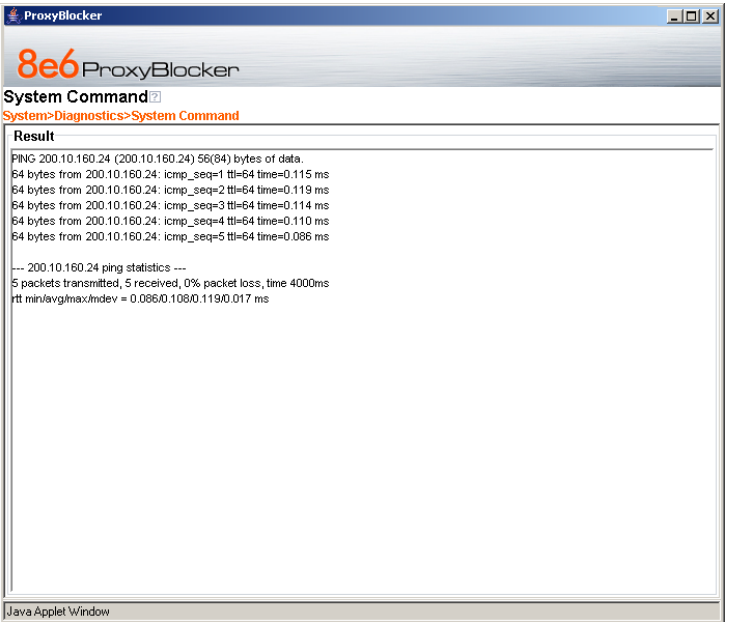


Fig. 2:1-29 System Command, Results window

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

Command Selections

Ping

The Ping diagnostic tool is used for verifying whether the ProxyBlocker can communicate with a machine at a given IP address within the network, and the speed of the network connection. Enter the IP address or host name of the specific Internet address to be contacted (pinged), and then click **Execute** to display results in the pop-up window.

Trace Route

The Trace Route diagnostic tool should be used if the ping utility was not able to help you diagnose the problem with your network configuration. This diagnostic tool records each hop the data packet made, identifying the IP addresses of gateway computers where the packet stopped en route to its final destination, and the length of time of each hop. Enter the IP address or host name of the specific Internet address to be validated, and then click **Execute** to display results in the pop-up window.

Process list

The Process list diagnostic tool is used for viewing a list of processes that have run on the server, and their statuses. When **Execute** is clicked, rows of processes display in the pop-up window, including the following information for each process: Process Identification Number, full device number of the controlling terminal, status code, amount of time it took to run the process, and command line.

TOP CPU processes

The TOP CPU processes diagnostic tool is used for analyzing how much memory and CPU power is being consumed by which processes. When **Execute** is clicked, the pop-up window displays the following information: the load average, number of processes that can run, current utilization by CPUs on the system, and memory and swap file space currently being used and currently available. A row of statistics displays for each process utilizing the most resources on the system.

NIC configuration

NIC Configuration is used for verifying the server's network interface configuration at bootup. When **Execute** is clicked, information about the NIC mode and RX packets and TX packets displays in the pop-up window.

Active connections

When Active Connections is selected and **Execute** is clicked, information about opened connections displays in the pop-up window. The first half of the results includes packet traffic data on configured network interfaces. The second half of the results includes a list of active UNIX domain sockets for each protocol.

Routing table

When Routing Table is selected and **Execute** is clicked, information about available routes and their statuses displays in the pop-up window. Each route consists of a destination host or network and a gateway to use in forwarding packets.

Current memory usage

When Current Memory Usage is selected and **Execute** is clicked, the pop-up window shows the amount of memory being used, and the amount of memory available for three intervals of one second each.

CPU usage

The CPU Usage diagnostic tool shows information on disk usage. When **Execute** is clicked, the pop-up window shows the average CPU usage, as well as the usage by device and file system/partition.

System performance

The System Performance diagnostic tool shows information on resources being used. When **Execute** is clicked, the pop-up window shows averages on various statistics. These results can be stored in a compact binary format and then viewed at later date, so that if you discover a system or application problem occurred, you can analyze system activity during that time period. With this data, you can specify start and end times for reporting on that data, and calculate average usage for periods of time when performance is most critical or during normal user hours.

Recent logins

The Recent Logins diagnostic tool is used for showing information on administrator login activity. When **Execute** is clicked, the pop-up window displays a row of data for each time an administrator logged on the ProxyBlocker server.

System uptime

The System uptime diagnostic tool is used for showing the amount of time the ProxyBlocker has been "up" and running. When **Execute** is clicked, the pop-up window displays a row of data showing the current time, the amount of time the ProxyBlocker has been up, the number of users, and the load averages for the past 1, 5 and 15 minute intervals.

df(disk usage)

The Disk Usage diagnostic tool is used for viewing disk usage information by file system. When **Execute** is clicked, rows of disk information display in the Result pop-up window, including the following information for each disk: Filesystem name, 1K-blocks on the disk, number of Used blocks, number of Available blocks, Use%, locations where the disk is Mounted on.

dmesg(print kernel ring buffer)

The Print Kernel Ring Buffer diagnostic tool is used for viewing the kernel ring buffer in which kernel messages are stored. When **Execute** is clicked, messages from the kernel ring buffer display in the Result pop-up window. These messages from system boot-up provide information about hardware and module initialization, useful for diagnosing system problems.

View Log File window

The View Log File window displays when View Log File is selected from the Diagnostics menu. This window is used for viewing the most recent log file results of various activities and for troubleshooting.

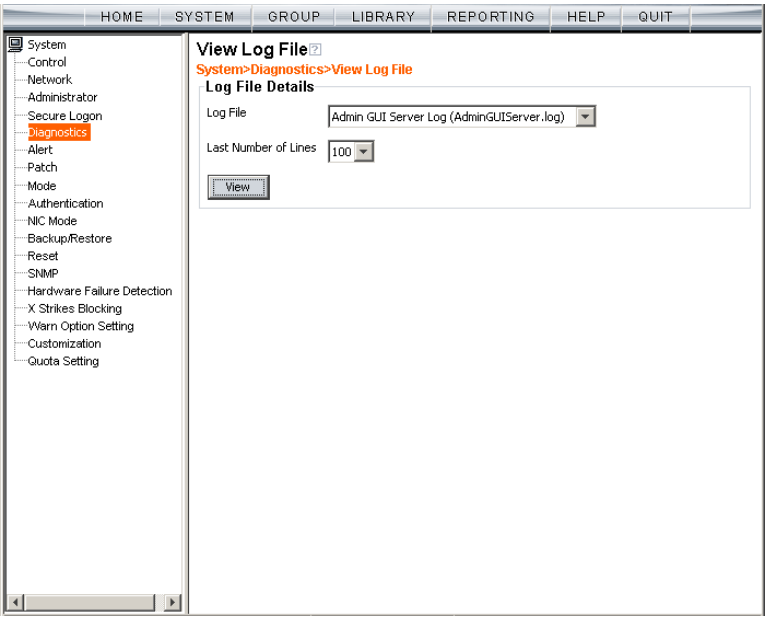


Fig. 2:1-30 View Log File window

View Log Results

In the Log File Details frame:

1. Select the type of **Log File** to view:
   - "Realtime Traffic Log (shadow.log)" - used for viewing the Internet activity of all users on the network.
   - "User Name Log (usage.log)" - used for viewing the time and date a user logged on and off the network, along with the user's profile information.
   - "Patch Log (patch.log)" - used for viewing the results of a software update application, such as which files were copied to the server, and whether the software update was successfully applied.
   - "Error Log (error.log)" - used only if an Alternate IP Address is being used in the Block Page Route frame of the Operation Mode window. This log only displays information if the IP address used for sending block pages is not being reconciled with the MAC address of the NIC card.
   - "Admin GUI Server Log (AdminGUIServer.log)" - used for viewing information on entries made by the administrator in the ProxyBlocker console.

***NOTE**: For information about the "Wbwatch Log (wbwatch.log)", "Authentication Log (AuthenticationServer.log)", "eDirectory Agent Debug Log (edirAgent.log)", "eDirectory Agent Event Log (edirEvent.log)" and "Authentication Module Log (authmodule.log)" options, see the View log results section in the 8e6 ProxyBlocker Authentication User Guide.*

2. Choose the **Last Number of Lines** to view (100-500) from that file.
3. Click **View** to to open a pop-up window containing the log results:

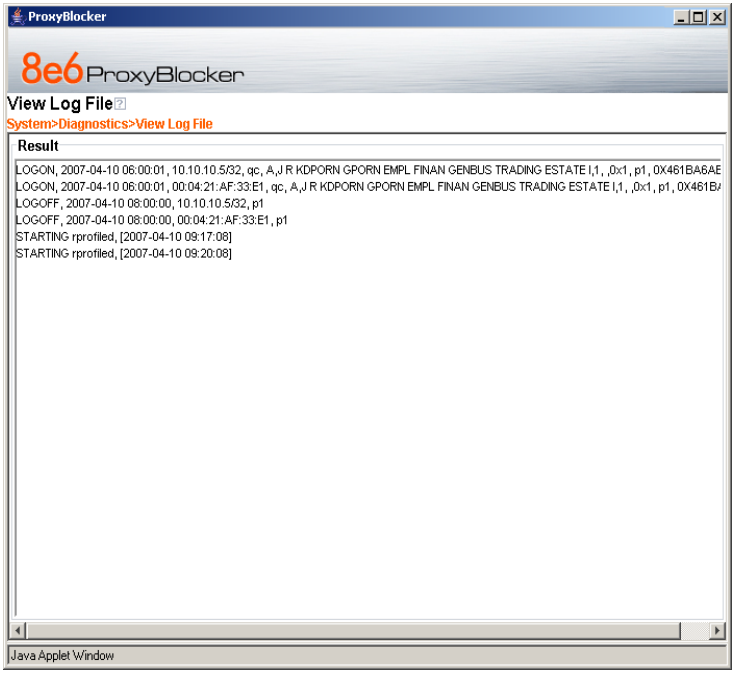


Fig. 2:1-31 View Log File, Results window

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

Troubleshooting Mode window

The Troubleshooting Mode window displays when Troubleshooting is selected from the Diagnostics menu. This window is used if the server is not sending or receiving packets as normal.

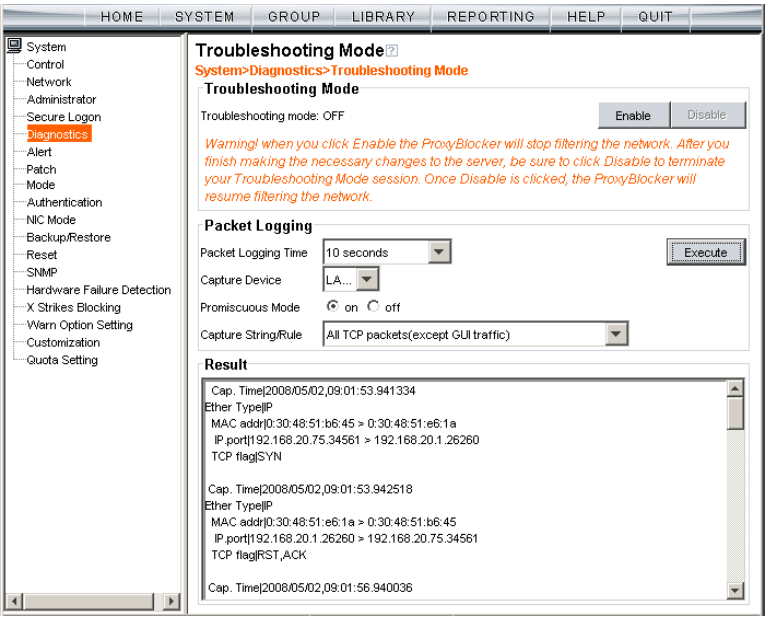


Fig. 2:1-32 Troubleshooting Mode window

WARNING: *This tool utilizes system resources, impacting the ProxyBlocker's performance. When you click Enable, the ProxyBlocker will stop filtering the network. After you finish making the necessary changes to the server, be sure to click Disable to terminate your Troubleshooting Mode session. Once Disable is clicked, the ProxyBlocker will resume filtering the network.*

NOTE*: See the Operation Mode window for information about the invisible mode listening devices.*

Use the Troubleshooting Mode

1. Click **Enable** to begin working in the troubleshooting mode.
2. In the Packet Logging frame, select the **Packet Logging Time** from the available selections (10 seconds, 30 seconds, 60 seconds). This time is the interval during which the server captures packets in real time, ranging from the moment the command is executed until the designated point of time in the future.
3. At the **Capture Device** field, the default listening device for the operation mode displays. If necessary, make a selection from the pull-down menu that corresponds to the operation mode used on the network—"LAN2" or "LAN1".
4. At the **Promiscuous Mode** field, the default choice ("on" or "off") displays, based on the operation mode that was selected. The promiscuous mode is a mode of operation in which each data packet that is sent will be received and read by the Network Interface Card (NIC).
5. If necessary, click the appropriate radio button to indicate whether to turn the promiscuous mode on or off. If "on" is selected, the ProxyBlocker will watch all network traffic as in the invisible mode. If "off" is selected, the ProxyBlocker will only capture packets sent to or from the ProxyBlocker.
6. At the **Capture String/Rule** field, select the type of packets to be captured: Transmission Control Protocol (TCP); Address Resolution Protocol (ARP); packets destined to a specified port (80, 443, 81); packets destined to the ProxyBlocker; packets sent to or from port 20 or 21; or packets sent to the Virtual IP address's port 137 or 139.
7. Click **Execute** to display results in the Result list box.

8. After performing the fixes on the ProxyBlocker server, return to this window and click **Disable** to resume filtering the network.

Active Profile Lookup window

The Active Profile Lookup window displays when Active Profile Lookup is selected from the Diagnostics menu. This window is used for verifying whether an entity has an active filtering profile.

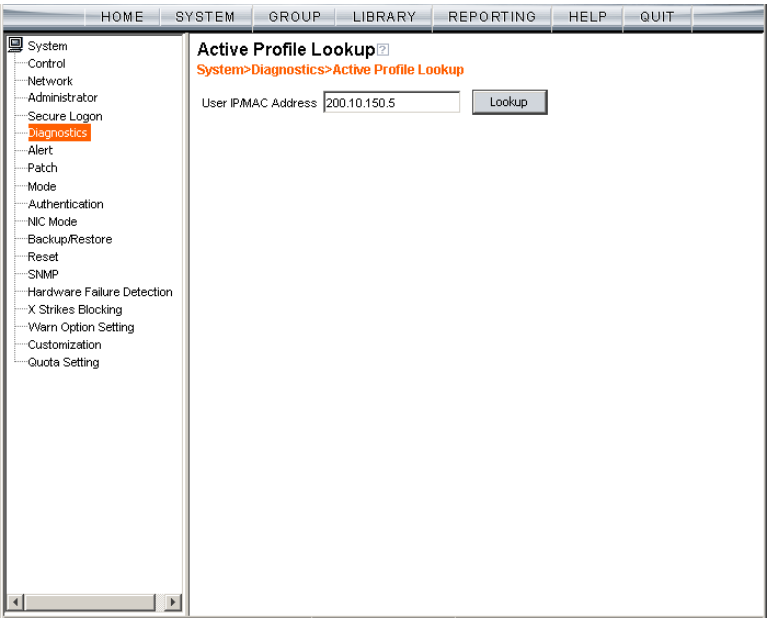


Fig. 2:1-33 Active Profile Lookup window

***NOTE**: In order to use this diagnostic tool, IP groups and/or members must be set up in the Group section of the Proxy-Blocker, and each IP group and/or member must have a filtering profile.*

Verify Whether a Profile is Active

1. In the **User IP/MAC Address** field, enter the IP address of the end user.
2. Click **Lookup** to verify whether or not a profile is active for that IP address.

   If the filtering profile is active, a pop-up box opens containing the Result frame that displays profile settings applied to the profile:

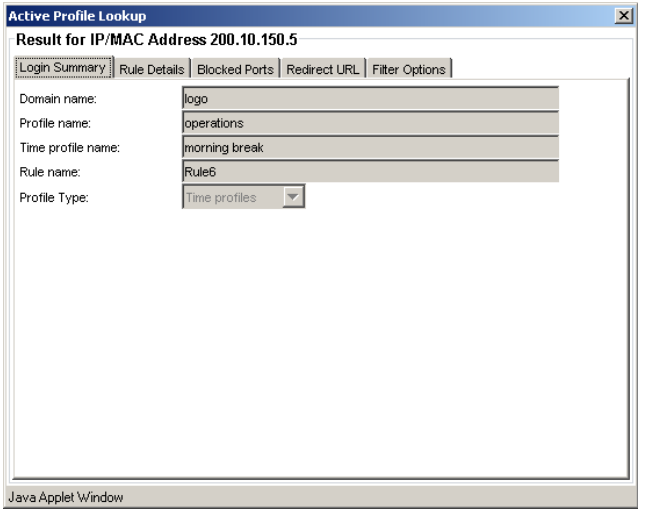


Fig. 2:1-34 Active Profile Lookup results

The default Login Summary tab displays the following information:

- Domain name - IP group domain name
- Profile name - name of the profile
- Time profile name - name of the time profile, if this is a time profile
- Rule name - rule number, if this profile uses a non-custom rule

- Profile Type - type of profile:
  - Regular profiles - IP group, sub-group, or individual profile
  - Global profile - Global group profile
  - Override profiles - Override Account profile
  - Lock profiles - X Strikes Blocking lock out profile
  - Time profiles - Time Profile

3. Click the following tabs to view information in that tab: Rule Details, Blocked Ports, Redirect URL, Filter Options.

   - **Rule Details** - In the Rule Details frame, the Category Groups tree displays group and library categories with filter settings that determine whether or not the end user can access URLs set up for that category group/ library category.

***TIP**: In the Category Groups tree, double-click the group envelope to open that segment of the tree and to view library categories belonging to that group.*

   A check mark inside a green circle displays in the Pass, Allow, Warn, Block column for the filter setting assigned to the category group/library category for the end user. These filter settings indicate the following:

   - Pass - URLs in this category will pass to the end user.
   - Allow - URLs in this category will be added to the end user's white list.
   - Warn - URLs in this category will warn the end user that the URL he/she requested can be accessed, but may be against the organization's policies. The end user can view the URL after seeing a warning message and agreeing to its terms.
   - Block - URLs in this category will be blocked.

- Quota - If a number displays in this column, the corresponding category group/library category was set up as passed but with a time limit, as defined by the number of minutes in that column. After spending 75 percent of the allotted time visiting URLs in that group/category, the user receives a quota warning message; after spending100 percent of the allotted time visiting URLs in that group/category, he/she receives a quota block page.

***NOTE**: If a category group does not display any filter setting (i.e. the check mark does not display in any column for the category group), one or more library categories within that group has a filter setting in a column other than the filter setting designated for all collective library categories within that group. For example, if in the Adult Content category group some of the library categories have a block setting and other library categories have a warn setting, there would be no category group filter setting, since all library categories do not have the same filter setting.*

At the bottom of the Rule Details frame, Uncategorized Sites are set to “Pass”, “Warn”, or “Block”, indicating that the selected setting applies to any non-classified URL. If the Overall Quota field is enabled, the user is restricted to the number of minutes shown here for visiting URLs in all groups/categories collectively in which a quota is specified.

- **Blocked Ports** (optional) - ports that have been set up to be blocked, if established.
- **Redirect URL** (optional) - the URL that will be used for redirecting the user away from a page that is blocked, if established.
- **Filter Options** (optional) - filter options to be used in the user’s profile: “X Strikes Blocking”, “Google/ Yahoo!/Ask.com/AOL Safe Search Enforcement”, “Search Engine Keyword Filter Control”, and/or “URL Keyword Filter Control” with/without the “Extend URL Keyword Filter Control” option selected.

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

Admin Audit Trail window

The Admin Audit Trail window displays when Admin Audit Trail is selected from the Diagnostics menu. This window is used for specifying FTP criteria so that a log of server changes made by an administrator will be sent to the FTP server. The log of changes made on the server can be viewed in this window.

Admin Audit Trail

The Admin Audit Trail tab displays by default:

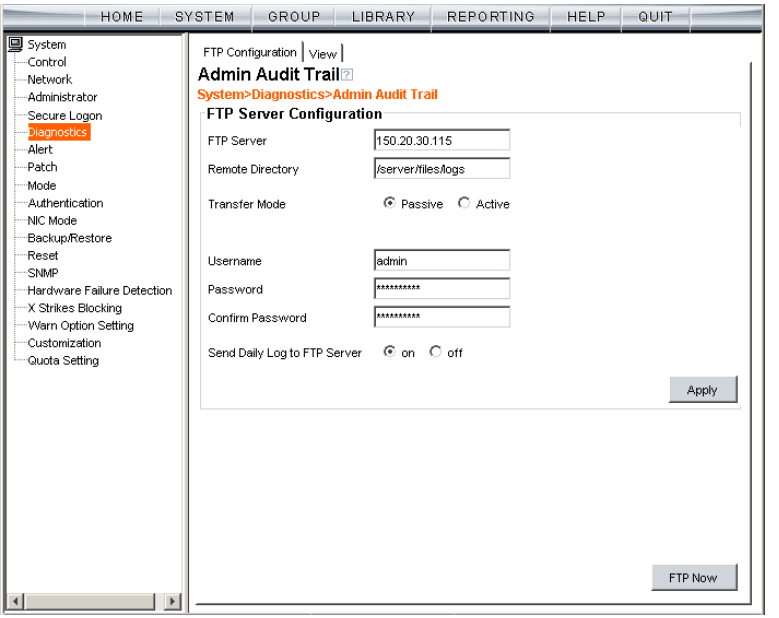


Fig. 2:1-35 Admin Audit Trail window

Specify FTP Criteria

1. Enter the IP address of the **FTP Server**.
2. The log will be sent to the current default directory, unless a **Remote Directory** is specified.
3. At the **Transfer Mode** field, “Passive” is selected by default, indicating that transfers will be made via unrestricted outgoing network connections. Click “Active” if transfers will be initiated by the server.
4. Type in the **Username** to be used.
5. Type in the **Password** to be used, and type it again in the **Confirm Password** field.
6. Specify whether or not to **Send Daily Log to FTP Server** by clicking either the “on” or “off” radio button.
7. Click **Apply** to apply your settings.

FTP the Log on Demand

Click **FTP Now** to transfer the log on demand.

View

View the Log of Administrator Changes

To view the log, click the View tab:

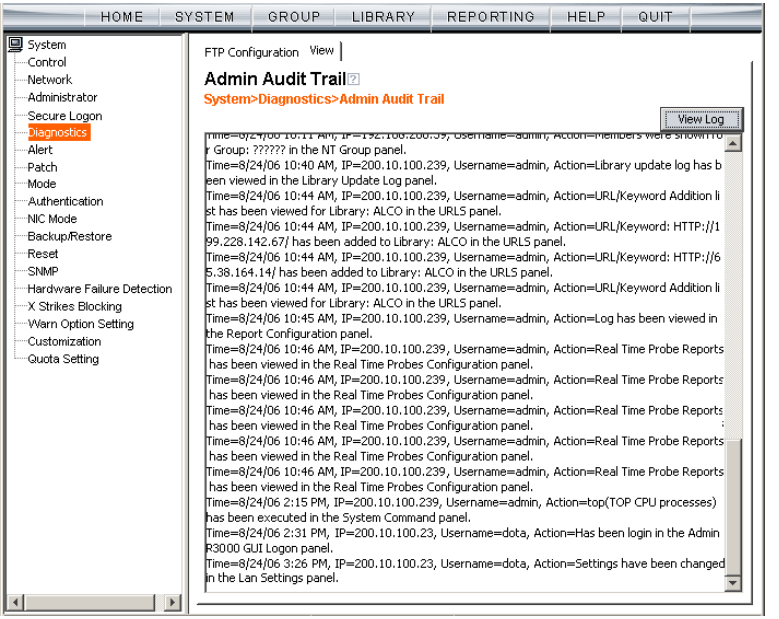


Fig. 2:1-36 Admin Audit Trail window, View tab

Click **View Log** to display data on recent activity. For each change made on the server, the log will contain the date and time the change was made (Time), IP address of the machine used by the administrator, administrator's Username, and a brief description of the Action performed on the server.

Alert

Alert includes options for setting up alert emails that notify designated individuals of problems on the network. Click the Alert link to view a menu of sub-topics: Alert Settings, and SMTP Server Settings.

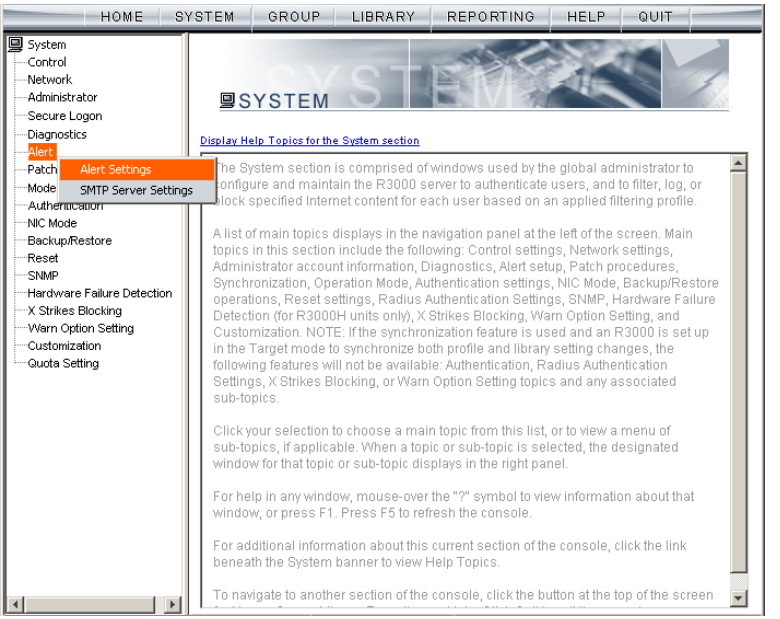


Fig. 2:1-37 System screen, Alert menu

Alert Settings window

The Alert Settings window displays when Alert Settings is selected from the Alert menu. This window is used for setting up and maintaining email addresses of contacts who will receive automated notifications if problems on the network are detected during the ProxyBlocker's self-monitoring process.

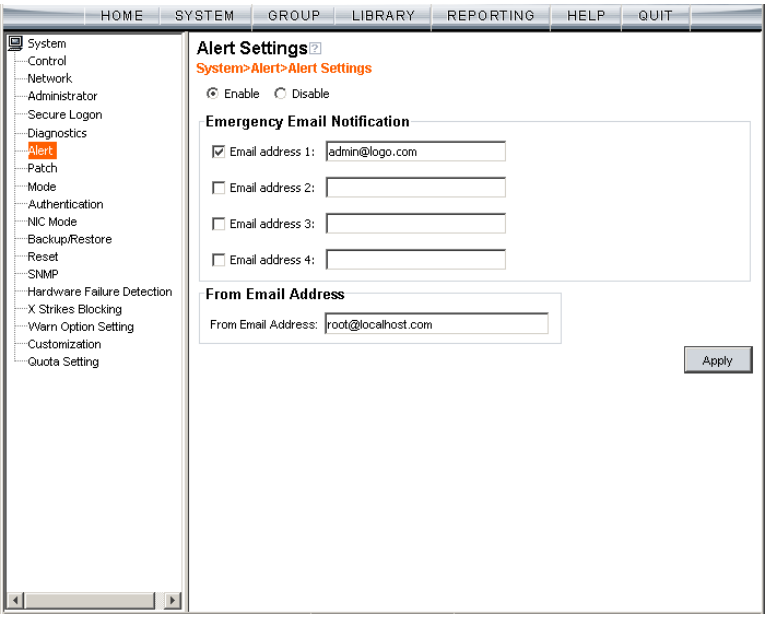


Fig. 2:1-38 Alert window

The following processes are monitored by the ProxyBlocker:

- **CPU Processes** - If any CPU process fails to run, the ProxyBlocker alerts the administrator about the failed process, and that an attempt will be made to reload the necessary process. The last few lines of any pertinent logs are included in the message to assist the administrator in troubleshooting the problem. In most cases, the reload procedure will fix the error, and no futher interven-

tion will be required. However, if the error is not fixed—such as if a misconfiguration was made that causes a process to be unable to load on the system—the ProxyBlocker repeats this procedure until an administrator fixes the error.

- **Hard Drive Utilization** - If the ProxyBlocker detects that hard drive utilization exceeds 80 percent, an alert is sent to the administrator. This problem usually occurs if the ProxyBlocker is unable to transfer log files to the reporting application—an 8e6 Enterprise Reporter (ER) server, or a designated third party FTP server. Action should be taken to prevent the hard drive from reaching 100 percent utilization.
- **Log File Transmission** - If the ProxyBlocker is unable to send log files as scheduled to an ER server or a third party FTP server, the log files are placed in a queue so they can be sent when a connection is established with the server. If these logs cannot be successfully transmitted after a period of time, an alert is sent to the administrator. The last few lines of the error log are included in the message to assist the administrator in troubleshooting the problem.

Enable the Alert Feature

By default, the “Disable” radio button is selected. To enable the feature for sending automated email notifications:

1. Click the “Enable” radio button to activate all elements in the Emergency Email Notification frame.
2. Enter up to four email addresses of contacts.
3. Click in the checkbox of each email address that should receive notifications regarding network problems.
4. If using an SMTP server for sending alert email messages to designated administrators, enter the email address of the ProxyBlocker in the **From Email Address** field.
5. Click **Apply** to apply your settings.

Modify Alert Settings

1. Make any of the following edits in the Emergency Email Notification frame:
   - change an email address by typing the new one over the existing one
   - deactivate a contact by removing the check mark from the checkbox corresponding to that contact’s email address
   - delete a contact by using your mouse to copy over the entire email address, and then pressing the Delete key on your keyboard
2. After all edits have been made, click **Apply** to apply your settings.

Disable the Alert Feature

1. Click the “Disable” radio button.
2. Click **Apply** to apply your settings.

SMTP Server Settings window

The SMTP Server Settings window displays when SMTP Server Settings is selected from the Alert menu. This window is used for entering settings for the Simple Mail Transfer Protocol that will be used for sending email alert messages to specified administrators.

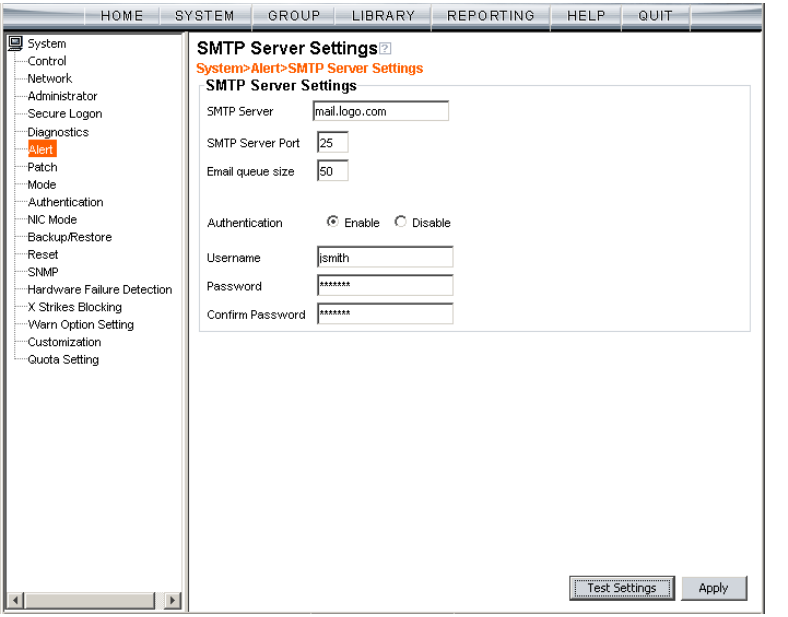


Fig. 2:1-39 SMTP Server Settings window

Enter, Edit SMTP Server Settings

1. Enter the **SMTP Server** name, for example: **mail.logo.com**.
2. By default, the **SMTP Server Port** number used for sending email is *25*. This should be changed if the sending mail connection fails.
3. By default, the **Email queue size** is *50*. This can be changed to specify the maximum number of requests

that can be placed into the queue awaiting an available outbound connection.

4. By default, **Authentication** is disabled. Click “Enable” if a username and password are required for logging into the SMTP server. This action activates the fields below.

   Make the following entries:

   a. Enter the **Username**.

   b. Enter the **Password** and make the same entry in the **Confirm Password** field.

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

Verify SMTP Settings

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

1. Click **Test Settings** to open the pop-up box:

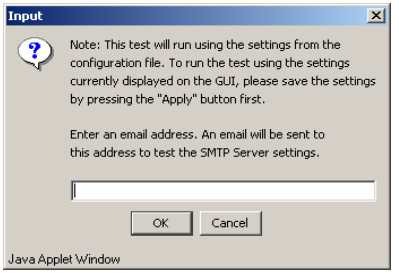


Fig. 2:1-40 SMTP Test Settings box

2. Enter the email address in the pop-up box.

3. Click **OK** to close the pop-up box and to process your request. If all SMTP Server Settings are accepted, the test email should be received at the specified address.

Patch

Patch includes options for uploading software updates. Click the Patch link to view a menu of sub-topics: Local Patch, and Patch Update Log.

Fig. 2:1-41 System screen, Patch menu

Local Patch window

The Local Patch window displays when Local Patch is selected from the Patch menu. This window is used for viewing information about software updates previously applied to the current server being configured, and for viewing information about software updates currently available.

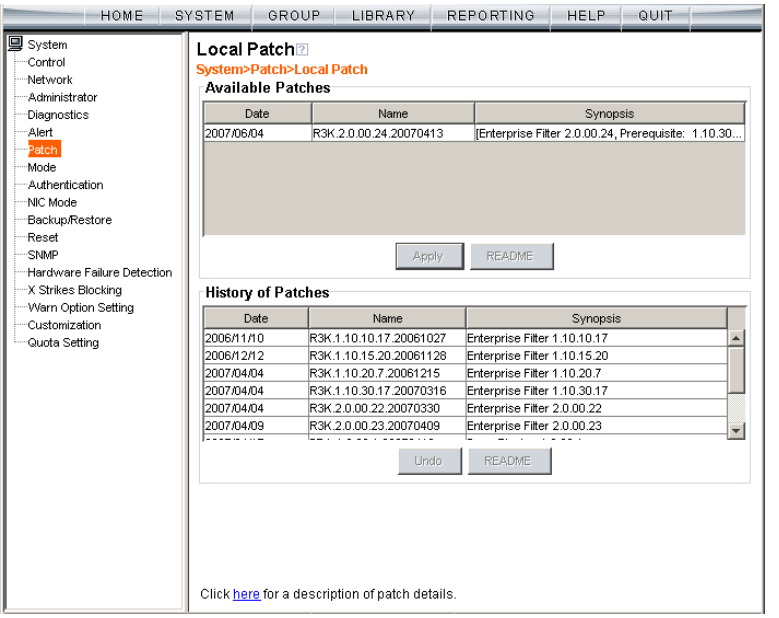


Fig. 2:1-42 Local Patch window

***NOTE**: Available software updates for the ProxyBlocker come from downloads made to the server via Traveler, 8e6's executable program that can run on demand, or be set to run at a scheduled time.*

***TIP**: Click the link ("here") at the bottom of the window to go to the Web page at 8e6 Technologies' public site (**http://www.8e6.com/software-updates/pba-software-updates**)) where release notes about software updates can be obtained.*

Read Information about a Software Update

In either the Available Patches frame or the History of Patches frame, the Date, Name, and Synopsis are included for each software update.

To read information about a software update:

1. Select a software update from the list.
2. Click the **README** button to open the README pop-up box that contains information about the software update:

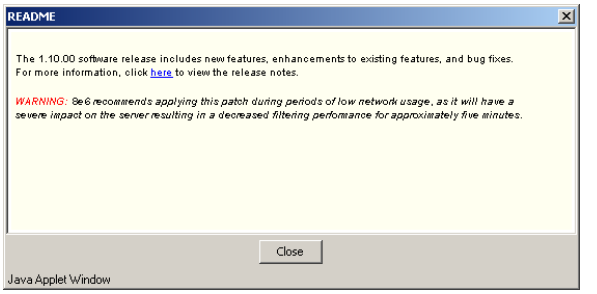


Fig. 2:1-43 Software update Readme

3. Click **Close** to close the pop-up box.

Select and Apply a Software Update

To apply a software update:

1. Go to the Available Patches frame and select the software update to be applied.

***NOTES**: Software updates must be applied to the server in sequential order. Be sure port 8082 is open on your network.*

2. Click **Apply** to open the software update installation dialog box:

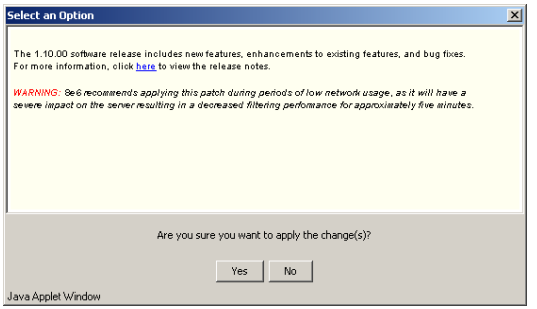


Fig. 2:1-44 Software update installation dialog box

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

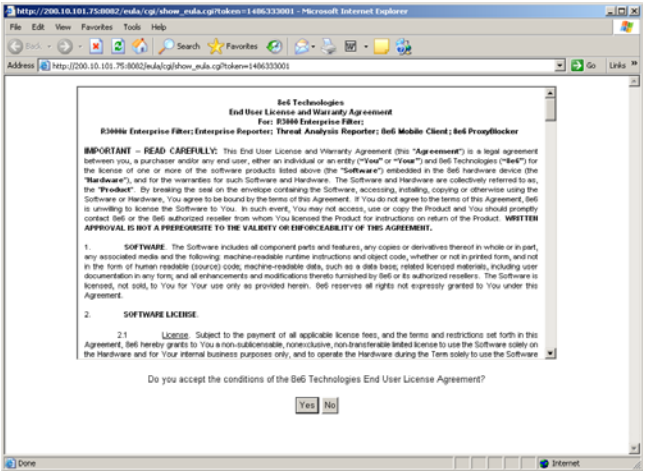


Fig. 2:1-45 EULA dialog box

4. After reading the contents of the End User License Agreement, click **Yes** if you agree to its terms. This action closes the EULA dialog box and opens the alert box verifying the software update application process:

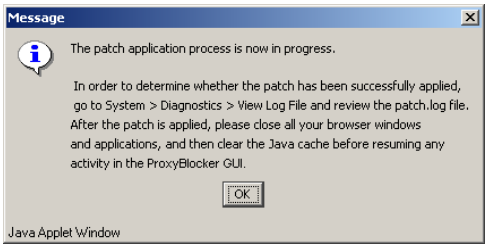


Fig. 2:1-46 Software update verification message box

***NOTE**: To verify whether or not a software update has been successfully applied, go to the View Log File window and select "Patch Log (patch.log)". See View Log File window for more information.*

5. Click **OK** to close the alert box and to proceed. This action opens the connection failure alert box, indicating that the connection to the ProxyBlocker server has been lost due to the software update application:

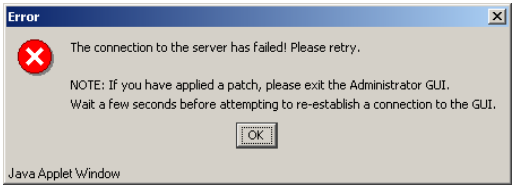


Fig. 2:1-47 Connection failure alert box

6. Click **OK** to close the alert box.
7. In the navigational bar, click **Quit** to exit the ProxyBlocker console, and also close the ProxyBlocker Introductory Window.
8. Wait a few minutes, and then log back into the ProxyBlocker console again.

***NOTE**: 8e6 recommends performing a backup of configuration files after applying a software update. (See the Backup/Restore window in this chapter for information on performing a backup.)*

Undo an Applied Software Update

***NOTE**: Only the most recently applied software update can be uninstalled.*

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

To unapply a software update:

1. Go to the History of Patches frame and select the software update to be unapplied.
2. Click **Undo**.

Patch Update Log window

The Patch Update Log window displays when Patch Update Log is selected from the Patch menu. This window is used for viewing the software update log that provides the status on the ProxyBlocker's software update activity, including checks for new software updates, and downloaded and applied software updates.

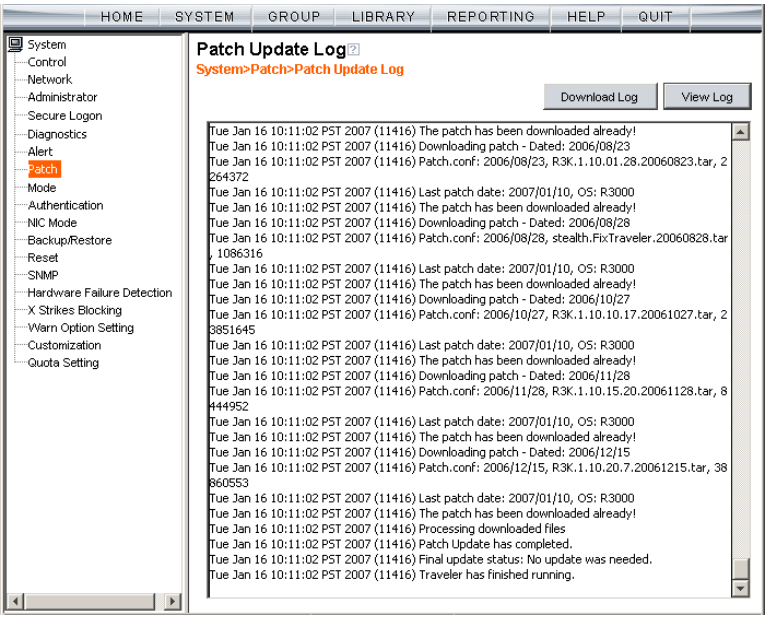


Fig. 2:1-48 Patch Update Log window

View Log Contents

Click **View Log** to display contents of the log in the frame below with the status of the software update.

Download Log, View, Print Contents

Download the Log

1. Click **Download Log** to open the alert box containing a message on how to download the log file to your workstation, if using Windows XP.
2. Click **OK** to close the alert box. Two pop-up boxes open:
   - A second alert box asks you to confirm that the file was successfully saved to your machine. Click **OK** in this box after the download is completed.
   - In the File Download dialog box, click **Save**:

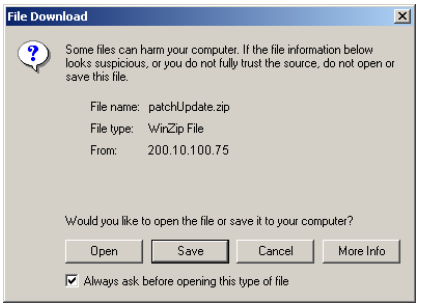


Fig. 2:1-49 Download Log dialog box

This action opens the **Save As** window:

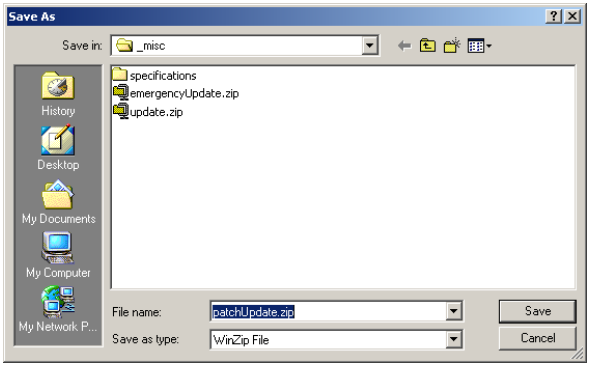


Fig. 2:1-50 Save As pop-up window

3. Find the folder in which to save the file, and then enter the **File name**, retaining the ".zip" file extension. Click **Save** to begin downloading the zip file to your workstation.

   After the file has completely downloaded, the Download complete dialog box opens:

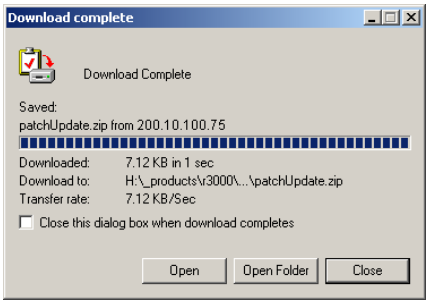


Fig. 2:1-51 Download Complete box

4. You can now open this file, open the folder where the file was saved, or close this dialog box.

***NOTE**: Proceed to View the Contents of the Log for information on viewing or printing the contents of the log file.*

5. Click **OK** to close the alert box asking you to verify that the software update log file was successfully saved to your machine.

View the Contents of the Log

Once the software update log file has been downloaded to your workstation, you can view its contents.

1. Find the log file in the folder, and right-click on it to open the pop-up menu:

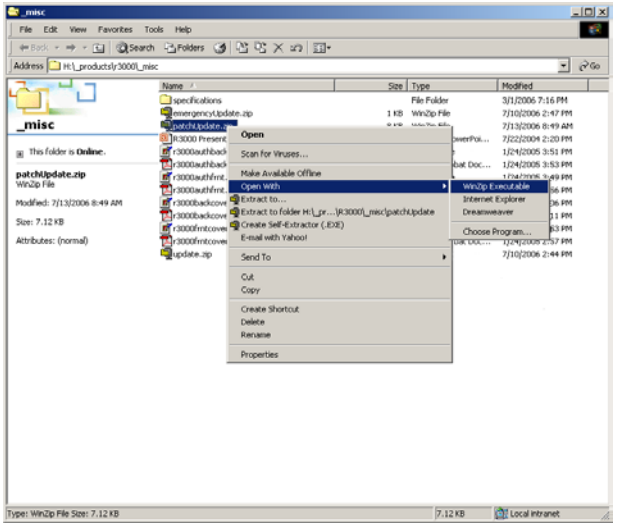


Fig. 2:1-52 Folder containing downloaded file

2. Choose “Open With” and then select a zip file executable program such as “WinZip Executable” to launch that application:

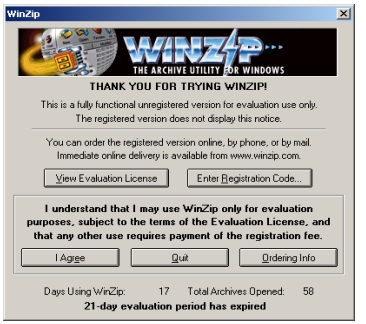


Fig. 2:1-53 WinZip Executable program

3. If using WinZip, click **I Agree** to open the window containing the zip file:

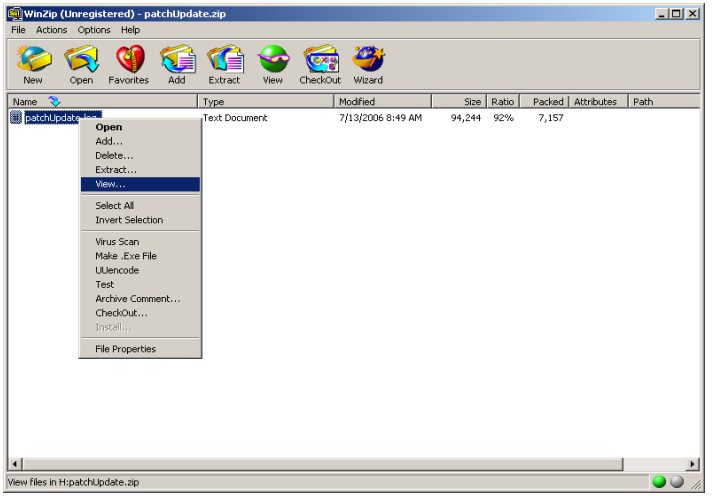


Fig. 2:1-54 WinZip window

4. Right-click the zip file to open the pop-up menu, and choose “View” to open the View dialog box:

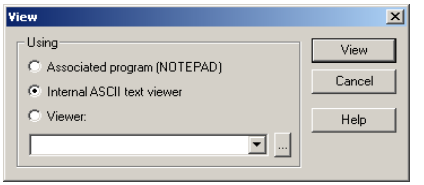


Fig. 2:1-55 View dialog box

5. Select “Internal ASCII text viewer”, and then click **View** to open the View window containing the log file contents:

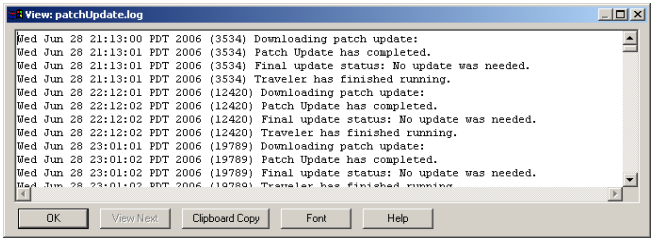


Fig. 2:1-56 View window

Save, Print the Log File Contents

With the log file displaying correctly formatted in WinZip’s View window, if you wish to save or print the contents of this file:

1. Click **Clipboard Copy**, wait for the dialog box to open and confirm that the text has been copied to the clipboard, and then click **OK** to close the dialog box.
2. Open Notepad:
   - in Windows XP: Start > All Programs > Accessories > Notepad
   - in Windows 2000: Start > Programs > Accessories > Notepad
3. Paste the contents from the clipboard into the Notepad file.

   The correctly formatted Notepad file can now be saved and/or printed.

Mode

Mode includes options for configuring the ProxyBlocker to filter the network. Click the Mode link to view a menu of sub-topics: Operation Mode and Proxy Environment Settings.

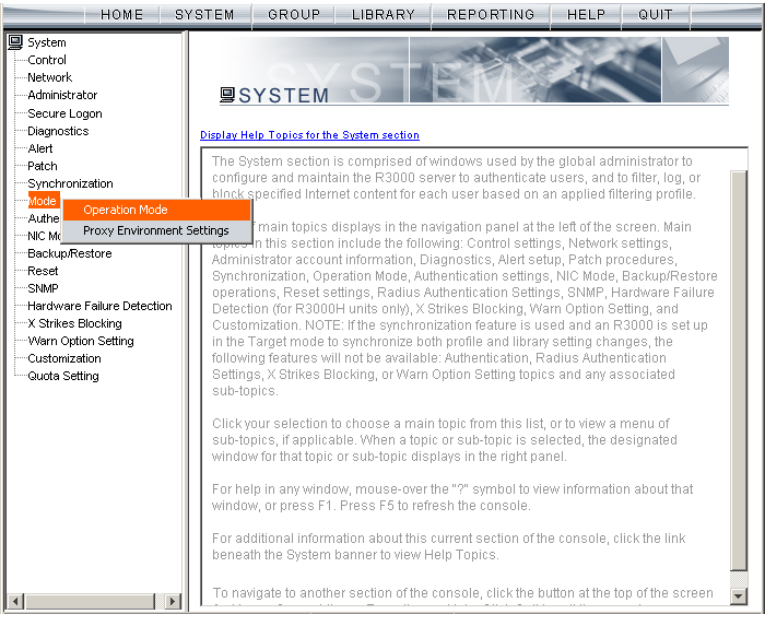


Fig. 2:1-57 System screen, Mode menu

Operation Mode window

The Operation Mode window displays when Operation Mode is selected from the Mode menu. This window is used for specifying criteria for the invisible operational mode the ProxyBlocker will use for filtering on the network, as well as the settings to be used for “listening to” traffic and sending traffic.

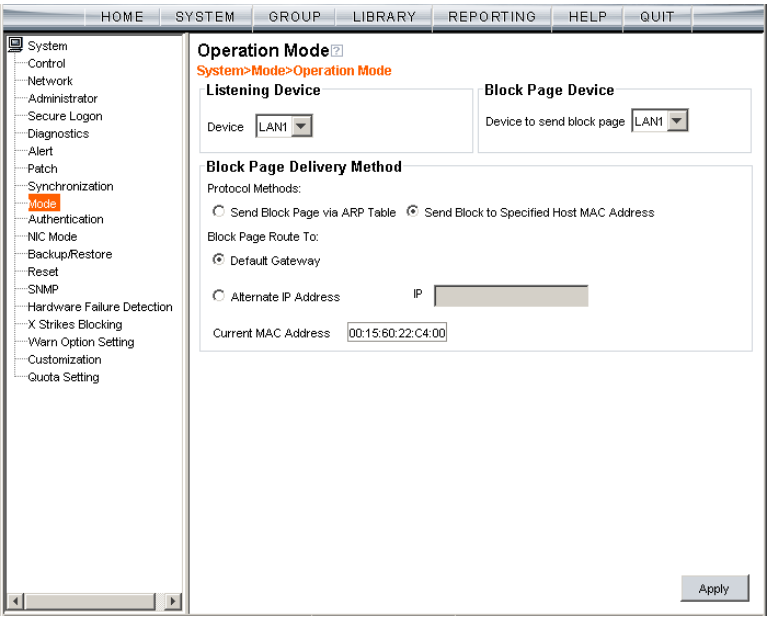


Fig. 2:1-58 Operation Mode window

Specify the Listening Device

In the Listening Device frame, select the default listening **Device** for the selected mode: “LAN1” or “LAN2”. “LAN1” displays by default.

Specify the Block Page Device

In the Block Page Device frame, “LAN2” displays as the default device for sending block pages to client PCs.

***TIP**: The block page device should be a different device than the one selected in the Listening Device frame.*

If necessary, at the **Device to send block page** pull-down menu, choose the network card that will be used to send the block page to client PCs.

***NOTES**: After making all selections in this window, click **Apply**.*

The LAN IP address saved for the Device to send block page will display in the IP field at the bottom of the Administrator console.

Specify the Block Page Delivery

In the Block Page Delivery Method frame, specify the block page delivery method by making the following selection(s):

Choose from either of the two **Protocol Methods**:

- “Send Block Page via ARP Table” - this option uses the Address Resolution Protocol method to find the best possible destination MAC address of a specified host, usually the ProxyBlocker gateway.
- “Send Block to Specified Host MAC Address” - using this preferred method, the block page will always be sent to the MAC address of a specified host, usually the Proxy-Blocker gateway.

  Using this option, choose from either of the two **Block Page Route To** selections:

  - “Default Gateway” - this option indicates that the default gateway on your network will be used for sending block pages. If the invisible mode is selected, “Default Gateway” displays by default as the Block Page Route To selection.

- "Alternate IP Address" - this option should be used if block pages are not being served.

  Enter the **IP** address of the router or device that will serve block pages.

***NOTES**: The Current MAC Address displays if there is a resolution between the IP address and the MAC address of the router or device used for serving block pages.*

If an Alternate IP Address is used, that address must be resolved with the MAC address in order for block pages to be served to client PCs.

Apply Settings

Click **Apply** to apply your settings.

Proxy Environment Settings window

The Proxy Environment Settings window displays when Proxy Environment Settings is selected from the Mode menu. This window is used for specifying whether the Proxy Blocker is in a proxy environment, and if the default Web server port number 80 will be enabled.

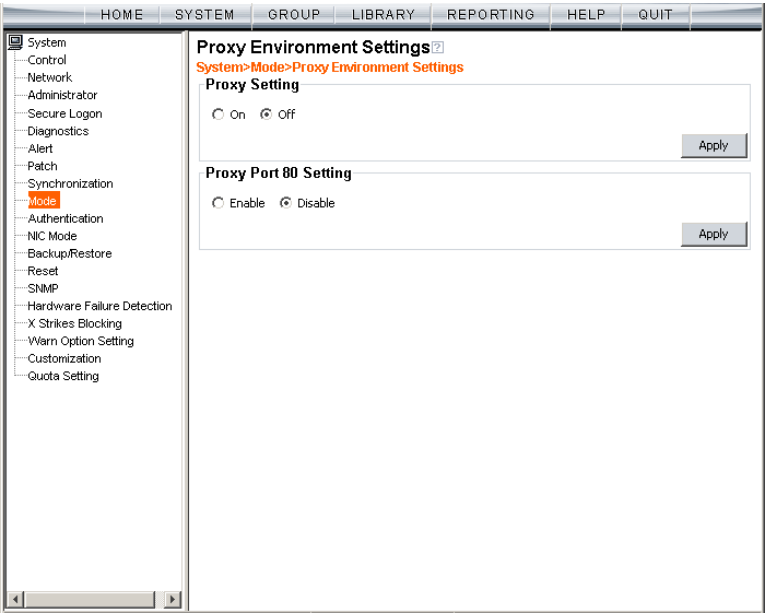


Fig. 2:1-59 Proxy Environment Settings window

***NOTE**: Basic Proxy Authentication must be used if using HTTPS in a proxy environment. The ProxyBlocker has been tested with ISA, Blue Coat, and Squid proxies.*

Use a Local Proxy Server

In the Proxy Setting frame, the default setting is “Off”. To specify that a local proxy server is used in the environment:

1. Click the “On” radio button. This selection indicates that the ProxyBlocker will perform a reverse lookup on packets to detect the source address and origin of packets.
2. Click **Apply** to apply your setting.

Use Proxy Port 80

In the Proxy Port 80 Setting frame, the default setting is “Disable”. To specify that the public proxy server will channel “https” traffic through Port 80:

1. Click the radio button corresponding to “Enable”.
2. Click **Apply** to apply your setting.

Authentication

Authentication includes options for configuring the Proxy-Blocker to authenticate and re-authenticate users on the network. Click the Authentication link to view a menu of sub-topics: Enable/Disable Authentication, Authentication Settings, and Authentication SSL Certificate.

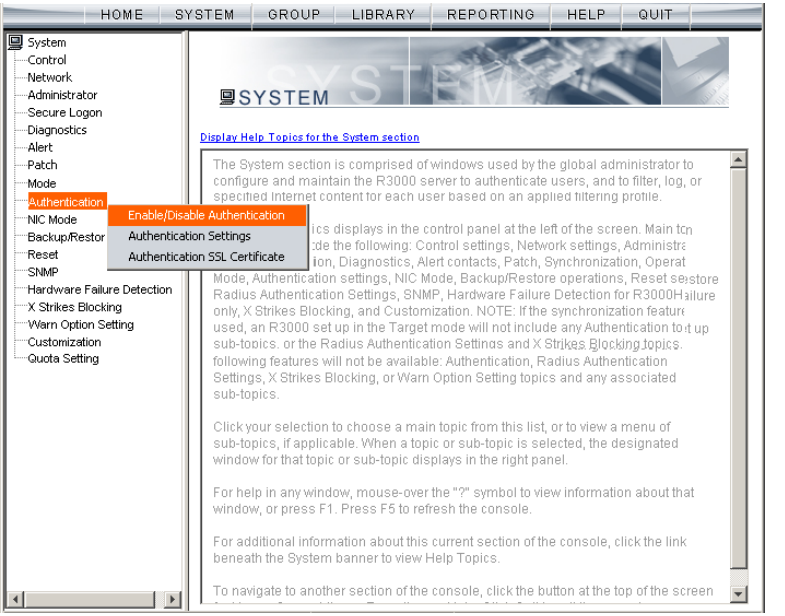


Fig. 2:1-60 System screen, Authentication menu

***NOTE**: Information about these sub-topics can be found in the 8e6 ProxyBlocker Authentication User Guide.*

NIC Mode

NIC Mode window

The NIC Mode window displays when NIC Mode is selected from the navigation panel. This window lets you specify the speed for the ProxyBlocker's Network Interface Card settings so that the ProxyBlocker can communicate with the network switch or hub.

