M86 Web Filtering and Reporting Suite

USER GUIDE

Software Version: 3.0.00
Document Version: 02.28.11

M86 Security Web Filtering and Reporting Suite User Guide

828 W. Taft Ave., Orange, CA 92865, USA

Version 1.01, published February 2011 for software release 3.0.00

Printed in the United States of America

Every effort has been made to ensure the accuracy of this document. However, M86 Security makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. M86 Security 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.m86security.com/support/wfr/documentation.asp

Trademarks

Part# WFR-UG_v1.01-1102

CONTENTS

WF GLOBAL ADMINISTRATOR SECTION 77

WFR Suite Overview

The M86 Security Web Filtering and Reporting Suite (WFR) consists of the M86 Web Filter and M86 Security Reporter, consolidated into one unit.

M86 Web Filter offers an enhanced solution for Internet filtering on a network. The Web Filter tracks each user's online activity, 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.

Data from the Web Filter is fed into the Security Reporter (SR), giving you the ability to interrogate massive datasets through flexible drill-down technology, until the desired view is obtained. This "view" can then be memorized and saved to a user-defined report menu for repetitive, scheduled execution and distribution. The SR also provides real time graphical snapshots of network Internet traffic, supported by remediation tools to manage and control user-generated Web threats. Simply by drilling down into the easy-to-read dashboard of gauges, you can target and halt the source of the threat.

Using the WFR Suite, threats to your network are quickly identified, thus arming you with the capability to take immediate action to secure your network.

***NOTE**: The SR application can be configured to accept logs from a M86 Secure Web Gateway (SWG) and generate security reports. See the M86 Secure Web Gateway User Guide at **http://www.m86security.com/support/Secure-Web-Gateway/Documentation.asp** for information on the SWG.*

How to Use this User Guide

Organization

This User Guide is organized into the following portions:

- **WFR Suite Overview** - This portion introduces the WFR product and explains how to use the WFR console and this user guide, and provides information on how to contact M86 Security technical support.
- **Web Filter (WF)** - Refer to this portion for information on configuring and maintaining the Web Filter application.
- **Security Reporter (SR)** - Refer to this portion for information on configuring and using the SR application to generate reports.
- **WFR Appendices** - Appendix I explains how to disable pop-up blocking software. Appendix II provides information on how to perform hardware maintenance and troubleshoot RAID on the 300 series and 500 series WFR chassis.
- **Index** - The index lists subjects and the first page numbers where they appear in 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 topic.*

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.*

IMPORTANT*: The "important" icon is followed by italicized text informing you about important information or procedures to follow to ensure maximum uptime on the WFR Server.*

Components and Environment

Components

Hardware

- High performance server equipped with RAID
- Two or four high-capacity hard drives
- Optional: One or more attached “NAS” storage devices (e.g. Ethernet connected, SCSI/Fibre Channel connected “SAN”)

Software

- Linux OS
- Administrator User Interface (UI) console utilized by an authorized administrator to configure and maintain the WFR server
- MySQL database

Environment

Network Requirements

- Power connection protected by an Uninterruptible Power Supply (UPS)
- HTTPS connection to M86 Security's software update server
- SR must be be fully configured, and the Structured Query Language (SQL) server must be installed on the network and connected to the Web access logging device(s) (e.g. Web Filter(s) and Secure Web Gateway—the latter device, if an SWG will be used with the SR)
- High speed access to the WFR server by authorized client workstations
- Internet connectivity for downloading Java virtual machine, if not already installed
- Port 1443 must be available for the Web Filter user interface to use, and ports 8443 and 8843 must be available for the SR user interface to use

***NOTE**: Administrators must be set up with software installation privileges in order to install Java used for accessing the Web Filter user interface.*

Administrator Workstation Requirements

System requirements for the administrator include the following:

- Windows XP, Vista, or 7 operating system running:
  - Internet Explorer (IE) 7.0 or 8.0
  - Firefox 3.6
- Macintosh OS X Version 10.5 or 10.6 running:

  - Safari 4.0
  - Firefox 3.6
- JavaScript enabled
- Java Virtual Machine
- Java Plug-in (minimum version 1.6.0_17, maximum version 1.6.0_21)

***NOTE**: Java 1.6.0_22 and later are incompatible with this software release.*

***TIP**: See **http://www.m86security.com/software/8e6/hlp/ifr/files/5help_java.html** for information about identifying the version of Java on your machine and downloading the latest version.*

- Pop-up blocking software, if installed, must be disabled
- Session cookies from the WFR server must be allowed in order for the Administrator consoles to function properly

***NOTES**: Information about disabling pop-up blocking software can be found in WFR Appendix I: Disable Pop-up Blocking Software.*

End User Workstation Requirements

System requirements for the end user include the following:

- Windows XP, Vista, or 7 operating system running:
  - Internet Explorer (IE) 7.0 or 8.0
  - Firefox 3.6
- Macintosh OS X Version 10.5 or 10.6 running:
  - Safari 4.0
  - Firefox 3.6
- JavaScript enabled
- Pop-up blocking software, if installed, must be disabled

How to Use the WFR on the Web

Initial Setup

To initially set up your M86 Web Filter and Reporter (WFR) server, the administrator installing the unit should follow the instructions in the M86 WFR Installation Guide, the booklet packaged with your WFR unit. This guide explains how to perform the initial configuration of the server so that it can be accessed via an IP address or host name on your network.

***NOTE**: If you do not have the M86 WFR Installation Guide, contact M86 Security immediately to have a copy sent to you.*

⚠ ***WARNING**: In order to prevent data from being lost or corrupted while the WFR server is running, the server should be connected to a UPS or other battery backup system. Once you turn on the WFR server, **DO NOT** interrupt the initial boot-up process. This process may take from five to 10 minutes per drive. If the process is interrupted, damage to key files may occur.*

Access the WFR Welcome Window

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

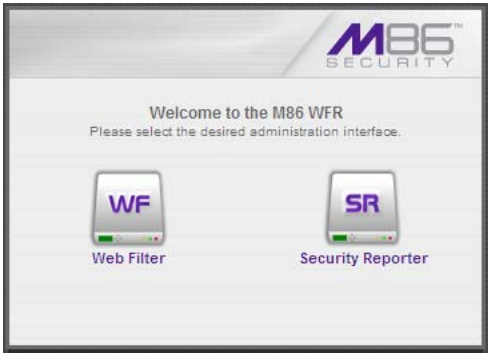
1. Launch an Internet browser window supported by the WFR.

2. In the address line of the browser window, type in “https://” and the WFR server’s IP address or host name, and use port number “:1443” for a secure network connection.

   For example, if your IP address is 210.10.131.34, type in **https://210.10.131.34:1443**. Using a host name example, if the host name is logo.com, type in **https://logo.com:1443**.

With a secure connection, the first time you attempt to access the WFR's user interface in your browser you will be prompted to accept the security certificate. In order to accept the security certificate for your browser, follow the instructions at: ***http://www.m86security.com/software/8e6/docs/ig/misc/sec-cert-wfr3.0.pdf***

3. Click **Go** to open the Welcome window of the WFR user interface:



Welcome to the M86 WFR

Please select the desired administration interface.

Fig. 1:1-1 WFR Welcome window

Using this portal you can click the icon corresponding to Web Filter or Security Reporter to access the user interface of that application, as described in the following sections of this user guide.

However, by logging into the SR Report Manager as the global administrator—as described on the next page—you will have access to the Web Filter, SR Report Manager and SR System Configuration administrator console on the WFR server, without needing to use this WFR Welcome portal to individually log into the two main applications.

Single Sign-On Access

Access all applications from the SR UI

Single Sign-On (SSO) access eliminates the process of choosing either the Web Filter or SR application from the WFR Welcome window, and then logging in to each application separately.

To enable SSO, be sure the same username and password combination set up in the wizard hardware installation process is saved in the Web Filter (System > Administrator—'Admin' account type profile). Also be sure the host name for the WFR is entered in the hosts file.

To use the single sign-on option:

1. Log in to SR using the Wizard username and password.
2. Go to the navigation links at the top of the Report Manager panel and select:
   - **Administration > System Configuration** to access the SR administrator console
   - **Administration > Web Filter > (IP address)** to access the Web Filter user interface

Default Usernames and Passwords

Without setting up single sign-on access for the global administrator account, default usernames and passwords for WFR applications are as follows:

Application	Username	Password
Web Filter	admin	user3
Security Reporter	admin	testpass

Note that since the default username for both the Web Filter and Security Reporter are identical (*admin*), but the passwords are dissimilar, the SSO feature will not function. Thus, in order to use SSO, M86 recommends setting up an administrator account in the Web Filter that matches the global administrator account set up in the SR (Administration > Admin Profiles).

Technical Support / Product Warranties

For technical assistance or warranty repair, please visit **http://www.m86security.com/support/** .

WEB FILTER INTRODUCTORY SECTION

Web Filter

M86 Security's Web Filter tracks each user's online activity, and can be configured to block specific Web sites, service ports, and pattern and file types, and lock out an end user from Internet access, thereby protecting your organization against lost productivity, network bandwidth issues, and possible legal problems that can result from the misuse of Internet resources.

The Web Filter provides an extensive library filtering category database, user authentication, implementation of time and quota filtering profiles, and tools for tailoring a user's filtering profile to comply with your organization's Internet usage policy, based on the end user's Internet usage habits.

About this Portion of the User Guide

The Web Filter portion of the user guide primarily addresses the network administrator designated to configure and manage the server on the network. This administrator is referred to as the "global administrator" throughout this portion of the user guide. In part, this portion of the user guide also addresses administrators who manage user groups on the network. These administrators are referred to as "group administrators" throughout this portion of the user guide.

See the M86 Web Filter Authentication User Guide at http://www.m86security.com/support/wf/documentation.asp for information on authentication.

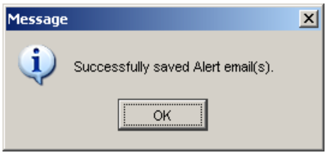
This portion of the user guide is organized into the following sections:

- **Web Filter Introductory Section** - This section is comprised of an overview on filtering, Web access logging, instant messaging and peer-to-peer blocking, and synchronizing multiple Web Filter units. This section also provides information on how to use this portion of the user guide to help you configure the Web Filter.
- **WF Global Administrator Section** - This section includes information for the global administrator—who has all rights and permissions on the Web Filter—to create group administrator accounts, and to configure the Web Filter for filtering the entire network.
- **WF 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 Web Filter. Group administrators also have rights to access certain library category functions.
- **Web Filter Appendices Section** - Appendix A includes formats and rules used in the filtering profile file. Appendix B includes information on creating a customized block page. Appendix C provides tips on how to override pop-up windows with pop-up blocker software installed. Appendix D explains how to install, configure, and use the Mobile Client. Appendix E features a glossary of technical terminology used in this portion of the user guide.

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.


Message

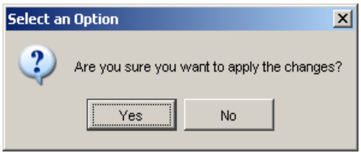
Successfully saved Alert email(s).

- **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.

☑ Profile

- **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.

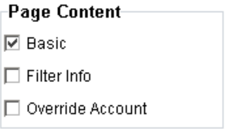

Select an Option

Are you sure you want to apply the changes?

- **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.

Short Name CHAT

- **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.



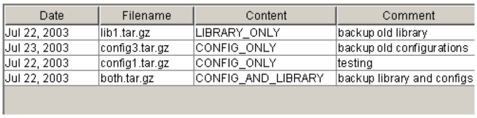
Page Content

☑ Basic

□ Filter Info

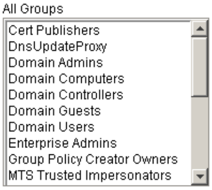
□ Override Account

- **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

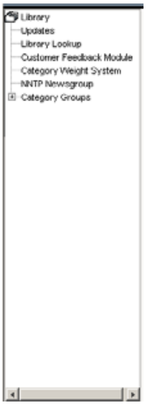
- **list box** - an area in a dialog box, window, or screen that accommodates and/or displays entries of items that can be added or removed.



All Groups

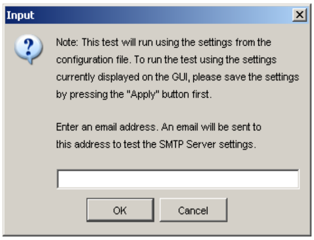
Cert Publishers
DnsUpdateProxy
Domain Admins
Domain Computers
Domain Controllers
Domain Guests
Domain Users
Enterprise Admins
Group Policy Creator Owners
MTS Trusted Impersonators

- **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.



Library
Updates
Library Lookup
Customer Feedback Module
Category Weight System
NNTP Newsgroup
⊞ Category Groups

- **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.



Note: This test will run using the settings from the configuration file. To run the test using the settings currently displayed on the GUI, please save the settings by pressing the "Apply" button first.

Enter an email address. An email will be sent to this address to test the SMTP Server settings.

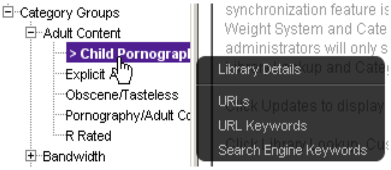
- **pull-down menu** - a field in a dialog box, window, or screen that contains a down-arrow to the right. When you click the arrow, a menu of items displays from which you make a selection.

- **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.

● On ○ Off

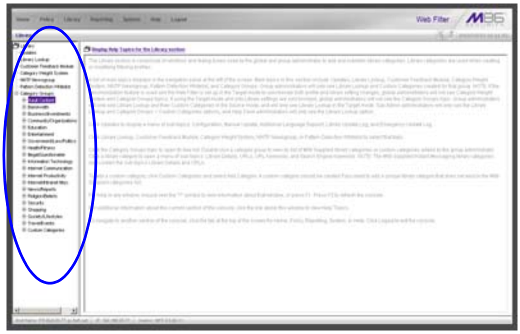
- **screen** - a main object of an application that displays across your monitor. A screen can contain panels, windows, frames, fields, tables, text boxes, list boxes, icons, buttons, and radio buttons.

- **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.

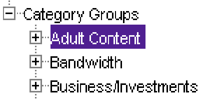


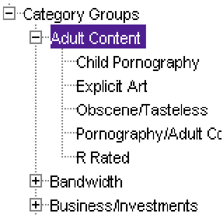
- **text box** - an area in a dialog box, window, or screen that accommodates your data entry. A text box is a type of field. (See “field”.)

- **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.

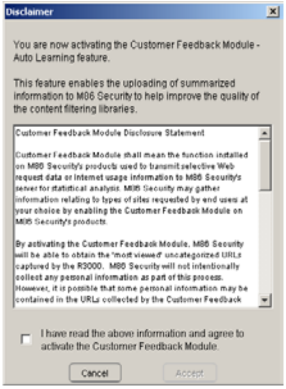


- **tree** - a tree displays in the navigation panel of a screen, and is comprised of a hierarchical list of items. An entity associated with a branch of the tree is preceded by a plus (+) sign when the branch is collapsed. By double-clicking the item, a minus (-) sign replaces the plus sign, and any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


Disclaimer

You are now activating the Customer Feedback Module - Auto Learning feature.

This feature enables the uploading of summarized information to M86 Security to help improve the quality of the content filtering libraries.

Customer Feedback Module Disclosure Statement

Customer Feedback Module shall mean the function installed on M86 Security's products used to transmit selective Web request data or Internet usage information to M86 Security's server for statistical analysis. M86 Security may gather information relating to types of sites requested by end users at your choice by enabling the Customer Feedback Module on M86 Security's products.

By activating the Customer Feedback Module, M86 Security will be able to obtain the "most viewed" uncategorized URLs captured by the R3000. M86 Security will not intentionally collect any personal information as part of this process. However, it is possible that some personal information may be contained in the URLs collected by the Customer Feedback

□ I have read the above information and agree to activate the Customer Feedback Module.

Overview

The Web Filter's Administrator console is used by the global administrator—and group administrator, as required—to configure the Web Filter 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 M86 Web Filter Authentication User Guide at **http://www.m86security.com/support/wf/documentation.asp** for information on setting up and using authentication.*

- synchronize multiple Web Filter units so that all servers will be updated with the same user profile and library configurations

To help you become familiar with the Web Filter 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 features information on synchronizing multiple Web Filter units. Chapter 4 includes details on getting started, with log in and log out procedures, and tips on navigating the Administrator console.

Chapter 1: Filtering Operations

Operational Modes

Based on the setup of your network, the Web Filter can be configured to use one of these operational modes for filtering the network:

- invisible mode
- router mode
- firewall mode

Invisible Mode

If the Web Filter is set up in the invisible mode, 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 Web Filter 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 Web Filter from any inclusion in the network connection path.

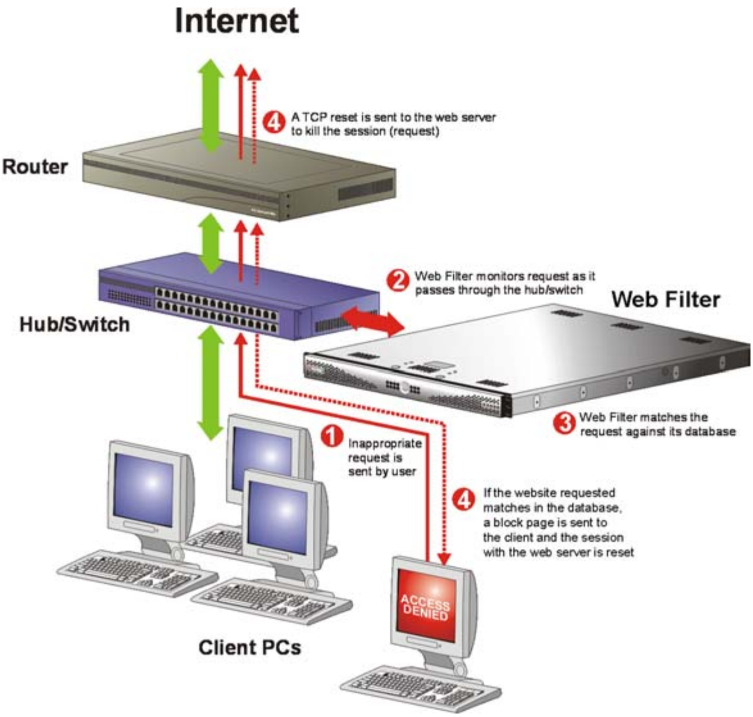

Internet
4 A TCP reset is sent to the web server to kill the session (request)
Router
2 Web Filter monitors request as it passes through the hub/switch
Web Filter
Hub/Switch
3 Web Filter matches the request against its database
1 Inappropriate request is sent by user
4 If the website requested matches in the database, a block page is sent to the client and the session with the web server is reset
ACCESS DENIED
Client PCs

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 Web Filter captures the request as the user's request (2) leaves the network. The Web Filter then determines the action (3) to either block or pass the request. If the Web Filter 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.

A Web Filter set up in the invisible mode can also work in the router mode. Figure 1:1-2 illustrates an example of a monitor mode setup, with the Web Filter connected to the managed switching hub. In this setup, the Web Filter port is configured with the port monitoring function enabled, so that the Web Filter's port mirrors the port connected to the router.

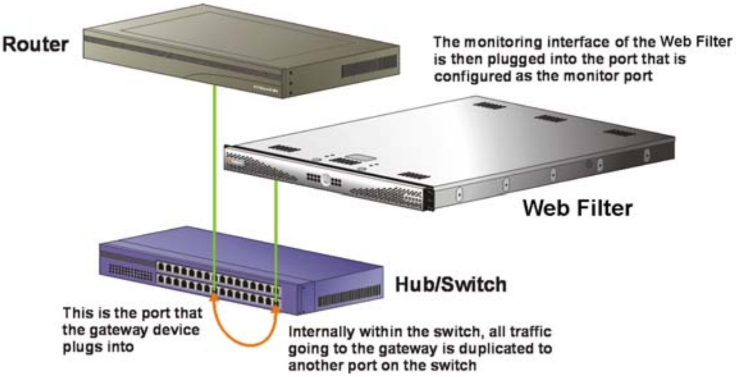

Router
The monitoring interface of the Web Filter is then plugged into the port that is configured as the monitor port
Web Filter
Hub/Switch
This is the port that the gateway device plugs into
Internally within the switch, all traffic going to the gateway is duplicated to another port on the switch

Fig. 1:1-2 Invisible mode diagram, with port monitoring

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

Router Mode

If the Web Filter is set up in the router mode, the unit will act as an Ethernet router, filtering IP packets as they pass from one card to another. While all original packets from client PCs are allowed to pass, if the Web Filter determines that a request is inappropriate, a block page is returned to the client to replace the actual requested Web page or service.

Since only outgoing packets need to be routed—and not return packets—the Web Filter only appears in the outgoing path of the network.

Figure 1:1-3 illustrates an example of the router mode setup, in which the Web Filter is set up to act as the Internet router.

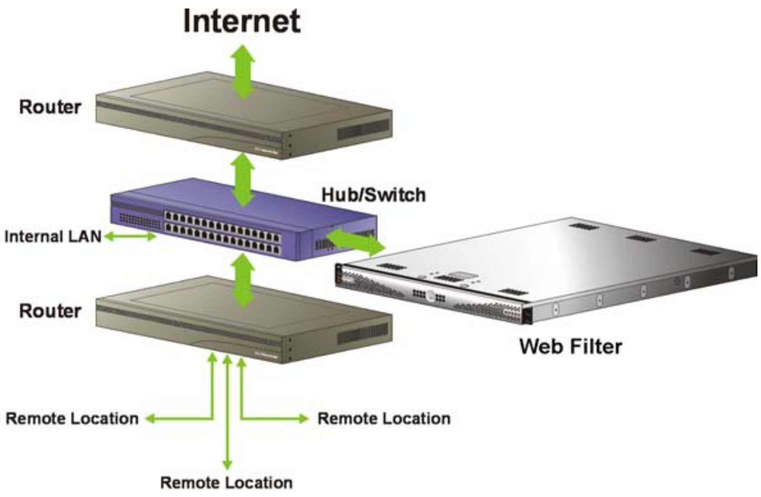


Fig. 1:1-3 Router mode diagram

As previously mentioned, a Web Filter set up in the router mode can also work in the invisible mode. The router mode setup also will work in the firewall mode.

WARNING: *M86 recommends contacting one of our solutions engineers if you need assistance with router mode setup procedures.*

Firewall Mode

The firewall mode is a modification of the router mode. With the Web Filter set up in this mode, the unit will filter all requests. If the request is appropriate, the original packet will pass unchanged. If the request is inappropriate, the original packet will be blocked from being routed through.

Using the firewall mode, while the outgoing request is delayed slightly—to allow filtering to take place before the packet leaves the gateway router of the network—return traffic remains unaffected.

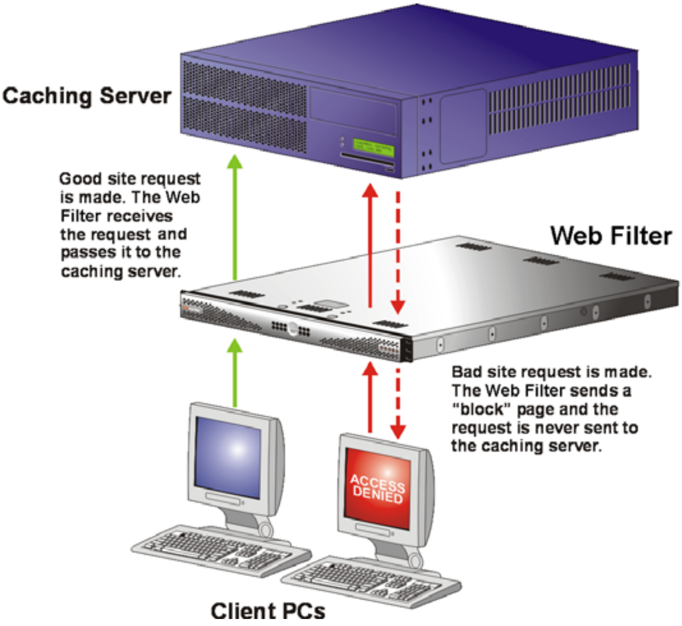

Caching Server
Good site request is made. The Web Filter receives the request and passes it to the caching server.
Web Filter
Bad site request is made. The Web Filter sends a "block" page and the request is never sent to the caching server.
ACCESS DENIED
Client PCs

Fig. 1:1-4 Firewall mode diagram, with firewall and cache setup

The firewall mode cannot be used with any other mode (invisible or router).

Figure 1:1-4 illustrates an example of a firewall mode setup in which requests are never sent to the caching server. In this scenario the local caching proxy will not affect the Web Filter—even if the server contains unfiltered, “bad” cached pages—since no request can pass until it is filtered.

Figure 1:1-5 illustrates an example of a firewall mode setup in which requests are always sent to the caching server. In this scenario the Web Filter *will* be affected if the caching proxy server contains unfiltered, “bad” cached pages. M86 recommends that cached content is cleared or expired after installing the Web Filter.

⚠ ***WARNING**: Contact a solutions engineer at M86 Security for setup procedures if you wish to use the firewall mode.*

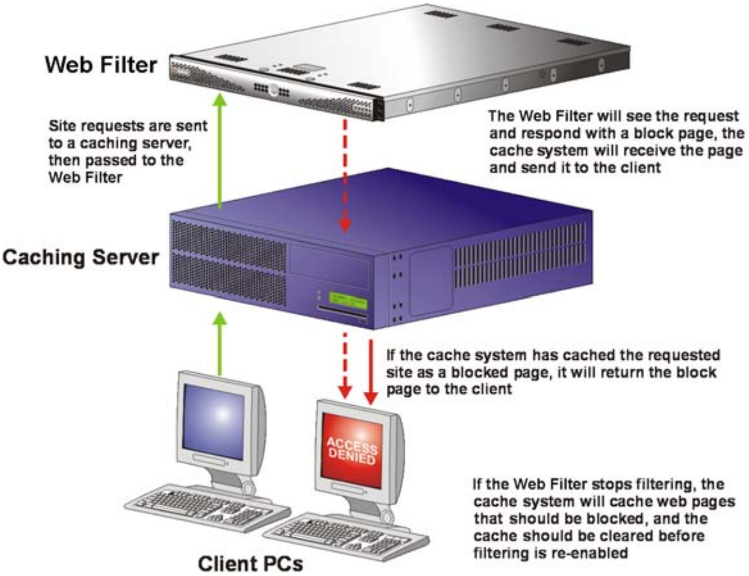

Web Filter
Site requests are sent to a caching server, then passed to the Web Filter
The Web Filter will see the request and respond with a block page, the cache system will receive the page and send it to the client
Caching Server
If the cache system has cached the requested site as a blocked page, it will return the block page to the client
ACCESS DENIED
If the Web Filter stops filtering, the cache system will cache web pages that should be blocked, and the cache should be cleared before filtering is re-enabled
Client PCs

Fig. 1:1-5 Firewall mode diagram, with filtering and cache setup

Group Types

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

In the Policy 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.

***NOTES**: If authentication is enabled, the global administrator can also access the LDAP branch of the tree.*

If multiple Web Filter units are set up on the network and the synchronization feature is used, a Web Filter that is set up to receive profile changes will only display the Global Group type in the tree list. (See Chapter 3: Synchronizing Multiple Units for more information on synchronization.)

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.

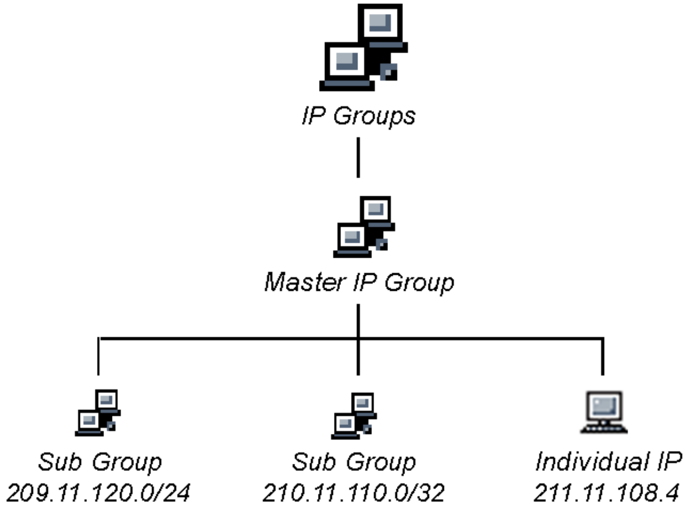


Fig. 1:1-6 IP diagram with a sample master IP group and its members

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 setup in the tree menu of the Policy 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 LDAP group members. This type of profile includes the workstation profile.

NOTE*: For information about authentication filtering profiles, see the M86 Web Filter Authentication User Guide.*

- **override account profile -** set up in either the Global Group section or the master IP group section of the console.
- **lock profile** - set up under X Strikes Blocking in the Filter Options section of the profile.
- **Radius profile** - used by end users on a Radius accounting server if the Radius server is connected to the Web Filter and the Radius authentication feature enabled.
- **TAR profile -** used by the Threat Analysis Reporter (TAR) module if an end user is locked out by TAR when attempting to access blocked content in a library category.

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 M86 Web Filter 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/Bing/Yahoo!/Ask/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.

M86 Supplied Categories

M86 furnishes a collection of library categories, grouped under the heading “Category Groups” (excluding the “Custom Categories” group). Updates to these categories are provided by M86 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 M86 supplied categories, additions and deletions can be made within a custom category. However, unlike M86 supplied categories, a custom category can be deleted.

***NOTE**: M86 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 Web Filter), 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

***NOTE**: A category that is allowed will override any blocked settings except if the minimum filtering level is set to block that category.*

- **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 (LDAP) profile—this includes a work-station profile—takes precedence over an individual IP member's time profile.

***NOTE**: A Radius profile is another type of authentication profile and is weighted the same as LDAP authentication profiles in the precedence hierarchy.*

7. A Threat Analysis Reporter (TAR) profile is a type of lockout profile used by the TAR module in the SR application. The TAR low level lockout profile takes precedence over an authentication profile or a time profile profile, locking out the end user from library categories specified in the lockout profile in the TAR module.

8. An override account profile takes precedence over a TAR lockout 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.*

9. An X Strikes lockout profile takes precedence over all filtering profiles. This profile is set up under Filter Options, by enabling the X Strikes Blocking feature.

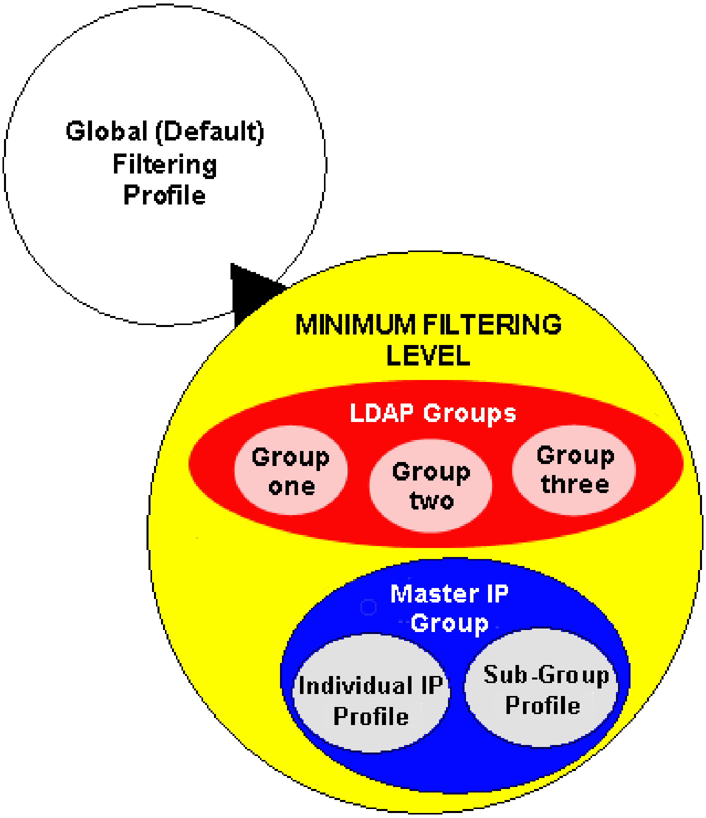


Fig. 1:1-7 Sample filtering hierarchy diagram

Chapter 2: Logging and Blocking

Web Access Logging

One of the primary functions of the Web Filter 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.

Log files from the Web Filter are transferred to the SR where they are "normalized" and then inserted into a MySQL database. The SR Report Manager accesses that database to generate queries and reports.

Instant Messaging, Peer-to-Peer Blocking

The Web Filter 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 Web Filter, 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 Web Filter compares packets on the network with IM libraries stored on the Web Filter. If a match is found, the Web Filter 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 Web Filter.*
- *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 Web Filter, 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 Web Filter compares packets on the network with the P2P library stored on the Web Filter. If a match is found, the Web Filter 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.m86security.com/software/8e6/hlp/ifr/files/1system_im_block.html**.

NOTE*: Please contact an M86 technical support representative or a solutions engineer if access is needed to one or more P2P services blocked by M86's supplied library category for P2P.*

3. In the Manual Update to M86 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 Policy section of the Administrator console.

If applying M86’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: Synchronizing Multiple Units

Web Filter Synchronization

The Web Filter can function in one of three modes—“Stand Alone” mode, “Source” mode, or “Target” mode—based on the setup within your organization. In a multi-Web Filter environment, all Web Filters should be set up with the same user profile data, so that no matter which Web Filter a user’s PC accesses on the network, that user’s Internet usage is appropriately filtered and blocked. The act of configuring multiple Web Filters to share the same user profile information is known as synchronization.

The synchronization feature allows an administrator to control multiple Web Filters without the need to configure each one independently. Web Filter synchronization uses a source/target configuration, in which one Web Filter is designated as the source server on which all configuration entries are made. All other Web Filters on the network are configured as target servers to the source Web Filter unit, receiving updates from the source server.

FUNCTIONAL MODES

Stand Alone Mode

In the Stand Alone mode, the Web Filter functions as the only Internet filter on the network. This mode is used if there is only one Web Filter on the network. Synchronization does not occur in this mode.

Source Mode

The Source mode is used in synchronization. In this mode the Web Filter is configured to not only function as a content filter, but also to act as a Centralized Management Console for all other Web Filters on the network. Whenever a filtering configuration change is made on the source Web Filter, that change is sent to all target Web Filters that have been identified by the source unit via the Synchronization Setup window of the Web Filter console. This means that all filtering configuration should be made on the source Web Filter. This also means that any user-level filter authentication should be performed on the source Web Filter so that these filtering changes can be disseminated to all Web Filter target units.

***NOTE**: If the failover detection synchronization feature is enabled, if a target server fails, the source server can be set up to detect the failed server and perform filtering for that server.*

Target Mode

As in the Source mode, the Target mode is used in synchronization. In this mode, filtering information from the source server will be uploaded to the target server. The only synchronization setup that needs to be made on the target server is to ensure that network interfaces are configured for network communication.

Synchronization Setup

To set up synchronization on a Web Filter, a selection must be made in Setup window from the System section of the Web Filter console to specify whether the Web Filter will function as a source server or as a target server. This selection affects the contents that display in the Setup window.

***NOTE**: This version of synchronization only supports the use of unique IP addresses throughout a network.*

Setting up a Source Server

When setting up an Web Filter to function as a source server, an IP address must be entered for each target Web Filter unit. This entry identifies the location of each target unit on the network.

***NOTE**: If synchronizing from a WFR to a standalone Web Filter server, please consult the chart at **http://www.m86security.com/software/8e6/hlp/ifr/files/1system_sync_versions.html** for software version compatibility between the two products.*

***WARNING**: If an Web Filter is set up in the Source mode with a Network Address Translation (NAT) device between the source and target server(s), be sure that ports 26262, 26268, and 88 are open on the source server. This setup is required so that the source server can communicate with the target server(s).*

Setting up a Target Server

When setting up a Web Filter to function as a target server, the IP address of the source server must be entered to identify the source server on the network. This IP address is used for security purposes, as the target server will only acknowledge and apply changes it receives from the designated source server. Additionally, this IP address is used by the target server to identify the source server from which it should receive its running filter configuration in the event of a reboot.

WARNING*: If a Web Filter server is set up in the Target mode with a NAT device between the target and source server, be sure that ports 26262 and 26268 are open on the target server. This setup is required so that the target server can communicate with the source server.*

Types of Synchronization Processes

Synchronization involves two types of processes: filtering profile synchronization, and library synchronization.

Filtering Profile Synchronization Process

In the filtering profile synchronization process, if a filtering change is made on the source server—whether the update is a global, IP, LDAP, minimum filtering bypass activation, or user profile update—the change is applied locally. Once locally applied on the source server, this update is sent to all target Web Filters. Each target server will then immediately apply this filtering change. The result is that profile updates occur on all Web Filter units in near real time.

In the event that a target server is unable to communicate with the source server, the target server will continue to run the last known configuration it received from the source server. The only exception to this scenario is that active profiles—such as LDAP or override accounts—will not run on the target server, since active profiles are timed out after a specified period of time. However, all IP based filters—such as the minimum filtering level, and the global rule that was last received from the source server—will be applied. When the target server resumes communication with the source server, it will actively download and apply the latest running configuration from the source server.

If the target server is rebooted for any reason (loss of power etc.) upon bootup, the target server will actively download and apply the current running configuration from the source server. It will then also receive future changes made on the source server.

Library Synchronization Process

In the library synchronization process, if a library change is made on the source server, the change is applied locally. Once locally applied on the source server, this update will be placed in a queue for submission to target Web Filters. The source server will then send the information in the queue to all target servers. Each target server will receive this information and apply the update.

On the source server, a separate queue exists for each identified target server. A queue is used as a repository in the event of a communication failure between the source server and target server. Information remains in this queue and is submitted to the target server once communications are re-established. The use of queues ensures that if a target server is taken offline for a period of time, when it is brought back online, it will be updated with the latest changes from the source server.

Delays in Synchronization

When a filtering profile is applied to the source server, there is a slight delay in the time it takes to apply the profile to the target server. This delay is caused by the amount of time it takes the source server to process the change, prepare the update for submission, send the update, and finally to activate the update on the target server. In practice, this should only be matter of seconds. In essence, filtering profiles are shared in near real time with this factor being the only delay.

The delay in activating a library change can take a little longer than in activating a filtering profile change. This is due to the fact that the library on the Web Filter is loaded into the physical memory. When a change is made to the library, a new library must be loaded into memory with the changes. So the delay between the library change taking place is the net of the amount of time it takes the source server to prepare the update for submission, and then the amount of time it takes for the update to be sent, received, and processed by the target server. Once processed, the new library is loaded into memory and activated, while the old version of the library is removed from memory. The total time of this process will vary depending upon custom library entries, but the entire procedure should take approximately one minute.

Synchronized, Non-Synchronized Items

It is important to note that while some items are synchronized to the target Web Filters, they do not become permanent configurations on the target Web Filter. These items are in essence functionally synchronized, since they are configurations that the target Web Filters will read from the source Web Filter upon load. These items will then be updated on an as needed basis from the source Web Filter. For purpose of differentiation, these items will be referred to as functionally synchronized for purposes of this user guide. These functionally synchronized items will be available for use on the target Web Filter.

The following options are available for synchronization: Synchronize all items (both profile and library changes), and synchronize only library items.

As you will see by the lists on the following pages, static configuration options—such as library changes—will be synchronized. All active options—such as profile changes—will be functionally synchronized. One time configuration options on the Web Filter—such as reporting configurations, or IP addresses—will not be synchronized.

Synchronize All Items

The following lists show which items will be synchronized when the option to synchronize all items is selected.

Synchronized Items (All)

- M86 Library additions/deletions
- Custom library creations
- Custom library additions/deletions
- Search Engine keyword additions/deletions
- Keywords in URL additions/deletions
- Approved Content settings in the Global Group profile

Functionally Synchronized Items

- Common Customization, Block Page Authentication settings, Authentication Form Customization, Lock Page Customization, Warn Page Customization, Profile Control settings, Quota Block Page Customization, Quota Notice Page Customization
- Minimum Filtering Level
- Rules
- Global Group Profile
- Override Account: addition/deletion, activation/deactivation
- Lock Profiles
- IP User/Group and sub-group: additions/deletions, changes, filter changes
- LDAP User/Group: additions/deletions, changes, filter changes, profile activation/deactivation
- Category Weight System additions/deletions

- Quota Setting

Non-synchronized Items

- Filter control settings
- Virtual IP and Authentication IP addresses
- IP addresses
- Default routes
- Software Update application
- Synchronization settings
- Filter Mode
- Backup/Restore
- SNMP configuration
- Warn Option Setting
- Reporter configuration
- CMC Management

Synchronize Only Library Items

The following lists show which items will be synchronized when the option to synchronize only library items is selected.

Synchronized Items (Library Only)

- M86 Library additions/deletions
- Custom library creations
- Custom library additions/deletions
- Search Engine keyword additions/deletions
- Keywords in URL additions/deletions

Functionally Synchronized Items

- Category Weight System additions/deletions

Non-synchronized Items

- Common Customization, Block Page Authentication settings, Authentication Form Customization, Lock Page Customization, Warn Page Customization, Profile Control settings, Quota Block Page Customization, Quota Notice Page Customization
- Minimum Filtering Level
- Rules
- Global Group Profile
- Override Account: addition/deletion, activation/deactivation
- Lock Profiles
- IP User/Group and sub-group: additions/deletions, changes, filter changes

- LDAP User/Group: additions/deletions, changes, filter changes, profile activation/deactivation
- Filter control settings
- Virtual IP and Authentication IP addresses
- IP addresses
- Default routes
- Software Update application
- Synchronization settings
- Filter Mode
- Backup/Restore
- Radius Authentication Settings
- SNMP configuration
- X Strikes Blocking settings
- Warn Option Setting
- Reporter configuration
- CMC Management

Server Maintenance Procedures

Source Server Failure Scenarios

In the event that the source Web Filter unit should fail, the target servers will continue to run using the last known configuration loaded from the source server. However, all dynamic authentication-based profiles will eventually time-out, since the source Web Filter server can no longer verify user credentials. When this occurs, the information on the server can no longer be trusted. In most cases, the failure of the source server can be quickly repaired, though it is possible the source server will be down for an extended period of time due to detailed troubleshooting that needs to be performed, or that the source server will need to be replaced due to hardware failure.

In cases in which the source Web Filter server is out of commission for an extended period of time, this server should be replaced as soon as possible so that individual user authentication can be executed, and the ability to control the filtering cluster is continually enabled. In cases in which the Web Filter will not be immediately replaced, one of the target Web Filter servers should be designated as the new source server.

Establish Backup Procedures

To prevent down time during a source server failure, M86 recommends establishing backup and restore procedures. It is important that regular backups of the source Web Filter server are saved using the Backup/Restore window in the System section of the Web Filter console. Once a backup is created, it can be downloaded to another machine for safe-keeping. ***A backup should be created and downloaded whenever a change is made to filtering settings on the source Web Filter.***

Use a Backup File to Set up a Source Server

In the event of a source server failure, the global administrator should designate a target server as the new source server.

Set up a Target Server as a Source Server

1. Log in to the console of the target server designated as the new source server.
2. In the System section of the console, go to the Backup/ Restore window and create a backup of the current running configuration on that server.
3. Download the server’s configuration to a safe storage place until it is needed.
4. In the LAN Settings window (accessible via System > Network), set up IP addresses to be the same as on the source server that is being replaced.
5. Go to the Reboot window (accessible via System > Control) and reboot the server.
6. Once the Web Filter is rebooted, reconnect to the console and access the Backup/Restore window.
7. Upload the last good configuration from the failed source server to the new source server. When the configuration file is uploaded and available in the Web Filter console, that file should be used for restoring configuration settings.
8. After the restoration of configuration settings is applied and a quick reload takes place, this Web Filter will now function as the source server in the Web Filter cluster.

Set up a Replacement Target Server

Once the original source server is replaced or repaired, it can then be configured to replace the empty spot created by the movement of the target server to the position of source server. Configure this Web Filter so that the IP addresses are that of the target server which became the source server. Upload the running target configuration, which was downloaded prior to converting the target server to a source server. Use this configuration to create a duplicate of the target server that was moved. Once this step is complete, the cluster is whole again and should operate normally.

Set up a New Source Server from Scratch

In the event that you do not have a reliable backup file that can be used for establishing a new source server, you must recreate the settings on the new source server.

Set up a Target Server as a Source Server

1. Log in to the console of the target server designated as the new source server.
2. In the System section of the console, access the Reset window and click Reset to remove all settings on the server.
3. Enter all settings from the failed source server on this “new” server. In the Setup window (accessible via System > Synchronization), specify that this is a source server.
4. Apply all software updates that were applied on the failed source server.
5. In the Policy section of the console, enter all groups and filtering profiles.
6. Make all necessary settings in all sections and windows of the console.

Chapter 4: Getting Started

Using the Administrator Console

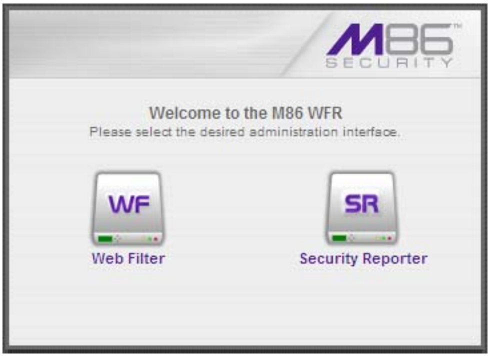
Access the Web Filter Login window

The Web Filter user interface is accessible in one of two ways:

- by clicking the WF icon in the WFR Welcome window (see Access the Web Filter from the WFR Portal)
- by launching an Internet browser window supported by the Web Filter and then entering the Web Filter's URL in the Address field (see Enter Web Filter's URL in the Address field)

Access the Web Filter from the WFR Portal

Click the WF icon in the WFR Welcome window:



Welcome to the M86 WFR

Please select the desired administration interface.

Fig. 1:4-1 Web Filter icon in WFR Welcome window

Clicking the WF icon opens a separate browser window/tab containing the Web Filter Login window (see Fig. 1:4-2).

Enter Web Filter’s URL in the Address field

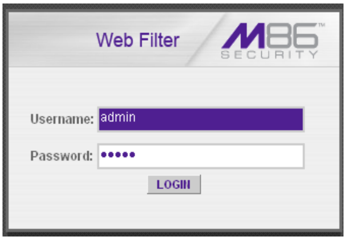
1. Launch an Internet browser window supported by the Web Filter.
2. In the address line of the browser window, type in “https://” and the Web Filter server’s IP address or host name, and use port number “:1443” for a secure network connection, plus “/login.jsp”.

   For example, if your IP address is 210.10.131.34, type in **https://210.10.131.34:1443/login.jsp**. Using a host name example, if the host name is logo.com, type in **https://logo.com:1443/login.jsp**.