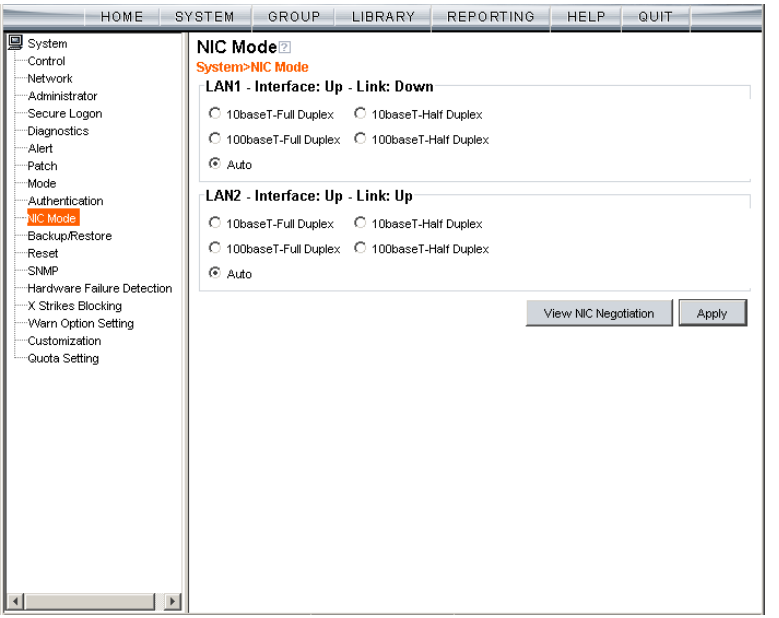


Fig. 2:1-61 NIC Mode window

By default the NIC mode for LAN1 and LAN2 is set to "Auto". The auto-negotiation setting indicates that both connected devices will negotiate the fastest possible commonly shared speed.

***NOTE**: The options available in this window depend on the hardware components installed for the ProxyBlocker unit.*

View the NIC Negotiation

To verify or correct the negotiation for a NIC, click **View NIC Negotiation** to open a window containing results from the mii-tool and the ethtool about the status of the NIC mode(s):

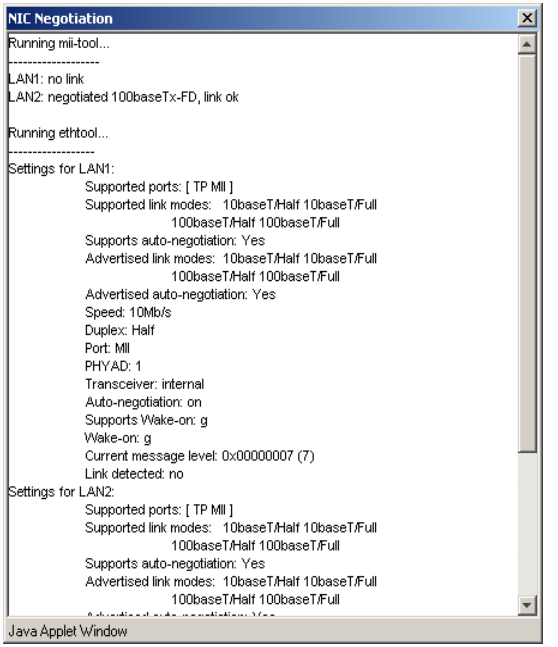


Fig. 2:1-62 NIC Negotiation window

Mii-tool checks or sets the status of a network interface's Media Independent Interface (MII) unit. Ethtool is a diagnostic and tuning tool that examines and tunes the NIC.

Modify the NIC Mode Setting

***WARNING**: If changing the NIC mode, be sure the hub/switch to which the ProxyBlocker is connected will support the selected NIC mode. An incorrect setting may prevent you from accessing the ProxyBlocker console.*

To modify the NIC setting, in the LAN1 or LAN2 frame:

1. Click the radio button for the available option you wish to select: 10baseT-Full Duplex, 10baseT-Half Duplex, 100baseT- Full Duplex, 100baseT-Half Duplex, or 1000baseT-Full Duplex, if available on your Proxy-Blocker model (see NIC Mode Speeds Chart).
2. Click **Apply** to activate the new NIC mode setting.

***NOTE**: The status (Up or Down) of the Interface displays to the right of the LAN1 and LAN2 labels. For an Interface with an "Up" status, the Link status (Up or Down) displays to the right of the Interface status.*

Backup/Restore

Backup/Restore window

The Backup/Restore window displays when Backup/Restore is selected from the navigation panel. This window is used for saving configuration settings and/or custom library additions/deletions on or off the server, and for restoring these settings/modifications later, if necessary.

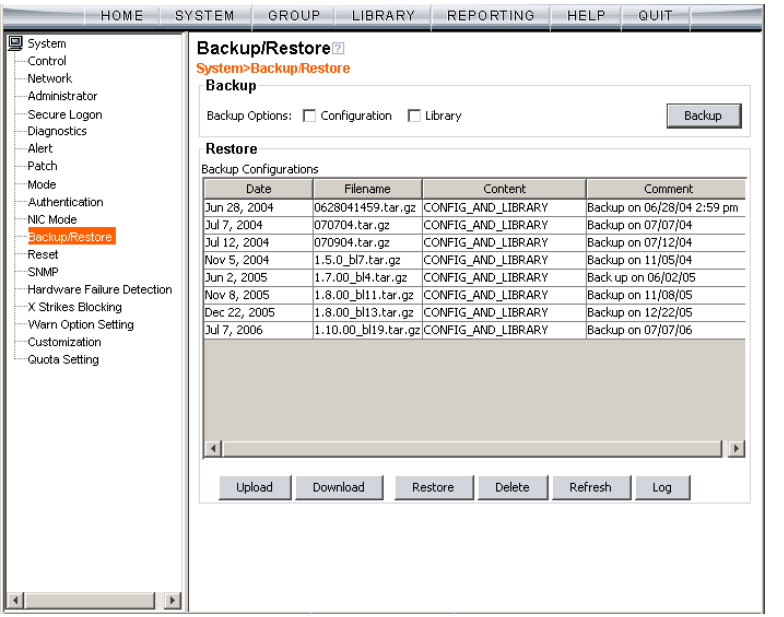


Fig. 2:1-63 Backup/Restore window

***WARNING**: A backup should be created and downloaded off the ProxyBlocker server whenever a change is made to filtering settings on the ProxyBlocker server.*

For each backup configuration created or uploaded via this window, a row is added to the Backup Configurations grid in the Restore frame. The newly added row includes the following information: Date the backup was executed, File-name of the backup file, general information about the Content of the file, and a Comment about the file.

***TIPS**: The order in which columns display in the grid can be changed by clicking the column header and sliding the column to another position in the grid.*

To change the sort order, click the header of a column. All rows will sort in order by that column.

*If text in any column displays truncated—followed by ellipses (...)—place the cursor over the beginning or ending of the column header. When the **<—>** character displays in place of the cursor, you can expand the width of the column. You also can use the scrollbar beneath the grid to view information to the right of the last column.*

Backup Procedures

8e6 recommends performing backup procedures whenever changes are made to system configurations or to library configurations. By creating backup files and saving these files off the ProxyBlocker server, prior server settings can later be retrieved and uploaded to the ProxyBlocker in the event that current settings are incorrect, or if you wish to revert to settings from a previous backup. Additionally, backup files are useful if the current server fails. These backup files can be uploaded to a new server, eliminating the need to re-enter the same settings from the old Proxy-Blocker in the console of the new ProxyBlocker.

Perform a Backup

To back up configuration and/or library modifications:

1. In the Backup frame, click the Configuration and/or Library checkbox(es) as appropriate.
2. Click **Backup** to open the ProxyBlocker Backup dialog box:

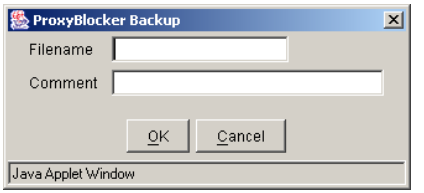


Fig. 2:1-64 ProxyBlocker Backup dialog box

3. Type in the **Filename** for the backup file.
4. Type in a descriptive **Comment** about that file.
5. Click **OK** to close the dialog box, and to open the Wait alert box that informs you it may take some time to back up configurations, based on the amount of data to be saved.
6. Click **OK** to close the Wait alert box. After configurations have been successfully saved, the Message alert box opens to display a confirmation message.
7. Click **OK** to close the Message alert box, and to add a new row to the Backup Configurations grid for that file.

***NOTE**: Once the file is added to the grid, it can be downloaded and saved on another machine, if necessary.*

Download a File

To download a file to your machine:

1. Select the file from the Backup Configurations grid.
2. Click **Download** to open the alert box containing a message on how to download the log file to your workstation, if using Windows XP.
3. Click **OK** to close the alert box.

   In the File Download dialog box that opens, click **Save**:

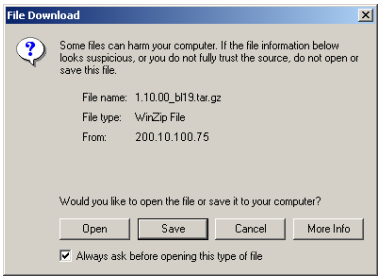


Fig. 2:1-65 File Download box

   This action opens the **Save As** window:

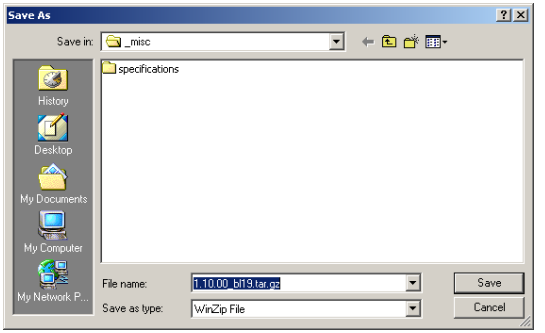


Fig. 2:1-66 Save As pop-up window

4. Find the folder in which to save the file, and then click **Save** to begin downloading the ".gz" file to your workstation.

After the file has completely downloaded, the Download complete dialog box opens:

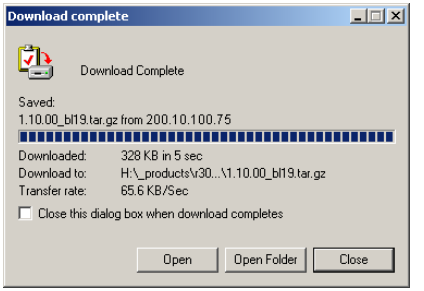


Fig. 2:1-67 Download complete box

You can now open this file, open the folder where the file was saved, or close this dialog box.

Perform a Restoration

To restore backup data to the server, the backup file must be listed in the Backup Configurations grid, and the restoration function must be executed. If the backup file is not included in the Backup Configurations grid, you must upload it to the server.

***WARNING**: Be sure the file you are restoring uses the same version of the software currently used by the ProxyBlocker Administrator console. Refer to the Local Patch window for available updates to the ProxyBlocker's software. (See the Patch window for more information about software updates.)*

Upload a File to the Server

To upload a .gzip file to the server:

1. Click **Upload** to open the Upload Backup GZIP File pop-up window:

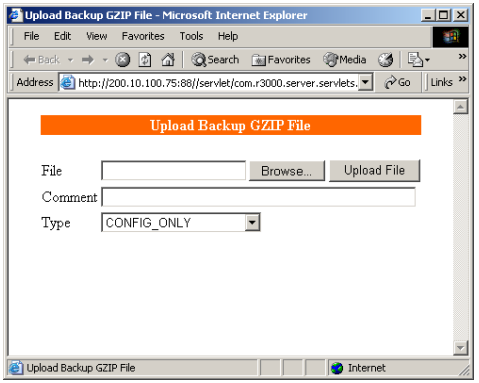


Fig. 2:1-68 Upload GZIP File pop-up window

2. Click **Browse** to open the Choose file window:

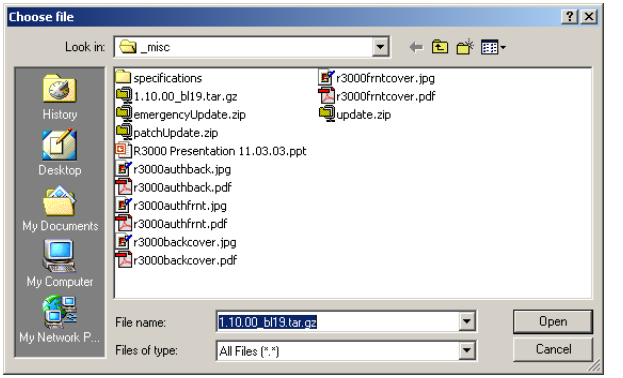


Fig. 2:1-69 Choose file window

3. Select the file to be uploaded. After the file is selected, the Choose file window closes.
4. In the pop-up window, type in a **Comment** about the file.
5. Select the **Type** of file to be uploaded (CONFIG_ONLY, LIBRARY_ONLY, or both CONFIG_AND_LIBRARY).
6. Click **Upload File** to upload this file to the server. If the file is successfully uploaded, the pop-up window's banner name says: "Upload Successful." After a few seconds, the pop-up window closes.
7. Click **Refresh** to display a new row for the uploaded file in the Backup Configurations grid.

Restore Configurations to the Server

To restore configurations or library modifications from a previous backup:

1. Select the file from the Backup Configurations grid.
2. Click **Restore** to overwrite the current settings.

Remove a Backup File

To remove a file from the Backup Configurations grid:

1. Select the file.
2. Click **Delete**.

View Backup and Restoration Details

To view details on backup and/or restoration activities:

1. Click **Log** to open the Backup/Restore Log pop-up box:

Fig. 2:1-70 Backup/Restore pop-up box

The pop-up box includes rows of data about backup and restore processes performed via the Backup/Restore window.

The following information displays for each row: the date and time a process was attempted to be executed, and a Message indicating whether that process succeeded or failed.

2. Click **OK** to close the pop-up box.

Reset

Reset window

The Reset window displays when Reset is selected from the navigation panel. This window is used for resetting the server back to the default settings when the box was first acquired.

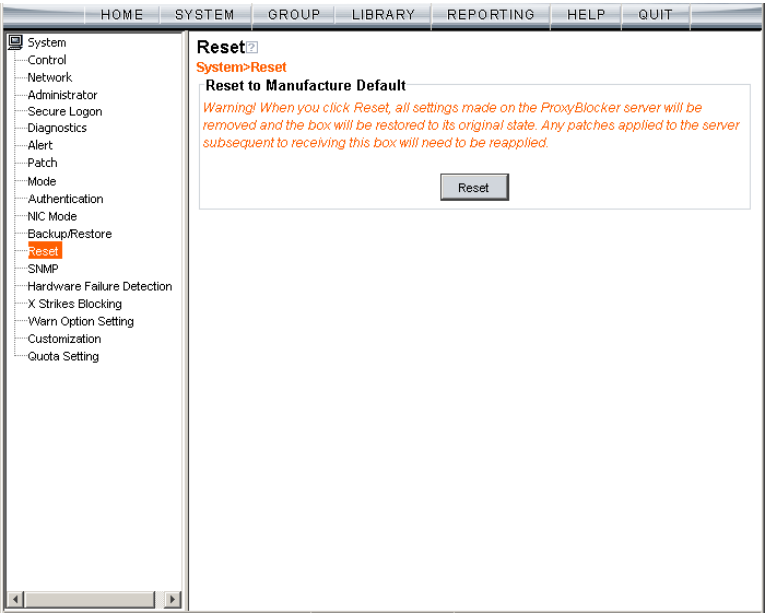


Fig. 2:1-71 Reset window

***WARNING**: When Reset is clicked, all settings made on the ProxyBlocker server will be removed and the box will be restored to its original state. Any software updates applied to the server subsequent to receiving this box will need to be reapplied.*

Reset All Server Settings

Click **Reset** to reset the box to the original default settings.

SNMP

SNMP window

The SNMP window displays when SNMP is selected from the navigation panel. This feature lets the global administrator use a third party Simple Network Management Protocol (SNMP) product for monitoring and managing the working status of the ProxyBlocker's filtering on a network.

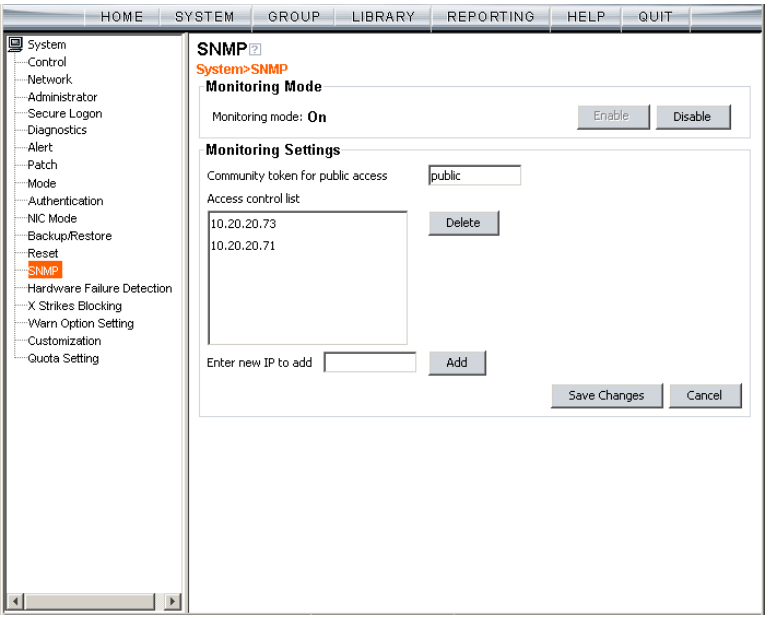


Fig. 2:1-72 SNMP window

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

Enable SNMP

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

Specify Monitoring Settings

Set up Community Token for Public Access

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

Create, Build the Access Control List

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

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

Maintain the Access Control List

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

Hardware Failure Detection

Hardware Failure Detection window

If using a ProxyBlocker SL unit, the Hardware Failure Detection window displays when Hardware Failure Detection is selected from the navigation panel. This feature shows the status of each drive on the RAID server.

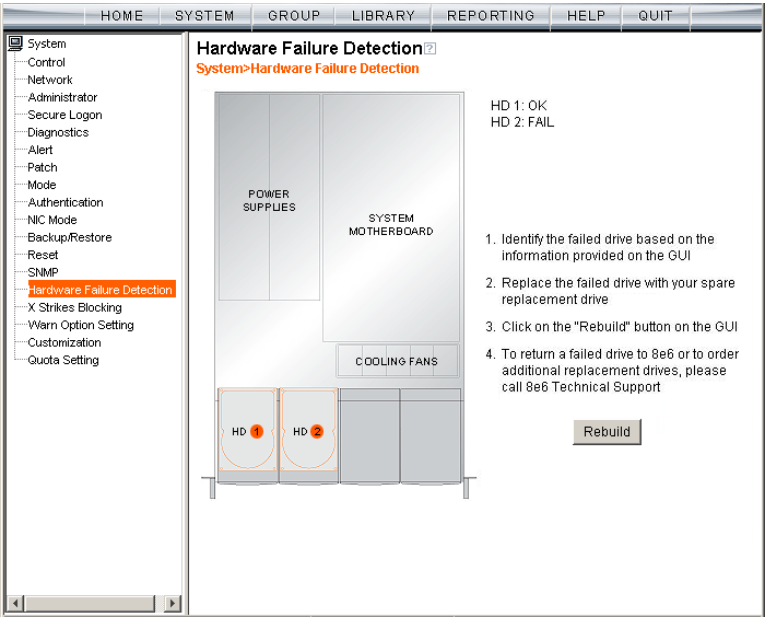


Fig. 2:1-73 Hardware Failure Detection window

View the Status of the Hard Drives

The Hardware Failure Detection window displays the current RAID Array Status for the two hard drives (HD 1, HD 2). If both hard drives are functioning without failure, the text "OK" displays to the right of the hard drive number, and no other text displays on the screen.

If any of the hard drives has failed, the message "FAIL" displays to the right of the hard drive number, and instructions for replacing the hard drive display below:

1. Identify the failed drive based on the information provided on the GUI
2. Replace the failed drive with your spare replacement drive
3. Click on the "Rebuild" button on the GUI
4. To return a failed drive to 8e6 or to order additional replacement drives, please call 8e6 Technical Support

***NOTE**: For information on troubleshooting RAID, refer to Appendix F: RAID Maintenance.*

X Strikes Blocking

X Strikes Blocking window

The X Strikes Blocking window displays when X Strikes Blocking is selected from the navigation panel. This feature lets a global administrator set criteria for blocking a user's access to “unacceptable” Internet sites and locking a user’s workstation, after the user makes a specified (“X”) number of attempts to such sites. “‘Unacceptable’ Internet sites” pertain to sites included in categories that are blocked in a user’s profile.

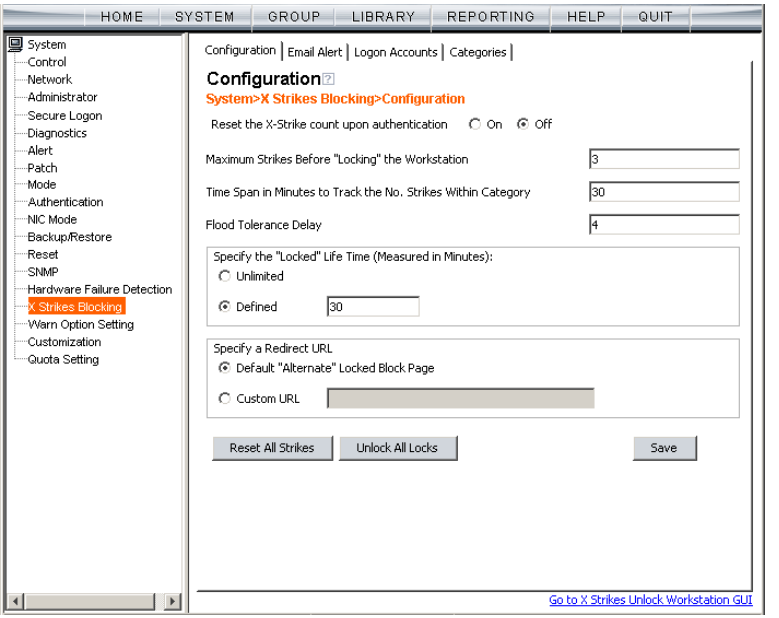


Fig. 2:1-74 X Strikes Blocking window, Configuration tab

***NOTE**: X Strikes Blocking settings are effective only for filtering profiles with the X Strikes Blocking filter option enabled. (See Filter Options in the Group screen section for information on setting up the X Strikes Blocking filter option.)*

Configuration

Set up Blocking Criteria

1. At **Reset the X-Strike count upon authentication**, “Off” is selected by default. To have all strikes reset before an end user is authenticated, click “On”.
2. Enter the **Maximum Strikes Before “Locking” the Workstation**. This is the number of attempts a user can make to access an unacceptable site before that user is prevented from using the Internet. The default is *5*, and the maximum limit is 1000.
3. Enter the **Time Span in Minutes to Track the No. of Strikes Within Category**. This is the amount of time between a given user's first strike and the strike that will lock out that user from his/her Internet access. The default setting is *5*, and the maximum limit is 1440 minutes (24 hours).
4. Enter the number of seconds for the **Flood Tolerance Delay**, which is the maximum amount of time that will elapse before a user who accesses the same inappropriate URL will receive another strike. The default setting and the maximum limit is *4* seconds.
5. **Specify the “Locked” Life Time (Measured in Minutes)**, which is the number of minutes a user's workstation will be locked. Choose either “Unlimited”, or “Defined”.

   If “Defined” is selected, enter the number of minutes in the text box. The default setting is *5.*
6. **Specify a Redirect URL** to be used when the end user is locked out from his/her workstation. By default, “Default "Alternate" Locked Block Page” is selected, indicating that the standard lock out block page will display.

To specify a different page, click “Custom URL” and enter the URL in the text box.

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

Reset All Workstations

The following buttons can be clicked to reset workstations:

- Click **Reset All Strikes** to remove all strikes from all workstations, and to unlock all locked workstations.
- Click **Unlock All Locks** to remove locks on all locked workstations.

Lock Page

A user who receives the final strike that locks him/her out the workstation will see the following lock page display on the screen:

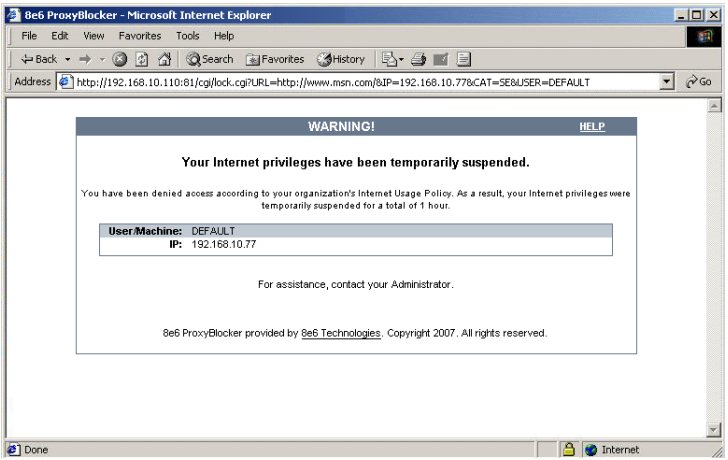


Fig. 2:1-75 Sample lock page

The text informs the user: “Your Internet privileges have been temporarily suspended. For assistance, contact your Administrator.”

The following information might also display in the lock page: “You have been denied access according to your organization's Internet Usage Policy. As a result, your Internet privileges were temporarily suspended for a total of ‘X’ (amount of time),” in which ‘X’ represents the number of minutes/hours the user will be locked out from Internet usage on that workstation.

***NOTE**: This message may differ, depending on whether or not alternate text and settings were made in the Lock Page Customization window and the Common Customization window. (See Customization in this chapter for more information.)*

The user will not be able to access the Internet from that workstation until the Defined amount of time specified in the “Locked” Life Time field passes, or unless an authorized staff member manually unlocks that user’s workstation (see Go to X Strikes Unlock Workstation GUI in this section).

Overblocking or Underblocking

***NOTES**: In order to prevent overblocking, unacceptable Internet images/links are allowed to pass by if they display within the four-second tolerance time range of a given strike. Thus, only one strike will count against a user who visits a Web page embedded with multiple, unacceptable images/links, if these images/links load within four seconds of that strike. Banners and IM/P2P sites included in the library are white listed and do not count as strikes.*

If users are receiving too many strikes or too few strikes within a given period of time, you may need to modify the configuration settings.

Sample Settings:

- Maximum strikes = ***5***
- Time span for the maximum number of strikes = ***5*** minutes

Within a five-minute period, if a user accesses five sites that contain blocked material, that user will be locked out of his/

her workstation for five minutes. However, since the tolerance timer is set at four seconds, a user could potentially receive five strikes within 16 seconds if he/she accesses a page with multiple, inappropriate images and/or links that load on each page within four seconds. In this scenario, the first strike would be delivered at 0 seconds, the second at 4 seconds, the third at 8 seconds, the fourth at 12 seconds, and the fifth at 16 seconds.

If the configuration settings for this example overblock too many users too frequently:

- the time span for the maximum number of strikes may need to be increased
- the maximum number of strikes may need to be increased

If these configuration settings do not block users often enough

- the time span for the maximum number of strikes may need to be reduced
- the maximum number of strikes may need to be reduced

Email Alert

Click the Email Alert tab to display Email Alert:

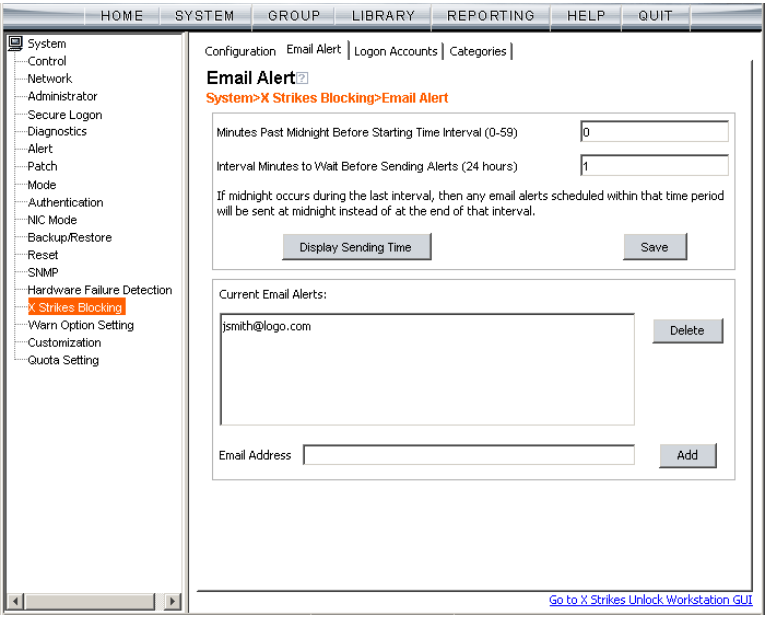


Fig. 2:1-76 X Strikes Blocking window, Email Alert tab

Set up Email Alert Criteria

1. In the **Minutes Past Midnight Before Starting Time Interval (0-59)** field, enter the number of minutes past midnight that a locked workstation email alert will first be sent to the specified recipient(s).
2. **In the Interval Minutes to Wait Before Sending Alerts (24 hours)** field, enter the number of minutes within the 24-hour period that should elapse between email alerts.

   For example, by entering ***300*** in this field and ***30*** in the previous field, if there are any email alerts they will be sent at 5:30:00 AM, 10:30:00 AM, 3:30:00 PM, 8:30:00 PM, and at midnight when the time interval is reset.

To check the time(s) the email alert is scheduled to occur, click the **Display Sending Time** button to open The Daily Schedule pop-up window that shows the alert time schedule in the (HH:MM:SS) format:

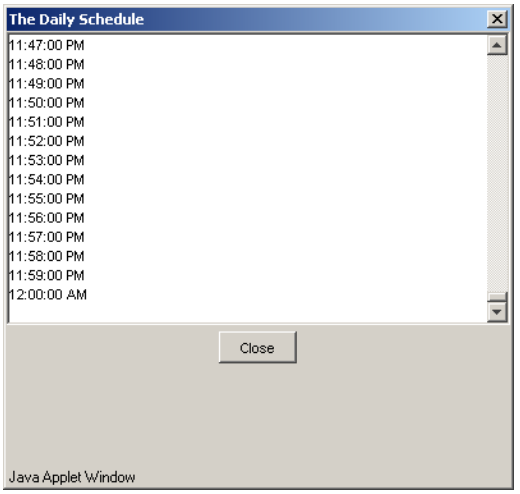


Fig. 2:1-77 The Daily Schedule pop-up window

Click **Close** to close the pop-up window.

3. Click **Save** to save the field entries.

Set up Email Alert Recipients

1. Enter the **Email Address** of an individual who will receive locked workstation email alerts.
2. Click **Add** to include the email address in the Current Email Alerts list box.

***NOTE**: The maximum number of email alert recipients is 50. If more than 50 recipients need to be included, 8e6 recommends setting up an email alias list for group distribution.*

Remove Email Alert Recipients

1. Select the email address(es) from the Current Email Alerts list box.
2. Click **Delete** to remove the email address(es) from list.

Logon Accounts

Click the Logon Accounts tab to display Logon Accounts:

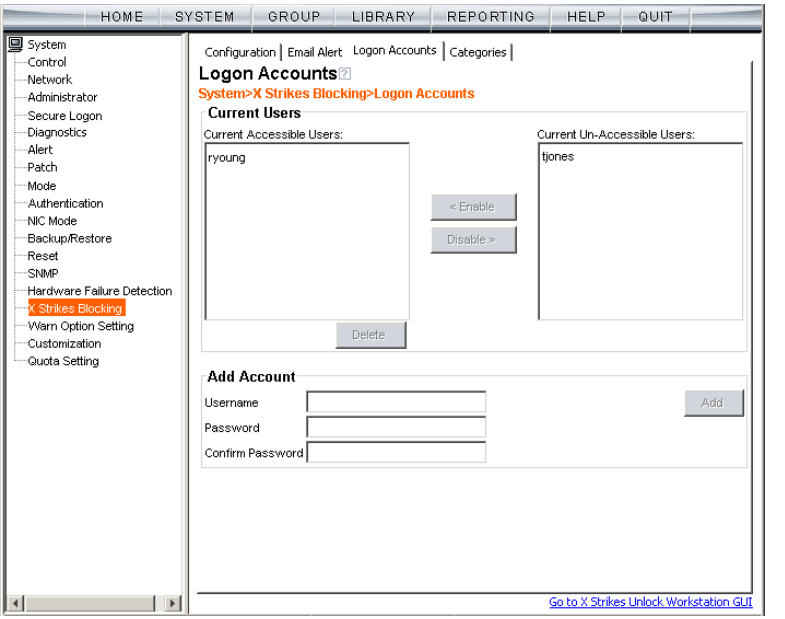


Fig. 2:1-78 X Strikes Blocking window, Logon Accounts tab

Set up Users Authorized to Unlock Workstations

1. Enter the **Username** of a staff member who is authorized to unlock workstations.
2. Enter the user's password in the **Password** and **Confirm Password** fields, using eight to 20 characters and at least one alpha character, one numeric character, and one special character. The password is case sensitive.

3. Click **Add** to include the username in the Current Accessible Users list box.

***NOTE**: When an authorized staff member is added to this list, that username is automatically added to the Current Un-Accessible Users list box in the Logon Accounts tab of the Real Time Probe window.*

Deactivate an Authorized Logon Account

To deactivate an authorized user's account:

1. Select the username from the Current Accessible Users list box.
2. Click **Disable** to move the username to the Current Un-Accessible Users list box.

Delete a Logon Account

To delete a user's account:

1. Select the username from the Current Accessible Users list box.
2. Click **Delete**.

***WARNING**: By deleting a logon account, in addition to not being able to unlock workstations, that user also will be removed from the list of users authorized to create real time probes. (See Chapter 4: Reporting screen, Real Time Probe for information on setting up and using real time probes.)*

Categories

Click the Categories tab to display Categories:

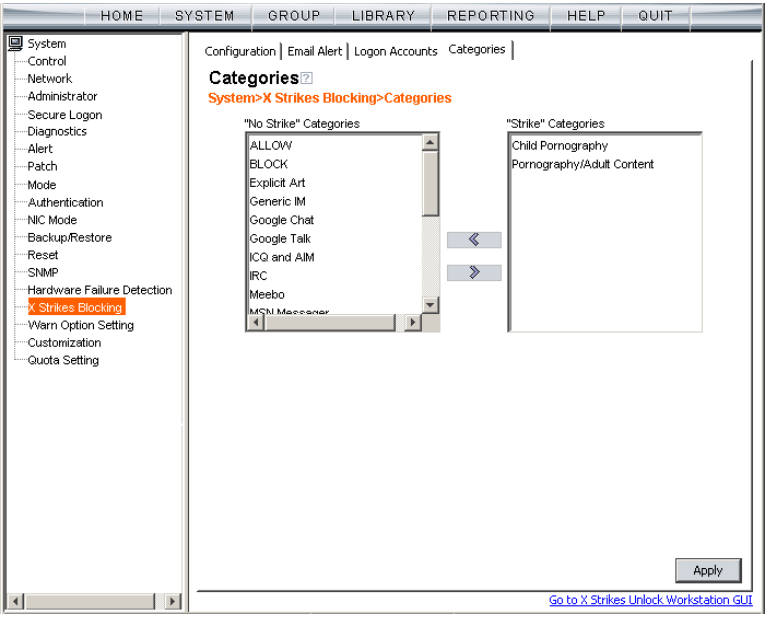


Fig. 2:1-79 X Strikes Blocking window, Categories tab

Set up Categories to Receive Strikes or No Strikes

1. Select library categories from the “No Strike” Categories list box.
2. Click the right arrow (>) to move the selected library categories to the “Strike” Categories list box.

***TIP**: Use the left arrow (<) to move selected “Strike” Categories to the “No Strike” Categories list box.*

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

***NOTE**: Library categories in the “Strike” Categories list box will only be effective for filtering profiles with the X Strikes Blocking Filter Option enabled.*

Go to X Strikes Unlock Workstation GUI

When the global administrator clicks **Go to X Strikes Unlock Workstation GUI**, either the Re-login window or the X Strikes Unlock Workstation pop-up window opens.

Re-login window

The Re-login window opens if the user's session needs to be validated:

Fig. 2:1-80 Re-login window

1. Enter your **Username**.
2. Enter your **Password**.
3. Click **OK** to close the Re-login window and to re-access the ProxyBlocker console.

X Strikes Unlock Workstation

The following information displays in the X Strikes Unlock Workstation pop-up window: IP Address, User Name, and Expire Date/Time of currently locked workstations.

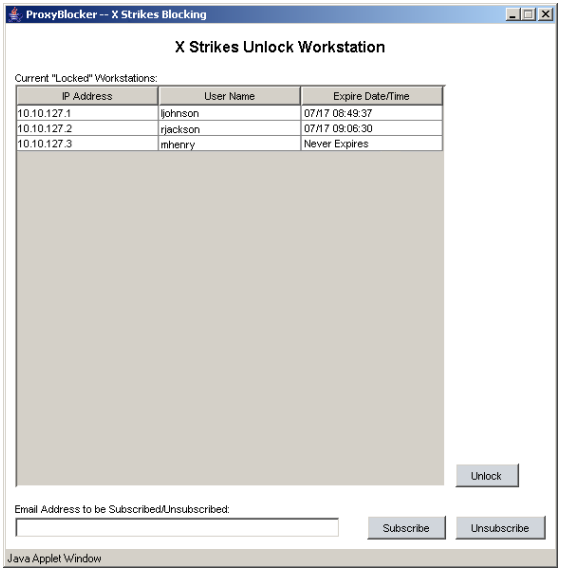


Fig. 2:1-81 X Strikes Unlock Workstation window

***NOTE**: An authorized staff member can click a link in an email alert, or type in **http://x.x.x.x:88/XStrike.html** in the address field of a browser window—in which "x.x.x.x" is the IP address of the ProxyBlocker—to view locked workstation criteria.*

Unlock a Workstation

To unlock a specified workstation:

1. Select that workstation from the grid.
2. Click **Unlock**.

Set up an Email Address to Receive Alerts

To send locked workstation information to a designated administrator:

1. Enter the email address in the **Email Address to be Subscribed/Unsubscribed** text box.
2. Click **Subscribe**.

Remove an Email Address from the Alert List

To remove an administrator's email address from the notification list:

1. Enter the email address in the **Email Address to be Subscribed/Unsubscribed** text box.
2. Click **Unsubscribe**.

Close the Pop-up Window

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

Warn Option Setting

Warn Option Setting window

The Warn Option Setting window displays when Warn Option Setting is selected from the navigation panel. This feature lets a global administrator specify the number of minutes for the interval of time in which a warning page will redisplay for the end user who accesses a URL in a library category with a Warn setting for his/her profile. If the end user accesses another URL in a category with a Warn setting, the warning page displays again and will continue to redisplay for the interval of time specified, as long as the end user's browser is open to any URL with a Warn setting.

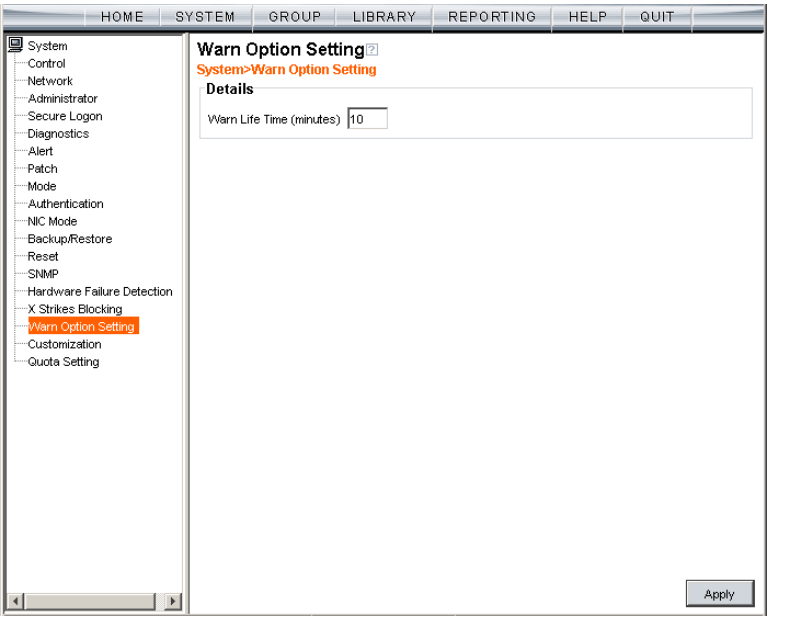


Fig. 2:1-82 Warn Option Setting window

***NOTE**: See the Warn Page Customization window in this chapter for information on customizing text in the warning page that displays for end users.*

Specify the Interval for Re-displaying the Warn page

1. In the **Warn Life Time (minutes)** field, by default *10* displays. Enter the number of minutes (1-480) to be used in the interval for re-displaying the warning page for the end user.
2. Click **Apply** to enable your setting.

Customization

Customization includes options to customize settings for HTML pages that display for end users who execute a command that triggers the associated pop-up window to open. Click the Customization link to view a menu of sub-topics: Common Customization, Authentication Form, Lock Page, Block Page, Warn Page, Profile Control, Quota Block Page, Quota Notice Page.

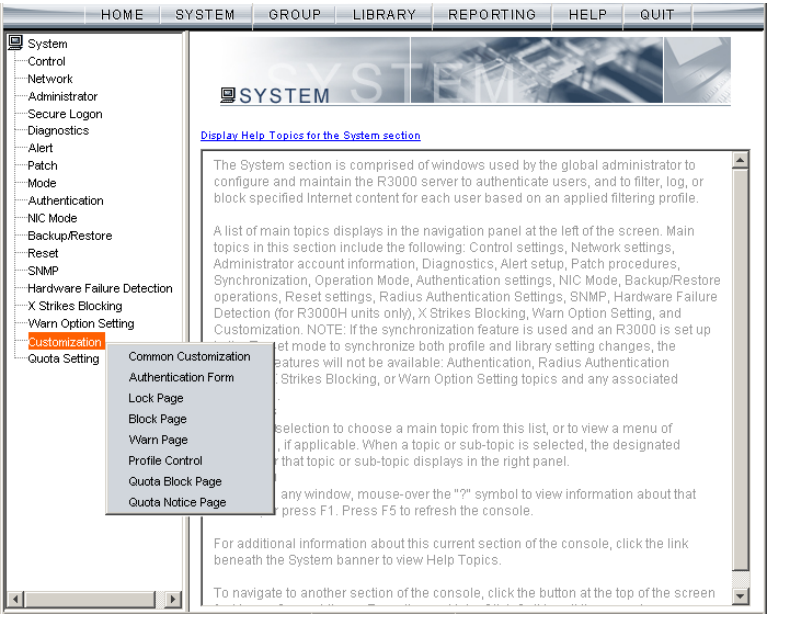


Fig. 2:1-83 System screen, Customization menu

***NOTE**: Refer to the 8e6 ProxyBlocker Authentication User Guide for information on using the Authentication Form Customization window.*

Common Customization window

The Common Customization window displays when Common Customization is selected from the Customization menu. This window is used for specifying elements to be included in block, lock, profile, and warning pages, and/or the authentication request form the end user will see.

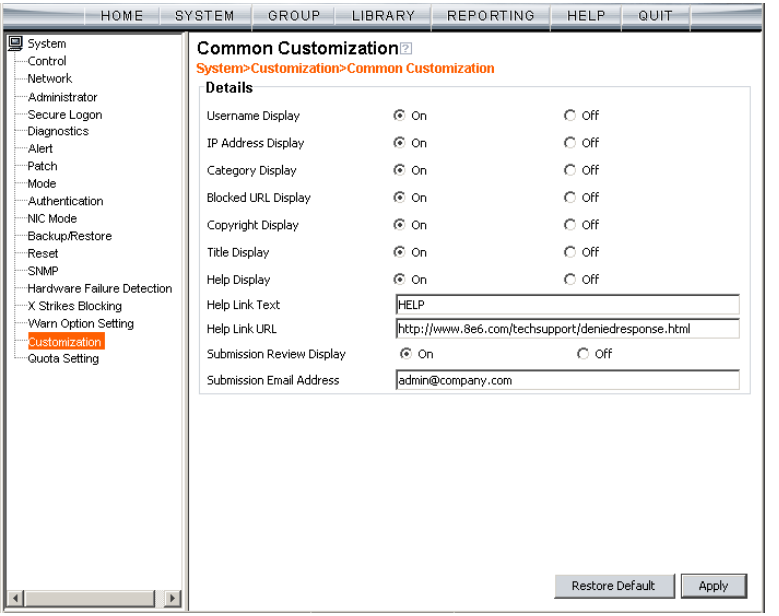


Fig. 2:1-84 Common Customization window

By default, in the Details frame all elements are selected to display in the HTML pages, the Help link points to the FAQs page on 8e6's public site that explains why access was denied, and a sample email address is included for administrator contact information. These details can be modified, as necessary.

Enable, Disable Features

1. Click “On” or “Off” to enable or disable the following elements in the HTML pages, and make entries in fields to display customized text, if necessary:

   - Username Display - if enabled, displays “User/Machine” followed by the end user’s username in block and lock pages
   - IP Address Display - if enabled, displays “IP” followed by the end user’s IP address in block and lock pages
   - Category Display - if enabled, displays “Category” followed by the long name of the blocked category in block pages
   - Blocked URL Display - if enabled, displays “Blocked URL” followed by the blocked URL in block pages
   - Copyright Display - if enabled, displays 8e6 Proxy-Blocker copyright information at the footer of block and lock pages, and the authentication request form
   - Title Display - if enabled, displays the title of the page in the title bar of the block and lock pages, and the authentication request form
   - Help Display - if enabled, displays the specified help link text in block and lock pages, and the authentication request form. The associated URL (specified in the Help Link URL field described below) is accessible to the end user by clicking the help link.

***NOTE**: If enabling the Help Display feature, both the Help Link Text and Help Link URL fields must be populated.*

   - **Help Link Text** - By default, *HELP* displays as the help link text. Enter the text to display for the help link.

- **Help Link URL** - By default, *http://www.8e6.com/tech-support/deniedresponse.html* displays as the help link URL. Enter the URL to be used when the end user clicks the help link text (specified in the Help Link Text field).
- Submission Review Display - if enabled, displays in block pages the email address of the administrator to receive requests for a review on sites the end users feel are incorrectly blocked. The associated email address (specified in the Submission Email Address field described below) is accessible to the end user by clicking the **click here** link.

***NOTE**: If enabling the Submission Review Display feature, an email address entry of the designated administrator in your organization must be made in the Submission Email Address field.*

- **Submission Email Address** - By default, *admin @company.com* displays in block pages as the email address of the administrator to receive feedback on content the end user feels has been incorrectly blocked. Enter the global administrator's email address.

2. Click **Apply** to save your entries.

***TIP**: Click **Restore Default** and then click **Apply** to revert to the default settings in this window.*

Lock Page Customization window

The Lock Page Customization displays when Lock Page is selected from the Customization menu. This window is used with the X Strikes Blocking feature, and lets you customize text in the lock page end users will see when attempting to access Internet content blocked for their profiles, and their workstations are currently locked. Entries saved in this window display in the customized lock page, if these features are also enabled in the Common Customization window, and the X Strikes Blocking feature is enabled.

***NOTE**: See X Strikes Blocking window in this chapter for information on using the X Strikes Blocking feature.*

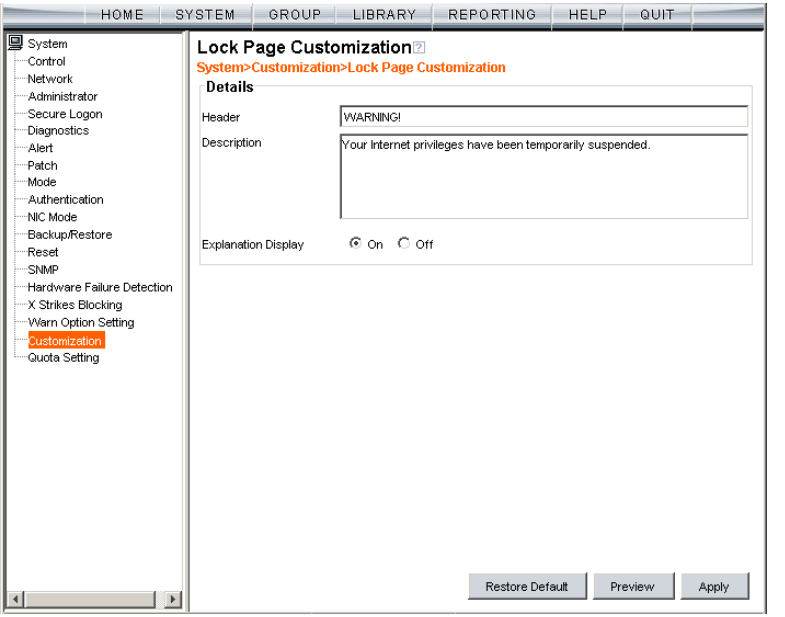


Fig. 2:1-85 Lock Page Customization window

***TIP**: An entry in any of the fields in this window is optional.*

Edit Entries, Setting

1. Make an entry in any of the following fields:
   - In the **Header** field, enter a static header to be displayed at the top of the lock page.
   - In the **Description** field, enter a static text message to be displayed beneath the lock page header.

   Any entries made in these fields will display centered in the customized lock page, using the Arial font type.
2. At the **Explanation Display** field, by default “On” is selected. This setting displays the reason the workstation is locked beneath the text from the Description field. Click “Off” to not have the explanatory text display in the lock page.
3. Click **Apply**.

***TIP**: Click **Restore Default** and then click **Apply** to revert to the default settings in this window.*

Preview Sample Lock Page

1. Click **Preview** to launch a separate browser window containing a sample customized lock page, based on entries saved in this window and in the Common Customization window:

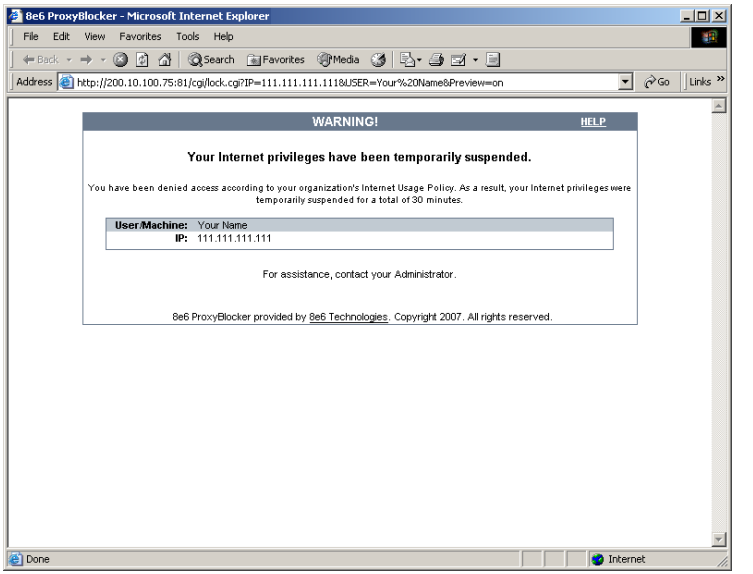


Fig. 2:1-86 Sample Customized Lock Page

By default, the following data displays in the User/ Machine frame:

- **User/Machine** field - The username displays for the NT/LDAP user. This field is blank for the IP group user.
- **IP** field - The user's IP address displays.

By default, the following standard links are included in the lock page:

- **HELP** - Clicking this link takes the user to 8e6's Technical Support page that explains why access to the site or service may have been denied.

- **8e6 Technologies** - Clicking this link takes the user to 8e6's Web site.

2. Click the "X" in the upper right corner of the window to close the sample customized lock page.

***TIP**: If necessary, make edits in the Lock Page Customization window or the Common Customization window, and then click **Preview** in this window again to view a sample lock page.*

Block Page Customization window

The Block Page Customization window displays when Block Page Customization is selected from the Customization menu. This feature is used if you want to display customized text and include a customized link in the block page end users will see when attempting to access Internet content blocked for their profiles. Entries saved in this window display in the customized block page, if these features are also enabled in the Common Customization window.

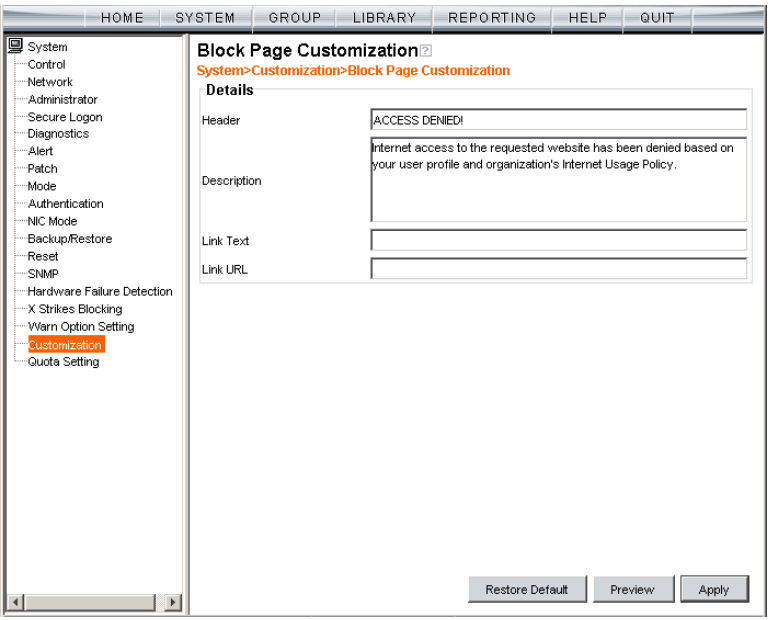


Fig. 2:1-87 Block Page Customization window

***NOTE**: See Appendix C: Create a Custom Block Page for information on creating a customized block page using your own design.*

***TIP**: An entry in any of the fields in this window is optional, but if an entry is made in the Link Text field, a corresponding entry must also be made in the Link URL field.*

Add, Edit Entries

1. Make an entry in any of the following fields:
   - In the **Header** field, enter a static header to be displayed at the top of the block page.
   - In the **Description** field, enter a static text message to be displayed beneath the block page header.
   - In the **Link Text** field, enter text for the link's URL, and in the **Link URL** field, enter the corresponding hyperlink in plain text using the *http://* or *https://* syntax.

   Any entries made in these fields will display centered in the customized block page, using the Arial font type.
2. Click **Apply**.

***TIP**: Click **Restore Default** and then click **Apply** to revert to the default settings in this window.*

Preview Sample Block Page

1. Click **Preview** to launch a separate browser window containing a sample customized block page, based on entries saved in this window and in the Common Customization window:

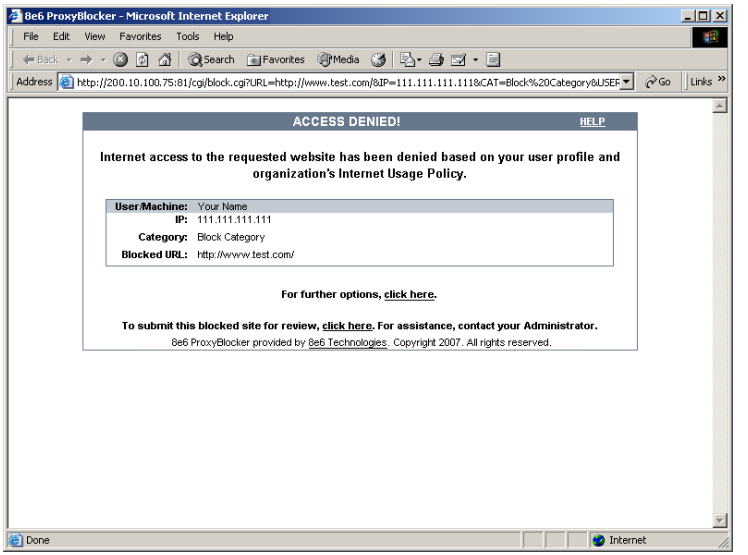


Fig. 2:1-88 Sample Customized Block Page

By default, the following data displays in the User/ Machine frame:

- **User/Machine** field - The username displays for the NT/LDAP user. This field is blank for the IP group user.
- **IP** field - The user's IP address displays.
- **Category** field - The name of the library category that blocked the user's access to the URL displays. If the content the user attempted to access is blocked by an Exception URL, "Exception" displays instead of the library category name.
- **Blocked URL** field - The URL the user attempted to access displays.

By default, the following standard links are included in the block page:

- **HELP** - Clicking this link takes the user to 8e6's Technical Support page that explains why access to the site or service may have been denied.
- **8e6 Technologies** - Clicking this link takes the user to 8e6's Web site.

By default, these links are included in the block page under the following conditions:

- **For further options, click here.** - This phrase and link is included if any option was selected at the Re-authentication Options field in the Block Page Authentication window. Clicking this link takes the user to the Options window.

***NOTE**: See the Options page in the Block Page Authentication window sub-section for information on options that display in the Options window.*

- **To submit this blocked site for review, click here.** - This phrase and link is included if an email address was entered in the Submission Email Address field in the Common Customization window. Clicking this link launches the user's default email client. In the composition window, the email address from the Submission Email Address field populates the "To" field. The user's message is submitted to the global administrator.

2. Click the "X" in the upper right corner of the window to close the sample customized block page.

***TIP**: If necessary, make edits in the Block Page Customization window or the Common Customization window, and then click **Preview** in this window again to view a sample block page.*

Warn Page Customization window

The Warn Page Customization window displays when Warn Page is selected from the Customization menu. This window is used with the Warn Option Setting feature, and lets you customize text in the pop-up window end users will see if attempting to access a URL in a library category set up with a Warn setting for his/her profile. Entries saved in this window display in the warning page, if these features are also enabled in the Common Customization window, and the Warn setting is applied to any library category or category group.

***NOTE**: See Warn Option Setting window in this chapter for more information about this feature.*

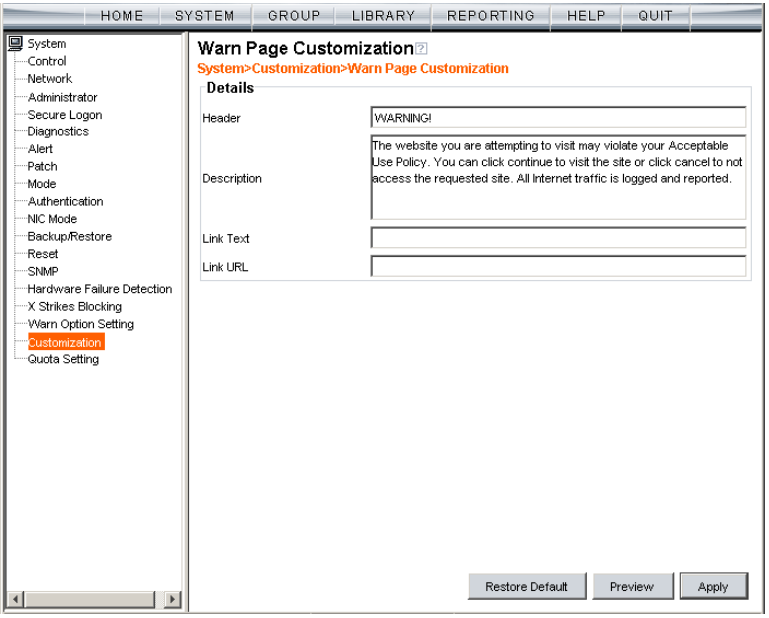


Fig. 2:1-89 Warn Page Customization window

***TIP**: An entry in any of the fields in this window is optional.*

Add, Edit Entries

1. Make an entry in any of the following fields:
   - In the **Header** field, enter a static header to be displayed at the top of the warning page.
   - In the **Description** field, enter a static text message to be displayed beneath the warning page header.
   - In the **Link Text** field, enter text for the link's URL, and in the **Link URL** field, enter the corresponding hyper-link in plain text using the *http://* or *https://* syntax.

   Any entries made in these fields will display centered in the customized warning page, using the Arial font type.
2. Click **Apply**.

***TIP**: Click **Restore Default** and then click **Apply** to revert to the default settings in this window.*

Preview Sample Warning Page

1. Click **Preview** to launch a separate browser window containing a sample customized warning page, based on entries saved in this window and in the Common Customization window:

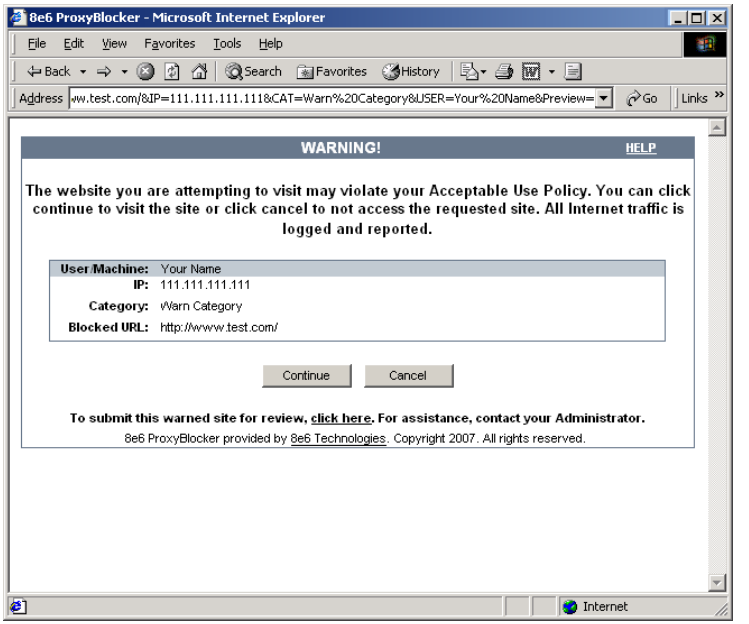


Fig. 2:1-90 Sample Customized Warning Page

By default, the following data displays in the User/ Machine frame:

- **User/Machine** field - The username displays for the NT/LDAP user. This field is blank for the IP group user.
- **IP** field - The user's IP address displays.
- **Category** field - The name of the library category that warned the user about accessing the URL displays.
- **Blocked URL** field - The URL the user attempted to access displays.

By default, the following standard links are included in the warning page:

- **HELP** - Clicking this link takes the user to 8e6's Technical Support page that explains why access to the site or service may have been denied.
- **8e6 Technologies** - Clicking this link takes the user to 8e6's Web site.

The following buttons are included in the warning page:

- **Continue** - Clicking this button closes the warning page and takes the user to the URL he/she requested. The number of minutes specified in the Warn Option Setting window determines when/if this warning page will redisplay for the user. If the user has his/her browser open to that URL for the number of minutes—or more—specified for the time interval, this warning page will redisplay, and the user must click this button once more in order to continue accessing the URL.

***NOTE**: If using the Real Time Probe feature, in the Real Time Information box the Filter Action column displays "Warn" for the first time the user saw the warning window and clicked Continue, and "Warned" for each subsequent time the warning window opened for the user and he/she clicked Continue.*

- **Cancel** - Clicking this button returns the user to the previous URL.

By default, this link is included in the warning page under the following conditions:

- **To submit this warned site for review, click here.** - This phrase and link is included if an email address was entered in the Submission Email Address field in the Common Customization window. Clicking this link launches the user's default email client. In the composition window, the email address from the Submission Email Address field populates the "To" field. The user's message is submitted to the global administrator.

2. Click the “X” in the upper right corner of the window to close the sample customized warning page.

***TIP**: If necessary, make edits in the Warn Page Customization window or the Common Customization window, and then click **Preview** in this window again to view a sample warning page.*

Profile Control window

The Profile Control window displays when Profile Control is selected from the Customization menu. This window is used with the Override Account feature, and lets you customize text in the pop-up window end users with override accounts will see when logging into their override accounts. Such accounts give authorized users access to Internet content blocked for other end users. Entries saved in this window display in the profile control pop-up window, if these features are also enabled in the Common Customization window, and override accounts are set up for designated end users.

***NOTE**: See Override Account window in the Group section for more information about this feature.*

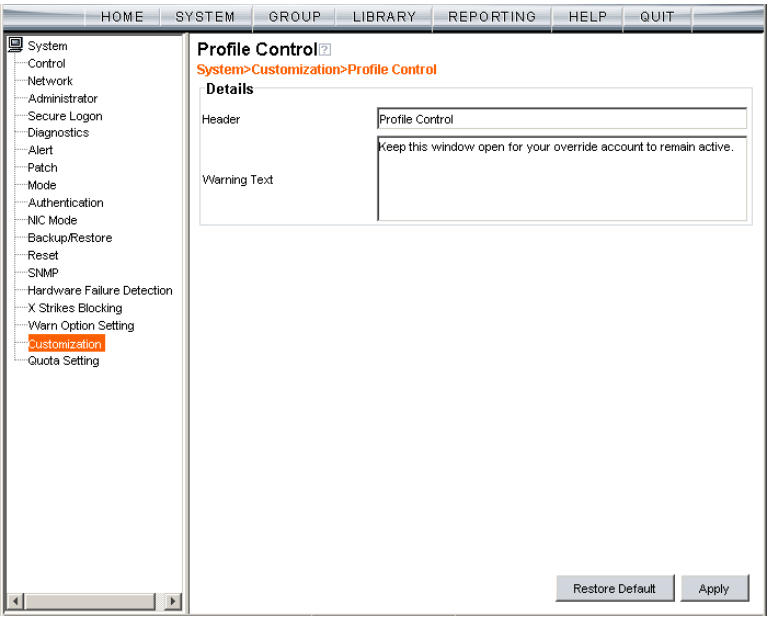


Fig. 2:1-91 Profile Control window

***TIP**: An entry in any of the fields in this window is optional.*

Edit Entries

1. Make an entry in any of the following fields:
   - In the **Header** field, enter a static header to be displayed at the top of the profile control pop-up window.
   - In the **Warning Text** field, enter a static text message to be displayed at the bottom of the pop-up window.
2. Click **Apply**.

***TIP**: Click **Restore Default** and then click **Apply** to revert to the default settings in this window.*

***NOTE**: For a sample profile control pop-up window, see Option 3 from the Options page section of the Block Page Authentication window.*

Quota Block Page Customization window

The Quota Block Page Customization window displays when Quota Block Page is selected from the Customization menu. This window is used for making customizations to the quota block page the end user will see if he/she has a quota time limit set for a passed category in his/her profile and has attained or exceeded that limit.

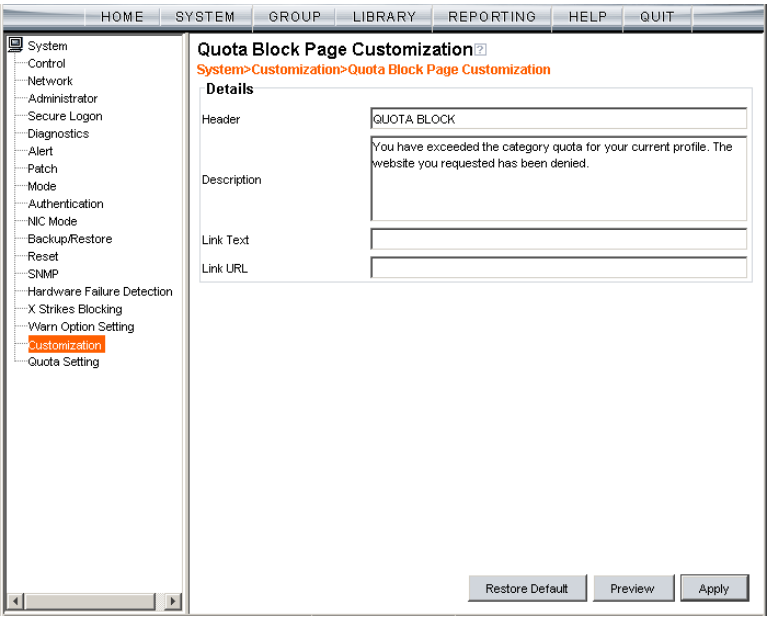


Fig. 2:1-92 Quota Block Page Customization window

***TIP**: An entry in any of the fields in this window is optional.*

***NOTE**: For more information about quotas, see the Quota Setting window in this chapter.*

Add, Edit Entries

1. Make an entry in any of the following fields:
   - In the **Header** field, enter a static header to display at the top of the quota block page.
   - In the **Description** field, enter a static text message to be displayed beneath the header.
   - In the **Link Text** field, enter text for the link's URL, and in the **Link URL** field, enter the corresponding hyper-link in plain text using the *http://* or *https://* syntax.

   Any entries made in these fields will display centered in the customized quota block page, using the Arial font type.
2. Click **Apply**.

***TIP**: Click **Restore Default** and then click **Apply** to revert to the default settings in this window.*

Preview Sample Quota Block Page

1. Click **Preview** to launch a separate browser window containing a sample customized quota block page, based on entries saved in this window and in the Common Customization window:

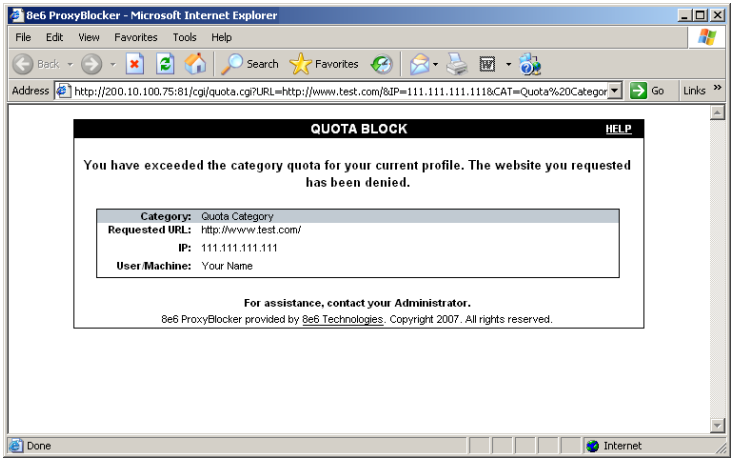


Fig. 2:1-93 Sample Customized Quota Block Page

By default, the following data displays in the Category frame:

- **Category** field - The name of the library category that blocked the user from accessing the URL displays.
- **Requested URL** field - The URL the user attempted to access displays.
- **IP** field - The user's IP address displays.
- **User/Machine** field - The username displays for the NT/LDAP user. This field is blank for the IP group user.

By default, the following standard links are included in the quota block page:

- **HELP** - Clicking this link takes the user to 8e6's Technical Support page that explains why access to the site or service may have been denied.

- **8e6 Technologies** - Clicking this link takes the user to 8e6's Web site.

2. Click the "X" in the upper right corner of the window to close the sample customized quota block page.

***TIP**: If necessary, make edits in the Quota Block Page Customization window or the Common Customization window, and then click **Preview** in this window again to view a sample quota block page.*

Quota Notice Page Customization window

The Quota Notice Page Customization window displays when Quota Notice Page is selected from the Customization menu. This window is used for making customizations to the quota notice page the end user will see if he/she has a quota time limit set for a passed category in his/her profile and has used 75 percent of the allotted time in that category.

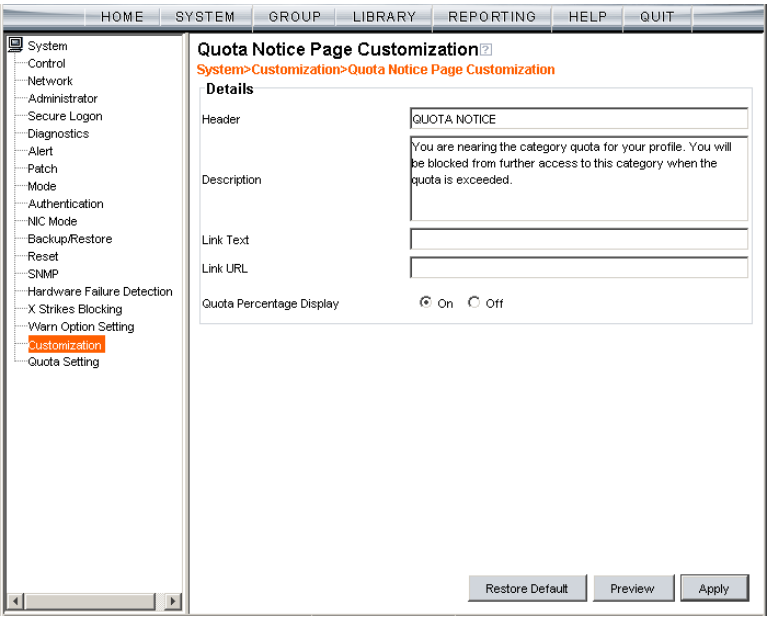


Fig. 2:1-94 Quota Notice Page Customization window

***TIP**: An entry in any of the fields in this window is optional.*

***NOTE**: For more information about quotas, see the Quota Setting window in this chapter.*

Add, Edit Entries

1. Make an entry in any of the following fields:
   - In the **Header** field, enter a static header to display at the top of the quota notice page.
   - In the **Description** field, enter a static text message to be displayed beneath the header.
   - In the **Link Text** field, enter text for the link's URL, and in the **Link URL** field, enter the corresponding hyper-link in plain text using the *http://* or *https://* syntax.

   Any entries made in these fields will display centered in the customized quota notice page, using the Arial font type.
2. By default, the **Quota Percentage Display** is enabled, indicating the percentage of quota used by the individual will display in the quota notice page. Click “Off” to not display this information in the quota notice page.
3. Click **Apply**.

***TIP**: Click **Restore Default** and then click **Apply** to revert to the default settings in this window.*

Preview Sample Quota Notice Page

1. Click **Preview** to launch a separate browser window containing a sample customized quota notice page, based on entries saved in this window and in the Common Customization window:

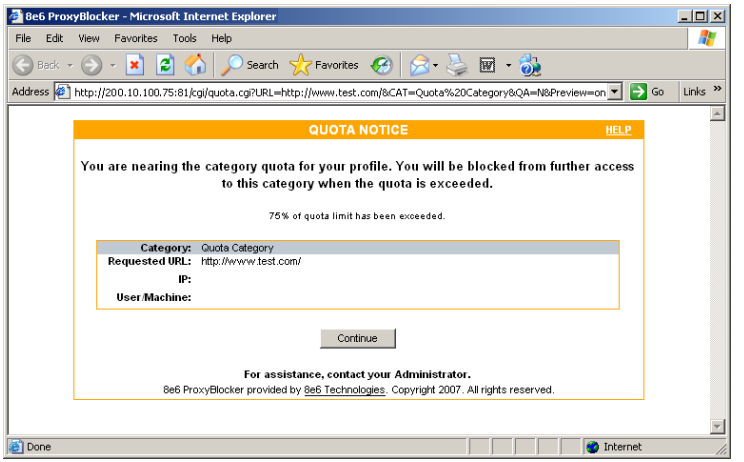


Fig. 2:1-95 Sample Customized Quota Notice Page

By default, the following data displays in the Category frame:

- **Category** field - The name of the library category containing a URL the user accessed—that triggered the quota notice—displays.
- **Requested URL** field - The URL the user accessed—that triggered the quota notice—displays.
- **IP** field - The user's IP address displays.
- **User/Machine** field - The username displays for the NT/LDAP user. This field is blank for the IP group user.

By default, the following standard links are included in the quota notice page:

- **HELP** - Clicking this link takes the user to 8e6's Technical Support page that explains why access to the site or service may have been denied.
- **8e6 Technologies** - Clicking this link takes the user to 8e6's Web site.

The following button is included in the quota notice page:

- **Continue** - Clicking this button closes the quota notice page and takes the user to the URL he/she requested.

2. Click the "X" in the upper right corner of the window to close the sample customized quota notice page.

***TIP**: If necessary, make edits in the Quota Block Page Customization window or the Common Customization window, and then click **Preview** in this window again to view a sample quota block page.*

Quota Setting

Quota Setting window

The Quota Setting window displays when Quota Setting is selected from the navigation panel. This window lets a global administrator configure URL hits that—along with quotas specified in filtering profiles—determine when a user will be blocked from further accessing URLs in a library group/category. This window is also used for resetting quotas so that users who have maxed-out their quota time will regain access to a library group/category with a quota time limit.

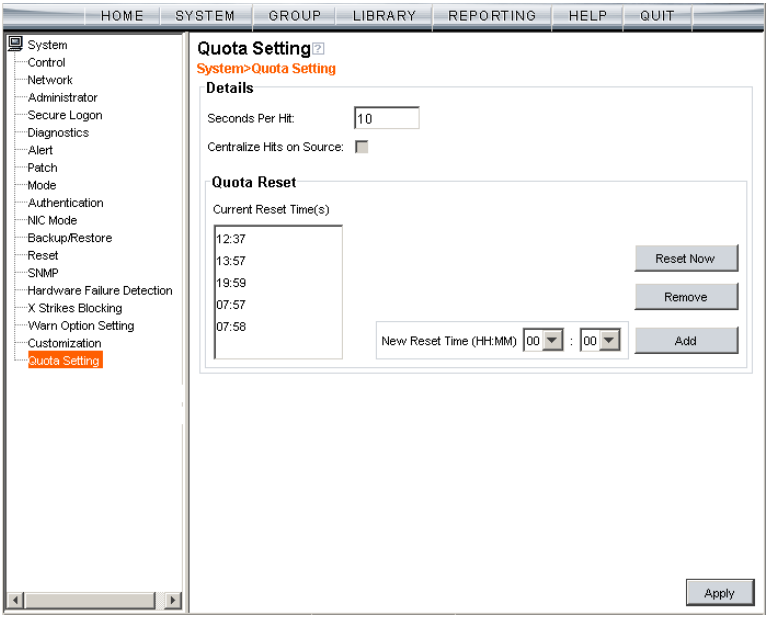


Fig. 2:1-96 Quota Setting window

***TIP**: After making all configuration settings in this window during this session, click **Apply**.*

Configure Quota Hit Settings

Enter the number of **Seconds Per Hit** to indicate how much time will be applied towards a "hit" (URL access) in any category with a quota. The default is *10* seconds per hit. The entry in this field combines with the minutes entered in the quota from the filtering profile to determine the amount of time the end user can access URLs in the specified passed library group/category in that profile.

A quota can be set for an amount of time ranging from one minute to 1439 minutes (one day minus one minute). A hit can be set for an amount of time ranging from one second to 3600 seconds (one hour).

As an example of how a quota works in conjunction with hits, if a quota is set to 10 minutes and the number of seconds per hit is set to 10 seconds, then the user will be blocked from accessing URLs in the library group/category when 60 hits are made to that category—i.e. 600 seconds (10 minutes) divided by 10 seconds.

***NOTE**: The Centralize Hits on Source field is greyed-out since all hits are centralized on this unit.*

***TIP**: After making all configuration settings in this window during this session, click **Apply**.*

Reset Quotas

Quotas are automatically reset at midnight, but also can be manually reset on demand or scheduled to be reset at specific times each day.

Reset Quotas Now

Click **Reset Now** to reset all quotas to zero ("0"). Users currently blocked from accessing URLs because of a quota time limit will now be able to access URLs in any library/ group category with a quota.

Set up a Schedule to Automatically Reset Quotas

A schedule can be set up to reset all quotas at the appointed hour(s) / minute(s) each day.

1. At the **New Reset Time (HH:MM)** field:
   - Select the hour at which the quota will be reset ("00" - "23")
   - Select the minute at which the quota will be reset ("00" - "59")
2. Click **Add** to include this reset time in the Current Reset Time(s) list box.

***TIP**: Repeat steps 1 and 2 for each quota reset time to be scheduled. After making all configuration settings in this window during this session, click **Apply**.*

Delete a Quota Reset Time from the Schedule

1. Select the quota reset time from the Current Reset Time(s) list box.
2. Click **Remove** to remove the quota reset time from the list box.

***TIP**: After making all configuration settings in this window during this session, click **Apply**.*

Quota Notice page

When the end user has spent 75 percent of time in a quota-restricted library group/category, the quota notice page displays:

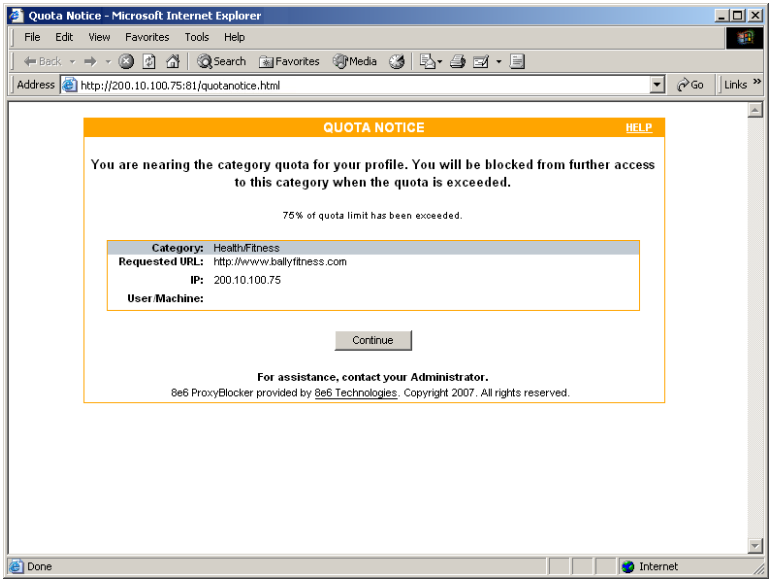


Fig. 2:1-97 Sample Quota Notice Page

By default, the following fields display:

- **Category** field - Name of the library category with the most hits.
- **Requested URL** field - The URL that triggered the Quota Notice page.
- **IP** field - The end user's IP address.
- **User/Machine** field - The username displays for the NT/LDAP user. This field is blank for the IP group user.

By default, the following standard links are included in the quota notice page:

- **HELP** - Clicking this link takes the user to 8e6's Technical Support page that explains why access to the site may have been denied.
- **8e6 Technologies** - Clicking this link takes the user to 8e6's Web site.

The end user can decide whether or not to access the requested URL. By clicking **Continue**, the user is redirected to the original requested site.

Quota Block page

When the end user has spent 100 percent of time in a quota-restricted library group/category, the quota block page displays:

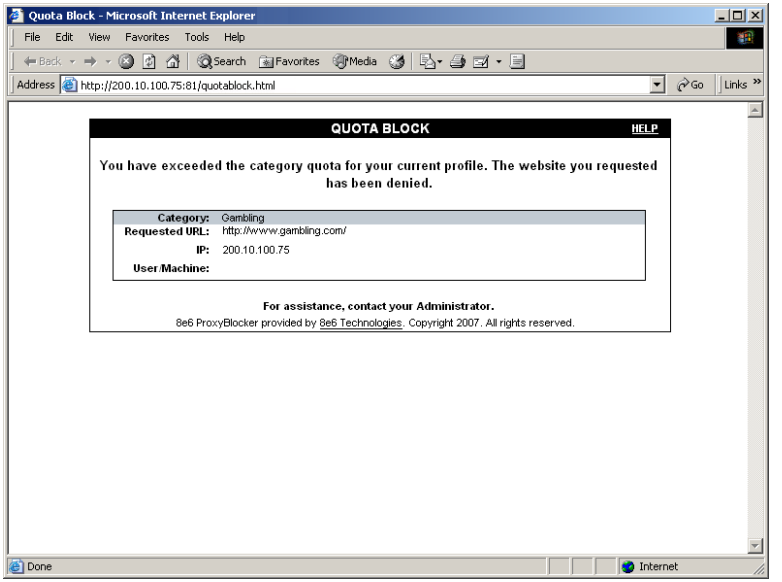


Fig. 2:1-98 Sample Quota Block Page

Once receiving a quota block page, the end user will not be able to access content in that library group/category until the quota is reset.

By default, the following fields display:

- **Category** field - The name of the library category that triggered the quota block page displays.
- **Requested URL** field - The URL the user attempted to access displays.
- **IP** field - The user's IP address displays.
- **User/Machine** field - The username displays for the NT/LDAP user. This field may be blank for the IP group user.

By default, the following standard links are included in the quota block page:

- **HELP** - Clicking this link takes the user to 8e6's Technical Support page that explains why access to the site or service may have been denied.
- **8e6 Technologies** - Clicking this link takes the user to 8e6's Web site.

Chapter 2: Group screen

The Group screen is comprised of windows and dialog boxes used for adding IP groups and/or NT/LDAP domains, and for creating filtering profiles for IP/NT/LDAP groups and their members.

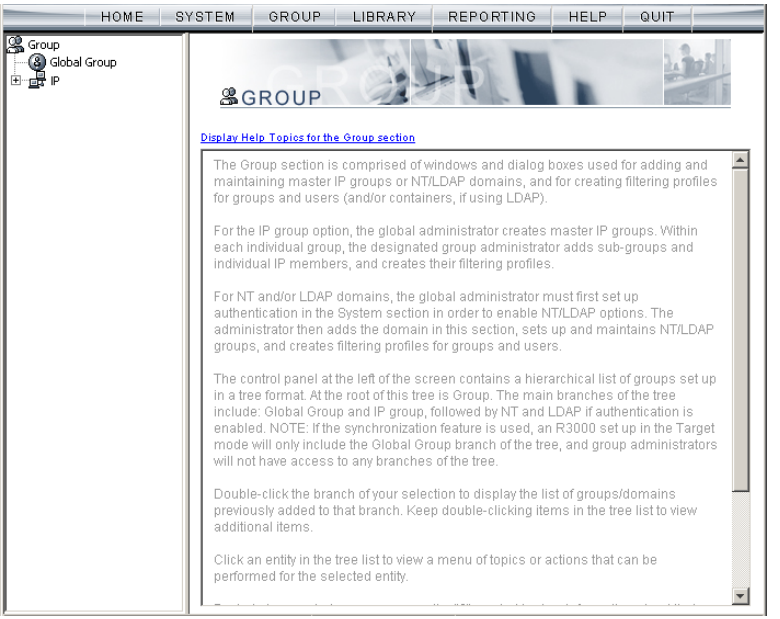


Fig. 2:2-1 Group screen

For the IP group branch, the global administrator creates master IP groups. For each master IP group, the designated group administrator creates sub-groups and individual IP members, and adds and maintains their filtering profiles.

For the NT and LDAP domain branches, the global administrator must first set up authentication in order to enable the NT/LDAP branch(es). For each domain, the administrator then sets up and maintains groups, and creates filtering profiles for groups and users.

The navigation panel at the left of the screen contains a hierarchical list of groups set up in a tree format. At the root of this tree is Group. The main branches of this tree include: Global Group and IP, followed by NT and LDAP if authentication is enabled.

Double-click the branch of your selection to display the list of groups/domains previously added to that branch. Keep double-clicking items in the tree list to view additional items.

Click an entity in the tree list to view a menu of topics or actions that can be performed for that entity.

***NOTES**: Information on NT and LDAP groups can be found in the 8e6 ProxyBlocker Authentication User Guide.*

Information on creating filtering profiles for IP groups can be found in the Group Administrator Section of this user guide.

Global Group

Global Group includes options for creating and maintaining groups. Click the Global Group link to view a menu of sub-topics: Range to Detect, Rules, Global Group Profile, Override Account, Minimum Filtering Level, and Refresh All.

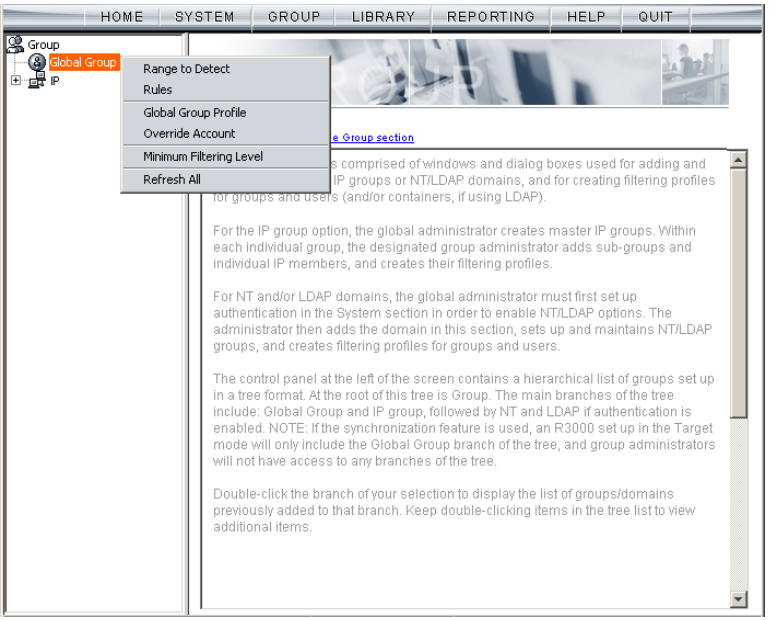


Fig. 2:2-2 Group screen, Global Group menu

Range to Detect window

The Range to Detect window displays when Range to Detect is selected from the Global Group menu. This window is used for defining segments of network traffic to be detected by the ProxyBlocker. Service ports that should be open—ignored by the ProxyBlocker—are also defined in this window.

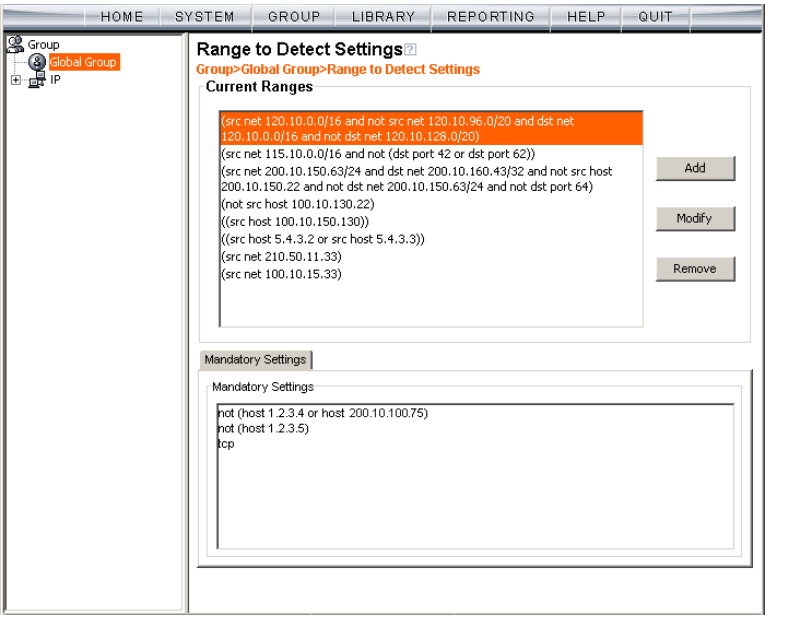


Fig. 2:2-3 Range to Detect Settings window, main window

The main window (Fig. 2:2-3) lets you add segments to the network, or modify or remove existing segments. The Current Ranges list box includes a list of segments previously added using this feature. The Mandatory Settings tab provides examples of settings that can be made.

Add a Segment to the Network

To add a segment to be detected on the network:

1. Click **Add** to go to the next page:

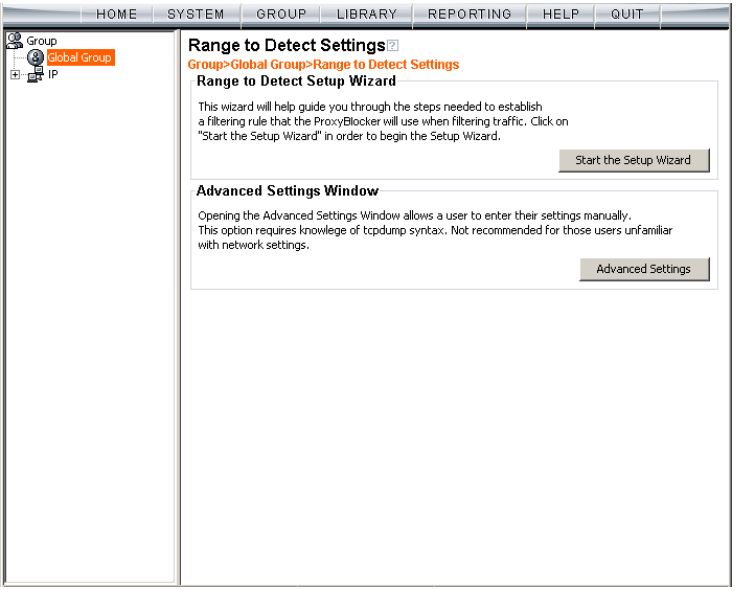


Fig. 2:2-4 Range to Detect Settings, second window

2. Click one of the following buttons to select the procedure for adding the segment:

   - **Start the Setup Wizard** - clicking this button takes you to the Range to Detect Setup Wizard. Follow the instructions in the Range to Detect Setup Wizard sub-section to complete the addition of the segment on the network.
   - **Advanced Settings** - clicking this button takes you to the Range to Detect Advanced Settings window. Follow the instructions in the Range to Detect Advanced Settings sub-section to complete the addition of the segment on the network.

Range to Detect Setup Wizard

Click the **Start the Setup Wizard** button to display Step 1 of the Range to Detect Setup Wizard. The Wizard is comprised of six steps. An entry is required in Step 1, but not in Steps 2 - 5. Settings made using the Wizard are saved in Step 6.

Step 1

In this step you define the source IP address(es) to be filtered.

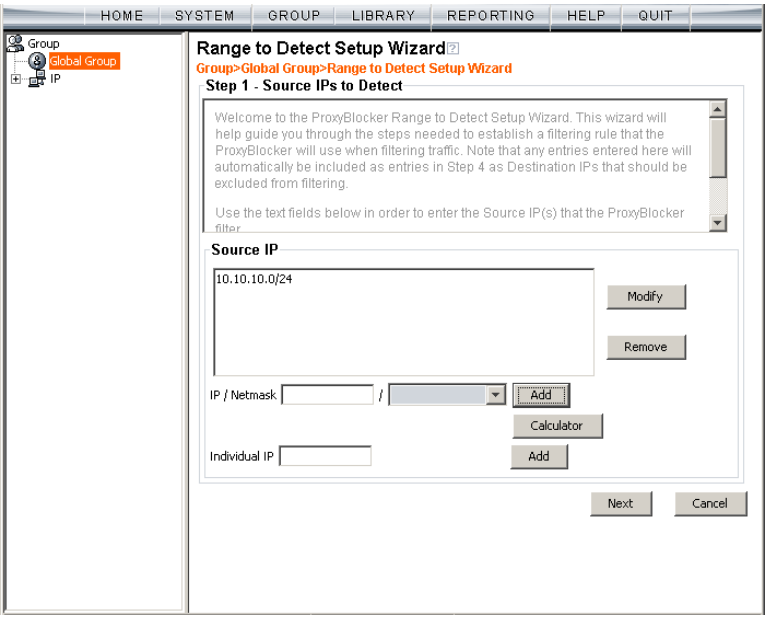


Fig. 2:2-5 Range to Detect Setup Wizard, Step 1

Since the first four pages of the Wizard contain the same fields and buttons, instructions provided for this step are not repeated for Steps 2 - 4.

1. Choose the appropriate option for entering the IP address(es):

- **IP / Netmask** - use these fields to specify a range of IP addresses
- **Individual IP** - use this field to enter a single IP address

2. Click **Add** to include the segment in the list box above.

***NOTE**: To modify the segment, select it from the list box and click **Modify** to move the segment to the field(s) below for editing. To remove the segment, select it from the list box and click **Remove**.*

3. Click **Next** to go to the next page of the Wizard.

***NOTE**: Click **Cancel** to be given the option to return to the main Range to Detect Settings window.*

Step 2: Optional

In this step you define the destination IP address(es) to be filtered.

***NOTE**: By making entries in Destination IP fields, traffic will be restricted to the range specified in the Source IP and Destination IP frames. This reduces the load on the ProxyBlocker, thus enabling it to handle more traffic.*

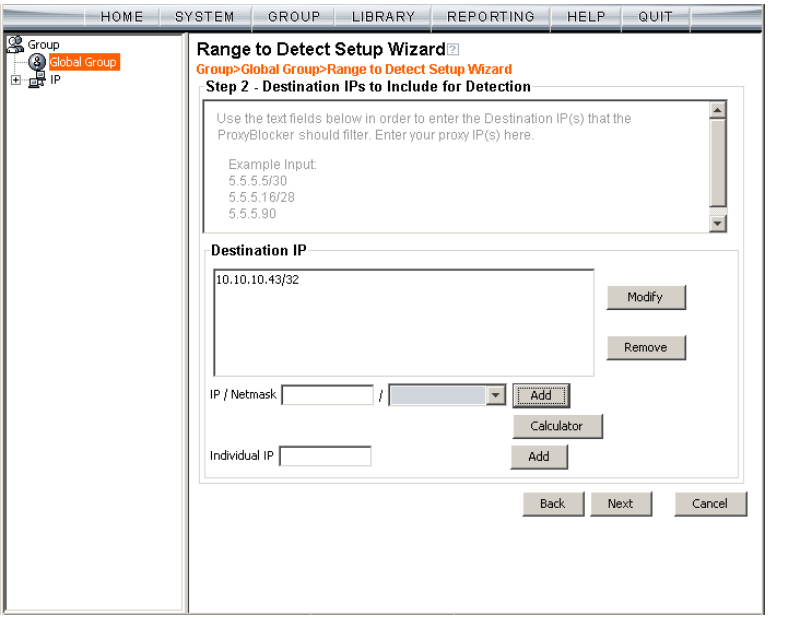


Fig. 2:2-6 Range to Detect Setup Wizard window, Step 2

***NOTE**: For Steps 2-6, click **Back** to return to the previous page of the Wizard.*

Step 3: Optional

In this step you define the source IP address(es) to be excluded from filtering.

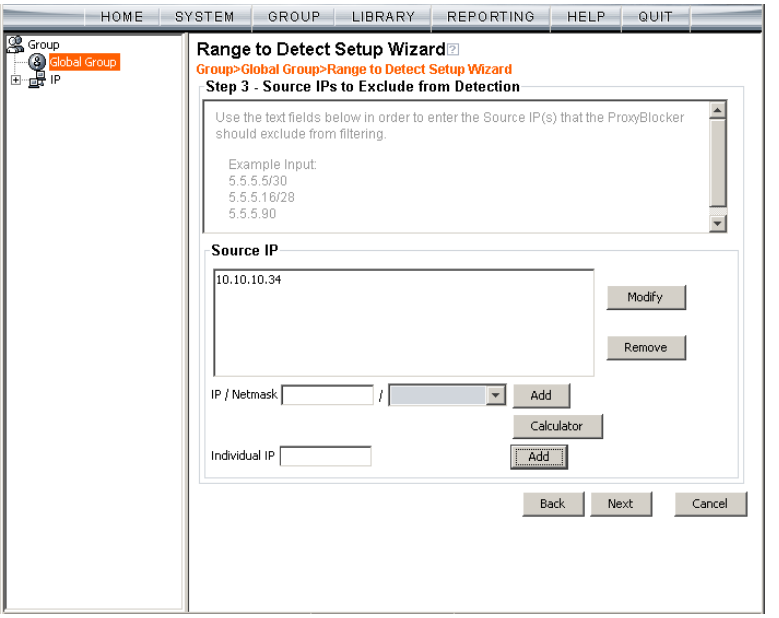


Fig. 2:2-7 Range to Detect Setup Wizard window, Step 3

Step 4: Optional

In this step you define the destination IP address(es) to be excluded from filtering. Any entries from the list box in Step 1 automatically display in the list box above.

***NOTE**: By making entries in Destination IP fields, traffic will be restricted to the range specified in the Source IP and Destination IP frames. This reduces the load on the ProxyBlocker, thus enabling it to handle more traffic.*

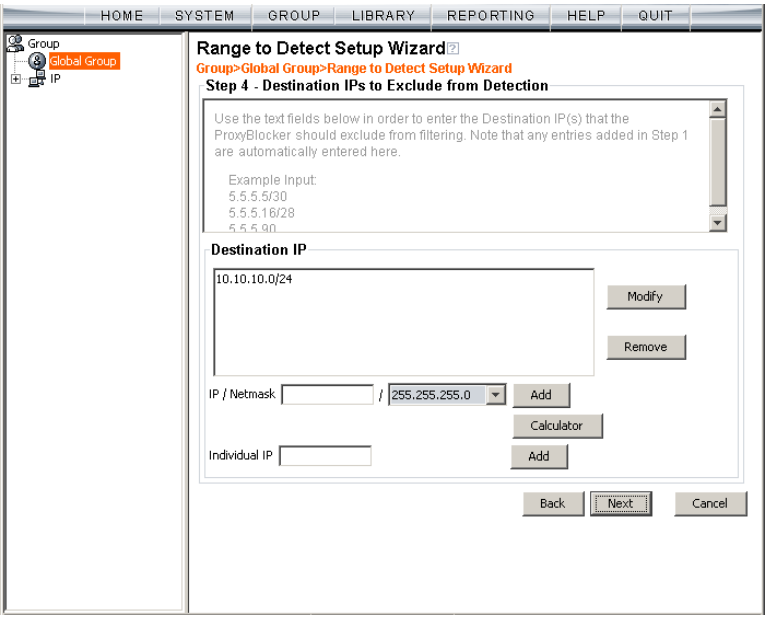


Fig. 2:2-8 Range to Detect Setup Wizard window, Step 4

Step 5: Optional

In this step you enter destination port numbers to be excluded from filtering.

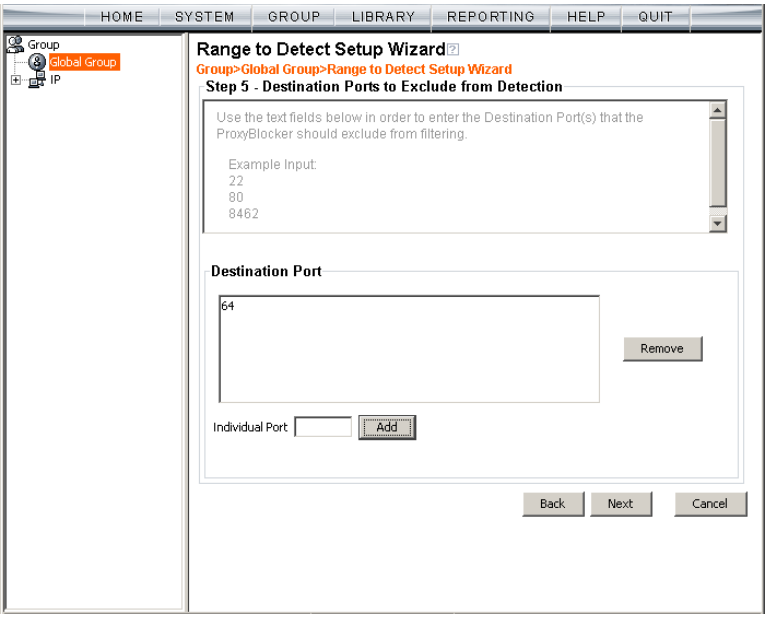


Fig. 2:2-9 Range to Detect Setup Wizard window, Step 5

1. In the **Individual Port** field, enter the port number to be excluded from filtering.
2. Click **Add** to include the entry in the list box above.

***NOTE**: To remove the port number, select it from the list box and click **Remove**.*

3. Click **Next** to go to the last page of the Wizard.

Step 6

In this final step of the Wizard you review your entries and make modifications, if necessary.

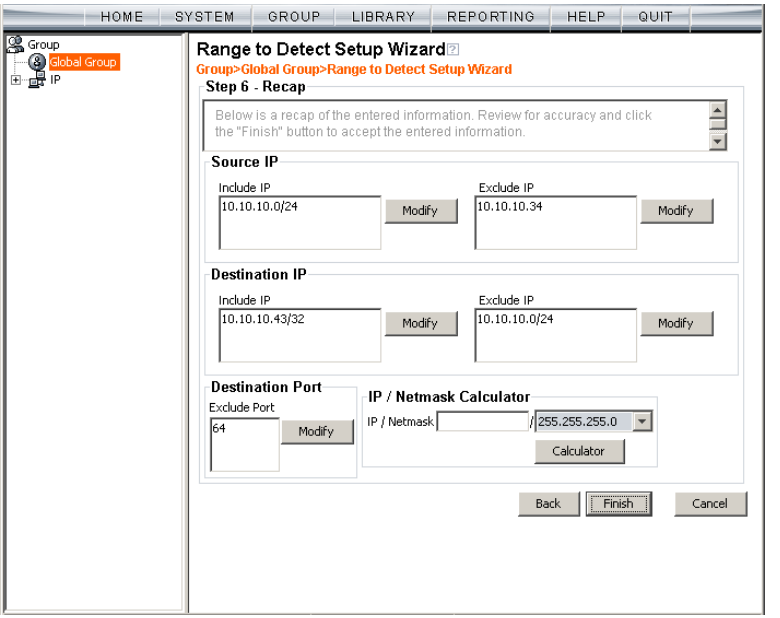


Fig. 2:2-10 Range to Detect Setup Wizard window, Step 6

1. Review the contents in all list boxes.
2. Perform one of the following actions:
   - click the **Modify** button to the right of the list box if you need to make changes. This action takes you to that page of the Wizard where you make your edits. Click **Next** until you return to Step 6.
   - click **Finish** to accept all your entries. This action takes you to the main Range to Detect Settings window where the segment you entered now displays in the Current Ranges list box.

Range to Detect Advanced Settings

Click the **Advanced Settings** button to display the Range to Detect Advanced Settings window:

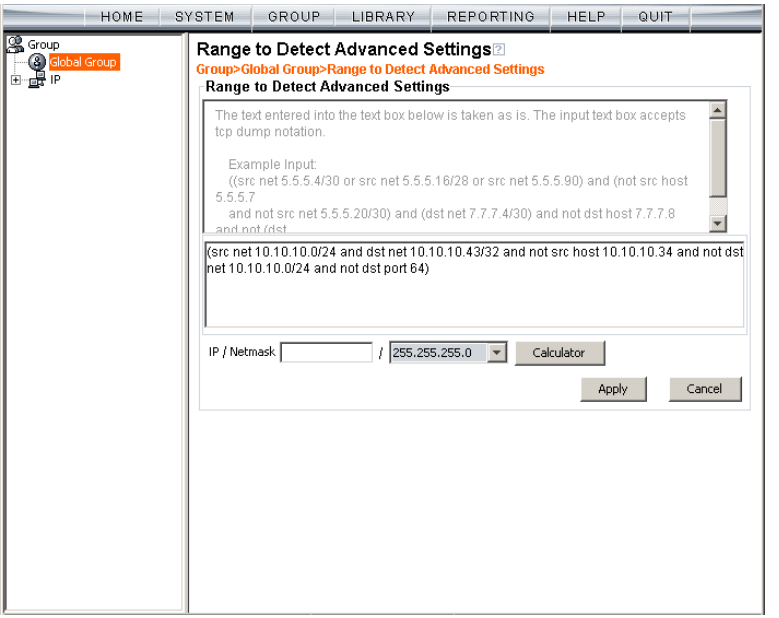


Fig. 2:2-11 Range to Detect Advanced Settings window

1. Enter the settings in the list box, using the correct syntax. Refer to the examples above.

***TIP**: Use the Calculator to calculate IP ranges without any overlaps. Enter the **IP** address, select the **Netmask**, and then click **Calculate** to display results in the Min Host and Max Host fields. Click **Close** to exit.*

***NOTE**: Click **Cancel** to be given the option to return to the main Range to Detect Settings window without saving your settings.*

2. Click **Apply** to accept your entries and to return to the main Range to Detect Settings window.

Modify a Segment of the Network

To modify a segment:

1. In the main Range to Detect Settings window (see Fig. 2:2-3), select the segment from the Current Ranges list box.
2. Click **Modify** to go to the second page (see Fig. 2:2-4).
3. Click one of the following buttons to select the procedure for modifying the segment:
   - **Start the Setup Wizard** - clicking this button takes you to Step 6 of the Range to Detect Setup Wizard (see Fig. 2:2-10). Follow the instructions in the Range to Detect Setup Wizard sub-section for Step 6.
   - **Advanced Settings** - clicking this button takes you to the Range to Detect Advanced Settings window (see Fig. 2:2-11). Follow the instructions in the Range to Detect Advanced Settings sub-section.

Remove a Segment from the Network

To remove a segment:

1. In the main Range to Detect Settings window (see Fig. 2:2-3), select the segment from the Current Ranges list box.
2. Click **Remove**.

Rules window

The Rules window displays when Rules is selected from the Global Group menu. This window is used for adding a filtering rule when creating a filtering profile for an entity.

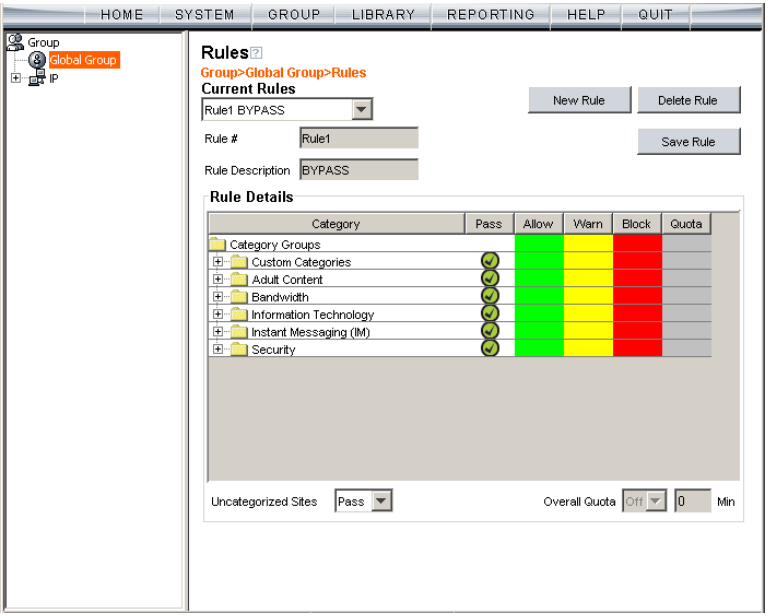


Fig. 2:2-12 Rules window

By default, “Rule1 BYPASS” displays in the **Current Rules** pull-down menu. The other choices in this pull-down menu are “Rule2 BLOCK Porn”, “Rule3 Block IM and Porn”, “Rule4 8e6 CIPA Compliance” (which pertains to the Children’s Internet Protection Act), and the “Block All” rule. By default, “Rule1” displays in the **Rule #** field, “BYPASS” displays in the **Rule Description** field, and **Uncategorized Sites** are allowed to Pass.

View Criteria for a Rule

Select the rule from the **Current Rules** pull-down menu to populate the Rule Details frame with settings made for that rule. If this rule is not an 8e6 pre-defined rule it can be modified or deleted. A rule that does not yet exist can be added using any rule in this list as a template, if necessary.

Add a Rule

To create a new rule:

1. Click **New Rule** to populate the **Rule #** field with the next consecutive rule number available.
2. Enter up to 20 characters for a unique **Rule Description** that describes the theme for that rule.
3. By default, in the Rule Details frame, all library categories in the Category Groups tree are set to pass—indicating that the end user can access URLs in all library categories. This filter setting is designated by the check mark inside a green circle in the **Pass** column.

***TIP**: In the Category Groups tree, double-click the group envelope to open that segment of the tree and to view library categories belonging to that group.*

To change the filter setting for a category group/library category, double-click the column (Allow, Warn, Block) in the row corresponding to that category group/library category to move the check mark to that column:

- **Allow** - URLs in this category will be added to the end user's white list.
- **Warn** - URLs in this category will warn the end user that the URL he/she requested can be accessed, but may be against the organization's policies. The end user can view the URL after seeing a warning message and agreeing to its terms.
- **Block** - URLs in this category will be blocked.

***NOTE**: If a category group does not display any filter setting (i.e. the check mark does not display in any column for the category group), one or more library categories within that group has a filter setting in a column other than the filter setting designated for all collective library categories within that group. For example, if in the Adult Content category group some of the library categories have a block setting and other library categories have a warn setting, there would be no category group filter setting, since all library categories do not have the same filter setting.*

***TIPS**: Multiple categories can be assigned the same filter setting by clicking each category while pressing the Ctrl key on your keyboard, and then double-clicking in the appropriate column.*

Blocks of categories can be assigned the same filter setting by clicking the first category, and then pressing the Shift key on your keyboard while clicking the last category, and then double-clicking in the appropriate column.

4. Make a selection from the **Uncategorized Sites** pull-down menu to specify how to handle a URL that has not yet been categorized: “Pass”, “Warn”, or “Block”.
5. To use the quota feature to restrict the end user’s access to a passed library group/category, do the following:
   - In the **Quota** column, enter the number of minutes the user will be able to access the library group/category. The minimum number of minutes is “1” and the maximum is “1439” (one day minus one minute). The number of minutes entered here combines with the seconds per hit (minimum one second to maximum 3600 seconds) defined in the Quota Settings window to determine when the end user will be blocked from further access to URLs in that library group/category.

***TIP**: If a quota entry is made for a category group, all library categories in that group will show the same number of quota minutes.*

***NOTE**: See the Quota Settings window in Chapter 1: System screen for more information on configuring quota settings and resetting quotas for end users currently blocked by quotas.*

- The **Overall Quota** field becomes enabled if a quota is entered for any library group/category. By default, the enabled Overall Quota is turned “Off”. If turned “On”, enter the number of minutes in the **Min** field to indicate when the end user’s access to passed library groups/ categories with quotas will be blocked. If the end user spends this amount of time at URLs in any quota-marked library group/category, the Overall Quota overrides the number of minutes defined for each individual quota.

6. Click **Add Rule** to include your rule to the list that displays in the pull-down menu.

Modify a Rule

After a rule is added, it can later be modified. To make changes to a rule:

1. Select the rule from the **Current Rules** pull-down menu.
2. Modify settings for library groups and categories in the Rule Details frame.
3. Click **Save Rule**.

Copy a Rule

As a time saving practice, a rule can be used as a basis when creating another similar rule. To copy a rule:

1. Select the rule to be copied from the list of **Current Rules**.
2. Click **New Rule** to populate the Rule # field with the next available rule number, and to activate the Rule Description field.
3. Enter up to 20 characters for a unique **Rule Description** that describes the theme for that rule.
4. Modify settings for library groups and categories in the Rule Details frame.

5. Click **Save Rule**.

Remove a Rule

To delete a rule:

1. Select the rule from the **Current Rules** pull-down menu.
2. Click **Delete Rule**.

Global Group Profile window

The Global Group Profile window displays when Global Group Profile is selected from the Global Group menu. This window is used for viewing/creating the global (default) filtering profile that will be used by all users on the network unless a unique filtering profile is created for an entity. Click the following tabs in this window: Category, Port, Default Redirect URL, and Filter Options. Entries in these tabs comprise the profile string for the global group.

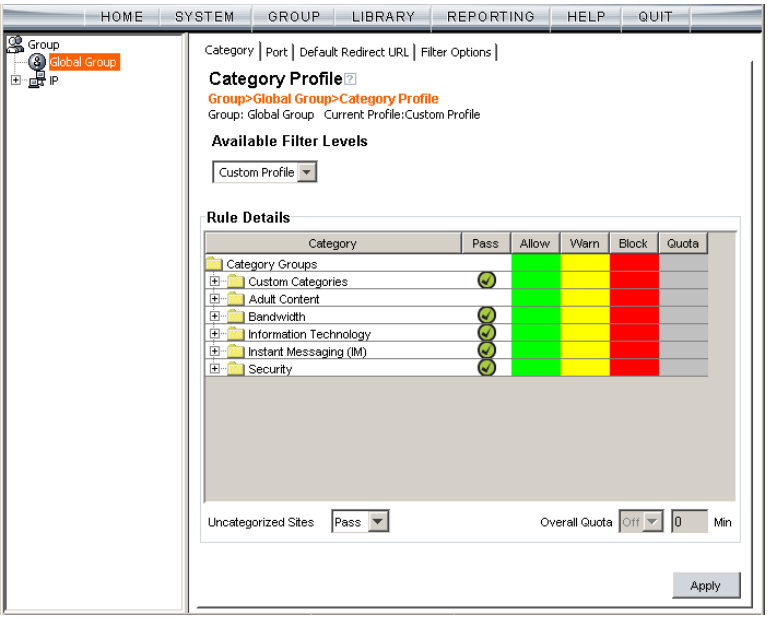


Fig. 2:2-13 Global Group Profile window, Category tab

Category Profile

Category Profile displays by default when Global Group Profile is selected from the Global Group menu, or when the Category tab is clicked. This tab is used for assigning filter settings to category groups/library categories for the global group profile.

By default, “Custom Profile” displays in the Available Filter Levels pull-down menu, and **Uncategorized Sites** are allowed to Pass.

Create, Edit a List of Selected Categories

For the category portion of the global group filtering profile, in the Rule Details frame all library categories in the Category Groups tree are set to pass, except “Child Pornography” and “Pornography/Adult Content”—indicating that the end user can access URLs in all other library categories. This filter setting is designated by the check mark inside a green circle in the **Pass** column for all category groups except Adult Content.

***TIP**: In the Category Groups tree, double-click the group envelope to open that segment of the tree and to view library categories belonging to that group.*

1. To change a category group/library category filter setting, double-click the column (Allow, Warn, Block) in the row corresponding to that category group/library category to move the check mark to that column:
   - **Allow** - URLs in this category will be added to the end user’s white list.
   - **Warn** - URLs in this category will warn the end user that the URL he/she requested can be accessed, but may be against the organization’s policies. The end user can view the URL after seeing a warning message and agreeing to its terms.

- **Block** - URLs in this category will be blocked.