   With a secure connection, the first time you attempt to access the Web Filter’s user interface in your browser you will be prompted to accept the security certificate. In order to accept the security certificate, follow the instructions at: ***http://www.m86security.com/software/8e6/docs/ig/misc/sec-cert-wf4.1.pdf***
3. After accepting the security certificate, click **Go** to open the Web Filter login window (see Fig. 1:4-2).

Log In

1. In the Login window, enter your **Username** and **Password**:



Username: admin

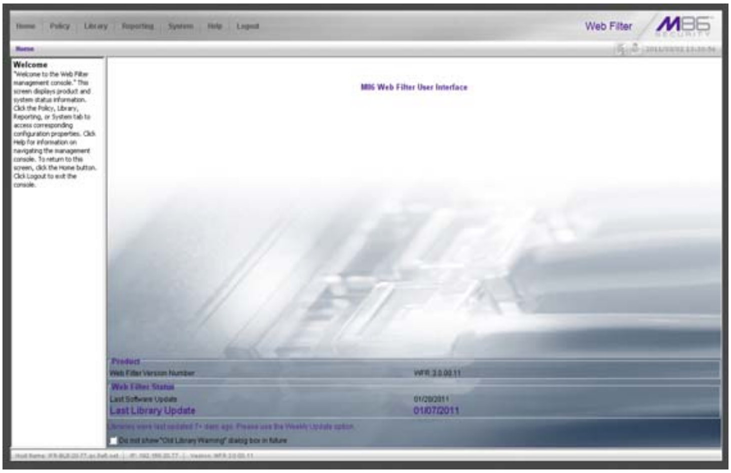
Password: •••••

Fig. 1:4-2 Web Filter Login window

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 WF Global Administrator Section) and create a global administrator account.*

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

2. Click **LOGIN** to access the Welcome screen of the Web Filter Administrator console:



Welcome

"Welcome to the Web Filter management console." This screen displays product and system status information. Click the Policy, Library, Reporting, or System tab to access corresponding configuration properties. Click Help for information on navigating the management console. To return to this screen, click the Home button. Click Logout to exit the console.

M86 Web Filter User Interface

Product

Web Filter Version Number WFR 2.0.00.11

Web Filter Status

Last Software Update 01/28/2011

Last Library Update 01/07/2011

Libraries were last updated 7+ days ago. Please use the Weekly Update option.

□ Do not show "Old Library Warning" dialog box in future

Fig. 1:4-3 Welcome screen

On this screen, the Web Filter Version Number displays in the Product frame, and dates for the Last Software Update and Last Library Update display in the Web Filter 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

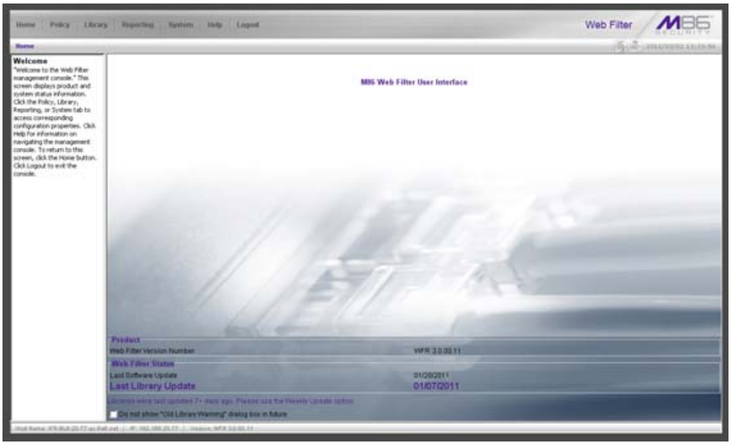
If it has been more than seven days since the Web Filter last received updates to library categories, upon logging into the Administrator console a pop-up dialog box opens and displays the following message: ”Libraries were last updated more than 7 days ago. Do you want to update your libraries now?” 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 M86 Supplied Categories window—in the Web Filter 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 purple colored text: "Libraries were last updated 7 days ago. Please use the Weekly Update option":



Welcome

"Welcome to the Web Filter management console." This screen displays product and system status information. Click the Policy, Library, Reporting, or System tab to access corresponding configuration properties. Click Help for information on navigating the management console. To return to this screen, click the Home button. Click Logout to exit the console.

M86 Web Filter User Interface

Product

Web Filter Version Number WFR 3.0.00.11

Web Filter Status

Last Software Update 01/20/2011

Last Library Update 01/07/2011

Libraries were last updated 7+ days ago. Please use the Weekly Update option

□ Do not show "Old Library Warning" dialog box in future

Fig. 1:4-4 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. 1:4:3 with today's date as the Last Library Update in black text.

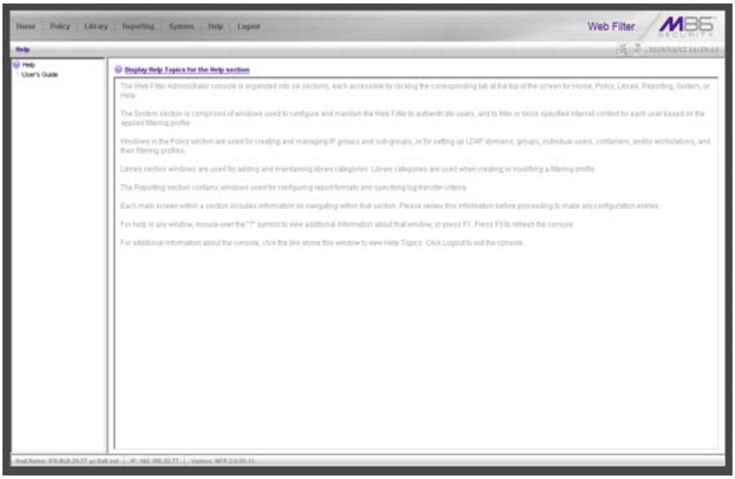
Navigation Tips

Access Main Sections

The Administrator console is organized into six sections, each accessible by clicking the corresponding link in the navigation toolbar at the top of the screen:

- **Home** - clicking this link displays the Welcome screen of the Administrator console.
- **Policy** - clicking this link displays the main screen for the Policy section. Windows in the Policy section are used for creating and managing master IP groups, sub-groups, and individual IP filtering profiles, or for setting up LDAP domains, groups, and individual users, and their filtering profiles.
- **Library** - clicking this link 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 link displays the main screen for the Reporting section. The Reporting section contains windows used for configuring reports on users' Internet activities.
- **System** - clicking this link 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.

- **Help** - clicking this link displays the Help screen. This screen includes navigation tips and a link to a page where you can access the latest user guides (in the .pdf format) for this application:



The Web Filter Administrator console is organized into six sections, each accessible by clicking the corresponding tab at the top of the screen for Home, Policy, Library, Reporting, System, or Help.

The System section is comprised of windows used to configure and maintain the Web Filter to authenticate users, and to filter or block specified Internet content for each user based on the applied filtering profile.

Windows in the Policy section are used for creating and managing IP groups and sub-groups, or for setting up LDAP domains, groups, individual users, containers, and/or workstations, and their filtering profiles.

Library section windows are used for adding and maintaining library categories. Library categories are used when creating or modifying a filtering profile.

The Reporting section contains windows used for configuring report formats and specifying log transfer criteria.

Each main screen within a section includes information on navigating within that section. Please review this information before proceeding to make any configuration entries.

For help in any window, mouse-over the "?" symbol to view additional information about that window, or press F1. Press F5 to refresh the console.

For additional information about the console, click the link above this window to view Help Topics. Click Logout to exit the console.

Fig. 1:4-5 Help screen

- **Logout** - click this link to log out of this application. When your session has been terminated, the login window re-displays.

Note that on each screen, in the right side of the navigation path bar beneath the banner, the following displays:

X Strikes Blocking icon - If the X Strikes Blocking feature is enabled, this icon can be clicked by authorized users to access the X Strikes Unlock Workstation window where workstations are unlocked.

Real Time Probe icon - If the Real Time Probe feature is enabled, this icon can be clicked by authorized users to access the Real Time Probe reporting tool.

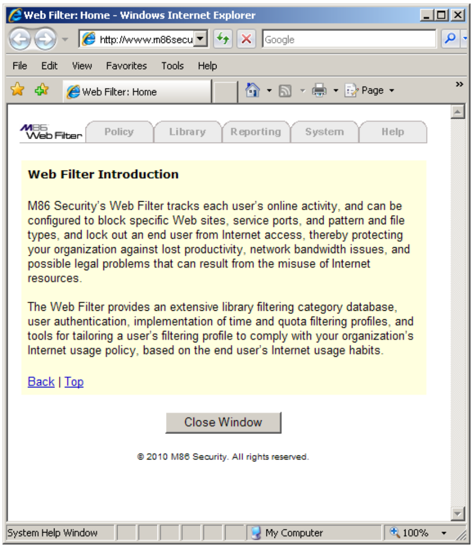
- system time - The system time displays using the YYYY/MM/DD HH:MM:SS date and time format

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:



Web Filter Introduction

M86 Security's Web Filter tracks each user's online activity, and can be configured to block specific Web sites, service ports, and pattern and file types, and lock out an end user from Internet access, thereby protecting your organization against lost productivity, network bandwidth issues, and possible legal problems that can result from the misuse of Internet resources.

The Web Filter provides an extensive library filtering category database, user authentication, implementation of time and quota filtering profiles, and tools for tailoring a user's filtering profile to comply with your organization's Internet usage policy, based on the end user's Internet usage habits.

Back | Top

© 2010 M86 Security. All rights reserved.

Fig. 1:4-6 Help Topics window

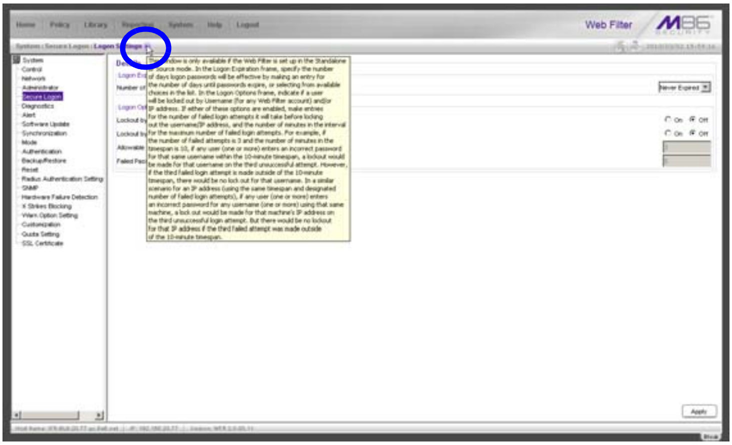
1. Click a link to go to a specified topic.
2. To view Help Topics for another section, click the tab for that section: Policy, Library, Reporting, System, or Help.
3. Click **Close Window** to close the Help Topics window.

Tooltips

In any window that features the ? icon in the navigation path bar beneath the banner, 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:



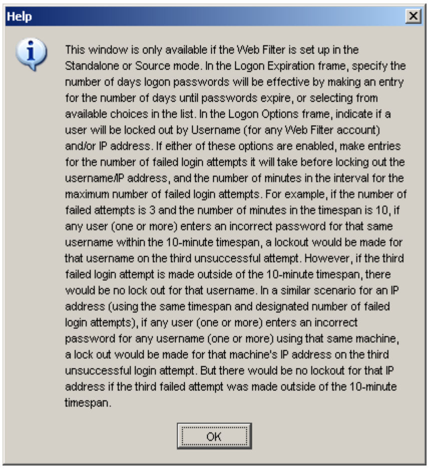
This window is only available if the Web Filter is set up in the Standalone or Source mode. In the Logon Expiration frame, specify the number of days logon passwords will be effective by making an entry for the number of days until passwords expire, or selecting from available choices in the list. In the Logon Options frame, indicate if a user will be locked out by Username (for any Web Filter account) and/or IP address. If either of these options are enabled, make entries for the number of failed login attempts it will take before locking out the username/IP address, and the number of minutes in the interval for the maximum number of failed login attempts. For example, 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 lock out 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.

Fig. 1:4-7 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:



This window is only available if the Web Filter is set up in the Standalone or Source mode. In the Logon Expiration frame, specify the number of days logon passwords will be effective by making an entry for the number of days until passwords expire, or selecting from available choices in the list. In the Logon Options frame, indicate if a user will be locked out by Username (for any Web Filter account) and/or IP address. If either of these options are enabled, make entries for the number of failed login attempts it will take before locking out the username/IP address, and the number of minutes in the interval for the maximum number of failed login attempts. For example, 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 lock out 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.

Fig. 1:4-8 Help pop-up box

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

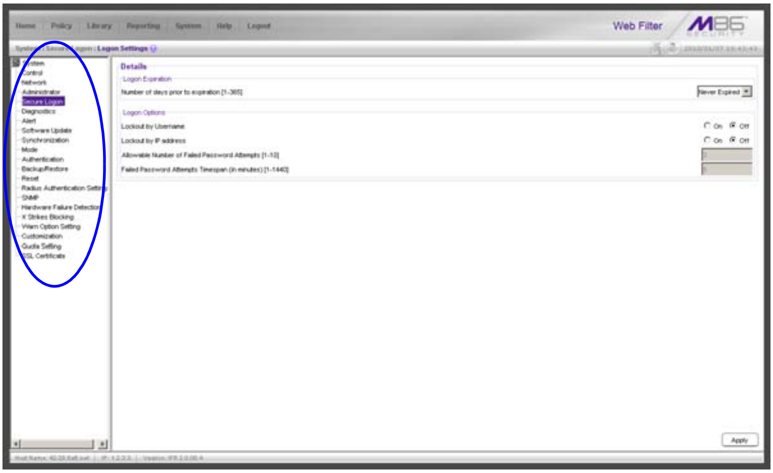
Screen and Window Navigation

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



Number of days prior to expiration [1-365]: Never Expired

Lockout by Username: ○ On ● Off

Lockout by IP address: ○ On ● Off

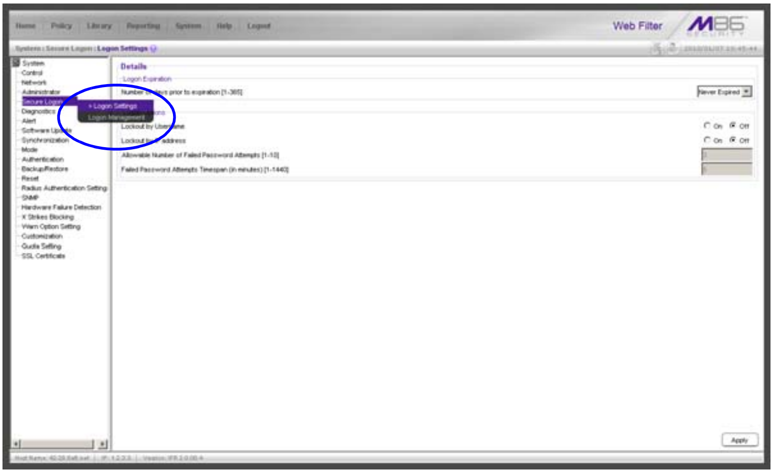
Allowable Number of Failed Password Attempts [1-10]

Failed Password Attempts Timespan (in minutes) [1-1440]

Fig. 1:4-9 Selected topic and its corresponding window

Select Sub-topics

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



Number of days prior to expiration [1-365]: Never Expired

Lockout by Username: ○ On ● Off

Lockout by IP address: ○ On ● Off

Allowable Number of Failed Password Attempts [1-10]

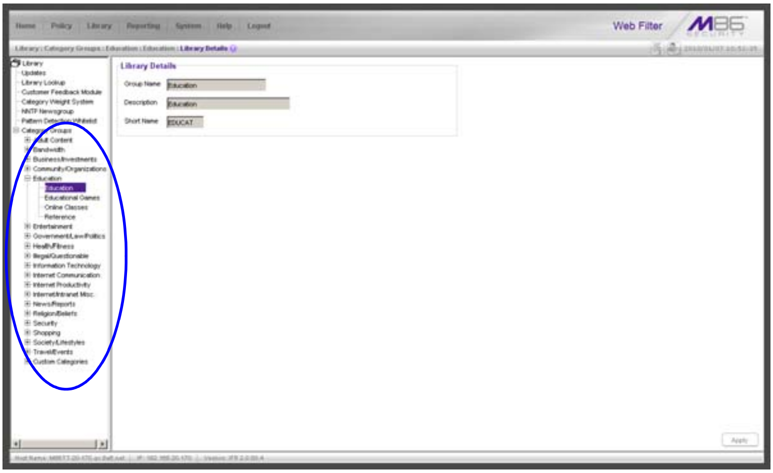
Failed Password Attempts Timespan (in minutes) [1-1440]

Fig. 1:4-10 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 Policy and Library screens.



Library Details

Group Name: Education

Description: Education

Short Name: EDUCAT

Fig. 1:4-11 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.

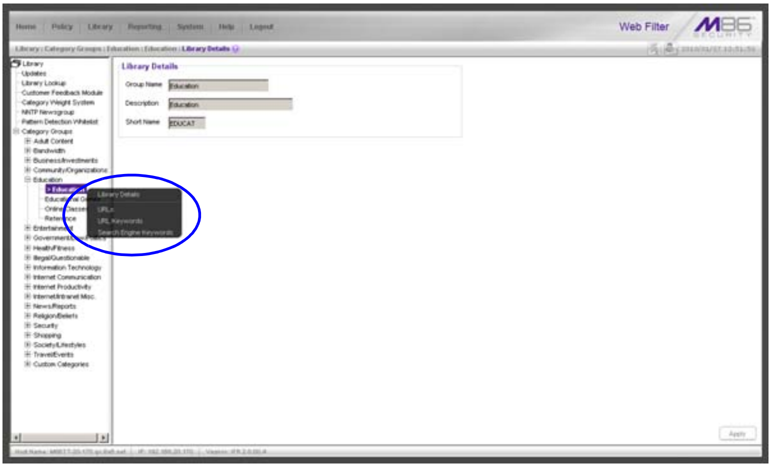
An item in the tree is selected by clicking it.

Tree List Topics and Sub-topics

Policy 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:



Library Details

Group Name: Education

Description: Education

Short Name: EDUCAT

Fig. 1:4-12 Tree list topics and sub-topics

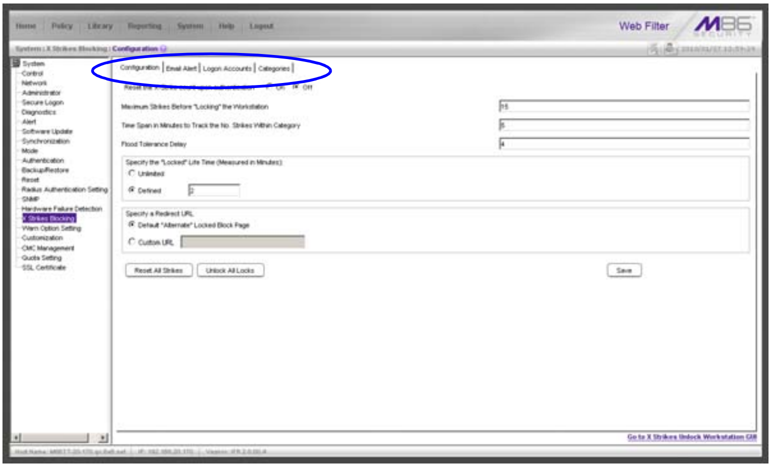
Clicking a sub-topic displays the corresponding window in the right panel, or opens a pop-up window or alert box, as appropriate.

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.*



Reset the X Strikes count upon authentication ○ On ● Off

Maximum Strikes Before "Locking" the Workstation 15

Time Span in Minutes to Track the No. Strikes Within Category 5

Flood Tolerance Delay 4

Specify the "Locked" Life Time (Measured in Minutes)
○ Unlimited
● Defined 2

Specify a Redirect URL
● Default "Alternate" Locked Block Page
○ Custom URL

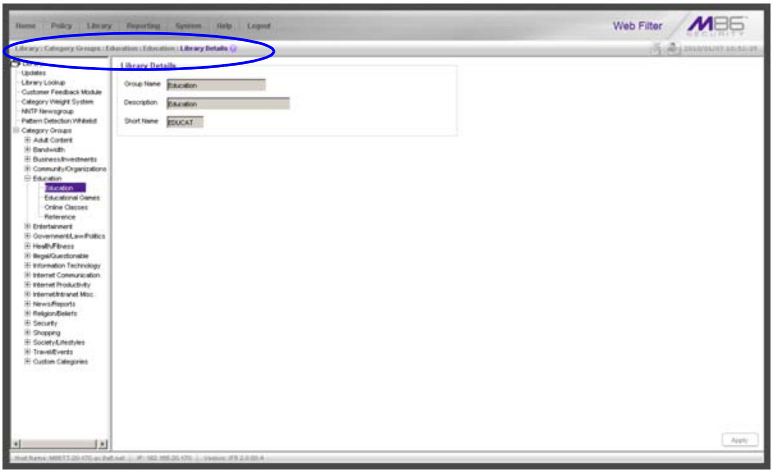
Fig. 1:4-13 Window with tabs

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:



Library : Category Groups : Education : Education : Library Details

Library Details

Group Name: Education

Description: Education

Short Name: EDUCAT

Fig. 1:4-14 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 Web Filter.

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 user interface 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.

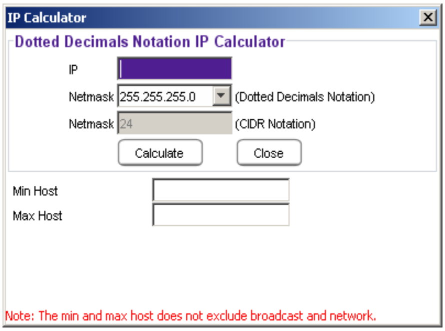
- **Paste command**

  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: Range to Detect and Members windows from the Policy section, and Block Page Route Table window from the System section.



Netmask 255.255.255.0 (Dotted Decimals Notation)

Netmask 24 (CIDR Notation)

Note: The min and max host does not exclude broadcast and network.

Fig. 1:4-15 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.

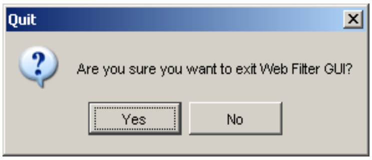
Re-size the User Interface

For greater ease in viewing content in any screen, re-size the browser window by placing your cursor at any edge or corner of the user interface, left clicking, and then dragging the cursor to the left or right, or inward or outward.

Log Out

To log out of the Web Filter Administrator console:

1. Click the **Logout** button in the navigation toolbar at the top of the screen. This action opens the Quit dialog box:


Quit

Are you sure you want to exit Web Filter GUI?

Fig. 1:4-16 Quit dialog box

2. Click **Yes** to return to the Login window.
3. Click the “X” in the upper right corner of the screen for the Login window to close it.

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

WF GLOBAL ADMINISTRATOR SECTION

Introduction

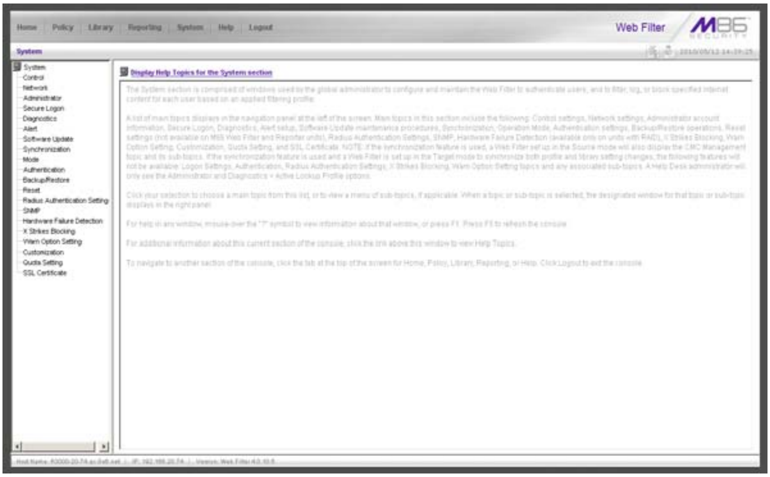
The WF Global Administrator Section of this portion of the user guide is comprised of four chapters, based on the layout of the Administrator console. This section is used by the authorized global administrator of the Web Filter for configuring and maintaining the Web Filter application on the WFR server.

The global administrator performs the following tasks:

- provides a suitable environment for the server, including high speed access to the server by authorized client workstations
- adds group administrators
- sets up administrators for receiving automatic alerts
- updates the WFR server with software supplied by M86
- 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.



Display Help Topics for the System section

The System section is comprised of windows used by the global administrator to configure and maintain the Web Filter to authenticate users, and to filter, log, or block specified Internet content for each user based on an applied filtering profile.

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 setup, Software Update maintenance procedures, Synchronization, Operation Mode, Authentication settings, Backup/Restore operations, Reset settings (not available on M86 Web Filter and Reporter units), Radius Authentication Settings, SNMP, Hardware Failure Detection (available only on units with RAID), X Strikes Blocking, Warn Option Setting, Customization, Quota Setting, and SSL Certificate. NOTE: If the synchronization feature is used, a Web Filter set up in the Source mode will also display the CMC Management topic and its sub-topics. If the synchronization feature is used and a Web Filter is set up in the Target mode to synchronize both profile and library setting changes, the following features will not be available: Logon Settings, Authentication, Radius Authentication Settings, X Strikes Blocking, Warn Option Setting topics and any associated sub-topics. A Help Desk administrator will only see the Administrator and Diagnostics > Active Lookup Profile options.

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.

For help in any window, mouse-over the "?" symbol to view information about that window, or press F1. Press F5 to refresh the console.

For additional information about this current section of the console, click the link above this window to view Help Topics.

To navigate to another section of the console, click the tab at the top of the screen for Home, Policy, Library, Reporting, or Help. Click Logout to exit the console.

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, Software Update, Synchronization, operation Mode, Authentication settings (see the M86 Web Filter Authentication User Guide for information about this topic), Backup/Restore operations, Reset settings, Radius Authentication Settings, SNMP, Hardware Failure Detection, X Strikes Blocking, Warn Option Setting, Customization, Quota Setting, and SSL Certificate.

***NOTES**: If the synchronization feature is used and a Web Filter is set up in the Source mode, the CMC Management topic and associated sub-topics are also available.*

If the synchronization feature is used and a Web Filter is set up in the Target mode to synchronize both profile and library setting changes, settings in the Filter window and Customization windows cannot be edited, and the following topics and any associated sub-topics are not available: Block Page Authentication, Authentication, Radius Authentication Settings, X Strikes Blocking, and Warn Option Setting. If a Web Filter is set up in the Target mode to synchronize only library setting changes, all topics and sub-topics are available.

A help desk administrator will only see the Administrator and Diagnostics topics.

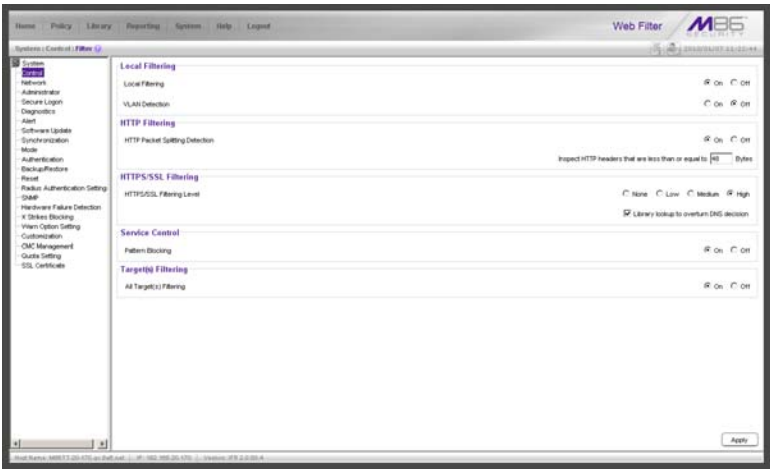
Click your selection to choose a main topic from this list, or to view a menu of sub-topics, if applicable. When a topic or sub-topic is selected, the designated window for that topic or sub-topic displays in the right panel.

Control

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

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.



Local Filtering

Local Filtering ● On ○ Off

VLAN Detection ○ On ● Off

HTTP Filtering

HTTP Packet Splitting Detection ● On ○ Off

Inspect HTTP headers that are less than or equal to 40 Bytes

HTTPS/SSL Filtering

HTTPS/SSL Filtering Level ○ None ○ Low ○ Medium ● High

☑ Library lookup to overturn DNS decision

Service Control

Pattern Blocking ● On ○ Off

Target(s) Filtering

All Target(s) Filtering ● On ○ Off

Fig. 2:1-2 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 Web Filters 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.m86security.com/software/8e6/hlp/ifr/files/1system_proxy_block .html** for a list of proxy pattern types set up to be blocked. When using this feature, the Pattern Detection Whitelist window can be used for setting up IP addresses to bypass pattern filtering (see Pattern Detection Whitelist window in Chapter 3: Library screen). Target(s) Filtering will only display if this server being configured is set up for synchronization in the Source mode. This frame is used for specifying whether filtering will take place on all Web Filters on the network set up in the Target mode.

***NOTE**: This window displays greyed-out if the synchronization feature is used, and this server being configured is set up in the Target mode to synchronize both profile and library setting changes.*

***TIP**: See the Web Filter Introductory Section for overviews on the following topics:*

- *IM and P2P (Chapter 2: Logging and Blocking)*
- *Synchronization (Chapter 3: Synchronizing Multiple Units)*

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 Web Filters 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 Web Filter to filter HTTPS sites
- “Low” - if you want the Web Filter to filter HTTPS sites without having the Web Filter communicate with IP addresses or hostnames of HTTPS servers
- “Medium” - if you want the Web Filter 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 Web Filter 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 library category sub-section in Chapter 2: Library screen from the WF Group Administrator Section for information on setting up a custom library category. See Global Group Profile window and Minimum Filtering Level window in Chapter 2: Policy screen 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 M86 Supplied Categories window.

***NOTE**: See **http://www.m86security.com/software/8e6/hlp/ifr/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 M86 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, “CHAT” and specified Instant Messaging M86 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 “CHAT” and appropriate Instant Messaging library categories set up to be blocked.

Additionally, to block specified users from accessing P2P services, the M86 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.

To create a whitelist of pattern IP addresses, see the Pattern Detection Whitelist window in Chapter 3: Library screen.

Disable Pattern Blocking

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

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

Target(s) Filtering

The Target(s) Filtering frame only displays if the Web Filter currently being configured is set up in the Source mode for synchronization. The default setting has **All Target(s) Filtering** “On”.

Disable Filtering on Target Servers

To disable **All Target(s) Filtering**, click the “Off” radio button. Each target server on the network will not filter the Range to Detect specified on that server.

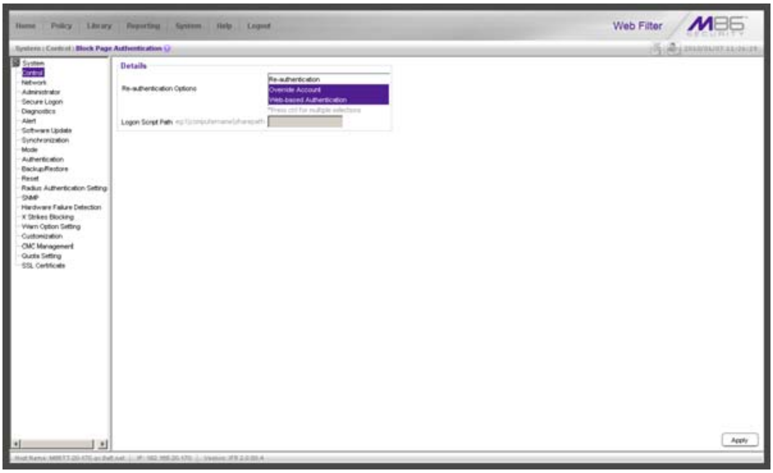
Enable Filtering on Target Servers

To enable **All Target(s) Filtering**, click the “On” radio button. Each target server on the network will filter the Range to Detect specified on that server.

***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 Web Filter 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.



Details

Re-authentication Options: Re-authentication [✓ Override Account] [✓ Web-based Authentication]

*Press ctrl for multiple selections

Logon Script Path eg:\\computername\sharepath

Fig. 2:1-3 Block Page Authentication window

***NOTE**: This feature is not available if the synchronization feature is used, and this server being configured is set up in the Target mode to synchronize both profile and library setting changes.*

See the Block Page Customization window and Common Customization window in this chapter for information on customizing the M86 block page. See Appendix B: 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, 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 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 M86 Web Filter 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:*

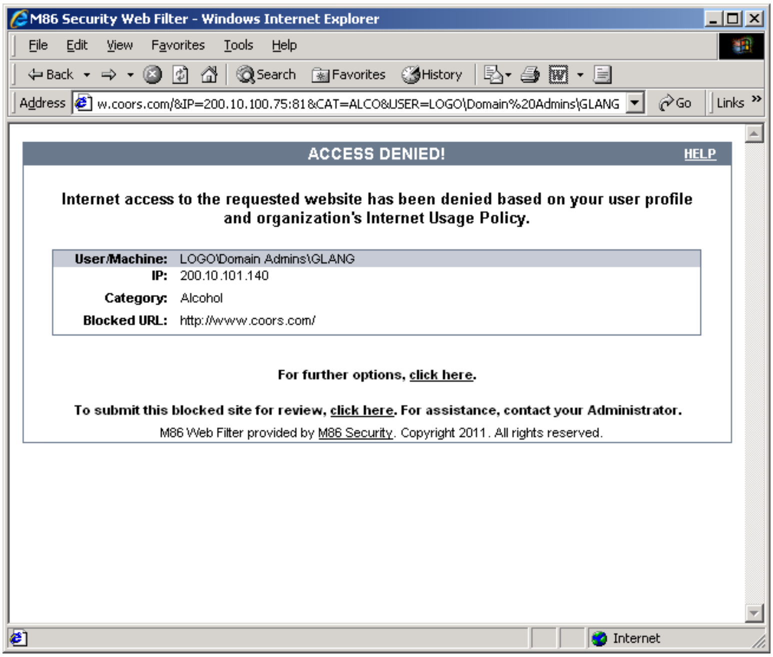
- *WF Global Administrator Section: Override Account window and Bypass Option window for the global group*
- *WF Group Administrator Section: Override Account window for IP groups, and Exception URL window for IP groups.*

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 Web Filter 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 backslashes, 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:


M86 Security Web Filter - Windows Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address
w.coors.com/&IP=200.10.100.75:81&CAT=ALCO&USER=LOGO\Domain%20Admins\GLANG
Go Links
Internet

ACCESS DENIED! HELP

Internet access to the requested website has been denied based on your user profile and organization's Internet Usage Policy.

User/Machine:	LOGO\Domain Admins\GLANG
IP:	200.10.101.140
Category:	Alcohol
Blocked URL:	http://www.coors.com/

For further options, click here.

To submit this blocked site for review, click here. For assistance, contact your Administrator.

M86 Web Filter provided by M86 Security. Copyright 2011. All rights reserved.

Fig. 2:1-4 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 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 M86's Technical Support page that explains why access to the site or service may have been denied.
- **M86 Security** - Clicking this link takes the user to M86's Web site.

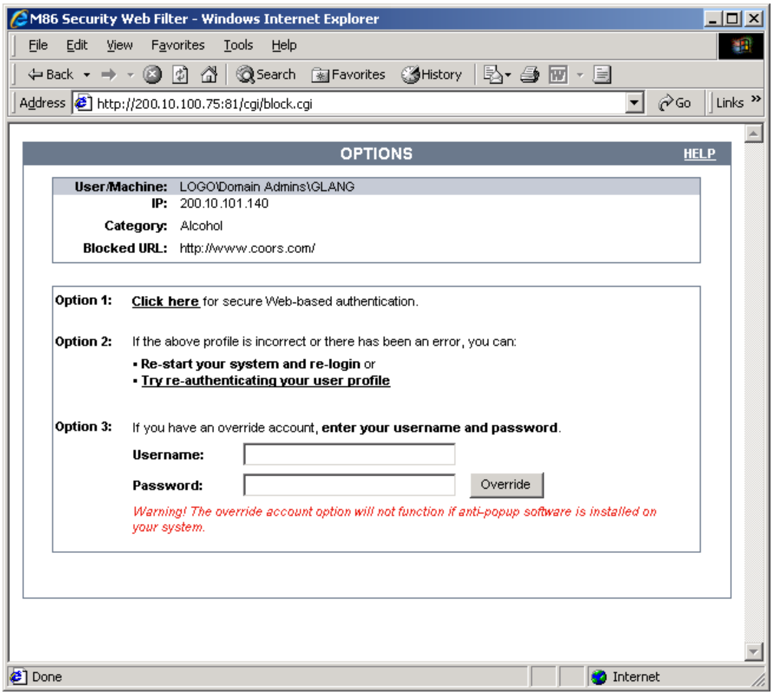
By default, these links are included in the block page under the following conditions:

- **For further options, <u>click here</u>. -** 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, <u>click here</u>. -** 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.**


M86 Security Web Filter - Windows Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://200.10.100.75:81/cgi/block.cgi
Go Links
Done
Internet

OPTIONS HELP

User/Machine: LOGO\Domain Admins\GLANG
IP: 200.10.101.140
Category: Alcohol
Blocked URL: http://www.coors.com/

Option 1: Click here for secure Web-based authentication.

Option 2: If the above profile is incorrect or there has been an error, you can:
- **Re-start your system and re-login** or
- **Try re-authenticating your user profile**

Option 3: If you have an override account, **enter your username and password**.

Username:

Password: Override

Warning! The override account option will not function if anti-popup software is installed on your system.

Fig. 2:1-5 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

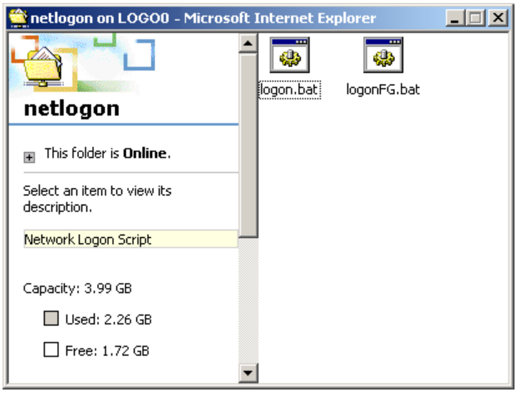
The frame beneath the User/Machine frame includes information for options (1, 2, and/or 3) based on settings made in this window and the Common Customization window.

***NOTE**: Information about Option 1 is included in the M86 Web Filter 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.
- **<u>Try re-authenticating your user profile</u>** - 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:



netlogon on LOGO0 - Microsoft Internet Explorer

netlogon

⊞ This folder is **Online.**

Select an item to view its description.

Network Logon Script

Capacity: 3.99 GB

□ Used: 2.26 GB

□ Free: 1.72 GB

logon.bat

logonFG.bat

Fig. 2:1-6 Re-authentication option

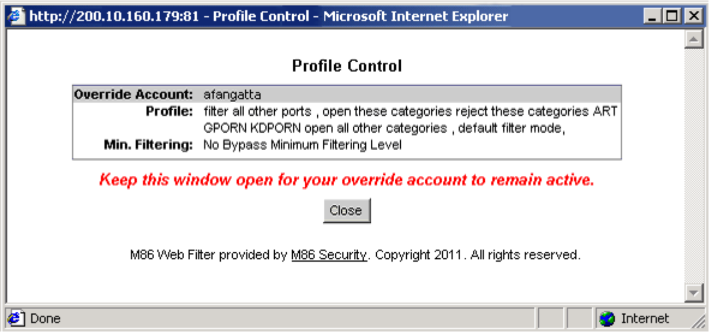
The user should click the **logon.bat** icon to run a script that will re-authenticate his/her profile on the network.

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:


http://200.10.160.179:81 - Profile Control - Microsoft Internet Explorer
Close
Done
Internet

Profile Control

Override Account:	afangatta
Profile:	filter all other ports , open these categories reject these categories ART GPORN KDPORN open all other categories , default filter mode,
Min. Filtering:	No Bypass Minimum Filtering Level

Keep this window open for your override account to remain active.

M86 Web Filter provided by M86 Security. Copyright 2011. All rights reserved.

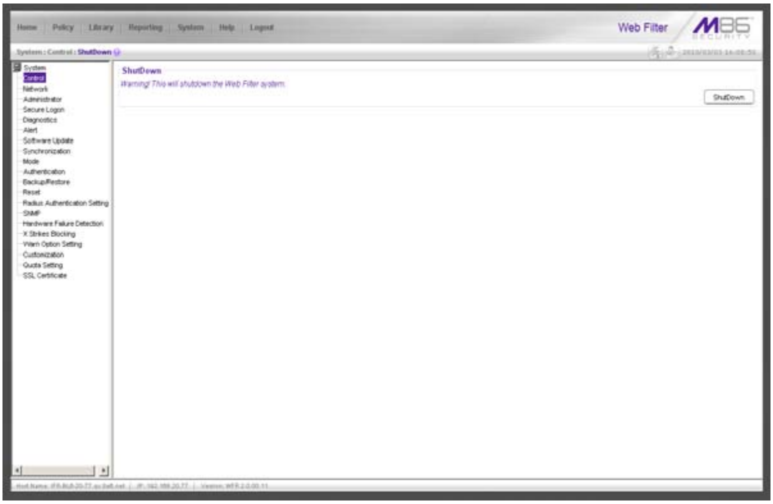
Fig. 2:1-7 Profile Control pop-up window

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 C: 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.



Warning! This will shutdown the Web Filter system.

Fig. 2:1-8 ShutDown window

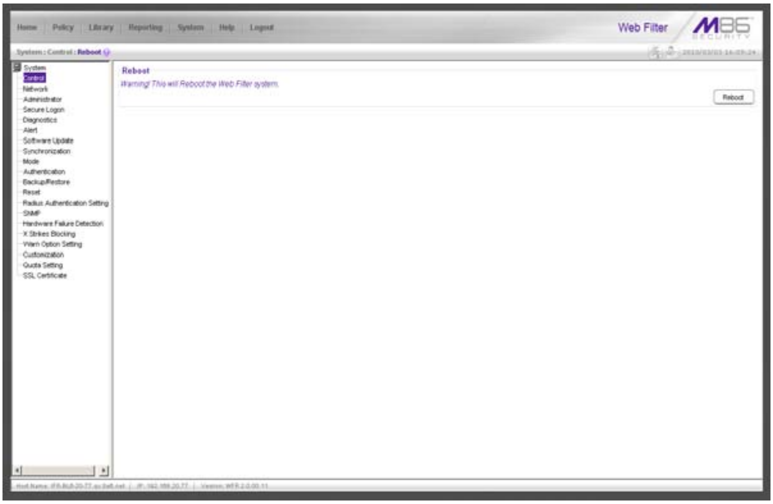
Shut Down the Server

In the ShutDown frame, click **ShutDown** to power off the server.

***NOTE**: See the WFR Overview for information about accessing the WFR user interface and logging back into the server.*

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.



Warning! This will Reboot the Web Filter system.

Fig. 2:1-9 Reboot window

Reboot the Server

1. In the Reboot frame, click **Reboot** to open the Reboot Web Filter 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.

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

   After the server is rebooted, the Web Filter status message box closes, and the Web Filter ready alert box opens.

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

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

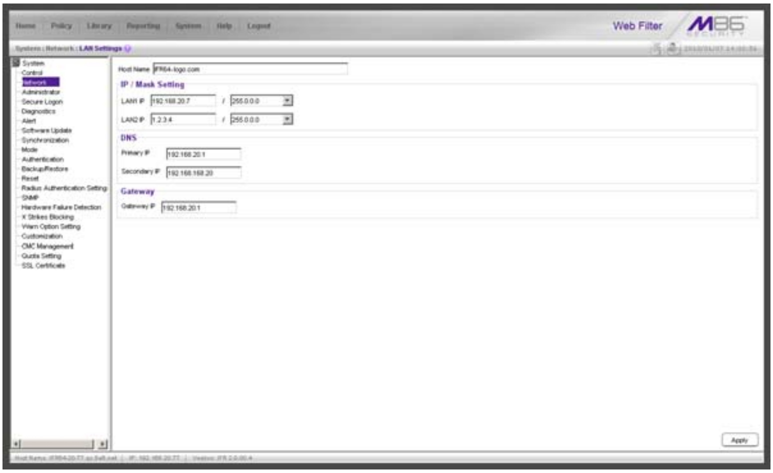
NOTE*: See the WFR Suite Overview and Chapter 4: Getting Started from the Introductory Section of the Web Filter portion of this user guide for information about accessing the WFR user interface and logging back into the server.*

Network

Network includes options for configuring the Web Filter 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.

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 WFR.



Host Name: IFR64-logo.com

IP / Mask Setting

LAN1 IP: 192.168.20.7 / 255.0.0.0

LAN2 IP: 1.2.3.4 / 255.0.0.0

DNS

Primary IP: 192.168.20.1

Secondary IP: 192.168.168.20

Gateway

Gateway IP: 192.168.20.1

Fig. 2:1-10 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 **wfr.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.

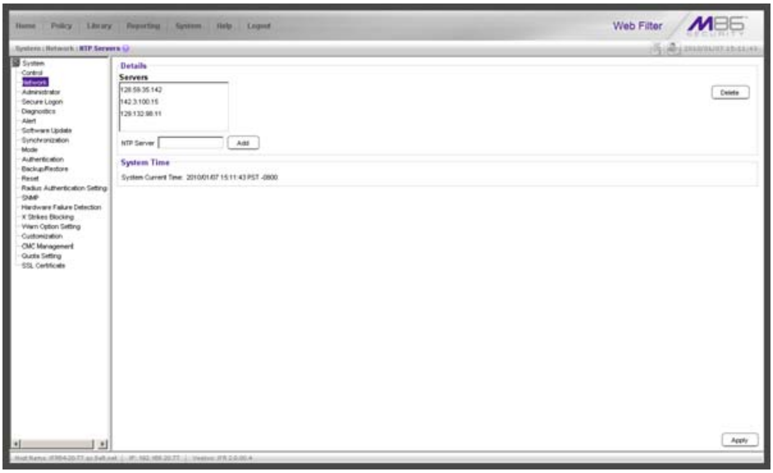
3. Click **Apply** to apply your settings.

__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 Web Filter 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.*



Servers:
128.59.35.142
142.3.100.15
129.132.98.11

System Current Time: 2010/01/07 15:11:43 PST -0800

Fig. 2:1-11 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 Web Filter 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.

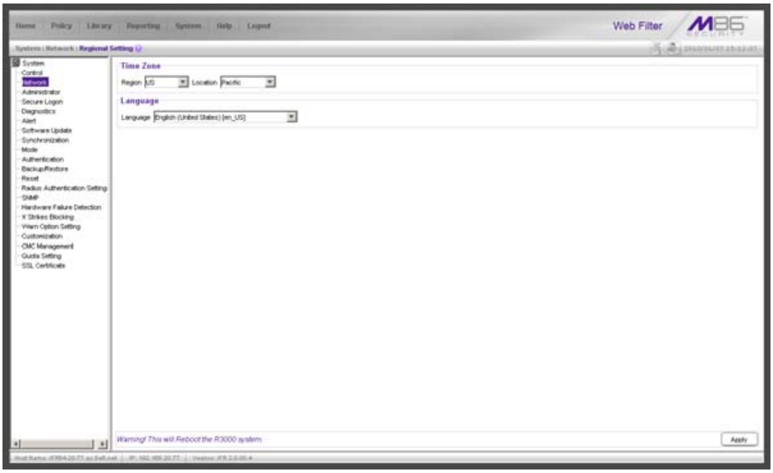
Remove an NTP Server

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.

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 Web Filter and the language set type, if necessary.



Region: US   Location: Pacific

Language: English (United States) [en_US]

Warning! This will Reboot the R3000 system.

Fig. 2:1-12 Regional Setting window

Specify the Time Zone, Language Set

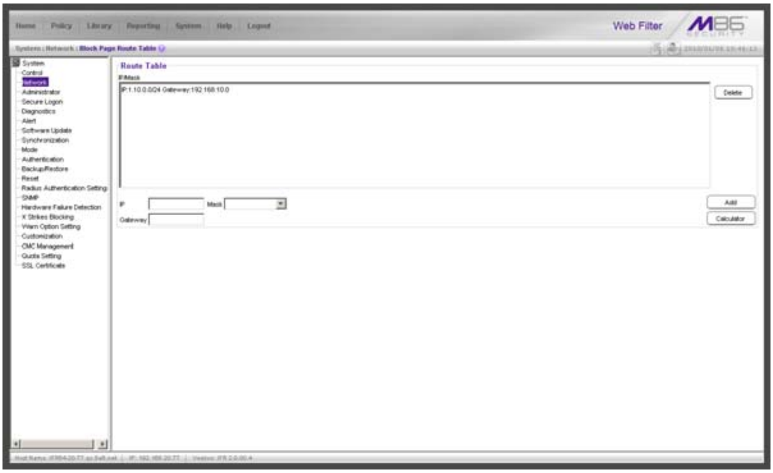
In the Details frame, the Region “US” and the Location “Pacific” display by default. To change these settings:

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 Web Filter.

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.



IP:1.10.0.0/24 Gateway:192.168.10.0

Fig. 2:1-13 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:

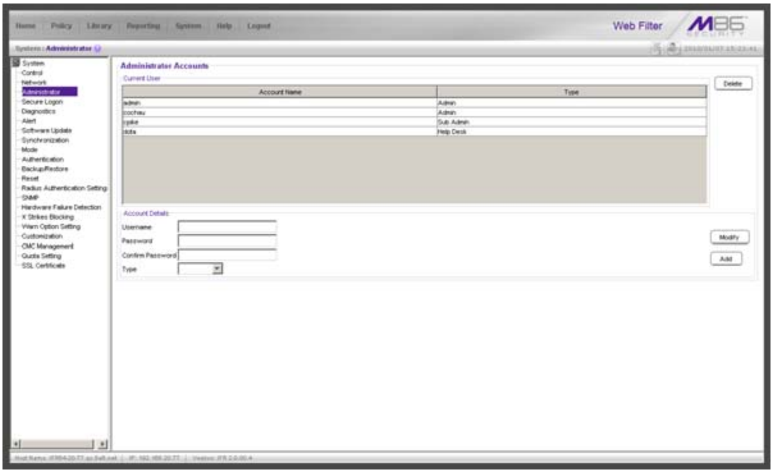
1. Select the router(s) from the list box.
2. Click **Delete**.

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), group administrator (Sub Admin), and help desk administrator (Help Desk) accounts. A Sub Admin manages LDAP entities and their filtering profiles. A Help Desk administrator can verify a user's current filtering profile status and can perform URL and search engine keyword lookups in library categories.

NOTE*: See the Group Details window in Chapter 1: Policy screen of the WF Group Administrator Section for information on setting up and maintaining accounts for IP group administrators. See the M86 Web Filter Authentication User Guide for more information on setting up and maintaining LDAP Sub Admin group administrator accounts. A help desk administrator will only see his/her account information and can only modify his/her password.*



Administrator Accounts

Current User

Account Name	Type
admin	Admin
cochau	Admin
cpike	Sub Admin
dota	Help Desk

Account Details

Username

Password

Confirm Password

Type

Fig. 2:1-14 Administrator window

***TIP**: The default Username is **admin** and the Password is **user3**. M86 recommends that you retain this default account and password in the event that the Web Filter unit cannot be accessed. An authorized M86 Security 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”, “Sub Admin”, or “Help Desk”) for each active global administrator, LDAP group administrator, or help desk administrator previously set up in this window.

Add an Administrator Account

To add an 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”, “Sub Admin”, or “Help Desk” 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, "Sub Admin" for LDAP group administrator, or "Help Desk" for help desk 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.

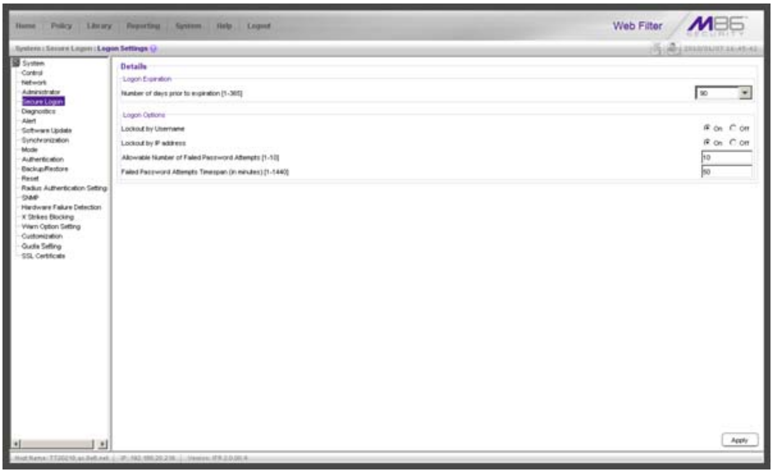
Secure Logon

Secure Logon includes options for setting user passwords to expire after a designated number of days, and/or locking out users from the Web Filter 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.

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 in which you define the number of days a password will be valid before a new password must be used. You can also 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.*



Details

Logon Expiration

Number of days prior to expiration [1-365]: 90

Logon Options

Lockout by Username: ● On ○ Off

Lockout by IP address: ● On ○ Off

Allowable Number of Failed Password Attempts [1-10]: 10

Failed Password Attempts Timespan (in minutes) [1-1440]: 50

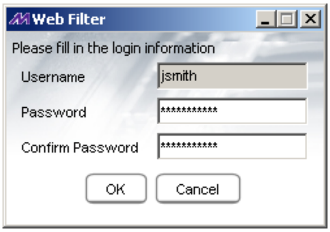
Fig. 2:1-15 Logon Settings window

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 window and clicks LOGIN, a login dialog box opens:*



Please fill in the login information

Username: jsmith

Password: ***********

Confirm Password: ***********

Fig. 2:1-16 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 Web Filter user 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 Web Filter.

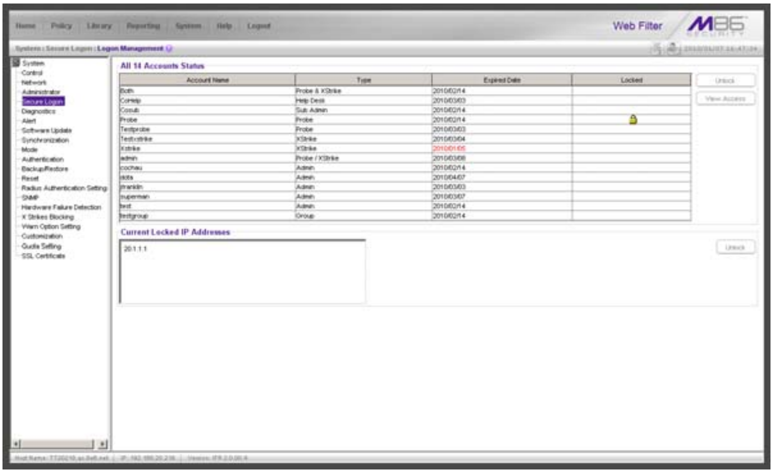
- At the **Failed Password Attempts Timespan (in minutes) [1-1440]** field—with the Lockout by Username and/or Lockout by IP address option(s) enabled—enter the number of minutes that defines the interval in which a user can enter an incorrect password—as specified in the Allowable Number of Failed Password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

***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 usernames/IP addresses are currently locked out of the Web Filter user interface—and for unlocking usernames and IPs currently locked out of the Web Filter. If the user account is a global (Admin), LDAP group administrator (Sub Admin), or help desk administrator (Help Desk) account, the areas of user interface accessible to that administrator can be viewed.



All 14 Accounts Status

Account Name	Type	Expired Date	Locked
Both	Probe & XStrike	2010/02/14	
CoHelp	Help Desk	2010/03/03	
Cosub	Sub Admin	2010/02/14	
Probe	Probe	2010/02/14	🔒
Testprobe	Probe	2010/03/03	
Testxstrike	XStrike	2010/03/04	
Xstrike	XStrike	2010/01/05	
admin	Probe / XStrike	2010/03/08	
cochau	Admin	2010/02/14	
dota	Admin	2010/04/07	
franklin	Admin	2010/03/03	
superman	Admin	2010/03/07	
test	Admin	2010/02/14	
testgroup	Group	2010/02/14	

Current Locked IP Addresses

20.1.1.1

Fig. 2:1-17 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 Web Filter being configured, including:

- Account Name - username
- Type of account:
  - Admin - global administrator account set up in the Administrator window
  - Sub Admin - LDAP group administrator account set up in the Administrator window
  - Help Desk - help desk administrator account set up in the Administrator window
  - Group - IP group administrator account set up in the IP branch of the Policy 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.

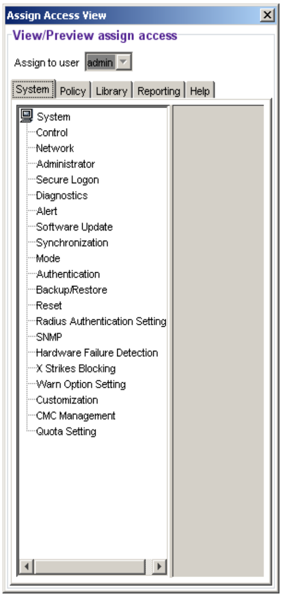
TIP*: Click No to close the dialog box.*

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 User Interface Access

To view the areas of the user interface accessible by a global administrator, LDAP group administrator, or help desk administrator:

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



Assign to user admin

Fig. 2:1-18 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, Policy, Library, Report, Help) to view menu topics, sub-topics, and branches of trees available to that administrator.

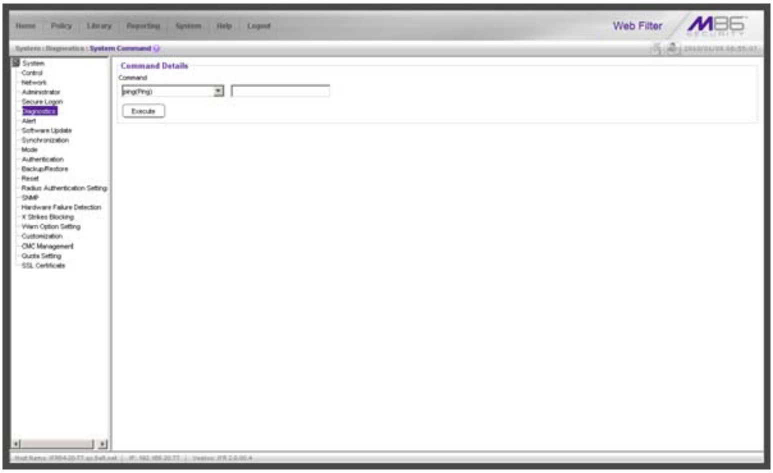
4. Click the “X” in the upper right corner of the window to close it.

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.

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.



Command Details

Command: ping(Ping)

Fig. 2:1-19 System Command window

WARNING: *Diagnostics tools utilize system resources, impacting the WFR’s performance.*

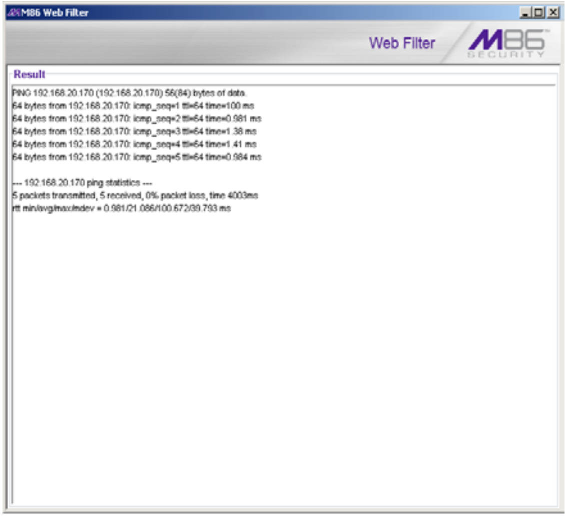
Perform a Diagnostic Test, View Data

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:



```
PING 192.168.20.170 (192.168.20.170) 56(84) bytes of data.
64 bytes from 192.168.20.170: icmp_seq=1 ttl=64 time=100 ms
64 bytes from 192.168.20.170: icmp_seq=2 ttl=64 time=0.981 ms
64 bytes from 192.168.20.170: icmp_seq=3 ttl=64 time=1.38 ms
64 bytes from 192.168.20.170: icmp_seq=4 ttl=64 time=1.41 ms
64 bytes from 192.168.20.170: icmp_seq=5 ttl=64 time=0.984 ms

--- 192.168.20.170 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 0.981/21.086/100.672/39.793 ms
```

Fig. 2:1-20 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 Web Filter 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 WFR.

System uptime

The System uptime diagnostic tool is used for showing the amount of time the WFR 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 WFR has been up, the number of users, and the load averages for the past 1, 5 and 15 minute intervals.

df(disk usage)

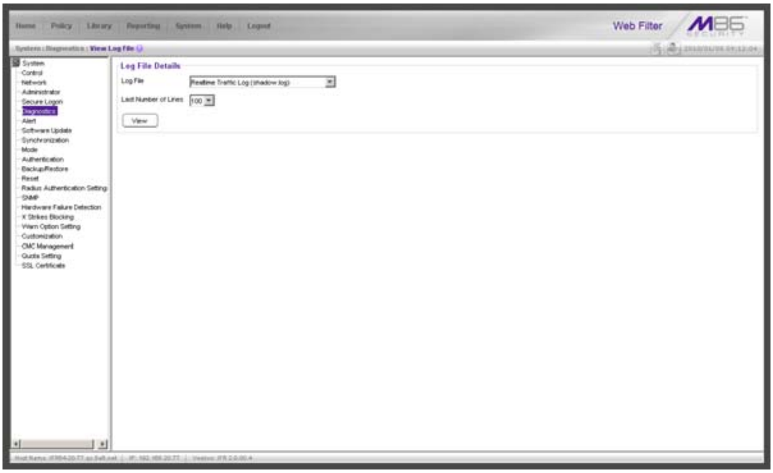
The Disk Usage diagnostic tool is used for viewing disk usage information by file system. When **Execute** is clicked, rows of disk information display in the Result pop-up window, including the following information for each disk: Filesystem name, 1K-blocks on the disk, number of Used blocks, number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



Log File Details

Log File: Realtime Traffic Log (shadow.log)

Last Number of Lines: 100

Fig. 2:1-21 View Log File window

View Log Results

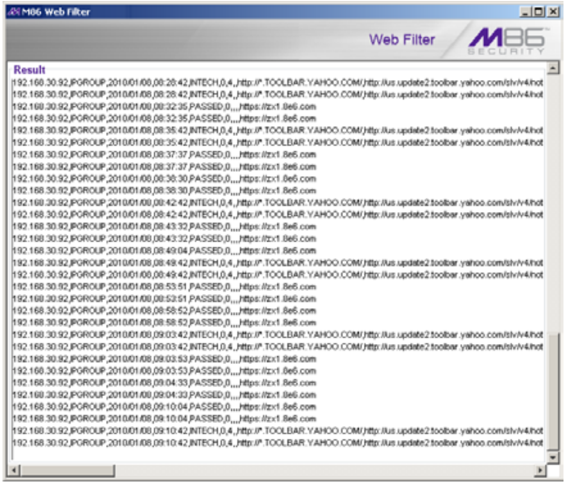
In the Log File Details frame:

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.
   - “Software Update 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 Web Filter console.

***NOTE**: For information about the "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 M86 Web Filter 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:



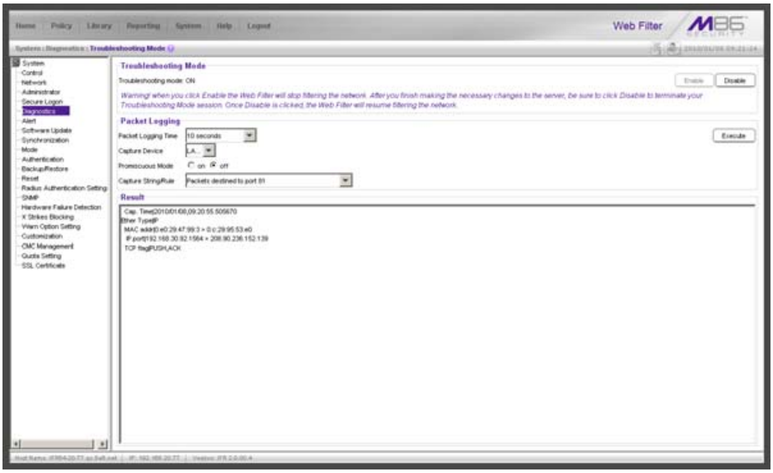
```
192.168.30.92,IPGROUP,2010/01/08,08:28:42,INTECH,0,4,,http://*.TOOLBAR.YAHOO.COM/,http://us.update2.toolbar.yahoo.com/slv/v4/hot
192.168.30.92,IPGROUP,2010/01/08,08:28:42,INTECH,0,4,,http://*.TOOLBAR.YAHOO.COM/,http://us.update2.toolbar.yahoo.com/slv/v4/hot
192.168.30.92,IPGROUP,2010/01/08,08:32:35,PASSED,0,,,,https://zx1.8e6.com
192.168.30.92,IPGROUP,2010/01/08,08:32:35,PASSED,0,,,,https://zx1.8e6.com
192.168.30.92,IPGROUP,2010/01/08,08:35:42,INTECH,0,4,,http://*.TOOLBAR.YAHOO.COM/,http://us.update2.toolbar.yahoo.com/slv/v4/hot
192.168.30.92,IPGROUP,2010/01/08,08:35:42,INTECH,0,4,,http://*.TOOLBAR.YAHOO.COM/,http://us.update2.toolbar.yahoo.com/slv/v4/hot
192.168.30.92,IPGROUP,2010/01/08,08:37:37,PASSED,0,,,,https://zx1.8e6.com
192.168.30.92,IPGROUP,2010/01/08,08:37:37,PASSED,0,,,,https://zx1.8e6.com
192.168.30.92,IPGROUP,2010/01/08,08:38:30,PASSED,0,,,,https://zx1.8e6.com
192.168.30.92,IPGROUP,2010/01/08,08:38:30,PASSED,0,,,,https://zx1.8e6.com
192.168.30.92,IPGROUP,2010/01/08,08:42:42,INTECH,0,4,,http://*.TOOLBAR.YAHOO.COM/,http://us.update2.toolbar.yahoo.com/slv/v4/hot
192.168.30.92,IPGROUP,2010/01/08,08:42:42,INTECH,0,4,,http://*.TOOLBAR.YAHOO.COM/,http://us.update2.toolbar.yahoo.com/slv/v4/hot
192.168.30.92,IPGROUP,2010/01/08,08:43:32,PASSED,0,,,,https://zx1.8e6.com
192.168.30.92,IPGROUP,2010/01/08,08:43:32,PASSED,0,,,,https://zx1.8e6.com
192.168.30.92,IPGROUP,2010/01/08,08:49:04,PASSED,0,,,,https://zx1.8e6.com
192.168.30.92,IPGROUP,2010/01/08,08:49:42,INTECH,0,4,,http://*.TOOLBAR.YAHOO.COM/,http://us.update2.toolbar.yahoo.com/slv/v4/hot
192.168.30.92,IPGROUP,2010/01/08,08:49:42,INTECH,0,4,,http://*.TOOLBAR.YAHOO.COM/,http://us.update2.toolbar.yahoo.com/slv/v4/hot
192.168.30.92,IPGROUP,2010/01/08,08:53:51,PASSED,0,,,,https://zx1.8e6.com
192.168.30.92,IPGROUP,2010/01/08,08:53:51,PASSED,0,,,,https://zx1.8e6.com
192.168.30.92,IPGROUP,2010/01/08,08:58:52,PASSED,0,,,,https://zx1.8e6.com
192.168.30.92,IPGROUP,2010/01/08,08:58:52,PASSED,0,,,,https://zx1.8e6.com
192.168.30.92,IPGROUP,2010/01/08,09:03:42,INTECH,0,4,,http://*.TOOLBAR.YAHOO.COM/,http://us.update2.toolbar.yahoo.com/slv/v4/hot
192.168.30.92,IPGROUP,2010/01/08,09:03:42,INTECH,0,4,,http://*.TOOLBAR.YAHOO.COM/,http://us.update2.toolbar.yahoo.com/slv/v4/hot
192.168.30.92,IPGROUP,2010/01/08,09:03:53,PASSED,0,,,,https://zx1.8e6.com
192.168.30.92,IPGROUP,2010/01/08,09:03:53,PASSED,0,,,,https://zx1.8e6.com
192.168.30.92,IPGROUP,2010/01/08,09:04:33,PASSED,0,,,,https://zx1.8e6.com
192.168.30.92,IPGROUP,2010/01/08,09:04:33,PASSED,0,,,,https://zx1.8e6.com
192.168.30.92,IPGROUP,2010/01/08,09:10:04,PASSED,0,,,,https://zx1.8e6.com
192.168.30.92,IPGROUP,2010/01/08,09:10:04,PASSED,0,,,,https://zx1.8e6.com
192.168.30.92,IPGROUP,2010/01/08,09:10:42,INTECH,0,4,,http://*.TOOLBAR.YAHOO.COM/,http://us.update2.toolbar.yahoo.com/slv/v4/hot
192.168.30.92,IPGROUP,2010/01/08,09:10:42,INTECH,0,4,,http://*.TOOLBAR.YAHOO.COM/,http://us.update2.toolbar.yahoo.com/slv/v4/hot
```

Fig. 2:1-22 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.



Troubleshooting Mode

Troubleshooting mode: ON

Warning! when you click Enable the Web Filter 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 Web Filter will resume filtering the network.

Packet Logging

Packet Logging Time: 10 seconds

Capture Device: LA...

Promiscuous Mode: ○ on ● off

Capture String/Rule: Packets destined to port 81

Result

```
Cap. Time[2010/01/08,09:20:55.505670
Ether Type[IP
MAC addr[0:e0:29:47:99:3 > 0:c:29:95:53:e0
IP port[192.168.30.92.1564 > 208.90.236.152:139
TCP flag[PUSH,ACK
```

Fig. 2:1-23 Troubleshooting Mode window

***WARNING:** This tool utilizes system resources, impacting the WFR’s performance. When you click Enable, the Web Filter 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 Web Filter will resume filtering the network.*

***NOTE**: See the Operation Mode window for information about invisible, router, and firewall modes, and listening devices.*

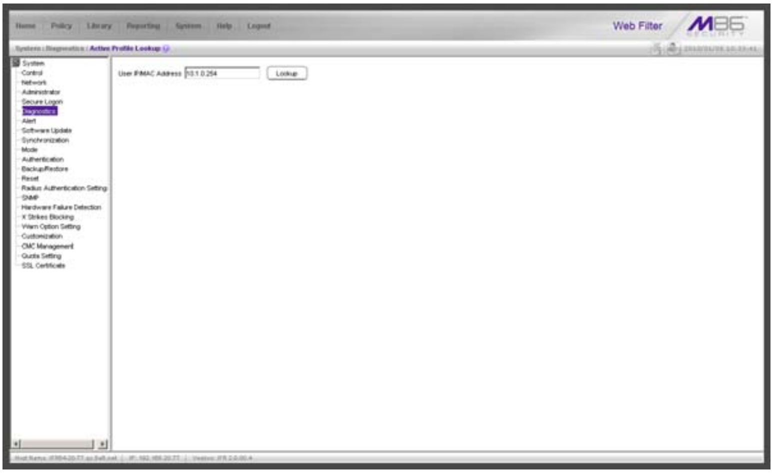
Use the Troubleshooting Mode

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 Web Filter will watch all network traffic as in the invisible mode. If “off” is selected, the Web Filter will only capture packets sent to or from the Web Filter.
6. At the **Capture String/Rule** field, select the type of packets to be captured: Transmission Control Protocol (TCP); packets destined to a specified port (80, 443, 81); packets destined to the Web Filter; packets sent to or from port 20 or 21; packets sent to the Virtual IP address’s port 137 or 139, or Address Resolution Protocol (ARP).
7. Click **Execute** to display results in the Result list box.

8. After performing the fixes on the Web Filter, 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. This window also is used for troubleshooting synchronization on "target" Web Filters, to verify whether settings for user profiles match the ones synced over from the "source" Web Filter.



User IP/MAC Address 10.1.0.254

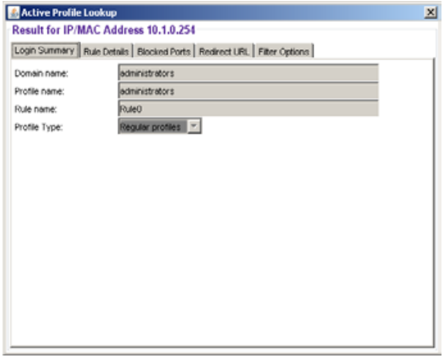
Fig. 2:1-24 Active Profile Lookup window

***NOTE**: In order to use this diagnostic tool, IP groups and/or members must be set up in the Policy section of the Web Filter, and each IP group and/or member must have a filtering profile. MAC addresses are used in the mobile mode only.*

Verify Whether a Profile is Active

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

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

   Result for IP/MAC Address 10.1.0.254

   Domain name: administrators

   Profile name: administrators

   Rule name: Rule0

   Profile Type: Regular profiles

   Fig. 2:1-25 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
   - additional profile information:
     - **Time profile name** - for time profiles, the name of the time profile displays
     - **Rule name** - if this profile uses a non-custom rule, the rule number displays
   - **Profile Type** - type of profile, greyed-out:
     - Regular profiles - IP group, sub-group, individual, or MAC profile

- Global profile - Global Group Profile
- Override profiles - Override Account profile
- Lock profiles - X Strikes Blocking lock out profile
- Time profiles - Time Profile
- TAR profile - Threat Analysis Reporter lock out profile
- Radius profile - Radius accounting server profile

***NOTE**: See the M86 Web Filter Authentication User Guide for information that displays in these fields if the domain is an LDAP domain.*

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/Bing/Yahoo!/Youtube/Ask/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.

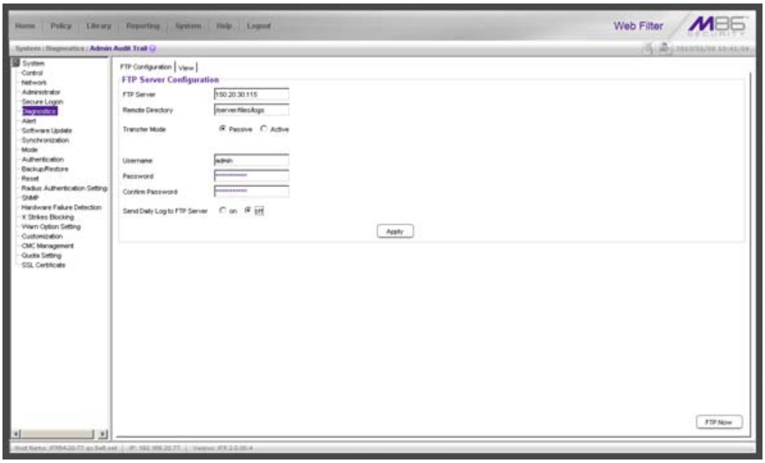
4. Click the "X" in the upper right corner of the pop-up box to close it.

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:



FTP Server Configuration

FTP Server: 150.20.30.115

Remote Directory: /server/files/logs

Transfer Mode: ● Passive ○ Active

Username: admin

Password: ************

Confirm Password: ************

Send Daily Log to FTP Server: ○ on ● off

Fig. 2:1-26 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.

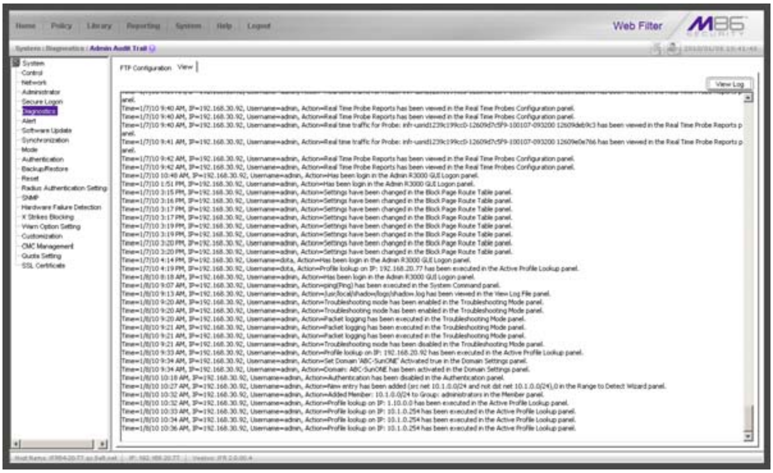
FTP the Log on Demand

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

View

View the Log of Administrator Changes

To view the log, click the View tab:



```
anel.
Time=1/7/10 9:40 AM, IP=192.168.30.92, Username=admin, Action=Real Time Probe Reports has been viewed in the Real Time Probes Configuration panel.
Time=1/7/10 9:40 AM, IP=192.168.30.92, Username=admin, Action=Real Time Probe Reports has been viewed in the Real Time Probes Configuration panel.
Time=1/7/10 9:40 AM, IP=192.168.30.92, Username=admin, Action=Real time traffic for Probe: infr-usrid1239c199cc0-12609d7c5f9-100107-093200 12609deb9c3 has been viewed in the Real Time Probe Reports p
anel.
Time=1/7/10 9:41 AM, IP=192.168.30.92, Username=admin, Action=Real time traffic for Probe: infr-usrid1239c199cc0-12609d7c5f9-100107-093200 12609e0e766 has been viewed in the Real Time Probe Reports p
anel.
Time=1/7/10 9:42 AM, IP=192.168.30.92, Username=admin, Action=Real Time Probe Reports has been viewed in the Real Time Probes Configuration panel.
Time=1/7/10 9:42 AM, IP=192.168.30.92, Username=admin, Action=Real Time Probe Reports has been viewed in the Real Time Probes Configuration panel.
Time=1/7/10 10:40 AM, IP=192.168.30.92, Username=admin, Action=Has been login in the Admin R3000 GUI Logon panel.
Time=1/7/10 1:51 PM, IP=192.168.30.92, Username=admin, Action=Has been login in the Admin R3000 GUI Logon panel.
Time=1/7/10 3:15 PM, IP=192.168.30.92, Username=admin, Action=Settings have been changed in the Block Page Route Table panel.
Time=1/7/10 3:16 PM, IP=192.168.30.92, Username=admin, Action=Settings have been changed in the Block Page Route Table panel.
Time=1/7/10 3:17 PM, IP=192.168.30.92, Username=admin, Action=Settings have been changed in the Block Page Route Table panel.
Time=1/7/10 3:17 PM, IP=192.168.30.92, Username=admin, Action=Settings have been changed in the Block Page Route Table panel.
Time=1/7/10 3:19 PM, IP=192.168.30.92, Username=admin, Action=Settings have been changed in the Block Page Route Table panel.
Time=1/7/10 3:19 PM, IP=192.168.30.92, Username=admin, Action=Settings have been changed in the Block Page Route Table panel.
Time=1/7/10 3:20 PM, IP=192.168.30.92, Username=admin, Action=Settings have been changed in the Block Page Route Table panel.
Time=1/7/10 3:20 PM, IP=192.168.30.92, Username=admin, Action=Settings have been changed in the Block Page Route Table panel.
Time=1/7/10 4:14 PM, IP=192.168.30.92, Username=dota, Action=Has been login in the Admin R3000 GUI Logon panel.
Time=1/7/10 4:19 PM, IP=192.168.30.92, Username=dota, Action=Profile lookup on IP: 192.168.20.77 has been executed in the Active Profile Lookup panel.
Time=1/8/10 8:18 AM, IP=192.168.30.92, Username=admin, Action=Has been login in the Admin R3000 GUI Logon panel.
Time=1/8/10 9:07 AM, IP=192.168.30.92, Username=admin, Action=ping(Ping) has been executed in the System Command panel.
Time=1/8/10 9:13 AM, IP=192.168.30.92, Username=admin, Action=/usr/local/shadow/logs/shadow.log has been viewed in the View Log File panel.
Time=1/8/10 9:20 AM, IP=192.168.30.92, Username=admin, Action=Troubleshooting mode has been enabled in the Troubleshooting Mode panel.
Time=1/8/10 9:20 AM, IP=192.168.30.92, Username=admin, Action=Troubleshooting mode has been enabled in the Troubleshooting Mode panel.
Time=1/8/10 9:20 AM, IP=192.168.30.92, Username=admin, Action=Packet logging has been executed in the Troubleshooting Mode panel.
Time=1/8/10 9:21 AM, IP=192.168.30.92, Username=admin, Action=Packet logging has been executed in the Troubleshooting Mode panel.
Time=1/8/10 9:21 AM, IP=192.168.30.92, Username=admin, Action=Packet logging has been executed in the Troubleshooting Mode panel.
Time=1/8/10 9:21 AM, IP=192.168.30.92, Username=admin, Action=Troubleshooting mode has been disabled in the Troubleshooting Mode panel.
Time=1/8/10 9:33 AM, IP=192.168.30.92, Username=admin, Action=Profile lookup on IP: 192.168.20.92 has been executed in the Active Profile Lookup panel.
Time=1/8/10 9:34 AM, IP=192.168.30.92, Username=admin, Action=Set Domain 'ABC-SunONE' Activated true in the Domain Settings panel.
Time=1/8/10 9:34 AM, IP=192.168.30.92, Username=admin, Action=Domain: ABC-SunONE has been activated in the Domain Settings panel.
Time=1/8/10 10:18 AM, IP=192.168.30.92, Username=admin, Action=Authentication has been disabled in the Authentication panel.
Time=1/8/10 10:27 AM, IP=192.168.30.92, Username=admin, Action=New entry has been added (src net 10.1.0.0/24 and not dst net 10.1.0.0/24),0 in the Range to Detect Wizard panel.
Time=1/8/10 10:32 AM, IP=192.168.30.92, Username=admin, Action=Added Member: 10.1.0.0/24 to Group: administrators in the Member panel.
Time=1/8/10 10:32 AM, IP=192.168.30.92, Username=admin, Action=Profile lookup on IP: 1.10.0.0 has been executed in the Active Profile Lookup panel.
Time=1/8/10 10:33 AM, IP=192.168.30.92, Username=admin, Action=Profile lookup on IP: 10.1.0.254 has been executed in the Active Profile Lookup panel.
Time=1/8/10 10:34 AM, IP=192.168.30.92, Username=admin, Action=Profile lookup on IP: 10.1.0.254 has been executed in the Active Profile Lookup panel.
Time=1/8/10 10:36 AM, IP=192.168.30.92, Username=admin, Action=Profile lookup on IP: 10.1.0.254 has been executed in the Active Profile Lookup panel.
```

Fig. 2:1-27 Admin Audit Trail window, View tab

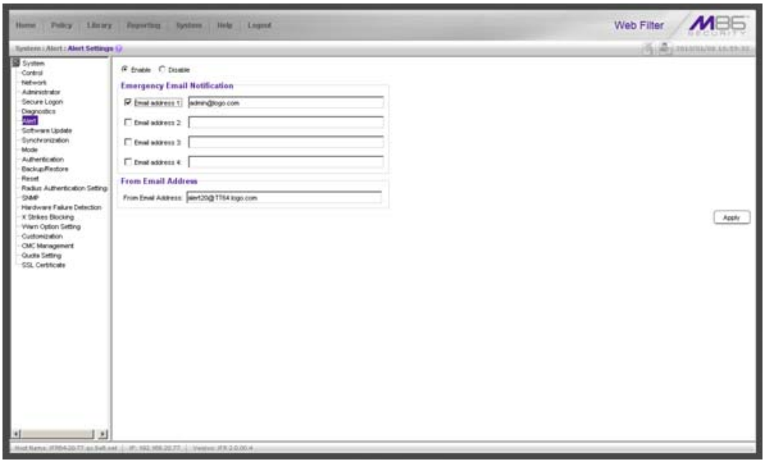
Click **View Log** to display data on recent activity. For each change made on the server, the log will contain the date and time the change was made (Time), IP address of the machine used by the administrator, administrator's Username, and a brief description of the Action performed on the server.

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.

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 WFR's self-monitoring process.



● Enable ○ Disable

Emergency Email Notification

☑ Email address 1: admin@logo.com

☐ Email address 2:

☐ Email address 3:

☐ Email address 4:

From Email Address

From Email Address: alert20@TT64.logo.com

Fig. 2:1-28 Alert Settings window

The following processes are monitored by the WFR:

- **CPU Processes** - If any CPU process fails to run, the WFR 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 intervention 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 WFR repeats this procedure until an administrator fixes the error.

- **Hard Drive Utilization** - If the WFR detects that hard drive utilization exceeds 80 percent, an alert is sent to the administrator. This problem usually occurs if the Web Filter is unable to transfer log files to the M86 Security Reporter. Action should be taken to prevent the hard drive from reaching 100 percent utilization.
- **Log File Transmission** - If the Web Filter is unable to send log files as scheduled to the SR, 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.
- **Synchronization Errors** - If the synchronization feature is used, an alert is sent to the administrator if a Web Filter set up in the Source mode cannot communicate with the target server(s) after numerous attempts, or if a Web Filter set up in the Target mode cannot communicate with the source server. 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 WFR in the **From Email Address** field.
5. Click **Apply** to apply your settings.

Modify Alert Settings

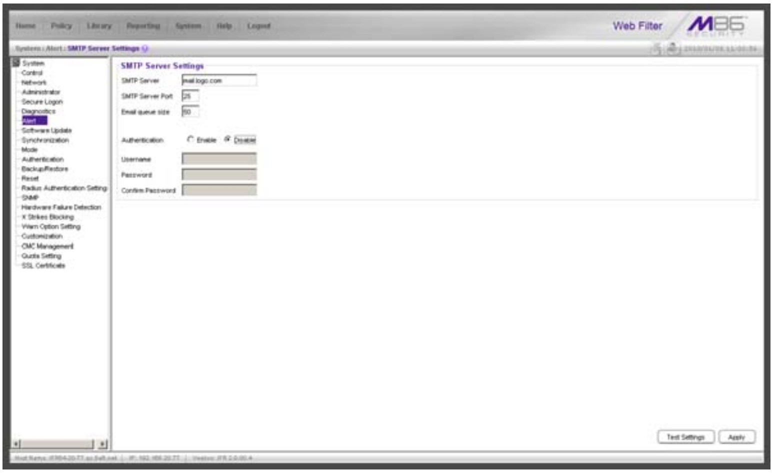
1. Make any of the following edits in the Emergency Email Notification frame:
   - change an email address by typing the new one over the existing one
   - deactivate a contact by removing the check mark from the checkbox corresponding to that contact’s email address
   - delete a contact by using your 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.



SMTP Server Settings

SMTP Server: mail.logo.com

SMTP Server Port: 25

Email queue size: 50

Authentication ○ Enable ● Disable

Username:

Password:

Confirm Password:

Fig. 2:1-29 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**.

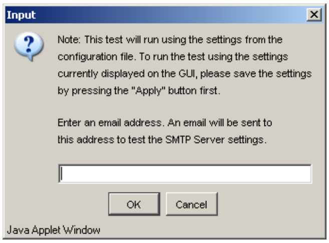
   b. Enter the **Password** and make the same entry in the **Confirm Password** field.

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:



Note: This test will run using the settings from the configuration file. To run the test using the settings currently displayed on the GUI, please save the settings by pressing the "Apply" button first.

Enter an email address. An email will be sent to this address to test the SMTP Server settings.

Fig. 2:1-30 SMTP Test Settings box

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

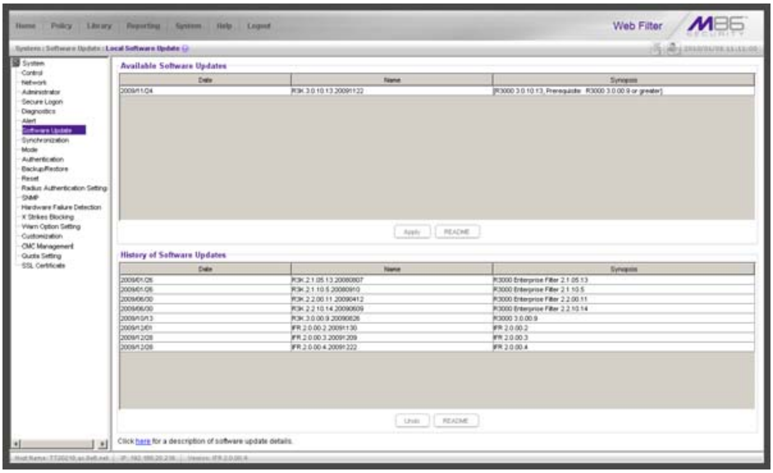
3. Click **OK** to close the pop-up box and to process your request. If all SMTP Server Settings are accepted, the test email should be received at the specified address.

Software Update

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

Local Software Update window

The Local Software Update window displays when Local Software Update is selected from the Software Update 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.



Available Software Updates

Date	Name	Synopsis
2009/11/04	R3K 3.0.10.13.20091122	[R3000 3.0.10.13, Prerequisite: R3000 3.0.00.9 or greater]

History of Software Updates

Date	Name	Synopsis
2009/01/26	R3K 2.1.05.13.20080807	R3000 Enterprise Filter 2.1.05.13
2009/01/26	R3K 2.1.10.5.20080910	R3000 Enterprise Filter 2.1.10.5
2009/06/30	R3K 2.2.00.11.20090412	R3000 Enterprise Filter 2.2.00.11
2009/06/30	R3K 2.2.10.14.20090609	R3000 Enterprise Filter 2.2.10.14
2009/10/13	R3K 3.0.00.9.20090826	R3000 3.0.00.9
2009/12/01	IFR 2.0.00.2.20091130	IFR 2.0.00.2
2009/12/08	IFR 2.0.00.3.20091209	IFR 2.0.00.3
2009/12/08	IFR 2.0.00.4.20091222	IFR 2.0.00.4

Click here for a description of software update details.

Fig. 2:1-31 Local Software Update window

***NOTE**: Available software updates come from downloads made to the server via Traveler, M86's executable program that can run on demand, or be set to run at a scheduled time.*

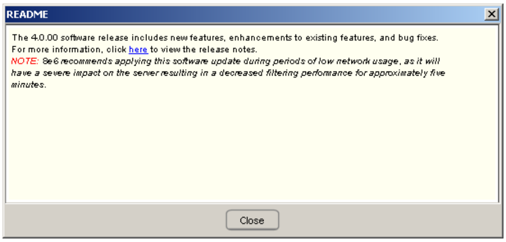
***TIP**: Click the link (“here”) at the bottom of the window to go to the Web page at M86 Security’s public site (**http://www.m86security.com/support/wfr/upgrade.asp**) where release notes about software updates can be obtained.*

Read Information about a Software Update

In either the Available Software Updates frame or the History of Software Updates 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:



The 4.0.00 software release includes new features, enhancements to existing features, and bug fixes.
For more information, click here to view the release notes.
NOTE: 8e6 recommends applying this software update during periods of low network usage, as it will have a severe impact on the server resulting in a decreased filtering perfomance for approximately five minutes.

Fig. 2:1-32 Software update Readme

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

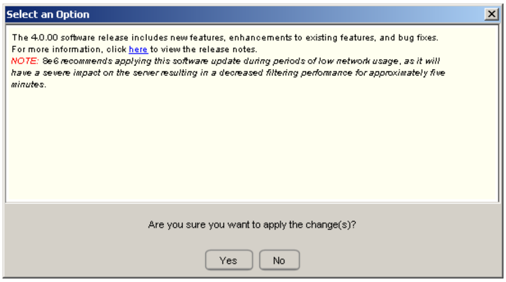
Select and Apply a Software Update

To apply a software update:

1. Go to the Available Software Updates 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:



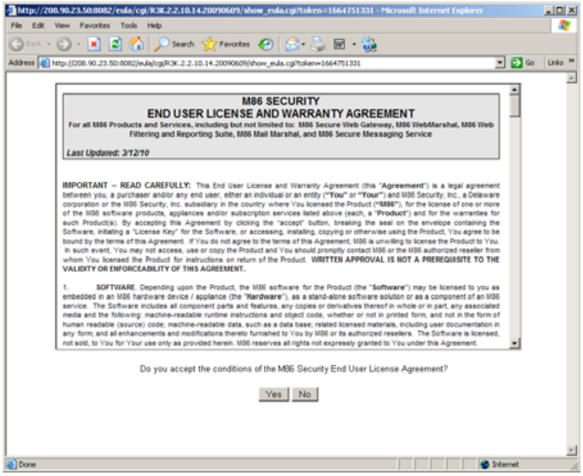
Select an Option

The 4.0.00 software release includes new features, enhancements to existing features, and bug fixes. For more information, click here to view the release notes.
NOTE: 8e6 recommends applying this software update during periods of low network usage, as it will have a severe impact on the server resulting in a decreased filtering performance for approximately five minutes.

Are you sure you want to apply the change(s)?