***NOTE**: If a category group does not display any filter setting (i.e. the check mark does not display in any column for the category group), one or more library categories within that group has a filter setting in a column other than the filter setting designated for all collective library categories within that group. For example, if in the Adult Content category group some of the library categories have a block setting and other library categories have a warn setting, there would be no category group filter setting, since all library categories do not have the same filter setting.*

***TIPS**: Multiple categories can be assigned the same filter setting by clicking each category while pressing the Ctrl key on your keyboard, and then double-clicking in the appropriate column.*

Blocks of categories can be assigned the same filter setting by clicking the first category, and then pressing the Shift key on your keyboard while clicking the last category, and then double-clicking in the appropriate column.

2. Make a selection from the **Uncategorized Sites** pull-down menu to specify how to handle a URL that has not yet been categorized: “Pass”, “Warn”, or “Block”.
3. To use the quota feature to restrict the end user’s access to a passed library group/category, do the following:
   - In the **Quota** column, enter the number of minutes the user will be able to access the library group/category. The minimum number of minutes is “1” and the maximum is “1439” (one day minus one minute). The number of minutes entered here combines with the seconds per hit (minimum one second to maximum 3600 seconds) defined in the Quota Settings window to determine when the end user will be blocked from further access to URLs in that library group/category.

***TIP**: If a quota entry is made for a category group, all library categories in that group will show the same number of quota minutes.*

***NOTE**: See the Quota Settings window in Chapter 1: System screen for more information on configuring quota settings and resetting quotas for end users currently blocked by quotas.*

- The **Overall Quota** field becomes enabled if a quota is entered for any library group/category. By default, the enabled Overall Quota is turned “Off”. If turned “On”, enter the number of minutes in the **Min** field to indicate when the end user’s access to passed library groups/ categories with quotas will be blocked. If the end user spends this amount of time at URLs in any quota-marked library group/category, the Overall Quota overrides the number of minutes defined for each individual quota.

4. Click **Apply** to apply your settings at the global level.

Port

Port displays when the Port tab is clicked. This tab is used for blocking access to specified ports for the global filtering profile.

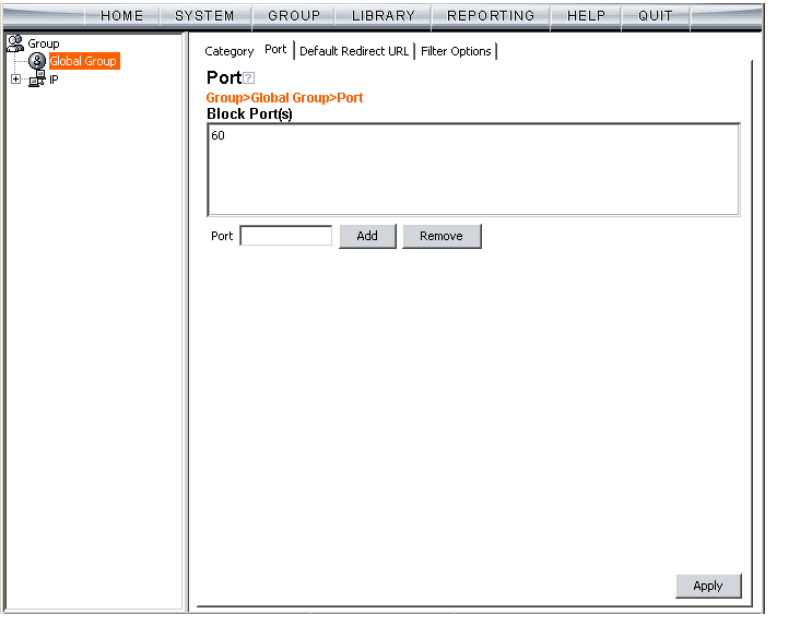


Fig. 2:2-14 Global Group Profile window, Port tab

Create, Edit a List of Service Ports

All service ports are filtered by default. To block a service port from being accessed by global filtering profile users:

1. Enter the port number in the **Port** field.
2. Click **Add**. Each port number you add displays in the Block Port(s) list box.
3. Click **Apply** to apply your settings at the global level.

To remove a port number from the list box:

1. Select the port number.

2. Click **Remove**.
3. Click **Apply** to apply your settings at the global level.

Default Redirect URL

Default Redirect URL displays when the Default Redirect URL tab is clicked. This tab is used for specifying the URL to be used for redirecting users who attempt to access a site or service set up to be blocked for the global filtering profile.

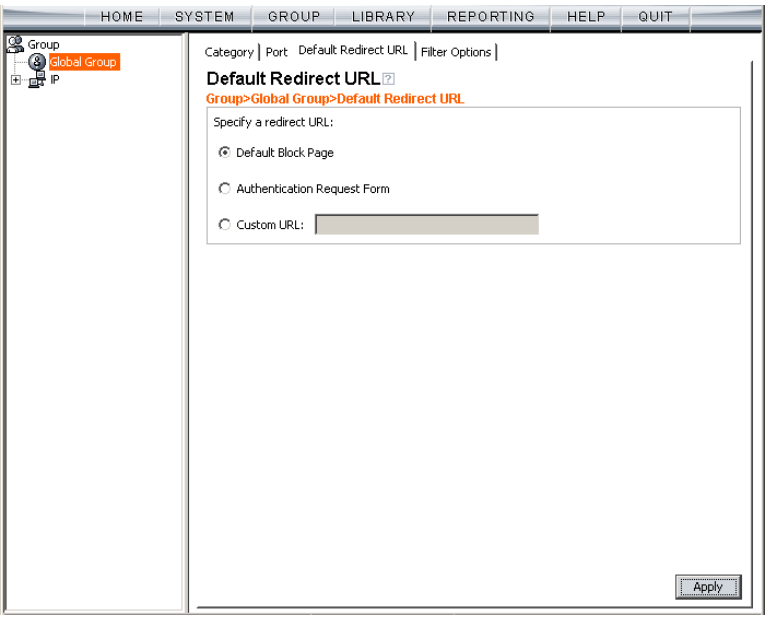


Fig. 2:2-15 Global Group Profile window, Default Redirect URL tab

Create, Edit the Redirect URL

1. Specify the type of redirect URL to be used: “Default Block Page”, “Authentication Request Form”, or “Custom URL”.

   If “Custom URL” is selected, enter the redirect URL in the corresponding text box. Users will be redirected to the designated page at this URL instead of the block page.

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

Filter Options

Filter Options displays when the Filter Options tab is clicked. This tab is used for specifying which filter option(s) will be applied to the global group filtering profile.

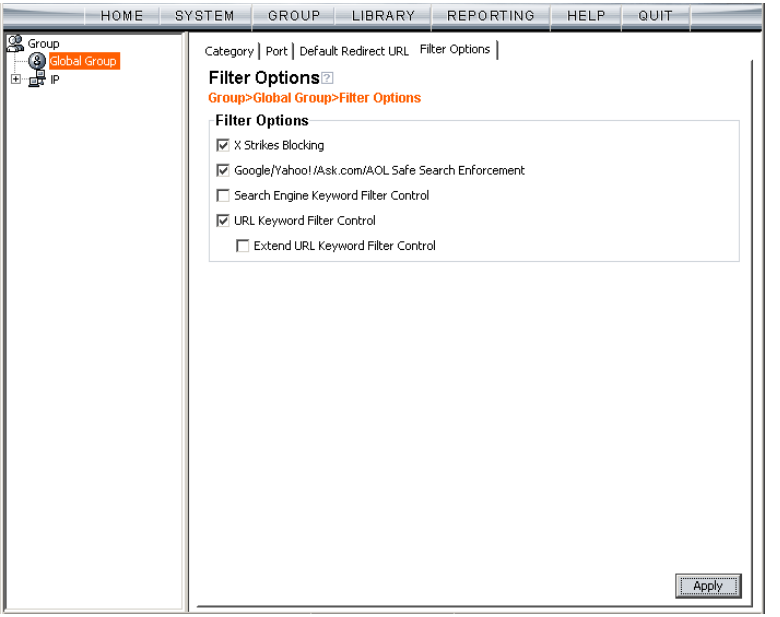


Fig. 2:2-16 Global Group Profile window, Filter Options tab

Create, Edit the Filter Options

1. Click the checkbox(es) corresponding to the option(s) to be applied to the global group filtering profile: “X Strikes Blocking”, “Google/Yahoo!/Ask.com/AOL Safe Search Enforcement”, “Search Engine Keyword Filter Control”, “URL Keyword Filter Control”. If URL Keyword Filter Control is selected, the “Extend URL Keyword Filter Control” option can be selected.
2. Click **Apply** to apply your settings.

X Strikes Blocking

With the X Strikes Blocking option enabled, an end user who attempts to access inappropriate sites on the Internet will be locked out from his/her workstation after a specified number of tries within a fixed time period.

***NOTE**: See the X Strikes Blocking window in Chapter 1: System screen for information on setting up the X Strikes Blocking feature.*

Google/Yahoo!/Ask.com/AOL Safe Search Enforcement

With the Google/Yahoo!/Ask.com/AOL Safe Search Enforcement option enabled, Google, Yahoo!, Ask.com, and AOL's "strict" SafeSearch Filtering option will be used whenever end users perform a Google, Yahoo!, Ask.com, or AOL Web search or Image search.

***WARNINGS**: This feature is not compatible with the proxy environment as it will cause overblocking.*

An inappropriate image will only be blocked if that image is included in 8e6's library or is blocked by Google, Yahoo!, Ask.com, or AOL.

If this option is used in conjunction with the X Strikes Blocking feature and a user is performing an inappropriate Google, Yahoo!, Ask.com, or AOL Image search, the number of strikes that user will receive is based upon the amount of time it will take for unacceptable Google, Yahoo!, Ask.com, or AOL images returned by the query to load on the page. The user will receive only one strike if all inappropriate images load within the tolerance time range of a given strike.

Search Engine Keyword Filter Control

With the Search Engine Keyword Filter Control option enabled, search engine keywords can be set up to be blocked. When a user enters a keyword in the search engine, if that keyword has been set up to be blocked, the search will not be performed. Search engine keywords are entered in the Search Engine Keywords window of 8e6 supplied library categories and custom library categories.

***NOTES**: Search engine keyword filtering relies on an exact keyword match. For example, if the word "sex" is set up to be blocked, but "sexes" is not set up to be blocked, a search will be allowed on "sexes" but not "sex". However, if the word "gin" is set up to be blocked, a search on "cotton gin" will be blocked since the word "gin" is blocked.*

To set up search engine keywords in a Search Engine Keywords window, see the following sections of this user guide for the specified library type:

- *8e6 Supplied Categories - see Chapter 3: Library screen, Search Engine Keywords window in this section.*
- *Custom Categories - see the Group Administrator Section, Chapter 2: Library screen, Search Engine Keywords window.*

URL Keyword Filter Control

With the URL Keyword Filter Control option enabled, URL keywords can be set up to be blocked. When a user enters a keyword in the address line of a browser window, if that keyword has been set up to be blocked, the user will be denied access to that site or service. URL keywords are entered in the URL Keywords window of 8e6 supplied library categories and custom library categories.

With the “Extend URL Keyword Filter Control” option enabled, a URL keyword search will be extended after the "?" character in a URL.

***NOTE**: To set up URL keywords in a URL Keywords window, see the following sections of this user guide for the specified library type:*

- *8e6 Supplied Categories - see Chapter 3: Library screen, URL Keywords window, in this section.*
- *Custom Category - see the Group Administrator Section, Chapter 2: Library screen, URL Keywords window.*

***WARNING**: If this feature is activated, use extreme caution when setting up URL keywords for filtering. If a keyword that is entered in a browser’s address window contains the same consecutive characters as a keyword set up to be blocked, users will be denied access to URLs that are not even within blocked categories. For example, if all URL keywords containing “sex” are blocked, users will not be able to access a non-pornographic site such as http://www.essex.com.*

Override Account window

The Override Account window displays when Override Account is selected from the Global Group menu. This window is used for creating an override account that allows an IP group user to bypass settings at the minimum filtering level. A user with an override account will be able to access categories and service ports blocked at the minimum filtering level.

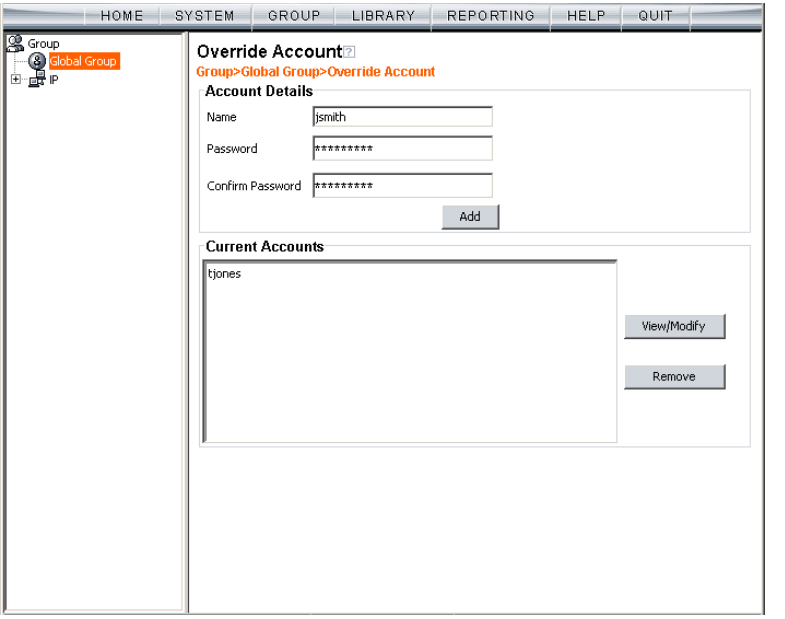


Fig. 2:2-17 Override Account window

***NOTES**: A user can have only one override account. If an override account was previously created for a user in a master IP group, only that override account will be effective, unless that account is deleted from the IP group. See the Override Account window in Chapter 1 of the Group Administrator Section for information on setting up an override account for a user in an IP group.*

See Appendix D: Override Pop-up Blockers for information on how a user with an override account can authenticate if a pop-up blocker is installed on his/her workstation.

Add an Override Account

To create an Override Account profile:

1. In the Account Details frame, enter the username in the **Name** field.
2. Enter the **Password**.
3. Make the same entry again in the **Confirm Password** field.
4. Click **Add** to include the username in the list box of the Current Accounts frame, and to open the pop-up window containing the Current Accounts name as well as tabs to be used for specifying the components of the override account profile.
5. Click each of the tabs (Rule, Redirect, Filter Options) and specify criteria to complete the override account profile. (See Category Profile, Redirect URL, and Filter Options in this sub-section for information on the Rule, Redirect, and Filter Options tabs.)
6. Click **Apply** to activate the override account.
7. Click **Close** to close the pop-up window.

Category Profile

The Rule tab is used for creating the categories portion of the override account profile.

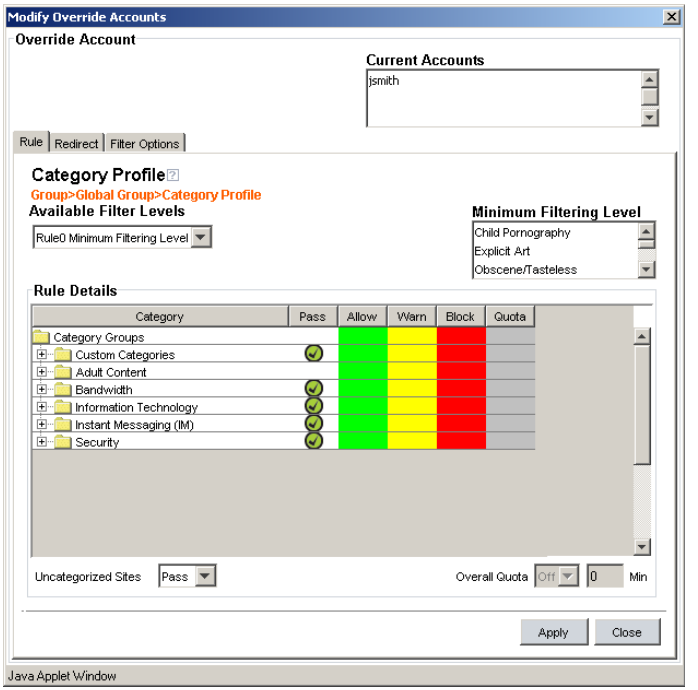


Fig. 2:2-18 Override Account pop-up window, Rule tab

To create the category profile:

1. Select a filtering rule from the available choices in the **Available Filter Levels** pull-down menu. This action automatically populates the Pass, Allow, Warn, and/or Block columns in the Rule Details frame with filter settings for each category group/library category in the Category Groups tree.

***TIP**: In the Category Groups tree, double-click the group envelope to open that segment of the tree and to view library categories belonging to that group.*

***NOTE**: If a category group does not display any filter setting (i.e. the check mark does not display in any column for the category group), one or more library categories within that group has a filter setting in a column other than the filter setting designated for all collective library categories within that group. For example, if in the Adult Content category group some of the library categories have a block setting and other library categories have a warn setting, there would be no category group filter setting, since all library categories do not have the same filter setting.*

2. To change the filter setting for a category group/library category, double-click the column (Pass, Allow, Warn, Block) in the row corresponding to that category group/library category to move the check mark to that column:
   - **Pass** - URLs in this category will pass to the end user.
   - **Allow** - URLs in this category will be added to the end user's white list.
   - **Warn** - URLs in this category will warn the end user that the URL he/she requested can be accessed, but may be against the organization's policies. The end user can view the URL after seeing a warning message and agreeing to its terms.
   - **Block** - URLs in this category will be blocked.

***TIPS**: Multiple categories can be assigned the same filter setting by clicking each category while pressing the Ctrl key on your keyboard, and then double-clicking in the appropriate column.*

Blocks of categories can be assigned the same filter setting by clicking the first category, and then pressing the Shift key on your keyboard while clicking the last category, and then double-clicking in the appropriate column.

3. Make a selection from the **Uncategorized Sites** pull-down menu to specify how to handle a URL that has not yet been categorized: "Pass", "Warn", or "Block".
4. To use the quota feature to restrict the end user's access to a passed library group/category, do the following:

- In the **Quota** column, enter the number of minutes the user will be able to access the library group/category. The minimum number of minutes is “1” and the maximum is “1439” (one day minus one minute). The number of minutes entered here combines with the seconds per hit (minimum one second to maximum 3600 seconds) defined in the Quota Settings window to determine when the end user will be blocked from further access to URLs in that library group/category.

***TIP**: If a quota entry is made for a category group, all library categories in that group will show the same number of quota minutes.*

***NOTE**: See the Quota Settings window in Chapter 1: System screen for more information on configuring quota settings and resetting quotas for end users currently blocked by quotas.*

- The **Overall Quota** field becomes enabled if a quota is entered for any library group/category. By default, the enabled Overall Quota is turned “Off”. If turned “On”, enter the number of minutes in the **Min** field to indicate when the end user’s access to passed library groups/categories with quotas will be blocked. If the end user spends this amount of time at URLs in any quota-marked library group/category, the Overall Quota overrides the number of minutes defined for each individual quota.

5. Click **Apply** to apply your settings to the override account profile.
6. Click another tab (Redirect or Filter Options) to continue creating the override account profile, or click **Close** to close the pop-up window and to return to the Override Account window.

Redirect URL

The Redirect tab is used for specifying the URL to be used for redirecting the user if he/she attempts to access a site or service set up to be blocked.

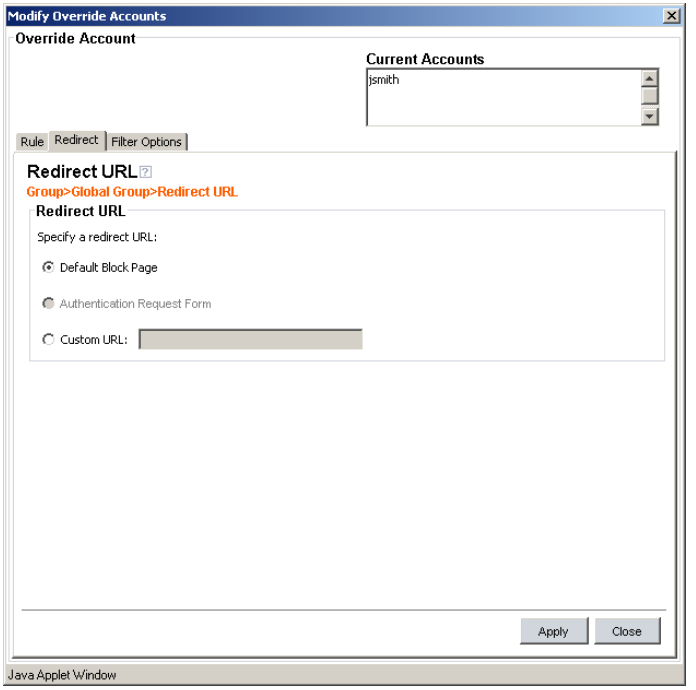


Fig. 2:2-19 Override Account pop-up window, Redirect tab

1. Specify the type of redirect URL to be used: “Default Block Page”, “Authentication Request Form”, or “Custom URL”.

   If “Custom URL” is selected, enter the redirect URL in the corresponding text box. The user will be redirected to the designated page at this URL instead of the block page.

2. Click **Apply** to apply your settings to the override account profile.

3. Click the Filter Options tab to continue creating the override account profile, or click **Close** to close the pop-up window and to return to the Override Account window.

Filter Options

The Filter Options tab is used for specifying which filter option(s) will be applied to the override account profile.

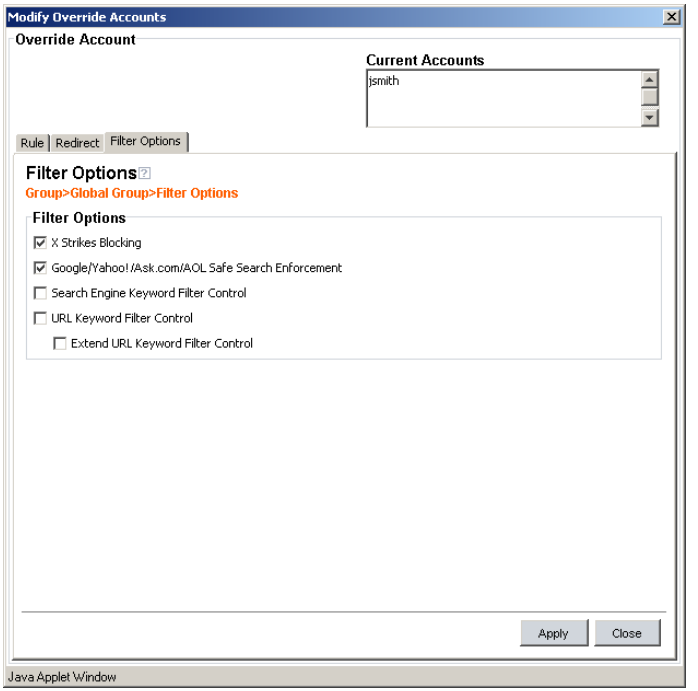


Fig. 2:2-20 Override Account pop-up window, Filter Options tab

1. Click the checkbox(es) corresponding to the option(s) to be applied to the override account filtering profile:
   - "X Strikes Blocking" - With the X Strikes Blocking option enabled, if the user attempts to access inappropriate sites on the Internet, he/she will be locked out from his/her workstation after a specified number of tries within a fixed time period.

***NOTE**: See the X Strikes Blocking window in Chapter 1: System screen for information on setting up the X Strikes Blocking feature.*

- "Google/Yahoo!/Ask.com/AOL Safe Search Enforcement" - With the Google/Yahoo!/Ask.com/AOL Safe Search Enforcement option enabled, Google, Yahoo!, Ask.com, and AOL's "strict" SafeSearch Filtering option will be used whenever the end user performs a Google, Yahoo!, Ask.com, or AOL Web search or Image search.

***WARNING**: If this option is used in conjunction with the X Strikes Blocking feature and a user is performing an inappropriate Google, Yahoo!, Ask.com, or AOL Image search, the number of strikes that user will receive is based upon the amount of time it will take for unacceptable Google, Yahoo!, Ask.com, or AOL images returned by the query to load on the page. The user will receive only one strike if all inappropriate images load within the tolerance time range of a given strike.*

- "Search Engine Keyword Filter Control" - With the Search Engine Keyword Filter Control option enabled, search engine keywords can be set up to be blocked. When the user enters a keyword in the search engine, if that keyword has been set up to be blocked, the search will not be performed. Search engine keywords are entered in the Search Engine Keywords window of 8e6 supplied library categories and custom library categories.

***NOTE**: To set up search engine keywords in a Search Engine Keywords window, see the following sections of this user guide for the specified library type:*

- *8e6 Supplied Categories - see Chapter 3: Library screen, Search Engine Keywords window.*
- *Custom Categories - see the Group Administrator Section, Chapter 2: Library screen, Search Engine Keywords window.*

- "URL Keyword Filter Control" - With the URL Keyword Filter Control option enabled, URL keywords can be set up to be blocked. When the user enters a keyword in the address line of a browser window, if that keyword has been set up to be blocked, the user will be denied access to that site or service. URL keywords are entered in the URL Keywords window of 8e6 supplied library categories and custom library categories.

  With the "Extend URL Keyword Filter Control" option enabled, a URL keyword search will be extended after the "?" character in a URL.

***NOTE**: To set up URL keywords in a URL Keywords window, see the following sections of this user guide for the specified library type:*

- *8e6 Supplied Categories - see Chapter 3: Library screen, URL Keywords window.*
- *Custom Category - see the Group Administrator Section, Chapter 2: Library screen, URL Keywords window.*

2. Click **Apply** to apply your settings to the override account profile.
3. Click **Close** to close the pop-up window and to return to the Override Account window.

Edit an Override Account

Change the Password

To change an override account's password:

1. In the Current Accounts frame, select the username from the list box.
2. In the Account Details frame, enter the username in the **Name** field.
3. Enter the new **Password**.
4. Make the same entry again in the **Confirm Password** field.
5. Click **View/Modify** to open the pop-up window.
6. Click **Apply**.
7. Click **Close** to close the pop-up window.

Modify an Override Account

To modify an override account:

1. In the Current Accounts frame, select the username from the list box.
2. Click **View/Modify** to open the pop-up window.
3. Click the tab in which to make modifications (Rule, Redirect, Filter Options).
4. Make your edits in this tab and in any other tab, if necessary.
5. Click **Apply**.
6. Click **Close** to close the pop-up window.

Delete an Override Account

To delete an override account:

1. In the Current Accounts frame, select the username from the list box.
2. Click **Remove**.

Minimum Filtering Level window

The Minimum Filtering Level window displays when Minimum Filtering Level is selected from the Global Group menu. This window is used for establishing the minimum filtering level that will apply to all users who belong to a group, and to any group using a filtering profile other than the global (default) filtering profile.

The minimum filtering level is created by making selections from the list of library categories and service ports. These settings can be bypassed if a user has an override account.

***NOTE**: See the Override Account window in this chapter and in Chapter 1 of the Group Administrator Section for more information about override accounts.*

Click the following tabs in this window: Category, Port, and Min. Filter Bypass. Entries in the Category and Port tabs comprise the profile string for the minimum filtering level.

Minimum Filtering Categories

Minimum Filtering Categories displays by default when Minimum Filtering Level is selected from the Global Group menu, or when the Category tab is clicked. This tab is used for making selections from the list of library categories, and specifying whether each of these selected categories will be opened or blocked at the minimum filtering level.

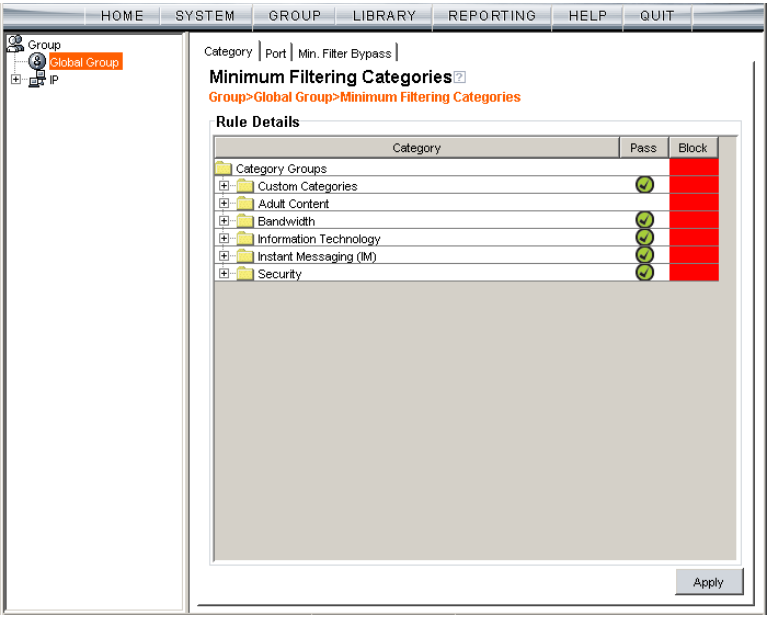


Fig. 2:2-21 Minimum Filtering Level window, Min. Filtering Categories

By default, “Child Pornography” and “Pornography/Adult Content” are assigned a Block filter setting, and all other active library categories are set to Pass. Filter settings are designated by the check mark inside a green circle in the Pass or Block column.

***TIP**: In the Category Groups tree, double-click the group envelope to open that segment of the tree and to view library categories belonging to that group.*

Create, Edit Minimum Filtering Categories

To create the categories portion of the minimum filtering level profile:

1. Double-click the column (Pass, Block) in the row corresponding to that category group/library category to move the check mark to that column:
   - **Pass** - URLs in this category will pass to the end user.
   - **Block** - URLs in this category will be blocked.

***TIPS**: Multiple categories can be assigned the same filter setting by clicking each category while pressing the Ctrl key on your keyboard, and then double-clicking in the appropriate column.*

Blocks of categories can be assigned the same filter setting by clicking the first category, and then pressing the Shift key on your keyboard while clicking the last category, and then double-clicking in the appropriate column.

2. Click **Apply** to apply your settings for the minimum filtering level.

Port

Port displays when the Port tab is clicked. This tab is used for blocking access to specified ports at the minimum filtering level.

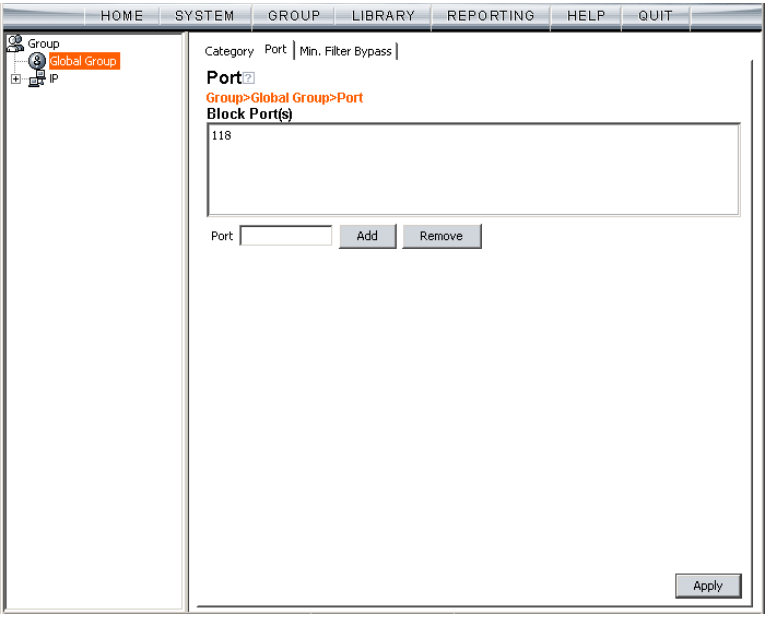


Fig. 2:2-22 Minimum Filtering Level window, Port tab

Create, Edit a List of Service Ports

All service ports are filtered by default. To block a service port from being accessed at the minimum filtering level:

1. Enter the port number in the **Port** field.
2. Click **Add**. Each port number you add displays in the Block Port(s) list box.
3. Click **Apply** to apply your settings at the minimum filtering level.

To remove a port number from the list box:

1. Select the port number.
2. Click **Remove**.
3. Click **Apply** to apply your settings at the minimum filtering level.

Minimum Filtering Bypass Options

Minimum Filtering Bypass Options displays when the Min. Filter Bypass tab is clicked. This tab is used for specifying whether users in a master IP group will be allowed to bypass the minimum filtering level with an override account or an exception URL.

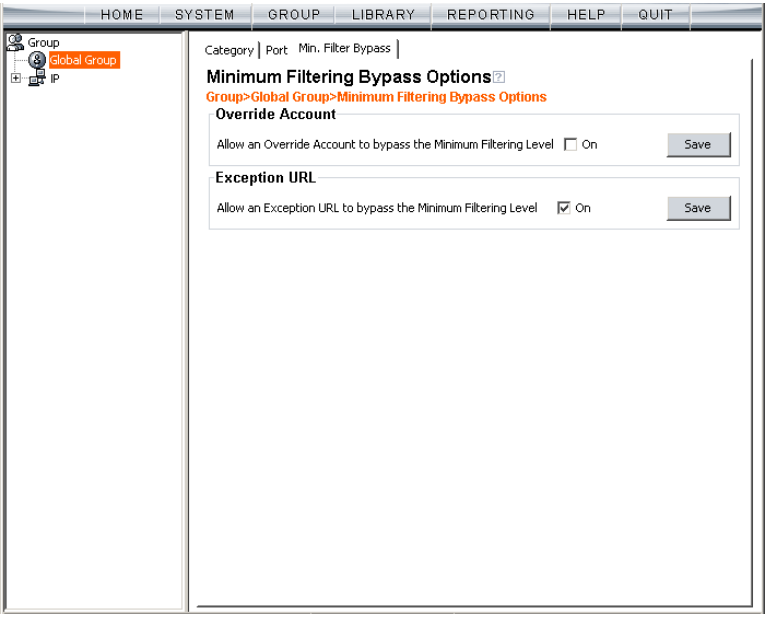


Fig. 2:2-23 Minimum Filtering Level window, Min. Filter Bypass tab

***NOTE**: See the Override Account window and Exception URL window of the Group screen in the Group Administrator Section of this user guide for information on setting up an override account and exception URLs.*

Specify Minimum Filtering Bypass Options

To allow a user to override settings made at the minimum filtering level:

1. In the Override Account frame, click the “On” checkbox. Any user who has an override account will be able to access content blocked at the minimum filtering level.
2. Click **Save** to apply your settings.

To allow users to bypass exception URLs set up to be blocked at the minimum filtering level:

1. In the Exception URL frame, click the “On” checkbox. Users will be able to bypass settings at the minimum filtering level, if URLs blocked at the minimum filtering level are set up to be accessed by users.
2. Click **Save** to apply your settings. (See the Exception URL window in the Group Administrator Section for more information.)

Refresh All

Refresh All Main Branches

From the Global Group menu, click Refresh All to refresh the main branches of the tree. This action should be performed whenever authentication has been enabled or disabled.

If authentication is enabled, when Refresh All is clicked, the NT and LDAP branches of the tree display. When authentication is disabled, when Refresh All is clicked only the IP branch of the tree displays.

IP

IP includes options for adding a master IP group and to refresh the tree list. Click the IP link to view a menu of sub-topics: Add Group, and Refresh.

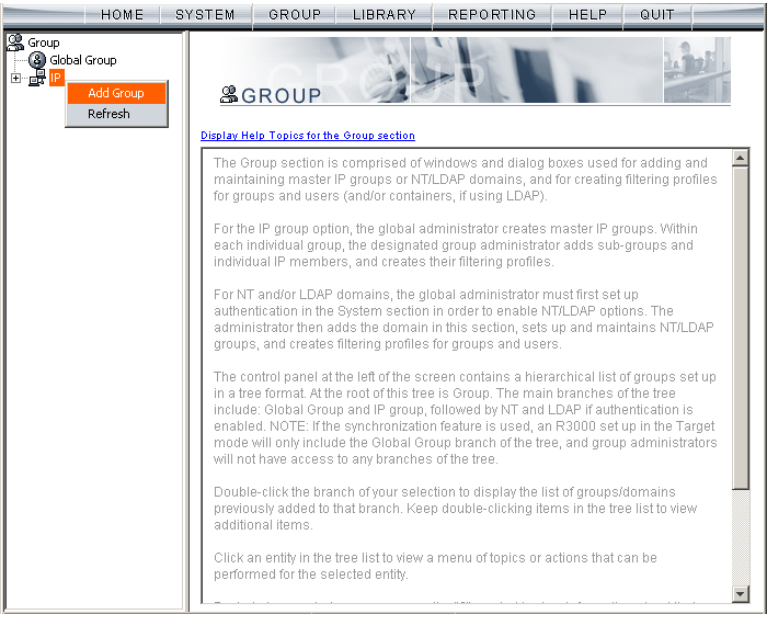


Fig. 2:2-24 Group screen, IP menu

Add Group

Add a Master IP Group

From the IP group menu:

1. Choose Add Group to open the Create New Group dialog box:

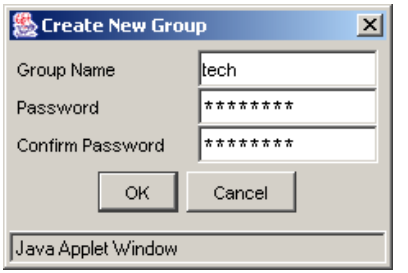


Fig. 2:2-25 Create New Group box

2. Enter up to 20 characters for the **Group Name**.

***NOTES**: The name of the master IP group must be less than 20 characters; cannot be "IP", "NT", or LDAP", and cannot contain spaces. The first character cannot be a digit.*

The following characters cannot be used in the name: "." (period), "," (comma), ":" (colon), ";" (semi-colon), "!" (exclamation point), "?" (question mark), "&" (ampersand), "*" (asterisk), """ (quotation mark), "'" (apostrophe), "`" (grave accent mark), "~" (tilde), "^" (caret), "_" (underscore), "|" (pipe), "/" (slash), "\", (backslash)", "\\" (double backslashes), "(" (left parenthesis), ")" (right parenthesis), "{" (left brace), "}" (right brace), "[" (left bracket), "]" (right bracket), "@" (at sign), "#" (pound sign), "$" (dollar sign), "%" (percent sign), "<" (less than symbol), ">" (greater than symbol), "+" (plus symbol), "-" (minus sign), "=" (equals sign).

3. Enter the **Password**, and re-enter it in the **Confirm Password** field, using eight to 20 characters and at least one alpha character, one numeric character, and one special character. The password is case sensitive.

4. Click **OK** to add the group to the tree.

***NOTE**: Information on defining the group and its members and establishing their filtering profiles can be found in the Group Administrator Section of this user guide.*

Refresh

Refresh IP Groups

From the IP group menu, click Refresh whenever changes have been made in this branch of the tree.

Chapter 3: Library screen

The Library screen is comprised of windows and dialog boxes used for adding and maintaining library categories. Library categories are used when creating or modifying filtering profiles.

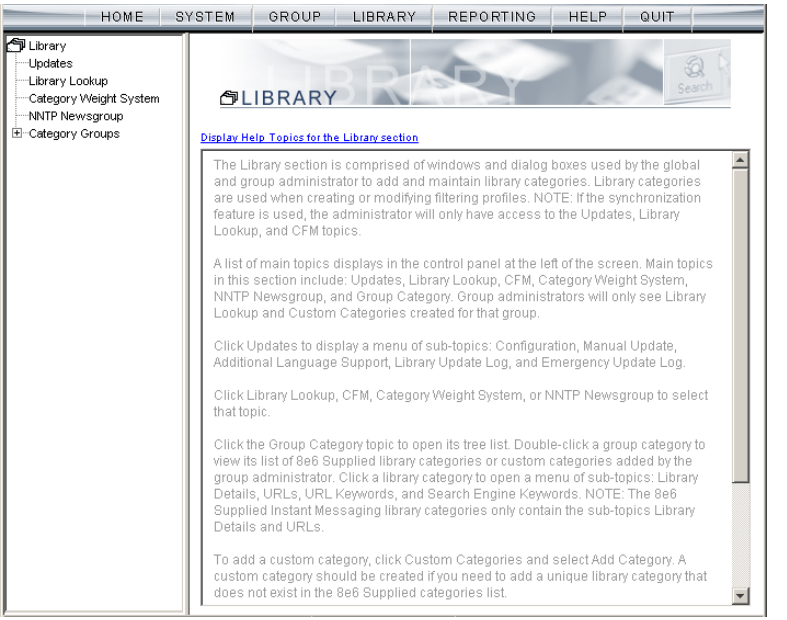


Fig. 2:3-1 Library screen

A list of main topics displays in the navigation panel at the left of the screen: Updates, Library Lookup, Category Weight System, NNTP Newsgroup, and Category Groups.

Click Updates to display a menu of sub-topics: Configuration, Manual Update, Additional Language Support, Library Update Log, and Emergency Update Log.

Click Library Lookup, Category Weight System, or NNTP Newsgroup to select that topic.

To view the list of category groups, double-click Category Groups to open the tree list. Double-click a category group

envelope—any envelope except Custom Categories—to view 8e6 supplied library categories for that group. Click a library category topic to view a menu of sub-topics for that library category item: Library Details, URLs, URL Keywords, and Search Engine Keywords.

To maintain a custom category, click Custom Categories and select either ALLOW or BLOCK to view a menu of sub-topics for that library category item: Library Details, URLs, URL Keywords, and Search Engine Keywords.

***NOTES**: See Appendix A in the Appendices Section for the URL to the page that provides a list of 8e6 supplied library categories. See Appendix B for information on messages that display in the Library Update Log window.*

Instant Messaging library categories only include Library Details and URLs sub-topics.

Updates

Updates includes options for making configurations for library category activities. Click the Updates link to view a menu of sub-topics: Configuration, Manual Update, Additional Language Support, Library Update Log, and Emergency Update Log.

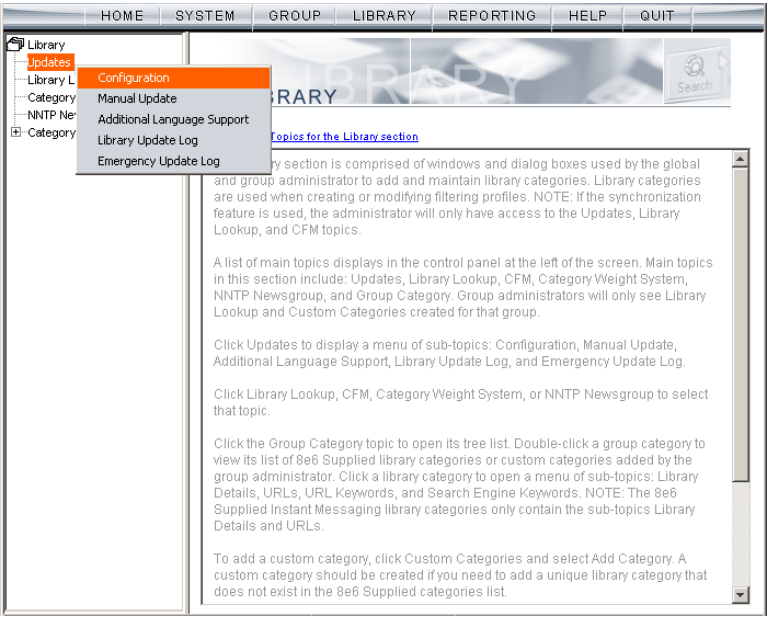


Fig. 2:3-2 Library screen, Updates menu

Configuration window

The Configuration window displays when Configuration is selected from the Updates menu. This window is used for making settings to allow the ProxyBlocker to receive 8e6 supplied library category updates on a daily basis.

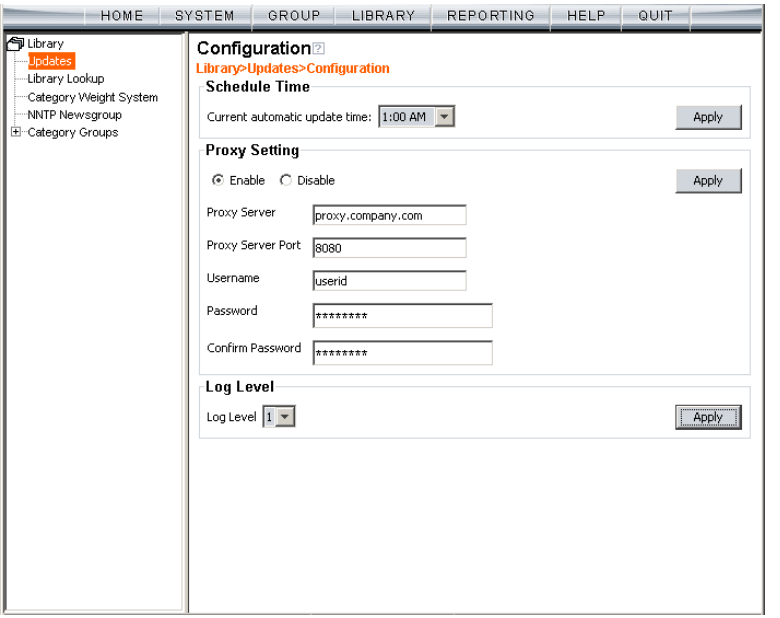


Fig. 2:3-3 Configuration window

Set a Time for Updates to be Retrieved

1. In the Schedule Time frame, by default “1:00 am” displays for the **Current automatic update time**. At this pull-down menu, specify the time at which library updates will be retrieved.
2. Click **Apply** to apply your setting.

Optional: Specify a Proxy Server

1. In the FTP Proxy Setting frame, by default “Disable” is selected. Click “Enable” if the server is in a proxy server environment. This selection activates the fields in this frame.
2. By default, *proxy.company.com* displays as the host name of the **Proxy Server**. Enter the host name for the proxy server in this field.
3. By default, *userid* displays in the **Username** field. Enter the username for the FTP account.
4. Enter the same password in the **Password** and **Confirm Password** fields.
5. Click **Apply** to apply your settings.

Select the Log Level

1. In the Log Level frame, select the log level to be used for specifying the log contents. Log Level 1 includes a summary of library and software update activity. Log Level 2 includes detailed information on library and software update activity.
2. Click **Apply** to apply your settings.

Manual Update window

The Manual Update to 8e6 Supplied Categories window displays when Manual Update is selected from the Updates menu. This window is used for updating specified 8e6 supplied library categories on demand from the update server, if the ProxyBlocker has not received daily updates due to an occurrence such as a power outage.

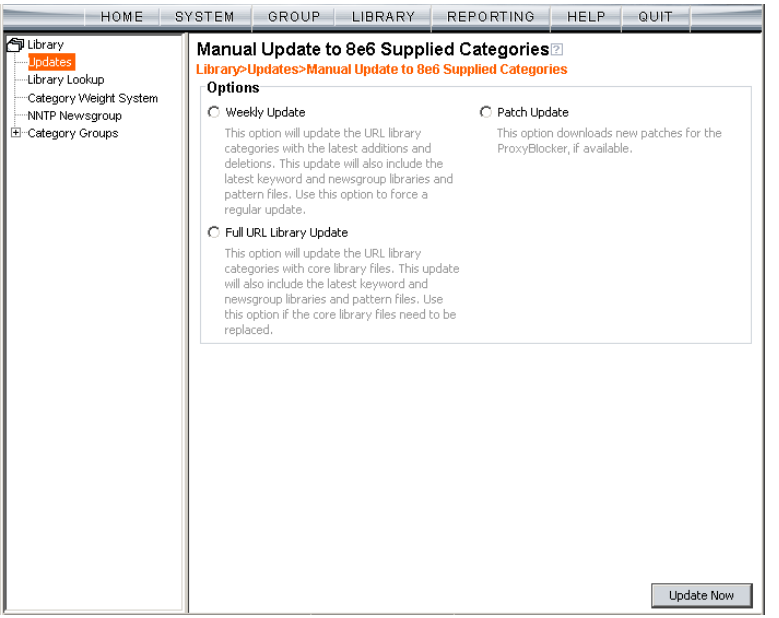


Fig. 2:3-4 Manual Update window

***NOTE**: The Configuration window should be used for scheduling the ProxyBlocker to automatically download libraries on a daily basis.*

Specify the Type of On Demand Update

1. Choose from the following service options by clicking the corresponding radio button:
   - **Weekly Update** - Select this option to update URL library categories with additions and deletions, and to update search engine keywords, newsgroup libraries, and IM/P2P pattern files. Choose this option to force a regular update.
   - **Full URL Library Update** - Select this option to update URL library categories with core library files, and to update search engine keywords, newsgroup libraries, and IM/P2P pattern files. Choose this option to replace the core library files.
   - **Patch Update** - Select this option to download new software updates for the ProxyBlocker, if available. Any software updates that are downloaded can be found in the System section of the console, in the Local Patch window. Using that window, a software update can be selected and applied.
2. Click **Update Now** to begin the update process.

***TIP**: To view update activity, select Library Update Log from the Updates menu. See Appendix B: Traveler Log Messages for a list of log file messages from "Traveler." Traveler is 8e6's executable program that downloads updates to your server from 8e6's main server.*

***NOTES**: For information on applying software updates, see the Patch window in Chapter 1: System screen.*

For information on viewing the status of downloaded software updates, see the Patch Update Log window in Chapter 1, and the Emergency Update Log window in this chapter.

Additional Language Support window

The Additional Language Support window displays when Additional Language Support is selected from the Updates menu. This window is used for including additional 8e6-supported languages in library downloads.

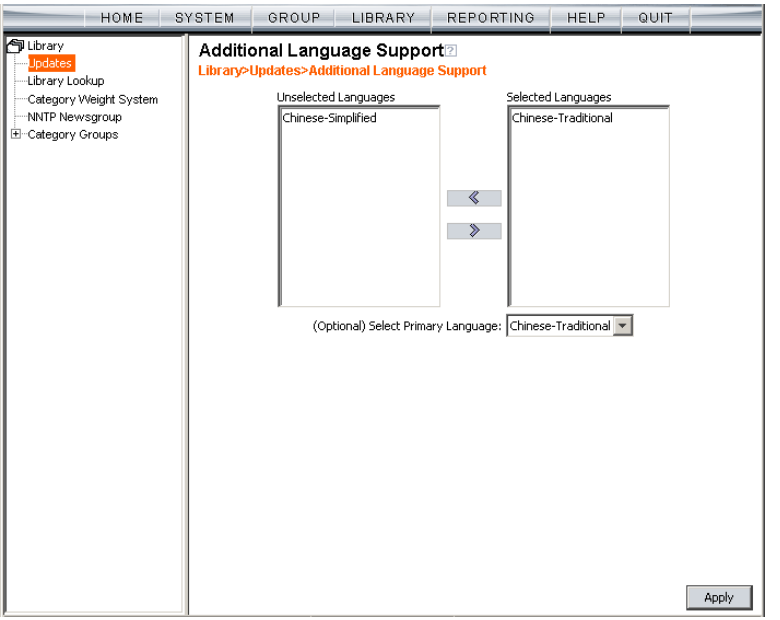


Fig. 2:3-5 Additional Language Support window

Select Additional Languages

1. Make a selection from the Unselected Languages list box and click the right arrow to move that selection to the Selected Languages list box.
2. Once the Selected Languages list box is populated, the (Optional) Select Primary Language pull-down menu includes the language selection(s) in addition to the default “None” selection.

To make an optional selection for a primary language, choose the language from the **(Optional) Select Primary Language** pull-down menu.

***TIP**: To move a language selection back to the Unselected Languages list box, select the item and then click the left arrow.*

3. Click **Apply** to have URLs from the selected language(s) included in the library categories.

Library Update Log window

The Library Update Log window displays when Library Update Log is selected from the Updates menu. This window is used for viewing transfer activity of library updates from the update server to your ProxyBlocker, and for downloading the activity log.

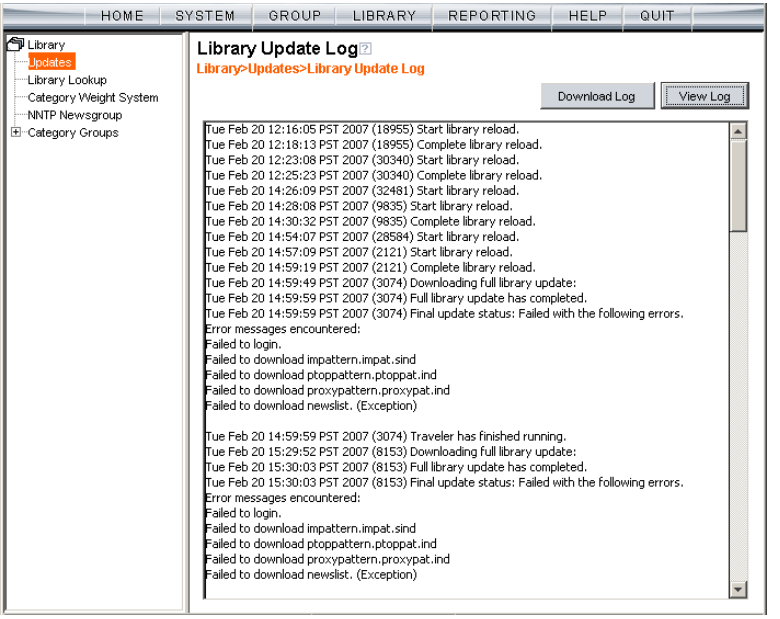


Fig. 2:3-6 Library Update Log window

View the Library Update Process

When performing a manual (on demand) library update, click **View Log** to display contents from the log file with the status of the library update. Keep clicking this button to continue viewing log file data.

***NOTE**: See Appendix B: Traveler Log Messages for information about messages that display in the log file.*

Download Log, View, Print Contents

Download the Log

1. Click **Download Log** to open the alert box containing a message on how to download the log file to your workstation, if using Windows XP.
2. Click **OK** to close the alert box. Two pop-up boxes open:
   - A second alert box asks you to confirm that the file was successfully saved to your machine. Click **OK** in this box after the download is completed.
   - In the File Download dialog box, click **Save**:

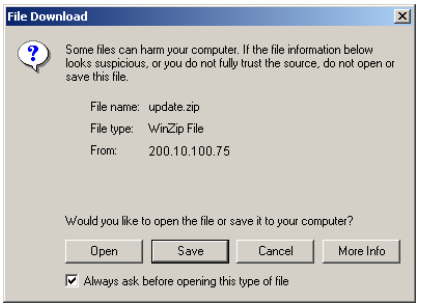


Fig. 2:3-7 Download Log dialog box

This action opens the Save As window:

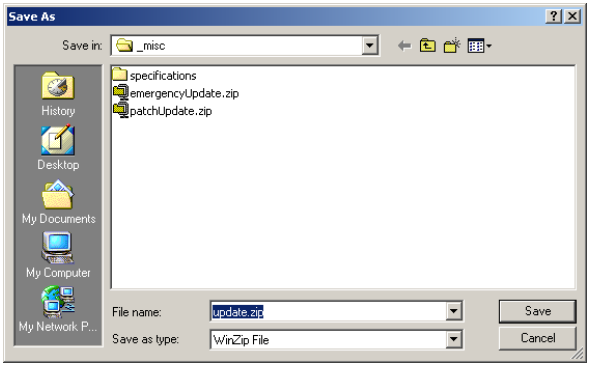


Fig. 2:3-8 Save As pop-up window

3. Find the folder in which to save the file, and then enter the **File name**, retaining the ".zip" file extension. Click **Save** to begin downloading the zip file to your workstation.

   After the file has completely downloaded, the Download complete dialog box opens:

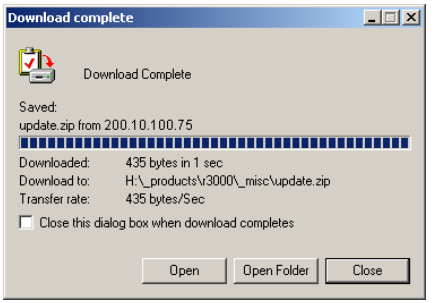


Fig. 2:3-9 Download Complete box

4. You can now open this file, open the folder where the file was saved, or close this dialog box.

***NOTE**: Proceed to View the Contents of the Log for information on viewing or printing the contents of the log file.*

5. Click **OK** to close the alert box asking you to verify that the log file was successfully saved to your machine.

View the Contents of the Log

Once the log file has been downloaded to your workstation, you can view its contents.

1. Find the log file in the folder, and right-click on it to open the pop-up menu:

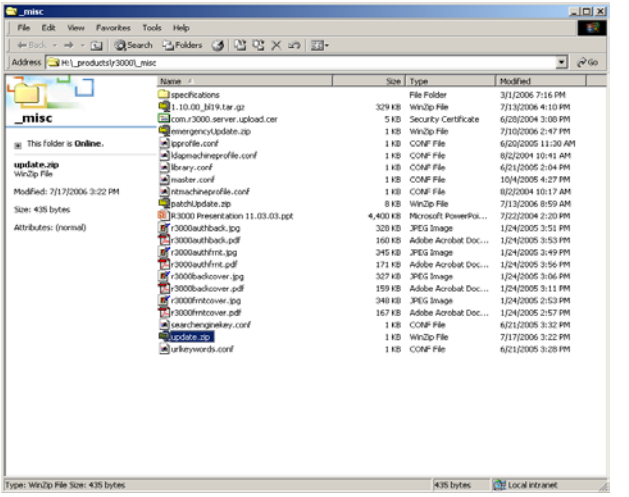


Fig. 2:3-10 Folder containing downloaded file

2. Choose “Open With” and then select a zip file executable program such as “WinZip Executable” to launch that application:

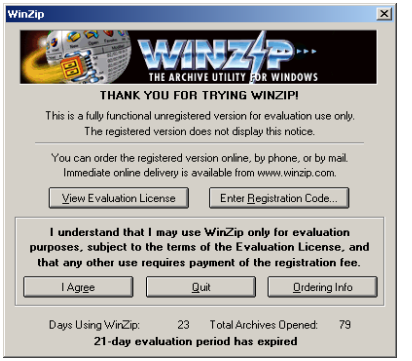


Fig. 2:3-11 WinZip Executable program

3. If using WinZip, click **I Agree** to open the window containing the zip file:

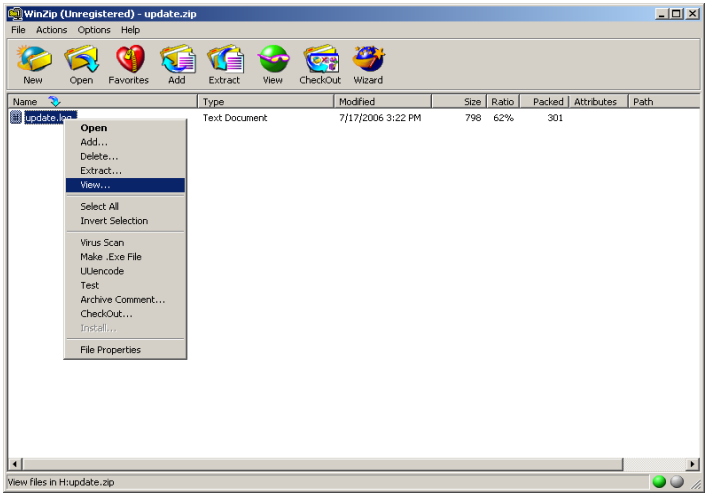


Fig. 2:3-12 WinZip window

4. Right-click the zip file to open the pop-up menu, and choose “View” to open the View dialog box:

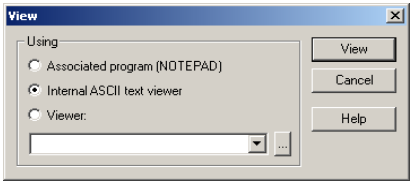


Fig. 2:2-13 View dialog box

5. Select “Internal ASCII text viewer”, and then click **View** to open the View window containing the log file contents:

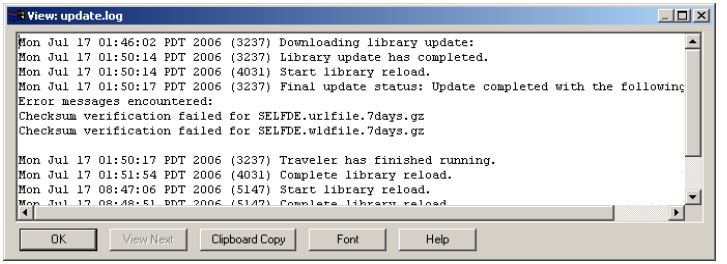


Fig. 2:3-14 View window

Save, Print the Log File Contents

With the log file displaying correctly formatted in WinZip's View window, if you wish to save or print the contents of this file:

1. Click **Clipboard Copy**, wait for the dialog box to open and confirm that the text has been copied to the clipboard, and then click **OK** to close the dialog box.
2. Open Notepad:
   - in Windows XP: Start > All Programs > Accessories > Notepad
   - in Windows 2000: Start > Programs > Accessories > Notepad
3. Paste the contents from the clipboard into the Notepad file:

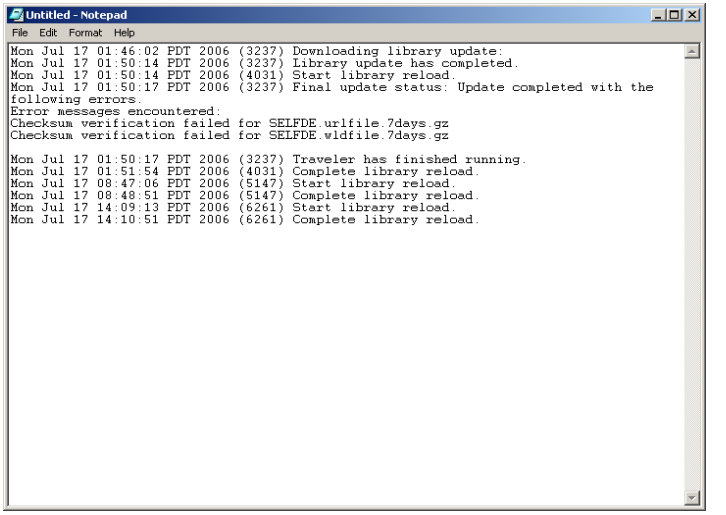


Fig. 2:3-15 Notepad

The correctly formatted Notepad file can now be saved and/or printed.

Emergency Update Log window

The Emergency Update Log window displays when Emergency Update Log is selected from the Updates menu. This window is used for viewing transfer activity of emergency software updates from the update server to your ProxyBlocker, and for downloading the activity log.

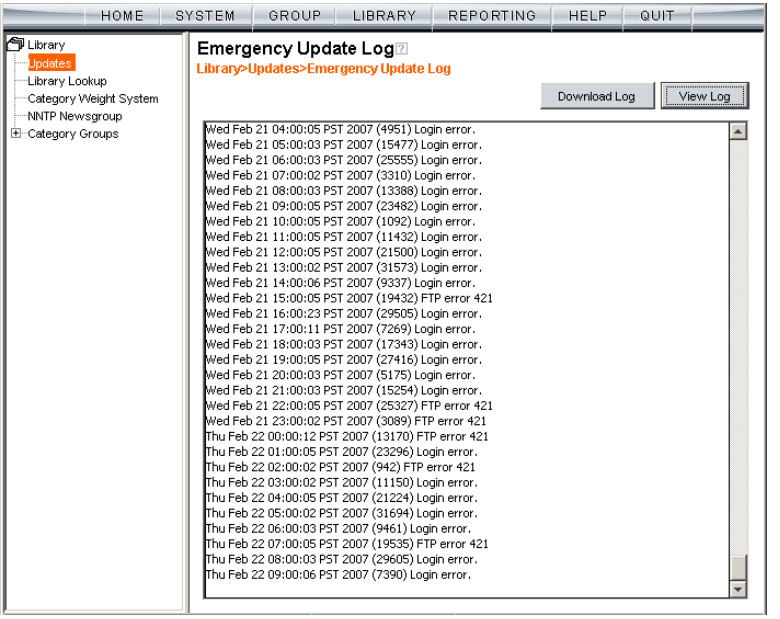


Fig. 2:3-16 Emergency Update Log window

View the Emergency Software Update Process

Click **View Log** to display contents from the emergency software update log file with the status of the software update.

***NOTES**: See Appendix B: Traveler Log Messages for information about messages that display in the log file.*

Download the Software Update Log File

***NOTE**: See Library Update Log window for screen shots pertaining to downloading the software update log file.*

1. Click **Download Log** to open the alert box containing a message on how to download the log file to your workstation, if using Windows XP.
2. Click **OK** to close the alert box. Two pop-up boxes open:
   - A second alert box asks you to confirm that the file was successfully saved to your machine. Click **OK** in this box after the download is completed.
   - In the File Download dialog box, click **Save**; this action opens the **Save As** window:
3. Find the folder in which to save the file, and then enter the **File name**, retaining the ".zip" file extension. Click **Save** to begin downloading the zip file to your workstation. After the file has completely downloaded, the Download complete dialog box opens.
4. You can now open this file, open the folder where the file was saved, or close this dialog box.
5. Click **OK** to close the alert box asking you to verify that the log file was successfully saved to your machine.

***NOTE**: See Library Update Log window for information on viewing the contents of the log file, and printing and/or saving the log file contents.*

Library Lookup

Library Lookup window

The Library Lookup window displays when Library Lookup is selected from the navigation panel. This window is used for verifying whether a URL or search engine keyword or keyword phrase exists in a library category, and to remove it, if necessary.

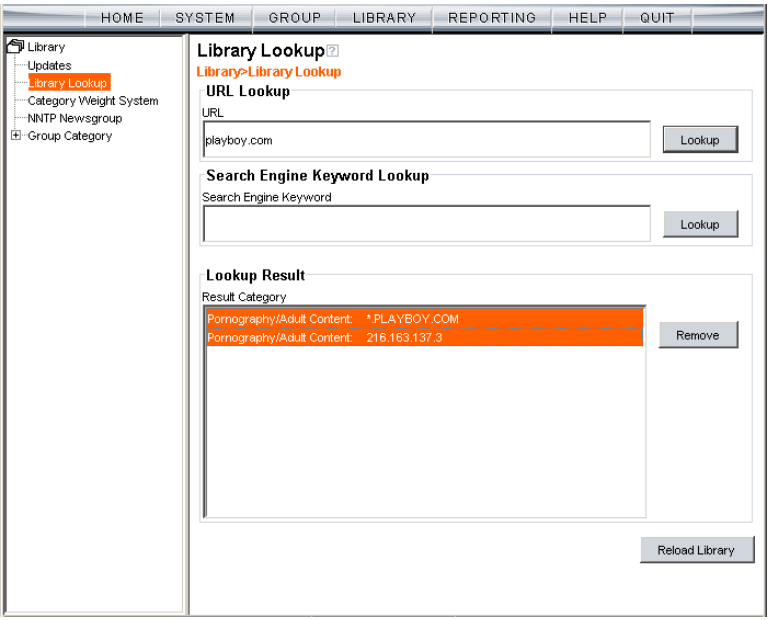


Fig. 2:3-17 Library Lookup window

URL Lookup, Removal

Perform a URL Check

To see if a URL has been included in the library:

1. In the URL Lookup frame, enter the **URL**. For example, enter **http://www.playboy.com**, **playboy.com**, or use a wildcard by entering ***.playboy.com**. A wildcard entry finds all URLs containing text that follows the period (.) after the asterisk (*).

   The following types of URL formats also can be entered in this field:

   - IP address - e.g. "209.247.228.221" in http://209.247.228.221
   - octal format - e.g. http\://0106.0125.0226.0322
   - hexadecimal short format - e.g. http\://0x465596d2
   - hexadecimal long format - e.g. http://0x46.0x55.0x96.0xd2
   - decimal value format - e.g. http://1180014290
   - escaped hexadecimal format - e.g. http://%57%57%57.%41%44%44%49%43%54%49%4E%47%47%41%4D%45%53.%43%4F%4D

***NOTE**: The minimum number of wildcard 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).*

2. Click **Lookup** to open the alert box asking you to wait while the search is being performed.
3. Click **OK** to close the alert box and to display any results in the Result Category list box, showing the long name of the library category, followed by the URL.

Remove a URL

To remove the URL:

1. Select the item from the Result Category list box.
2. Click **Remove**.

Submit an Email to the Administrator

If using a non-Web based email client such as Outlook, you can send an email to the administrator at your organization regarding a URL or search engine keyword that appears to be incorrectly categorized.

1. Select the item(s) from the Result Category list box.
2. Click **Email Result**.

Search Engine Keyword Lookup, Removal

Perform a Search Engine Keyword Check

To see if a search engine keyword or keyword phrase has been included in any library category:

1. In the Search Engine Keyword Lookup frame, enter the **Search Engine Keyword** or keyword phrase, up to 75 alphanumeric characters.
2. Click **Lookup** to display results in the Result Category list box, showing the long name of all categories that contain the search engine keyword/phrase.

Remove a Search Engine Keyword

To remove a search engine keyword/phrase from library categories:

1. After performing the search engine keyword search, select the categories from the Result Category list box.
2. Click **Remove**.

Reload the Library

Once all changes have been made to library windows, click **Reload Library** to refresh.

***NOTE**: Since reloading the library utilizes system resources that impact the performance of the ProxyBlocker, 8e6 recommends clicking Reload Library only **after** modifications to **all** library windows have been made.*

Category Weight System

Category Weight System window

The Category Weight System window displays when Category Weight System is selected from the navigation panel. This feature lets you choose which category will be logged and reported for a URL request that exists in multiple categories (possibly both 8e6 supplied and custom library categories) with the same operational precedence.

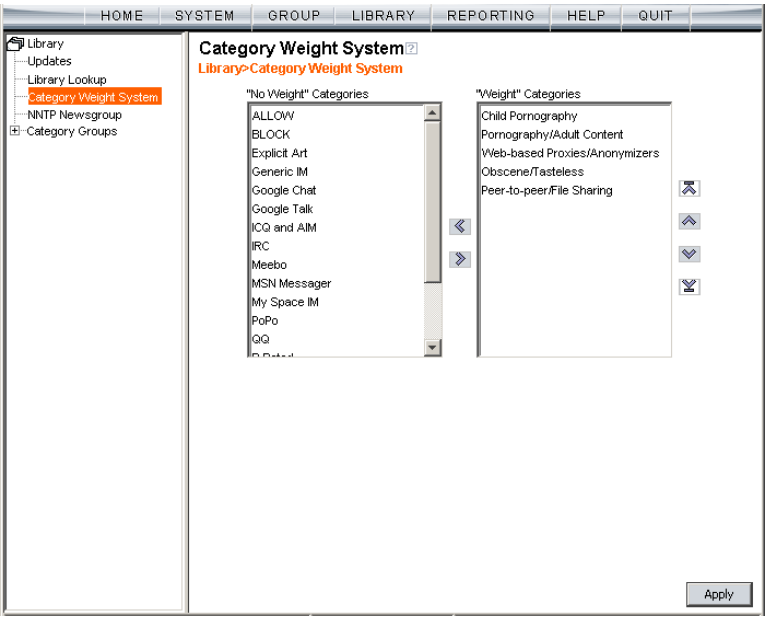


Fig. 2:3-18 Category Weight System window

View the Current Selections

This window contains two list boxes:

- "No Weight" Categories - Populated with 8e6 supplied categories
- "Weight" Categories - Pre-populated by default with categories 8e6 suggests you might want to use for this feature.

The contents in each list box, combined with the end user's profile, help to determine what will appear in the log for the end user's Internet activity.

Method for Weighting Library Categories

The order of operational precedence is: Always Allowed, Blocked, and Pass.

In the event that an end user attempts to access a URL that exists in multiple categories, the highest operational precedence would be logged.

If a URL exists in a category that is Always Allowed, as well as a category set to be Blocked for that user, Always Allowed would be logged because it holds the highest operational precedence.

However, if an end user attempts to access a URL set to be Blocked in several categories, the category with the highest weighting would be logged.

***NOTE**: If a URL exists in multiple un-weighted categories of the same operational precedence, the category logged would be the first one returned by the ProxyBlocker database. Since there is no precedence given, the order in which the category is returned would be random. While it is not necessary to weight all categories, it is recommended that the categories considered a threat should be weighted according to your organization's threat assessment for each category.*

Weighting Library Categories

1. Select the category from the "No Weight" Categories list box.

***TIP**: Multiple categories can be selected by clicking each category while pressing the Ctrl key on your keyboard. Blocks of categories can be selected by clicking the first category, and then pressing the Shift key on your keyboard while clicking the last category.*

2. Use the right arrow to move the selection to the "Weight" Categories list box.

***TIP**: To remove categories from the "Weight" Categories list box, select the ones you wish to remove and use the left arrow to move them to the "No Weight" Categories list box.*

Once the "Weight" Categories list box is populated with categories you wish to include, select a category and use the arrow keys to "weight" it against other categories.

***TIP**: There are four arrow keys to the right of the "Weight" Categories list box. From top to bottom, the first arrow key moves the selection to the top of the list. The second arrow key moves the selection up one position higher in the list. The third arrow key moves the selection down one position lower in the list. The fourth arrow key moves the selection to the bottom of the list.*

3. Click **Apply**. The category positioned at the top of the list will receive the highest "weight" when ranked against other categories, based upon an end user's URL request that appears in multiple library categories set up with the same operational precedence in the end user's filtering profile.

NNTP Newsgroup

NNTP Newsgroup window

The NNTP Newsgroup window displays when NNTP Newsgroup is selected from the navigation panel. This window is used for adding or removing a newsgroup from the libraries.

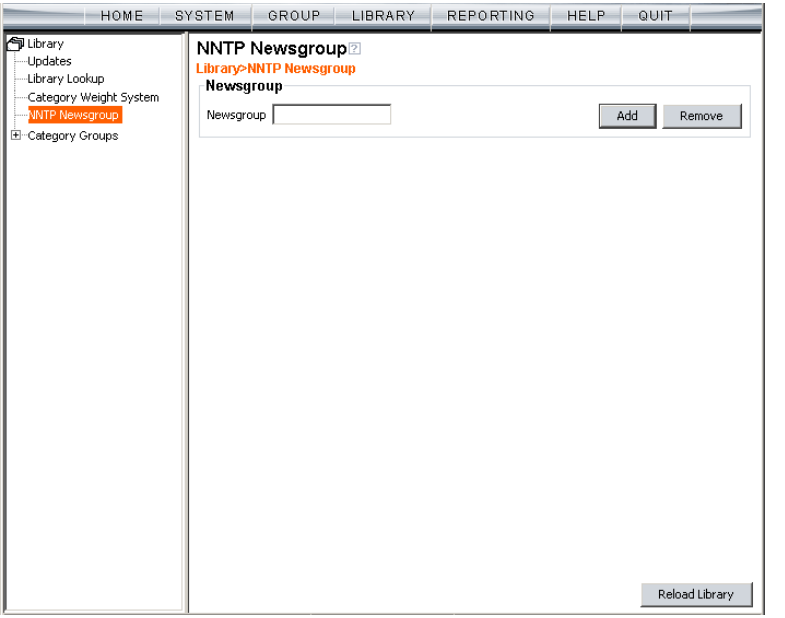


Fig. 2:3-19 NNTP Newsgroup window

Add a Newsgroup to the Library

To add a newsgroup to the library:

1. In the Newsgroup frame, enter the **Newsgroup** address.
2. Click **Add**. If the newsgroup already exists, an alert box will open to inform you that it exists.

Remove a Newsgroup from the Library

To remove a newsgroup from the library:

1. In the Newsgroup frame, enter the **Newsgroup** address.
2. Click **Remove**.

After all changes have been made to library windows, click **Reload Library** to refresh.

***NOTE**: Since reloading the library utilizes system resources that impact the performance of the ProxyBlocker, 8e6 recommends clicking Reload Library only **after** modifications to **all** library windows have been made.*

Category Groups

Category Groups is represented by a tree of library category groups, with each group comprised of 8e6 supplied library categories. 8e6 supplied library categories are updated regularly with new URLs via Traveler, 8e6's executable program that supplies updates to the ProxyBlocker.

Category Groups also contains the Custom Categories category group. The ALLOW and BLOCK library categories within this category group must be maintained by the global administrator.

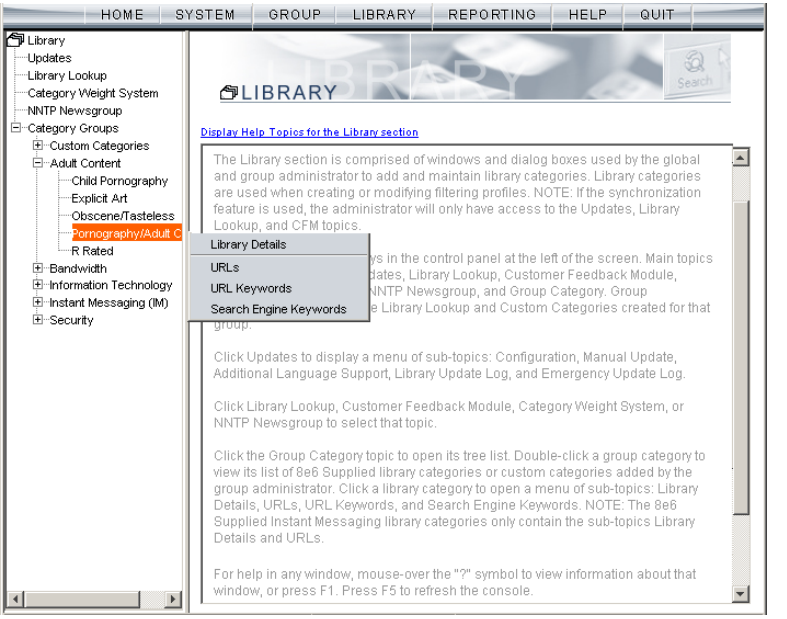


Fig. 2:3-20 Library screen, Category Groups menu

Double-click Category Groups to open the tree and to display category groups.

Double-click a category group's envelope to open that segment of the tree and to view library categories belonging to that group.

Click the 8e6 supplied category link or the ALLOW or BLOCK link in Custom Categories to view a menu of sub-topics: Library Details, URLs, URL Keywords, and Search Engine Keywords. (Menus for Instant Messaging library categories only include the sub-topics Library Details, and URLs).

Library Details window

The Library Details window displays when Library Details is selected from the library category's menu of sub-topics. This window is a view only window.

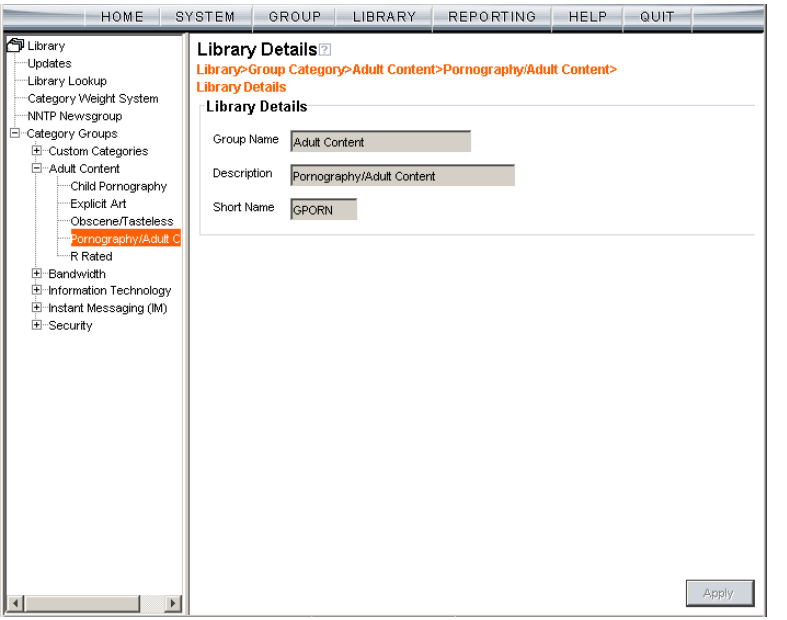


Fig. 2:3-21 Library Details window

View Library Details

This window displays the **Group Name**, **Description**, and **Short Name** of the 8e6 supplied library category.

URLs window

The URLs window displays when URLs is selected from the library category's menu of sub-topics. This window is used for viewing, or adding and/or removing a URL from a library category. A URL can contain a domain name—such as "playboy" in **http://www.playboy.com**—or an IP address—such as "209.247.228.221" in **http://209.247.228.221**. A wildcard asterisk (*) symbol followed by a period (.) can be entered in a format such as ***.playboy.com**, for example, to block access to all URLs ending in ".playboy.com". A URL is used in a filtering profile for blocking a user's access to a specified site or service.

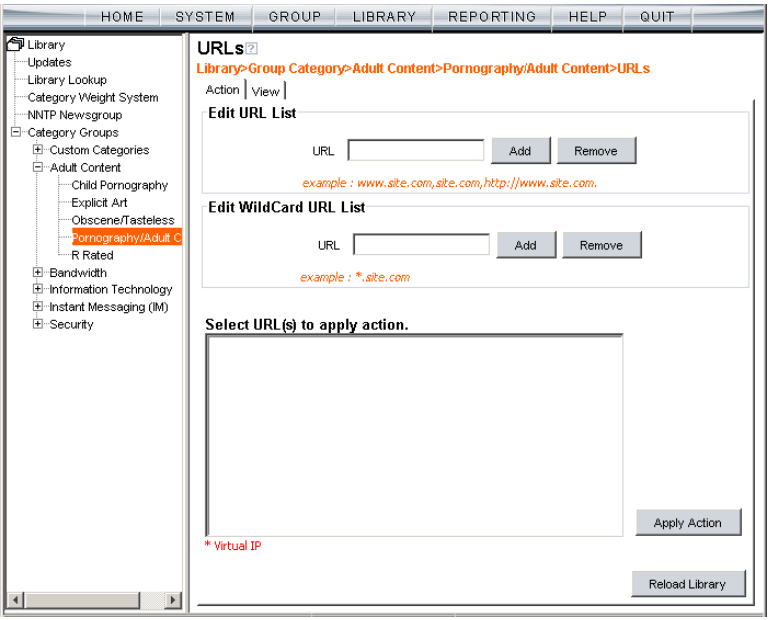


Fig. 2:3-22 URLs window, Action tab

View a List of URLs in the Library Category

To view a list of all URLs that either have been added or deleted:

1. Click the View tab.
2. Make a selection from the pull-down menu for “Addition List”, “Deletion List”, “Wildcard Addition List”, or “Wildcard Deletion List”.
3. Click **View List** to display the specified items in the Select List list box:

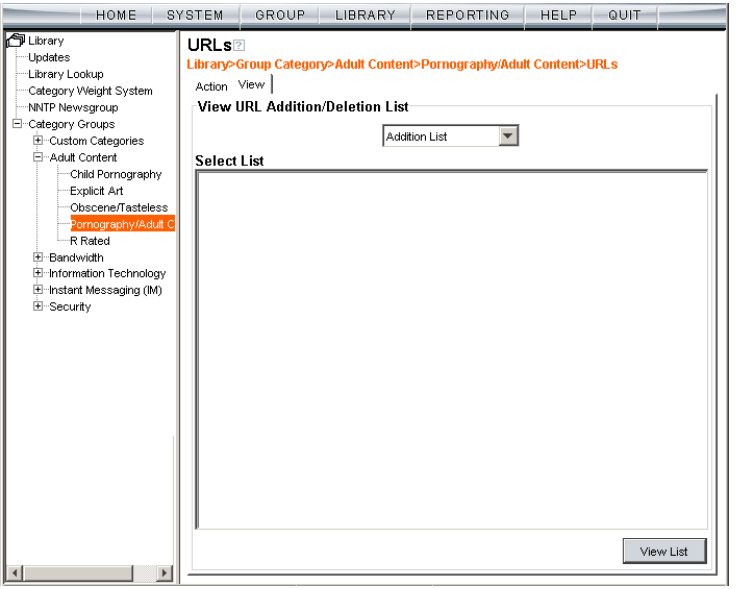


Fig. 2:3-23 URLs window, View tab

Add or Remove URLs, Reload the Library

The Action tab is used for making entries in the URLs window for adding or removing a URL, or reloading the library.

Add a URL to the Library Category

To add a URL to the library category:

1. In the Edit URL List frame, enter the **URL** in a format such as **http://www.playboy.com**, **www.playboy.com**, or **playboy.com**.

   The following types of URL formats also can be entered in this field:

   - IP address - e.g. "209.247.228.221" in http://209.247.228.221
   - octal format - e.g. http\://0106.0125.0226.0322
   - hexadecimal short format - e.g. http\://0x465596d2
   - hexadecimal long format - e.g. http://0x46.0x55.0x96.0xd2
   - decimal value format - e.g. http://1180014290
   - escaped hexadecimal format - e.g. http://%57%57%57.%41%44%44%49%43%54%49%4E%47%47%41%4D%45%53.%43%4F%4D

2. Click **Add** to display the associated URL(s) in the list box below.
3. Select the URL(s) that you wish to add to the category.

***TIP**: Multiple URLs can be selected by clicking each URL while pressing the Ctrl key on your keyboard. Blocks of URLs can be selected by clicking the first URL, and then pressing the Shift key on your keyboard while clicking the last URL.*

4. Click **Apply Action**.

Add a Wildcard URL to the Library Category

***NOTE**: Wildcards are to be used for blocking only. They are not designed to be used for the exceptions function or the always allowed white listing function.*

To add a URL containing a wildcard to the library category:

1. In the Edit WildCard URL List frame, enter the asterisk (*) wildcard symbol, a period (.), and the **URL**.

***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).*

2. Click **Add** to display the associated wildcard URL(s) in the list box below.
3. Select the wildcard URL(s) that you wish to add to the category.
4. Click **Apply Action**.

***NOTE**: Wildcard URL query results include all URLs containing text following the period (.) after the wildcard (*) symbol. For example, an entry of *.porn.com would find a URL such as http://sex.porn.com. However, if a specific URL was added to a library category that is **not** set up to be blocked, and a separate wildcard entry containing a portion of that URL is added to a category that **is** set up to be blocked, the end user will be able to access the non-blocked URL but not any URLs containing text following the wildcard. For example, if http://www.sex.com is added to a category that is not set up to be blocked, and *.sex.com is added to a category set up to be blocked, the end user will be able to access http://www.sex.com since it is a direct match, but will not be able to access http://www.videos.sex.com, since direct URL entries take precedence over wildcard entries.*

Remove a URL from the Library Category

To remove a URL or wildcard URL from the library category:

1. Click the Action tab.
2. Enter the **URL** in the Edit URL List frame or Edit Wild-Card URL List frame, as pertinent.
3. Click **Remove** to display the associated URLs in the list box below.
4. Select the URL(s) that you wish to remove from the category.
5. Click **Apply Action**.

Reload the Library

After all changes have been made to library windows, click **Reload Library** to refresh.

***NOTE**: Since reloading the library utilizes system resources that impact the performance of the ProxyBlocker, 8e6 recommends clicking Reload Library only **after** modifications to **all** library windows have been made.*

URL Keywords window

The URL Keywords window displays when URL Keywords is selected from the library category's menu of sub-topics. This window is used for adding and removing URL keywords from a library category. A library category uses URL keywords to block a user's access to Internet addresses containing keywords included in its list.

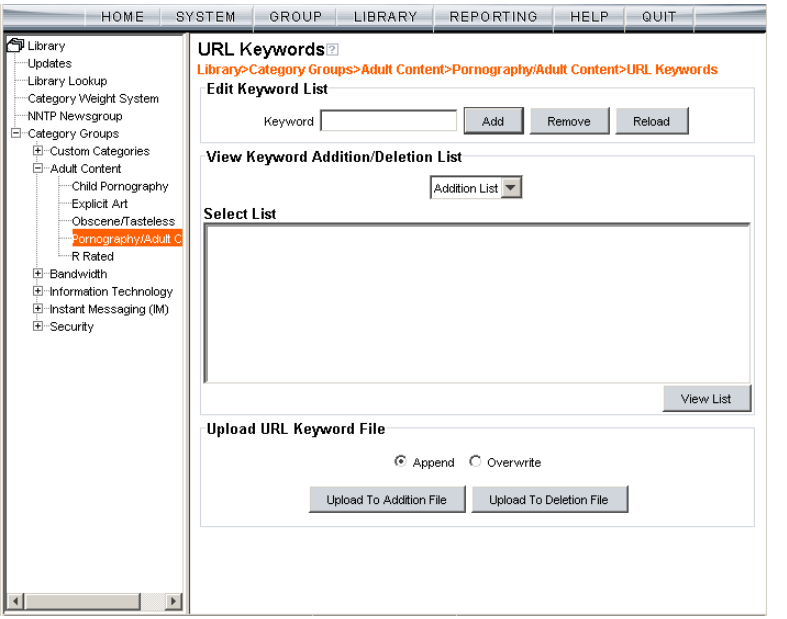


Fig. 2:3-24 URL Keywords window

***NOTE**: If the feature for URL keyword filtering is not enabled in a filtering profile, URL keywords can be added in this window but URL keyword filtering will not be in effect for the user(s). (See the Filter Options tab in the Group screen section for information about enabling URL keyword filtering.)*

***WARNING**: Use extreme caution when setting up URL keywords for filtering. If a keyword contains the same consecutive characters as a keyword set up to be blocked, users will be denied access to URLs that are not even within blocked categories. For example, if all URL keywords containing "sex" are blocked, users will not be able to access a non-pornographic site such as http://www.essex.com.*

View a List of URL Keywords

To view a list of all URL keywords that either have been added or deleted:

1. In the View Keyword Addition/Deletion List frame, make a selection from the pull-down menu for "Addition List", or "Deletion List".
2. Click **View List** to display the specified items in the Select List list box.

Add or Remove URL Keywords

Add a URL Keyword to the Library Category

To add a URL keyword to the library category:

1. Enter the **Keyword** in the Edit Keyword List frame.
2. Click **Add**.

Remove a URL Keyword from the Library

To remove a URL keyword from the library category:

1. Enter the **Keyword** in the Edit Keyword List frame.
2. Click **Remove**.

Upload a List of URL Keywords to the Library

Before uploading a text file with URL keyword additions or deletions, in the Upload URL Keyword File frame, specify whether the contents of this file will add to the current file, or overwrite the current file on the server, by clicking the "Append" or "Overwrite" radio button.

Upload a List of URL Keyword Additions

To upload a text file with URL keyword additions:

1. Click **Upload To Addition File** to open the Upload Library Keyword pop-up window:

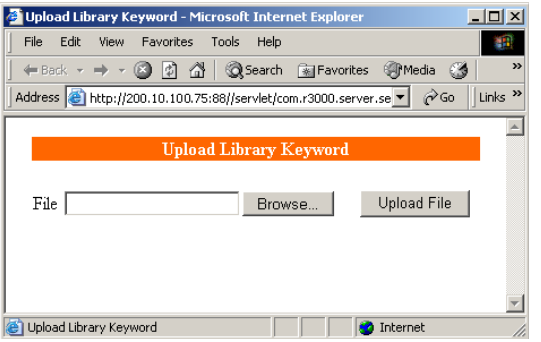


Fig. 2:3-25 Upload Library Keyword pop-up window

2. Click **Browse** to open the Choose file window.
3. Select the file to be uploaded.
4. Click **Upload File** to upload this file to the server.

***NOTE**: A URL keyword text file must contain one URL keyword per line.*

***WARNING**: The text file uploaded to the server will overwrite the current file.*

Upload a List of URL Keyword Deletions

To upload a text file with URL keyword deletions:

1. Click **Upload To Deletion File** to open the Upload Library Keyword pop-up window (see Fig. 2:3-25).
2. Click **Browse** to open the Choose file window.
3. Select the file to be uploaded.
4. Click **Upload File** to upload this file to the server.

Reload the Library

After all changes have been made to library windows, click **Reload** to refresh.

***NOTE**: Since reloading the library utilizes system resources that impact the performance of the ProxyBlocker, 8e6 recommends clicking Reload only **after** modifications to **all** library windows have been made.*

Search Engine Keywords window

The Search Engine Keywords window displays when Search Engine Keywords is selected from the library category's menu of sub-topics. This window is used for adding and removing search engine keywords/phrases to and from a library category. A library category uses search engine keywords to block searches on subjects containing keywords included in its list.

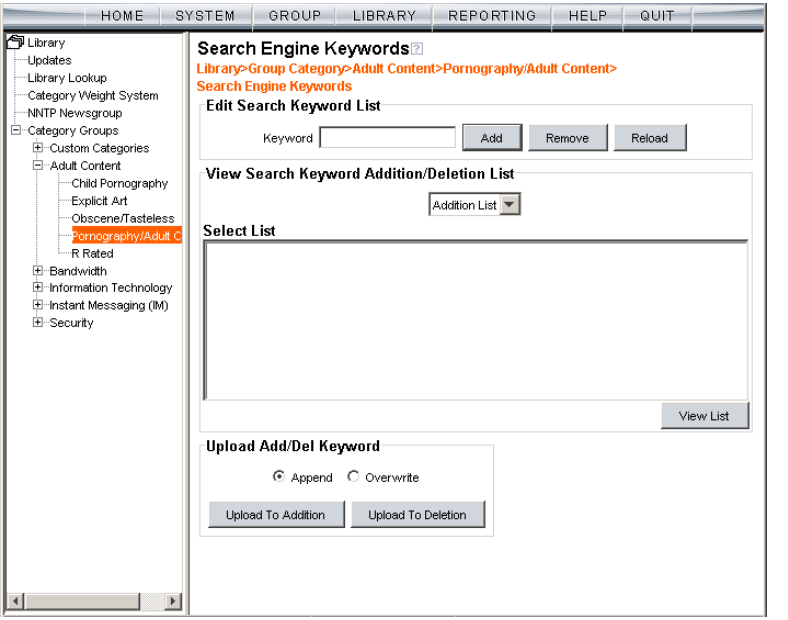


Fig. 2:3-26 Search Engine Keywords window

***NOTE**: Master lists cannot be uploaded to any 8e6 supplied library category. See the Custom Categories sub-section of the Group Administrator Section of this user guide for information on uploading a master list to the server.*

***NOTE**: If the feature for search engine keyword filtering is not enabled in a filtering profile, search engine keywords can be added in this window but search engine keyword filtering will not be in effect for the user(s). (See the Filter Options tab in the Group screen section for information about enabling search engine keyword filtering.)*

***WARNING**: Use extreme caution when setting up search engine keywords for filtering. If a non-offending keyword contains the same consecutive characters as a keyword set up to be blocked, users will be denied the ability to perform a search using keywords that are not even in blocked categories. For example, if all searches on "gin" are set up to be blocked, users will not be able to run a search on a subject such as "cotton gin". However, if the word "sex" is set up to be blocked, a search will be allowed on "sexes" but not "sex" since a search engine keyword must exactly match a word set up to be blocked.*

View a List of Search Engine Keywords

To view a list of all search engine keywords/phrases that either have been added or deleted:

1. In the View Search Keyword Addition/Deletion List frame, make a selection from the pull-down menu for "Addition List", or "Deletion List".
2. Click **View List** to display the specified items in the Select List list box.

Add or Remove Search Engine Keywords

Add a Search Engine Keyword to the Library

To add a search engine keyword/phrase to the library category:

1. In the Edit Search Keyword List frame, enter up to 75 alphanumeric characters in the **Keyword** field.
2. Click **Add**.

Remove a Search Engine Keyword from the Library

To remove a search engine keyword/phrase from the library category:

1. In the Edit Search Keyword List frame, enter up to 75 alphanumeric characters in the **Keyword** field.
2. Click **Remove**.

Upload a List of Search Engine Keywords

Before uploading a text file with search engine keyword/phrase additions or deletions, in the Upload Add/Del Keyword frame, specify whether the contents of this file will add to the current file, or overwrite the current file on the server by clicking the “Append” or “Overwrite” radio button.

Upload a List of Search Engine Keyword Additions

To upload a text file with search engine keyword/phrase additions:

1. Click **Upload To Addition** to open the Upload Library Keyword pop-up window (see Fig. 2:3-25).
2. Click **Browse** to open the Choose file window. Select the file to be uploaded.
3. Click **Upload File** to upload this file to the server.

***NOTE**: A search engine keywords text file must contain one keyword/phrase per line.*

***WARNING**: The text file uploaded to the server will overwrite the current file.*

Upload a List of Search Engine Keyword Deletions

To upload a text file with search engine keyword/phrase deletions:

1. Click **Upload To Deletion** to open the Upload Library Keyword pop-up window (see Fig. 2:3-25).
2. Click **Browse** to open the Choose file window. Select the file to be uploaded.
3. Click **Upload File** to upload this file to the server.

Reload the Library

After all changes have been made to library windows, click **Reload** to refresh.

***NOTE**: Since reloading the library utilizes system resources that impact the performance of the ProxyBlocker, 8e6 recommends clicking Reload only **after** modifications to **all** library windows have been made.*

Chapter 4: Reporting screen

The Reporting screen contains options for transferring and/or reviewing Internet usage data collected by the Proxy-Blocker.

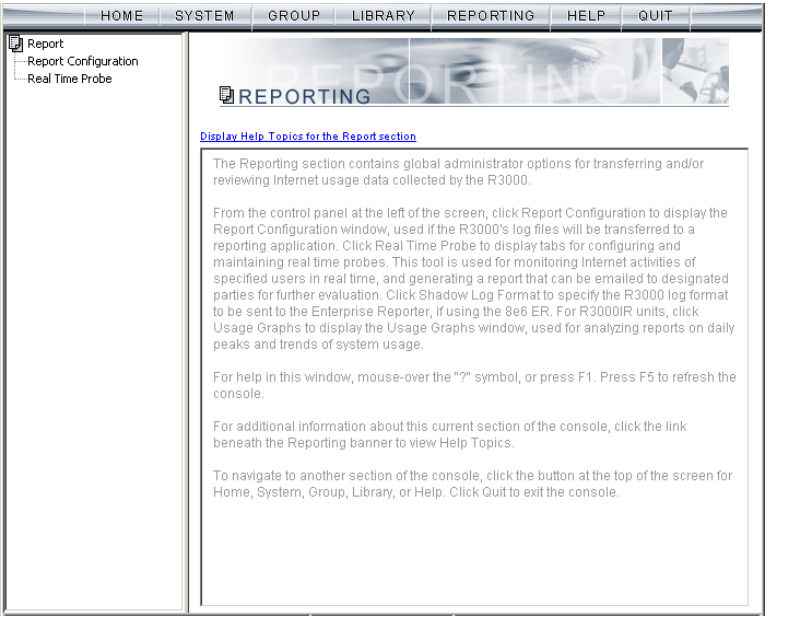


Fig. 2:4-1 Reporting screen

From the navigation panel at the left of the screen, click Report Configuration to display the Report Configuration window, used if the ProxyBlocker's log files will be transferred to a reporting application. Click Real Time Probe to display windows for configuring and maintaining real time probes. This tool is used for monitoring Internet activities of specified users in real time.

***NOTE**: Information on configuring the Enterprise Reporter (ER) to work with the ProxyBlocker can be found in Appendix E of the Appendices Section.*

Report Configuration

Report Configuration window

The Report Configuration window displays when Report Configuration is selected from the navigation panel. This window is used if a reporting application needs to be set up to receive logs from the ProxyBlocker.

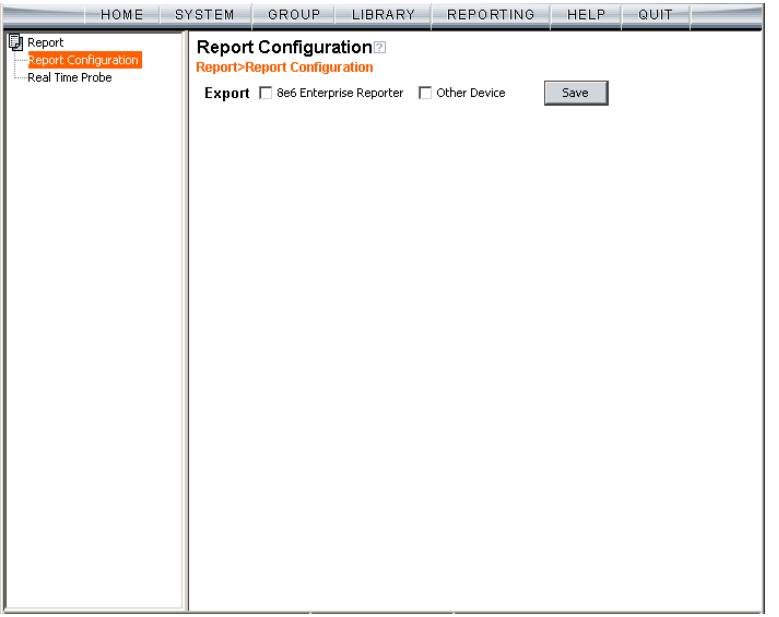


Fig. 2:4-2 Report Configuration window

Specify the Reporting Device

By default, no option is selected at the **Export** field.

If ProxyBlocker logs will be exported to a reporting application:

1. Click the checkbox corresponding to the reporter to be used for transferring logs: “8e6 Enterprise Reporter”, or “Other Device”.

2. Click **Save**.

8e6 Enterprise Reporter

If “8e6 Enterprise Reporter” was selected, the 8e6 Enterprise Reporter tab displays by default. On this tab, you need to specify criteria for the ER server that will receive logs from the ProxyBlocker.

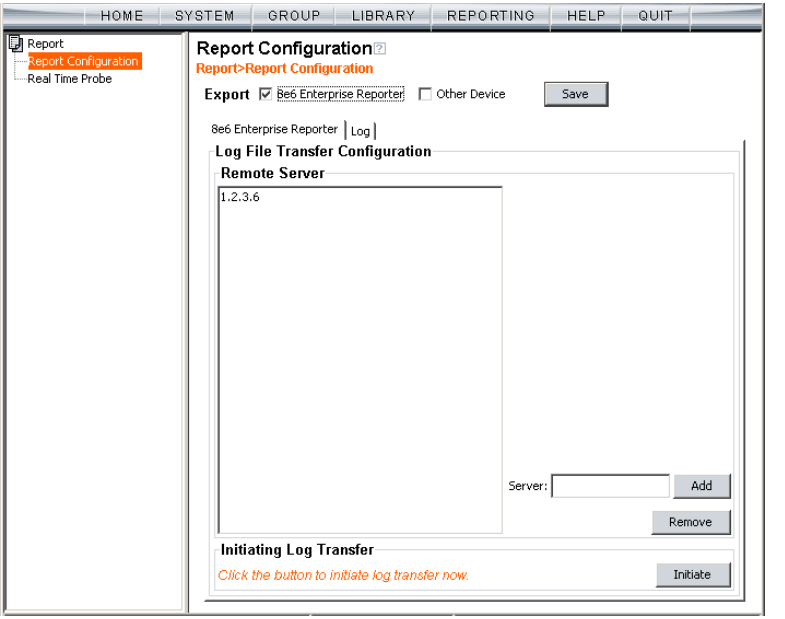


Fig. 2:4-3 Report Configuration window, 8e6 ER option, ER tab

Edit ER Server Information

In the Log File Transfer Configuration frame, by default the IP address *1.2.3.6* displays in the Remote Server list box.

To add the IP address assigned to the ER server:

1. Enter the LAN 1 IP address in the **Server** field.
2. Click **Add** to include this IP address in the Remote Server list box.

To remove an IP address from the list box:

1. Select the IP address.

2. Click **Remove**.

Execute Log Transfer Now

In the Initiating Log Transfer frame, click **Initiate** to transfer the log on demand.

View Transfer Activity to the ER

After the ER has been configured and logs have been transferred from the ProxyBlocker to the ER, you can view transfer activity.

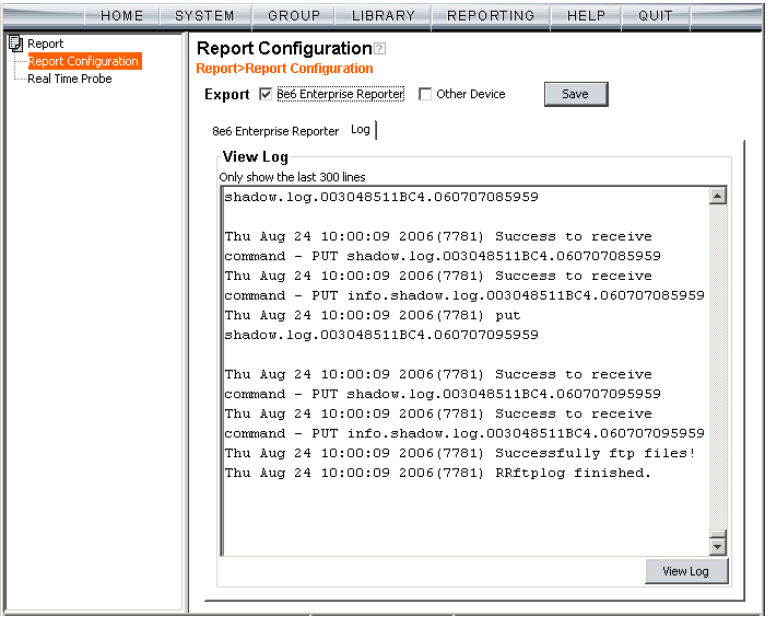


Fig. 2:4-4 Report Configuration window, 8e6 ER option, Log tab

1. Click the Log tab.

2. Click **View Log** to view up to the last 300 lines of transfer activity in the View Log frame.

Other Device

If “Other Device” was selected, the Other Device tab displays by default. On this tab, you need to specify criteria for the reporter that will receive logs from the ProxyBlocker.

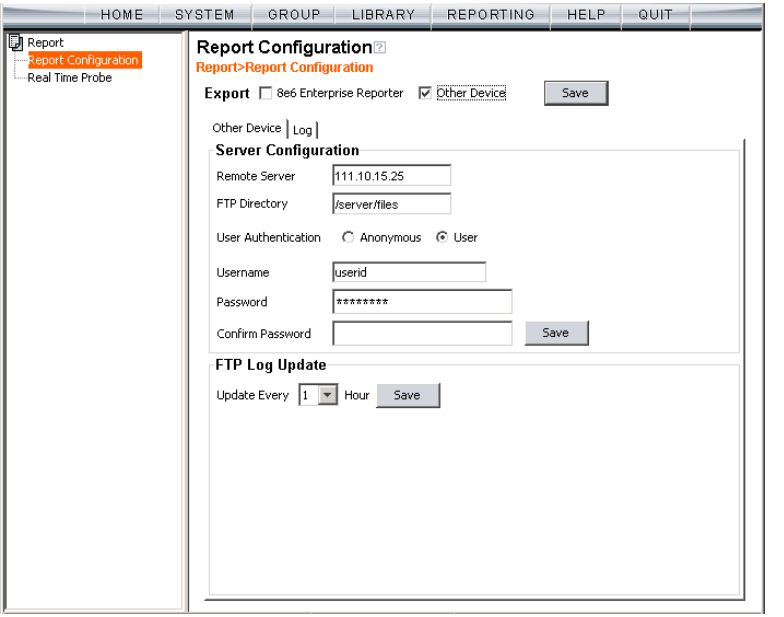


Fig. 2:4-5 Report Configuration window, Other Device option and tab

Enter or Edit Server Information

In the Server Configuration frame:

1. In the **Remote Server** field, enter the IP address of the remote server.
2. In the **FTP Directory** field, enter the path where log files will be stored.

3. At the User Authentication field, “User” is selected by default, indicating that a username and password will be required for FTP transfers. Click the “Anonymous” radio button if no user authentication will be required for FTP transfers.
4. By default, the **Username** field is activated. For this option, *userid* displays by default. Change the username by entering a valid one for FTP transfers.
5. Enter the same password in the **Password** and **Confirm Password** fields.

***NOTE**: If “Anonymous” is selected, these fields are deactivated.*

6. Click **Save**.

In the FTP Log Update frame:

1. At the **Hour** field, make a selection from the pull-down menu (1, 2, 3, 4, 6, 8, 12, 24) to specify the interval between hours—in military time—when the update should occur:

   1 = updates occur each hour.

   2 = updates occur every two hours, at these intervals of time: 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24.

   3 = updates occur every three hours, at these intervals of time: 3, 6, 9, 12, 15, 18, 21, 24.

   4 = updates occur every four hours, at these intervals of time: 4, 8, 12, 16, 20, 24.

   6 = updates occur every six hours, at these intervals of time: 6, 12, 18, 24.

   8 = updates occur every eight hours, at these intervals of time: 8, 16, 24.

   12 = updates occur every 12 hours, at these intervals of time: 12, and 24.

   24 = updates occur every 24 hours.
2. Click **Save**.

View Transfer Activity to the Reporting Device

After logs have been transferred from the ProxyBlocker to the reporting device, the Log tab can be clicked to view transfer activity.

On this tab, click **View Log** to view up to the last 300 lines of transfer activity in the View Log frame.

Real Time Probe

Real Time Probe window

The Real Time Probe window displays when Real Time Probe is selected from the navigation panel. This feature lets the probe administrator monitor a user's Internet usage in real time to see if that user is using the Internet appropriately.

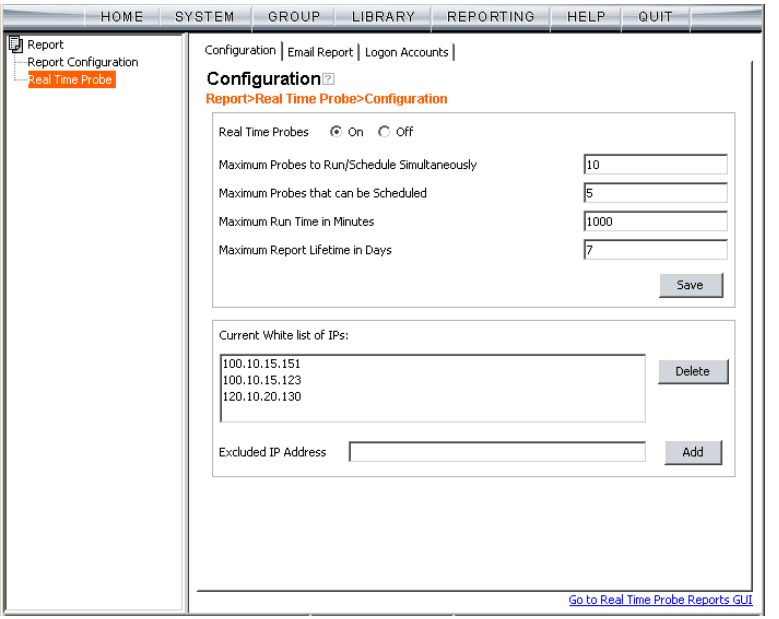


Fig. 2:4-6 Real Time Probe window, Configuration tab

Configuration

Enable Real Time Probes

1. On the Configuration tab, click “On”.
2. Click **Save** to enable the Real Time Probes feature. As a result, all elements in this window become activated.

Set up Real Time Probes

1. Enter the **Maximum Probes to Run/Schedule Simultaneously**, up to 99 probes. The default setting is *10* probes.
2. Enter the **Maximum Probes that can be Scheduled**, equal to or less than the maximum probes that can run at the same time. The default setting is *5* probes.
3. Enter the **Maximum Run Time in Minutes** the probe will search for URLs, up to 1440 minutes (24 hours). The default setting is *1000* minutes.
4. Enter the **Maximum Report Lifetime in Days** to keep a saved report before deleting it. The default setting is *7* days.
5. Click **Save**.

Exclude an IP Address from Real Time Probing

1. Enter the **Excluded IP Address** of a machine to be bypassed from real time probing.
2. Click **Add** to add the IP address in the Current White list of IPs.

Remove IPs from the White List

1. Select the IP address(es) from the Current White list of IPs list box.
2. Click **Delete** to remove the IP address(es) from the white list.

Report Recipients

Click the Report Recipients tab to display Email Report:

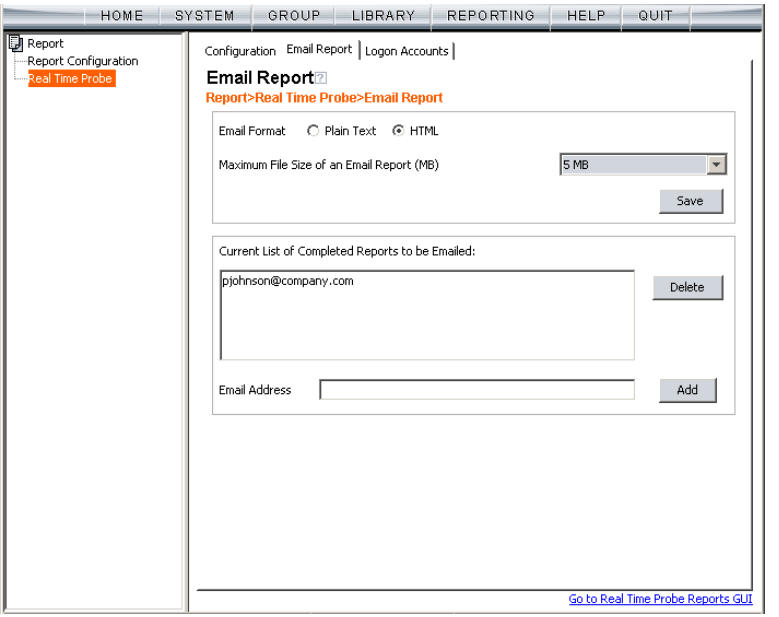


Fig. 2:4-7 Real Time Probe window, Report Recipients tab

Specify Email File Criteria

1. Click the radio button corresponding the to the **Email Format** to be used for the file: “Plain Text” or “HTML”. By default, “HTML” is selected.

2. Select the **Maximum File Size of an Email Report (MB)** that can be sent, from 1MB increments up to 20MB. The default is *5* MB.
3. Click **Save**.

Set up Email Addresses to Receive Reports

1. Enter the **Email Address** of an individual who will receive completed probe reports.
2. Click **Add** to include the email address in the Current List of Completed Reports to be Emailed list box.

***NOTE**: The maximum number of report recipients is 50. If more than 50 recipients need to be included, 8e6 recommends setting up an email alias list for group distribution.*

Remove Email Addresses

1. Select the email address(es) from the Current List of Completed Reports to be Emailed list box.
2. Click **Delete** to remove the email address(es) from list.

Logon Accounts

Click the Logon Accounts tab to display Logon Accounts:

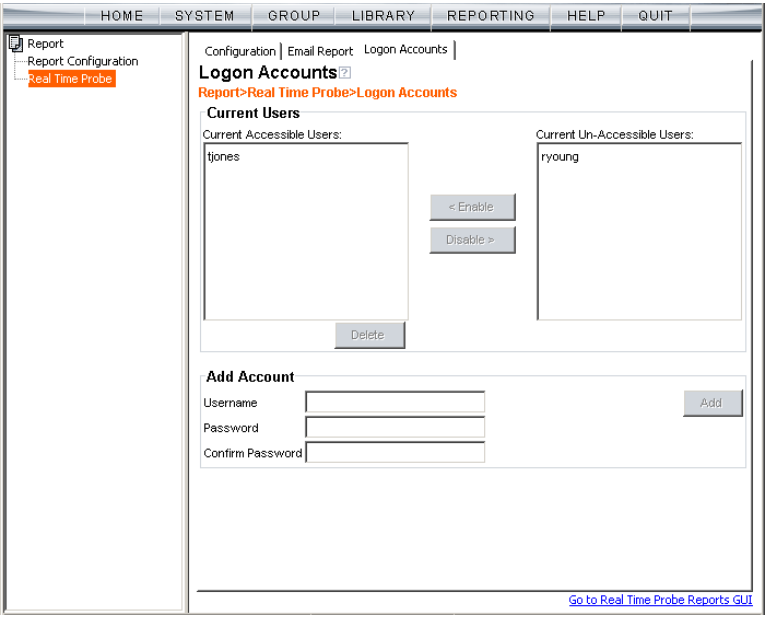


Fig. 2:4-8 Real Time Probe window, Logon Accounts tab

Set up Users Authorized to Create Probes

1. Enter the **Username** of a staff member who is authorized to create real time probes.
2. Enter the user's password in the **Password** and **Confirm Password** fields, using eight to 20 characters and at least one alpha character, one numeric character, and one special character. The password is case sensitive.
3. Click **Add** to include the username in the Current Accessible Users list box.

***NOTE**: When an authorized staff member is added to this list, that username is automatically added to the Current Un-Accessible Users list box in the Logon Accounts tab of the X Strikes Blocking window.*

Deactivate an Authorized Logon Account

To deactivate an authorized user's account:

1. Select the username from the Current Accessible Users list box.
2. Click **Disable** to move the username to the Current Un-Accessible Users list box.

Delete a Logon Account

To delete a user's account:

1. Select the username from the Current Accessible Users list box.
2. Click **Delete**.

***WARNING**: By deleting a logon account, in addition to not being able to create real time probes, that user will also be removed from the list of users authorized to unlock workstations. (See Chapter 1: System screen, X Strikes Blocking for information on reseting strikes and unlocking workstations.)*

Go to Real Time Probe Reports GUI

When the global administrator clicks **Go to Real Time Probe Reports GUI**, either the Re-login window or the Real Time Probe Reports pop-up window opens.

Re-login window

The Re-login window opens if the user's session needs to be validated:

Fig. 2:4-9 Re-login window

1. Enter your **Username**.
2. Enter your **Password**.
3. Click **OK** to close the Re-login window and to re-access the ProxyBlocker console.

Real Time Probe Reports

The Real Time Probe Reports window is comprised of the View and Create tabs. The View tab displays by default (see Fig. 2:4-11), showing the global administrator information on all active probes.