Fig. 2:1-33 Software update installation dialog box

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



http://208.90.23.50:8082/eula/cgi/R3K.2.2.10.14.20090609/show_eula.cgi?token=1664751331 - Microsoft Internet Explorer

http://208.90.23.50:8082/eula/cgi/R3K.2.2.10.14.20090609/show_eula.cgi?token=1664751331

M86 SECURITY
END USER LICENSE AND WARRANTY AGREEMENT
For all M86 Products and Services, including but not limited to: M86 Secure Web Gateway, M86 WebMarshal, M86 Web Filtering and Reporting Suite, M86 Mail Marshal, and M86 Secure Messaging Service

Last Updated: 3/12/10

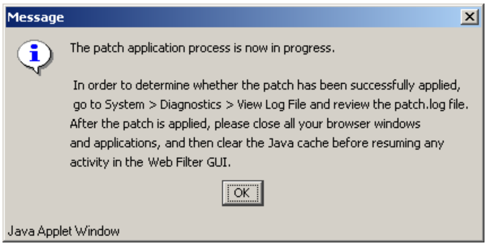
IMPORTANT – READ CAREFULLY: This End User License and Warranty Agreement (this "**Agreement**") is a legal agreement between you, a purchaser and/or any end user, either an individual or an entity ("**You**" or "**Your**") and M86 Security, Inc., a Delaware corporation or the M86 Security, Inc. subsidiary in the country where You licensed the Product ("**M86**"), for the license of one or more of the M86 software products, appliances and/or subscription services listed above (each, a "**Product**") and for the warranties for such Product(s). By accepting this Agreement by clicking the "accept" button, breaking the seal on the envelope containing the Software, initiating a "License Key" for the Software, or accessing, installing, copying or otherwise using the Product, You agree to be bound by the terms of this Agreement. If You do not agree to the terms of this Agreement, M86 is unwilling to license the Product to You. In such event, You may not access, use or copy the Product and You should promptly contact M86 or the M86 authorized reseller from whom You licensed the Product for instructions on return of the Product. **WRITTEN APPROVAL IS NOT A PREREQUISITE TO THE VALIDITY OR ENFORCEABILITY OF THIS AGREEMENT.**

1. **SOFTWARE**. Depending upon the Product, the M86 software for the Product (the "**Software**") may be licensed to you as embedded in an M86 hardware device / appliance (the "**Hardware**"), as a stand-alone software solution or as a component of an M86 service. The Software includes all component parts and features, any copies or derivatives thereof in whole or in part, any associated media and the following: machine-readable runtime instructions and object code, whether or not in printed form, and not in the form of human readable (source) code; machine-readable data, such as a data base; related licensed materials, including user documentation in any form; and all enhancements and modifications thereto furnished to You by M86 or its authorized resellers. The Software is licensed, not sold, to You for Your use only as provided herein. M86 reserves all rights not expressly granted to You under this Agreement.

Do you accept the conditions of the M86 Security End User License Agreement?

Fig. 2:1-34 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:



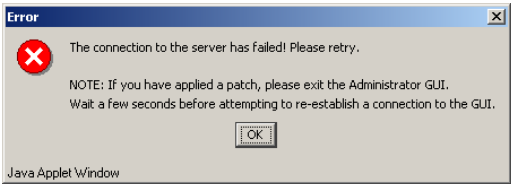
The patch application process is now in progress.

In order to determine whether the patch has been successfully applied, go to System > Diagnostics > View Log File and review the patch.log file. After the patch is applied, please close all your browser windows and applications, and then clear the Java cache before resuming any activity in the Web Filter GUI.

Fig. 2:1-35 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 “Software Update 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 WFR has been lost due to the software update application:



The connection to the server has failed! Please retry.

NOTE: If you have applied a patch, please exit the Administrator GUI. Wait a few seconds before attempting to re-establish a connection to the GUI.

Fig. 2:1-36 Connection failure alert box

6. Click **OK** to close the alert box.
7. In the navigation toolbar, click **Quit** to exit the Web Filter console.
8. Wait a few minutes, and then log back into the Web Filter console again.

***NOTE**: M86 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.*

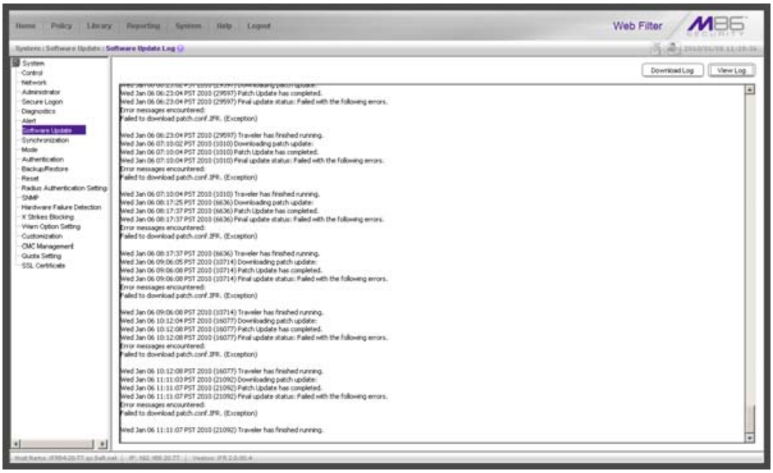
***WARNING**: If a software update is uninstalled, configuration settings will revert to the previous settings, before the software update was applied.*

To unapply a software update:

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

Software Update Log window

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



```
Wed Jan 06 06:23:04 PST 2010 (29597) Patch Update has completed.
Wed Jan 06 06:23:04 PST 2010 (29597) Final update status: Failed with the following errors.
Error messages encountered:
Failed to download patch.conf.JPR. (Exception)

Wed Jan 06 06:23:04 PST 2010 (29597) Traveler has finished running.
Wed Jan 06 07:10:02 PST 2010 (1010) Downloading patch update:
Wed Jan 06 07:10:04 PST 2010 (1010) Patch Update has completed.
Wed Jan 06 07:10:04 PST 2010 (1010) Final update status: Failed with the following errors.
Error messages encountered:
Failed to download patch.conf.JPR. (Exception)

Wed Jan 06 07:10:04 PST 2010 (1010) Traveler has finished running.
Wed Jan 06 08:17:25 PST 2010 (6636) Downloading patch update:
Wed Jan 06 08:17:37 PST 2010 (6636) Patch Update has completed.
Wed Jan 06 08:17:37 PST 2010 (6636) Final update status: Failed with the following errors.
Error messages encountered:
Failed to download patch.conf.JPR. (Exception)

Wed Jan 06 08:17:37 PST 2010 (6636) Traveler has finished running.
Wed Jan 06 09:06:05 PST 2010 (10714) Downloading patch update:
Wed Jan 06 09:06:08 PST 2010 (10714) Patch Update has completed.
Wed Jan 06 09:06:08 PST 2010 (10714) Final update status: Failed with the following errors.
Error messages encountered:
Failed to download patch.conf.JPR. (Exception)

Wed Jan 06 09:06:08 PST 2010 (10714) Traveler has finished running.
Wed Jan 06 10:12:04 PST 2010 (16077) Downloading patch update:
Wed Jan 06 10:12:08 PST 2010 (16077) Patch Update has completed.
Wed Jan 06 10:12:08 PST 2010 (16077) Final update status: Failed with the following errors.
Error messages encountered:
Failed to download patch.conf.JPR. (Exception)

Wed Jan 06 10:12:08 PST 2010 (16077) Traveler has finished running.
Wed Jan 06 11:11:03 PST 2010 (21092) Downloading patch update:
Wed Jan 06 11:11:07 PST 2010 (21092) Patch Update has completed.
Wed Jan 06 11:11:07 PST 2010 (21092) Final update status: Failed with the following errors.
Error messages encountered:
Failed to download patch.conf.JPR. (Exception)

Wed Jan 06 11:11:07 PST 2010 (21092) Traveler has finished running.
```

Fig. 2:1-37 Software 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, select the “save” option; this action opens the window on your workstation where you specify the filename for the file and where to save the file.
3. Select 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.

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

4. After the file has successfully downloaded to your workstation, click **OK** to close the alert box asking you to verify that the software update log file was successfully saved.

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:

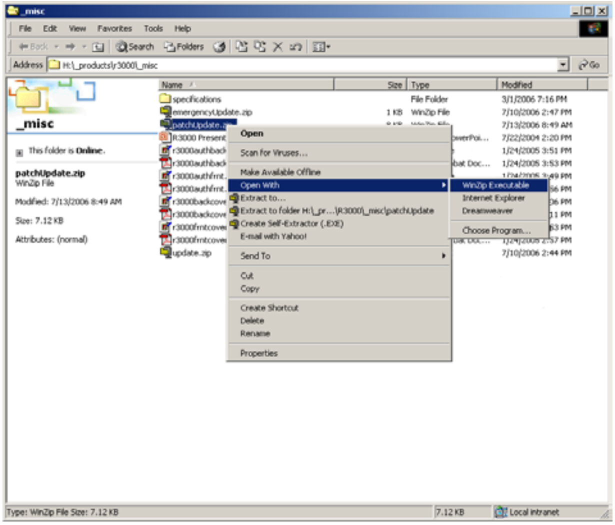
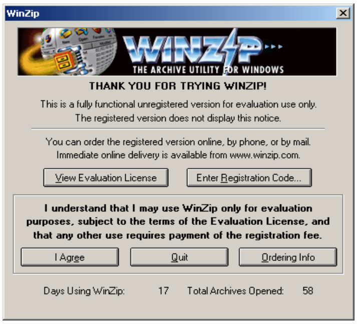

_misc
File Edit View Favorites Tools Help
Back Search Folders
Address H:_products\r3000_misc
Go
_misc
This folder is Online.
patchUpdate.zip
WinZip File
Modified: 7/13/2006 8:49 AM
Size: 7.12 KB
Attributes: (normal)
Name Size Type Modified
specifications File Folder 3/1/2006 7:16 PM
emergencyUpdate.zip 1 KB WinZip File 7/10/2006 2:47 PM
patchUpdate.zip 7/13/2006 8:49 AM
R3000 Present 7/22/2004 2:20 PM
r3000authback 1/24/2005 3:51 PM
r3000authback 1/24/2005 3:53 PM
r3000authfmt
r3000authfmt
r3000backcove
r3000backcove
r3000fmtcover
r3000fmtcover
update.zip 7/10/2006 2:44 PM
Open
Scan for Viruses...
Make Available Offline
Open With
Extract to...
Extract to folder H:_pr...\R3000_misc\patchUpdate
Create Self-Extractor (.EXE)
E-mail with Yahoo!
Send To
Cut
Copy
Create Shortcut
Delete
Rename
Properties
WinZip Executable
Internet Explorer
Dreamweaver
Choose Program...
Type: WinZip File Size: 7.12 KB
7.12 KB
Local intranet

Fig. 2:1-38 Folder containing downloaded file

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



THANK YOU FOR TRYING WINZIP!

This is a fully functional unregistered version for evaluation use only. The registered version does not display this notice.

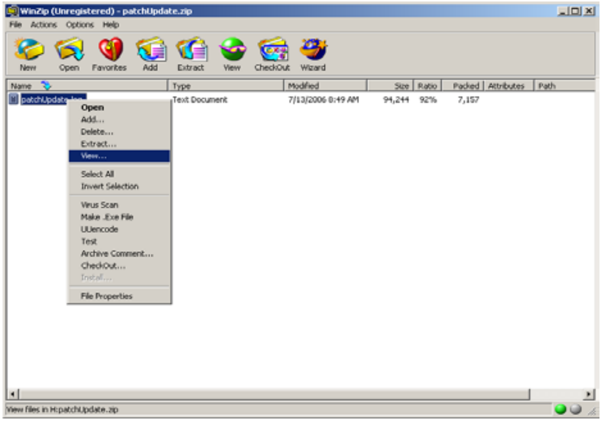
You can order the registered version online, by phone, or by mail. Immediate online delivery is available from www.winzip.com.

I understand that I may use WinZip only for evaluation purposes, subject to the terms of the Evaluation License, and that any other use requires payment of the registration fee.

Days Using WinZip: 17 Total Archives Opened: 58

Fig. 2:1-39 WinZip Executable program

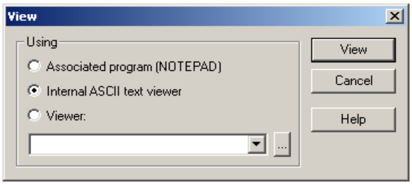
3. If using WinZip, click **I Agree** to open the window containing the zip file:



Name	Type	Modified	Size	Ratio	Packed	Attributes	Path
patchUpdate.log	Text Document	7/13/2006 8:49 AM	94,244	92%	7,157		

Fig. 2:1-40 WinZip window

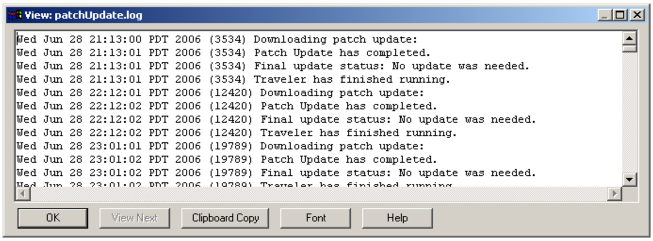
4. Right-click the zip file to open the pop-up menu, and choose “View” to open the View dialog box:



Using
○ Associated program (NOTEPAD)
● Internal ASCII text viewer
○ Viewer:

Fig. 2:1-41 View dialog box

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



```
Wed Jun 28 21:13:00 PDT 2006 (3534) Downloading patch update:
Wed Jun 28 21:13:01 PDT 2006 (3534) Patch Update has completed.
Wed Jun 28 21:13:01 PDT 2006 (3534) Final update status: No update was needed.
Wed Jun 28 21:13:01 PDT 2006 (3534) Traveler has finished running.
Wed Jun 28 22:12:01 PDT 2006 (12420) Downloading patch update:
Wed Jun 28 22:12:02 PDT 2006 (12420) Patch Update has completed.
Wed Jun 28 22:12:02 PDT 2006 (12420) Final update status: No update was needed.
Wed Jun 28 22:12:02 PDT 2006 (12420) Traveler has finished running.
Wed Jun 28 23:01:01 PDT 2006 (19789) Downloading patch update:
Wed Jun 28 23:01:02 PDT 2006 (19789) Patch Update has completed.
Wed Jun 28 23:01:02 PDT 2006 (19789) Final update status: No update was needed.
Wed Jun 28 23:01:02 PDT 2006 (19789) Traveler has finished running.
```

Fig. 2:1-42 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
3. Paste the contents from the clipboard into the Notepad file.

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

Synchronization

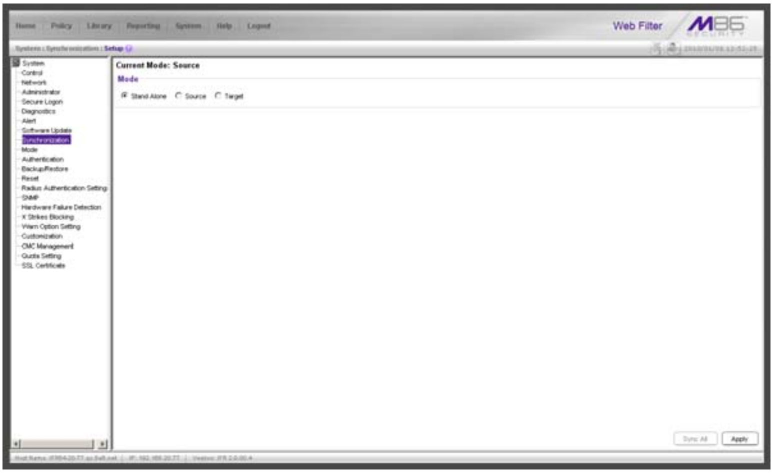
By default, the Synchronization pop-up menu includes the Setup option that lets you specify the Web Filter’s function on the network: whether it will be a stand alone unit, or whether it will send profile/library setting changes to—or receive such setting changes from—another Web Filter. If the Web Filter is set up to either send or receive profile/library setting changes in the aforementioned manner, the menu option for Status also becomes available in the pop-up menu. If the Web Filter is set up to send profile/library setting changes, that Web Filter will function as a Centralized Management Console, and thus the CMC Management topic becomes available in the navigation panel.

***NOTE**: For an overview on synchronization, see Chapter 3: Synchronizing Multiple Units, from the Web Filter Introductory Section.*

***WARNING**: This version of synchronization only supports the use of unique IP addresses throughout a network.*

Setup window

The Setup window displays when Setup is selected from the Synchronization menu. This window is used for establishing the function of the Web Filter, especially if there is more than one Web Filter on the network. When there are multiple Web Filters, it is important to set up one as a "source" server and others as "targets," so that user profiles and/or library settings can be copied to other servers. This process ensures that all servers run in parallel on the network, thereby eliminating the need to manually configure profile and library settings on each server.



Current Mode: Source

Mode

● Stand Alone ○ Source ○ Target

Fig. 2:1-43 Setup window, Stand Alone mode

Using Only One Web Filter on the Network

By default, the “Stand Alone” mode is selected in the Mode frame. This indicates that all settings on the Web Filter that is currently being configured apply only to that Web Filter.

For the Stand Alone mode setting:

1. In the Mode frame, click “Stand Alone”.
2. Click **Apply**.

Using More than One Web Filter on the Network

Using the synchronization process, all target servers are updated with profile/library setting changes, so that no matter which Web Filter the user’s client PC accesses, the user’s Internet session will be appropriately filtered and blocked.

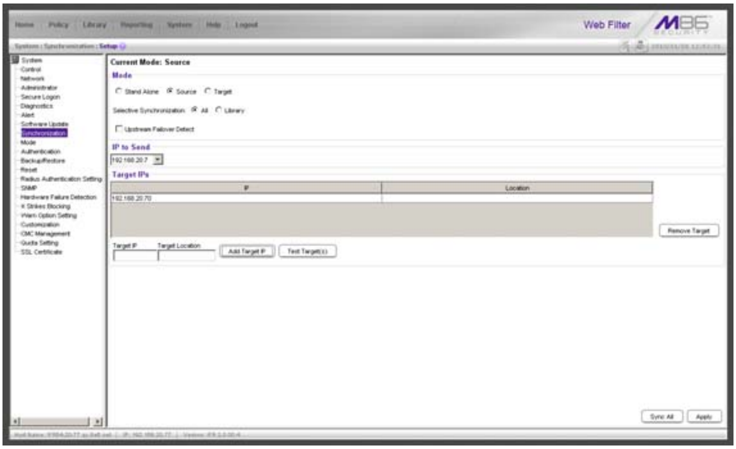
Set up a Web Filter to be a Source Server

A Web Filter configured to be a “source” server will send profile/library setting changes to other Web Filter (“target”) servers.

⚠ ***WARNING****: If a Web Filter is set up in the Source mode with a Network Address Translation (NAT) device between the source and target server(s), be sure that ports 26262, 26268, and 88 are open on the source server. This setup is required so that the source server can communicate with the target server(s).*

For the Source mode setting:

1. In the Mode frame, click “Source” to display the Source mode view:



Current Mode: Source

Mode

○ Stand Alone ● Source ○ Target

Selective Synchronization: ● All ○ Library

□ Upstream Failover Detect

IP to Send

192.168.20.7

Target IPs

IP	Location
192.168.20.70	

Target IP
Target Location

Fig. 2:1-44 Setup window, Source mode

2. At the **Selective Synchronization** field, by default “All” is selected. This choice includes both profile and library setting changes. Choose “Library” if only library category additions/deletions (including search engine keywords and URL keywords additions/deletions)—and not profiles—should be synced to target servers.

3. By default, the “Upstream Failover Detect” checkbox is unpopulated. Click this checkbox if this source server will be set up to detect any failed Web Filter “node” and filter that target server. Using this option, the source server will function as the "upstream" Web Filter and all target servers will function as "downstream" Web Filters.

NOTES*: In order to use the failover detection feature, for each target Web Filter, Appliance Watchdog software release 3.0.00 must first be installed on a separate workstation and set up to watch that Web Filter. Go to* ***http://www.m86security.com/support/Watchdog/upgrade.asp*** *to download this release.*

If using the failover detection feature:

- *Local Filtering on this source server must be enabled*
- *Troubleshooting on this source server must be disabled*
- *The Operation Mode on this source server and all target servers must be set to use the same mode*

- *The mobile mode cannot be used*
- *If “Library” Selective Synchronization is enabled, end users for the failed Web Filter “node” might be given the Global Group Profile instead of their active filtering profiles*
- *If a target server fails, the Range to Detect Settings window displays a Node tab with IP range information for the failed “downstream” server.*

4. In the IP to Send frame, select either the LAN 1 or LAN 2 IP address from the **IP to Send** pull-down menu. This IP address will be used for sending profile/library setting changes to the target server(s).

NOTE*: LAN 1 and LAN 2 IP addresses that display in this menu were previously entered in the LAN Settings window on this server.*

5. In the Target IPs frame, enter the **Target IP** address of the Web Filter that will receive profile/library setting changes from this server being configured.

NOTE*: If a target server is set up with a NAT device, the NAT IP address must be used instead of the target server’s own IP address.*

6. An entry in the **Target Location** field is optional. This alphanumeric entry serves as a label for readily identifying the server being configured.
7. Click **Add Target IP** to include this IP address—and corresponding Location information, if applicable—in the list box.

   The following optional steps can be performed:

   - Follow steps 5 to 7 for each server that should receive profile/library setting changes from this server being configured.
   - Click **Test Target(s)** to open an alert box that provides the server mode status for each IP address you entered. Click **OK** to close the alert box, and make any adjustments, if necessary.

- To remove an IP address from the list box, select it and click **Remove Target**.

***NOTE**: This test only verifies whether this server can contact the target server(s). In order for synchronization to be operable on the network, the target server(s) must also be able to contact this source server being configured.*

8. Click **Apply** after all settings have been made. Note that the CMC Management topic becomes available in the navigation panel for this source server when settings in this window are saved.

Sync All Target Servers with the Same Settings

If all target servers have been configured and now need to be set with the same settings, click **Sync All** from the source server. *This action should only be performed if all target* servers need to have the same user filtering profile/ library settings as the source server.

Two scenarios in which this feature might be used involve restoring backup data to the Web Filter:

- In the first scenario, library configurations from a previous date in time are restored to the source server, and each target server needs to have these same library configurations as well. Sync All should be clicked after entries are made in the Backup/Restore window.
- In the second scenario, the source server has failed and needs to be replaced with another server. One of the target servers is promoted to function as the new source server. The newly designated source server should be updated with the most recent configurations, via the latest valid backup from the failed source server. Once this data is restored to the new source server, each target server should be sent these same library configurations using the Sync All button.

***NOTE**: See the Backup/Restore window for information on restoring data to a server.*

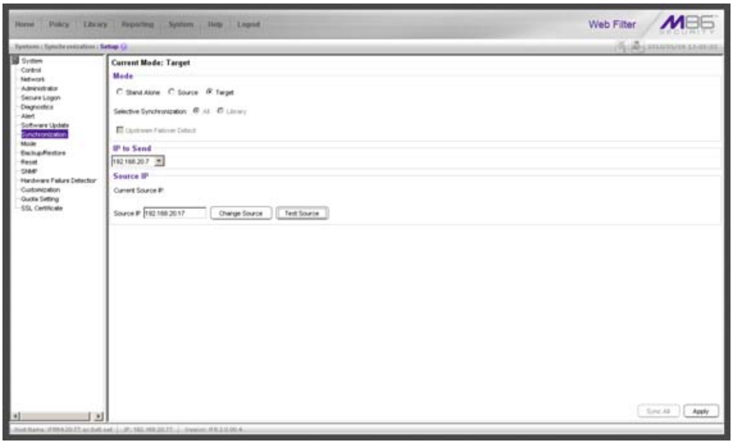
Set up a Web Filter to be a Target Server

A Web Filter configured to be a target server will receive profile/library setting changes from the source server only.

***WARNING**: If a Web Filter is set up in the Target mode with a NAT device between the target and source server, be sure that ports 26262 and 26268 are open on the target server. This setup is required so that the target server can communicate with the source server.*

For the Target mode setting:

1. In the Mode frame, click “Target” to display the Target mode view:



Current Mode: Target

Mode

○ Stand Alone ○ Source ● Target

Selective Synchronization: ● All ○ Library

□ Upstream Failover Detect

IP to Send

192.168.20.7

Source IP

Current Source IP

Source IP 192.168.20.17

Fig. 2:1-45 Setup window, Target mode

In the IP to Send frame, the LAN1 and LAN2 IP addresses set up in the LAN Settings window on this server display in the **IP to Send** pull-down menu.

2. In the Source IP frame, enter the **Source IP** address to use for sending profile/library setting changes to this server being configured.

***NOTE**: If a source server is set up with a NAT device, the NAT IP address must be used instead of the source server's own IP address.*

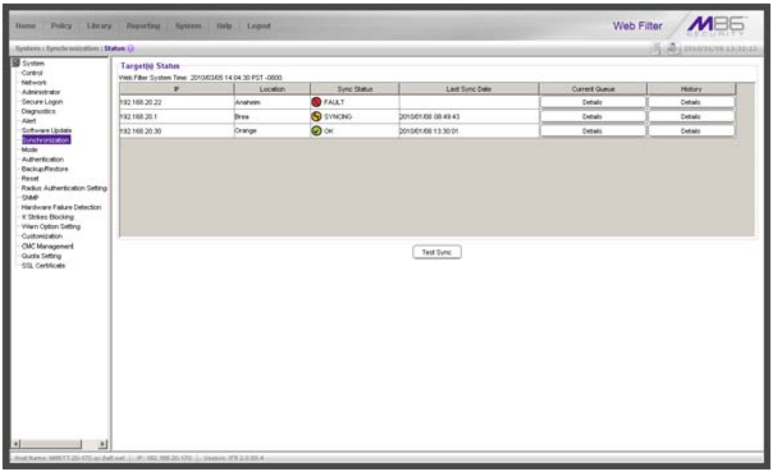
3. Click **Test Source** to open an alert box that provides the server mode status for the IP address you entered.
4. Click **OK** to close the alert box, and make any adjustments, if necessary.
5. After validating the source IP address, click **Change Source** to display this IP address in the **Current Source IP** display field.
6. Click **Apply** after all settings have been made.

***NOTE**: This test only verifies whether this server can contact the source server. In order for synchronization to be operable on the network, the source server must also be able to contact this target server being configured.*

Status window

The Status window displays when Status is selected from the Synchronization menu. This menu selection is available only if this server currently being configured is either set up in the Source mode or Target mode.

If set up in the Source mode, this window is used for verifying that profile updates are being sent to the target server(s), as in the example below:



Target(s) Status

Web Filter System Time: 2010/03/05 14:04:30 PST -0800

IP	Location	Sync Status	Last Sync Date	Current Queue	History
192.168.20.22	Anaheim	FAULT		Details	Details
192.168.20.1	Brea	SYNCING	2010/01/08 08:49:43	Details	Details
192.168.20.30	Orange	OK	2010/01/08 13:30:01	Details	Details

Fig. 2:1-46 Status window, Source mode

If set up in the Target mode, this window is used for verifying that profile/library setting updates are being received from the source server.

View the Sync Status of Targets from the Source

If the server is set up in the Source mode, the Web Filter System Time displays at the top of the Target(s) Status frame. This is the current date and time from the Web Filter—using the YYYY/MM/DD and HH:MM:SS format—and includes the UTC code for the time zone.

For each target server, the grid displays the IP address, Location, and Sync Status ("OK" if the target server can be accessed by the source server, "SYNCING" if synchronization is occurring, and "FAULT" if the target server cannot be reached or if there is a problem with synchronization). The Last Sync Date column displays the date and time synchronization last occurred for the target server.

***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 descending order by that column.

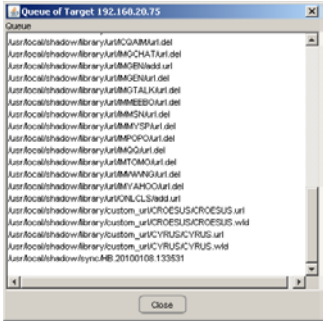
If text in any column displays truncated—followed by ellipses (...)—place the cursor over the beginning or ending of the column header. When the **<—>** *character displays in place of the cursor, you can expand the width of the column. You also can use the scrollbar beneath the grid to view information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

View Items in the Queue

If a “FAULT” message displays in the Sync Status column for a target server, items still remain in the queue, waiting to be synced.

To view items in the queue for a specified target server:

1. In the Current Queue column for that server, click **Details** to open the Queue of Target pop-up window:



```
/usr/local/shadow/library/url/ICQAIM/url.del
/usr/local/shadow/library/url/IMGCHAT/url.del
/usr/local/shadow/library/url/IMGEN/add.url
/usr/local/shadow/library/url/IMGEN/url.del
/usr/local/shadow/library/url/IMGTALK/url.del
/usr/local/shadow/library/url/IMMEEBO/url.del
/usr/local/shadow/library/url/IMMSN/url.del
/usr/local/shadow/library/url/IMMYSP/url.del
/usr/local/shadow/library/url/IMPOPO/url.del
/usr/local/shadow/library/url/IMQQ/url.del
/usr/local/shadow/library/url/IMTOMO/url.del
/usr/local/shadow/library/url/IMWWNG/url.del
/usr/local/shadow/library/url/IMYAHOO/url.del
/usr/local/shadow/library/url/ONLCLS/add.url
/usr/local/shadow/library/custom_url/CROESUS/CROESUS.url
/usr/local/shadow/library/custom_url/CROESUS/CROESUS.wld
/usr/local/shadow/library/custom_url/CYRUS/CYRUS.url
/usr/local/shadow/library/custom_url/CYRUS/CYRUS.wld
/usr/local/shadow/sync/HB.20100108.133531
```

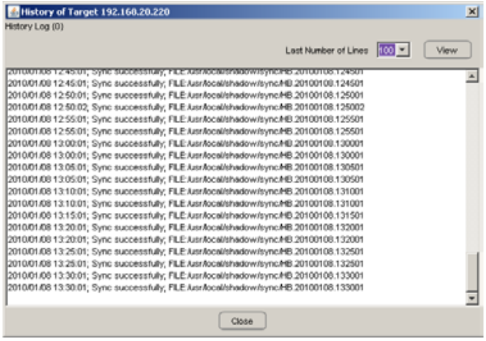
Fig. 2:1-47 Queue of Target pop-up window

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

View Items Previously Synced to the Server

To view items previously synced to a specified target server:

1. In the History column for that server, click **Details** to open the History of Target pop-up window.
2. Select the maximum **Last Number of Lines** from the pull-down menu (100, 200, 300, 400, 500) for the most recent synchronization history that you wish to view.
3. Click **View** to display lines of items in the History Log:



History Log (0)

Last Number of Lines: 100

```
2010/01/08 12:45:01; Sync successfully; FILE:/usr/local/shadow/sync/HB.20100108.124501
2010/01/08 12:45:01; Sync successfully; FILE:/usr/local/shadow/sync/HB.20100108.124501
2010/01/08 12:50:01; Sync successfully; FILE:/usr/local/shadow/sync/HB.20100108.125001
2010/01/08 12:50:02; Sync successfully; FILE:/usr/local/shadow/sync/HB.20100108.125002
2010/01/08 12:55:01; Sync successfully; FILE:/usr/local/shadow/sync/HB.20100108.125501
2010/01/08 12:55:01; Sync successfully; FILE:/usr/local/shadow/sync/HB.20100108.125501
2010/01/08 13:00:01; Sync successfully; FILE:/usr/local/shadow/sync/HB.20100108.130001
2010/01/08 13:00:01; Sync successfully; FILE:/usr/local/shadow/sync/HB.20100108.130001
2010/01/08 13:05:01; Sync successfully; FILE:/usr/local/shadow/sync/HB.20100108.130501
2010/01/08 13:05:01; Sync successfully; FILE:/usr/local/shadow/sync/HB.20100108.130501
2010/01/08 13:10:01; Sync successfully; FILE:/usr/local/shadow/sync/HB.20100108.131001
2010/01/08 13:10:01; Sync successfully; FILE:/usr/local/shadow/sync/HB.20100108.131001
2010/01/08 13:15:01; Sync successfully; FILE:/usr/local/shadow/sync/HB.20100108.131501
2010/01/08 13:20:01; Sync successfully; FILE:/usr/local/shadow/sync/HB.20100108.132001
2010/01/08 13:20:01; Sync successfully; FILE:/usr/local/shadow/sync/HB.20100108.132001
2010/01/08 13:25:01; Sync successfully; FILE:/usr/local/shadow/sync/HB.20100108.132501
2010/01/08 13:25:01; Sync successfully; FILE:/usr/local/shadow/sync/HB.20100108.132501
2010/01/08 13:30:01; Sync successfully; FILE:/usr/local/shadow/sync/HB.20100108.133001
2010/01/08 13:30:01; Sync successfully; FILE:/usr/local/shadow/sync/HB.20100108.133001
```

Fig. 2:1-48 History of Target pop-up window

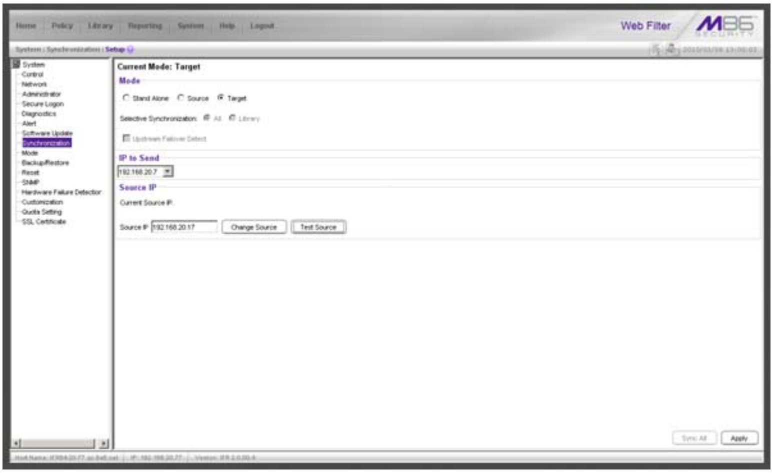
4. Click **Close** to close the pop-up window.

Place Items in Queue for Syncing

To place new sync items in queue for the target server(s), click **Test Sync**.

View the Sync Status of the Target Server

If the server is set up in the Target mode, the Web Filter System Time displays above the Target Sync Status frame. This is the current date and time from the Web Filter—using the YYYY/MM/DD and HH:MM:SS format—and includes the UTC code for the time zone.



Current Mode: Target

Mode

○ Stand Alone ○ Source ● Target

Selective Synchronization: ● All ○ Library

☐ Upstream Failover Detect

IP to Send

192.168.20.7

Source IP

Current Source IP:

Source IP 192.168.20.17

Fig. 2:1-49 Status window, Target mode

The Target Sync Status frame includes the following information:

- **Source IP** - The IP address of the source server displays.
- **Connection Status** - “OK” or “FAULT” displays, indicating whether or not there is a connection to the source server.

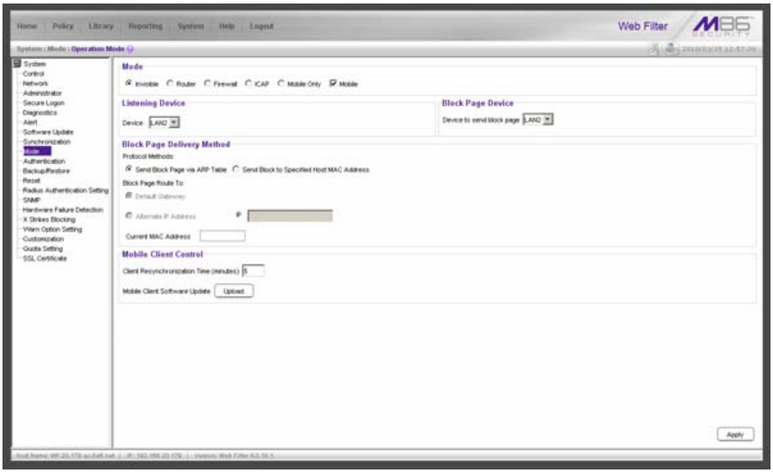
- **Last Successful Sync** - The date and time of the last successful synchronization displays, using the YYYY/ MM/DD and HH:MM:SS format.
- **History Log** - Click the **Details** button to open the History of Target pop-up window. See View Items Previously Synced to the Server in this section for information on accessing and viewing the contents of this window.

Mode

Mode includes options for configuring the Web Filter to filter the network. Click the Mode link to view a menu of subtopics: Operation Mode and Proxy Environment Settings.

Operation Mode window

The Operation Mode window displays when Operation Mode is selected from the Mode menu. This window is used for specifying the operational mode the Web Filter will use to filter the network, and the settings the Web Filter will use for "listening to" traffic and sending traffic. This window is also used for configuring the Web Filter to perform other operational capacities. Using the mobile mode in conjunction with one of the three filtering modes (Invisible, Router, or Firewall) the Web Filter will also filter end users whose machines are not located in house. In the Mobile Only mode, the Web Filter will solely filter workstations outside of the server location. In the ICAP mode, the Web Filter offloads specific content normally handled by a Web Filter, such as filtering.



Mode

● Invisible ○ Router ○ Firewall ○ ICAP ○ Mobile Only ☑ Mobile

Listening Device

Device: LAN2

Block Page Device

Device to send block page: LAN2

Block Page Delivery Method

Protocol Methods:

● Send Block Page via ARP Table ○ Send Block to Specified Host MAC Address

Block Page Route To:

● Default Gateway

○ Alternate IP Address IP

Current MAC Address

Mobile Client Control

Client Resynchronization Time (minutes): 5

Mobile Client Software Update

Fig. 2:1-50 Operation Mode window

Set the Operation Mode

The default Mode setting is “Invisible”. To change this setting, click the radio button corresponding to “Router”, “Firewall”, “ICAP”, or “Mobile Only”. Selecting ICAP would make the Web Filter function in a capacity other than filtering users on the network.

If there are users with mobile PCs physically located outside of the organization and you wish to filter these units on this Web Filter, click the “Mobile” checkbox to use the mobile mode in conjunction with the selected filtering mode.

***WARNING**: If using the router or firewall mode, M86 recommends contacting one of our solutions engineers if you need any assistance with setup procedures.*

***NOTE**: If using the firewall mode, the bandwidth module in the Security Reporter will not capture incoming traffic.*

Specify the Listening Device

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

If using the invisible mode, “LAN1” displays by default. If using the router or firewall mode, you may need to select the network card that will be used to “listen to”—as opposed to “send”—traffic on the network.

Specify the Block Page Device

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

***TIP**: For the invisible mode, the block page device should be a different device than the one selected in the Listening Device frame. For the router and firewall modes, the device should be the same as the one selected in the Listening Device frame.*

If using the router or firewall mode, at the **Device to send block page** pull-down menu, you may need to 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.

Invisible Option: Specify the Block Page Delivery

The Block Page Delivery Method frame displays if the Invisible operation mode is selected. 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 Web Filter 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 Web Filter 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.

ICAP Option: Specify ICAP Server Settings

The ICAP Server Settings frame displays if the ICAP operation mode is selected. This option should be used if this Web Filter is designated to function with an Internet Content Adaptation Protocol (ICAP) server to off-load specific content normally processed by the Web Filter, such as Internet filtering.

With an ICAP server, the Web Filter will not capture any network packets but will solely work with ICAP requests from an ICAP client (proxy server). When an end user makes a request for Internet content, this request is routed to the proxy server, which then submits the request to the ICAP server. The ICAP server sends back a response to the proxy server—which may send the request to the original Web Filter in some network setups, and then return a response to the proxy server. Based on the end user's filtering profile, the proxy server either fulfills the request or returns a block page.

The ICAP Server Settings frame is used for configuring options response settings for the ICAP Web Filter:

1. In the **ISTAG** field, enter the ISTag (ICAP Service Tag) which is a 128-maximum alphanumeric quoted string of data (including quotation marks but never the null character) used in the options response-header field. This tag provides a way for ICAP servers to send a service-specific “cookie” to ICAP clients so that the ICAP server can communicate with the ICAP client. For example: "835nb0-20a5-3e52671"

2. In the **URI** field, enter the Uniform Resource Identifier that must specify the complete hostname and path of the resource being requested. For example: icap://icap.logo.com:1344/services/icap-services

NOTE*: This string must match what is set up on the ICAP server in order for the ICAP client's request to be accepted by the ICAP server.*

3. In the **Max Connections (4-150)** field, enter the maximum connections the ICAP server will allow for ICAP clients. By default, *30* displays.
4. In the **Options TTL in Sections (0-86400)** field, enter the time (in seconds) in which the options response is valid. By default, *3600* displays.
5. In the **Preview Bytes (0-4096)** field, enter the number of bytes to be included in the response header to be sent by the ICAP client for preview by the ICAP server, before the entire request is submitted to the ICAP server. By default, *1024* displays.
6. In the **Port** field, enter the port number to be used by the ICAP server. By default, this port number is *1344*.

NOTE*: The port number must be the same one entered for the URI.*

WARNING*: Go to* ***http://www.m86security.com/software/8e6/hlp/ifr/files/1system_opmode_icap.html*** *to review a list of items to be considered when using the ICAP mode.*

Mobile Option: Specify the Mobile Client Control

The Mobile Client Control frame displays if the Mobile Only operational mode or the Mobile option is selected. Either selection should be made if this Web Filter will additionally filter end user workstations physically located outside of the organization.

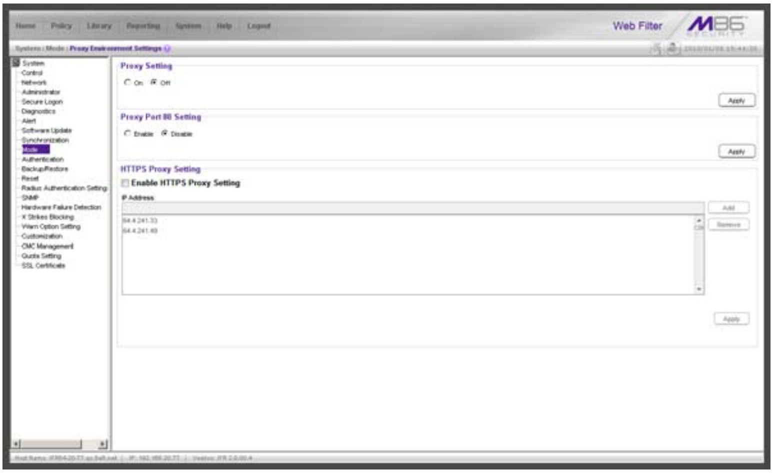
***NOTE**: See Appendix D: Mobile Client for information on setting up and using the Mobile Client.*

Apply Operation Mode Settings

Click **Apply** to apply your settings in the Mode frame.

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 WFR is in a proxy environment, if the default Web server port number 80 will be enabled, and if HTTPS traffic will be allowed to pass without being overblocked.



Proxy Setting

○ On ● Off

Proxy Port 80 Setting

○ Enable ● Disable

HTTPS Proxy Setting

□ Enable HTTPS Proxy Setting

IP Address

64.4.241.33
64.4.241.49

Fig. 2:1-51 Proxy Environment Settings window

***NOTE**: Basic Proxy Authentication must be used if using HTTPS in a proxy environment. The Web Filter 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 Web Filter 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.

Enable HTTPS Filtering

In the HTTPS Proxy Setting frame, indicate whether HTTPS filtering will be allowed to pass by making these settings:

1. Click **Enable HTTPS Proxy Setting** to activate the objects in this frame.
2. Enter the **IP Address** of each proxy server to recognize HTTPS traffic, and then click **Add** to include that IP address in the list box below.

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

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

Authentication

Authentication includes options for configuring the Web Filter 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.

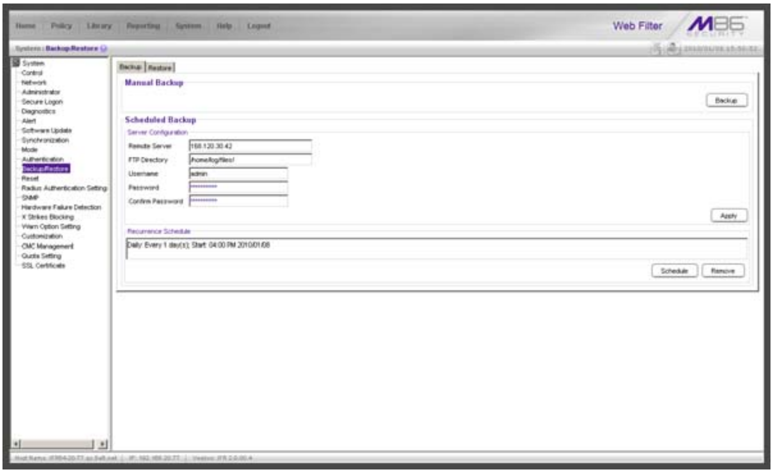
NOTES*: Information about these sub-topics can be found in the M86 Web Filter Authentication User Guide.*

The Authentication topic and sub-topics do not display if the synchronization feature is used, and this server being configured is set up in the Target mode to synchronize both profile and library setting changes.

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.



Remote Server: 168.120.30.42
FTP Directory: /home/log/files/
Username: admin
Password: **********
Confirm Password: **********

Daily: Every 1 day(s); Start: 04:00 PM 2010/01/08

Fig. 2:1-52 Backup/Restore window, Backup tab

WARNING: *A backup should be created and downloaded off the WFR server whenever a change is made to filtering settings in the Web Filter user interface.*

For each backup configuration created or uploaded via this window, a row is added to the Backup Configurations grid in the Restore tab. The newly added row includes the following information: Date the backup was executed, Filename 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

M86 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 WFR server, prior server settings can later be retrieved and uploaded to the Web Filter 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 Web Filter in the console of the new Web Filter.

***NOTE**: See Server Maintenance Procedures from the Web Filter Introductory Section’s Chapter 3: Synchronizing Multiple Units, for an overview on establishing backup procedures when using more than one Web Filter on the network.*

Perform a Backup on Demand

1. In the Manual Backup frame on the Backup tab, click **Backup** to open the Web Filter Backup dialog box:

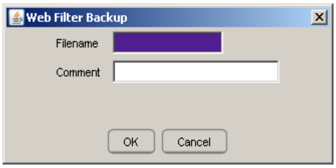


Fig. 2:1-53 Web Filter Backup dialog box

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

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

Schedule a Backup

Configure FTP Server Settings

1. In the Server Configuration section of the Scheduled Backup frame, enter the IP address of the **Remote Server**.
2. In the **FTP Directory** field, enter the path where log files will be stored.
3. In the **Username** field, type in the valid username for FTP transfers.
4. In the **Password** and **Confirm Password** fields, type in the password for the username specified in the FTP Directory field.
5. Click **Apply** to open the Server Configuration dialog box asking if you wish to save your settings.

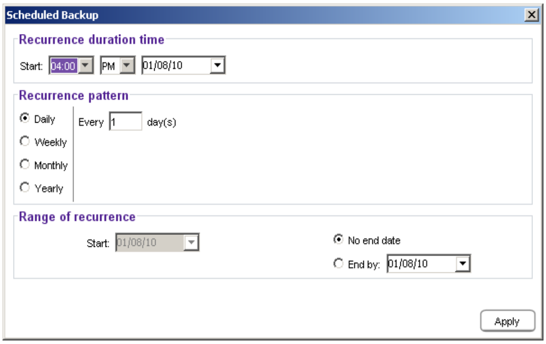
***TIP**: Click No to close the dialog box without saving your settings.*

6. Click **Yes** to close the dialog box and to open a Message alert box indicating that your settings have been saved.
7. Click **OK** to close the alert box.