***NOTE**: An authorized staff member can click a link in an email alert or type in **http://x.x.x.x:88/RtProbe.jsp** in the address field of a browser window—in which "x.x.x.x" is the IP address of the ProxyBlocker—to only see probes he/she created.*

Create a Real Time Probe

Click the Create tab to enter and specify criteria for the report you wish to generate:

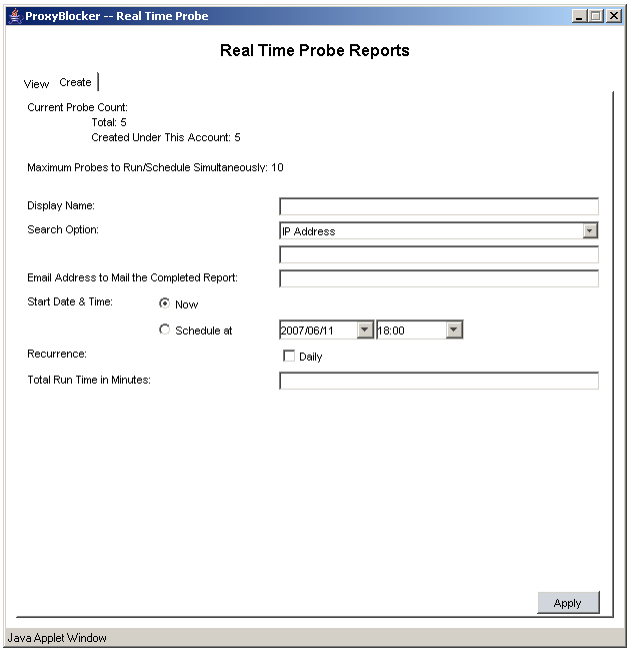


Fig. 2:4-10 Real Time Probe Reports, Create tab

The Current Probe Count displays the Total number of active probes, and the number of probes Created Under This Account. The Maximum Probes to Run/Schedule Simultaneously entered on the Configuration tab displays.

1. Enter up to 40 characters for the **Display Name**. This label will be used for the probe in the View tab and in the email report to be sent to the designated recipient(s).
2. Select the **Search Option**: “IP Address”, “User Name”, “URL”, or “Category”.
3. Enter or specify criteria for the selected Search Option:
   - “IP Address”: Enter the IP address to be probed. This selection generates a report with data for the specified IP address.
   - “User Name”: Enter the characters to be included in the User Name(s) to be probed. The entry in this field is case-sensitive. This selection generates a report with data for all usernames containing the consecutive characters you specified.

     In this example, if ***ART*** is entered, “ART”, “GARTH”, and “MARTA” would be included in the report. But “Art” or “BARRETT” would not be included, since the former username does not contain all uppercase letters, and the latter username does not contain consecutive characters.
   - “URL”: Enter the characters to be included in the URL(s) to be probed. The entry in this field is case-sensitive and the asterisk (*) character is not allowed. This selection generates a report with data for all URLs containing the consecutive characters you specified.

     In this example, if ***mail*** is entered, “http://www.hotmail.com” and “http://loginnet.passport.com/login.srf?id=2&svc=mail&cbid=24325&msppjph=1&tw=0&fs=1&fsa=1&fsat=1296000&lc=1033&_lang=EN” would be included in the report.

- "Category": Select the library category to be probed. This selection generates a report with data for the specified library category.

***NOTE**: Up to 250 characters will be accepted for the IP Address, User Name, or URL.*

4. If you wish to send the completed report to a specified email address, enter the **Email Address to Mail the Completed Report**.
5. Specify the **Start Date & Time** by clicking the appropriate radio button:
   - "Now" - click this radio button to run the probe now.
   - "Schedule at" - click this radio button to schedule a time for running the probe. Select the date and time from the pull-down menus.

     A probe that is scheduled to run at a specified date and time can be scheduled to run on a daily basis by checking the "Daily" checkbox at the **Recurrence** field.
6. Enter the **Total Run Time in Minutes**.
7. Click **Apply**.

View Real Time Probe Details

Click the View tab to view details about active probes:

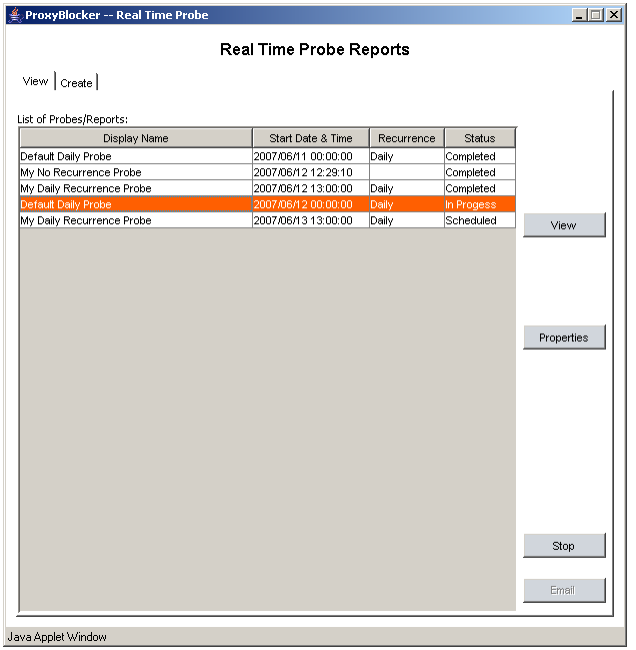


Fig. 2:4-11 Real Time Probe Reports, View tab

The Display Name shows the name assigned to the probe on the Create tab. The Start Date & Time displays in the YYYY/MM/DD HH:MM:SS format. “Daily” displays in the Recurrence column if the probe is scheduled to run on a daily basis. The Status of the probe displays: “Completed”, “In Progress”, or “Scheduled”.

By selecting a probe, buttons for the probe become activated, based on the state of the probe. The following options are available for each of the probe statuses:

- Completed: View, Properties, Delete, Email
- In Progress: View, Properties, Stop
- Scheduled: Properties, Delete

View option

If a probe is Completed or In Progress, clicking **View** opens the Real Time Information box:

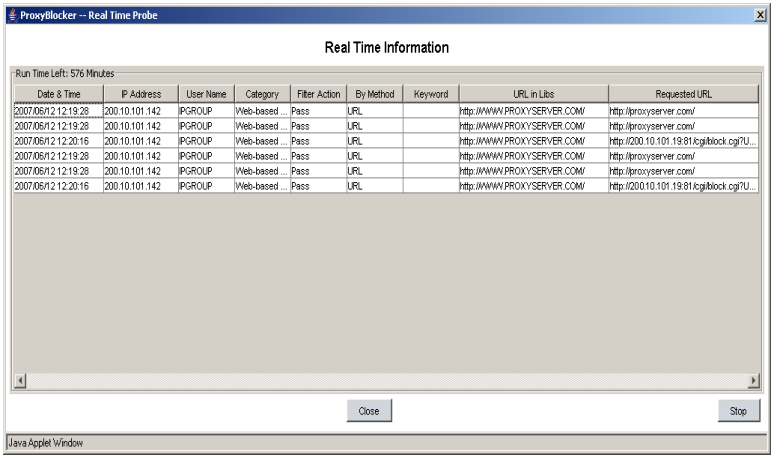


Fig. 2:4-12 Real Time Information box

This box displays the number of minutes left for the probe to run (Run Time Left), and user details for each item in the grid: Date & Time (in the YYYY/MM/DD HH:MM:SS format); IP Address; User Name; library Category; Filter Action set up in the profile (Pass, Block, reserved for ER, Warn, Warned, X Strike, Quota); By Method—the method used in creating the entry (SE Keyword, URL Keyword, URL, Wildcard, Strict HTTPS, Filter Action, Pattern, File Type, Moderate HTTPS); Keyword (displays the matching

keyword if the method is an SE Keyword or a URL Keyword); URL in Libraries, and Requested URL.

The following actions can be performed in this box:

- Click a URL to open a window that accesses the designated site.
- If the probe is currently in progress, clicking **Stop** halts the real time probe and changes this button to “Email”.
- After the probe is completed, the Email button is available instead of the Stop button. Clicking **Email** opens the Email option dialog box in which you specify an email address to send the completed report (see Email option).
- Click **Close** to close the Real Time Information box.

Properties option

Clicking **Properties** opens the Probe Properties box:

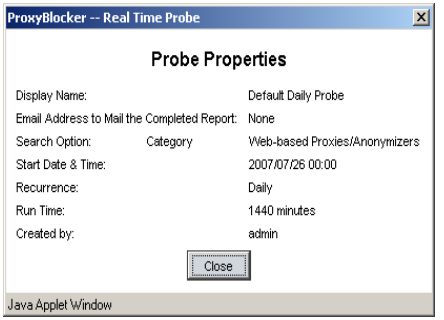


Fig. 2:4-13 Probe Properties box

This box includes the following information for the probe: Display Name; Email Address to Mail the Completed Report; Search Option criteria; Start Date & Time; Run Time; and User ID of the creator of the probe (Created by).

Click **Close** to close this box.

Stop, Delete options

Clicking **Stop** halts the probe and gives it a Completed status. This option is also available in the Real Time Information box via the “Stop” button.

Clicking **Delete** opens the following dialog box, asking if you want to delete the probe:

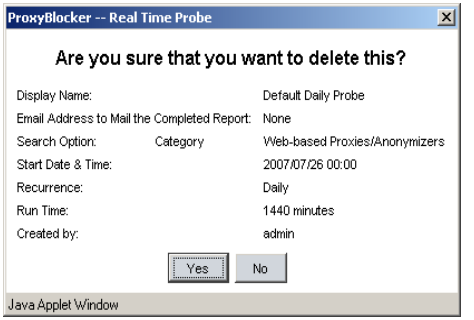


Fig. 2:4-14 Probe Properties deletion box

Click **Yes** to delete the probe and remove it from the View tab.

Email option

Clicking **Email** opens the Email Address box:

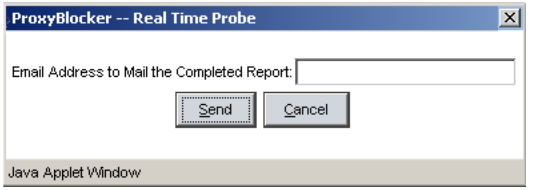


Fig. 2:4-15 Email Address box

Enter the **Email Address to Mail the Completed Report** and click **Send** to send the completed report to the designated email address.

GROUP ADMINISTRATOR SECTION

Introduction

The Group Administrator Section of this user guide is comprised of two chapters that include information on functions performed by the group administrator.

Chapter 1 includes information on setting up and maintaining master IP groups and group members. Chapter 2 includes information on maintaining exception URLs.

The group administrator performs the following tasks:

- defines members of a master IP group
- adds sub-group members and/or individual IP members and creates their filtering profiles
- grants designated users access to Internet content blocked at the global level—as appropriate—via an override account and/or exception URL setup
- uses the lookup tool to remove URLs or search engine keywords from customized libraries

Chapter 1: Group screen

Group administrators use group screen windows to add members to a master IP group, create sub-groups and/or individual IP members, and define and maintain members' filtering profiles. A member is associated with an IP address and may contain a netmask within a valid IP address range.

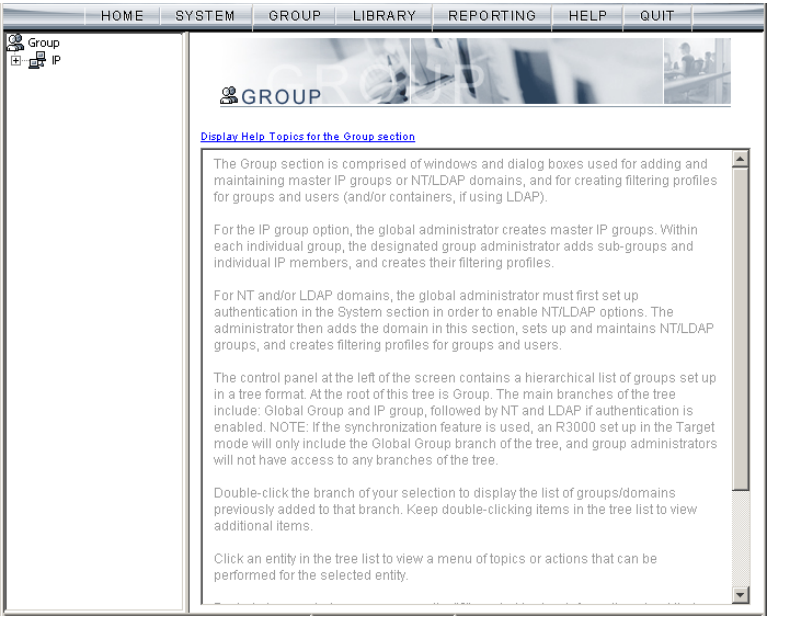


Fig. 3:1-1 Group screen

The navigation panel at the left of the screen contains the IP branch of the Group tree.

Double-click the IP branch of the tree to open it and to display the master IP group. Double-click the master IP group to open it and to display any IP sub-groups and/or individual IP members previously set up in the tree list.

Click an entity in the tree list to view a menu of topics or actions that can be performed for that entity.

IP

Refresh

Refresh the Master IP Group, Member

Click Refresh whenever a change has been made to the master IP group or member level of the tree.

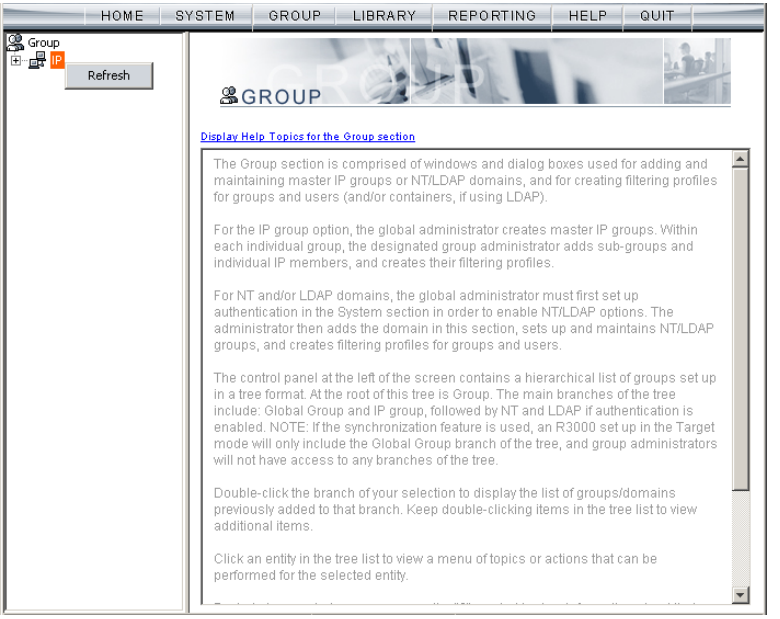


Fig. 3:1-2 Group screen, IP menu

Master IP Group

Master IP group includes options for defining and maintaining group accounts, setting up an override account and/or exception URLs to bypass global settings, and uploading or downloading IP profiles. Click the master IP group's link to view a menu of sub-topics: Group Details, Members, Override Account, Group Profile, Exception URL, Time Profile, Upload/Download IP Profile, Add Sub Group, Add Individual IP, Delete Group, and Paste Sub Group.

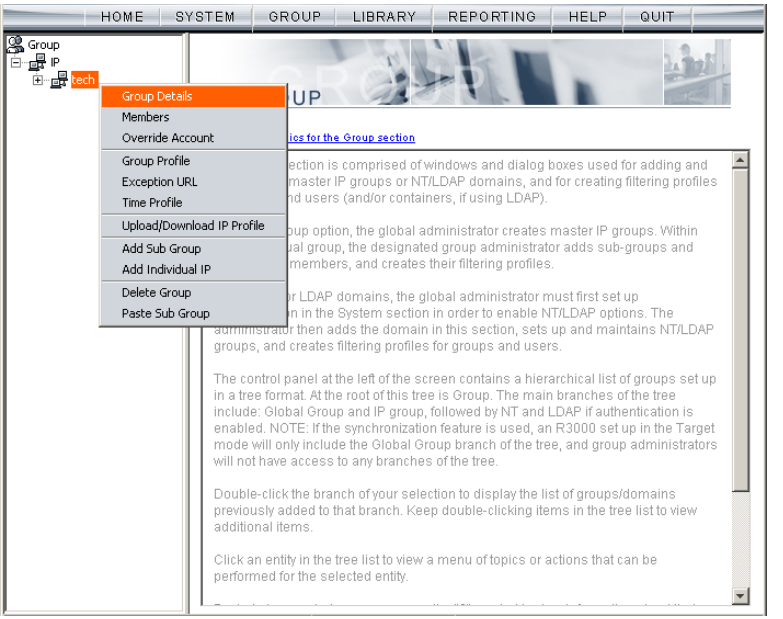


Fig. 3:1-3 Group screen, master IP group menu

Group Details window

The Group Details window displays when Group Details is selected from the menu. This window is used for viewing the Group Name and for changing the password of the group administrator.

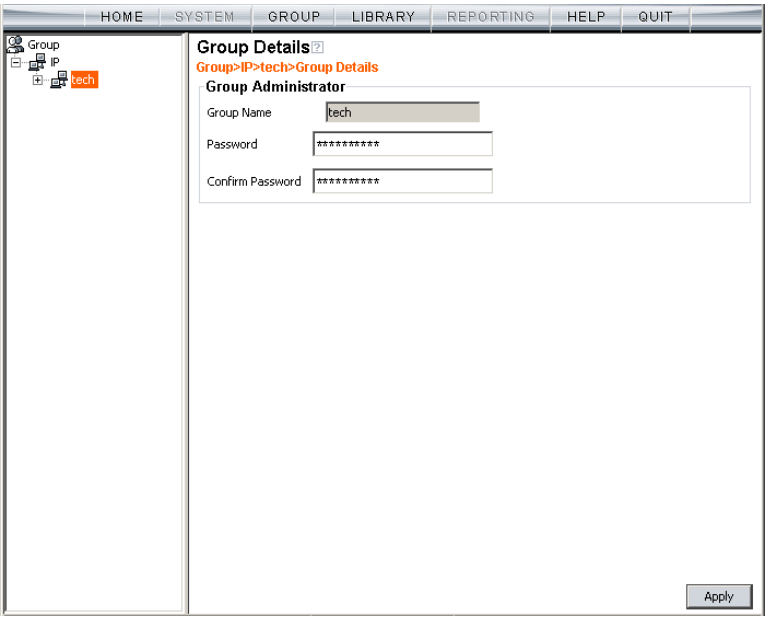


Fig. 3:1-4 Group window

Change the Group Administrator Password

In the Group Administrator frame, the **Group Name** displays.

To change the password for this group:

1. Enter the password in the **Password** and **Confirm Password fields**, using eight to 20 characters and at least one alpha character, one numeric character, and one special character. The password is case sensitive.
2. Click **Apply** to apply your settings.

Members window

The Members window displays when Members is selected from the menu. This window is used for adding and managing members of a master IP group. A member is comprised of an associated IP address, and a sub-group may also contain a netmask.

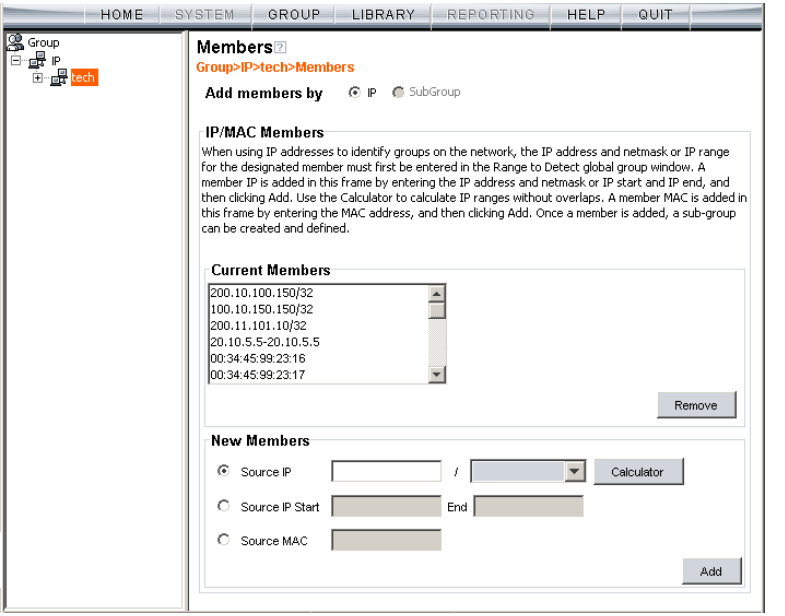


Fig. 3:1-5 Members window

Add the IP Address of the Member

1. Specify whether to add an IP address range with or without a netmask by selecting either “Source IP” or “Source IP Start / End”.
   - If “Source IP” was selected, enter the IP address, and specify the netmask in the **Source IP** fields.
   - If “Source IP Start / End” was selected, enter the **Start** and **End** of the IP address range.

2. Click **Add** to include the IP address entry in the Current Members list box.

***TIP**: Click **Calculator** to open the IP Calculator, and calculate IP ranges without any overlaps. Enter the **IP** address, specify the **Netmask**, and then click **Calculate** to display results in the Min Host and Max Host fields. Click **Close** to exit.*

Remove a Member from the Group

To remove an entry from the Current Members list box:

1. Select the member from the list box.
2. Click **Remove**.

Override Account window

The Override Account window displays when Override Account is selected from the menu. This window is used for creating an override account that allows an end user from a master IP group to bypass settings at the minimum filtering level. A user with an override account will be able to access categories and service ports blocked at the minimum filtering level, if the option to bypass the minimum filtering level is activated.

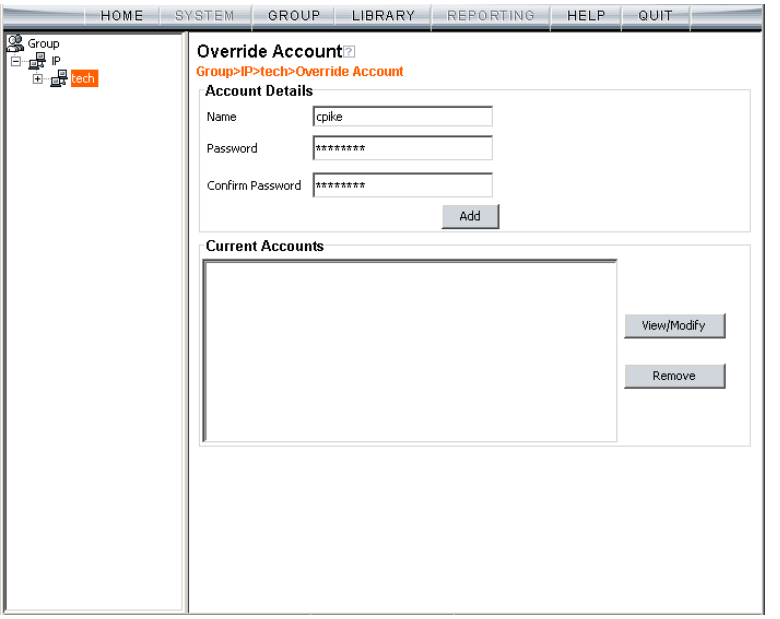


Fig. 3:1-6 Override Account window

***NOTES**: Override accounts can be created for any authorized user. In order for a user with an override account to access categories and ports set up to be blocked at the master IP group level, the global administrator must first activate the option to allow an override account to bypass minimum filtering level settings.*

A user can have only one override account. See the Override Account window in Chapter 2 of the Global Administrator Section for information on setting up a global group user's override account.

See Appendix D: Override Pop-up Blockers for information on how a user with an override account can authenticate if a pop-up blocker is installed on his/her workstation.

Add an Override Account

To create an Override Account profile:

1. In the Account Details frame, enter the username in the **Name** field.
2. Enter the **Password**.
3. Make the same entry again in the **Confirm Password** field.
4. Click **Add** to include the username in the list box of the Current Accounts frame, and to open the pop-up window containing the Current Accounts name as well as tabs to be used for specifying the components of the override account profile.
5. Click each of the tabs (Rule, Redirect, Filter Options) and specify criteria to complete the override account profile. (See Category Profile, Redirect URL, and Filter Options in this sub-section for information on the Rule, Redirect, and Filter Options tabs.)
6. Click **Apply** to activate the override account.
7. Click **Close** to close the pop-up window.

Category Profile

The Rule tab is used for creating the categories portion of the override account profile.

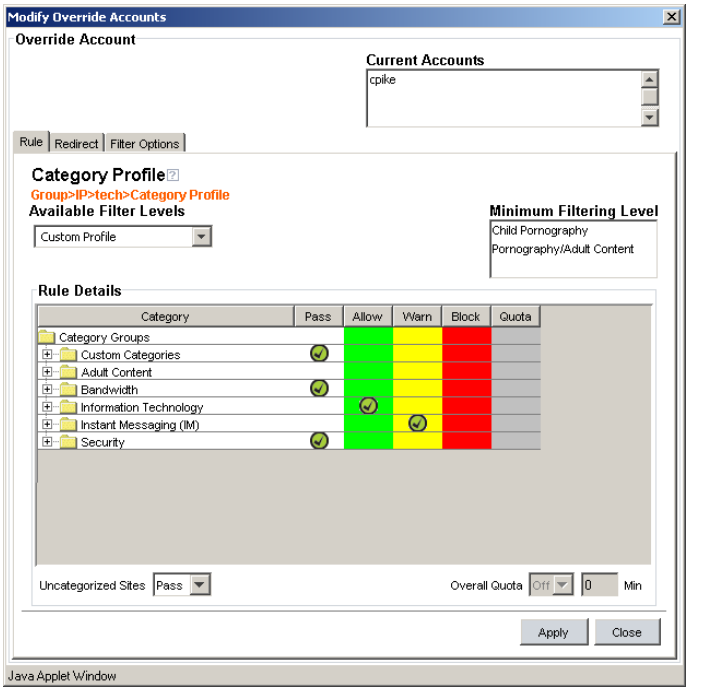


Fig. 3:1-7 Override Account pop-up window, Rule tab

To create the category profile:

1. Select a filtering rule from the available choices in the **Available Filter Levels** pull-down menu. This action automatically populates the Pass, Allow, Warn, and/or Block columns in the Rule Details frame with filter settings for each category group/library category in the Category Groups tree.

***TIP**: In the Category Groups tree, double-click the group envelope to open that segment of the tree and to view library categories belonging to that group.*

***NOTE**: If a category group does not display any filter setting (i.e. the check mark does not display in any column for the category group), one or more library categories within that group has a filter setting in a column other than the filter setting designated for all collective library categories within that group. For example, if in the Adult Content category group some of the library categories have a block setting and other library categories have a warn setting, there would be no category group filter setting, since all library categories do not have the same filter setting.*

2. To change the filter setting for a category group/library category, double-click the column (Pass, Allow, Warn, Block) in the row corresponding to that category group/library category to move the check mark to that column:
   - **Pass** - URLs in this category will pass to the end user.
   - **Allow** - URLs in this category will be added to the end user's white list.
   - **Warn** - URLs in this category will warn the end user that the URL he/she requested can be accessed, but may be against the organization's policies. The end user can view the URL after seeing a warning message and agreeing to its terms.
   - **Block** - URLs in this category will be blocked.

***TIPS**: Multiple categories can be assigned the same filter setting by clicking each category while pressing the Ctrl key on your keyboard, and then double-clicking in the appropriate column.*

Blocks of categories can be assigned the same filter setting by clicking the first category, and then pressing the Shift key on your keyboard while clicking the last category, and then double-clicking in the appropriate column.

3. Make a selection from the **Uncategorized Sites** pull-down menu to specify how to handle a URL that has not yet been categorized: "Pass", "Warn", or "Block".
4. To use the quota feature to restrict the end user's access to a passed library group/category, do the following:

- In the **Quota** column, enter the number of minutes the user will be able to access the library group/category. The minimum number of minutes is “1” and the maximum is “1439” (one day minus one minute). The number of minutes entered here combines with the seconds per hit (minimum one second to maximum 3600 seconds) defined in the Quota Settings window to determine when the end user will be blocked from further access to URLs in that library group/category.

***TIP**: If a quota entry is made for a category group, all library categories in that group will show the same number of quota minutes.*

***NOTE**: See the Quota Settings window in Chapter 1: System screen for more information on configuring quota settings and resetting quotas for end users currently blocked by quotas.*

- The **Overall Quota** field becomes enabled if a quota is entered for any library group/category. By default, the enabled Overall Quota is turned “Off”. If turned “On”, enter the number of minutes in the **Min** field to indicate when the end user’s access to passed library groups/categories with quotas will be blocked. If the end user spends this amount of time at URLs in any quota-marked library group/category, the Overall Quota overrides the number of minutes defined for each individual quota.

5. Click **Apply** to apply your settings to the override account profile.
6. Click another tab (Redirect or Filter Options) to continue creating the override account profile, or click **Close** to close the pop-up window and to return to the Override Account window.

Redirect URL

The Redirect tab is used for specifying the URL to be used for redirecting the user if he/she attempts to access a site or service set up to be blocked.

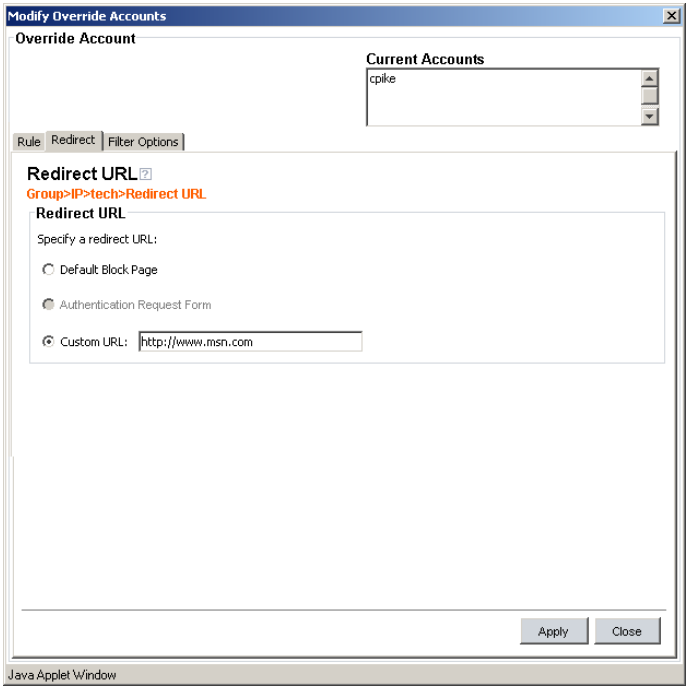


Fig. 3:1-8 Override Account pop-up window, Redirect tab

Specify the type of redirect URL to be used: “Default Block Page”, “Authentication Request Form”, or “Custom URL”.

If “Custom URL” is selected, enter the redirect URL in the corresponding text box. The user will be redirected to the designated page at this URL instead of the block page.

Filter Options

The Filter Options tab is used for specifying which filter option(s) will be applied to the override account profile.

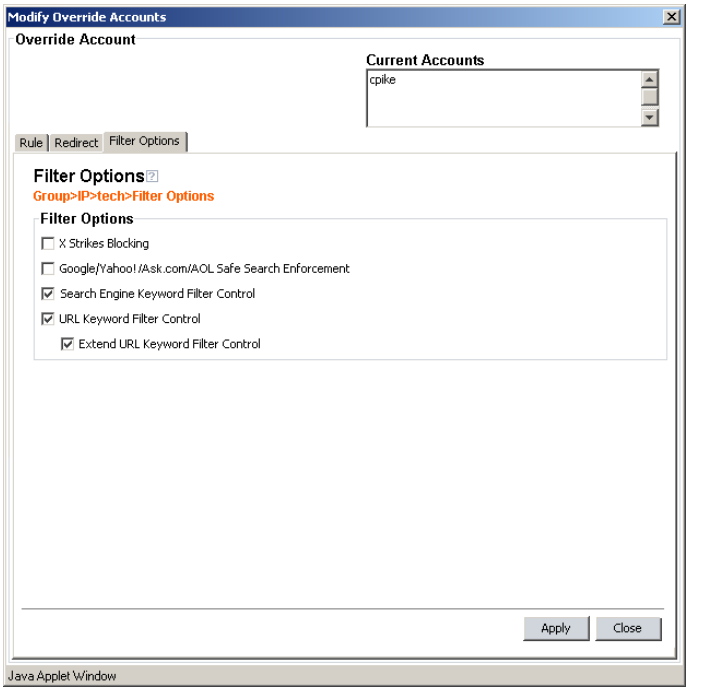


Fig. 3:1-9 Override Account pop-up window, Filter Options tab

Click the checkbox(es) corresponding to the option(s) to be applied to the override account filtering profile:

- "X Strikes Blocking" - With the X Strikes Blocking option enabled, if the user attempts to access inappropriate sites on the Internet, he/she will be locked out from his/her workstation after a specified number of tries within a fixed time period.

***NOTE**: See the X Strikes Blocking window in Chapter 1: System screen of the Global Group Section for information on setting up the X Strikes Blocking feature.*

- "Google/Yahoo!/Ask.com/AOL Safe Search Enforcement" - With the Google/Yahoo!/Ask.com/AOL Safe Search Enforcement option enabled, Google, Yahoo!, Ask.com, and AOL's "strict" SafeSearch Filtering option will be used whenever the end user performs a Google, Yahoo!, Ask.com, or AOL Web search or Image search.

***WARNING**: If this option is used in conjunction with the X Strikes Blocking feature and the user is performing an inappropriate Google, Yahoo!, Ask.com, or AOL Image search, the number of strikes that user will receive is based upon the amount of time it will take for unacceptable Google, Yahoo!, Ask.com, or AOL images returned by the query to load on the page. The user will receive only one strike if all inappropriate images load within the tolerance time range of a given strike.*

- "Search Engine Keyword Filter Control" - With the Search Engine Keyword Filter Control option enabled, search engine keywords can be set up to be blocked. When the user enters a keyword in the search engine, if that keyword has been set up to be blocked, the search will not be performed. Search engine keywords are entered in the Search Engine Keywords window of custom library categories.

***NOTE**: To set up search engine keywords in a Search Engine Keywords window, see Search Engine Keywords window in Chapter 2.*

- "URL Keyword Filter Control" - With the URL Keyword Filter Control option enabled, URL keywords can be set up to be blocked. When the user enters a keyword in the address line of a browser window, if that keyword has been set up to be blocked, the user will be denied access to that site or service. URL keywords are entered in the URL Keywords window of custom library categories.

  With the "Extend URL Keyword Filter Control" option enabled, a URL keyword search will be extended after the "?" character in a URL.

***NOTE**: To set up URL keywords in a URL Keywords window, see the URL Keywords window in Chapter 2.*

Edit an Override Account

Change the Password

To change an override account's password:

1. In the Current Accounts frame, select the username from the list box.
2. In the Account Details frame, enter the username in the **Name** field.
3. Enter the new **Password**.
4. Make the same entry again in the **Confirm Password** field.
5. Click **View/Modify** to open the pop-up window.
6. Click **Apply**.
7. Click **Close** to close the pop-up window.

Modify an Override Account

To modify an override account:

1. In the Current Accounts frame, select the username from the list box.
2. Click **View/Modify** to open the pop-up window.
3. Click the tab in which to make modifications (Rule, Redirect, Filter Options).
4. Make your edits in this tab and in any other tab, if necessary.
5. Click **Apply**.
6. Click **Close** to close the pop-up window.

Delete an Override Account

To delete an override account:

1. In the Current Accounts frame, select the username from the list box.
2. Click **Remove**.

Group Profile window

The Group Profile window displays when Group Profile is selected from the group menu. This window is used for viewing/creating the group's filtering profile. Click the following tabs in this window: Category, Redirect URL, and Filter Options. Entries in these tabs comprise the profile string for the group.

Category Profile

Category Profile displays by default when Group Profile is selected from the group menu, or when the Category tab is clicked. This tab is used for assigning filter settings to category groups/library categories for the group's filtering profile.

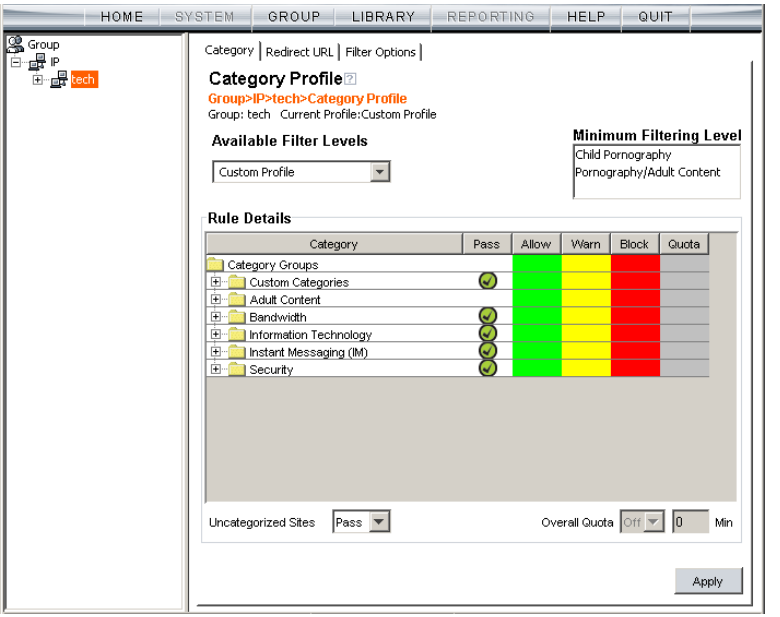


Fig. 3:1-10 Group Profile window, Profile tab

***NOTE**: In order to use this tab, filtering rules profiles must already have been set up by the global administrator.*

By default, “Rule0 Minimum Filtering Level” displays in the **Available Filter Levels** pull-down menu, and the Minimum Filtering Level box displays “Child Pornography” and “Pornography/Adult Content”. By default, **Uncategorized Sites** are allowed to Pass.

***NOTE**: By default, the Available Filter Levels pull-down menu also includes these five rule choices: Rule1 BYPASS”, “Rule2 BLOCK Porn”, “Rule3 Block IM and Porn”, “Rule4 8e6 CIPA Compliance”, and “Block All”.*

Create, Edit a List of Selected Categories

To create the category profile:

1. Select a filtering rule from the available choices in the **Available Filter Levels** pull-down menu. This action automatically populates the Pass, Allow, Warn, and/or Block columns in the Rule Details frame with filter settings for each category group/library category in the Category Groups tree.

***TIP**: In the Category Groups tree, double-click the group envelope to open that segment of the tree and to view library categories belonging to that group.*

***NOTE**: If a category group does not display any filter setting (i.e. the check mark does not display in any column for the category group), one or more library categories within that group has a setting in a column other than the filter setting designated for all collective library categories within that group. For example, if in the Adult Content category group some of the library categories have a block setting and other library categories have a warn setting, there would be no category group filter setting, since all library categories do not have the same filter setting.*

2. To change the filter setting for a category group/library category, double-click the column (Pass, Allow, Warn, Block) in the row corresponding to that category group/library category to move the check mark to that column:
   - **Pass** - URLs in this category will pass to the end user.

- **Allow** - URLs in this category will be added to the end user's white list.
- **Warn** - URLs in this category will warn the end user that the URL he/she requested can be accessed, but may be against the organization's policies. The end user can view the URL after seeing a warning message and agreeing to its terms.
- **Block** - URLs in this category will be blocked.

***TIPS**: Multiple categories can be assigned the same filter setting by clicking each category while pressing the Ctrl key on your keyboard, and then double-clicking in the appropriate column.*

Blocks of categories can be assigned the same filter setting by clicking the first category, and then pressing the Shift key on your keyboard while clicking the last category, and then double-clicking in the appropriate column.

3. Make a selection from the **Uncategorized Sites** pull-down menu to specify how to handle a URL that has not yet been categorized: "Pass", "Warn", or "Block".
4. To use the quota feature to restrict the end user's access to a passed library group/category, do the following:
   - In the **Quota** column, enter the number of minutes the user will be able to access the library group/category. The minimum number of minutes is "1" and the maximum is "1439" (one day minus one minute). The number of minutes entered here combines with the seconds per hit (minimum one second to maximum 3600 seconds) defined in the Quota Settings window to determine when the end user will be blocked from further access to URLs in that library group/category.

***TIP**: If a quota entry is made for a category group, all library categories in that group will show the same number of quota minutes.*

***NOTE**: See the Quota Settings window in Chapter 1: System screen for more information on configuring quota settings and resetting quotas for end users currently blocked by quotas.*

5. Click **Apply** to apply your settings to the override account profile.
6. Click another tab (Redirect or Filter Options) to continue creating the override account profile, or click **Close** to close the pop-up window and to return to the Override Account window.

Redirect URL

Redirect URL displays when the Redirect URL tab is clicked. This tab is used for specifying the URL to be used for redirecting users who attempt to access a site or service set up to be blocked at the group level.

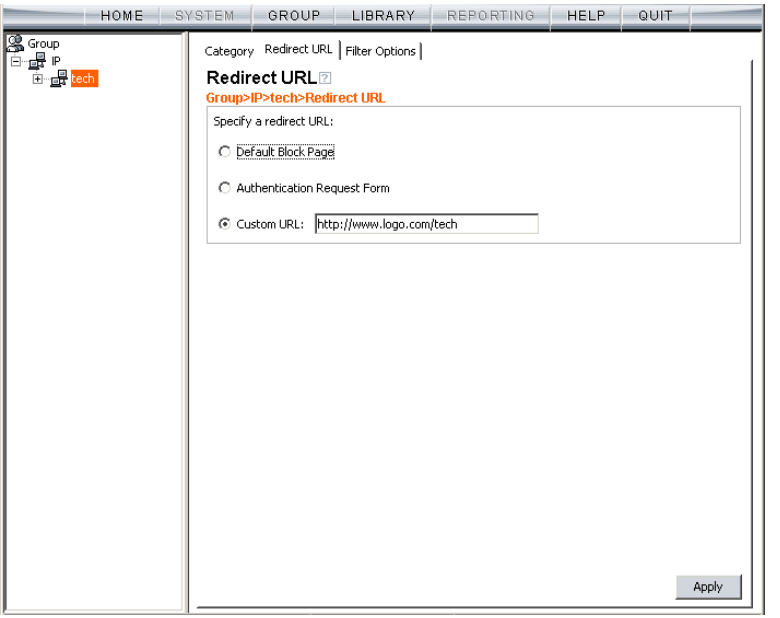


Fig. 3:1-11 Group Profile window, Redirect URL tab

Create, Edit the Redirect URL

1. Specify the type of redirect URL to be used: “Default Block Page”, “Authentication Request Form”, or “Custom URL”.

If “Custom URL” is selected, enter the redirect URL in the corresponding text box. Users will be redirected to the designated page at this URL instead of the block page.

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

Filter Options

Filter Options displays when the Filter Options tab is clicked. This tab is used for specifying which filter option(s) will be applied to the group’s filtering profile.

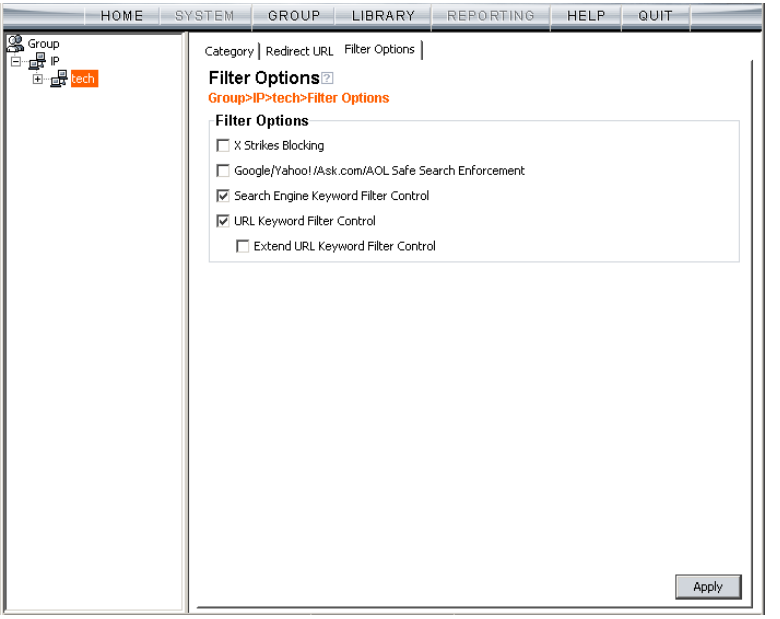


Fig. 3:1-12 Group Profile window, Filter Options tab

Create, Edit the Filter Options

1. Click the checkbox(es) corresponding to the option(s) to be applied to the sub-group filtering profile: “X Strikes Blocking”, “Google/Yahoo!/Ask.com/AOL Safe Search Enforcement”, “Search Engine Keyword Filter Control”, “URL Keyword Filter Control”.

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

X Strikes Blocking

With the X Strikes Blocking option enabled, an end user who attempts to access inappropriate sites on the Internet will be locked out from his/her workstation after a specified number of tries within a fixed time period.

***NOTE**: See the X Strikes Blocking window in Chapter 1: System screen of the Global Group Section for information on setting up the X Strikes Blocking feature.*

Google/Yahoo!/Ask.com/AOL Safe Search Enforcement

With the Google/Yahoo!/Ask.com/AOL Safe Search Enforcement option enabled, Google, Yahoo!, Ask.com, and AOL's "strict" SafeSearch Filtering option will be used whenever end users perform a Google, Yahoo!, Ask.com, or AOL Web search or Image search.

***WARNINGS**: This feature is not compatible with the proxy environment as it will cause overblocking.*

An inappropriate image will only be blocked if that image is included in 8e6's library or is blocked by Google, Yahoo!, Ask.com, or AOL.

If this option is used in conjunction with the X Strikes Blocking feature and a user is performing an inappropriate Google, Yahoo!, Ask.com, or AOL Image search, the number of strikes that user will receive is based upon the amount of time it will take for unacceptable Google, Yahoo!, Ask.com, or AOL images returned by the query to load on the page. The user will receive only one strike if all inappropriate images load within the tolerance time range of a given strike.

Search Engine Keyword Filter Control

With the Search Engine Keyword Filter Control option enabled, search engine keywords can be set up to be blocked. When a user enters a keyword in the search

engine, if that keyword has been set up to be blocked, the search will not be performed. Search engine keywords are entered in the Search Engine Keywords window of custom library categories.

***NOTES**: Search engine keyword filtering relies on an exact keyword match. For example, if the word "sex" is set up to be blocked, but "sexes" is not set up to be blocked, a search will be allowed on "sexes" but not "sex". However, if the word "gin" is set up to be blocked, a search on "cotton gin" will be blocked since the word "gin" is blocked.*

To set up search engine keywords in a Search Engine Keywords window for Custom Categories, see Chapter 2: Library screen, Search Engine Keywords window.

URL Keyword Filter Control

With the URL Keyword Filter Control option enabled, URL keywords can be set up to be blocked. When a user enters a keyword in the address line of a browser window, if that keyword has been set up to be blocked, the user will be denied access to that site or service. URL keywords are entered in the URL Keywords window of custom library categories.

With the "Extend URL Keyword Filter Control" option enabled, a URL keyword search will be extended after the "?" character in a URL.

***NOTE**: To set up URL keywords in a URL Keywords window for Custom Categories, see Chapter 2: Library screen, URL Keywords window.*

***WARNING**: If this feature is activated, use extreme caution when setting up URL keywords for filtering. If a keyword that is entered in a browser's address window contains the same consecutive characters as a keyword set up to be blocked, users will be denied access to URLs that are not even within blocked categories. For example, if all URL keywords containing "sex" are blocked, users will not be able to access a non-pornographic site such as http://www.essex.com.*

Exception URL window

The Exception URL window displays when Exception URL is selected from the group menu. This window is used for blocking group members' access to specified URLs and/or for letting group members access specified URLs blocked at the minimum filtering level.

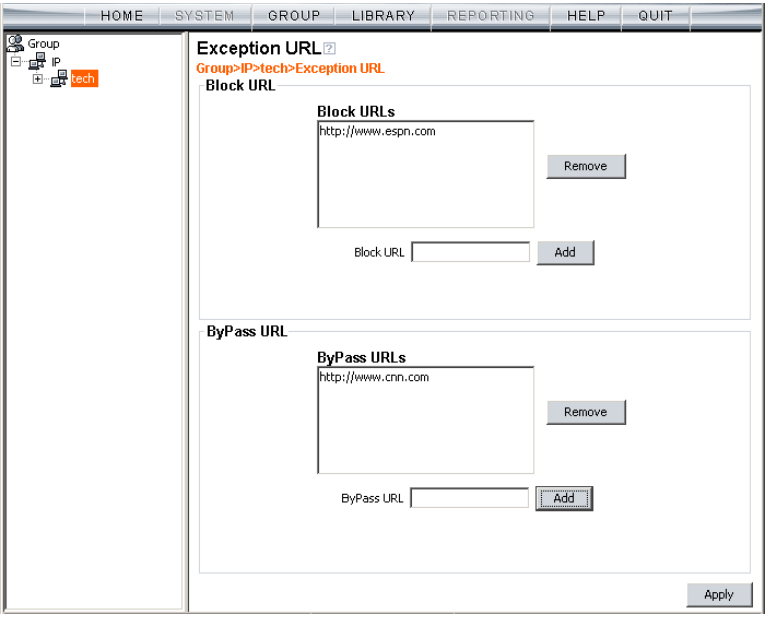


Fig. 3:1-13 Exception URL window

***NOTE**: Settings in this window work in conjunction with those made in the Override Account window and in the Minimum Filtering Level window maintained by the global administrator. Users with an override account will be able to access URLs set up to be blocked in this window, if the global administrator activates bypass settings in the Minimum Filtering Bypass Options tab. (See the Override Account window in this section for information on setting up an override account to allow a user to bypass group settings and minimum filtering level settings, if allowed.)*

Block URL frame

To block the group's access to a URL:

1. In the **Block URL** field, enter the URL.
2. Click **Add** to include the URL in the Block URLs list box.

To allow the URL to be accessed by the group again:

1. Select the URL from the Block URLs list box.
2. Click **Remove**.

ByPass URL frame

To allow a URL that is blocked at the minimum filtering level to be accessed by the group:

1. In the **ByPass URL** field, enter the URL.
2. Click **Add** to include the URL in the ByPass URLs list box.

To block the group's access to the URL again:

1. Select the URL from the ByPass URLs list box.
2. Click **Remove**.

Apply Settings

Click **Apply** to apply your settings after adding or removing a URL.

Time Profile window

The Time Profile window displays when Time Profile is selected from the group menu. This window is used for setting up or modifying a filtering profile to be activated at a specified time.

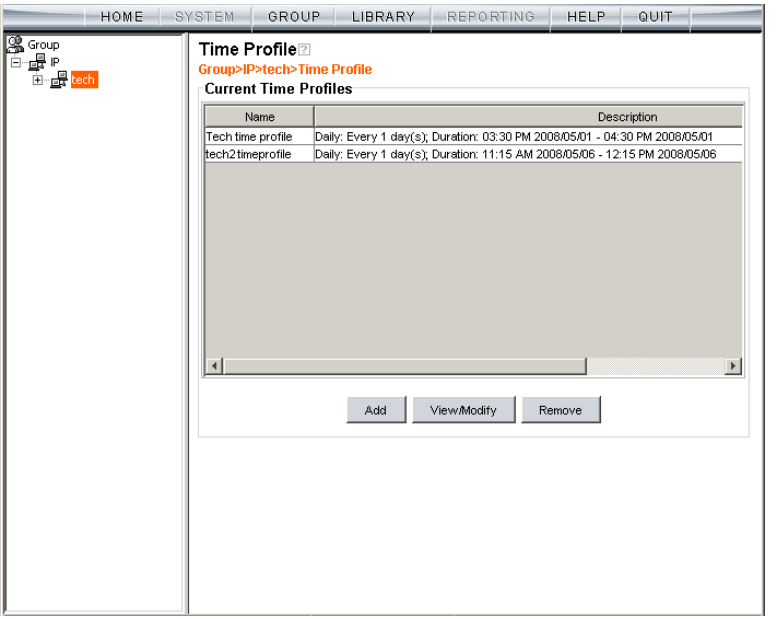


Fig. 3:1-14 Time Profile window

The Current Time Profiles list box displays the Name and Description of any time profiles previously set up for the entity that are currently active.

Add a Time Profile

To create a time profile:

1. Click **Add** to open the Adding Time Profile pop-up box:

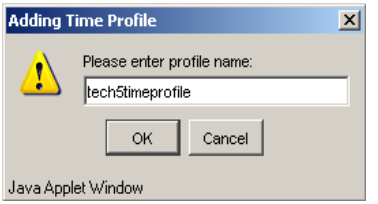


Fig. 3:1-15 Adding Time Profile

2. Type in three to 20 alphanumeric characters—the underscore (_) character can be used—for the profile name.
3. Click **OK** to close the pop-up box and to open the Adding Time Profile pop-up window that displays the name of this profile at the top of the Time Profile frame:

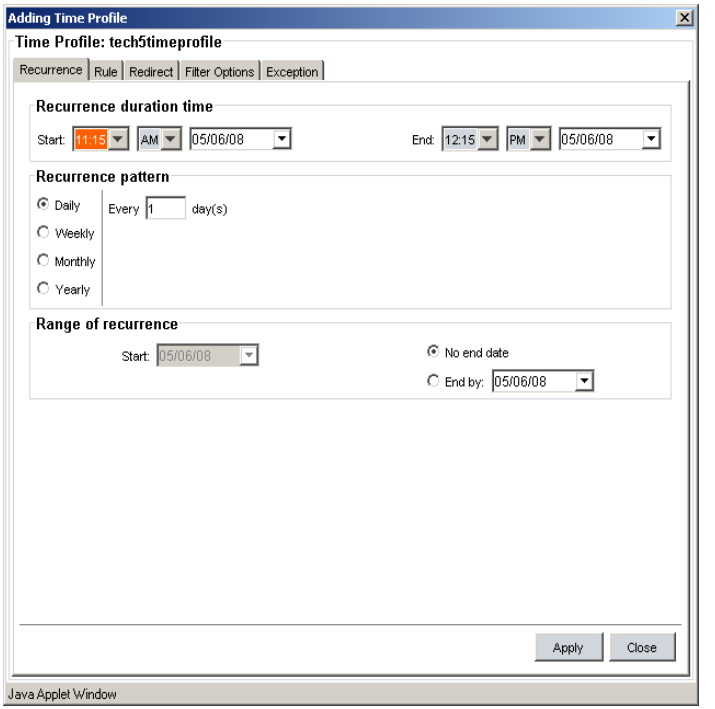


Fig. 3:1-16 Time Profile window Recurrence tab

4. In the Recurrence duration time frame, specify **Start** and **End** time range criteria:

   a. Select from a list of time slots incremented by 15 minutes: “12:00” to “11:45”. By default, the Start field displays the closest 15-minute future time, and the End field displays a time that is one hour ahead of that time. For example, if the time is currently 11:12, “*11:15*” displays in the Start field, and “*12:15*” displays in the End field.

   b. Indicate whether this time slot is “AM” or “PM”.

   c. Today’s date displays using the MM/DD/YY format. To choose another date, click the arrow in the date drop-down menu to open the calendar pop-up box:

   In this pop-up box you can do the following:

   - Click the left or right arrow at the top of this box to navigate to the prior month or the next month.
   - Double-click a date to select it and to close this box, populating the date field with that date.
   - Click **Today** to close this box, populating the date field with today’s date.

5. In the Recurrence pattern frame, choose the frequency this time profile will be used:

- **Daily** - If this selection is made, enter the interval for the number of days this time profile will be used. By default, "*1*" displays, indicating this profile will be used each day during the specified time period.

  If ***5*** is entered, this profile will be used every five days at the specified time.

- **Weekly** - If this selection is made, enter the interval for the weeks this time profile will be used, and specify the day(s) of the week ("Sunday" - "Saturday"). By default, "*1*" displays and today's day of the week is selected. If today is Tuesday, these settings indicate this profile will be used each Tuesday during the specified time period.

  If ***2*** is entered and "Wednesday" and "Friday" are selected, this profile will be used every two weeks on Wednesday and Friday.

- **Monthly** - If this selection is made, first enter the interval for the months this time profile will be used, and next specify which day of the month:

  - If **Day** is chosen, select from "1" - "31".
  - If a non-specific day is chosen, make selections from the two pull-down menus for the following:

    - week of the month: "First" - "Fourth", or "Last"

    - day of the month: "Sunday" - "Saturday", "Day", "Weekday", "Weekend".

  "By default, "*1*" displays and today's Day of the month is selected. If today is the 6th, these settings indicate this profile will be used on the 6th each month during the specified time period.

  If ***3*** is entered and the "Third" "Weekday" are selected, this profile will be used every three months on the third week day of the month. If the month begins on a Thursday (for example, May 1st), the third week day would be the following Monday (May 5th in this example).

- **Yearly** - If this selection is made, the year(s), month, and day for this time profile's interval must be specified:

  First enter the year(s) for the interval. By default "*1*" displays, indicating this time profile will be used each year.

  Next, choose from one of two options to specify the day of the month for the interval:

  - The first option lets you choose a specific month ("January" - "December") and day ("1" - "31"). By default the current month and day are selected.
  - The second option lets you make selections from the three pull-down menus for the following:

    - week of the month: "First" - "Fourth", or "Last"

    - day of the month: "Sunday" - "Saturday", "Day", "Weekday", "Weekend"

    - month: "January" - "December".

    By default, the "First" "Sunday" of "January" are selected.

  If ***2*** is entered and the "First" "Monday" of "June" are selected, this profile will be used every two years on the first Monday in June. For example, if the current month and year are May 2008, the first Monday in June this year would be the 2nd. The next time this profile would be used will be in June 2010.

6. In the Range of recurrence frame, the **Start** date displays greyed-out; this is the same date as the Start date shown in the Recurrence duration time frame. Specify whether or not the time profile will be effective up to a given date:

   - **No end date** - If this selection is made, the time profile will be effective indefinitely.

- **End by** - If this selection is made, by default today's date displays using the MM/DD/YY format. To choose another date, click the arrow in the date drop-down menu to open the calendar pop-up box. (See the information on the previous pages on how to use the calendar box.)

7. Click each of the tabs (Rule, Redirect, Filter Options, Exception) and specify criteria to complete the time profile. (See Category Profile, Redirect URL, Filter Options, and Exception URL in this sub-section for information on the Rule, Redirect, Filter Options, and Exception tabs.)
8. Click **Apply** to activate the time profile for the IP group at the specified time.
9. Click **Close** to close the Adding Time Profile pop-up window and to return to the Time Profile window. In this window, the Current Time Profiles list box now shows the Name and Description of the time profile that was just added.

***WARNING**: If there is an error in a time profile, the Description for that time profile displays in red text. Select that time profile and click **View/Modify** to make any necessary corrections.*

Category Profile

The Rule tab is used for creating the categories portion of the time profile.