You can now set up a schedule for a backup in the Recurrence Schedule section of the Scheduled Backup frame.

Create a Backup Schedule

1. In the Recurrence Schedule section of the Scheduled Backup frame, click **Schedule** to open the Scheduled Backup pop-up box:



Scheduled Backup

Recurrence duration time

Start: 04:00 PM 01/08/10

Recurrence pattern

● Daily
○ Weekly
○ Monthly
○ Yearly

Every 1 day(s)

Range of recurrence

Start: 01/08/10

● No end date
○ End by: 01/08/10

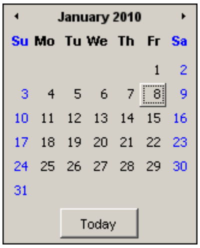
Fig. 2:1-54 Scheduled Backup pop-up box

2. 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:



January 2010

Su	Mo	Tu	We	Th	Fr	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

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.

3. 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 2010, the first Monday in June this year would be the 7th. The next time this profile would be used will be in June 2012.

4. 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.)
5. Click **Apply** to close the Scheduled Backup pop-up box and to open a Message alert box informing you that the backup schedule will be activated at the specified time.
6. Click **OK** to close the Message alert box. The Backup/ Restore window now shows the schedule in the Recurrence Schedule section of the Scheduled Backup frame.

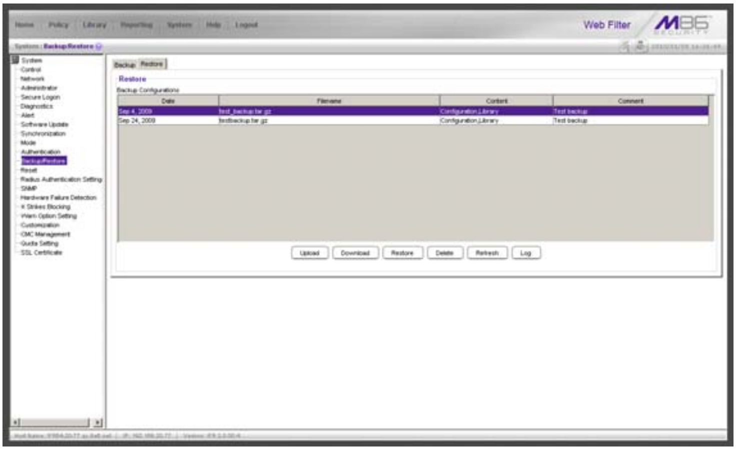
Remove a Backup Schedule

Click **Remove** to remove the schedule from the Recurrence Schedule section of the Scheduled Backup frame.

Download a File

To download a file to your machine:

1. In the Restore tab, select the file from the Backup Configurations grid:



Restore

Backup Configurations

Date	Filename	Content	Comment
Sep 4, 2009	test_backup.tar.gz	Configuration,Library	Test backup
Sep 24, 2009	testbackup.tar.gz	Configuration,Library	Test backup

Fig. 2:1-55 Backup/Restore window, Restore tab

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 and to open the file download dialog box.
4. Select the “save” option; this action opens the window on your workstation where you specify the filename for the file and where to save the file.
5. Select the folder in which to save the file, and then enter the **File name**, retaining the “.gz” file extension. Click **Save** to begin downloading the .gz file to your workstation.

Perform a Restoration

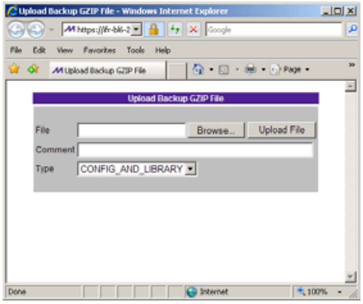
To restore backup data to the server, the backup file must be listed in the Backup Configurations grid in the Restore tab, and the restoration function must be executed. If the backup file is not included in the Backup Configurations grid, you must upload it to the server.

***WARNING**: Be sure the file you are restoring uses the same version of the software currently used by the Web Filter Administrator console. Refer to the Local Software Update window for available updates to the Web Filter's software. (See the Local Software Update 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:



File

Comment

Type CONFIG_AND_LIBRARY

Fig. 2:1-56 Upload GZIP File pop-up window

2. Click **Browse...** to open the 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

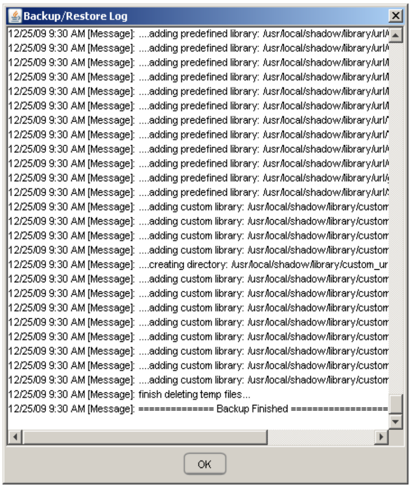
To remove a file from the Backup Configurations grid:

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:



```
12/25/09 9:30 AM [Message]: ....adding predefined library: /usr/local/shadow/library/url/
12/25/09 9:30 AM [Message]: ....adding predefined library: /usr/local/shadow/library/url/
12/25/09 9:30 AM [Message]: ....adding predefined library: /usr/local/shadow/library/url/
12/25/09 9:30 AM [Message]: ....adding predefined library: /usr/local/shadow/library/url/
12/25/09 9:30 AM [Message]: ....adding predefined library: /usr/local/shadow/library/url/
12/25/09 9:30 AM [Message]: ....adding predefined library: /usr/local/shadow/library/url/
12/25/09 9:30 AM [Message]: ....adding predefined library: /usr/local/shadow/library/url/
12/25/09 9:30 AM [Message]: ....adding predefined library: /usr/local/shadow/library/url/
12/25/09 9:30 AM [Message]: ....adding predefined library: /usr/local/shadow/library/url/
12/25/09 9:30 AM [Message]: ....adding predefined library: /usr/local/shadow/library/url/
12/25/09 9:30 AM [Message]: ....adding predefined library: /usr/local/shadow/library/url/
12/25/09 9:30 AM [Message]: ....adding predefined library: /usr/local/shadow/library/url/
12/25/09 9:30 AM [Message]: ....adding custom library: /usr/local/shadow/library/custom
12/25/09 9:30 AM [Message]: ....adding custom library: /usr/local/shadow/library/custom
12/25/09 9:30 AM [Message]: ....adding custom library: /usr/local/shadow/library/custom
12/25/09 9:30 AM [Message]: ....adding custom library: /usr/local/shadow/library/custom
12/25/09 9:30 AM [Message]: ....creating directory: /usr/local/shadow/library/custom_ur
12/25/09 9:30 AM [Message]: ....adding custom library: /usr/local/shadow/library/custom
12/25/09 9:30 AM [Message]: ....adding custom library: /usr/local/shadow/library/custom
12/25/09 9:30 AM [Message]: ....adding custom library: /usr/local/shadow/library/custom
12/25/09 9:30 AM [Message]: ....adding custom library: /usr/local/shadow/library/custom
12/25/09 9:30 AM [Message]: ....adding custom library: /usr/local/shadow/library/custom
12/25/09 9:30 AM [Message]: ....adding custom library: /usr/local/shadow/library/custom
12/25/09 9:30 AM [Message]: ....adding custom library: /usr/local/shadow/library/custom
12/25/09 9:30 AM [Message]: ....adding custom library: /usr/local/shadow/library/custom
12/25/09 9:30 AM [Message]: finish deleting temp files...
12/25/09 9:30 AM [Message]: ============= Backup Finished ==================
```

Fig. 2:1-57 Backup/Restore pop-up box

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

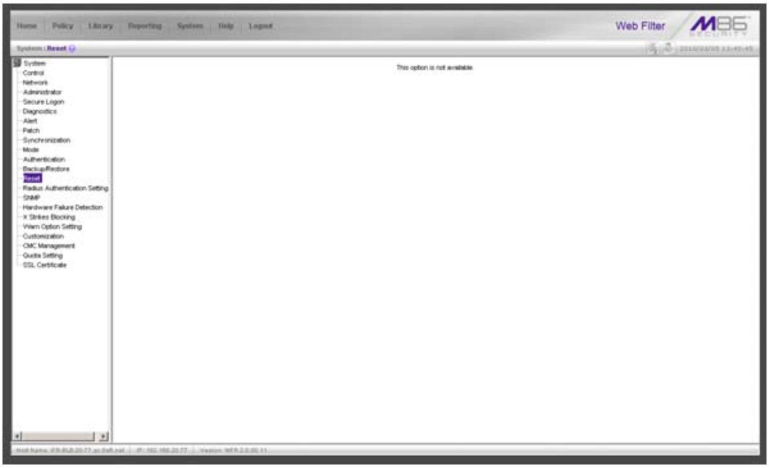
   The following information displays for each row: the date and time a process was attempted to be executed, and a Message indicating whether that process succeeded or failed.

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 function, used for resetting the server to factory default settings, is not available in WFR.



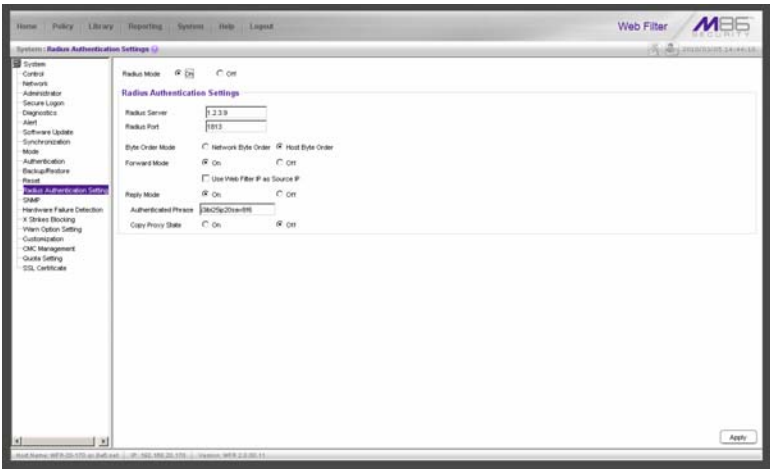
This option is not available.

Fig. 2:1-58 Reset window

Radius Authentication Settings

Radius Authentication Settings window

The Radius Authentication Settings window displays when Radius Authentication Settings is selected from the navigation panel. This window is used for controlling filtering levels of dial-up users.



Radius Mode ● On ○ Off

Radius Authentication Settings

Radius Server 1.2.3.9

Radius Port 1813

Byte Order Mode ○ Network Byte Order ● Host Byte Order

Forward Mode ● On ○ Off

□ Use Web Filter IP as Source IP

Reply Mode ● On ○ Off

Authenticated Phrase [illegible]

Copy Proxy State ○ On ● Off

Fig. 2:1-59 Radius Authentication Settings window

***NOTE**: The Radius Authentication Settings topic does not display if the synchronization feature is used, and this server being configured is set up in the Target mode to synchronize both profile and library setting changes.*

The Radius feature uses an external Radius accounting server that determines which accounts will be filtered and how they will be filtered. The user profile in the Radius accounting server holds the filter definition for the user.

Depending on your network setup, there may be more than one accounting server. Also there may be a client (Network Access Server or proxy server) that sends accounting request packets to the external Radius accounting server.

Enable Radius

The **Radius Mode** is “Off” by default. To use Radius, click the “On” radio button. This action displays the Radius Authentication Settings frame.

Specify Radius Authentication Settings

1. In the **Radius Server** field, *1.2.3.9* displays by default. Enter the IP address of the Radius accounting server.
2. In the **Radius Port** number field, *1813* displays by default. Change this number only if the Radius accounting server uses a different port number.
3. In the **Byte Order Mode** field, specify the format in which bytes will be transferred:
   - Click the radio button corresponding to **Network Byte Order** to transfer the most significant byte first.
   - Click the radio button corresponding to **Host Byte Order** to use the byte order stored in the server (big endian or little endian order).

***NOTE**: The byte order should match the setting on the Radius accounting server.*

4. In the **Forward Mode** field, specify whether accounting request packets will be delivered from the client (NAS or proxy server) to the Radius accounting server.

   To enable the Forward Mode option:

   - Click the “On” radio button. The NAS will forward accounting request packets to the Radius accounting server.
   - Check the box for **Use Web Filter IP as Source IP**, if the IP address of the Web Filter (LAN1 or LAN2) should be used when forwarding packets instead of the IP address of the NAS.

To disable the Forward Mode option, click the “Off” radio button. This action causes the **Use Web Filter IP as Source IP** field to display greyed out.

5. In the **Reply Mode** field, specify whether the server that sent a request should receive a response.

   To enable the Reply Mode option:

   - Click the “On” radio button. A reply and accounting response packet will be submitted to the sender (NAS or Radius server).
   - Enter an **Authenticated Phrase** to be shared by the Radius server and NAS.
   - At the **Copy Proxy State** field, click the “On” radio button if you wish to copy the proxy state attribute to the packet.

***NOTE**: The copy proxy state attribute will only be added to the response packet if the Reply Mode is “On”. If the Radius accounting server is in the Forward Mode and the Reply Mode is “Off”, the copy proxy state attribute will be forwarded to the destination server but will not reply back to the client.*

Apply Settings

Click **Apply** to save your settings.

Disable Radius

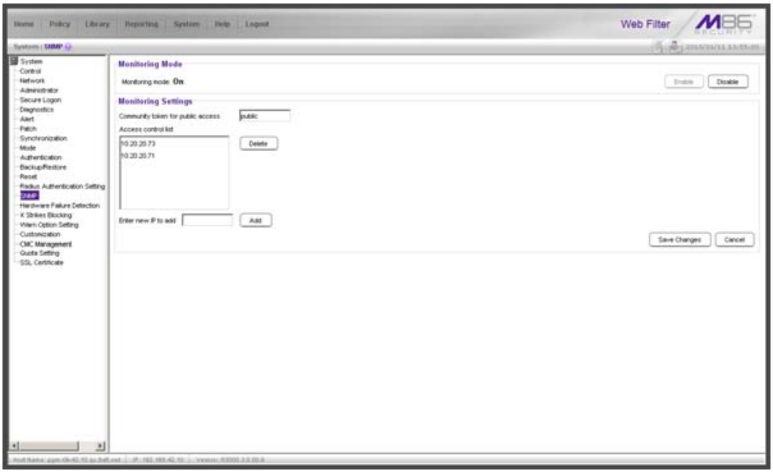
To disable the Radius feature:

1. At the **Radius Mode** field, click the “Off” radio button.
2. Click **Apply**.

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 Web Filter's filtering on a network.



Monitoring mode: On

Community token for public access: public

Access control list:
10.20.20.73
10.20.20.71

Enter new IP to add:

Fig. 2:1-60 SNMP window

The following aspects of the WFR 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 Web Filter 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**.

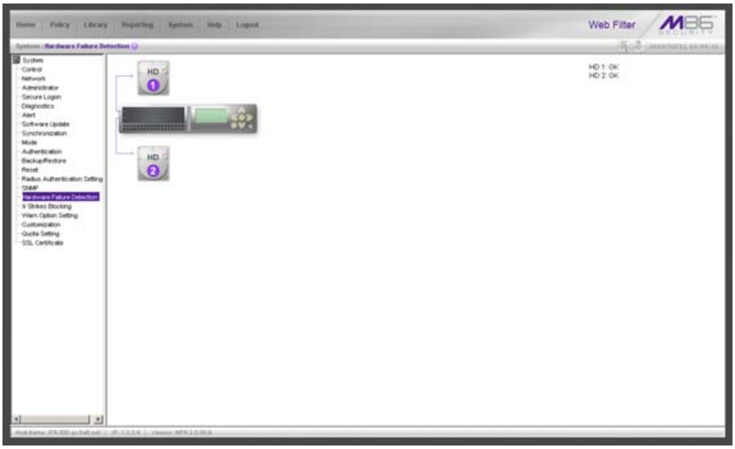
Maintain the Access Control List

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

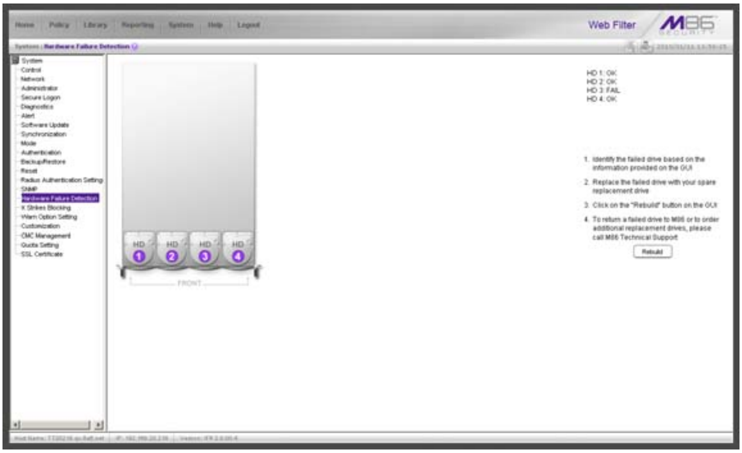
Hardware Failure Detection window

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.



HD 1: OK
HD 2: OK

Fig. 2:1-61 Hardware Failure Detection window, 300 series model



HD 1: OK
HD 2: OK
HD 3: FAIL
HD 4: OK

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 M86 or to order additional replacement drives, please call M86 Technical Support

Fig. 2:1-62 Hardware Failure Detection window, 500 series model

View the Status of the Hard Drives

The Hardware Failure Detection window displays the current RAID Array Status for each of the hard drives (HD 1 and HD 2 for 300 series hardware models, and HD 1 through HD 4 for 500 series hardware models). If all 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:

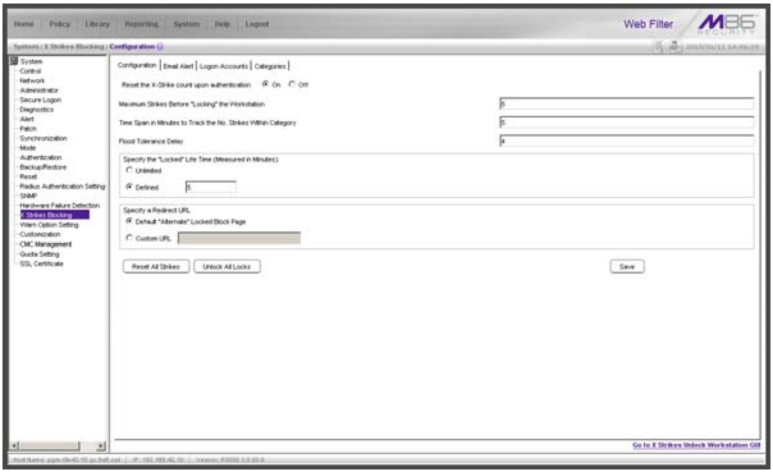
1. Identify the failed drive based on the information provided on the GUI
2. Replace the failed drive with your spare replacement drive
3. Click on the “Rebuild” button on the GUI
4. To return a failed drive to M86 or to order additional replacement drives, please call M86 Technical Support

NOTE*: For information on troubleshooting RAID, refer to WFR Appendix II: RAID and Hardware 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.



Reset the X-Strike count upon authentication ● On ○ Off

Maximum Strikes Before "Locking" the Workstation: 5

Time Span in Minutes to Track the No. Strikes Within Category: 5

Flood Tolerance Delay: 4

Specify the "Locked" Life Time (Measured in Minutes)
○ Unlimited
● Defined 5

Specify a Redirect URL
● Default "Alternate" Locked Block Page
○ Custom URL

Fig. 2:1-63 X Strikes Blocking window, Configuration tab

***NOTES**: The X Strikes Blocking topic does not display if the synchronization feature is used, and this server being configured is set up in the Target mode to synchronize both profile and library setting changes.*

X Strikes Blocking settings are effective only for filtering profiles with the X Strikes Blocking filter option enabled. (See Filter Options in the Policy 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.

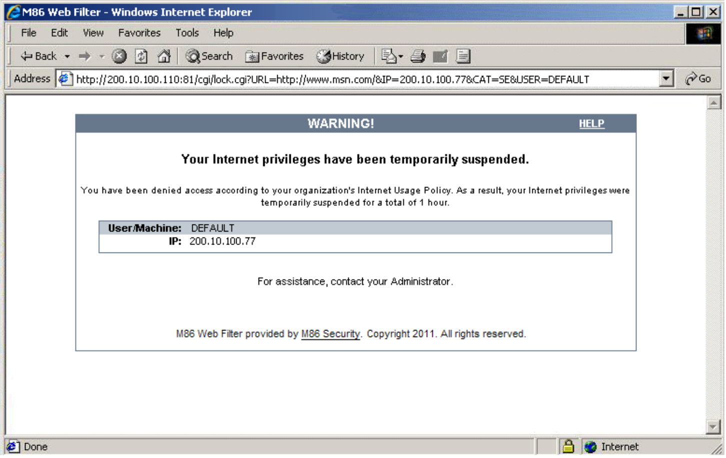
Reset All Workstations

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:


M86 Web Filter - Windows Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address
Go

http://200.10.100.110:81/cgi/lock.cgi?URL=http://www.msn.com/&IP=200.10.100.77&CAT=SE&USER=DEFAULT

WARNING! HELP

Your Internet privileges have been temporarily suspended.

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 1 hour.

User/Machine: DEFAULT
IP: 200.10.100.77

For assistance, contact your Administrator.

M86 Web Filter provided by M86 Security. Copyright 2011. All rights reserved.

Fig. 2:1-64 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:

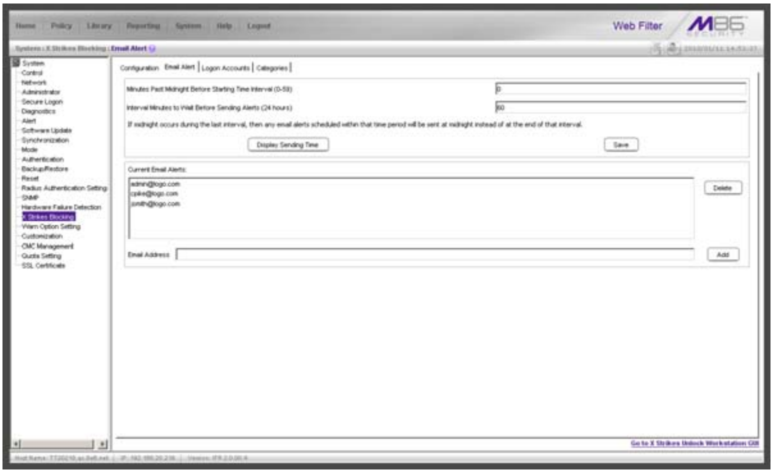
- the time span for the maximum number of strikes may need to be increased
- the maximum number of strikes may need to be increased

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:



Minutes Past Midnight Before Starting Time Interval (0-59): 0

Interval Minutes to Wait Before Sending Alerts (24 hours): 60

If midnight occurs during the last interval, then any email alerts scheduled within that time period will be sent at midnight instead of at the end of that interval.

Current Email Alerts:

admin@logo.com
cpike@logo.com
jsmith@logo.com

Email Address:

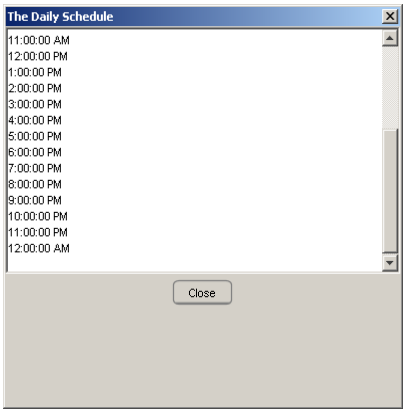
Fig. 2:1-65 X Strikes Blocking window, Email Alert tab

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:



The Daily Schedule

11:00:00 AM
12:00:00 PM
1:00:00 PM
2:00:00 PM
3:00:00 PM
4:00:00 PM
5:00:00 PM
6:00:00 PM
7:00:00 PM
8:00:00 PM
9:00:00 PM
10:00:00 PM
11:00:00 PM
12:00:00 AM

Fig. 2:1-66 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, M86 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:

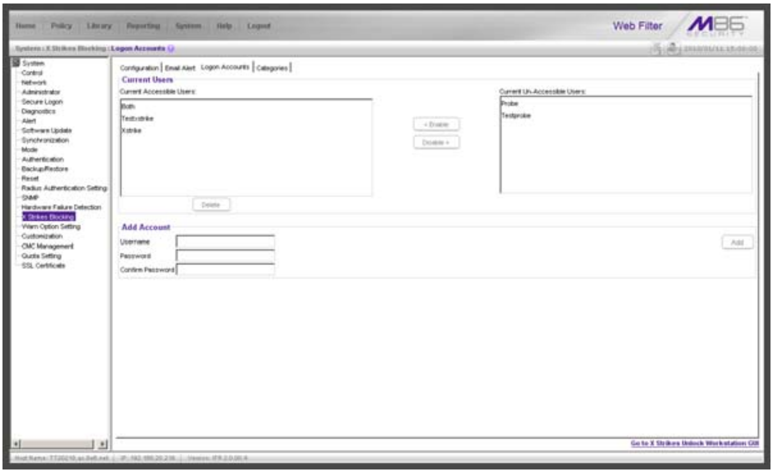


Fig. 2:1-67 X Strikes Blocking window, Logon Accounts tab

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

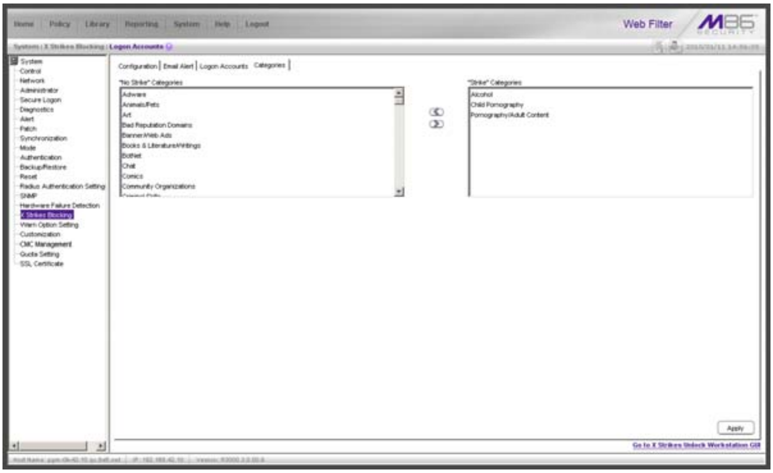
To delete a user’s account:

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:



"No Strike" Categories

- Adware
- Animals/Pets
- Art
- Bad Reputation Domains
- Banner/Web Ads
- Books & Literature/Writings
- BotNet
- Chat
- Comics
- Community Organizations

"Strike" Categories

- Alcohol
- Child Pornography
- Pornography/Adult Content

Fig. 2:1-68 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.

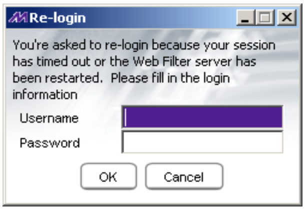
***NOTE**: Library categories in the "Strike" Categories list box will only be effective for filtering profiles with the X Strikes Blocking Filter Option enabled.*

Go to X Strikes Unlock Workstation GUI

When any administrator clicks the X Strikes Blocking icon or **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:



Re-login

You're asked to re-login because your session has timed out or the Web Filter server has been restarted. Please fill in the login information

Username

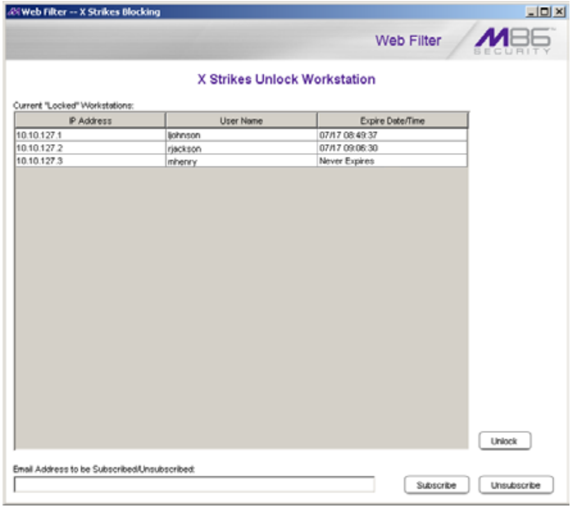
Password

Fig. 2:1-69 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 Web Filter 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.



X Strikes Unlock Workstation

Current "Locked" Workstations:

IP Address	User Name	Expire Date/Time
10.10.127.1	ljohnson	07/17 08:49:37
10.10.127.2	rjackson	07/17 09:06:30
10.10.127.3	mhenry	Never Expires

Email Address to be Subscribed/Unsubscribed:

Fig. 2:1-70 X Strikes Unlock Workstation window

Unlock a Workstation

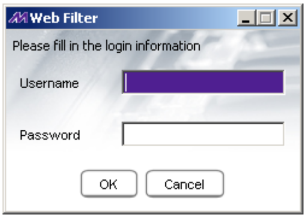
To unlock a specified workstation:

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

***NOTE**: An authorized staff member can click a link in an email alert, or type in **https://x.x.x.x:1443/XStrike.html** in the address field of a browser window—in which "x.x.x.x" is the IP address of the Web Filter—to view locked workstation criteria.*

When using the aforementioned URL, the following occurs:

- *The Login window opens:*



Web Filter

Please fill in the login information

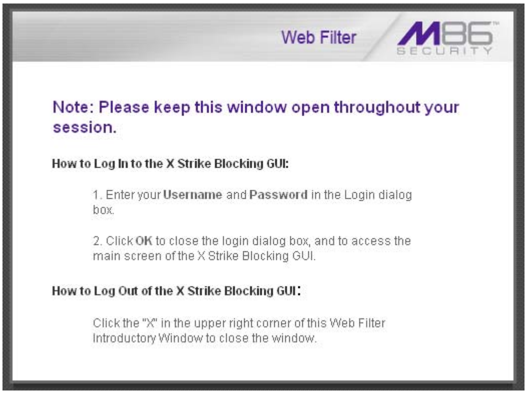
Username

Password

Fig. 2:1-71 Login window

*Enter the Username and Password and click **OK** to open the X Strikes Unlock Workstation pop-up window (see Fig. 2:1-70).*

- *The Web Filter Introductory Window for X Strikes simultaneously opens with the Login window:*



Note: Please keep this window open throughout your session.

How to Log In to the X Strike Blocking GUI:

1. Enter your **Username** and **Password** in the Login dialog box.

2. Click **OK** to close the login dialog box, and to access the main screen of the X Strike Blocking GUI.

How to Log Out of the X Strike Blocking GUI:

Click the "X" in the upper right corner of this Web Filter Introductory Window to close the window.

Fig. 2:1-72 X Strikes introductory window

This window must be left open during the entire session.

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**.

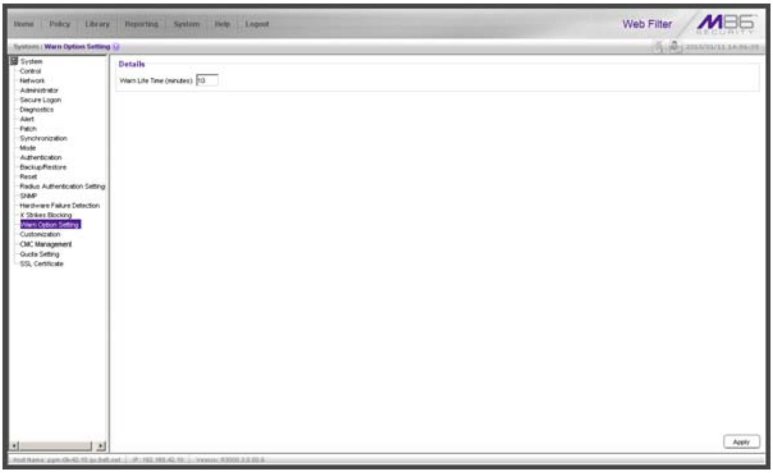
Close the Pop-up Window

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.



Warn Life Time (minutes): 10

Fig. 2:1-73 Warn Option Setting window

***NOTES**: If using the synchronization feature, the Warn Option Setting window is available in the Stand Alone and Source mode. This topic does not display if this server being configured is set up in the Target mode to synchronize both profile and library setting changes.*

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

Specify 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

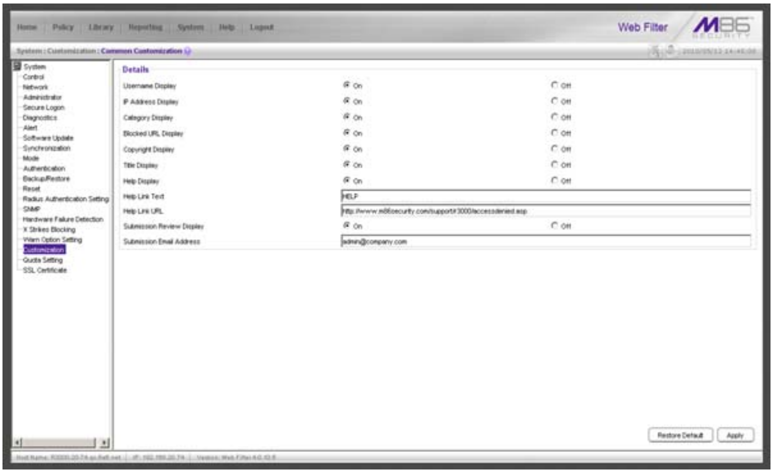
Customization includes options to customize settings for HTML pages that display for end users who execute a command that triggers the associated pop-up window to open. Click the Customization link to view a menu of sub-topics: Common Customization, Authentication Form, Lock Page, Block Page, Warn Page,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

***NOTES**: All Customization windows display greyed-out if the synchronization feature is used, and this server being configured is set up in the Target mode to synchronize both profile and library setting changes.*

Refer to the M86 Web Filter 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.



Details

Username Display	● On	○ Off
IP Address Display	● On	○ Off
Category Display	● On	○ Off
Blocked URL Display	● On	○ Off
Copyright Display	● On	○ Off
Title Display	● On	○ Off
Help Display	● On	○ Off
Help Link Text	HELP	
Help Link URL	http://www.m86security.com/support#3000/accessdenied.asp	
Submission Review Display	● On	○ Off
Submission Email Address	admin@company.com	

Fig. 2:1-74 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 M86'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 M86 Web Filter 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.m86security.com/support/r3000/accessdenied.asp* 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.

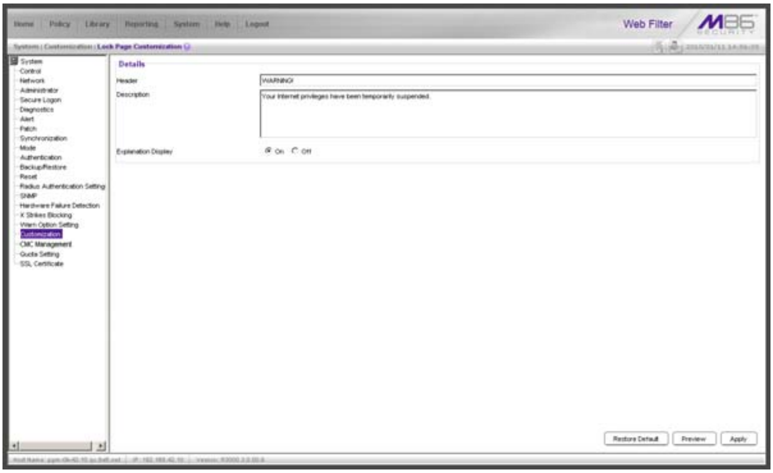
2. Click **Apply** to save your entries.

***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.*



Header: WARNING!

Description: Your Internet privileges have been temporarily suspended.

Explanation Display: ● On ○ Off

Fig. 2:1-75 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.

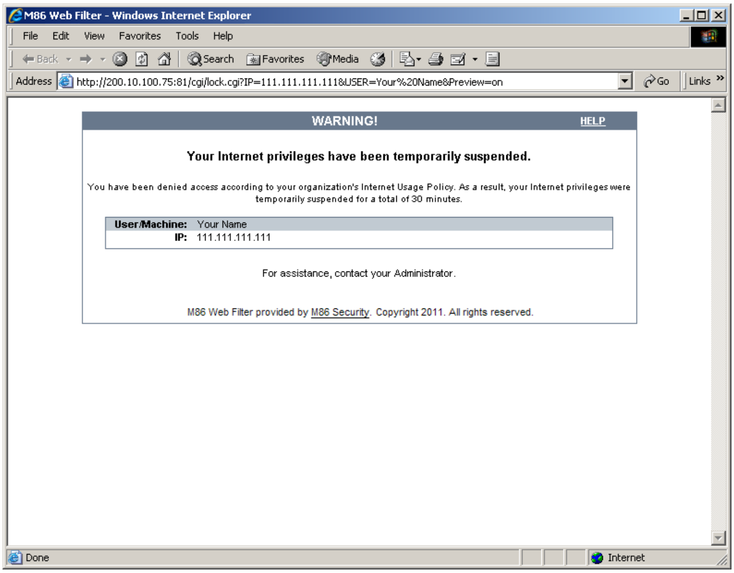
2. At the **Explanation Display** field, by default “On” is selected. This setting displays the reason the workstation is locked beneath the text from the Description field. Click “Off” to not have the explanatory text display in the lock page.

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:


M86 Web Filter - Windows Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Links
Done
Internet

http://200.10.100.75:81/cgi/lock.cgi?IP=111.111.111.111&USER=Your%20Name&Preview=on

WARNING! HELP

Your Internet privileges have been temporarily suspended.

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 30 minutes.

User/Machine:	Your Name
IP:	111.111.111.111

For assistance, contact your Administrator.

M86 Web Filter provided by M86 Security. Copyright 2011. All rights reserved.

Fig. 2:1-76 Sample Customized Lock Page

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

- **User/Machine** field - The username displays for the 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 M86’s Technical Support page that explains why access to the site or service may have been denied.

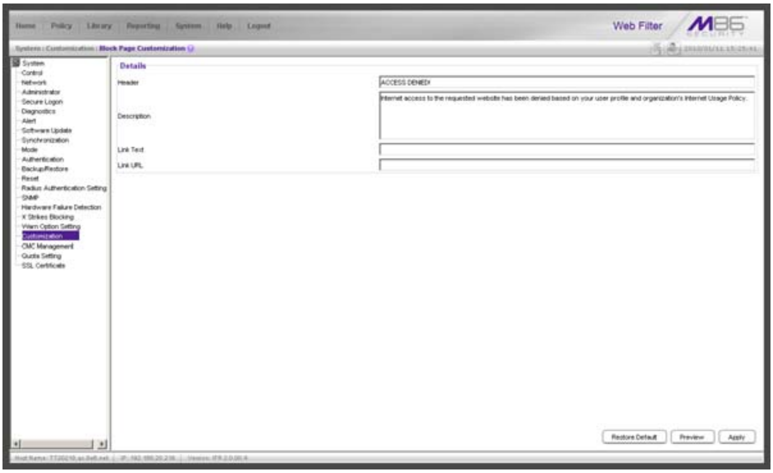
- **M86 Security** - Clicking this link takes the user to M86’s Web site.

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.



Header: ACCESS DENIED!

Description: Internet access to the requested website has been denied based on your user profile and organization's Internet Usage Policy.

Link Text:

Link URL:

Fig. 2:1-77 Block Page Customization window

NOTE: *See Appendix B: 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

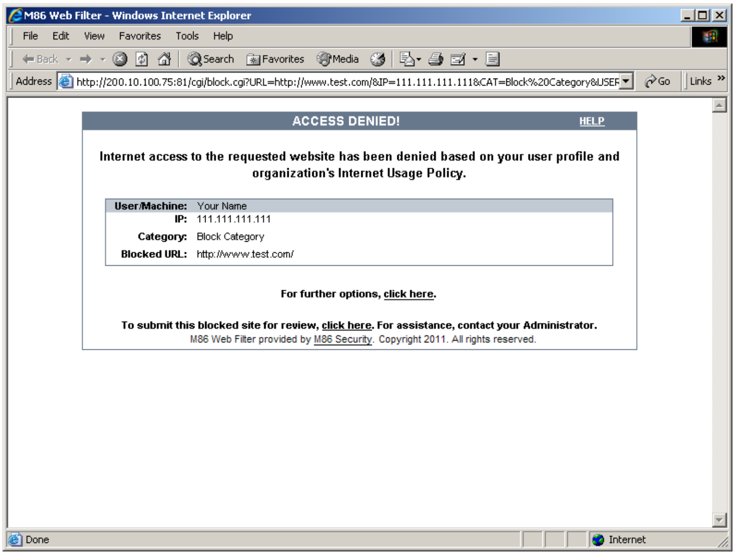
1. Make an entry in any of the following fields:
   - In the **Header** field, enter a static header to be displayed at the top of the block page.
   - In the **Description** field, enter a static text message to be displayed beneath the block page header.
   - In the **Link Text** field, enter text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



M86 Web Filter - Windows Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
Go
Links
Done
Internet

http://200.10.100.75:81/cgi/block.cgi?URL=http://www.test.com/&IP=111.111.111.111&CAT=Block%20Category&USER

ACCESS DENIED! HELP

Internet access to the requested website has been denied based on your user profile and organization's Internet Usage Policy.

User/Machine:	Your Name
IP:	111.111.111.111
Category:	Block Category
Blocked URL:	http://www.test.com/

For further options, click here.

To submit this blocked site for review, click here. For assistance, contact your Administrator.

M86 Web Filter provided by M86 Security. Copyright 2011. All rights reserved.

Fig. 2:1-78 Sample Customized Block Page

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

- **User/Machine** field - The username displays for the 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 M86's Technical Support page that explains why access to the site or service may have been denied.
- **M86 Security** - Clicking this link takes the user to M86'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.

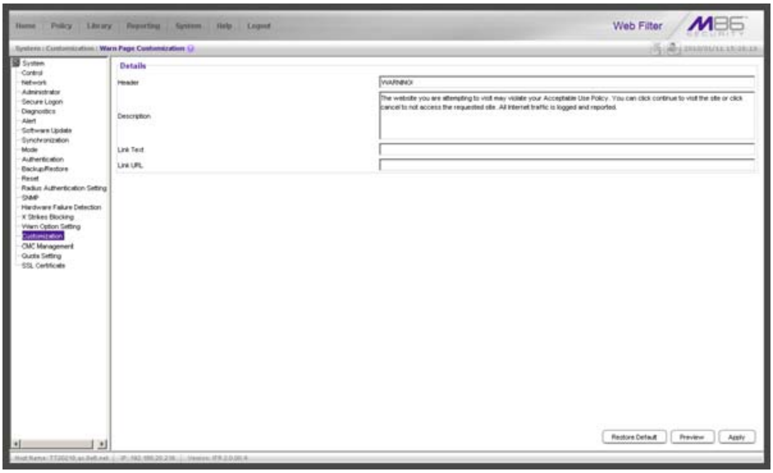
2. Click the "X" in the upper right corner of the window to close the sample customized block page.

***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.*



Header: WARNING!

Description: The website you are attempting to visit may violate your Acceptable Use Policy. You can click continue to visit the site or click cancel to not access the requested site. All Internet traffic is logged and reported.

Link Text:

Link URL:

Fig. 2:1-79 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 hyperlink in plain text using the *http://* or *https://* syntax.

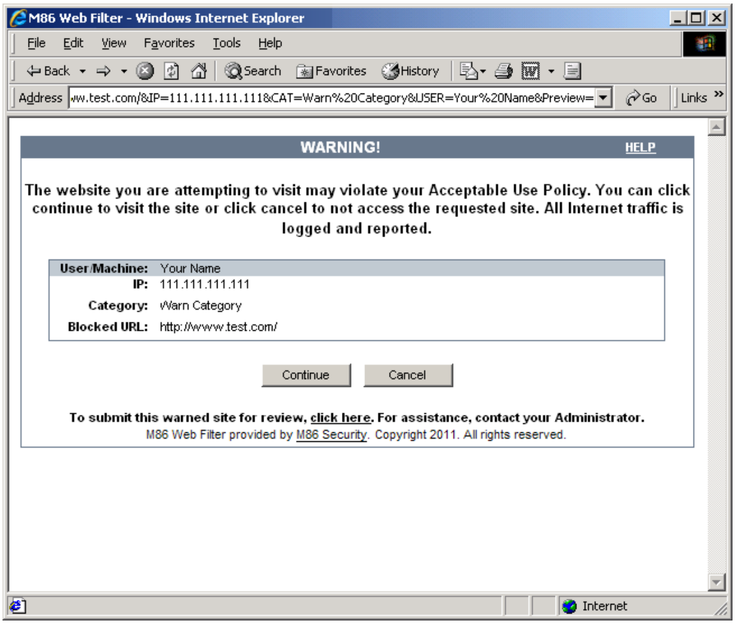
   Any entries made in these fields will display centered in the customized warning page, using the Arial font type.

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:


M86 Web Filter - Windows Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address ww.test.com/&IP=111.111.111.111&CAT=Warn%20Category&USER=Your%20Name&Preview= Go Links
Internet

WARNING! HELP

The website you are attempting to visit may violate your Acceptable Use Policy. You can click continue to visit the site or click cancel to not access the requested site. All Internet traffic is logged and reported.

User/Machine: Your Name
IP: 111.111.111.111
Category: Warn Category
Blocked URL: http://www.test.com/

Continue Cancel

To submit this warned site for review, click here. For assistance, contact your Administrator.
M86 Web Filter provided by M86 Security. Copyright 2011. All rights reserved.

Fig. 2:1-80 Sample Customized Warning Page

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

- **User/Machine** field - The username displays for the 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 M86's Technical Support page that explains why access to the site or service may have been denied.
- **M86 Security** - Clicking this link takes the user to M86'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.

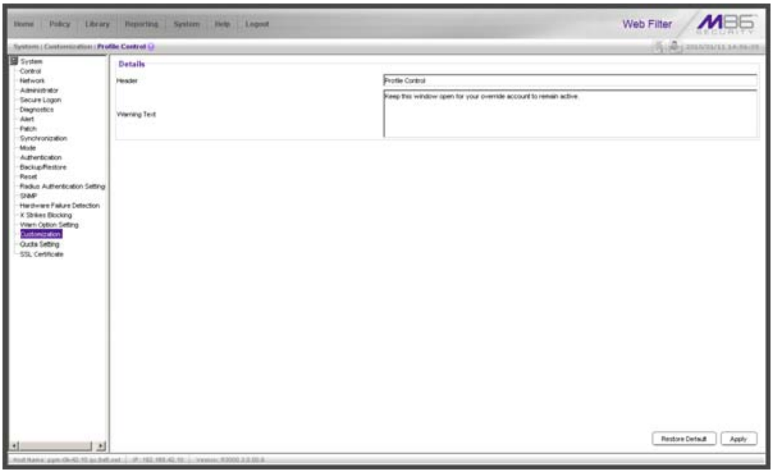
2. Click the “X” in the upper right corner of the window to close the sample customized warning page.

***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 Policy section for more information about this feature.*



Details

Header Profile Control

Warning Text Keep this window open for your override account to remain active.

Fig. 2:1-81 Profile Control window

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

Edit Entries

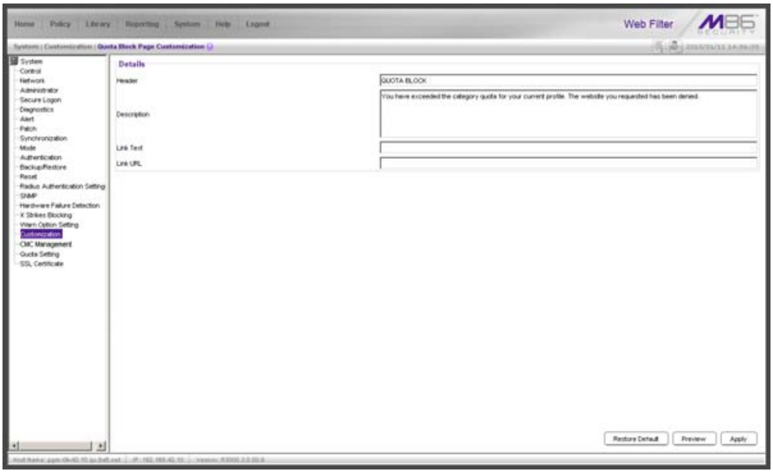
1. Make an entry in any of the following fields:
   - In the **Header** field, enter a static header to be displayed at the top of the profile control pop-up window.
   - In the **Warning Text** field, enter a static text message to be displayed at the bottom of the pop-up window.
2. Click **Apply**.

***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.



Header QUOTA BLOCK

Description You have exceeded the category quota for your current profile. The website you requested has been denied.

Link Text

Link URL

Fig. 2:1-82 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 hyperlink in plain text using the *http://* or *https://* syntax.

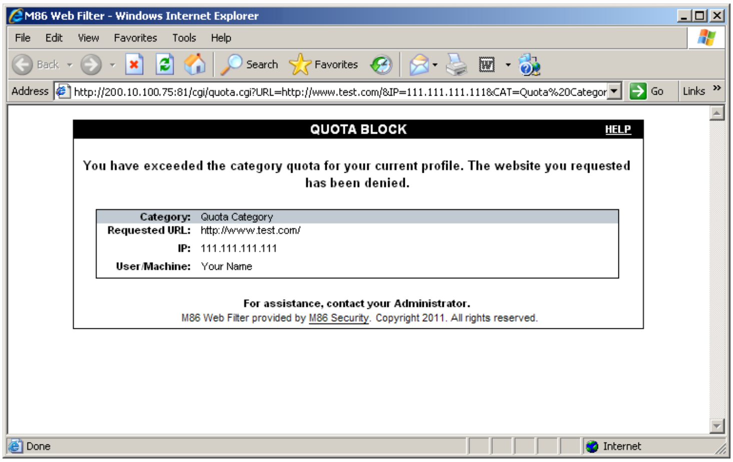
Any entries made in these fields will display centered in the customized quota block page, using the Arial font type.

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:



http://200.10.100.75:81/cgi/quota.cgi?URL=http://www.test.com/&IP=111.111.111.111&CAT=Quota%20Categor

QUOTA BLOCK HELP

You have exceeded the category quota for your current profile. The website you requested has been denied.

Category: Quota Category
Requested URL: http://www.test.com/
IP: 111.111.111.111
User/Machine: Your Name

For assistance, contact your Administrator.
M86 Web Filter provided by M86 Security. Copyright 2011. All rights reserved.

Fig. 2:1-83 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 LDAP user. This field is blank for the IP group user.

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

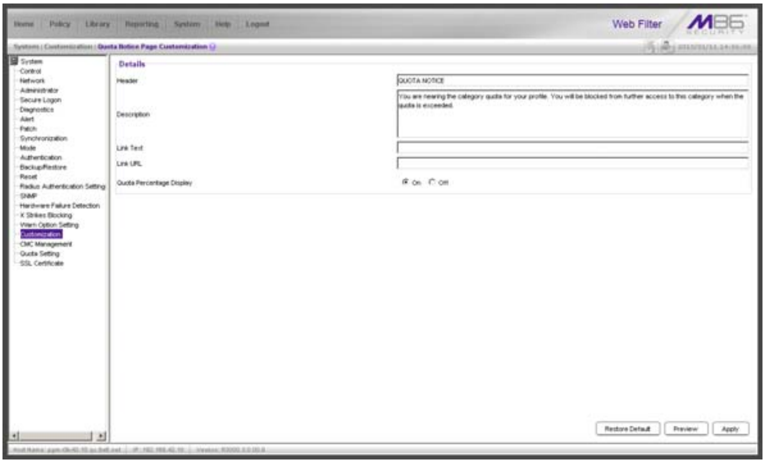
- **HELP** - Clicking this link takes the user to M86's Technical Support page that explains why access to the site or service may have been denied.
- **M86 Security** - Clicking this link takes the user to M86's Web site.

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.



Details

Header: QUOTA NOTICE

Description: You are nearing the category quota for your profile. You will be blocked from further access to this category when the quota is exceeded.

Link Text:

Link URL:

Quota Percentage Display: ● On ○ Off

Fig. 2:1-84 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 hyperlink 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.

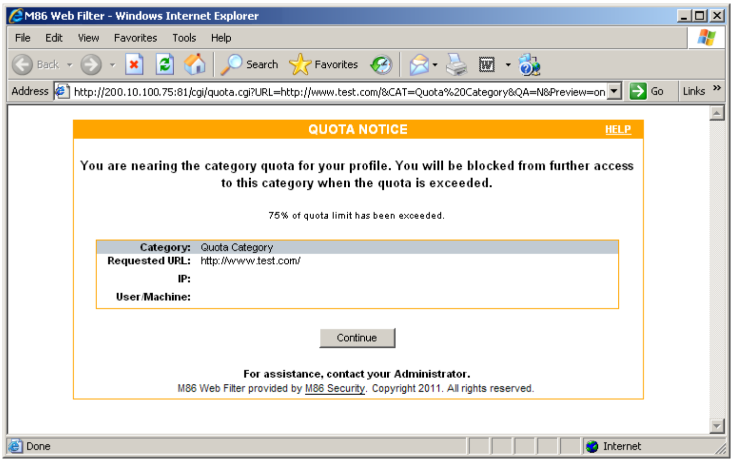
2. By default, the **Quota Percentage Display** is enabled, indicating the percentage of quota used by the individual will display in the quota notice page. Click “Off” to not display this information in the quota notice page.

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:



http://200.10.100.75:81/cgi/quota.cgi?URL=http://www.test.com/&CAT=Quota%20Category&QA=N&Preview=on

QUOTA NOTICE HELP

You are nearing the category quota for your profile. You will be blocked from further access to this category when the quota is exceeded.

75% of quota limit has been exceeded.

Category: Quota Category
Requested URL: http://www.test.com/
IP:
User/Machine:

Continue

For assistance, contact your Administrator.
M86 Web Filter provided by M86 Security. Copyright 2011. All rights reserved.

Fig. 2:1-85 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 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 M86's Technical Support page that explains why access to the site or service may have been denied.
- **M86 Security** - Clicking this link takes the user to M86'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.

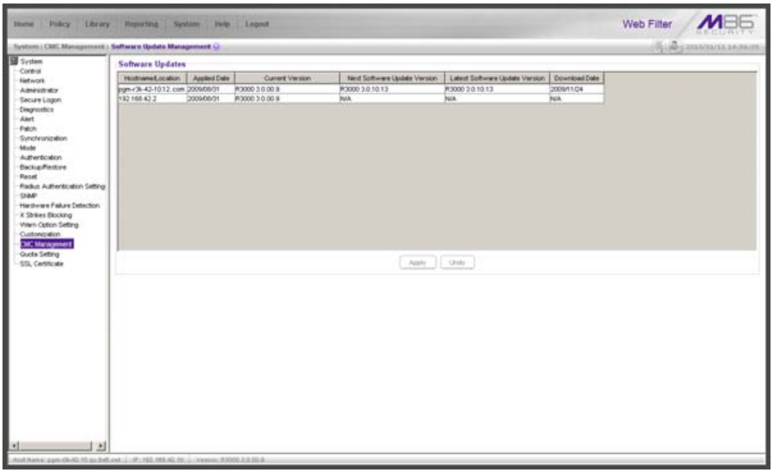
***TIP**: If necessary, make edits in the Quota Block Page Customization window or the Common Customization window, and then click **Preview** in this window again to view a sample quota block page.*

CMC Management

CMC Management displays on a Web Filter set up in the Source mode, and includes Centralized Management Console options for viewing the filtering statuses of this source server and its target server(s), and managing software updates on these servers.

Software Update Management window

The Software Update Management window displays when Software Update Management is selected from the CMC Management menu. This window is used for viewing software updates currently applied to the source and target servers and any available software updates, and applying software updates to these servers.



Software Updates

Hostname/Location	Applied Date	Current Version	Next Software Update Version	Latest Software Update Version	Download Date
pgm-r3k-42-10.12.com	2009/06/31	R3000 3.0.00.9	R3000 3.0.10.13	R3000 3.0.10.13	2009/11/24
192.168.42.2	2009/06/31	R3000 3.0.00.9	N/A	N/A	N/A

Fig. 2:1-86 Software Update Management window

View Software Update Information

The Software Updates frame displays the software update statuses of the source and each target Web Filter: Hostname/Location (information entered in the LAN Settings window for the source server's hostname, or the information entered for the target server in the Target Location field in the Setup window); Applied Date (date the software update was applied to the server, using the YYYY/MM/DD format); Current Version (software update build name and number); Next Software Update Version (name and number of the next software update to be applied, or N/A if there is none available); Latest Software Update Version (name and number of the latest software update, or N/A if there is none available); Download Date (date the latest software update was downloaded to the server, or N/A if there is none available).

***TIPS**: The entire grid can be viewed by using the scroll bar at the bottom of the Software Updates frame to scroll to the right and left.*

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.

*Columns can be resized by mousing over the line in the header between two columns so that a double-ended arrow (**<—>**) displays, and then clicking and dragging the cursor to the left or right.*

Apply or Undo a Software Update

To apply a software update:

1. Click to select the row(s) corresponding to the servers to be updated.
2. Click **Apply**.

***NOTES**: If the source server is selected for a software update, the EULA displays when the software update is about to be applied. See the sub-section for the Local Software Updates window for information about the EULA and applying software updates.*

Only a software update number that is lesser to, or equal to, the source server's software update number can be applied to a target server.

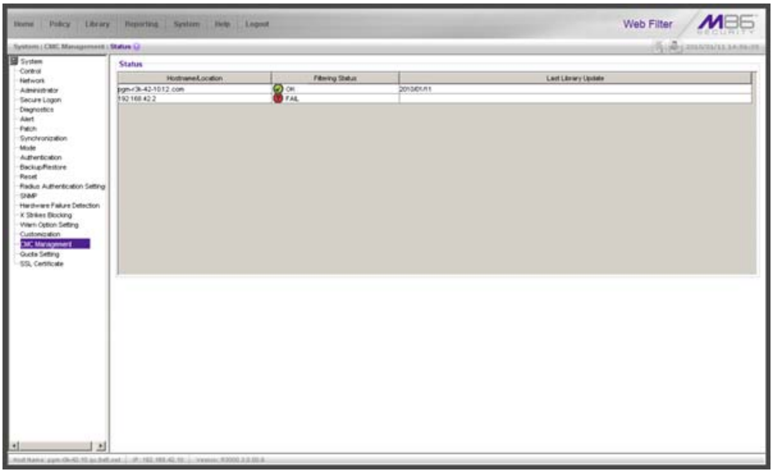
***TIP**: Multiple target servers can be selected to have a software update applied, if these target servers are currently running the same software version number.*

To undo a software update:

1. Select the row(s) corresponding to the server(s) that need(s) to have the last software update removed.
2. Clicking **Undo** to remove that software update from the server(s).

Status window

The Status window displays when Status is selected from the CMC Management menu. This window is used for viewing the filtering status of the source and target server(s) for troubleshooting purposes.



Hostname/Location	Filtering Status	Last Library Update
pgm-r3k-42-1012.com	✓ OK	2010/01/11
192.168.42.2	✕ FAIL	

Fig. 2:1-87 Status window, CMC Management menu

View Filtering Status Information

The Status frame displays the following columns of information:

- Hostname/Location - criteria entered in the LAN Settings window for the source server's hostname, or the information entered for the target server in the Target Location field of the Setup window
- Filtering Status - “OK” displays if the server is being filtered, or “FAIL” displays if the server is not being filtered

***NOTE**: Filtering Status information will only display if the “Upstream Failover Detect” option is enabled in the Synchronization > Setup window.*

- Last Library Update - most recent date the library was updated on the server, using the YYYY/MM/DD format, if this information is available.

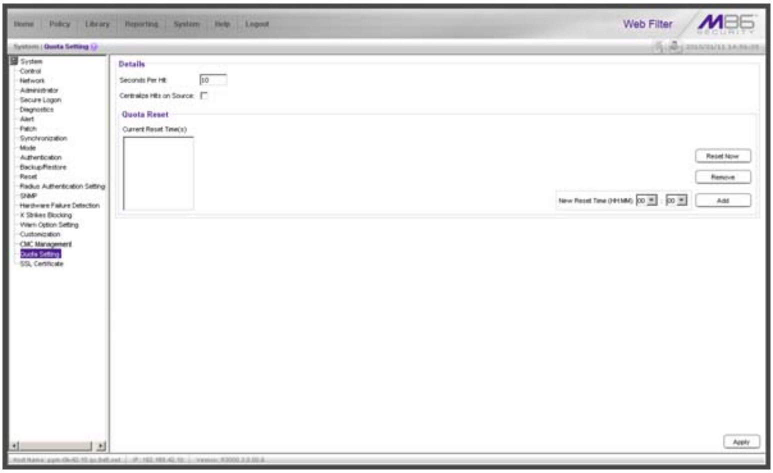
***TIPS**: The order in which columns display in the grid can be changed by clicking the column header and sliding the column to another position in the grid.*

*Columns can be resized by mousing over the line in the header between two columns so that a double-ended arrow (**<—>**) displays, and then clicking and dragging the cursor to the left or right.*

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.



Seconds Per Hit: 10

Centralize Hits on Source: □

New Reset Time (HH:MM): 00 : 00

Fig. 2:1-88 Quota Setting window

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

Configure Quota Hit Settings

1. 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**: This field is greyed-out if the Web Filter is set up as a target server in the synchronization mode.*

2. If this Web Filter is set up with synchronization and is a source server, enable **Centralize Hits on Source** only if all hits should be made on this Web Filter.

***NOTE**: This field is greyed-out on a Web Filter set up as either a standalone server or as target server in the synchronization mode.*

***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***.

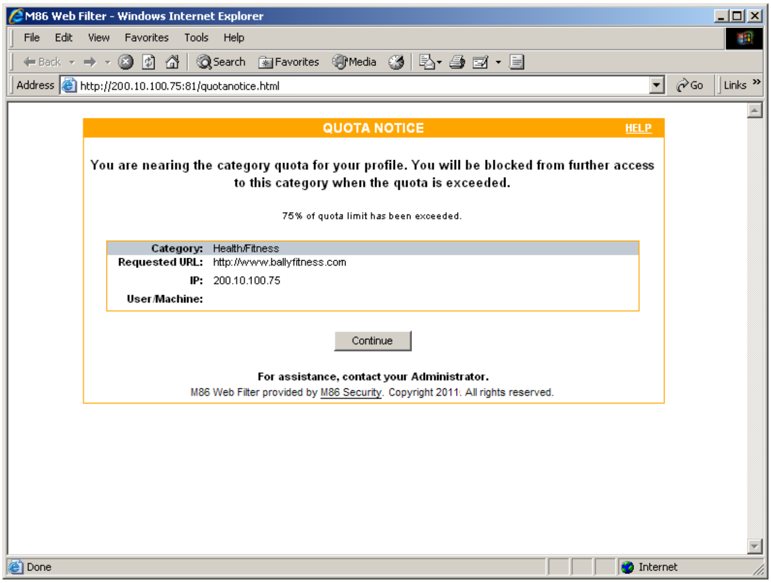
Delete a Quota Reset Time from the Schedule

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:


M86 Web Filter - Windows Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://200.10.100.75:81/quotanotice.html
Go Links
Done
Internet

QUOTA NOTICE HELP

You are nearing the category quota for your profile. You will be blocked from further access to this category when the quota is exceeded.

75% of quota limit has been exceeded.

Category:	Health/Fitness
Requested URL:	http://www.ballyfitness.com
IP:	200.10.100.75
User/Machine:	

Continue

For assistance, contact your Administrator.
M86 Web Filter provided by M86 Security. Copyright 2011. All rights reserved.

Fig. 2:1-89 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 LDAP user. This field is blank for the IP group user.

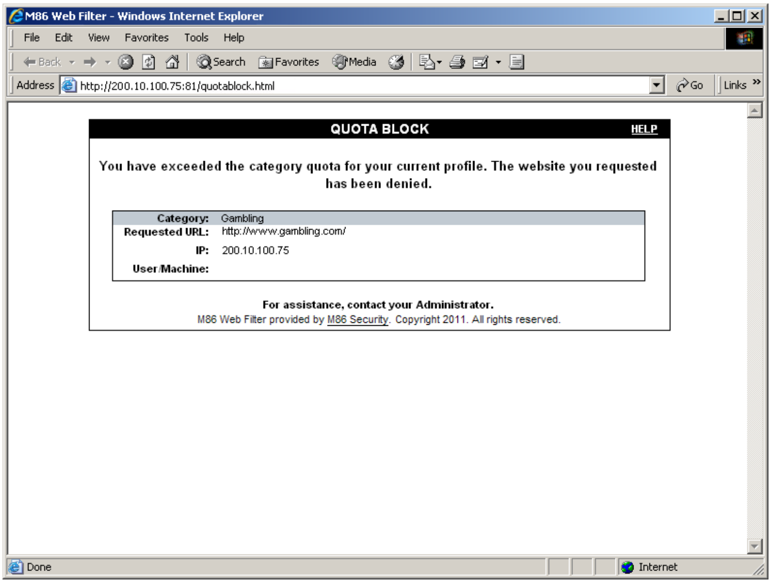
By default, the following standard links are included in the quota notice page:

- **HELP** - Clicking this link takes the user to M86's Technical Support page that explains why access to the site may have been denied.
- **M86 Security** - Clicking this link takes the user to M86'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:


M86 Web Filter - Windows Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://200.10.100.75:81/quotablock.html
Go Links
Done
Internet

QUOTA BLOCK HELP

You have exceeded the category quota for your current profile. The website you requested has been denied.

Category:	Gambling
Requested URL:	http://www.gambling.com/
IP:	200.10.100.75
User/Machine:	

For assistance, contact your Administrator.

M86 Web Filter provided by M86 Security. Copyright 2011. All rights reserved.

Fig. 2:1-90 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 LDAP user. This field may be blank for the IP group user.

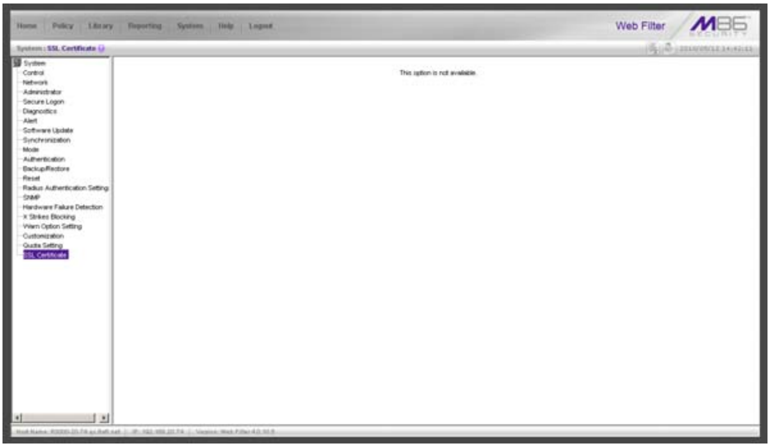
By default, the following standard links are included in the quota block page:

- **HELP** - Clicking this link takes the user to M86's Technical Support page that explains why access to the site or service may have been denied.
- **M86 Security** - Clicking this link takes the user to M86's Web site.

SSL Certificate

SSL Certificate window

The SSL Certificate window displays when SSL Certificate is selected from the navigation panel. This window is not available in the Web Filter user interface of the WFR since this function is executed in the Security Reporter user interface.

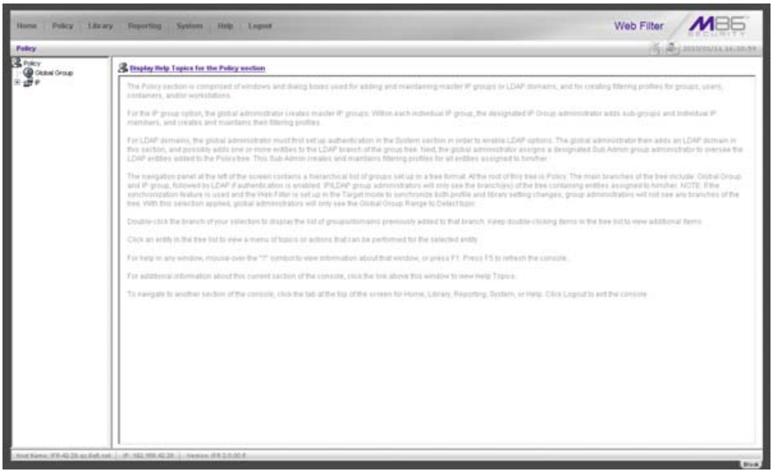


This option is not available.

Fig. 2:1-91 SSL Certificate window

Chapter 2: Policy screen

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



Display Help Topics for the Policy section

The Policy section is comprised of windows and dialog boxes used for adding and maintaining master IP groups or LDAP domains, and for creating filtering profiles for groups, users, containers, and/or workstations.

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

For LDAP domains, the global administrator must first set up authentication in the System section in order to enable LDAP options. The global administrator then adds an LDAP domain in this section, and possibly adds one or more entities to the LDAP branch of the group tree. Next, the global administrator assigns a designated Sub Admin group administrator to oversee the LDAP entities added to the Policy tree. This Sub Admin creates and maintains filtering profiles for all entities assigned to him/her.

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 Policy. The main branches of the tree include: Global Group and IP group, followed by LDAP if authentication is enabled. IP/LDAP group administrators will only see the branch(es) of the tree containing entities assigned to him/her. NOTE: If the synchronization feature is used and the Web Filter is set up in the Target mode to synchronize both profile and library setting changes, group administrators will not see any branches of the tree. With this selection applied, global administrators will only see the Global Group Range to Detect topic.

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 the selected entity.

For help in any window, mouse-over the "?" symbol to view information about that window, or press F1. Press F5 to refresh the console.

For additional information about this current section of the console, click the link above this window to view Help Topics.

To navigate to another section of the console, click the tab at the top of the screen for Home, Library, Reporting, System, or Help. Click Logout to exit the console.

Fig. 2:2-1 Policy 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 LDAP domain branch, the global administrator must first set up authentication in order to enable the 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 Policy. The main branches of this tree include: Global Group and IP, followed by 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 LDAP groups can be found in the M86 Web Filter Authentication User Guide.*

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

If using the synchronization feature, if the Web Filter being configured is set up in the Target mode to synchronize both profile and library setting changes, the only branch that displays in the tree is Global Group.

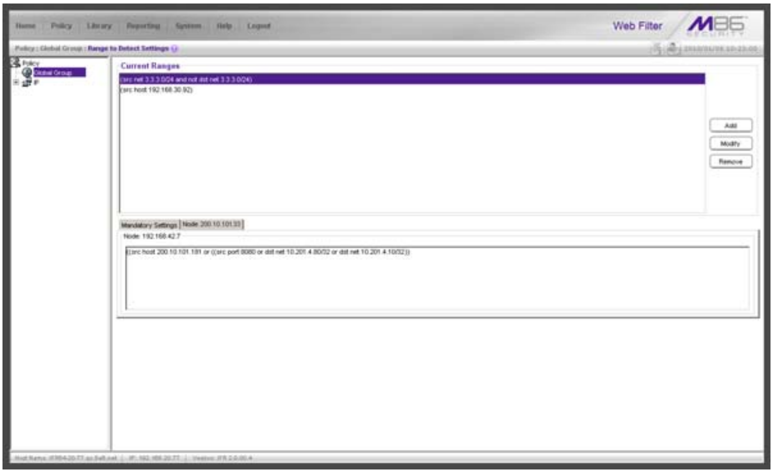
Global Group

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, Approved Content (incl. VuSafe), Minimum Filtering Level, and Refresh All.

NOTE*: If the synchronization feature is used and this Web Filter being configured is set up in the Target mode to synchronize both profile and library setting changes, the only sub-topic that displays is Range to Detect.*

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 Web Filter in the invisible or router mode. Service ports that should be open—ignored by the Web Filter—are also defined in this window.



(src net 3.3.3.0/24 and not dst net 3.3.3.0/24)
(src host 192.168.30.92)

Node: 192.168.42.7

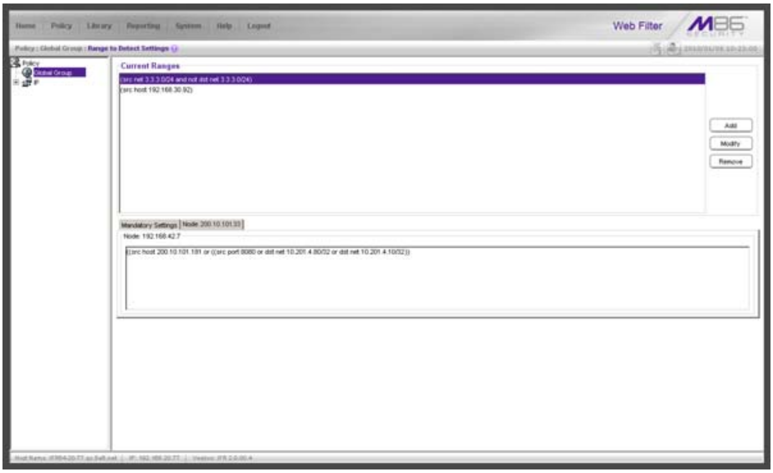
((src host 200.10.101.181 or ((src port 8080 or dst net 10.201.4.80/32 or dst net 10.201.4.10/32))

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

***NOTE**: Segments of network traffic should not be defined if using the firewall mode.*

The main window (Fig. 2:2-2) 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.

***NOTE**: If this Web Filter is using the Source mode and the Upstream Failover Detect feature is enabled, if a downstream target server fails—as detected by the Appliance Watchdog—the Current Ranges information from the failed downstream target "node" displays in a Node tab following the Mandatory Settings tab in this window:*



Current Ranges

(src net 3.3.3.0/24 and not dst net 3.3.3.0/24)
(src host 192.168.30.92)

Mandatory Settings | Node 200.10.101.33

Node: 192.168.42.7

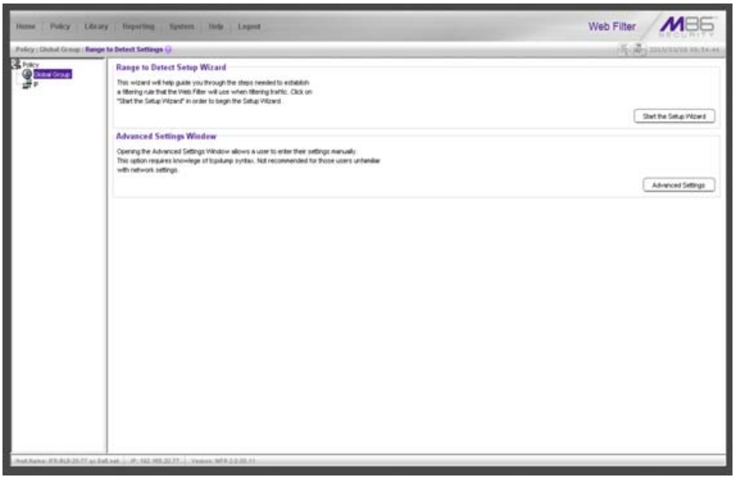
((src host 200.10.101.181 or ((src port 8080 or dst net 10.201.4.80/32 or dst net 10.201.4.10/32))

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

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:



Range to Detect Setup Wizard

This wizard will help guide you through the steps needed to establish a filtering rule that the Web Filter will use when filtering traffic. Click on "Start the Setup Wizard" in order to begin the Setup Wizard.

Advanced Settings Window

Opening the Advanced Settings Window allows a user to enter their settings manually. This option requires knowledge of tcpdump syntax. Not recommended for those users unfamiliar with network settings.

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:

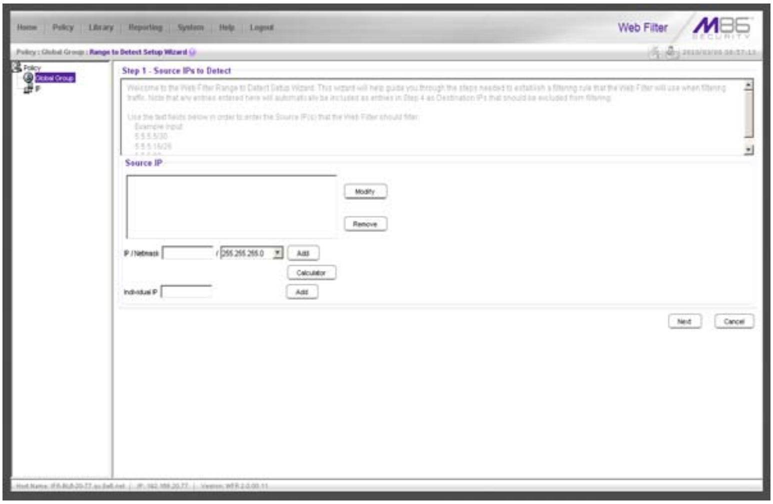
   - **Start the Setup Wizard** - clicking this button takes you to the Range to Detect Setup Wizard. Follow the instructions in the Range to Detect Setup Wizard sub-section to complete the addition of the segment on the network.
   - **Advanced Settings** - clicking this button takes you to the Range to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



Home | Policy | Library | Reporting | System | Help | Logout
Web Filter
M86 SECURITY
Policy : Global Group : Range to Detect Setup Wizard
Policy
Global Group
IP
Source IP
Modify
Remove
Add
Calculator
Add
Next
Cancel

Step 1 - Source IPs to Detect

Welcome to the Web Filter Range to Detect Setup Wizard. This wizard will help guide you through the steps needed to establish a filtering rule that the Web Filter will use when filtering traffic. Note that any entries entered here will automatically be included as entries in Step 4 as Destination IPs that should be excluded from filtering.

Use the text fields below in order to enter the Source IP(s) that the Web Filter should filter:
Example input:
5.5.5.5/30
5.5.5.16/28

IP / Netmask: / 255.255.255.0

Individual IP:

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**.*

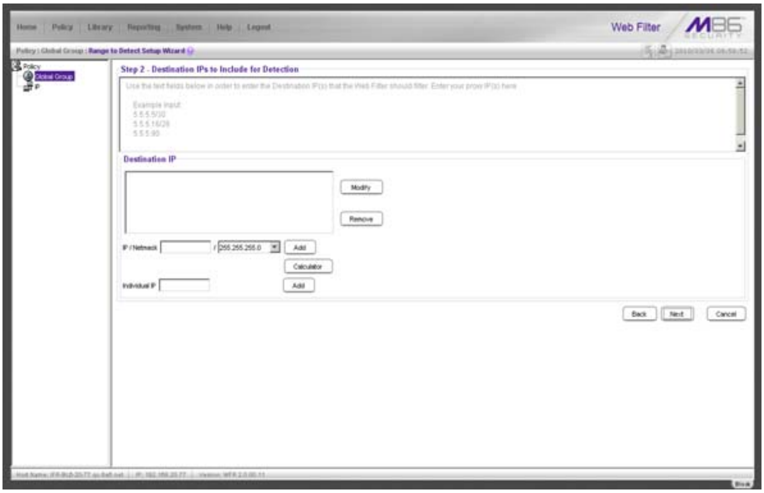
3. Click **Next** to go to the next page of the Wizard.

***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 Web Filter, thus enabling it to handle more traffic.*



Step 2 - Destination IPs to Include for Detection

Use the text fields below in order to enter the Destination IP(s) that the Web Filter should filter. Enter your proxy IP(s) here.

Example input:
5.5.5.5/30
5.5.5.16/28
5.5.5.90

Destination IP

IP / Netmask / 255.255.255.0

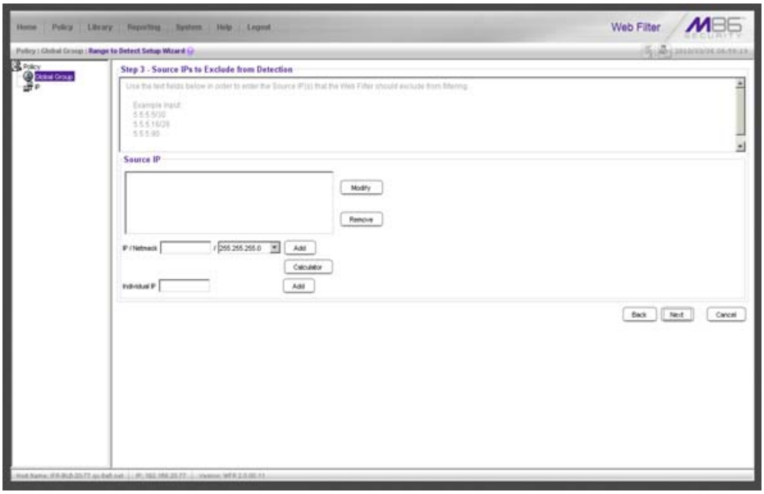
Individual IP

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.


Home | Policy | Library | Reporting | System | Help | Logout
Web Filter
M86 SECURITY
Policy : Global Group : Range to Detect Setup Wizard
Policy
Global Group
IP
Step 3 - Source IPs to Exclude from Detection
Source IP
Modify
Remove
IP / Netmask
Add
Calculator
Individual IP
Add
Back
Next
Cancel

Use the text fields below in order to enter the Source IP(s) that the Web Filter should exclude from filtering.

Example input:
5.5.5.5/30
5.5.5.16/28
5.5.5.90

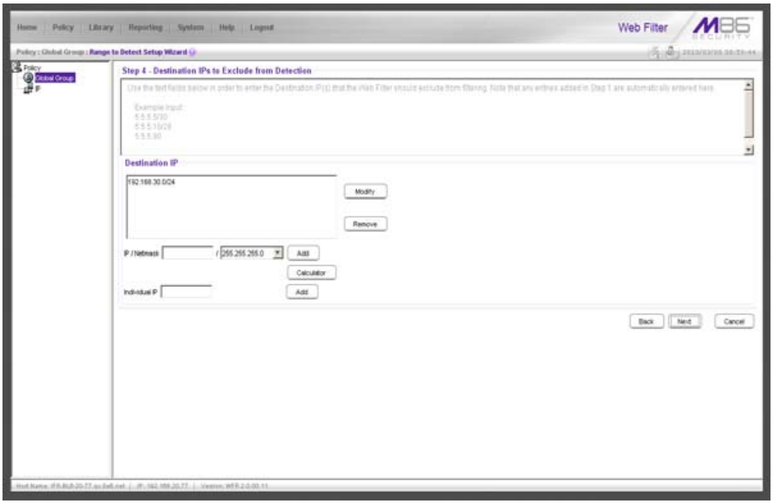
IP / Netmask: / 255.255.255.0

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 Web Filter, thus enabling it to handle more traffic.*



Step 4 - Destination IPs to Exclude from Detection

Use the text fields below in order to enter the Destination IP(s) that the Web Filter should exclude from filtering. Note that any entries added in Step 1 are automatically entered here.

Example input:
5.5.5.5/30
5.5.5.10/28
5.5.5.90

Destination IP

192.168.30.0/24

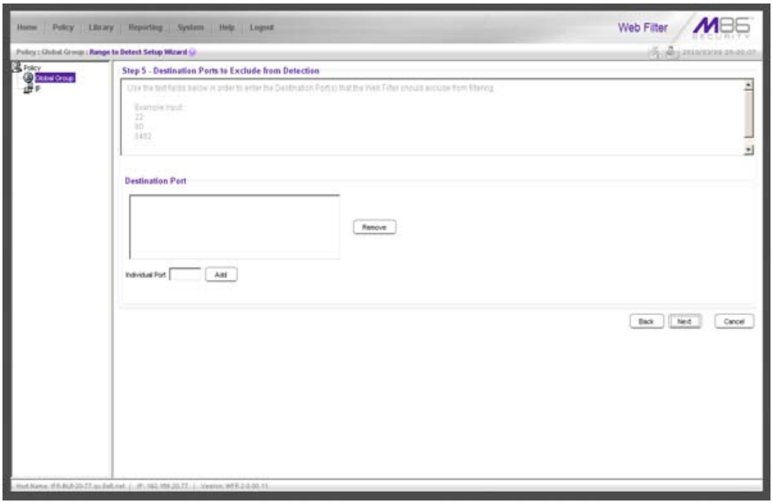
IP / Netmask: / 255.255.255.0

Individual IP:

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.



Step 5 - Destination Ports to Exclude from Detection

Use the text fields below in order to enter the Destination Port(s) that the Web Filter should exclude from filtering.

Example input:
22
80
8452

Destination Port

Individual Port:

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

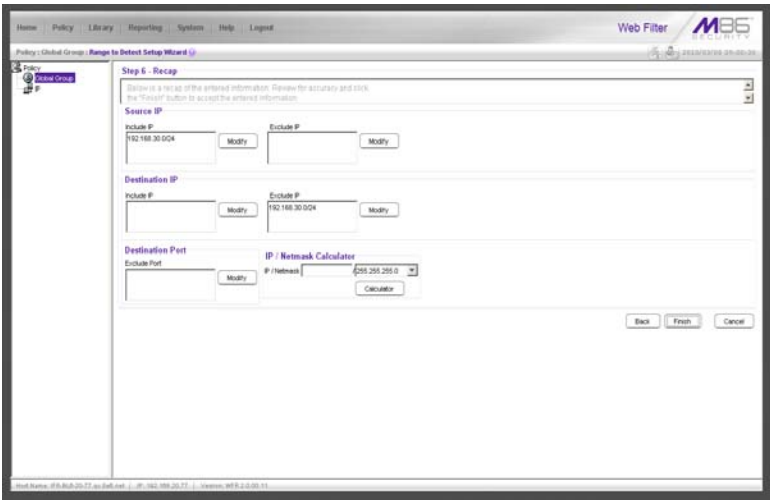
1. In the **Individual Port** field, enter the port number to be excluded from filtering.
2. Click **Add** to include the entry in the list box above.

***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.



Step 6 - Recap

Below is a recap of the entered information. Review for accuracy and click the "Finish" button to accept the entered information.

Source IP

Include IP: 192.168.30.0/24

Exclude IP:

Destination IP

Include IP:

Exclude IP: 192.168.30.0/24

Destination Port

Exclude Port:

IP / Netmask Calculator

IP / Netmask: 255.255.255.0

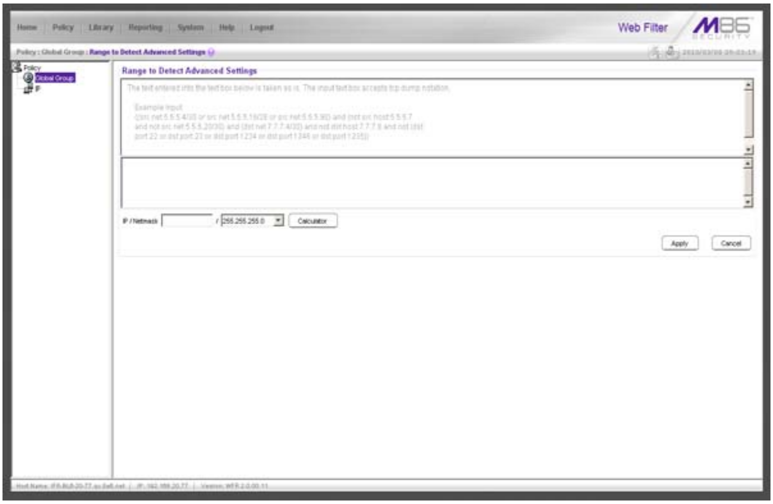
Fig. 2:2-10 Range to Detect Setup Wizard window, Step 6

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:



The text entered into the text box below is taken as is. The input text box accepts tcp dump notation.

Example Input:
(src net 5.5.5.4/30 or src net 5.5.5.16/28 or src net 5.5.5.8/30) and (not src host 5.5.5.7
and not src net 5.5.5.20/30) and (dst net 7.7.7.4/30) and not dst host 7.7.7.8 and not (dst
port 22 or dst port 23 or dst port 1234 or dst port 1345 or dst port 12345))

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. 2:2-2), 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.

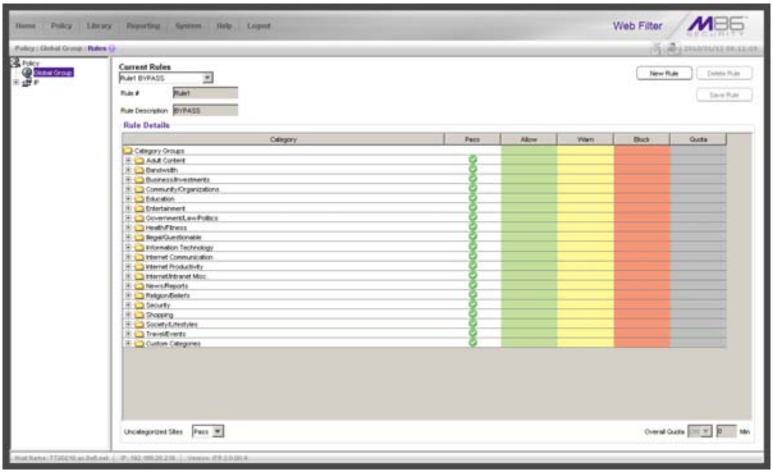
Remove a Segment from the Network

To remove a segment:

1. In the main Range to Detect Settings window (see Fig. 2:2-2), 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.



Current Rules: Rule1 BYPASS

Rule #: Rule1

Rule Description: BYPASS

Category	Pass	Allow	Warn	Block	Quota
Category Groups					
Adult Content	✓				
Bandwidth	✓				
Business/Investments	✓				
Community/Organizations	✓				
Education	✓				
Entertainment	✓				
Government/Law/Politics	✓				
Health/Fitness	✓				
Illegal/Questionable	✓				
Information Technology	✓				
Internet Communication	✓				
Internet Productivity	✓				
Internet/Intranet Misc	✓				
News/Reports	✓				
Religion/Beliefs	✓				
Security	✓				
Shopping	✓				
Society/Lifestyles	✓				
Travel/Events	✓				
Custom Categories	✓				

Uncategorized Sites: Pass

Overall Quota: Off 0 Min

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 M86 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 M86 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**.

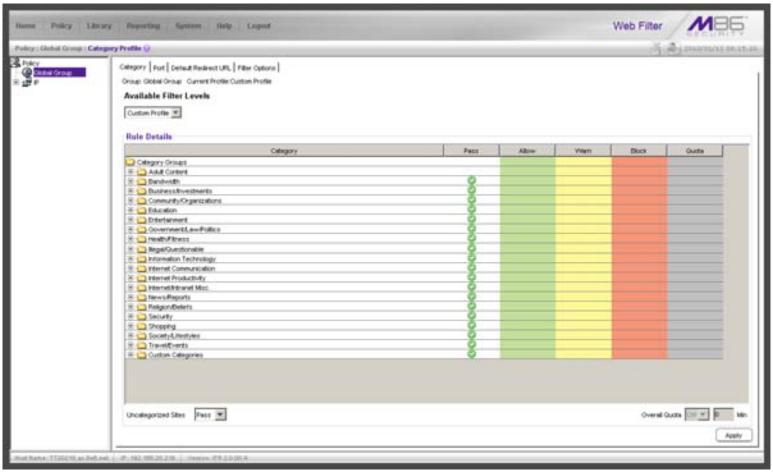
Remove a Rule

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.


Home
Policy
Library
Reporting
System
Help
Logout
Web Filter
M86 SECURITY
Policy : Global Group : Category Profile
Policy
Global Group
IP
Category | Port | Default Redirect URL | Filter Options |
Apply

Group: Global Group Current Profile: Custom Profile

Available Filter Levels: Custom Profile

Rule Details

Category	Pass	Allow	Warn	Block	Quota
Category Groups					
Adult Content					
Bandwidth	✓				
Business/Investments	✓				
Community/Organizations	✓				
Education	✓				
Entertainment	✓				
Government/Law/Politics	✓				
Health/Fitness	✓				
Illegal/Questionable	✓				
Information Technology	✓				
Internet Communication	✓				
Internet Productivity	✓				
Internet/Intranet Misc	✓				
News/Reports	✓				
Religion/Beliefs	✓				
Security	✓				
Shopping	✓				
Society/Lifestyles	✓				
Travel/Events	✓				
Custom Categories	✓				

Uncategorized Sites: Pass

Overall Quota: Off 0 Min

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.

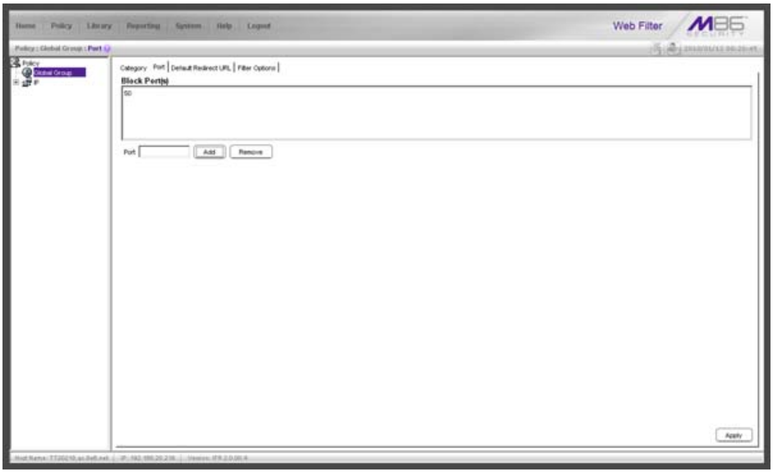


Fig. 2:2-14 Global Group Profile window, Port tab

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:

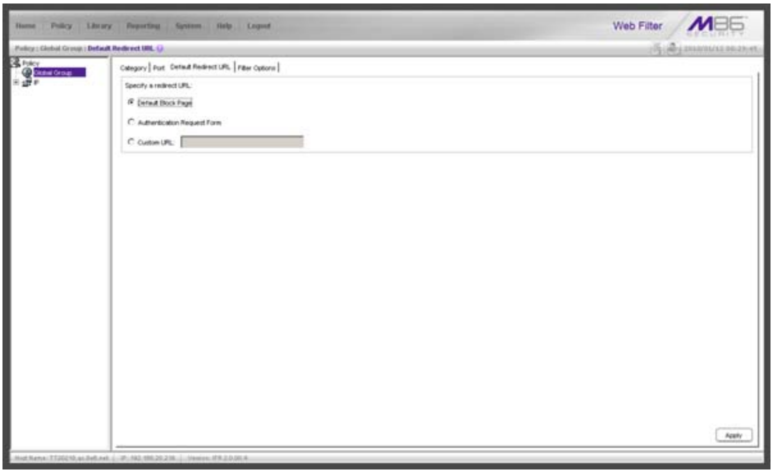
1. Enter the port number in the **Port** field.
2. Click **Add**. Each port number you add displays in the Block Port(s) list box.
3. Click **Apply** to apply your settings at the global level.