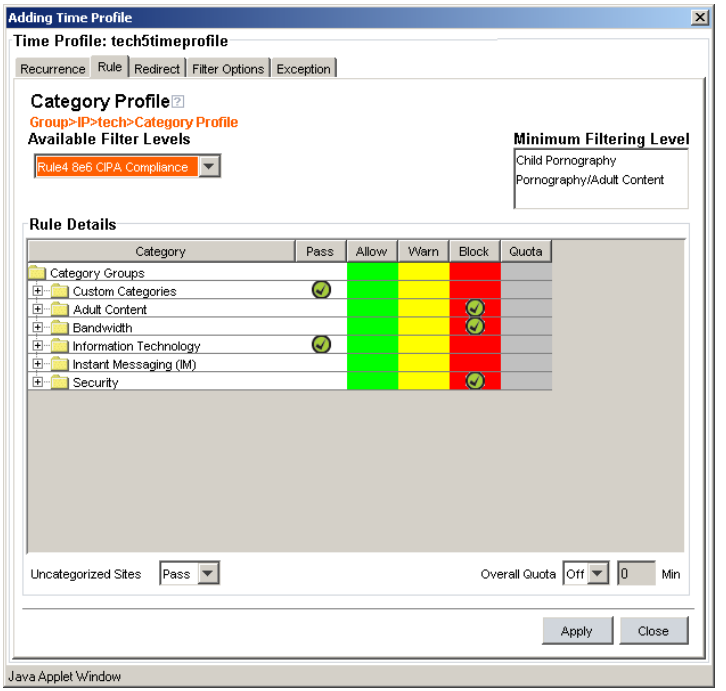


Fig. 3:1-17 Time Profile pop-up window, Rule tab

***NOTE**: See the Override Account window, Category Profile sub-section in this chapter for information about entries that can be made for this component of the filtering profile.*

Redirect URL

The Redirect tab is used for specifying the URL to be used for redirecting users who attempt to access a site or service set up to be blocked.

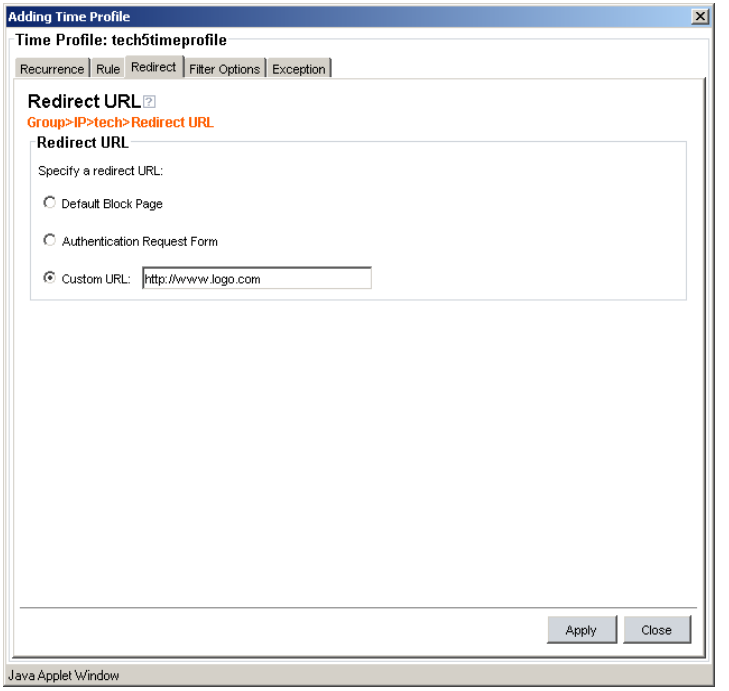


Fig. 3:1-18 Time Profile pop-up window, Redirect URL tab

***NOTE**: See the Override Account window, Redirect URL sub-section in this chapter for information about entries that can be made for this component of the filtering profile.*

Filter Options

The Filter Options tab is used for specifying which filter option(s) will be applied to the time profile.

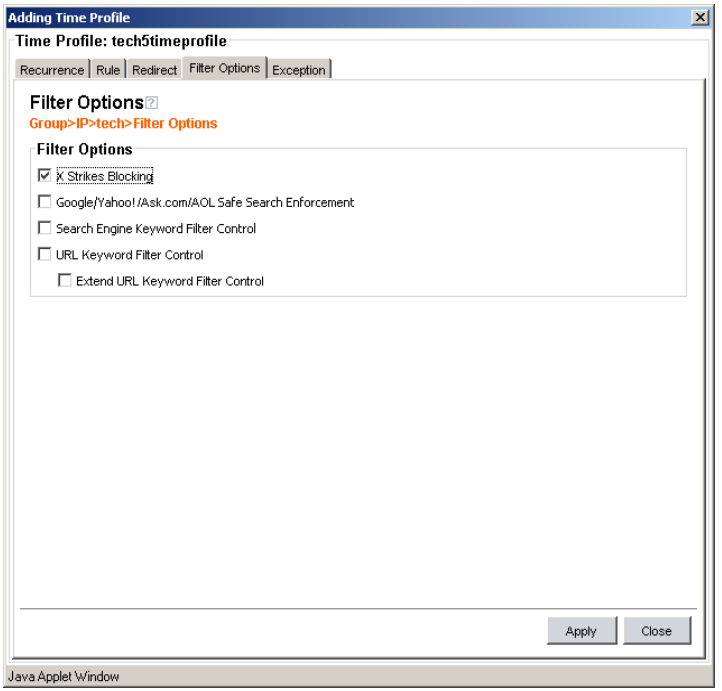


Fig. 3:1-19 Time Profile pop-up window, Filter Options tab

***NOTE**: See the Override Account window, Filter Options sub-section in this chapter for information about entries that can be made for this component of the filtering profile.*

Exception URL

The Exception tab is used for allowing users to be blocked from accessing specified URLs and/or to be allowed to access specified URLs blocked at the minimum filtering level.

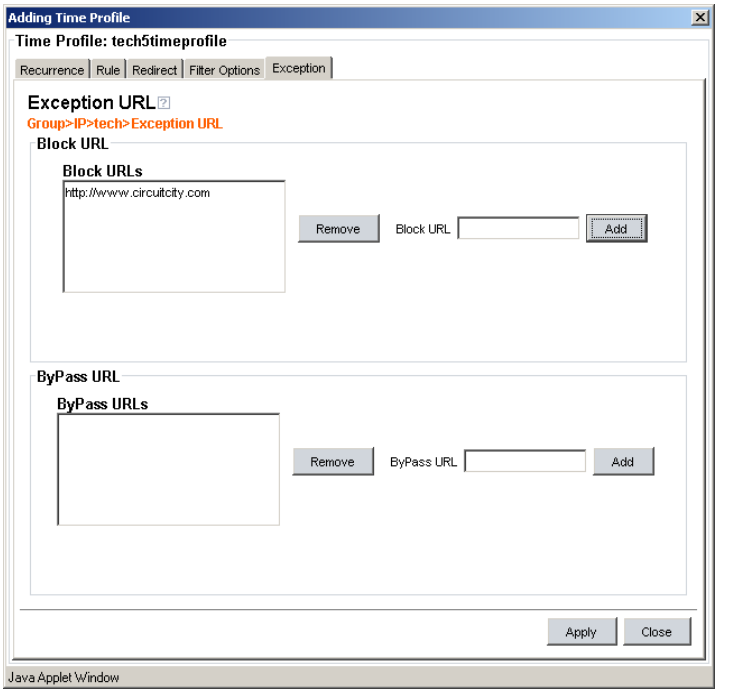


Fig. 3:1-20 Time Profile pop-up window, Exception tab

***NOTE**: Settings in this window work in conjunction with those made in the Override Account window and in the Minimum Filtering Level window maintained by the global administrator. Users with an override account will be able to access URLs set up to be blocked in this window, if the global administrator activates bypass settings in the Minimum Filtering Bypass Options tab. (See the Override Account window in this section for information on setting up an override account to allow a user to bypass group settings and minimum filtering level settings, if allowed.)*

To block the group's access to a URL:

1. In the **Block URL** field, enter the URL.
2. Click **Add** to include the URL in the Block URLs list box.

To allow the URL to be accessed by the group again:

1. Select the URL from the Block URLs list box.
2. Click **Remove**.

To allow a URL that is blocked at the minimum filtering level to be accessed by the group:

1. In the **ByPass URL** field, enter the URL.
2. Click **Add** to include the URL in the ByPass URLs list box.

To block the group's access to the URL again:

1. Select the URL from the ByPass URLs list box.
2. Click **Remove**.

Modify a Time Profile

To modify an existing time profile:

1. Select the time profile from the Current Time Profiles list box.
2. Click **View/Modify** to open the Modify Time Profiles pop-up window.
3. Make modifications in the default Recurrence tab and/or click the tab in which to make modifications (Rule, Redirect, Filter Options, Exception).
4. Make edits in this tab and in any other tab, if necessary.
5. Click **Apply**.
6. Click **Close** to close the Modify Time Profiles pop-up window, and to return to the Time Profile window.

Delete a Time Profile

To delete a time profile:

1. Select the time profile from the Current Time Profiles list box.
2. Click **Remove**.

Upload/Download IP Profile window

The Upload/Download IP Profile window displays when Upload/Download IP Profile is selected from the group menu. This window is used for uploading or downloading a text file containing filtering profiles of multiple users or sub-groups.

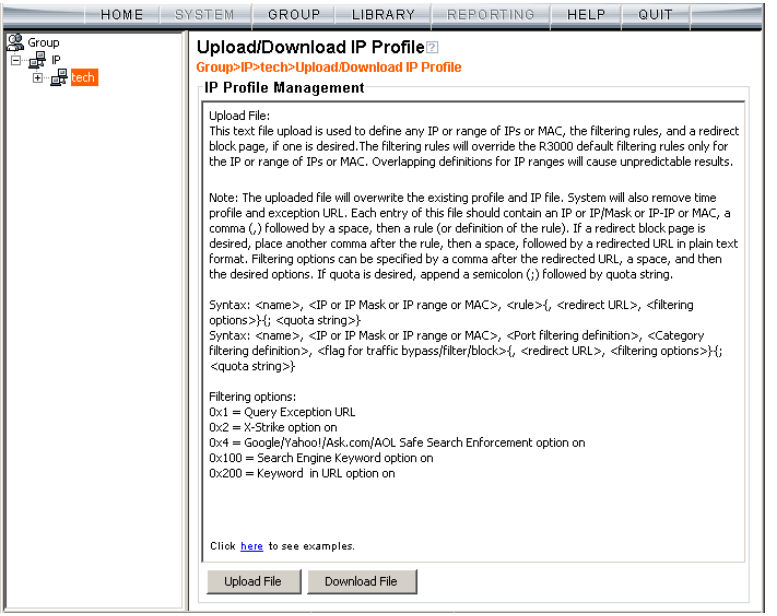


Fig. 3:1-21 Upload/Download IP Profile window

Upload IP Profiles

1. Click **Upload File** to open both the refresh message dialog box and the Upload IP Profiles pop-up window:

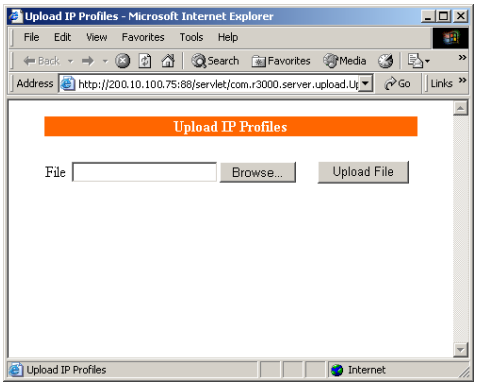


Fig. 3:1-22 Upload IP Profiles pop-up window

***NOTE**: Leave the message dialog box open until the file containing the profile has been uploaded.*

2. Click **Browse** to open the Choose file window in which you find and select the file containing the IP profiles to be uploaded. This text file of user/group profiles must be entered in a specific format.

***NOTE**: For examples of entries to include in a profile file, go to **http://www.8e6.com/pbahelp/files/2group_ipprofiles.html**.*

Once the file is selected, the path displays in **File** field.

***WARNING**: Any existing profiles will be overwritten by the contents of the uploaded file.*

3. Click **Upload File** in this pop-up window to display the message “Upload IP Profiles Successfully.”
4. Click the “X” in the upper right corner of the Upload IP Profiles pop-up window to close it.
5. Click **OK** in the message dialog box to refresh the IP groups branch of the tree.

Download Profile

If profiles have been created and/or uploaded to the server:

1. Click **Download Profile** to open a browser window containing the profiles:

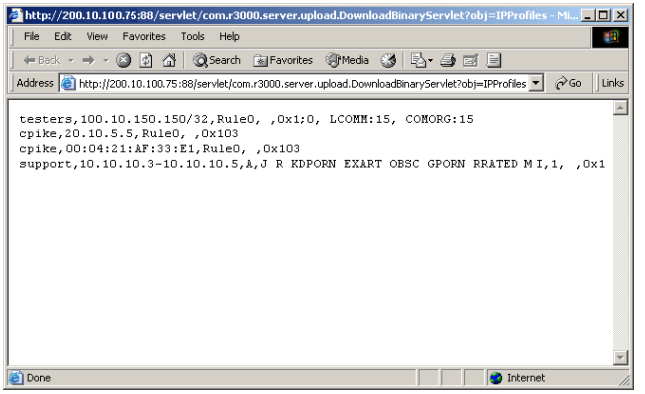


Fig. 3:1-23 Download IP Profiles window

   The contents of this window can viewed, printed, and/or saved.

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

Add Sub Group

Add an IP Sub Group

From the group menu:

1. Click Add Sub Group to open the Create Sub Group dialog box:

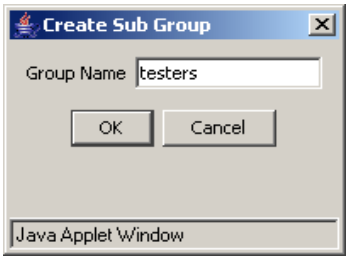


Fig. 3:1-24 Create Sub Group box

2. Enter the **Group Name** for the sub-group.

***NOTES**: The name of the sub-group must be less than 20 characters; cannot be "IP", "NT", or LDAP", and cannot contain spaces. The first character cannot be a digit.*

The following characters cannot be used in the name: "." (period), "," (comma), ":" (colon), ";" (semi-colon), "!" (exclamation point), "?" (question mark), "&" (ampersand), "*" (asterisk), """ (quotation mark), "'" (apostrophe), "`" (grave accent mark), "~" (tilde), "^" (caret), "_" (underscore), "|" (pipe), "/" (slash), "\", (backslash)", "\\" (double backslashes), "(" (left parenthesis), ")" (right parenthesis), "{" (left brace), "}" (right brace), "[" (left bracket), "]" (right bracket), "@" (at sign), "#" (pound sign), "$" (dollar sign), "%" (percent sign), "<" (less than symbol), ">" (greater than symbol), "+" (plus symbol), "-" (minus sign), "=" (equals sign).

3. Click **OK** to close the dialog box and to add the sub-group to the master IP group tree.

***WARNING**: When adding a sub-group to the tree list, sub-group users will be blocked from Internet access until the minimum filtering level profile is defined via the Minimum Filtering Level window. The minimum filtering level is established by the global administrator.*

Add Individual IP

Add an Individual IP Member

From the group menu:

1. Click Add Individual IP to open the Create Individual IP dialog box:

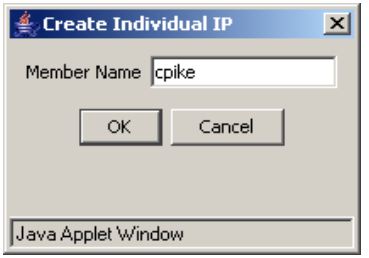


Fig. 3:1-25 Create Individual IP box

2. Enter the **Member Name** for the Individual IP address.

***NOTES**: The name of the individual IP address must be less than 20 characters; cannot be "IP", "NT", or LDAP", and cannot contain spaces. The first character cannot be a digit.*

The following characters cannot be used in the name: "." (period), "," (comma), ":" (colon), ";" (semi-colon), "!" (exclamation point), "?" (question mark), "&" (ampersand), "*" (asterisk), """ (quotation mark), "'" (apostrophe), "`" (grave accent mark), "~" (tilde), "^" (caret), "_" (underscore), "|" (pipe), "/" (slash), "\", (backslash)", "\\" (double backslashes), "(" (left parenthesis), ")" (right parenthesis), "{" (left brace), "}" (right brace), "[" (left bracket), "]" (right bracket), "@" (at sign), "#" (pound sign), "$" (dollar sign), "%" (percent sign), "<" (less than symbol), ">" (greater than symbol), "+" (plus symbol), "-" (minus sign), "=" (equals sign).

3. Click **OK** to close the dialog box and to add the individual IP member to the master IP group tree.

***WARNING**: When adding an Individual IP member to the tree list, the user will be blocked from Internet access until the minimum filtering level profile is defined via the Minimum Filtering Level window. The minimum filtering level is established by the global administrator.*

Delete Group

Delete a Master IP Group Profile

To delete a group profile, choose Delete Group from the group menu. This action removes the master IP group from the tree.

Paste Sub Group

The Paste Sub Group function is used for expediting the process of creating sub-groups, if the sub-group to be added has the same configuration settings as one that already exists.

A sub-group can be “pasted”—or copied—to a group if the Copy Sub Group function was first performed at the sub-group level.

Paste a Copied IP Sub Group

From the group menu:

1. Select Paste Sub Group to open the Paste Sub Group dialog box:

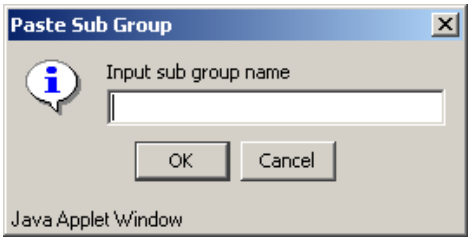


Fig. 3:1-26 Paste Sub Group dialog box

2. In the **Input sub group name** field, enter the name of the sub-group.
3. Click **OK** to add the sub-group to the group tree.

Sub Group

Sub Group includes options for creating and maintaining the filtering profile for the sub-group. Click the sub-group's link to view a menu of sub-topics: Sub Group Details, Members, Sub Group Profile, Exception URL, Time Profile, Delete Sub Group, and Copy Sub Group.

Fig. 3:1-27 Group screen, Sub Group menu

Sub Group (IP Group) window

The Sub Group (IP Group) window displays when Sub Group Details is selected from the menu. This window is used for viewing and adding or editing details on an IP group member.

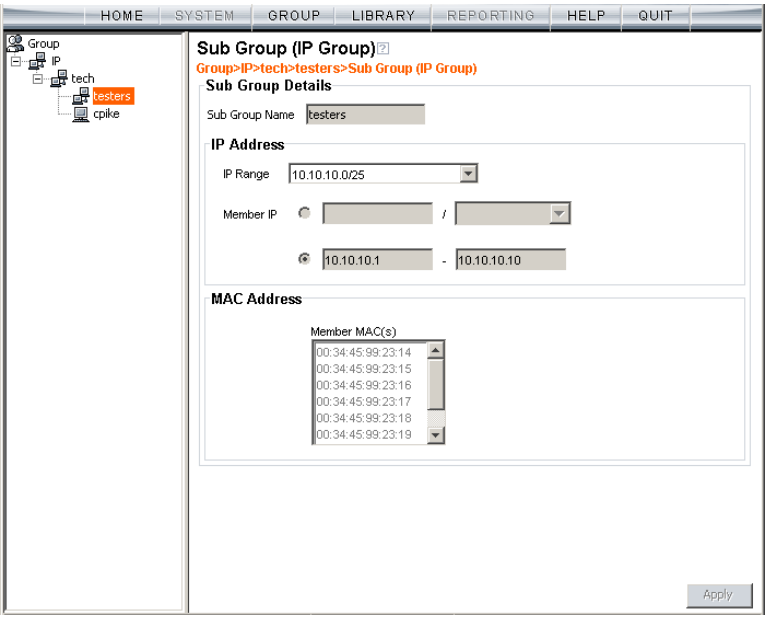


Fig. 3:1-28 Sub Group (IP Group) window, view only

View IP Sub-Group Details

If the sub-group was previously defined, the fields in the Sub Group Details frame cannot be edited. The following information displays:

- Sub Group Name
- IP Range
- Member IP address and netmask or IP address range.

Add IP Sub-Group Details

If the sub-group was not previously defined, the fields in the IP Address frame and the Apply button remain activated.

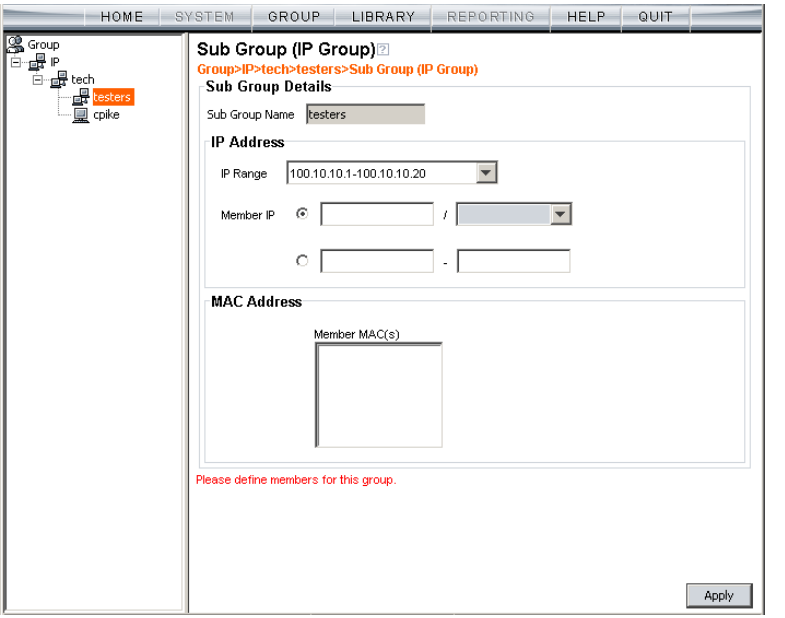


Fig. 3:1-29 Sub Group (IP Group) window, fields activated

1. In the IP Address frame, click the appropriate radio button corresponding to the type of **Member IP** address range to be entered: IP address with netmask, or IP address range.

***TIP**: Use the IP Range pull-down menu to view the IP address(es) that can be entered in these fields.*

2. Corresponding to the selected radio button:
   - enter the IP address and specify the netmask, or
   - enter the IP address range in the text boxes.

3. Click **Apply** to save your entries. Once applied, the Member fields become greyed-out and the Apply button becomes deactivated (see Fig. 3:1-28).

Members window

The Members window displays when Members is selected from the menu. This window is used for modifying the sub-group's Member IP address.

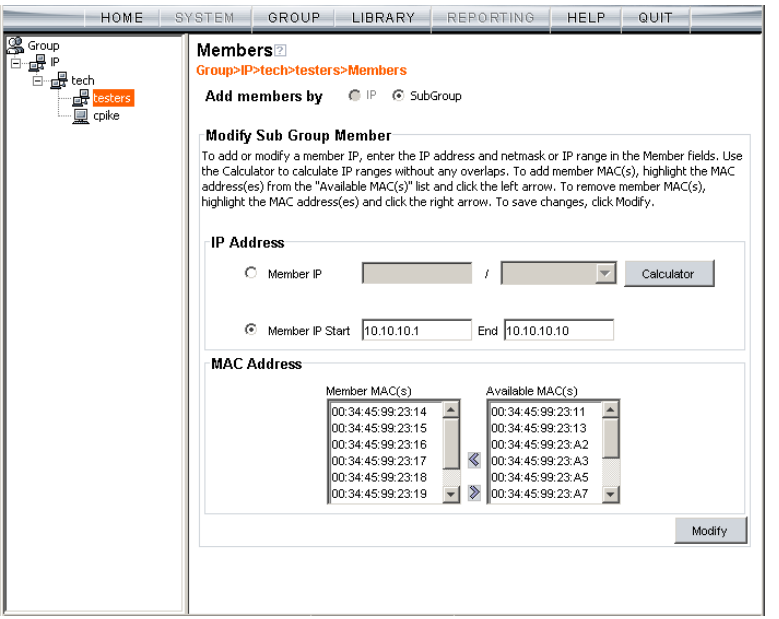


Fig. 3:1-30 Members window

Modify Sub-Group Members

The Modify Sub Group Member frame is comprised of the IP Address and MAC Address frames.

1. In the IP Address frame, specify whether to add or edit an IP address range with or without a netmask by selecting either “Member IP” or “Member IP Start / End”.
   - If “Member IP” was selected, enter the IP address and specify the netmask in the **Member IP** fields.
   - If “Member IP Start / End” was selected, enter the **Member IP Start** and **End** of the IP address range.

***TIP**: Click **Calculator** to open the IP Calculator, and calculate IP ranges without any overlaps.*

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

Sub Group Profile window

The Sub Group Profile window displays when Sub Group Profile is selected from the sub-group menu. This window is used for viewing/creating the sub-group’s filtering profile. Click the following tabs in this window: Category, Redirect URL, and Filter Options. Entries in these tabs comprise the profile string for the sub-group.

***NOTE**: See the Group Profile window in this chapter for information about entries that can be made for the following components of the filtering profile: Category Profile, Redirect URL, Filter Options.*

Exception URL window

The Exception URL window displays when Exception URL is selected from the sub-group menu. This window is used for blocking sub-group members' access to specified URLs and/or for letting sub-group members access specified URLs blocked at the minimum filtering level.

***NOTE**: See the Exception URL window in the group tree section of this chapter for information on entries that can be made in this window.*

Time Profile window

The Time Profile window displays when Time Profile is selected from the sub-group menu. This window is used for setting up or modifying a filtering profile to be activated at a specified time.

***NOTE**: See the Time Profile window in the group tree section of this chapter for information on entries that can be made for the following components of the filtering profile: Category Profile, Redirect URL, Filter Options, Exception URL.*

Delete Sub Group

Delete an IP Sub-Group

To delete a sub-group, choose Delete Sub Group from the sub-group menu. This action removes the sub-group from the tree.

Copy Sub Group

The Copy Sub Group function is used for expediting the process of creating sub-groups, if the sub-group to be added has the same configuration settings as one that already exists.

Copy an IP Sub-Group

To copy configurations made for a specified sub-group:

1. Choose Copy Sub Group from the sub-group menu.
2. Select the group from the tree and choose Paste Sub Group from the group menu to paste the sub-group to the group. (See Paste Sub Group dialog box in the Group section of this chapter.)

Individual IP

Individual IP includes options for creating and maintaining the filtering profile for the Individual IP member. Click the individual IP member's link to view a menu of sub-topics: Members, Individual IP Profile, Exception URL, Time Profile, Delete Individual IP.

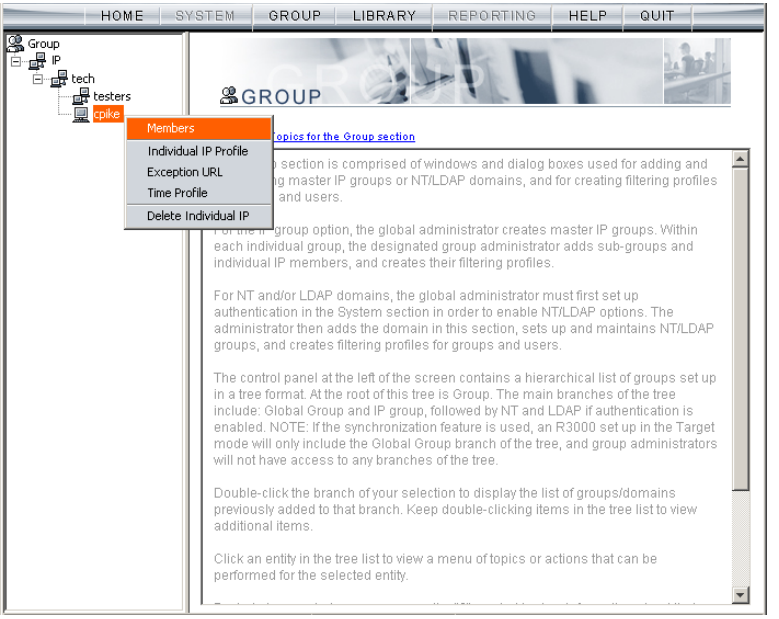


Fig. 3:1-31 Group screen, Individual IP menu

Member window

The member window displays when Members is selected from the menu. This window is used for modifying the individual IP member's IP address.

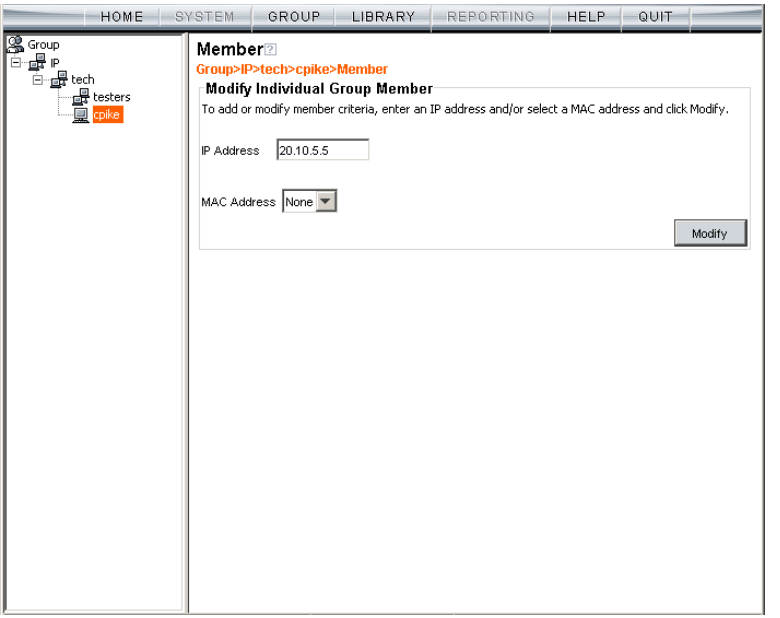


Fig. 3:1-32 Member window

Enter the IP Address of the Member

In the Modify Individual Group Member frame:

1. Enter the IP address in the **Member** field.
2. Click **Modify** to apply your changes.

Individual IP Profile window

The Individual IP Profile window displays when Individual IP Profile is selected from the individual IP member menu. This window is used for viewing/creating the member's filtering profile. Click the following tabs in this window: Category, Redirect URL, and Filter Options. Entries in these tabs comprise the profile string for the member.

***NOTE**: See the Group Profile window in this chapter for information about entries that can be made for the following components of the filtering profile: Category Profile, Redirect URL, Filter Options.*

Exception URL window

The Exception URL window displays when Exception URL is selected from the individual IP member menu. This window is used for blocking the member's access to specified URLs and/or for letting the member access specified URLs blocked at the minimum filtering level.

***NOTE**: See the Exception URL window in the group tree section of this chapter for information on entries that can be made in this window.*

Time Profile window

The Time Profile window displays when Time Profile is selected from the individual IP member menu. This window is used for setting up or modifying a filtering profile to be activated at a specified time.

***NOTE**: See the Time Profile window in the group tree section of this chapter for information on entries that can be made for the following components of the filtering profile: Category Profile, Redirect URL, Filter Options, Exception URL.*

Delete Individual IP

Delete an Individual IP Member

To delete an individual IP member, choose Delete Individual IP from the individual IP member menu. This action removes the member from the tree.

Chapter 2: Library screen

Group administrators use windows and dialog boxes in the Library screen to look up URLs in library categories. Library categories are used when creating or modifying filtering profiles.

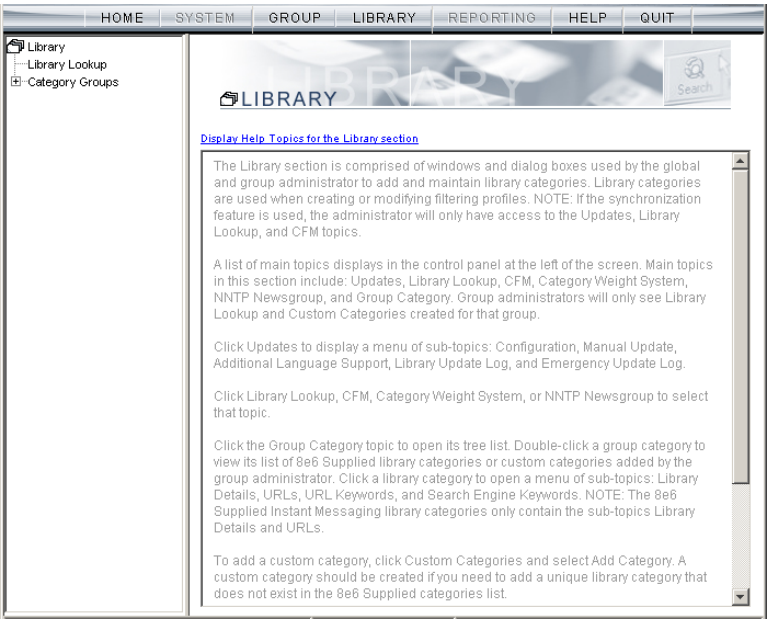


Fig. 3:2-1 Library screen

A list of main topics displays in the navigation panel at the left of the screen. Main topics in this section include the following: Library Lookup and Category Groups, the latter topic containing the Custom Categories sub-topic which is only activated for the global administrator.

Library Lookup

Library Lookup window

The Library Lookup window displays when Library Lookup is selected from the navigation panel. This window is used for verifying whether or not a URL or search engine keyword or keyword phrase exists in a library category.

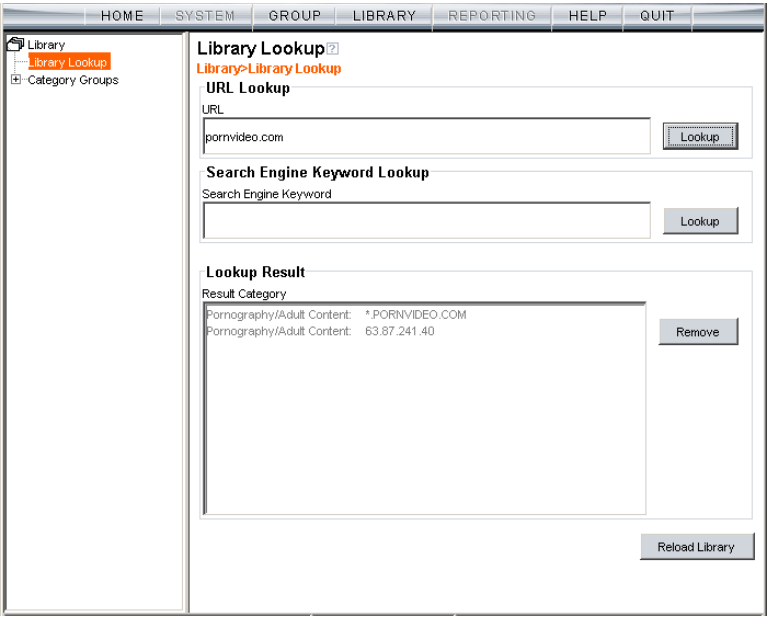


Fig. 3:2-2 Library Lookup window

***NOTE**: This window is also used by global administrators, except their permissions let them remove URLs and search engine keywords/phrases. The reload library function is used after making changes to the library.*

Look up a URL

1. In the URL Lookup frame, enter the **URL**. For example, enter **http://www.playboy.com**, **playboy.com**, or use a wildcard by entering ***.playboy.com**. A wildcard entry finds all URLs containing text that follows the period (.) after the asterisk (*).

   The following types of URL formats also can be entered in this field:

   - IP address - e.g. "209.247.228.221" in http://209.247.228.221
   - octal format - e.g. http\://0106.0125.0226.0322
   - hexadecimal short format - e.g. http\://0x465596d2
   - hexadecimal long format - e.g. http://0x46.0x55.0x96.0xd2
   - decimal value format - e.g. http://1180014290
   - escaped hexadecimal format - e.g. http://%57%57%57.%41%44%44%49%43%54%49%4E%47%47%41%4D%45%53.%43%4F%4D

***NOTE**: The minimum number of wildcard 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).*

2. Click **Lookup** to open the alert box asking you to wait while the search is being performed.
3. Click **OK** to close the alert box and to display any results in the Result Category list box, showing the long name of the library category, followed by the URL.

Look up a Search Engine Keyword

To see if a search engine keyword or keyword phrase has been included in any library category:

1. In the Search Engine Keyword Lookup frame, enter the **Search Engine Keyword** or keyword phrase, up to 75 alphanumeric characters.
2. Click **Lookup** to display results in the Result Category list box, showing the long name of all categories that contain the search engine keyword/phrase.

Custom Categories

Custom Categories includes the ALLOW and BLOCK library categories. Click either ALLOW or BLOCK to view a menu of sub-topics: Library Details, URLs, URL Keywords, and Search Engine Keywords.

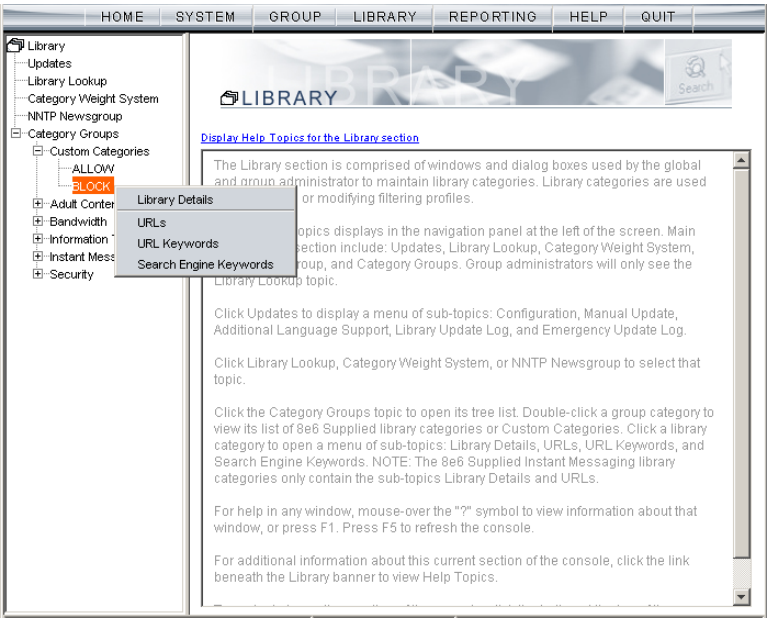


Fig. 3:2-3 Library screen, custom library category menu

***NOTE**: Maintaining the list of custom category URLs and keywords is the responsibility of the global administrator.*

Library Details window

The Library Details window displays when Library Details is selected from the ALLOW or BLOCK library category's menu of sub-topics. This window is used for editing the long name of the custom library category, and for viewing name criteria previously entered.

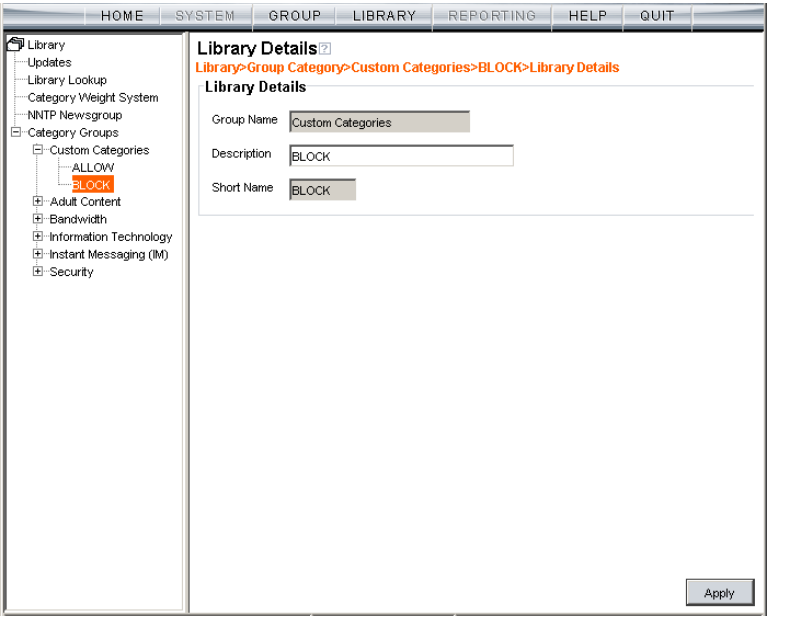


Fig. 3:2-4 Library Details window

View, Edit Library Details

The following display and cannot be edited: Custom Categories **Group Name** and library category **Short Name**.

1. The long **Description** name displays and can be edited.
2. After modifying the description for the library category, click **Apply** to save your entry.

URLs window

The URLs window displays when URLs is selected from the custom library category's menu of sub-topics. This window is used for viewing, adding and/or removing a URL from a custom library category's master URL list or master wildcard URL list. A URL can contain a domain name—such as "playboy" in **http://www.playboy.com**—or an IP address—such as "209.247.228.221" in **http://209.247.228.221**. A wildcard asterisk (*) symbol followed by a period (.) can be entered in a format such as ***.playboy.com**, for example, to block access to all URLs ending in ".playboy.com". A URL is used in a filtering profile for blocking a user's access to a specified site or service.

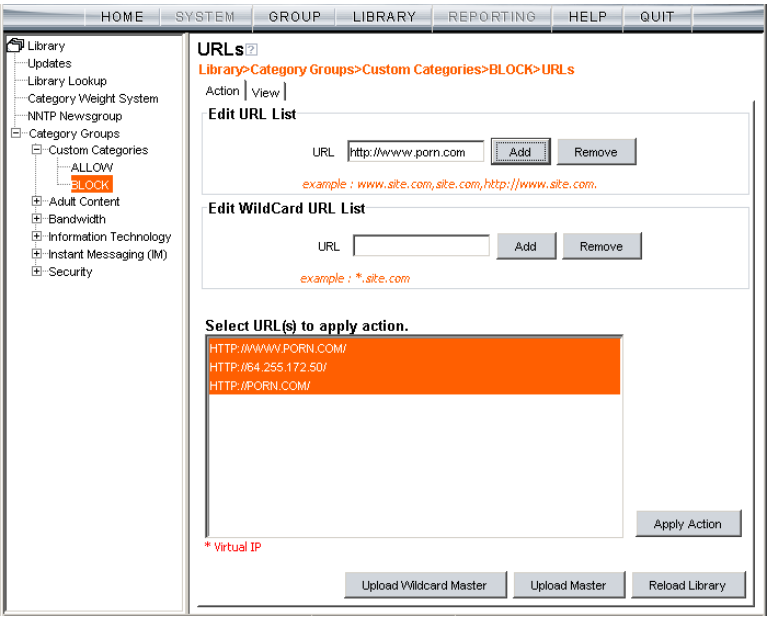


Fig. 3:2-5 URLs window, Action tab

View a List of URLs in the Library Category

To view a list of all URLs that either have been added or deleted from the master URL list or master wildcard URL list:

1. Click the View tab.
2. Make a selection from the pull-down menu for “Master List”, or “Wild Card Master List”.
3. Click **View List** to display the specified items in the Select List list box:

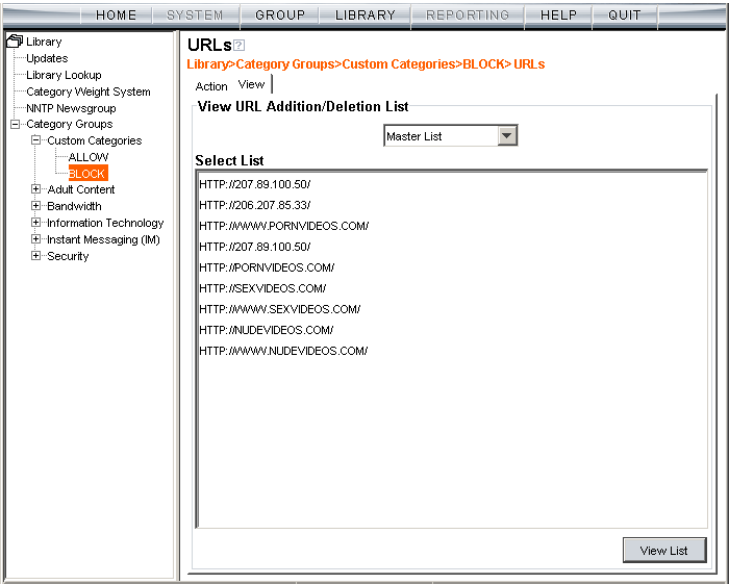


Fig. 3:2-6 URLs window, View tab

Add or Remove URLs or Wildcard URLs

The Action tab is used for making entries in the URLs window for adding or removing a URL or wildcard URL, uploading a master URL list or master wildcard URL list, or reloading the library.

Add a URL to the Library Category

To add a URL to the library category:

1. In the Edit URL List frame, enter the **URL** in a format such as **http://www.playboy.com**, **www.playboy.com**, or **playboy.com**.

   The following types of URL formats also can be entered in this field:

   - IP address - e.g. "209.247.228.221" in http://209.247.228.221
   - octal format - e.g. http\://0106.0125.0226.0322
   - hexadecimal short format - e.g. http\://0x465596d2
   - hexadecimal long format - e.g. http://0x46.0x55.0x96.0xd2
   - decimal value format - e.g. http://1180014290
   - escaped hexadecimal format - e.g. http://%57%57%57.%41%44%44%49%43%54%49%4E%47%47%41%4D%45%53.%43%4F%4D
2. Click **Add** to display the associated URL(s) in the list box below.
3. Select the URL(s) that you wish to add to the category.

***TIP**: Multiple URLs can be selected by clicking each URL while pressing the Ctrl key on your keyboard. Blocks of URLs can be selected by clicking the first URL, and then pressing the Shift key on your keyboard while clicking the last URL.*

4. Click **Apply Action**.

Add a Wildcard URL to the Library Category

***NOTE**: Wildcards are to be used for blocking only. They are not designed to be used for the exceptions function or the always allowed white listing function.*

To add a URL containing a wildcard to the library category:

1. In the Edit WildCard URL List frame, enter the asterisk (*) wildcard symbol, a period (.), and the **URL**.

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

2. Click **Add** to display the associated wildcard URL(s) in the list box below.
3. Select the wildcard URL(s) that you wish to add to the category.
4. Click **Apply Action**.

***NOTE**: Wildcard URL query results include all URLs containing text following the period (.) after the wildcard (*) symbol. For example, an entry of *.porn.com would find a URL such as http://sex.porn.com. However, if a specific URL was added to a library category that is **not** set up to be blocked, and a separate wildcard entry containing a portion of that URL is added to a category that **is** set up to be blocked, the end user will be able to access the non-blocked URL but not any URLs containing text following the wildcard. For example, if http://www.sex.com is added to a category that is not set up to be blocked, and *.sex.com is added to a category set up to be blocked, the end user will be able to access http://www.sex.com since it is a direct match, but will not be able to access http://www.videos.sex.com, since direct URL entries take precedence over wildcard entries.*

Remove a URL from the Library Category

To remove a URL or wildcard URL from the library category:

1. Click the Action tab.
2. Enter the **URL** in the Edit URL List frame or Edit Wild-Card URL List frame, as pertinent.
3. Click **Remove** to display the associated URLs in the list box below.
4. Select the URL(s) that you wish to remove from the category.
5. Click **Apply Action**.

Upload a Master List to the Library

Upload a Master List of URLs

To upload a master file with URL additions:

1. Click **Upload Master** to open the Upload Custom Library URL pop-up window:

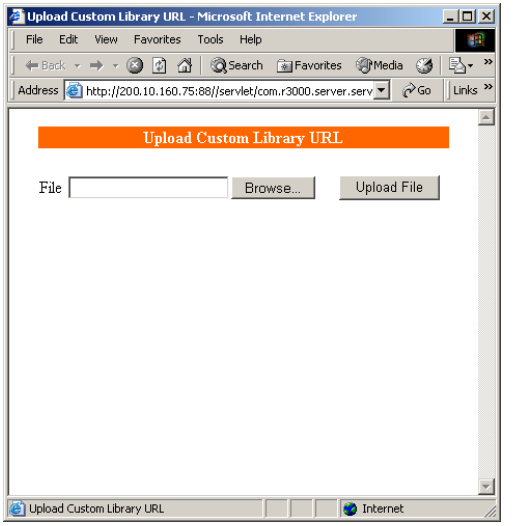


Fig. 3:2-7 Upload Custom Library URL window

2. Click **Browse** to open the Choose file pop-up window.
3. Select the file to be uploaded.

***TIP**: A URL text file must contain one URL per line.*

***WARNING**: The text file uploaded to the server will overwrite the current file.*

***NOTE**: Before the file is uploaded to the server, it will first be validated.*

4. Click **Upload File** to display the results of the library file content validation in the Library File Content/IP Lookup Options pop-up window:

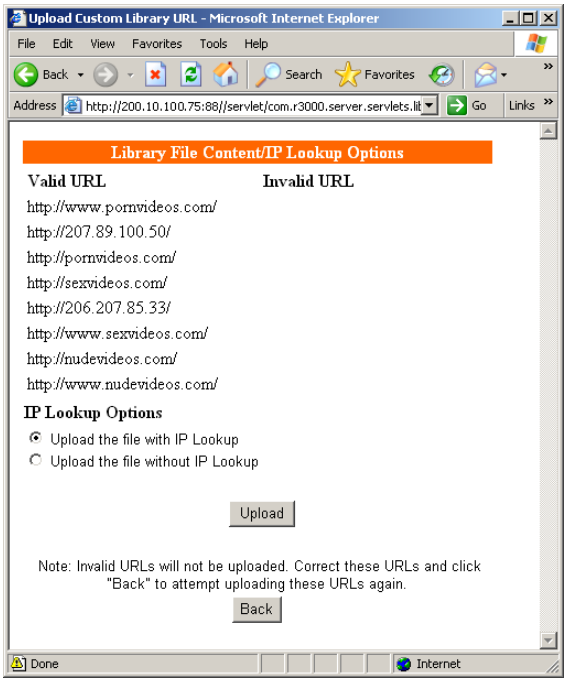


Fig. 3:2-8 Library File Content/IP Lookup Options

URLs contained in the file are listed under the column for either Valid URL or Invalid URL.

5. If the file contains invalid URLs, click **Back** to return to the Upload URL window. Another attempt to validate the file can be made after corrections have been made to the file.

   If the file contains valid URLs:

   a. Go to the **IP Lookup Options** section and click the radio button corresponding to the option to be used when uploading the file:

      • “Upload the file with IP Lookup” - If this option is

selected, IP addresses that correspond to URLs in the uploaded file will be blocked along with the URLs.

- "Upload the file without IP Lookup" - If this option is selected, an IP lookup for IP addresses that correspond to URLs in the uploaded file will not be performed.

b. Click **Upload** to open the Upload Successful pop-up window.

***NOTE**: In order for the URLs to take effect, library categories must be reloaded.*

Upload a Master List of Wildcard URLs

To upload a master file with wildcard URL additions:

1. Click **Upload Wildcard Master** to open the Upload Custom Library WildCard URL pop-up window:

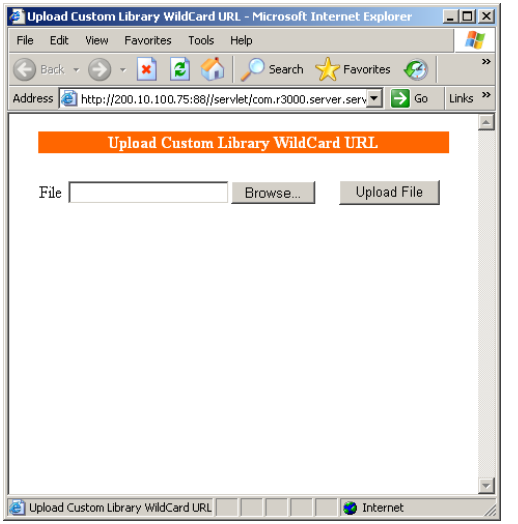


Fig. 3:2-9 Upload Custom Library WildCard URL window

2. Click **Browse** to open the Choose file pop-up window.

3. Select the file to be uploaded.

***TIP**: A wildcard URL text file must contain one wildcard URL per line.*

***WARNING**: The text file uploaded to the server will overwrite the current file.*

***NOTE**: Before the file is uploaded to the server, it will first be validated.*

4. Click **Upload File** to display the results of the library file content validation in the Library File Content/IP Lookup Options pop-up window:

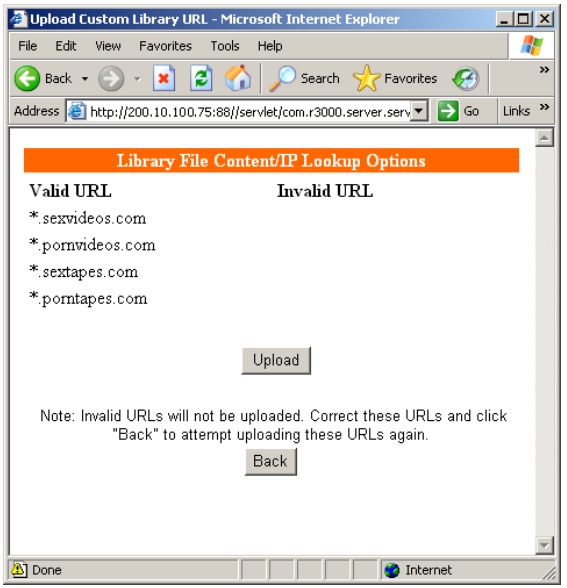


Fig. 3:2-10 Library File Content/IP Lookup Options

Wildcard URLs contained in the file are listed under the column for either Valid URL or Invalid URL.

5. If the file contains invalid wildcard URLs, click **Back** to return to the Upload WildCard URL window. Another attempt to validate the file can be made after corrections have been made to the file.

If the file contains valid wildcard URLs, click **Upload** to open the Upload Successful pop-up window.

***NOTE**: In order for the URLs to take effect, library categories must be reloaded.*

Reload the Library

After all changes have been made to library windows, click **Reload Library** to refresh.

***NOTE**: Since reloading the library utilizes system resources that impact the performance of the ProxyBlocker, 8e6 recommends clicking Reload Library only after modifications to all library windows have been made.*

URL Keywords window

The URL Keywords window displays when URL Keywords is selected from the ALLOW or BLOCK library category's menu of sub-topics. This window is used for adding or removing a URL keyword from a custom library category's master list. A library category uses URL keywords to block a user's access to Internet addresses containing keywords included in its list.

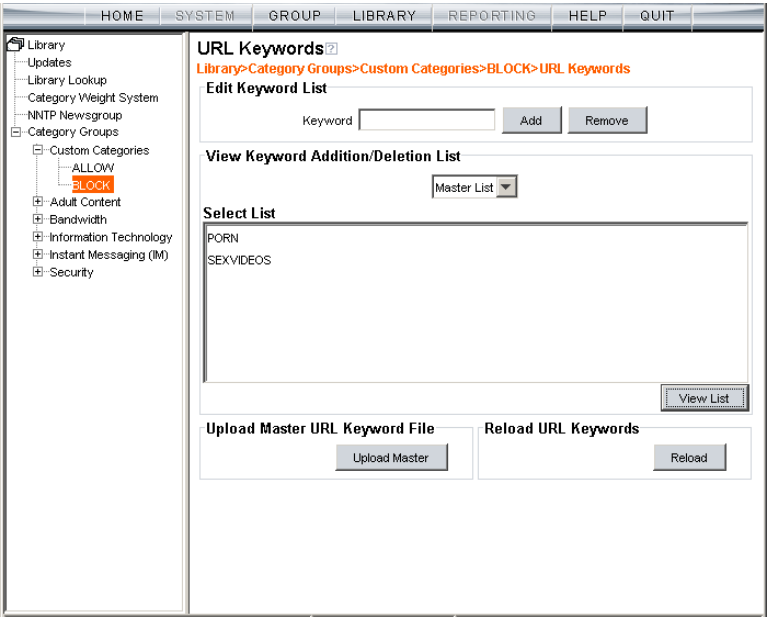


Fig. 3:2-11 URL Keywords window

***NOTE**: If the feature for URL keyword filtering is not enabled in a filtering profile, URL keywords can be added in this window but URL keyword filtering will not be in effect for the user(s). (See the Filter Options tab in the Group screen section for information about enabling URL keyword filtering.)*

***WARNING**: Use extreme caution when setting up URL keywords for filtering. If a keyword contains the same consecutive characters as a keyword set up to be blocked, users will be denied access to URLs that are not even within blocked categories. For example, if all URL keywords containing "sex" are blocked, users will not be able to access a non-pornographic site such as http://www.essex.com.*

View a List of URL Keywords

To view a list of all URL keywords that either have been added or deleted:

1. In the View Keyword Addition/Deletion List frame, make a selection from the pull-down menu for "Master List".
2. Click **View List** to display the specified items in the Select List list box.

Add or Remove URL Keywords

Add a URL Keyword to the Library Category

To add a URL keyword to the library category:

1. Enter the **Keyword** in the Edit Keyword List frame.
2. Click **Add**.

Remove a URL Keyword from the Library

To remove a URL keyword from the library category:

1. Enter the **Keyword**.
2. Click **Remove**.

Upload a List of URL Keywords to the Library

To upload a text file containing URL keyword additions:

1. In the Upload Master URL Keyword File frame, click **Upload Master** to open the Upload Library Keyword pop-up window:

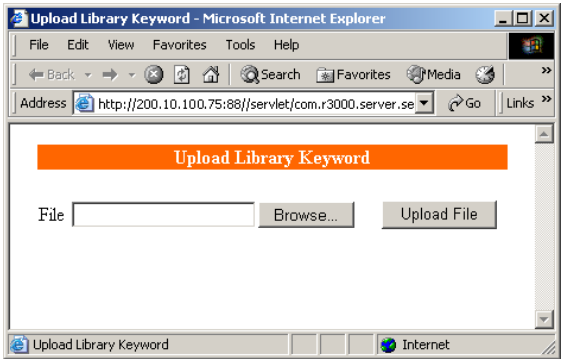


Fig. 3:2-12 Upload Library Keyword pop-up window

2. Click **Browse** to open the Choose file window.
3. Select the file to be uploaded.
4. Click **Upload File** to upload this file to the server.

***NOTE**: A URL keywords text file must contain one URL keyword per line.*

***WARNING**: The text file uploaded to the server will overwrite the current file.*

Reload the Library

After all changes have been made to library windows, in the Reload URL Keywords frame, click **Reload** to refresh.

***NOTE**: Since reloading the library utilizes system resources that impact the performance of the ProxyBlocker, 8e6 recommends clicking Reload only **after** modifications to **all** library windows have been made.*

Search Engine Keywords window

The Search Engine Keywords window displays when Search Engine Keywords is selected from the ALLOW or BLOCK library category's menu of sub-topics. This window is used for adding and removing search engine keywords and phrases to and from a custom library category's master list. A library category uses search engine keywords to block searches on subjects containing keywords included in its list.

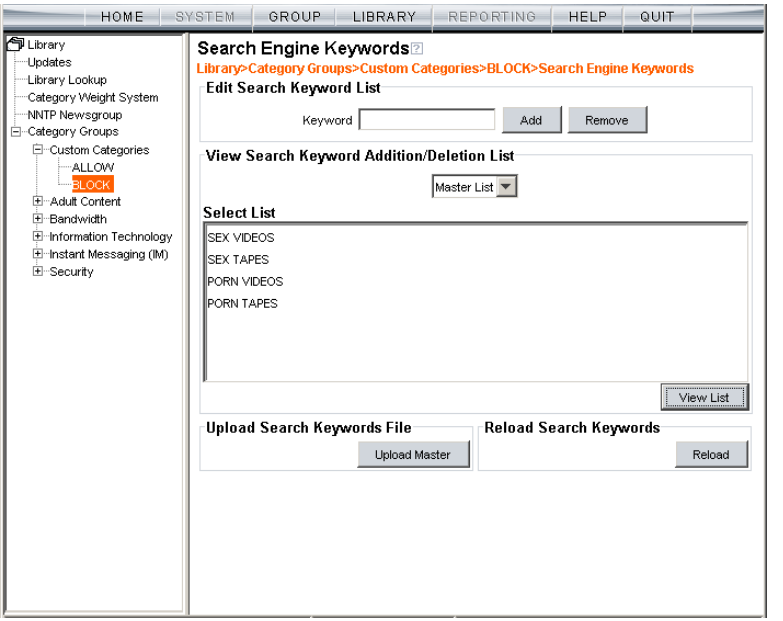


Fig. 3:2-13 Search Engine Keywords window

***NOTE**: If the feature for search engine keyword filtering is not enabled in a filtering profile, search engine keywords can be added in this window but search engine keyword filtering will not be in effect for the user(s). (See the Filter Options tab in the Group screen section for information about enabling search engine keyword filtering.)*

***WARNING**: Use extreme caution when setting up search engine keywords for filtering. If a non-offending keyword contains the same consecutive characters as a keyword set up to be blocked, users will be denied the ability to perform a search using keywords that are not even in blocked categories. For example, if all searches on "gin" are set up to be blocked, users will not be able to run a search on a subject such as "cotton gin". However, if the word "sex" is set up to be blocked, a search will be allowed on "sexes" but not "sex" since a search engine keyword must exactly match a word set up to be blocked.*

View a List of Search Engine Keywords

To view a list of all search engine keywords that either have been added or deleted:

1. In the View Search Keyword Addition/Deletion List frame, make a selection from the pull-down menu for "Master List".
2. Click **View List** to display the specified items in the Select List list box.

Add or Remove Search Engine Keywords

Add a Search Engine Keyword to the Library

To add a search engine keyword or keyword phrase to the library category:

1. In the Edit Search Keyword List frame, enter up to 75 alphanumeric characters in the **Keyword** field.
2. Click **Add**.

Remove a Search Engine Keyword

To remove a search engine keyword or keyword phrase from a library category:

1. In the Edit Search Keyword List frame, enter up to 75 alphanumeric characters in the **Keyword** field.
2. Click **Remove**.

Upload a Master List of Search Engine Keywords

To upload a master list containing search engine keyword/ phrase additions:

1. In the Upload Search Keywords File frame, click **Upload Master** to open the Upload Library Keyword pop-up window (see Fig. 3:2-12).
2. Click **Browse** to open the Choose file window.
3. Select the file to be uploaded.

***TIP**: A search engine keyword text file must contain one keyword/ phrase per line.*

***WARNING**: The text file uploaded to the server will overwrite the current file.*

4. Click **Upload File** to upload this file to the server.

Reload the Library

After all changes have been made to library windows, in the Reload Search Keywords frame, click **Reload** to refresh.

***NOTE**: Since reloading the library utilizes system resources that impact the performance of the ProxyBlocker, 8e6 recommends clicking Reload only **after** modifications to **all** library windows have been made.*

Delete Category

Delete a Custom Category

To delete a custom library category, choose Delete Category from the menu. This action removes the library category from the Custom Categories list.

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

Filtering Profile Format and Rules

A filtering profile must be set up in a specified format, containing the following items:

1. The username or group name
2. IP address
3. Filtering profile criteria:
   - Rule number (Rule0, Rule1, etc.), or
   - rule criteria:
     a. Ports to Block or Filter
     b. Categories to Block or Open
     c. Filter Mode
4. Redirect URL (optional)
5. Filter Options (optional). For IP profiles, the code 0x1 should be placed at the end with all filter options disabled.
6. Quotas (optional).

***NOTE**: Each filtering profile should be entered on a separate line in the file.*

Rule Criteria

Rule criteria consists of selections made from the following lists of codes that are used in profile strings:

- **Port command codes:**

  A = Filter all ports
  B = Filter the defined port number(s)
  I = Open all ports
  J = Open the defined port number(s)
  M = Set the defined port number(s) to trigger a warn message
  Q = Block all ports
  R = Block the defined port number(s)

- **Port Numbers:**

  21 = FTP (File Transfer Protocol)
  80 = HTTP (Hyper Text Transfer Protocol)
  119 = NNTP (Network News Transfer Protocol)
  443 = HTTPS (Secured HTTP Transmission)
  Other

- **Filter Mode Values:**

  1 = Default, Block Mode
  2 = Monitoring Mode
  4 = Bypassing Mode

- **Category command codes:**

  Category command codes must be entered in the following order: J, R, M, I. “PASSED” should either be entered after J, R, or M, or after a string of category codes following J, R, or M.

  J = Positioned before the category/categories defined as "always allowed."

  R = Positioned before the category/categories defined as "blocked."

  M = Positioned before the category/categories defined as containing URLs potentially against the organization’s policies, and accompanied by a warning message.

  I = Positioned at the end of a profile string, indicating that all other categories should “pass.”

  PASSED = When positioned at the end of a string of categories or after a category command code, this code indicates that unidentified categories will follow suit with categories defined by that code: J (pass), R (block), or M (receive warning message).

- **Category Codes:**

  For the list of category codes (short names) and their corresponding descriptions (long names), go to **http://www.8e6.com/pbahelp/files/2group_textfile_cat.html#cat**

NOTE**: The list of library category codes and corresponding descriptions is subject to change due to the addition of new categories and modification of current categories. For explanations and examples of category items, go to **http://www.8e6.com/database-categories.html

- **Filter Option codes:**

  • 0x1 = Exception URL Query (always enabled)
  • 0x2 = X Strikes Blocking
  • 0x4 = Google/Yahoo!/Ask.com/AOL Safe Search Enforcement
  • 0x100 = Search Engine Keyword
  • 0x200 = URL Keyword
  • 0x1000= Extend URL Keyword Filter Control

***NOTE**: To enable multiple filter codes, add the codes together. For example, to enable all features for an IP profile, add 1 + 2 + 4 + 100 + 200 + 1000 = 1307, which means that **0x1307** should be entered at the end of the profile string (unless the quota option is used, in which case the quota should be entered at the end of the profile string). To disable all filter codes for an IP profile, enter **0x1** for the filter option.*

- **Quota format**

  To include quotas in a profile string, enter them after the filter options using this format: A semicolon (**;**), Overall Quota minutes, a comma (**,**), the first library category code, a colon (**:**), the number of quota minutes, and a comma between each quota. For example: ***;10, EMPL:30, FINAN:30, GENBUS:30, TRADING:30, ESTATE:30***

***NOTES**: See **http://www.8e6.com/pbahelp/files/2group_ipprofiles.html** for examples of filtering profile entries.*

Appendix B

Traveler Log Messages

Your ProxyBlocker receives 8e6 supplied library category updates and software updates via Traveler, 8e6's executable program for updating the ProxyBlocker server. You can run Traveler on demand via the Manual Update to 8e6 Supplied Categories window, or schedule Traveler to launch at a specified time via the Configuration window. (See the Library screen's Configuration window and Manual Update window in the Global Group Section for more information about updating 8e6 supplied library categories.)

***NOTE**: In the Global Administrator Section: Library screen, see the Library Update Log window for information about viewing the library update log.*

Messages in this Appendix are grouped according to the type of activity Traveler attempts to perform:

- General Activity
- Weekly Update (7 Days Library)
- Full URL Library Update
- All Library Updates (includes all other messages)
- Patch Update
- Emergency Update

General Activity

Startup, Finish

- Logging to: <log file>
- Start running Traveler
- Traveler has finished running.

Command Executed More than Once

- Traveler is running, cannot start another traveler.
- Installscript is running, cannot start another traveler.
- Traveler_Full_Download is running, cannot start another traveler.

System Command Execution

- Run system command: <killCmd>
- Failed in executing : <killCmd>

Temp Files

- Create tmp file.
- getpid().
- Write pid to tmp file.
- Traveler failed to create the tmp file:

  <ServerConstants.TRAVELER_TEMP>
- Temp file deleted.
- Fail to rename <szFileUrlTemp> to final <szFileUrl>

Library Download Process

- <filename> needs to be updated.
- <filename> does not need to be updated.
- Preparing for download
- Prepare for download -- Fail
- Downloading files
- Processing downloaded files
- Processing downloaded files -- Fail
- Decrypting file...
- Decryption success.
- A problem occurred while deleting: <filename>
- HTTPS download complete: <filename> <--For HTTPS downloads
- File does not exist on the update server.
- Login error.
- Could not write history file! (exception)
- Could not read emergency date from: <emergency update file>.
- Failed to download <filename> (Exception)
- Finished updating libraries!

Customer Feedback Module Option

- To start CFM
- To run CFM
- Starting usage feedback/reporting upload
- Running usage feedback/reporting upload

Library Update Process

- Wrong Argument!
- Error occurred during the Traveler process!
- Connection is lost.
- Finished updating library!
- Fail to download all libraries
- Failed to sort the library files!
- Started reloading library!
- Finished reloading library!
- Library <filename> does not exist!
- Fail to encrypt <category> library!

Printstack Trace

- PrintstackTrace - Fail to back up file for <FileUrl>
- PrintStackTrace - <java error message>
- PrintstackTrace - Fail to back up file for <category>.sew
- PrintstackTrace - Fail to copy file for merging

Error Messages

- Running Traveler encounters an exception.
- Alert emails could not be read. "<email alert configuration file>" does not exist.
- Reloading library encounters an exception
- Send alert encountered an exception
- Traveler exits after reaching time limit: <time limit> mins
- Log file could not be set. (Exception)
- List could not be read from file.

Weekly Update (7 Days Library)

- Download library update:
- Download thread interrupted during retries.
- Successfully downloaded <deleted category>
- Failed to download <deleted category>
- Failed to download <category> library
- Successfully downloaded <category> library
- Fail to unzip <category>
- Weekly Update has completed.

Summary Messages

- Failed to download.
- File does not exist.
- Failed to unzip.
- Was not a primary language deletion file.
- Failed to sort the library files.
- Failed to merge files for <category>
- File is the most current version.
- Successfully updated.
- Checksum verification failed.

Full URL Library Update (URLs, URL Keywords)

- Download full library:
- Failed to download <category> library
- Successfully download <category> library!
- Failed to unzip <category>
- Full URL Library Update has completed.

All Library Updates (includes all other msgs.)

- Download full library & keyword library all categories:
- Successfully download <category> deletion library!
- Fail to download <category> deletion library!
- Trial <itotal>: Fail to download <category> deletion library!
- Complete Update has successfully completed.

IM and P2P Pattern File Update

- Successfully downloaded <pattern>
- Failed to download <pattern>
- IM and P2P Update has successfully completed.

Newsgroup Library Update (News)

- Download newsgroup:
- Successfully downloaded newslist
- Failed to download newslist
- Newsgroup Library Update has successfully completed.

Search Engine Keywords Library Update

- Download keyword library:
- Fail to download <category> keyword library due to connection fail!
- Successfully downloaded <category>
- Fail to download <category>
- Search Engine Keyword Library Update has successfully completed.

Patch Update

- Download patch:
- Downloading patch - Dated: <patchdate>
- The patch has been downloaded already!
- Successfully processed <patch>
- Failed to download <patch>
- Patch Update has completed.

Emergency Update

- Emergency update:
- Could not read emergency date from: <emergency update file>.
- Emergency Update has completed.

Appendix C

Create a Custom Block Page

8e6 offers ways for you to customize the block page so that the page can have a different look while retaining the information/functionality provided in 8e6's default block page.

***NOTE**: The solutions provided in this appendix will only let you customize the Block page, not the Options page.*

Part I: Modify the ProxyBlocker

1. Enable block page redirection

Select either of the following options to modify the ProxyBlocker. Option 1 lets you modify the back end, and Option 2 lets you modify the ProxyBlocker console.

Option 1: Modify the back end

- *PROS: No need to set up the redirect URL for each group.*
- *CONS: Redirect URL must be set up in the back end.*

LDC_http_default_redirecturl http://<server for block_page>[:<port for block page>]/<blockpage>

LDC_fother_default_redirecturl http://<server for block_page>[:<port for block page>]/<blockpage>

LDC_proxy_default_redirecturl http://<server for block_page>[:<port for block page>]/<blockpage>

Option 2: Modify the ProxyBlocker console

- *PROS: Can be done from the ProxyBlocker console.*
- *CONS: Must be set up for each sub-group.*

1. Make modifications in one of the redirect URL tabs:
   - Go to: Group > IP > “Group Name” > “Sub-Group Name” > Sub Group Profile > Redirect URL
   - Go to: Group > Global Group > Global Group Profile > Default Redirect URL
2. Set the redirect URL to: http://<server for block_page>[:<port for block page>]/<blockpage>

***NOTE**: The ProxyBlocker does not accept the URL with a port setting (:<port for block page>), so to get around this the block page must be placed at the default HTTP port, which is 80. Since the console may not allow certain characters (e.g. “_”), if such characters are used in the URL a modified name must be used instead for the <blockpage>.*

As a result, the ProxyBlocker will redirect the block page to the customized one with the following link format:

http://<server for block_page>[:<port for block page>]/<blockpage>?URL=<blocked url>&IP=<client IP>&CAT=<URL category>&USER=<client User Name>

2. Exclude filtering <server for block page> IP

1. Go to: GUI: Group > Global Group > Range to Detect
2. Input the IP address under “Destination IP” > ”Exclude IP”

   Without excluding this IP address, the ProxyBlocker may capture/filter/block the following redirect link:

   http://<server for block_page>[:<port for block page>]/<blockpage>?URL=<blocked url>&IP=<client IP>&CAT=<URL category>&USER=<client User Name>

Part II: Customize the Block Page

1. Set up a Web server

A Web server must be set up to hold the customized block page.

2. Create a customized block page

The customized block page must be accessible via this link:

http://<server for block_page>[:<port for block page>]/<blockpage>

Show 8e6's information in the block page (optional)

The following information is passed to the <blockpage> through the query string:

Name	Description: *Value*
URL	Blocked URL: *From the query string of the block page URL*
IP	IP that accessed the blocked URL: *(see URL)*
CAT	Category of the blocked URL: *(see URL)*
USER	User Name that accessed the blocked URL: *(see URL)*

Implement the "further option" (optional)

The "further option" is included in 8e6's default block page. If used, the <block page> needs to provide a link back to ProxyBlocker's Options page and post the required hidden form data (shown in the table below):

Name	Description: *Value*
SITE	Optional value: *_BLOCK_SITE_*
URL	Blocked URL: *From the query string of the* block page URL
IP	IP that accessed the blocked URL: *(see URL)*
CAT	Category of the blocked URL: *(see URL)*
USER	User Name that accessed the blocked URL: *(see URL)*
STEP	Required value: *STEP 2*

Customized block page examples

The examples in the Reference portion of this appendix illustrate how form data is parsed and posted in the customized block page. Examples include:

1. HTML (using Java Script to parse/post form data)
2. CGI written in Perl
3. CGI written in C

See the Reference portion of this appendix for coding details.

***NOTE**: Don't forget to replace <ProxyBlocker IP> with the real IP in the HTML/CGI before using these samples.*

Part III: Restart the ProxyBlocker

You must restart the unit to make your changes effective.

Reference

HTML

```
<!-- Description: Sample HTML for ProxyBlocker customized block page
-->
<!-- Replace <ProxyBlocker IP> with real IP before using -->
<!-- Revision: 1 -->
<!-- Date: 03/08/2004 -->

<html>
<head>
<script language=javascript>
function parseData(str, start, end)
{
        result = "";
        i = str.indexOf(start);
        if (i >= 0) {
                len = str.length;
                substr = str.substr(i+start.length, len -
start.length);

                j = substr.indexOf(end);
                if ( j > 0) {
                        result = substr.substring(0, j);
                }
                else {
                        if ( j != 0) {
                                len = substr.length;
                                result = substr.substr(0, len);
                        }
                }
        }
        return result;
}
function getData(){
        str = document.location.href;
        len = str.length;
        i = str.indexOf("?");
        if ( i>= 0) {
                query = str.substr(i+1, len-i-1);
                url = parseData(query, "URL=", "&");
                document.block.URL.value = url;
                ip = parseData(query, "IP=", "&");
                document.block.IP.value = ip;
                cat = parseData(query, "CAT=", "&");
                document.block.CAT.value = cat;
```

```
                user = parseData(query, "USER=", "&");
                document.block.USER.value = user;
        }
}
function showData(){
        document.write("URL:" + document.block.URL.value + "<br>");
        document.write("IP:" + document.block.IP.value + "<br>");
        document.write("CAT:" + document.block.CAT.value + "<br>");
        document.write("USER:" + document.block.USER.value +
"<br>");
}
function do_options(){
        document.block.action="http://<ProxyBlocker IP>:81/cgi/
block.cgi"
        document.block.submit();
}
</script>

</head>

<body>

<form method=post name=block >
        <input type=hidden name="SITE" value="_BLOCK_SITE_">
        <input type=hidden name="URL" value="">
        <input type=hidden name="IP" value="">
        <input type=hidden name="CAT" value="">
        <input type=hidden name="USER" value="">
        <input type=hidden name="STEP" value="STEP2">
</form>

<br>ProxyBlocker Customized Block Page (HTML using Java Script to
parse and post form data)<br>
<script language=javascript>
        getData();
        showData();
</script>
<br>For further options, <a
href="javascript:do_options()">click here</a><br>

</body>
</html>
```

CGI written in Perl

There are two methods for CGI written in Perl: One lets you embed data in the query string to pass data to the Options CGI, and the other lets you use Java Script to post form data to the Options CGI.

Embed data in query string

```
#!/usr/bin/perl
# Original Filename: cusp_block1.cgi
# File Type:     CGI
# Description:   Sample Perl script for ProxyBlocker customized
block page
# Replace the <ProxyBlocker IP> with the real IP before using.
# This script provide data to the options CGI through query string
# Revision:      1
# Date: 03/08/2004

$method = $ENV{'REQUEST_METHOD'};

if ($method=~ /post/i) {
    $string = <STDIN>;
} else {
    $string= $ENV{"QUERY_STRING"};
}

$url = $1 if ($string =~ /URL=(\S+)&IP=/i);
$ip = $1 if ($string =~ /IP=(\S+)&CAT=/i);
$cat = $1 if ($string =~ /CAT=(\S+)&USER=/i);
$user = $1 if ($string =~ /USER=(\S+)/i);

print "Content-type: text/html\n\n";
print "<html>\n";
print "<head>\n";
print "</head>\n";
print "<body>\n";

print "<br>ProxyBlocker Customized Block Page (CGI written with
Perl)<br>\n";

print "URL: $url<br>\n";
print "IP: $ip<br>\n";
print "CAT: $cat<br>\n";
print "USER: $user<br>\n";
```

```
print "<br>For further options, <a href=\"http://<ProxyBlocker
IP>:81/cgi/
block.cgi?URL=$url&IP=$ip&CAT=$cat&USER=$user&STEP=STEP2\">click
here</a><br>\n";

print "</body>\n";
print "</html>\n";
```

Use Java Script to post form data

```
#!/usr/bin/perl
# Original Filename: cusp_block2.cgi
# File Type:         CGI
# Description:       Sample Perl script for ProxyBlocker customized
block page
# Replace the <ProxyBlocker IP> with the real IP before using.
# This script uses Java Script to post form data to
# options CGI
# Revision:          1
# Date: 03/08/2004

$method = $ENV{'REQUEST_METHOD'};

if ($method=~ /post/i) {
    $string = <STDIN>;
} else {
    $string= $ENV{"QUERY_STRING"};
}

$url = $1 if ($string =~ /URL=(\S+)&IP=/i);
$ip = $1 if ($string =~ /IP=(\S+)&CAT=/i);
$cat = $1 if ($string =~ /CAT=(\S+)&USER=/i);
$user = $1 if ($string =~ /USER=(\S+)/i);

print "Content-type: text/html\n\n";
print "<html>\n";

print "<head>\n";

print "<script language=\"JavaScript\">\n";
print "function do_options()\n";
print "{\n";
print "document.block.action=\"http://<ProxyBlocker IP>:81/cgi/
block.cgi\"\n";
print "document.block.submit()\n";
print "}\n";
print "</script>\n";
print "</head>\n";
```

```
print "<body>\n";

print "<form method=post name=block>\n";
print "<input type=hidden name=\"SITE\"
value=\"_BLOCK_SITE_\">\n";
print "<input type=hidden name=\"IP\" value=\"$ip\">\n";
print "<input type=hidden name=\"URL\" value=\"$url\">\n";
print "<input type=hidden name=\"CAT\" value=\"$cat\">\n";
print "<input type=hidden name=\"USER\" value=\"$user\">\n";
print "<input type=hidden name=\"STEP\" value=\"STEP2\">\n";

print "<br>ProxyBlocker Customized Block Page (CGI written with Perl
using Java Script to post form data)<br>\n";

print "URL: $url<br>\n";
print "IP: $ip<br>\n";
print "CAT: $cat<br>\n";
print "USER: $user<br>\n";

print "<br>For further options, <a
href=\"javascript:do_options()\">click here</a><br>\n";
print "</form>";

print "</body>\n";
print "</html>\n";
```

CGI written in C

```
/*
 * cusc_block.c
 * Description: sample C source code of CGI for customized block page
 * Replace <ProxyBlocker IP> with real IP and recompile before using
 * Revision: 1
 * Date: 03/08/2004
 */
#include <stdio.h>

struct {
    char *name;
    char *val;
} entries[20];

char szIP[16];
char szURL[1024];
char szUserName[1024];
char szCategory[8];

/*function prototypes*/
void printhtml();
void unescape_url(char *url);
char x2c(char *what);
char *makeword(char *line, char stop);
void plustospace(char *str);
char *fmakeword(FILE *f, char stop, int *cl);
int to_upper(char *string);
void getquery(char *paramd, char **paramv);
void getnextquery(char **paramv);

int main(int argc, char **argv)
{
    int data_size; /* size (in bytes) of POST input */
    int index;
    char *paramd, *paramn, *paramv;
    char step[120];

    printf("content-type: text/html\n\n");

    /* If using the GET method */
    if (strcmp((char *)getenv("REQUEST_METHOD"), "GET") == 0)
    {
        paramd = (char *)strdup((char *)getenv("QUERY_STRING"));
        getquery(paramd, &paramv);
        while (paramv)
        {
            plustospace(paramv);
```

```
                unescape_url(paramv);
                paramn = (char *)makeword(paramv, '=');
                to_upper(paramn);

                if (strcmp(paramn, "IP") == 0)
                    strcpy(szIP, paramv);
                else if (strcmp(paramn, "URL") == 0)
                    strcpy(szURL, paramv);
                else if (strcmp(paramn, "CAT") == 0)
                    strcpy(szCategory, paramv);
                else if (strcmp(paramn, "USER") == 0)
                    strcpy(szUserName, paramv);

                getnextquery(&paramv);
            }
            free(paramd);
        }
        else
        {
            /*=================================================
            Read stdin and convert form data into an array; set
            a variety of global variables to be used by other
            areas of the program
            =================================================*/
            data_size = atoi(getenv("CONTENT_LENGTH"));
            for(index = 0; data_size && (!feof(stdin)); index++)
            {
                entries[index].val = (char *)fmakeword(stdin, '&',
        &data_size);
                plustospace(entries[index].val);
                unescape_url(entries[index].val);
                entries[index].name = (char
        *)makeword(entries[index].val, '=');

                if (strcmp(entries[index].name, "IP") == 0)
                    strcpy(szIP, entries[index].val);
                else if (strcmp(entries[index].name, "URL") == 0)
                    strcpy(szURL, entries[index].val);
                else if (strcmp(entries[index].name, "CAT") == 0)
                    strcpy(szCategory, entries[index].val);
                else if (strcmp(entries[index].name, "USER") == 0)
                    strcpy(szUserName, entries[index].val);
            }
        }

        printhtml();
    }

    void printhtml()
```

```
{
    printf("<html>\n");
    printf("<head>\n");
    printf("<script language=\"JavaScript\">\n");
    printf("function do_options()\n");
    printf("{\n");
    printf("document.block.action=\"http://<ProxyBlocker IP>:81/
cgi/
block.cgi\"\n");
    printf("document.block.submit()\n");
    printf("}\n");
    printf("</script>\n");
    printf("</head>\n");

    printf("<form method=post name=block >\n");
    printf("<input type=hidden name=\"SITE\"
value=\"_BLOCK_SITE_\">\n");
    printf("<input type=hidden name=\"IP\" value=\"%s\">\n", szIP);
    printf("<input type=hidden name=\"URL\" value=\"%s\">\n",
szURL);
    printf("<input type=hidden name=\"CAT\" value=\"%s\">\n",
szCategory);
    printf("<input type=hidden name=\"USER\" value=\"%s\">\n",
szUserName);
    printf("<input type=hidden name=\"STEP\"
value=\"STEP2\">\n");
    printf("<br>ProxyBlocker Customized Block Page (CGI written
with C
using Java Script to post form data)<br>\n");

    printf("URL: %s<br>\n", szURL);
    printf("IP: %s<br>\n", szIP);
    printf("CAT: %s<br>\n", szCategory);
    printf("USER: %s<br>\n", szUserName);

    printf("<br>For further options, <a
href=\"javascript:do_options()\">click here</a><br>\n");

    printf("</form>\n");
    printf("</body>\n");
    printf("</html>\n");
}

/* functions to get the CGI parameters */
void unescape_url(char *url)
{
        register int x,y;

        for(x=0,y=0;url[y];++x,++y)
```

```
        {
            if((url[x] = url[y]) == '%')
            {
                url[x] = x2c(&url[y+1]);
                y+=2;
            }
        }
    url[x] = '\0';
}

char x2c(char *what)
{
    register char digit;

    digit = (what[0] >= 'A' ? ((what[0] & 0xdf) - 'A')+10 :
(what[0] - '0'));
    digit *= 16;
    digit += (what[1] >= 'A' ? ((what[1] & 0xdf) - 'A')+10 :
(what[1] - '0'));
    return(digit);
}

char *makeword(char *line, char stop)
{
    int x = 0, y;
    char *word = (char *) malloc(sizeof(char) * (strlen(line) +
1));

    for(x=0;((line[x]) && (line[x] != stop));x++)
        word[x] = line[x];

    word[x] = '\0';
    if(line[x]) ++x;
    y=0;

    while(line[y++] = line[x++]);
    return word;
}

void plustospace(char *str)
{
        register int x;

        for(x=0;str[x];x++)
            if(str[x] == '+')
                str[x] = ' ';
}

char *fmakeword(FILE *f, char stop, int *cl)
```

```
{
        int wsize;
        char *word;
        int ll;

        wsize = 102400;
        ll=0;
        word = (char *) malloc(sizeof(char) * (wsize + 1));

        while(1)
        {
            word[ll] = (char)fgetc(f);
            if(ll==wsize)
            {
                word[ll+1] = '\0';
                wsize+=102400;
                word = (char
*)realloc(word,sizeof(char)*(wsize+1));
            }
            --(*cl);
            if((word[ll] == stop) || (feof(f)) || (!(*cl)))
            {
                if(word[ll] != stop)
                    ll++;
                word[ll] = '\0';
                return word;
        }
        ++ll;
    }
}
/* to_upper:
 * Change the string to upper case
 */
int to_upper(char *string)
{
    int len;
    int i;
    char *tmp=NULL;

    if (string && strlen(string))
    {
        if (!(tmp=(char*)strdup(string)))
            return 0;
        len=strlen(string);
        for (i=0; i<len; i++)
        {
            string[i]=toupper(tmp[i]);
        }
        free(tmp);
```

```
}
return 1;
}

void getquery(char *paramd, char **paramv)
{
    if (paramd == NULL)
        *paramv = NULL;
    else
        *paramv = (char *)strtok(paramd, "&");
}

void getnextquery(char **paramv)
{
    *paramv = (char *)strtok(NULL, "&");
}
```

Appendix D

Override Pop-up Blockers

An override account user with pop-up blocking software installed on his/her workstation will need to temporarily disable pop-up blocking in order to authenticate him/herself via the Options page:

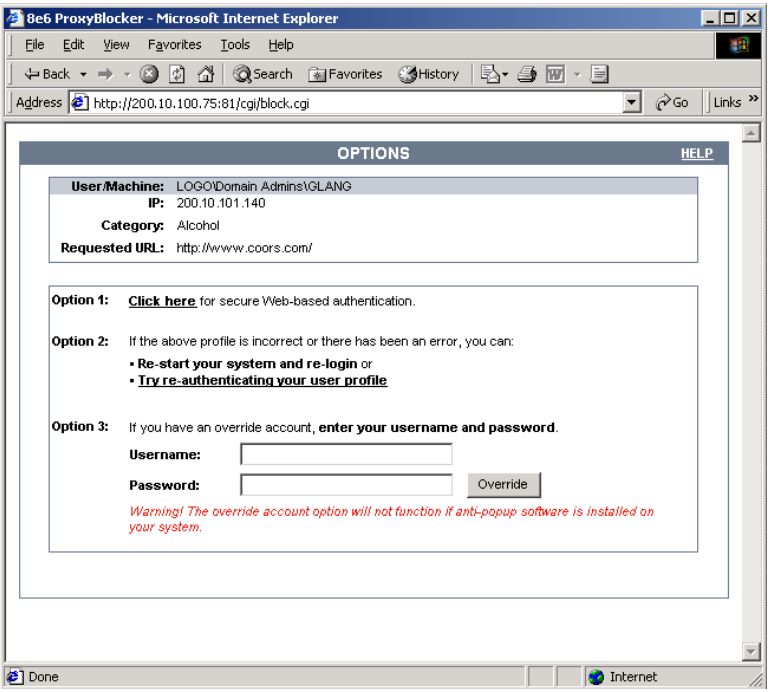


Fig. D-1 Options page

This appendix provides instructions on how to use an override account if typical pop-up blocking software is installed, as in the following products: Yahoo! Toolbar, Google Toolbar, AdwareSafe, Mozilla Firefox, and Windows XP Service Pack 2 (SP2).

Yahoo! Toolbar Pop-up Blocker

If Pop-up Blocking is Enabled

1. In the Options page (see Fig. D-1), enter your **Username** and **Password**.
2. Press and hold the **Ctrl** key on your keyboard while simultaneously clicking the **Override** button—this action opens the override account pop-up window.

Add Override Account to the White List

If the override account window 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:

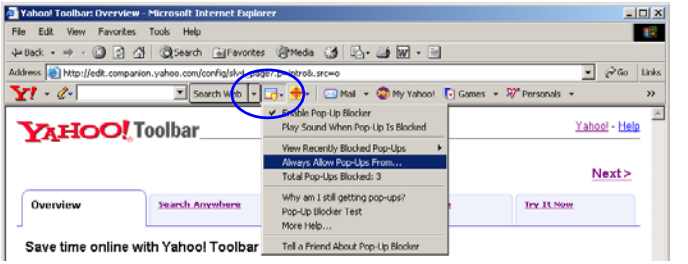


Fig. D-2 Select menu option Always Allow Pop-Ups From

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

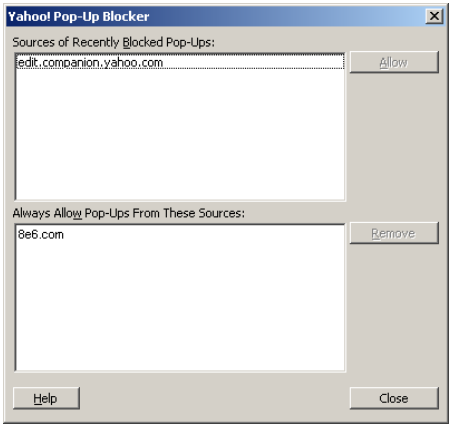


Fig. D-3 Allow pop-ups from source

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

If Pop-up Blocking is Enabled

1. In the Options page (see Fig. D-1), enter your **Username** and **Password**.
2. Press and hold the **Ctrl** key on your keyboard while simultaneously clicking the **Override** button—this action opens the override account pop-up window.

Add Override Account to the White List

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

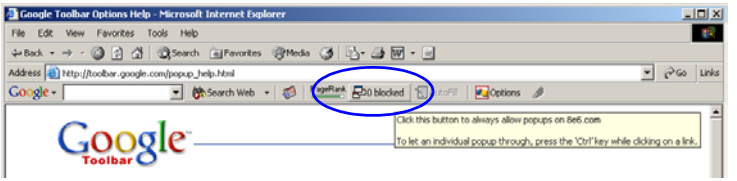


Fig. D-4 # blocked icon enabled

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

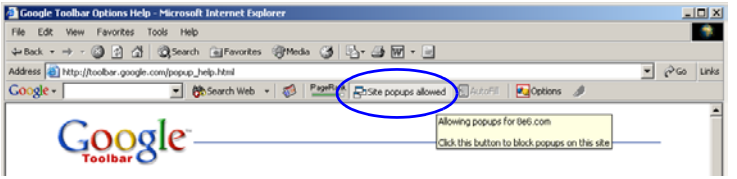


Fig. D-5 Site pop-ups allowed icon enabled

AdwareSafe Pop-up Blocker

If Pop-up Blocking is Enabled

1. In the Options page (see Fig. D-1), enter your **Username** and **Password**.
2. Press and hold the **Ctrl** key on your keyboard while simultaneously clicking the **Override** button—this action opens the override account pop-up window.

Temporarily 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. In the Options page (see Fig. D-1), enter your **Username** and **Password**.
3. Click the **Override** button to open the override account pop-up window.
4. 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.

Mozilla Firefox Pop-up Blocker

Add Override Account to the White List

1. From the browser, open the Preferences dialog box.
2. Go to the Category list box and select Privacy & Security > Popup Windows to display the Popup Windows page:

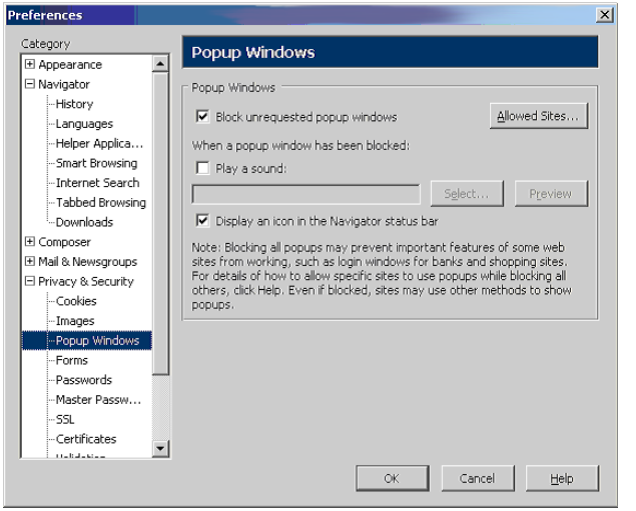


Fig. D-6 Mozilla Firefox Popup Windows Preferences

3. With the “Block unrequested popup windows” checkbox checked, click **Allowed Sites** and enter the URL to allow the override account window to pass.
4. Click **OK** to save your changes and to close the dialog box.

Windows XP SP2 Pop-up Blocker

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:

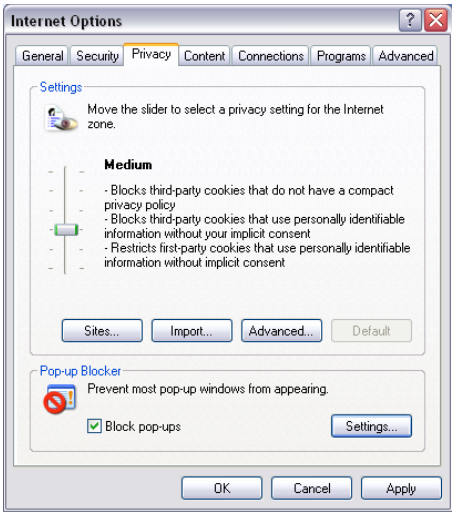


Fig. D-7 Enable pop-up blocking

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:

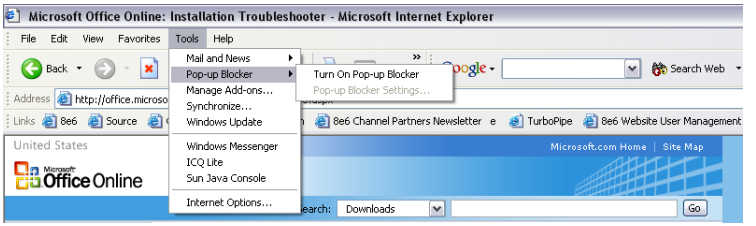


Fig. D-8 Toolbar setup

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.

Temporarily Disable Pop-up Blocking

1. In the Options page (see Fig. D-1), enter your **Username** and **Password**.
2. Press and hold the **Ctrl** key on your keyboard while simultaneously clicking the **Override** button—this action opens the override account pop-up window.

Add Override Account to the White List

There are two ways to disable pop-up blocking for the override account and to add the override account 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:

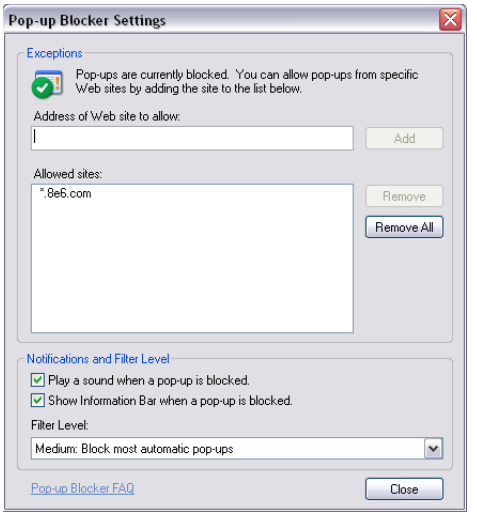


Fig. D-9 Pop-up Blocker Settings

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 override account window has now been added to your white list.
3. In the Options page (see Fig. D-1), enter your **Username** and **Password**.
4. Click the **Override** button to open the override account pop-up window.

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. D-9).
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 your Override Account

1. In the Options page (see Fig. D-1), enter your **Username** and **Password**.
2. Click the **Override** button. This action displays the following message in the Information Bar: “Pop-up blocked. To see this pop-up or additional options click here...”:

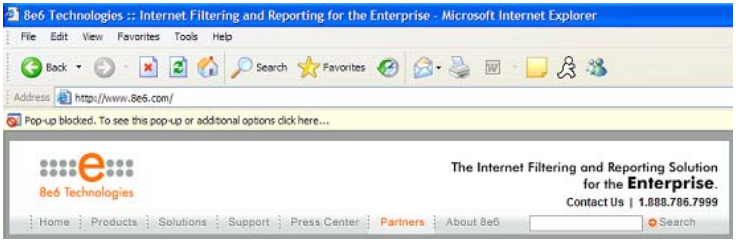


Fig. D-10 Information Bar showing blocked pop-up status

3. Click the Information Bar for settings options:

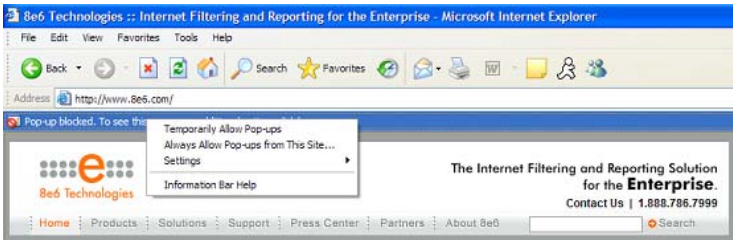


Fig. D-11 Information Bar menu options

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

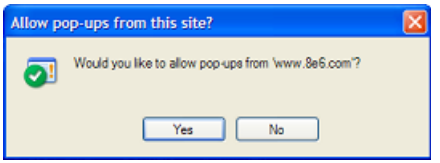


Fig. D-12 Allow pop-ups dialog box

5. Click **Yes** to add the override account 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. D-9) and see the entries in the Allowed sites list box.*

6. Go back to the Options page and click **Override** to open the override account window.

Appendix E

Configure ProxyBlocker for ER Reporting

When configuring the ProxyBlocker to be used with an ER unit, the following procedures must be completed in order for the ER to receive logs from the ProxyBlocker.

Entries in the ProxyBlocker Admin console

1. Choose Reporting > Report Configuration to display the Report Configuration window.
2. Click the “8e6 Enterprise Reporter” checkbox to display the 8e6 Enterprise Reporter tab:

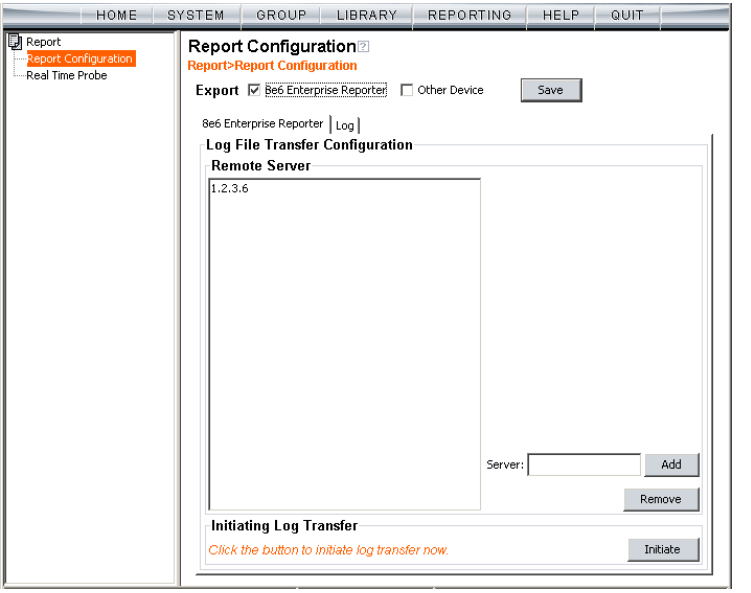


Fig. E-1 Report Configuration window, ER tab

3. In the Log File Transfer Configuration frame, enter the LAN 1 IP address assigned to the ER **Server**, and then

click **Add** to include this IP address in the Remote Server list box.

***NOTE**: To remove an IP address from the list box, select it and click Remove.*

4. After the ER has been configured, and logs have been transferred from the ProxyBlocker to the ER, click the Log tab to view transfer activity.

5. On the Log tab, click **View Log** to view up to the last 300 lines of transfer activity in the View Log frame.

***NOTE**: It is recommended you wait one to two hours after the initial configuration so sufficient data is available for viewing.*

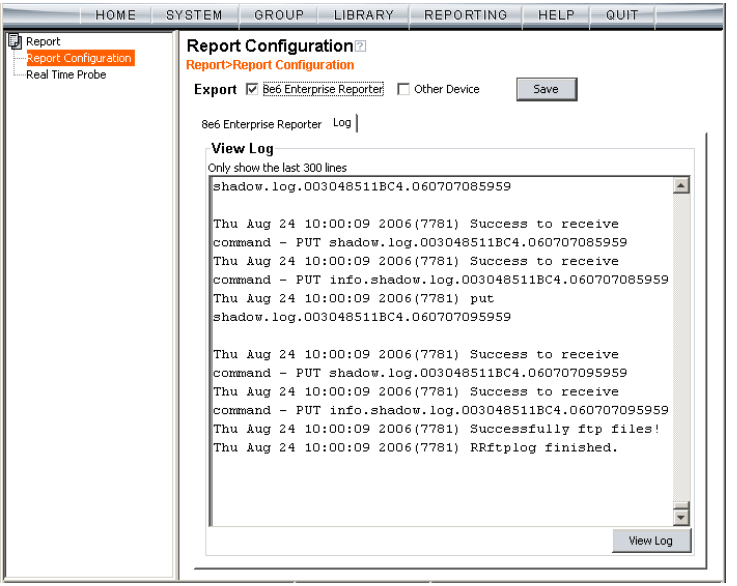


Fig. E-2 Report Configuration window, Log tab

Entries in the ER Administrator console

To see if log files have transferred:

1. Access the ER's Administrator console.
2. From the Database pull-down menu, choose Tools to display the Tools screen.
3. From the Database Status menu, choose File Watch Log.
4. Click **View** to open the File Watch Status pop-up box. If logs are being transferred, you will see an entry that includes the date, time, and IMPORTING: shadow.log.machine1. Once you see an entry, reporting information will be available one hour after the timestamp of the import listing.

***NOTE**: Transfers occur each hour.*

Appendix F

RAID Maintenance

This appendix pertains to ProxyBlocker “SL” 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 ProxyBlocker “SL” 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:

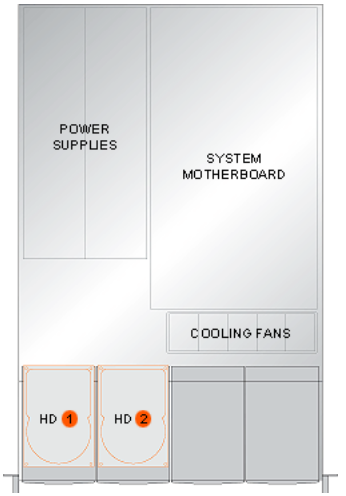
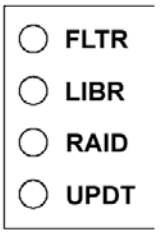


Fig. F-1 ProxyBlocker RAID Server components

Part 2: Server Interface

LED indicators in SL units

On an “SL” unit, the following LED indicators for software and hardware status monitoring display on the left side of the front panel:



- FLTR = Filtering Status
- LIBR = Library Update Status
- RAID = Hard Drive Status
- UPDT = Software Update Status

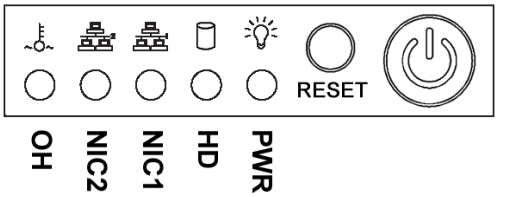
LED Indicator Chart

Below is a chart of LED indicators in the “SL” unit:

LED Indicator	Color	Condition	Description
FLTR	Green	On	Filtering traffic
	Amber	On	Library being uploaded or one or more processes being started
	Red	On	Not filtering traffic
LIBR	Green	On	Library updated within the past two days or less
	Amber	On	Library updated more than two days ago, but within the past three days
	Red	On	Library updated more than three days ago
RAID	Green	On	RAID mode enabled and running
	--	Off	RAID mode is inactive
	Red	On	Hard drive fault or failure
UPDT	Amber	On	Software update detected
	--	Off	No software update detected

Front control panels on SL 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:

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 an amber LED. 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.

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 Failure Detection 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 Failure Detection window in the Administrator console is accessible via the **System > Hardware Failure Detection** menu selection:

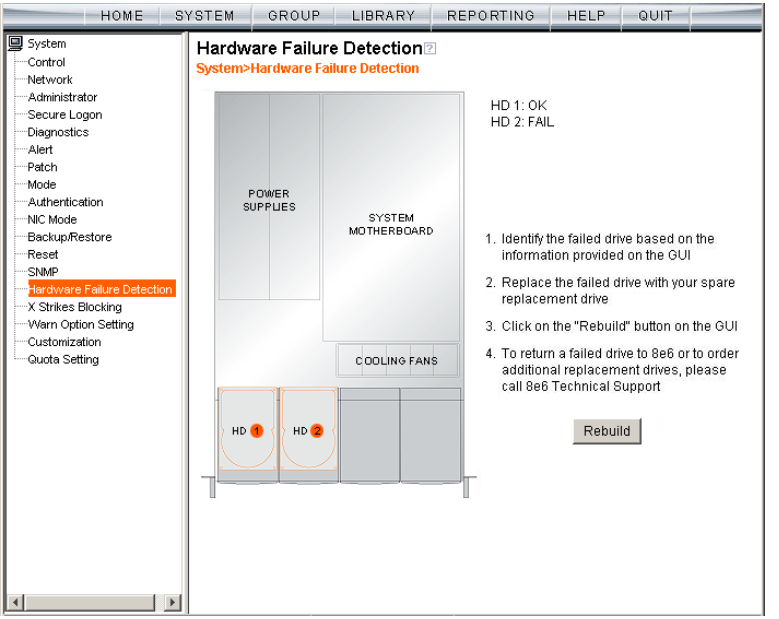


Fig. F-2 Hardware Failure Detection window

The Hardware Failure Detection window displays the current RAID Array Status for the two hard drives (HD 1 and HD 2) at the right side of the window.

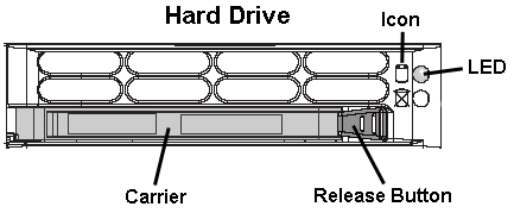
Normally, when both hard drives are functioning without failure, the text “OK” displays to the right of the hard drive number, and no other text displays in the window.

However, if a hard drive has failed, the message “FAIL” displays to the right of the hard drive number.

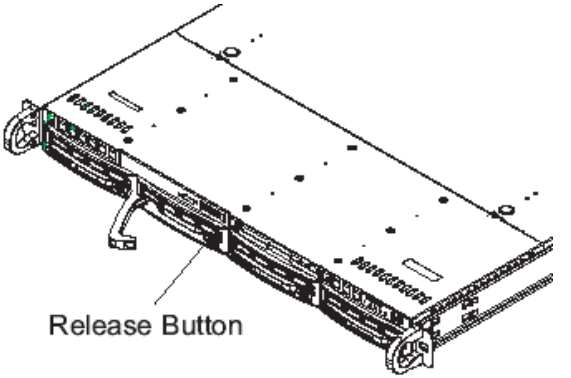
Before taking any action in this window, proceed to Step 3.

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

Once the failed hard drive has been replaced, return to the Hardware Failure Detection window in the Administrator console, and click **Rebuild** to proceed with the rebuild process.

***WARNING**: When the RAID array reconstruction process begins, the Administrator console will close and the hard drive will become inaccessible.*

Step 5: Contact Technical Support

Contact Technical Support to order a new replacement hard drive and for instructions on returning your failed hard drive to 8e6.

Power supply failure

Step 1: Identify the failed power supply

The administrator of the server is alerted to a power supply failure on the chassis by an audible alarm and an amber power supply LED—or an unlit LED—on the front and rear of the chassis.

***NOTE**: A steady amber power supply LED also may indicate a disconnected or loose power supply cord. Verify that the power supply cord is plugged in completely before removing a power supply.*

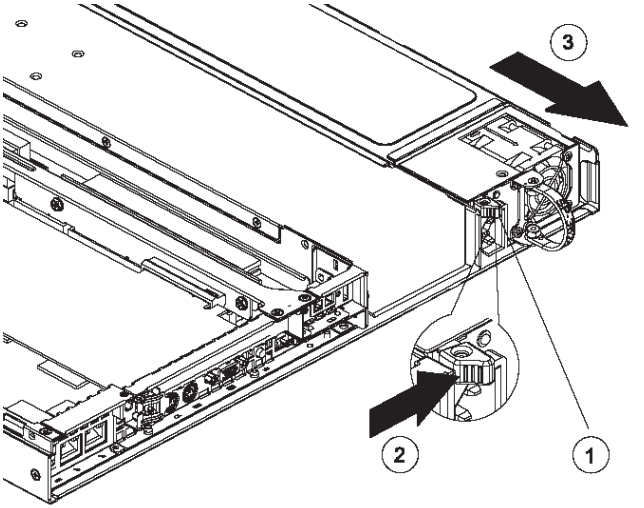
***WARNING**: Be sure the correct failed power supply has been identified. Removing the wrong power supply will cause the system to crash.*

Step 2: Unplug the power cord

To prevent electrical shock to yourself and damage to the unit, unplug the power cord from the failed power supply.

Step 3: Replace the failed power supply

Remove the failed power supply by locating the red release tab (1) and pushing it to the right (2), then lifting the curved metal handle and pulling the power supply module towards you (3).



Note that an audible alarm sounds and the LED is unlit when the power supply is disengaged. Replace the failed power supply with your spare replacement power supply. The alarm will turn off and the LED will be a steady green when the replacement power supply is securely locked in place.

Step 4: Contact Technical Support

Contact Technical Support to order a new replacement power supply and for instructions on returning your failed power supply to 8e6.

Fan failure

Identify a fan failure

A flashing red LED indicates a fan failure. If this displays on your unit, contact Technical Support for an RMA (Return Merchandise Authorization) number and for instructions on returning the unit to 8e6.

A steady red LED (on and not flashing) indicates an over-heating condition, which may be caused by cables obstructing the airflow in the system or the ambient room temperature being too warm. Check the routing of the cables and make sure all fans are present and operating normally. The LED will remain steady as long as the over-heating condition exists.

Appendix H

Glossary

This glossary includes definitions for terminology used in this user guide.

8e6 supplied category - A library category that was created by 8e6, and includes a list of URLs, URL keywords, and search engine keywords to be blocked.

always allowed - A filter category or port given this designation will be included in the white list.

block setting - A setting assigned to a service port or library category when creating a rule, or when setting up a filtering profile or the minimum filtering level. If an item is given a block setting, users will be denied access to it.

custom category - Includes the ALLOW and BLOCK library categories maintained by an administrator, and include URLs, URL keywords, and search engine keywords to be passed or blocked. Group administrators manage the ALLOW and BLOCK custom library categories for their own group.

filter setting - A setting made for a service port. A service port with a filter setting uses filter settings created for library categories (block, open, or always allow settings) to determine whether users should be denied or allowed access to that port.

global administrator - An authorized administrator of the network who maintains all aspects of the ProxyBlocker, except for managing master IP groups and their members, and their associated filtering profiles. The global administrator configures the ProxyBlocker, sets up master IP groups, and performs routine maintenance on the server.

group administrator - An authorized administrator of the network who maintains a master IP group, setting up and managing members within that group. This administrator also adds and maintains customized library categories for the group.

group name - The name of a group set up for a domain on an NT server. For example: “production” or “sales”.

individual IP member - An entity of a master IP group with a single IP address.

instant messaging - IM involves direct connections between workstations either locally or across the Internet. Using this feature of the ProxyBlocker, groups and/or individual client machines can be set up to block the use of IM services specified in the library category.

invisible mode - The ProxyBlocker uses the invisible mode to filter all connections on the Ethernet between client PCs and the Internet, without stopping each IP packet on the same Ethernet segment. The unit will only intercept a session if an inappropriate request was submitted by a client.

keyword - A word or term used for accessing Internet content. A keyword can be part of a URL address or it can be a search term. An example of a URL keyword is the word “essex” in http://www.essex.com. An example of a search engine keyword is the entry “essex”.

library category - A list of URLs, URL keywords, and search engine keywords set up to be blocked.

LDAP - One of two authentication method protocols used by the ProxyBlocker. Lightweight Directory Access Protocol (LDAP) is a directory service protocol based on entries (Distinguished Names).

machine name - Pertains to the name of the user’s workstation machine (computer).

master IP group - An IP group set up in the tree menu in the Group section of the console, comprised of sub-groups and/or individual IP filtering profiles.

master list - A list of additional URLs that is uploaded to a custom category's URLs window.

minimum filtering level - A set of library categories and service ports defined at the global level to be blocked or opened. If the minimum filtering level is established, it is applied in conjunction with a user's filtering profile. If a user does not belong to a group, or the user's group does not have a filtering profile, the default (global) filtering profile is used, and the minimum filtering level does not apply to that user.

name resolution - A process that occurs when the ProxyBlocker attempts to resolve the IP address of the authentication server with the machine name of that server. This continuous and regulated automated procedure ensures the connection between the two servers is maintained.

net use - A command that is used for connecting a computer to—or disconnecting a computer from—a shared resource, or displaying information about computer connections. The command also controls persistent net connections.

NetBIOS - Network Basic Input Output System is an application programming interface (API) that augments the DOS BIOS by adding special functions to local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. NetBIOS relies on a message format called Server Message Block (SMB).

Network Address Translation (NAT) - Allows a single real IP address to be used by multiple PCs or servers. This is accomplished via a creative translation of inside "fake" IP addresses into outside real IP addresses.

open setting - A setting assigned to a service port or library category when creating a rule, or when setting up a filtering profile or the minimum filtering level. If an item is given an open (pass) setting, users will have access to it.

override account - An account created by the global group administrator or the group administrator to give an authorized user the ability to access Internet content blocked at the global level or the group level.

PDC - A Primary Domain Controller functions as the authentication server on a Windows NT domain. This server maintains the master copy of the directory database used for validating users.

peer-to-peer - P2P involves communication between computing devices—desktops, servers, and other smart devices—that are linked directly to each other. Using this feature of the ProxyBlocker, groups and/or individual client machines can be set up to block the use of P2P services specified in the library category.

profile string - The string of characters that define a filtering profile. A profile string can consist of the following components: category codes, service port numbers, and redirect URL.

protocol - A type of format for transmitting data between two devices. LDAP and SMB are types of authentication method protocols.

proxy server - An appliance or software that accesses the Internet for the user's client PC. When a client PC submits a request for a Web page, the proxy server accesses the page from the Internet and sends it to the client. A proxy server may be used for security reasons or in conjunciton with caching for bandwidth and performance reasons.

quota - The number of minutes configured for a passed library category in an end user's profile that lets him/her

access URLs for a specified time before being blocked from further access to that category

Real Time Probe - On the ProxyBlocker, 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.

rule - A filtering component comprised of library categories set up to be blocked, opened, or always allowed. Each rule created by the global administrator is assigned a number and a name that should be indicative of its theme. Rules are used when creating filtering profiles for entities on the network.

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.

service port - Service ports can be set up to blocked. Examples of these ports include File Transfer Protocol (FTP), Hyper Text Transfer Protocol (HTTP), Network News Transfer Protocol (NNTP), Secured HTTP Transmission (HTTPS), and Other ports such as Secure Shell (SSH).

SMTP - Simple Mail Transfer Protocol is used for transferring email messages between servers.

SNMP - For the ProxyBlocker, a Simple Network Management Protocol is a third party product used for monitoring and managing the working status of the ProxyBlocker's filtering on a network.

sub-group - An entity of a master IP group with an associated member IP address, and filtering profile.

time profile - A customized filtering profile set up to be effective at a specified time period for designated users.

Traveler - 8e6's executable program that downloads updates to your ProxyBlocker on demand or at a scheduled time.

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").

virtual IP address - The IP address used for communicating with all users who log on the network.

VLAN - Virtual Local Area Network is a network of computers that may be located on different segments of a LAN but communicate as if they were on the same physical LAN segment.

warn setting - A setting assigned to a library category or uncategorized URLs when creating a rule, or when setting up a filtering profile. This designation indicates URLs in the library category or uncategorized URLs may potentially be in opposition to the organization's policies, and are flagged with a warning message that displays for the end user if a URL from that library category or an uncategorized URL is requested.

white list - A list of approved library categories for a specified entity's filtering profile.

INDEX

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X