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.



Specify a redirect URL:

● Default Block Page

○ Authentication Request Form

○ Custom URL:

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

Create, Edit the Redirect URL

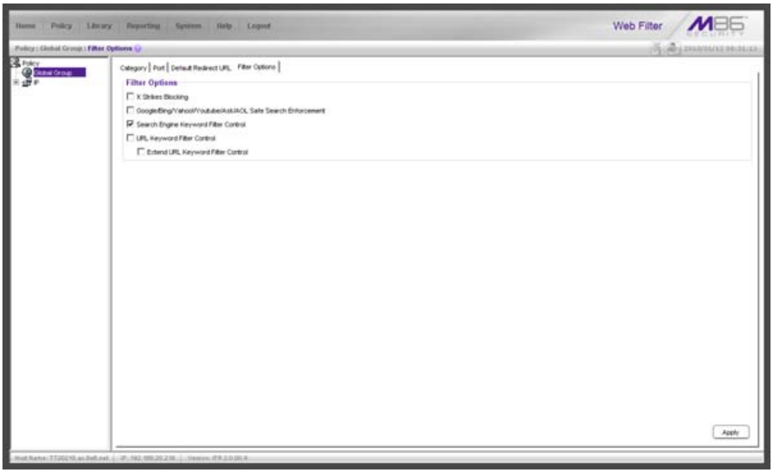
1. Specify the type of redirect URL to be used: “Default Block Page”, “Authentication Request Form”, or “Custom URL”.

   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.



Filter Options

☐ X Strikes Blocking
☐ Google/Bing/Yahoo!/Youtube/Ask/AOL Safe Search Enforcement
☑ Search Engine Keyword Filter Control
☐ URL Keyword Filter Control
☐ Extend URL Keyword Filter Control

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/Bing/Yahoo!/Youtube/Ask/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/Bing/Yahoo!/Youtube/Ask/AOL Safe Search Enforcement

With the Google/Bing/Yahoo!/Youtube/Ask/AOL Safe Search Enforcement option enabled, Google, Bing.com, Yahoo!, YouTube, Ask.com, and AOL’s “strict” SafeSearch Filtering option will be used whenever end users perform a Google, Bing.com, Yahoo!, YouTube, 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 M86’s library or is blocked by Google, Bing.com, Yahoo!, YouTube, 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, Bing.com, Yahoo!, YouTube, 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, Bing.com, Yahoo!, YouTube, Ask.com, or AOL images returned by the query to load on the page. The user receives 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 M86 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:

- *M86 Supplied Categories - see Chapter 3: Library screen, Search Engine Keywords window in this section.*
- *Custom Categories - see the WF 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 M86 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:*

- *M86 Supplied Categories - see Chapter 3: Library screen, URL Keywords window, in this section.*
- *Custom Category - see the WF 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.

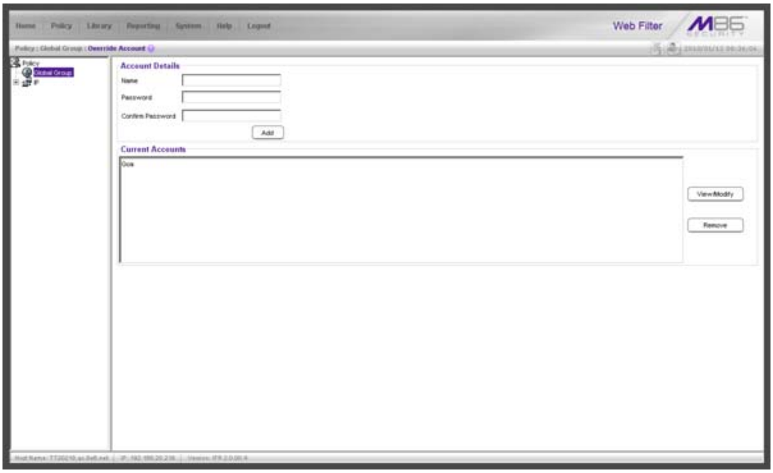


Fig. 2:2-17 Override Account window

***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 WF Group Administrator Section for information on setting up an override account for a user in an IP group.*

See Appendix C: 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.

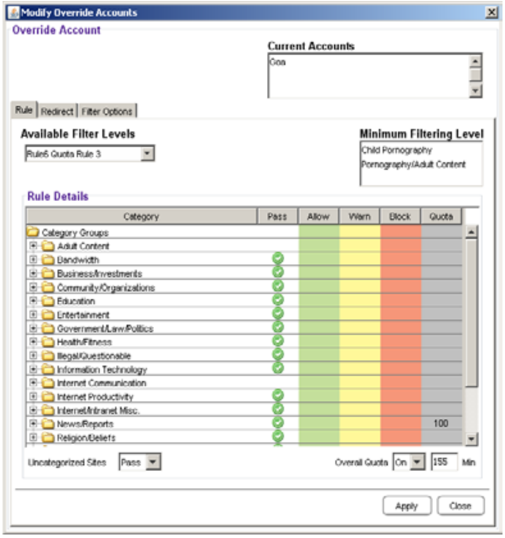
Add an Override Account

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.



Current Accounts: Goa

Available Filter Levels: Rule6 Quota Rule 3

Minimum Filtering Level: Child Pornography, Pornography/Adult Content

Category	Pass	Allow	Warn	Block	Quota
Category Groups					
Adult Content					
Bandwidth	✓				
Business/Investments	✓				
Community/Organizations	✓				
Education	✓				
Entertainment	✓				
Government/Law/Politics	✓				
Health/Fitness	✓				
Illegal/Questionable	✓				
Information Technology	✓				
Internet Communication					
Internet Productivity	✓				
Internet/Intranet Misc.	✓				
News/Reports	✓				100
Religion/Beliefs	✓				

Uncategorized Sites: Pass

Overall Quota: On 155 Min

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.*

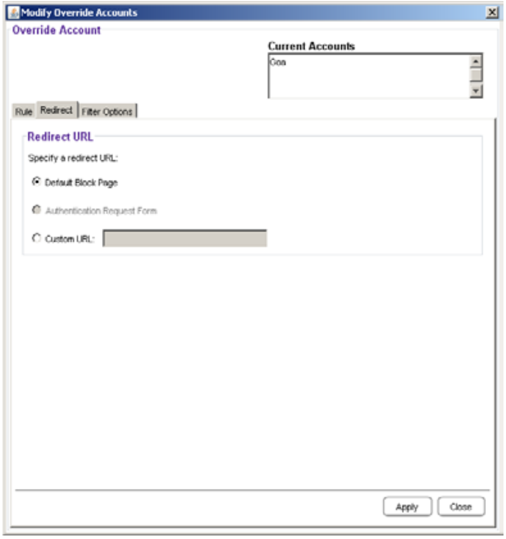
- The **Overall Quota** field becomes enabled if a quota is entered for any library group/category. By default, the enabled Overall Quota is turned “Off”. If turned “On”, enter the number of minutes in the **Min** field to indicate when the end user’s access to passed library groups/categories with quotas 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.



Current Accounts: Gon

Specify a redirect URL:

● Default Block Page

○ Authentication Request Form

○ Custom URL:

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”.

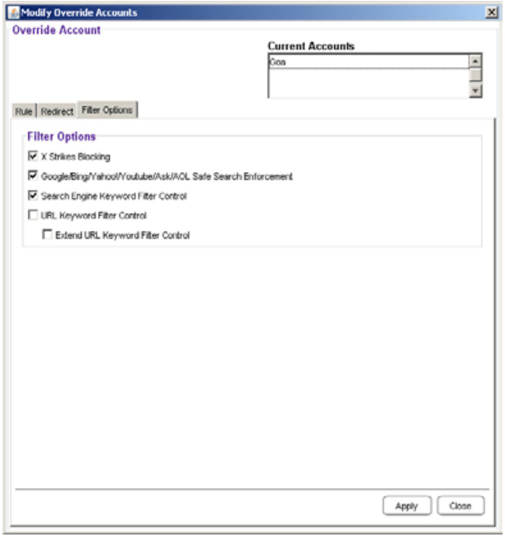
   If “Custom URL” is selected, enter the redirect URL in the corresponding text box. The user will be redirected to the designated page at this URL instead of the block page.

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.



Current Accounts: Goa

Filter Options

- ☑ X Strikes Blocking
- ☑ Google/Bing/Yahoo!/Youtube/Ask/AOL Safe Search Enforcement
- ☑ Search Engine Keyword Filter Control
- ☐ URL Keyword Filter Control
  - ☐ Extend URL Keyword Filter Control

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/Bing/Yahoo!/Youtube/Ask/AOL Safe Search Enforcement” - With the Google/Yahoo!/Youtube/Ask/ AOL Safe Search Enforcement option enabled, Google, Bing.com, Yahoo!, YouTube, Ask.com, and AOL’s “strict” SafeSearch Filtering option will be used whenever the end user performs a Google, Bing.com, Yahoo!, YouTube, 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, Bing.com, Yahoo!, YouTube, 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, Bing.com, Yahoo!, YouTube, 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 M86 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:*

- *M86 Supplied Categories - see Chapter 3: Library screen, Search Engine Keywords window.*
- *Custom Categories - see the WF 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 M86 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:*

- *M86 Supplied Categories - see Chapter 3: Library screen, URL Keywords window.*
- *Custom Category - see the WF 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.

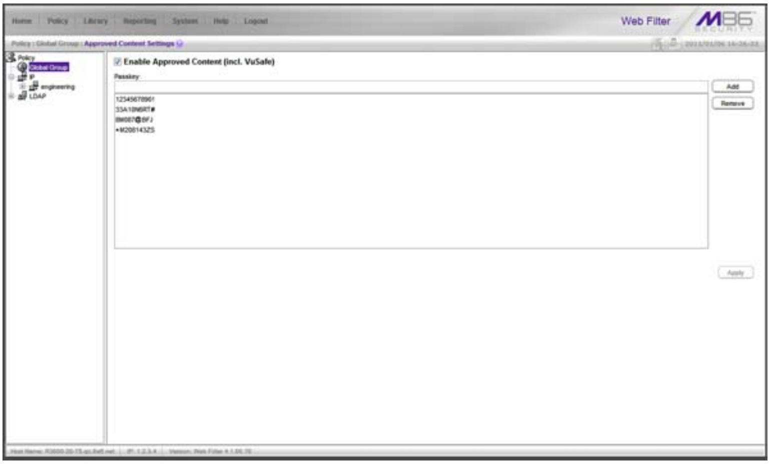
Delete an Override Account

To delete an override account:

1. In the Current Accounts frame, select the username from the list box.
2. Click **Remove**.

Approved Content Settings window

The Approved Content Settings window displays when Approved Content (incl. VuSafe) is selected from the Global Group menu. This window is used for granting designated users access to a specified set of approved online videos posted to YouTube or SchoolTube via a portal managed by someone within your organization.



☑ Enable Approved Content (incl. VuSafe)

Passkey:

12345678901
33A10N6RT#
8M087@BFJ
+M20814325

Fig. 2:2-21 Approved Content Settings window

Approved Content feature and VuSafe

The Approved Content feature, primarily used by the education sector, lets administrators specify which online videos posted to YouTube or SchoolTube are appropriate for students to view, while blocking all other videos posted to these video viewing Web sites.

VuSafe is an online content library to which educators can post approved, educational videos for students to watch in a secure environment. VuSafe removes all outside content on sites such as YouTube.com, eliminating access to inappropriate material. This free Web-based service requires no additional software or hardware setup. Enabling the

Approved Content feature in a user’s profile gives that user access to videos posted to VuSafe.

Approved Content setup and configuration

There are two parts to set up in order to use the Approved Content feature:

- A portal for viewing videos must be created
- The passkey of each approved video must be entered in the Approved Content Settings window for the user’s profile

NOTE*: If Pattern Blocking is enabled (System > Control > Filter > Service Control frame), then the filtering profile must "Allow" the Flash Video (FLV) pattern (Category Groups > Bandwidth > Streaming Media > Flash Video).*

Approved Content portal setup

To create a portal for users to view approved YouTube and/or SchoolTube videos, you will need the following:

- Online Web page or intranet page that you or someone in your organization will maintain for users to view approved videos
- Text editor tool such as Notepad or TextPad
- MD5 checksum calculator tool

Once you have access to the aforementioned items, follow the instructions in the M86 Approved Content Portal Setup document at **http://www.m86security.com/software/8e6/docs/ug/misc/wf.ac.4.1.00.pdf** .

As explained in the portal setup document, a passkey must be created for each video to be included in the portal. This passkey needs to be entered in the Approved Content Settings window associated with the user’s profile.

Approved Content Settings entries

Once you have passkeys created for the approved videos, you can begin making entries in the Approved Content Settings window.

Step 1: Enable Global Group Passkey inheritance

To allow any user to inherit a set of passkeys if the Approved Content feature is enabled in his/her profile, click the “Enable Approved Content (incl. VuSafe)” checkbox.

Step 2: Add/Remove Passkeys

To add a passkey to the Passkey list box:

1. Enter the eight to 20 character code (comprised of at least one alpha character, one numeric character, and one special character).

__TIP__: The passkey entry is case-sensitive and must precisely match the passkey used for the video.

2. Click **Add**.

__TIP__: To remove a passkey from the list box, select it and then click __Remove__.

Step 3: Save your entries

Click **Apply** to save your entries.

__NOTE__: By disabling the inheritance of passkeys, none of the passkeys entered and saved in the Passkeys list box will be available for users set up in the Policy tree. Though these users can be set up to use the Approved Content feature, they will need to have passkeys entered and saved in their profiles.

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.

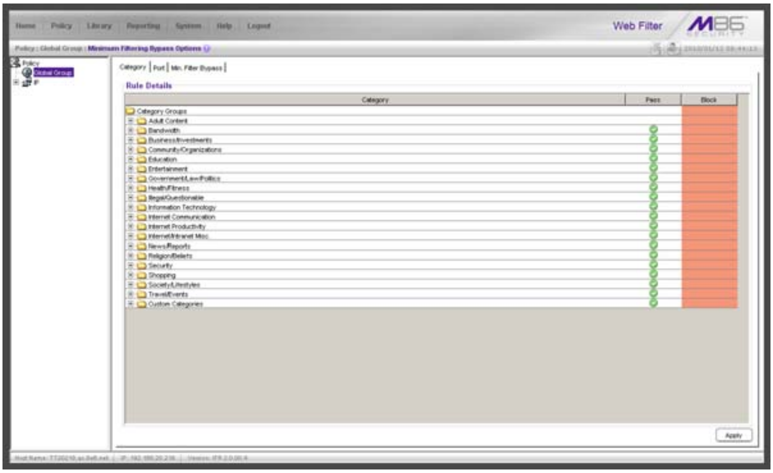
The minimum filtering level is created by making selections from the list of library categories and service ports. These settings can be bypassed if a user has an override account.

NOTE*: See the Override Account window in this chapter and in Chapter 1 of the WF 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.



Rule Details

Category	Pass	Block
Category Groups		
Adult Content		
Bandwidth	✓	
Business/Investments	✓	
Community/Organizations	✓	
Education	✓	
Entertainment	✓	
Government/Law/Politics	✓	
Health/Fitness	✓	
Illegal/Questionable	✓	
Information Technology	✓	
Internet Communication	✓	
Internet Productivity	✓	
Internet/Intranet Misc	✓	
News/Reports	✓	
Religion/Beliefs	✓	
Security	✓	
Shopping	✓	
Society/Lifestyles	✓	
Travel/Events	✓	
Custom Categories	✓	

Fig. 2:2-22 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.

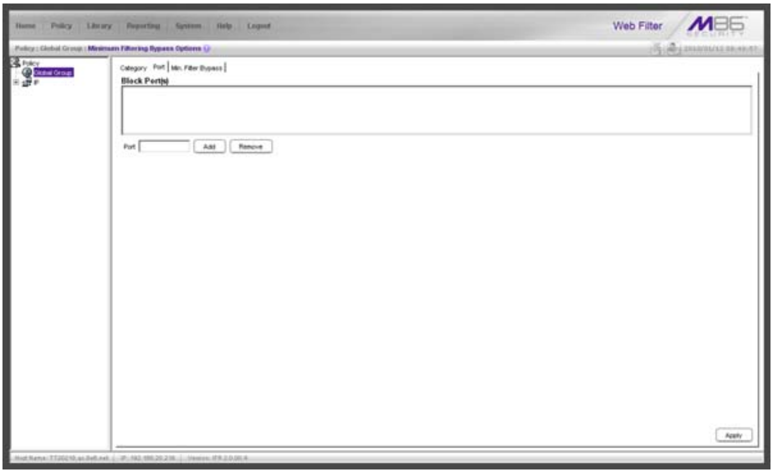


Fig. 2:2-23 Minimum Filtering Level window, Port tab

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.

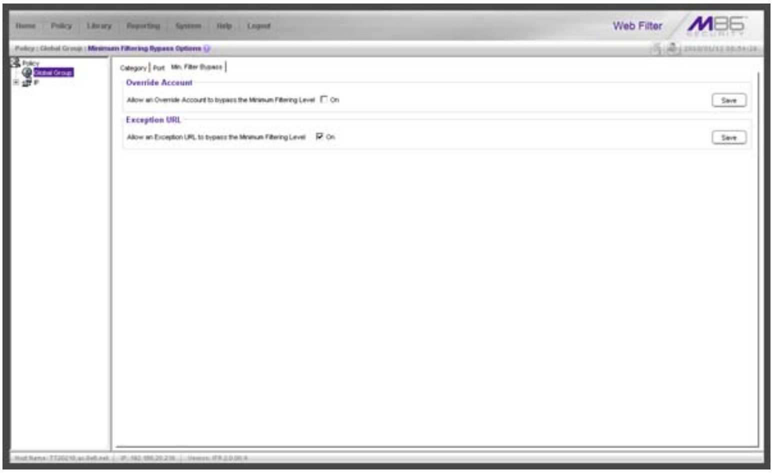
To remove a port number from the list box:

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.



Override Account

Allow an Override Account to bypass the Minimum Filtering Level □ On

Exception URL

Allow an Exception URL to bypass the Minimum Filtering Level ☑ On

Fig. 2:2-24 Minimum Filtering Level window, Min. Filter Bypass tab

***NOTE**: See the Override Account window and Exception URL window of the Policy 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 WF 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 LDAP branch of the tree displays. 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.

Add Group

Add a Master IP Group

From the IP group menu:

1. Choose Add Group to open the Create New Group dialog box:

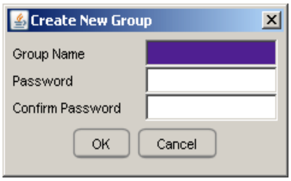


Fig. 2:2-25 Create New Group box

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” 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.*

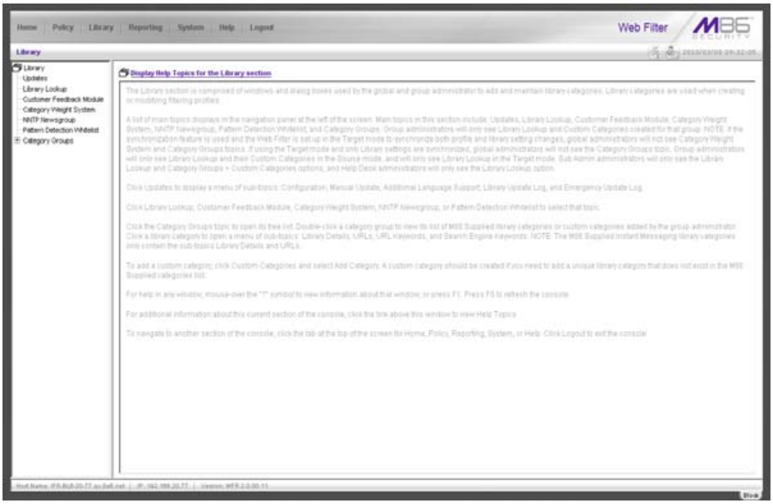
Refresh

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.



The Library section is comprised of windows and dialog boxes used by the global and group administrator to add and maintain library categories. Library categories are used when creating or modifying filtering profiles.

A list of main topics displays in the navigation panel at the left of the screen. Main topics in this section include: Updates, Library Lookup, Customer Feedback Module, Category Weight System, NNTP Newsgroup, Pattern Detection Whitelist, and Category Groups. Group administrators will only see Library Lookup and Custom Categories created for that group. NOTE: If the synchronization feature is used and the Web Filter is set up in the Target mode to synchronize both profile and library setting changes, global administrators will not see Category Weight System and Category Groups topics. If using the Target mode and only Library settings are synchronized, global administrators will not see the Category Groups topic. Group administrators will only see Library Lookup and their Custom Categories in the Source mode, and will only see Library Lookup in the Target mode. Sub Admin administrators will only see the Library Lookup and Category Groups > Custom Categories options, and Help Desk administrators will only see the Library Lookup option.

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, Customer Feedback Module, Category Weight System, NNTP Newsgroup, or Pattern Detection Whitelist to select that topic.

Click the Category Groups topic to open its tree list. Double-click a category group to view its list of M86 Supplied library categories or custom categories added by the group administrator. Click a library category to open a menu of sub-topics: Library Details, URLs, URL Keywords, and Search Engine Keywords. NOTE: The M86 Supplied Instant Messaging library categories only contain the sub-topics Library Details and URLs.

To add a custom category, click Custom Categories and select Add Category. A custom category should be created if you need to add a unique library category that does not exist in the M86 Supplied categories list.

For help in any window, mouse-over the "?" symbol to view information about that window, or press F1. Press F5 to refresh the console.

For additional information about this current section of the console, click the link above this window to view Help Topics.

To navigate to another section of the console, click the tab at the top of the screen for Home, Policy, Reporting, System, or Help. Click Logout to exit the console.

Host Name: [illegible] | IP: 192.168.20.77 | Version: WFR 2.0.00.11

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, Customer Feedback Module, Category Weight System, NNTP Newsgroup, Pattern Detection Whitelist, and Category Groups.

NOTE*: If the synchronization feature is used, a Web Filter set up in the Target mode to synchronize both profile and library setting changes will only display the Updates, Library Lookup, Customer Feedback Module, NNTP Newsgroup, and Pattern Detection Whitelist topics.*

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, Customer Feedback Module, Category Weight System, NNTP Newsgroup, or Pattern Detection Whitelist 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 M86 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 add a custom category, click Custom Categories and select Add Category.

NOTES*: Information on creating and maintaining Custom Categories can be found in the Group Administrator Section of this portion of the user guide.*

See Appendix A in the Appendices Section for the URL to the page that provides a list of M86 supplied library categories.

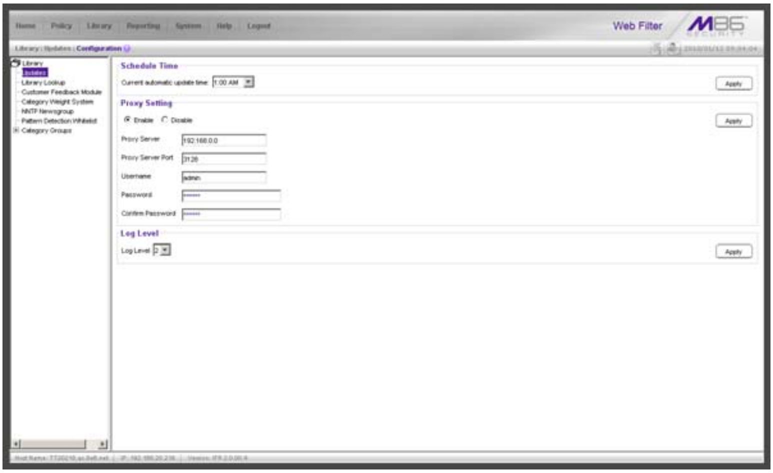
Instant Messaging library categories only include Library Details and URLs sub-topics.

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.

Configuration window

The Configuration window displays when Configuration is selected from the Updates menu. This window is used for making settings to allow the Web Filter to receive M86 supplied library category updates on a daily basis.



Schedule Time

Current automatic update time: 1:00 AM

Proxy Setting

● Enable ○ Disable

Proxy Server: 192.168.0.0

Proxy Server Port: 3128

Username: admin

Password: ••••••

Confirm Password: ••••••

Log Level

Log Level: 2

Fig. 2:3-2 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

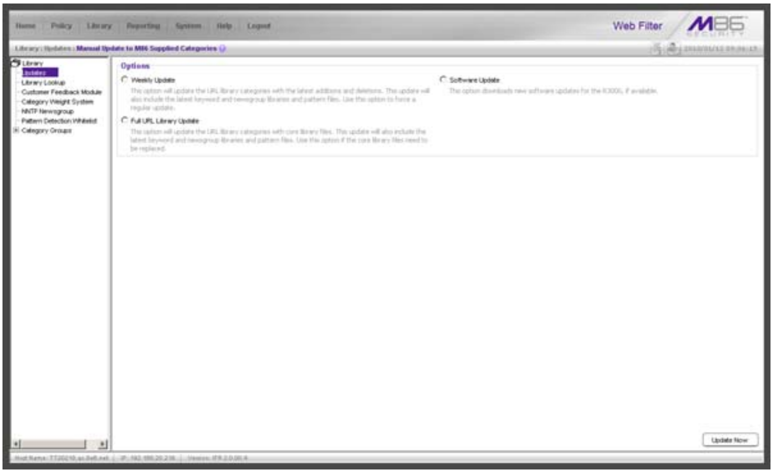
1. In the FTP Proxy Setting frame, by default “Disable” is selected. Click “Enable” if the server is in a proxy server environment. This selection activates the fields in this frame.
2. By default, *proxy.company.com* displays as the host name of the **Proxy Server**. Enter the host name for the proxy 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 M86 Supplied Categories window displays when Manual Update is selected from the Updates menu. This window is used for updating specified M86 supplied library categories on demand from the update server, if the Web Filter has not received daily updates due to an occurrence such as a power outage.



Options

○ Weekly Update

This option will update the URL library categories with the latest additions and deletions. This update will also include the latest keyword and newsgroup libraries and pattern files. Use this option to force a regular update.

○ Full URL Library Update

This option will update the URL library categories with core library files. This update will also include the latest keyword and newsgroup libraries and pattern files. Use this option if the core library files need to be replaced.

○ Software Update

This option downloads new software updates for the R3000, if available.

Fig. 2:3-3 Manual Update window

***NOTE**: The Configuration window should be used for scheduling the Web Filter 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.
- **Software Update -** Select this option to download new software updates for the Web Filter, if available. Any software updates that are downloaded can be found in the System section of the console, in the Local Software Update 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.*

NOTES: *For information on applying software updates, see the Local Software Update window in Chapter 1: System screen.*

For information on viewing the status of downloaded software updates, see the Software 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 M86-supported languages in library downloads.

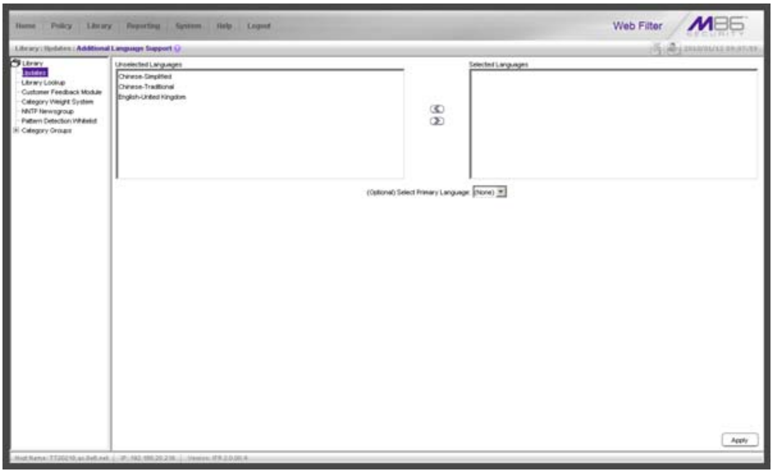


Fig. 2:3-4 Additional Language Support window

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.

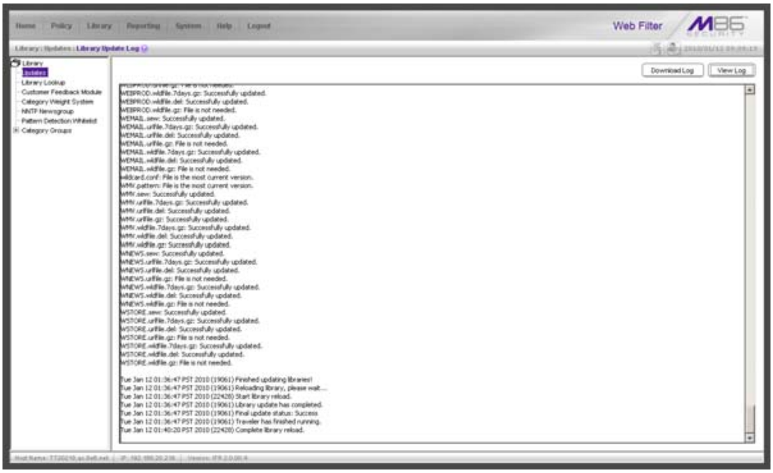
   To make an optional selection for a primary language, choose the language from the **(Optional) Select Primary Language** pull-down menu.

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 Web Filter, and for downloading the activity log.



```
WEBPROD.wldfile.7days.gz: Successfully updated.
WEBPROD.wldfile.del: Successfully updated.
WEBPROD.wldfile.gz: File is not needed.
WEMAIL.sew: Successfully updated.
WEMAIL.urlfile.7days.gz: Successfully updated.
WEMAIL.urlfile.del: Successfully updated.
WEMAIL.urlfile.gz: File is not needed.
WEMAIL.wldfile.7days.gz: Successfully updated.
WEMAIL.wldfile.del: Successfully updated.
WEMAIL.wldfile.gz: File is not needed.
wildcard.conf: File is the most current version.
WMV.pattern: File is the most current version.
WMV.sew: Successfully updated.
WMV.urlfile.7days.gz: Successfully updated.
WMV.urlfile.del: Successfully updated.
WMV.urlfile.gz: Successfully updated.
WMV.wldfile.7days.gz: Successfully updated.
WMV.wldfile.del: Successfully updated.
WMV.wldfile.gz: Successfully updated.
WNEWS.sew: Successfully updated.
WNEWS.urlfile.7days.gz: Successfully updated.
WNEWS.urlfile.del: Successfully updated.
WNEWS.urlfile.gz: File is not needed.
WNEWS.wldfile.7days.gz: Successfully updated.
WNEWS.wldfile.del: Successfully updated.
WNEWS.wldfile.gz: File is not needed.
WSTORE.sew: Successfully updated.
WSTORE.urlfile.7days.gz: Successfully updated.
WSTORE.urlfile.del: Successfully updated.
WSTORE.urlfile.gz: File is not needed.
WSTORE.wldfile.7days.gz: Successfully updated.
WSTORE.wldfile.del: Successfully updated.
WSTORE.wldfile.gz: File is not needed.

Tue Jan 12 01:36:47 PST 2010 (19061) Finished updating libraries!
Tue Jan 12 01:36:47 PST 2010 (19061) Reloading library, please wait....
Tue Jan 12 01:36:47 PST 2010 (22428) Start library reload.
Tue Jan 12 01:36:47 PST 2010 (19061) Library update has completed.
Tue Jan 12 01:36:47 PST 2010 (19061) Final update status: Success
Tue Jan 12 01:36:47 PST 2010 (19061) Traveler has finished running.
Tue Jan 12 01:40:20 PST 2010 (22428) Complete library reload.
```

Fig. 2:3-5 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.

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, select the “save” option; this action opens the window on your workstation where you specify the filename for the file and where to save the file.
3. Select 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.

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

4. After the file has successfully downloaded to your workstation, click **OK** to close the alert box asking you to verify that the software update log file was successfully saved.

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 in it to open the pop-up menu:

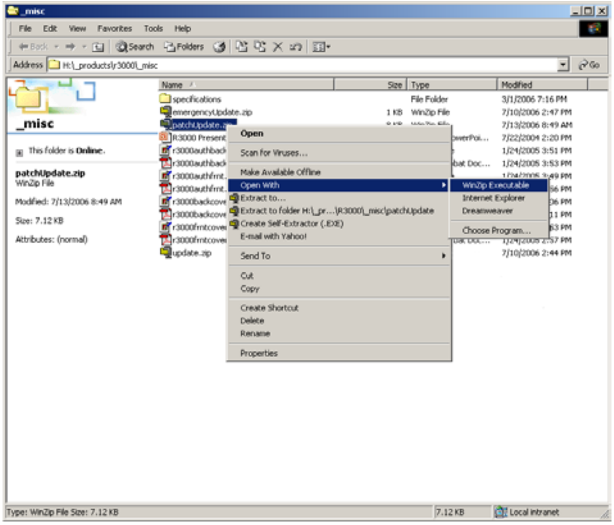
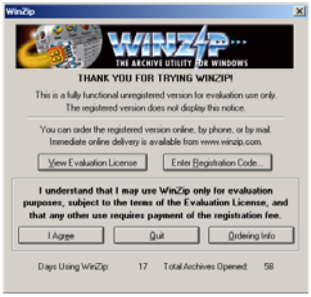

_misc
File Edit View Favorites Tools Help
Back Search Folders
Address H:_products\r3000_misc
Go
_misc
This folder is Online.
patchUpdate.zip
WinZip File
Modified: 7/13/2006 8:49 AM
Size: 7.12 KB
Attributes: (normal)
Name Size Type Modified
specifications File Folder 3/1/2006 7:16 PM
emergencyUpdate.zip 1 KB WinZip File 7/10/2006 2:47 PM
patchUpdate.zip 7/13/2006 8:49 AM
R3000 Present 7/22/2004 2:20 PM
r3000authback 1/24/2005 3:51 PM
r3000authback 1/24/2005 3:53 PM
r3000authfmt.
r3000authfmt.
r3000backcove
r3000backcove
r3000fmtcove
r3000fmtcove
update.zip 7/10/2006 2:44 PM
Open
Scan for Viruses...
Make Available Offline
Open With
Extract to...
Extract to folder H:_pr...\R3000_misc\patchUpdate
Create Self-Extractor (.EXE)
E-mail with Yahoo!
Send To
Cut
Copy
Create Shortcut
Delete
Rename
Properties
WinZip Executable
Internet Explorer
Dreamweaver
Choose Program...
Type: WinZip File Size: 7.12 KB
7.12 KB
Local intranet

Fig. 2:3-6 Folder containing downloaded file

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



THANK YOU FOR TRYING WINZIP!

This is a fully functional unregistered version for evaluation use only. The registered version does not display this notice.

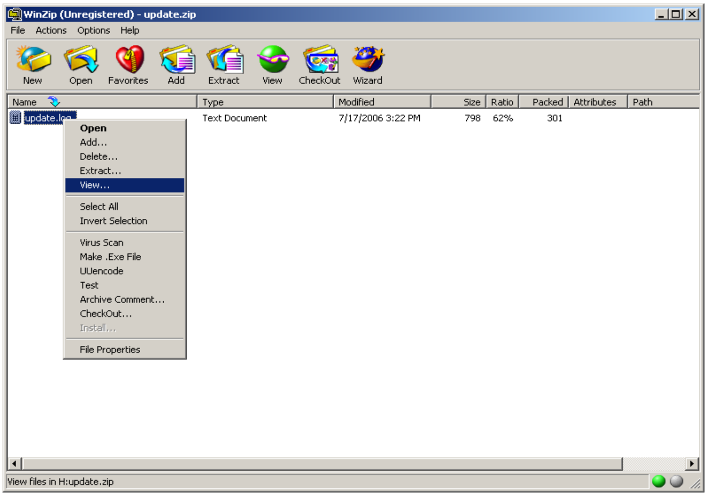
You can order the registered version online, by phone, or by mail. Immediate online delivery is available from www.winzip.com.

I understand that I may use WinZip only for evaluation purposes, subject to the terms of the Evaluation License, and that any other use requires payment of the registration fee.

Days Using WinZip: 17 Total Archives Opened: 58

Fig. 2:3-7 WinZip Executable program

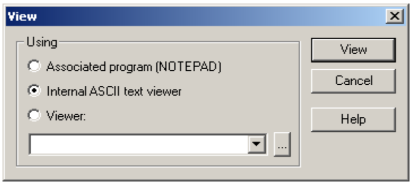
3. If using WinZip, click **I Agree** to open the window containing the zip file:



Name	Type	Modified	Size	Ratio	Packed	Attributes	Path
update.log	Text Document	7/17/2006 3:22 PM	798	62%	301		

Fig. 2:3-8 WinZip window

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



Using

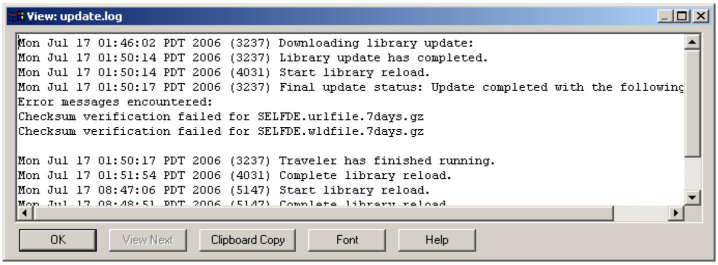
○ Associated program (NOTEPAD)

● Internal ASCII text viewer

○ Viewer:

Fig. 2:2-9 View dialog box

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



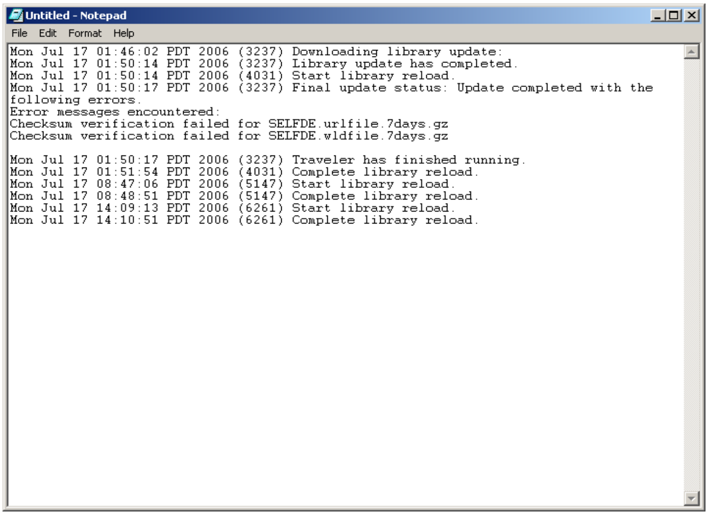
```
Mon Jul 17 01:46:02 PDT 2006 (3237) Downloading library update:
Mon Jul 17 01:50:14 PDT 2006 (3237) Library update has completed.
Mon Jul 17 01:50:14 PDT 2006 (4031) Start library reload.
Mon Jul 17 01:50:17 PDT 2006 (3237) Final update status: Update completed with the following
Error messages encountered:
Checksum verification failed for SELFDE.urlfile.7days.gz
Checksum verification failed for SELFDE.wldfile.7days.gz

Mon Jul 17 01:50:17 PDT 2006 (3237) Traveler has finished running.
Mon Jul 17 01:51:54 PDT 2006 (4031) Complete library reload.
Mon Jul 17 08:47:06 PDT 2006 (5147) Start library reload.
Mon Jul 17 08:48:51 PDT 2006 (5147) Complete library reload
```

Fig. 2:3-10 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
3. Paste the contents from the clipboard into the Notepad file:



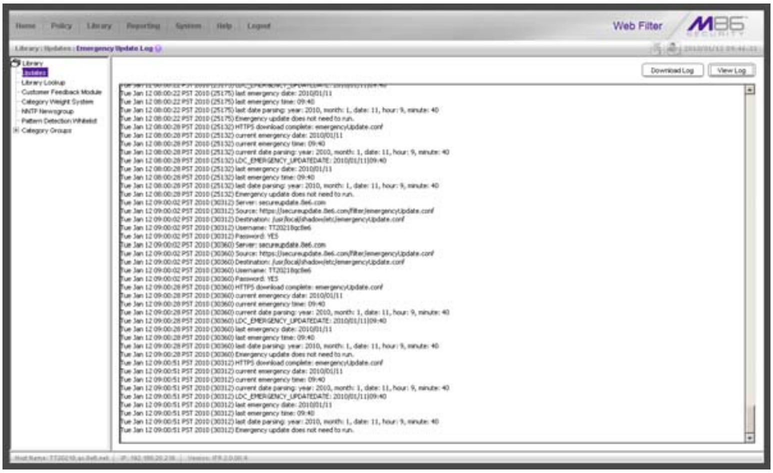
```
Mon Jul 17 01:46:02 PDT 2006 (3237) Downloading library update:
Mon Jul 17 01:50:14 PDT 2006 (3237) Library update has completed.
Mon Jul 17 01:50:14 PDT 2006 (4031) Start library reload.
Mon Jul 17 01:50:17 PDT 2006 (3237) Final update status: Update completed with the
following errors.
Error messages encountered:
Checksum verification failed for SELFDE.urlfile.7days.gz
Checksum verification failed for SELFDE.wldfile.7days.gz

Mon Jul 17 01:50:17 PDT 2006 (3237) Traveler has finished running.
Mon Jul 17 01:51:54 PDT 2006 (4031) Complete library reload.
Mon Jul 17 08:47:06 PDT 2006 (5147) Start library reload.
Mon Jul 17 08:48:51 PDT 2006 (5147) Complete library reload.
Mon Jul 17 14:09:13 PDT 2006 (6261) Start library reload.
Mon Jul 17 14:10:51 PDT 2006 (6261) Complete library reload.
```

Fig. 2:3-11 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 Web Filter, and for downloading the activity log.



```
Tue Jan 12 08:00:22 PST 2010 (25175) last emergency date: 2010/01/11
Tue Jan 12 08:00:22 PST 2010 (25175) last emergency time: 09:40
Tue Jan 12 08:00:22 PST 2010 (25175) last date parsing: year: 2010, month: 1, date: 11, hour: 9, minute: 40
Tue Jan 12 08:00:22 PST 2010 (25175) Emergency update does not need to run.
Tue Jan 12 08:00:28 PST 2010 (25132) HTTPS download complete: emergencyUpdate.conf
Tue Jan 12 08:00:28 PST 2010 (25132) current emergency date: 2010/01/11
Tue Jan 12 08:00:28 PST 2010 (25132) current emergency time: 09:40
Tue Jan 12 08:00:28 PST 2010 (25132) current date parsing: year: 2010, month: 1, date: 11, hour: 9, minute: 40
Tue Jan 12 08:00:28 PST 2010 (25132) LDC_EMERGENCY_UPDATEDATE: 2010/01/11|09:40
Tue Jan 12 08:00:28 PST 2010 (25132) last emergency date: 2010/01/11
Tue Jan 12 08:00:28 PST 2010 (25132) last emergency time: 09:40
Tue Jan 12 08:00:28 PST 2010 (25132) last date parsing: year: 2010, month: 1, date: 11, hour: 9, minute: 40
Tue Jan 12 08:00:28 PST 2010 (25132) Emergency update does not need to run.
Tue Jan 12 09:00:02 PST 2010 (30312) Server: secureupdate.8e6.com
Tue Jan 12 09:00:02 PST 2010 (30312) Source: https://secureupdate.8e6.com/filter/emergencyUpdate.conf
Tue Jan 12 09:00:02 PST 2010 (30312) Destination: /usr/local/shadow/etc/emergencyUpdate.conf
Tue Jan 12 09:00:02 PST 2010 (30312) Username: TT20218qc8e6
Tue Jan 12 09:00:02 PST 2010 (30312) Password: YES
Tue Jan 12 09:00:02 PST 2010 (30360) Server: secureupdate.8e6.com
Tue Jan 12 09:00:02 PST 2010 (30360) Source: https://secureupdate.8e6.com/filter/emergencyUpdate.conf
Tue Jan 12 09:00:02 PST 2010 (30360) Destination: /usr/local/shadow/etc/emergencyUpdate.conf
Tue Jan 12 09:00:02 PST 2010 (30360) Username: TT20218qc8e6
Tue Jan 12 09:00:02 PST 2010 (30360) Password: YES
Tue Jan 12 09:00:28 PST 2010 (30360) HTTPS download complete: emergencyUpdate.conf
Tue Jan 12 09:00:28 PST 2010 (30360) current emergency date: 2010/01/11
Tue Jan 12 09:00:28 PST 2010 (30360) current emergency time: 09:40
Tue Jan 12 09:00:28 PST 2010 (30360) current date parsing: year: 2010, month: 1, date: 11, hour: 9, minute: 40
Tue Jan 12 09:00:28 PST 2010 (30360) LDC_EMERGENCY_UPDATEDATE: 2010/01/11|09:40
Tue Jan 12 09:00:28 PST 2010 (30360) last emergency date: 2010/01/11
Tue Jan 12 09:00:28 PST 2010 (30360) last emergency time: 09:40
Tue Jan 12 09:00:28 PST 2010 (30360) last date parsing: year: 2010, month: 1, date: 11, hour: 9, minute: 40
Tue Jan 12 09:00:28 PST 2010 (30360) Emergency update does not need to run.
Tue Jan 12 09:00:51 PST 2010 (30312) HTTPS download complete: emergencyUpdate.conf
Tue Jan 12 09:00:51 PST 2010 (30312) current emergency date: 2010/01/11
Tue Jan 12 09:00:51 PST 2010 (30312) current emergency time: 09:40
Tue Jan 12 09:00:51 PST 2010 (30312) current date parsing: year: 2010, month: 1, date: 11, hour: 9, minute: 40
Tue Jan 12 09:00:51 PST 2010 (30312) LDC_EMERGENCY_UPDATEDATE: 2010/01/11|09:40
Tue Jan 12 09:00:51 PST 2010 (30312) last emergency date: 2010/01/11
Tue Jan 12 09:00:51 PST 2010 (30312) last emergency time: 09:40
Tue Jan 12 09:00:51 PST 2010 (30312) last date parsing: year: 2010, month: 1, date: 11, hour: 9, minute: 40
Tue Jan 12 09:00:51 PST 2010 (30312) Emergency update does not need to run.
```

Fig. 2:3-12 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.

Download the Software Update Log File

***NOTE**: See Library Update Log window for screen shots pertaining to downloading the software update log file.*

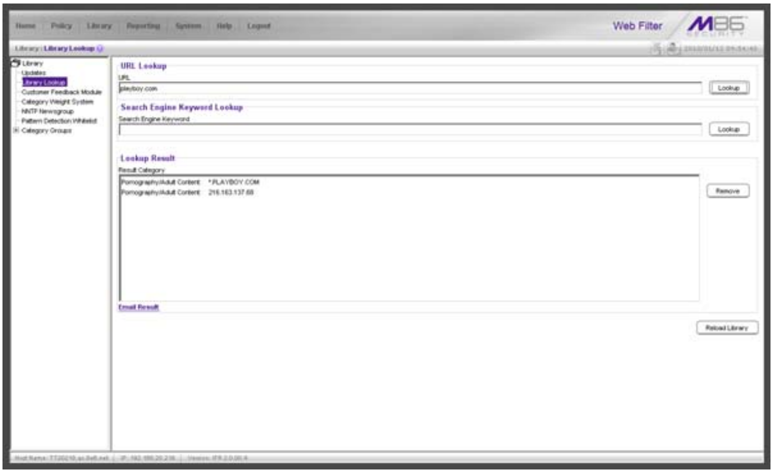
1. Click **Download Log** to open the alert box containing a message on how to download the log file to your workstation, if using Windows XP.
2. Click **OK** to close the alert box. Two pop-up boxes open:
    - A second alert box asks you to confirm that the file was successfully saved to your machine. Click **OK** in this box after the download is completed.
    - In the file download dialog box, select the “save” option; this action opens the window on your workstation where you specify the filename for the file and where to save the file.
3. Select 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.
4. After the file has successfully downloaded to your workstation, click **OK** to close the alert box asking you to verify that the software update log file was successfully saved.

***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.



URL: playboy.com

Search Engine Keyword:

Result Category

Pornography/Adult Content *.PLAYBOY.COM
Pornography/Adult Content 216.163.137.68

Fig. 2:3-13 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.coors.com**, **coors.com**, or use a wildcard by entering ***.coors.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
- query string - e.g. http://www.youtube.com/watch?v=3_Wfnj1llMU

***NOTES**: The pound sign (#) character is not allowed in this entry. 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

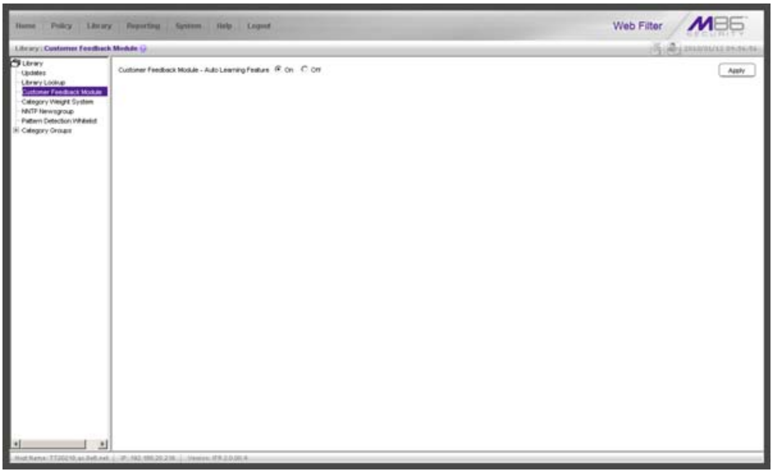
Once all changes have been made to library windows, click **Reload Library** to refresh.

NOTE*: Since reloading the library utilizes system resources that impact the performance of the Web Filter, M86 recommends clicking Reload Library only* ***after*** *modifications to* ***all*** *library windows have been made.*

Customer Feedback Module

Customer Feedback Module window

The Customer Feedback Module window displays when Customer Feedback Module is selected from the navigation panel. This window is used for enabling the Customer Feedback Module feature, in which the most frequently visited non-categorized URLs in your Web Filter's filter log will be FTPed to M86 on a daily basis. The URLs collected by M86 will be reviewed and added to M86's standard library categories, as appropriate, so they can be blocked.



Customer Feedback Module - Auto Learning Feature ● On ○ Off

Fig. 2:3-14 Customer Feedback Module window

***WARNING**: This feature is enabled by default. Please refer to the sub-section Enable Customer Feedback Module to review the contents of the disclaimer that applies when this feature is enabled.*

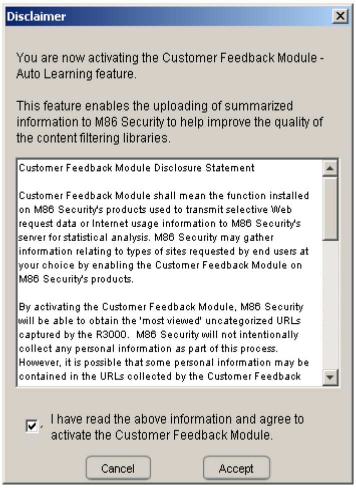
***NOTE**: For optimum results when using this feature, M86 recommends enabling Alert Settings and entering at least one email address that an M86 technical suppport representative can use to contact you for assistance. (See Alert Settings window in Chapter 1: System screen for information about enabling this feature.)*

Disable Customer Feedback Module

1. At the **Customer Feedback Module - Auto Learning Feature** field, click “Off” to indicate that you wish to disable the Customer Feedback Module.
2. Click **Apply**.

Enable Customer Feedback Module

1. At the **Customer Feedback Module - Auto Learning Feature** field, click “On” to indicate that you wish to enable the Customer Feedback Module.
2. Click **Apply** to open the Disclaimer dialog box:



You are now activating the Customer Feedback Module - Auto Learning feature.

This feature enables the uploading of summarized information to M86 Security to help improve the quality of the content filtering libraries.

Customer Feedback Module Disclosure Statement

Customer Feedback Module shall mean the function installed on M86 Security's products used to transmit selective Web request data or Internet usage information to M86 Security's server for statistical analysis. M86 Security may gather information relating to types of sites requested by end users at your choice by enabling the Customer Feedback Module on M86 Security's products.

By activating the Customer Feedback Module, M86 Security will be able to obtain the 'most viewed' uncategorized URLs captured by the R3000. M86 Security will not intentionally collect any personal information as part of this process. However, it is possible that some personal information may be contained in the URLs collected by the Customer Feedback

☑ I have read the above information and agree to activate the Customer Feedback Module.

Fig. 2:3-15 Disclaimer box

3. Scroll down to read the text in this box:

   “Customer Feedback Module Disclosure Statement

   “Customer Feedback Module shall mean the function installed on M86 Security’s products used to transmit selective Web request data or Internet usage information to M86 Security’s server for statistical analysis. M86 Security may gather information relating to types of sites requested by end users at your choice by enabling the Customer Feedback Module on M86 Security’s products.

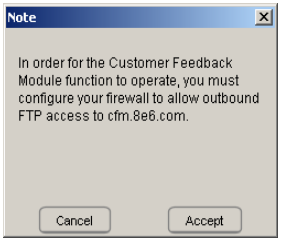
   “By activating the Customer Feedback Module, M86 Security will be able to obtain the ‘most viewed’ uncategorized URLs captured by the Web Filter. M86 Security will not intentionally collect any personal information as part of this process. However, it is possible that some personal information may be contained in the URLs collected by the Customer Feedback Module and sent to M86 Security. At no time will any personal information collected be released publicly, nor will the Web request data be used for any purpose other than enhancing the URL library and related categories used by M86 Security for the purpose of filtering and reporting.

   “M86 Security agrees to discuss the information collected by the Customer Feedback Module only with M86 Security’s employees who have a need to know and who have been informed of the confidential nature of the information and of their personal obligation not to disclose or use such information.

   “M86 Security may disclose personal Information if, in its sole discretion, M86 Security believes that it is reasonable to do so, including; to satisfy laws, or governmental or legal requests for such information; to disclose information that is necessary to identify, contact, or bring legal action against someone who may be violating M86 Security’s Acceptable Use Policy or other user policies; or to protect M86 Security and its Customers.

"Your agreement to activate the Customer Feedback Module will be transmitted back to M86 Security once you click the 'Accept' button."

4. After reading this text, if you agree with the terms, click in the checkbox to activate the Accept button.
5. Click **Accept** to close the Disclaimer box and to open the Note dialog box:



In order for the Customer Feedback Module function to operate, you must configure your firewall to allow outbound FTP access to cfm.8e6.com.

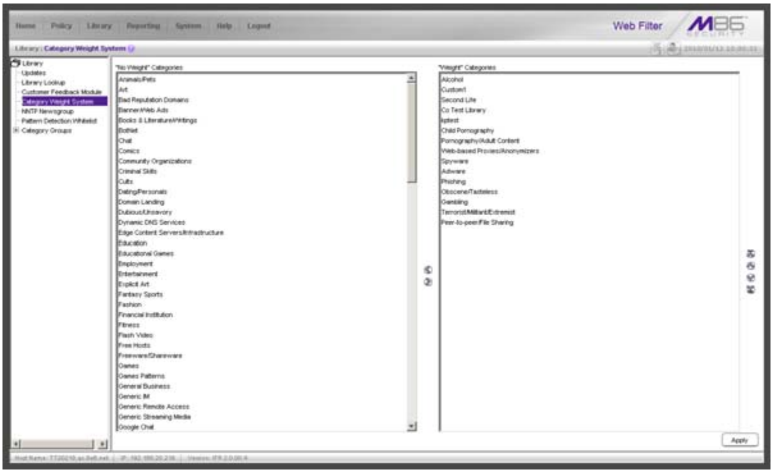
Fig. 2:3-16 Note dialog box

6. If you do not have a firewall, or if you agree to open your firewall to **cfm.8e6.com**, click **Accept** to proceed.

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 M86 supplied and custom library categories) with the same operational precedence.



"No Weight" Categories
Animals/Pets
Art
Bad Reputation Domains
Banner/Web Ads
Books & Literature/Writings
BotNet
Chat
Comics
Community Organizations
Criminal Skills
Cults
Dating/Personals
Domain Landing
Dubious/Unsavory
Dynamic DNS Services
Edge Content Servers/Infrastructure
Education
Educational Games
Employment
Entertainment
Explicit Art
Fantasy Sports
Fashion
Financial Institution
Fitness
Flash Video
Free Hosts
Freeware/Shareware
Games
Games Patterns
General Business
Generic IM
Generic Remote Access
Generic Streaming Media
Google Chat

"Weight" Categories
Alcohol
Custom1
Second Life
Co Test Library
iptest
Child Pornography
Pornography/Adult Content
Web-based Proxies/Anonymizers
Spyware
Adware
Phishing
Obscene/Tasteless
Gambling
Terrorist/Militant/Extremist
Peer-to-peer/File Sharing

Fig. 2:3-17 Category Weight System window

View the Current Selections

This window contains two list boxes:

- “No Weight” Categories - Populated with M86 supplied categories
- “Weight” Categories - Pre-populated by default with categories M86 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 Web Filter 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.

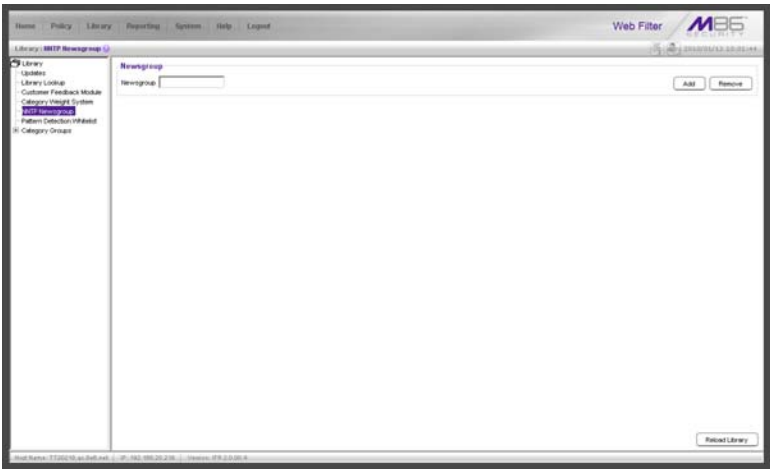


Fig. 2:3-18 NNTP Newsgroup window

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**.

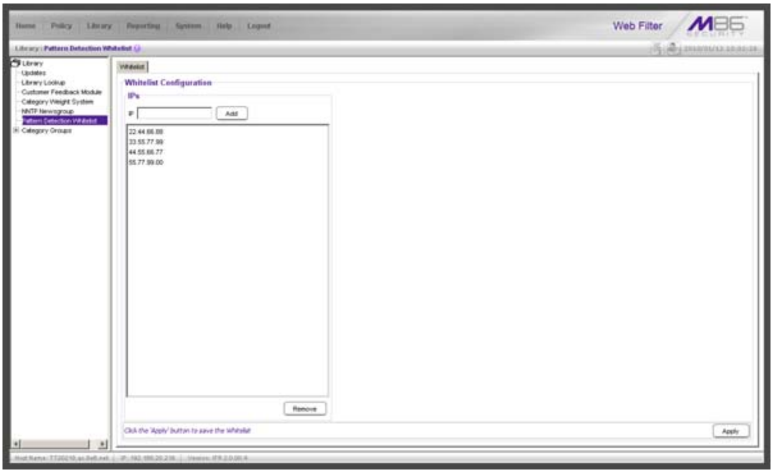
After all changes have been made to library windows, click **Reload Library** to refresh.

***NOTE**: Since reloading the library utilizes system resources that impact the performance of the Web Filter, M86 recommends clicking Reload Library only **after** modifications to **all** library windows have been made.*

Pattern Detection Whitelist

Pattern Detection Whitelist window

The Pattern Detection Whitelist window displays when Pattern Detection Whitelist is selected from the navigation panel. This window is used for creating a list of IP addresses always allowed to bypass pattern detection filtering.



22.44.66.88
33.55.77.99
44.55.66.77
55.77.99.00

Click the 'Apply' button to save the Whitelist

Fig. 2:3-19 Pattern Detection Whitelist window

***NOTE**: This feature can be used in conjunction with the Pattern Blocking feature, which, when enabled, blocks IP address patterns. (See the Filter window sub-section in Chapter 1: System screen.)*

Create, Maintain a Whitelist of IP Addresses

1. Enter the **IP** address to bypass pattern detection filtering.
2. Click **Add** to include the IP address in the IPs list box.

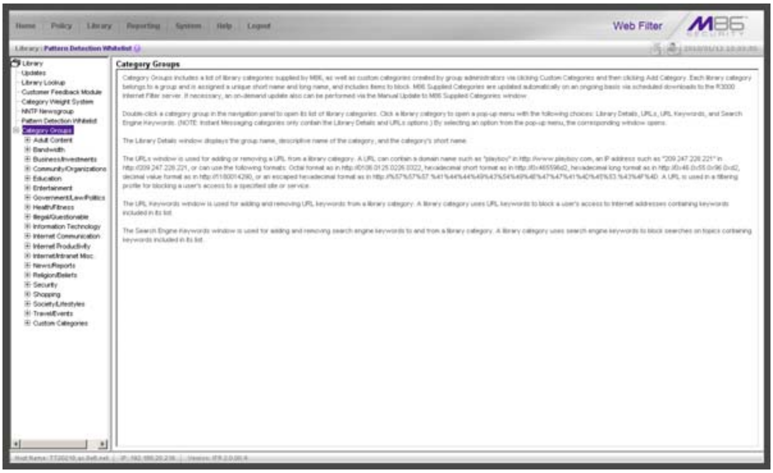
TIP*: To remove an IP address from the list, select the IP address from the IPs list box, and then click Remove. Multiple IP addresses can be selected by clicking each IP address while simultaneously pressing down the Ctrl key on the keyboard. A block of IP addresses can be selected by clicking the first IP address in the list, and then pressing down the Shift key on the keyboard while simultaneously clicking the last IP address in the list.*

3. After all IP addresses have been added and/or removed, click **Apply**.

Category Groups

Category Groups is represented by a tree of library category groups, with each group comprised of M86 supplied library categories. M86 supplied library categories are updated regularly with new URLs via Traveler, M86's executable program that supplies updates to the Web Filter.

Category Groups also contains the Custom Categories category group. Customized category groups and library categories must be set up and maintained by global or group administrators.



Category Groups

Category Groups includes a list of library categories supplied by M86, as well as custom categories created by group administrators via clicking Custom Categories and then clicking Add Category. Each library category belongs to a group and is assigned a unique short name and long name, and includes items to block. M86 Supplied Categories are updated automatically on an ongoing basis via scheduled downloads to the R3000 Internet Filter server. If necessary, an on-demand update also can be performed via the Manual Update to M86 Supplied Categories window.

Double-click a category group in the navigation panel to open its list of library categories. Click a library category to open a pop-up menu with the following choices: Library Details, URLs, URL Keywords, and Search Engine Keywords. (NOTE: Instant Messaging categories only contain the Library Details and URLs options.) By selecting an option from the pop-up menu, the corresponding window opens.

The Library Details window displays the group name, descriptive name of the category, and the category's short name.

The URLs window is used for adding or removing a URL from a library category. A URL can contain a domain name such as "playboy" in http://www.playboy.com, an IP address such as "209.247.228.221" in http://209.247.228.221, or can use the following formats: Octal format as in http://0106.0125.0226.0322, hexadecimal short format as in http://0x465596d2, hexadecimal long format as in http://0x46.0x55.0x96.0xd2, decimal value format as in http://1180014290, or an escaped hexadecimal format as in http://%57%57%57.%41%44%44%49%43%54%49%4E%47%47%41%4D%45%53.%43%4F%4D. A URL is used in a filtering profile for blocking a user's access to a specified site or service.

The URL Keywords 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.

The Search Engine Keywords window is used for adding and removing search engine keywords to and from a library category. A library category uses search engine keywords to block searches on topics containing keywords included in its list.

Fig. 2:3-20 Library screen, Category Groups menu

***NOTE**: See the Custom Categories sub-section of the WF Group Administrator Section for information on setting up customized category groups and library categories.*

***WARNING**: The maximum number of library categories that can be saved is 512. This figure includes both M86 supplied categories and custom categories.*

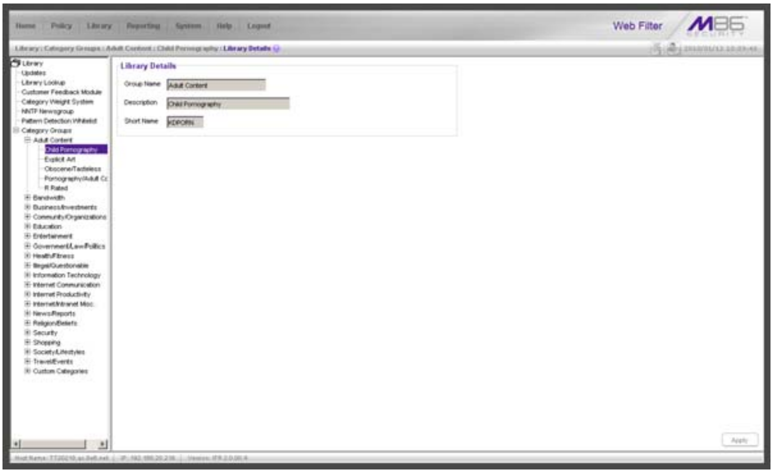
Double-click Category Groups to open the tree and to display category groups.

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 M86 supplied category link 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.



Library Details

Group Name: Adult Content

Description: Child Pornography

Short Name: KDPORN

Fig. 2:3-21 Library Details window

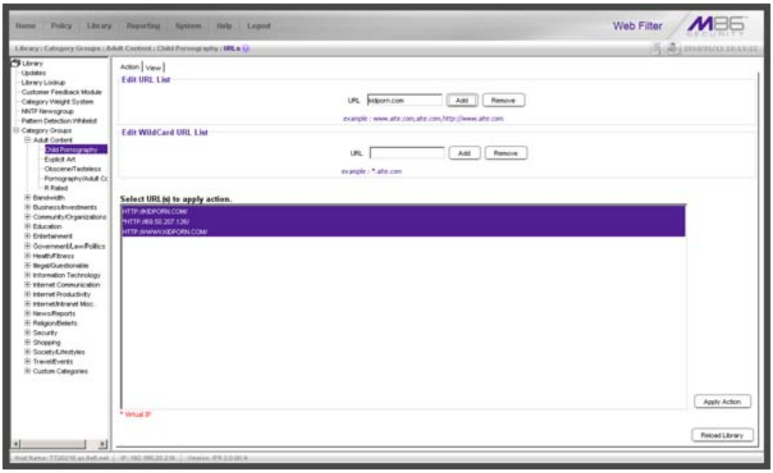
View Library Details

This window displays the **Group Name**, **Description**, and **Short Name** of the M86 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 is used in a filtering profile for blocking a user's access to a specified site or service.

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 query string can be entered to block access to a specific URL.



Library : Category Groups : Adult Content : Child Pornography : URLs

Edit URL List

URL kidporn.com

example : www.ahe.com,ahe.com,http://www.ahe.com

Edit WildCard URL List

URL

example : *.ahe.com

Select URL(s) to apply action.

HTTP://KIDPORN.COM/
*HTTP://69.50.207.126/
HTTP://WWW.KIDPORN.COM/

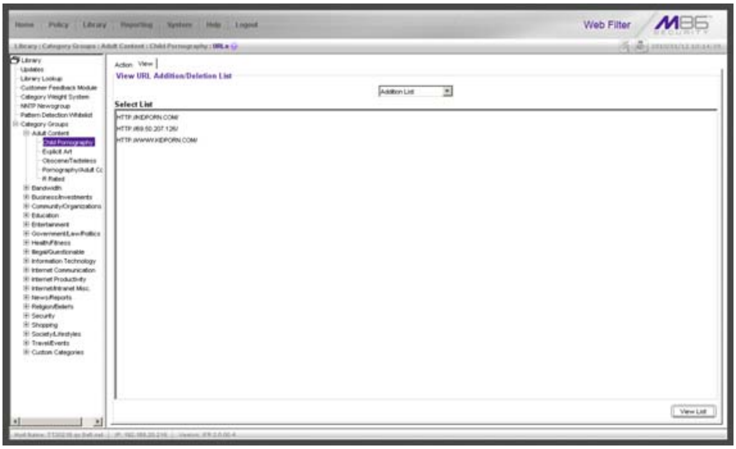
* Virtual IP

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:



View URL Addition/Deletion List

Addition List

Select List

HTTP://KIDPORN.COM/
HTTP://69.50.207.126/
HTTP://WWW.KIDPORN.COM/

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.coors.com**, **www.coors.com**, or **coors.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
   - query string - e.g. http://www.youtube.com/watch?v=3_Wfnj1IIMU

NOTE*: The pound sign (#) character is not allowed in this entry.*

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 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 *.beer.com would find a URL such as http://virtualbartender.beer.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.cnn.com is added to a category that is not set up to be blocked, and *.cnn.com is added to a category set up to be blocked, the end user will be able to access http://www.cnn.com since it is a direct match, but will not be able to access http://www.sports.cnn.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**.

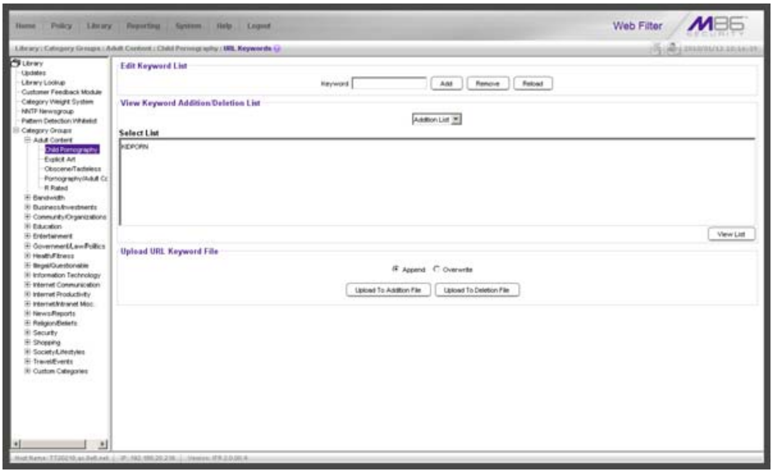
Reload the Library

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 Web Filter, M86 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.



Addition List

Select List: KIDPORN

● Append ○ Overwrite

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 Policy 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:

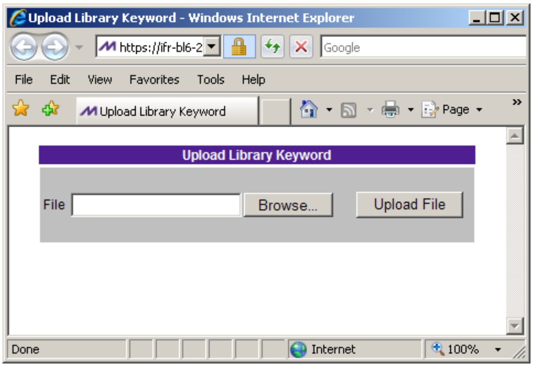


Fig. 2:3-25 Upload Library Keyword pop-up window

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.

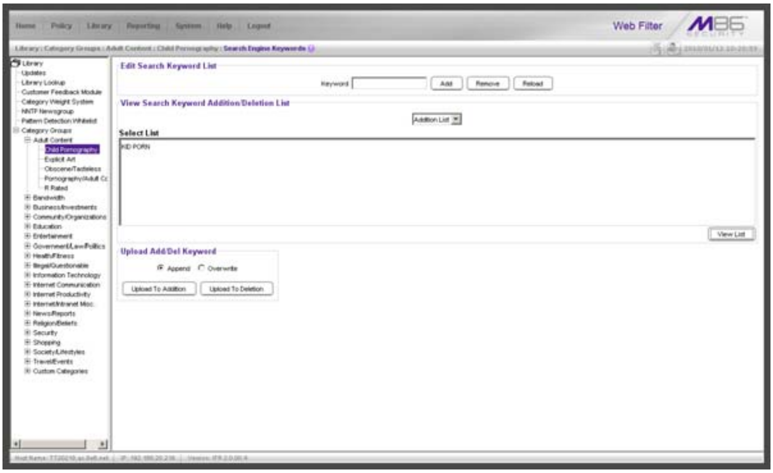
Reload the Library

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 Web Filter, M86 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.



Select List

KID PORN

● Append ○ Overwrite

Fig. 2:3-26 Search Engine Keywords window

***NOTES**: Master lists cannot be uploaded to any M86 supplied library category. See the Custom Categories sub-section of the WF Group Administrator Section of this user guide for information on uploading a master list to the server.*

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 Policy 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.

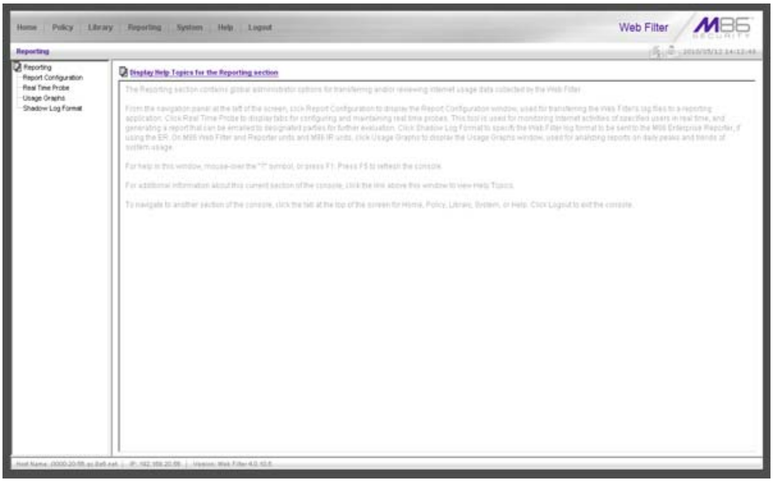
Reload the Library

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 Web Filter, M86 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 Web Filter.



The Reporting section contains global administrator options for transferring and/or reviewing Internet usage data collected by the Web Filter.

From the navigation panel at the left of the screen, click Report Configuration to display the Report Configuration window, used for transferring the Web Filter's log files to a reporting application. Click Real Time Probe to display tabs for configuring and maintaining real time probes. This tool is used for monitoring Internet activities of specified users in real time, and generating a report that can be emailed to designated parties for further evaluation. Click Shadow Log Format to specify the Web Filter log format to be sent to the M86 Enterprise Reporter, if using the ER. On M86 Web Filter and Reporter units and M86 IR units, click Usage Graphs to display the Usage Graphs window, used for analyzing reports on daily peaks and trends of system usage.

For help in this window, mouse-over the "?" symbol, or press F1. Press F5 to refresh the console.

For additional information about this current section of the console, click the link above this window to view Help Topics.

To navigate to another section of the console, click the tab at the top of the screen for Home, Policy, Library, System, or Help. Click Logout to exit the console.

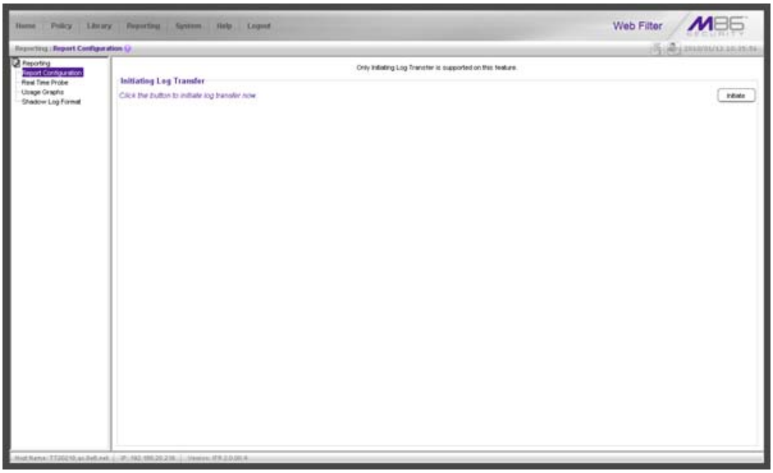
Fig. 2:4-1 Reporting screen

From the navigation panel at the left of the screen, click Report Configuration to display the Report Configuration window, used for transferring Web Filter log files to the SR Administration module on demand. 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. Click Usage Graphs to display the Usage Graphs window, used for analyzing reports on daily peaks and trends of Internet usage. Click Shadow Log Format to specify the format in which Web Filter logs will be sent to the SR.

Report Configuration

Report Configuration window

The Report Configuration window displays when Report Configuration is selected from the navigation panel. This window is used for initiating an on demand log transfer to the SR.



Only Initiating Log Transfer is supported on this feature.

Initiating Log Transfer

Click the button to initiate log transfer now

Fig. 2:4-2 Report Configuration window

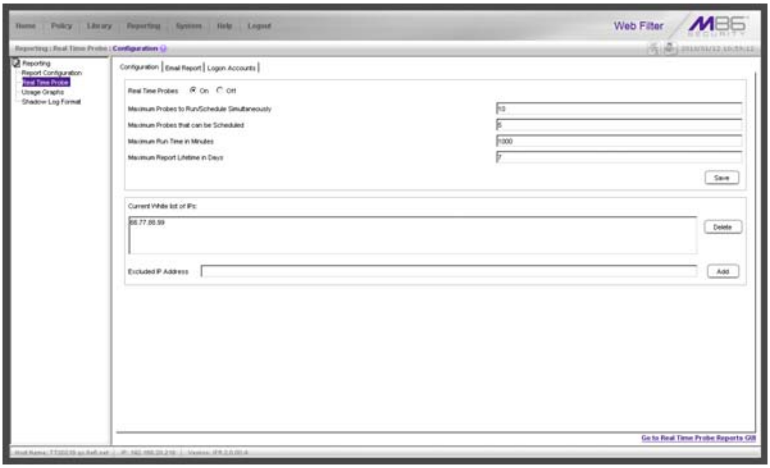
Execute Log Transfer Now

In the Initiating Log Transfer frame, click **Initiate** to transfer the log on demand.

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.



Real Time Probes ● On ○ Off

Maximum Probes to Run/Schedule Simultaneously: 10

Maximum Probes that can be Scheduled: 5

Maximum Run Time in Minutes: 1000

Maximum Report Lifetime in Days: 7

Current White list of IPs: 66.77.88.99

Excluded IP Address:

Fig. 2:4-3 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

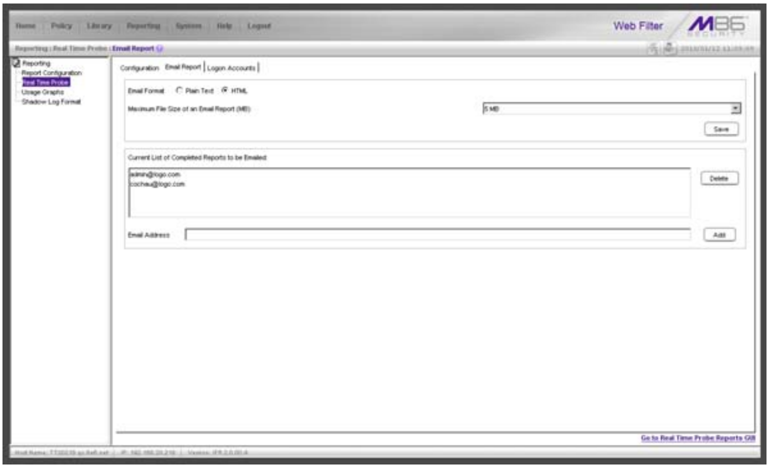
1. Enter the **Excluded IP Address** of a machine to be bypassed from real time probing.
2. Click **Add** to add the IP address in the Current White list of IPs.

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:



Email Format ○ Plain Text ● HTML

Maximum File Size of an Email Report (MB): 5 MB

Current List of Completed Reports to be Emailed

admin@logo.com
cochau@logo.com

Email Address

Fig. 2:4-4 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.

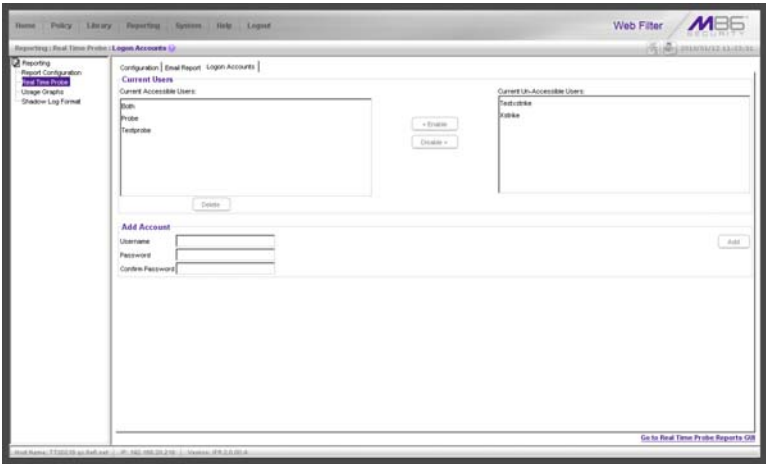
NOTE*: The maximum number of report recipients is 50. If more than 50 recipients need to be included, M86 recommends setting up an email alias list for group distribution.*

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:



Current Accessible Users: Both, Probe, Testprobe

Current Un-Accessible Users: Testxstrike, Xstrike

Fig. 2:4-5 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**.

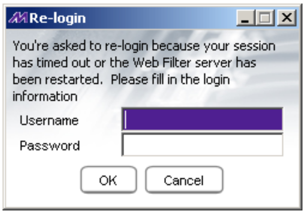
⚠ ***WARNING****: By deleting a logon account, in addition to not being able to create real time probes, that user will also be removed from the list of users authorized to unlock workstations. (See Chapter 1: System screen, X Strikes Blocking for information on reseting strikes and unlocking workstations.)*

Go to Real Time Probe Reports GUI

When any administrator clicks the Real Time Probe icon or **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:



You're asked to re-login because your session has timed out or the Web Filter server has been restarted. Please fill in the login information

Username

Password

Fig. 2:4-6 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 Web Filter console.

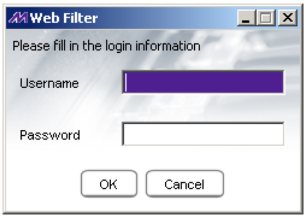
Real Time Probe Reports

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 **https://x.x.x.x:1443/RtProbe.jsp** in the address field of a browser window—in which “x.x.x.x” is the IP address of the Web Filter—to only see probes he/she created.*

When using the aforementioned URL, the following occurs:

- *The Login window opens:*



Web Filter

Please fill in the login information

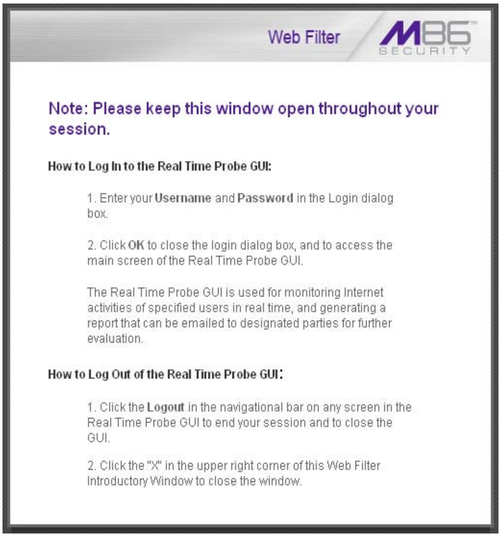
Username

Password

Fig. 2:4-7 Login window

*Enter the Username and Password and click **OK** to open the Real Time Probe Reports pop-up window (see Fig. 2:4-8).*

- *The Web Filter Introductory Window for Real Time Probes simultaneously opens with the Login window:*



Note: Please keep this window open throughout your session.

How to Log In to the Real Time Probe GUI:

1. Enter your **Username** and **Password** in the Login dialog box.

2. Click **OK** to close the login dialog box, and to access the main screen of the Real Time Probe GUI.

The Real Time Probe GUI is used for monitoring Internet activities of specified users in real time, and generating a report that can be emailed to designated parties for further evaluation.

How to Log Out of the Real Time Probe GUI:

1. Click the **Logout** in the navigational bar on any screen in the Real Time Probe GUI to end your session and to close the GUI.

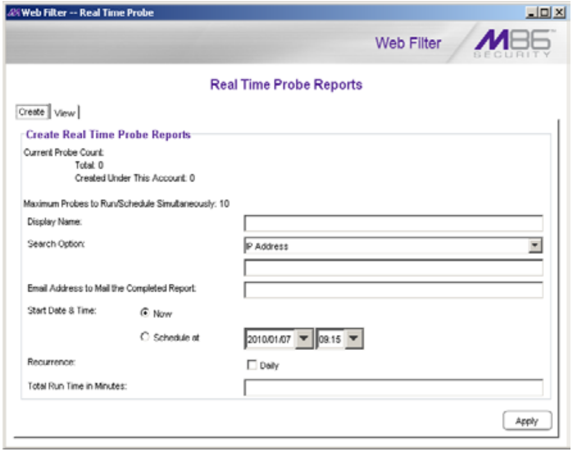
2. Click the "X" in the upper right corner of this Web Filter Introductory Window to close the window.

Fig. 2:4-8 Real Time Probes introductory window

This window must be left open during the entire session.

Create a Real Time Probe

Click the Create tab to enter and specify criteria for the report you wish to generate:



Real Time Probe Reports

Create Real Time Probe Reports

Current Probe Count:
Total: 0
Created Under This Account: 0

Maximum Probes to Run/Schedule Simultaneously: 10

Display Name:

Search Option: IP Address

Email Address to Mail the Completed Report:

Start Date & Time: ● Now

○ Schedule at 2010/01/07 09:15

Recurrence: □ Daily

Total Run Time in Minutes:

Fig. 2:4-9 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.

***TIP**: Select “Approved Content” from the drop-down menu to probe instances of the Approved Content online video viewing feature.*

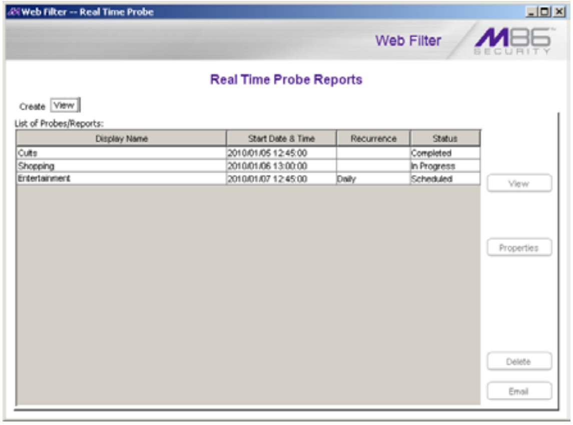
***NOTE**: Up to 250 characters will be accepted for the IP Address, User Name, or URL.*

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:



Real Time Probe Reports

List of Probes/Reports:

Display Name	Start Date & Time	Recurrence	Status
Cults	2010/01/05 12:45:00		Completed
Shopping	2010/01/06 13:00:00		In Progress
Entertainment	2010/01/07 12:45:00	Daily	Scheduled

Fig. 2:4-10 Real Time Probe Reports, View tab

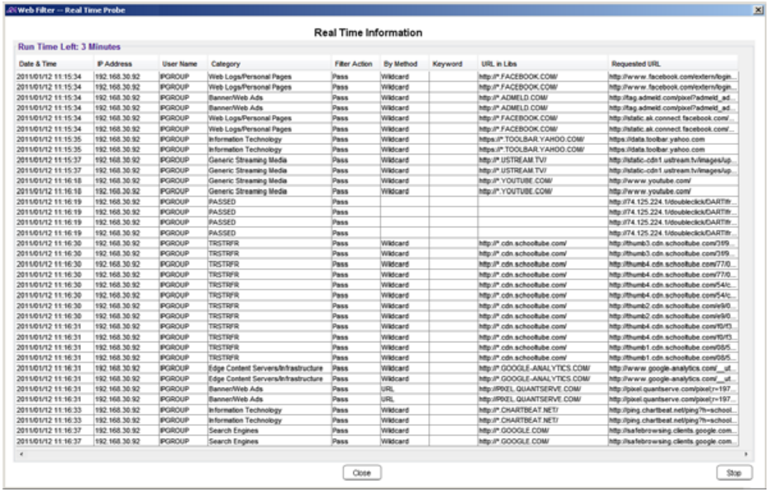
The Display Name shows the name assigned to the probe on the Create tab. The Start Date & Time displays in the YYYY/MM/DD HH:MM:SS format. “Daily” displays in the Recurrence column if the probe is scheduled to run on a daily basis. The Status of the probe displays: “Completed”, “In Progress”, or “Scheduled”.

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 window:



Real Time Information

Run Time Left: 3 Minutes

Date & Time	IP Address	User Name	Category	Filter Action	By Method	Keyword	URL in Libs	Requested URL
2011/01/12 11:15:34	192.168.30.92	IPGROUP	Web Logs/Personal Pages	Pass	Wildcard		http://*.FACEBOOK.COM/	http://www.facebook.com/extern/login...
2011/01/12 11:15:34	192.168.30.92	IPGROUP	Web Logs/Personal Pages	Pass	Wildcard		http://*.FACEBOOK.COM/	http://www.facebook.com/extern/login...
2011/01/12 11:15:34	192.168.30.92	IPGROUP	Banner/Web Ads	Pass	Wildcard		http://*.ADMELD.COM/	http://tag.admeld.com/pixel?admeld_ad...
2011/01/12 11:15:34	192.168.30.92	IPGROUP	Banner/Web Ads	Pass	Wildcard		http://*.ADMELD.COM/	http://tag.admeld.com/pixel?admeld_ad...
2011/01/12 11:15:34	192.168.30.92	IPGROUP	Web Logs/Personal Pages	Pass	Wildcard		http://*.FACEBOOK.COM/	http://static.ak.connect.facebook.com/...
2011/01/12 11:15:34	192.168.30.92	IPGROUP	Web Logs/Personal Pages	Pass	Wildcard		http://*.FACEBOOK.COM/	http://static.ak.connect.facebook.com/...
2011/01/12 11:15:35	192.168.30.92	IPGROUP	Information Technology	Pass	Wildcard		https://*.TOOLBAR.YAHOO.COM/	https://data.toolbar.yahoo.com
2011/01/12 11:15:35	192.168.30.92	IPGROUP	Information Technology	Pass	Wildcard		https://*.TOOLBAR.YAHOO.COM/	https://data.toolbar.yahoo.com
2011/01/12 11:15:37	192.168.30.92	IPGROUP	Generic Streaming Media	Pass	Wildcard		http://*.USTREAM.TV/	http://static-cdn1.ustream.tv/images/up...
2011/01/12 11:15:37	192.168.30.92	IPGROUP	Generic Streaming Media	Pass	Wildcard		http://*.USTREAM.TV/	http://static-cdn1.ustream.tv/images/up...
2011/01/12 11:16:18	192.168.30.92	IPGROUP	Generic Streaming Media	Pass	Wildcard		http://*.YOUTUBE.COM/	http://www.youtube.com/
2011/01/12 11:16:18	192.168.30.92	IPGROUP	Generic Streaming Media	Pass	Wildcard		http://*.YOUTUBE.COM/	http://www.youtube.com/
2011/01/12 11:16:19	192.168.30.92	IPGROUP	PASSED	Pass				http://74.125.224.1/doubleclick/DARTIfr...
2011/01/12 11:16:19	192.168.30.92	IPGROUP	PASSED	Pass				http://74.125.224.1/doubleclick/DARTIfr...
2011/01/12 11:16:19	192.168.30.92	IPGROUP	PASSED	Pass				http://74.125.224.1/doubleclick/DARTIfr...
2011/01/12 11:16:19	192.168.30.92	IPGROUP	PASSED	Pass				http://74.125.224.1/doubleclick/DARTIfr...
2011/01/12 11:16:30	192.168.30.92	IPGROUP	TRSTRFR	Pass	Wildcard		http://*.cdn.schooltube.com/	http://thumb3.cdn.schooltube.com/3f/9...
2011/01/12 11:16:30	192.168.30.92	IPGROUP	TRSTRFR	Pass	Wildcard		http://*.cdn.schooltube.com/	http://thumb3.cdn.schooltube.com/3f/9...
2011/01/12 11:16:30	192.168.30.92	IPGROUP	TRSTRFR	Pass	Wildcard		http://*.cdn.schooltube.com/	http://thumb4.cdn.schooltube.com/77/0...
2011/01/12 11:16:30	192.168.30.92	IPGROUP	TRSTRFR	Pass	Wildcard		http://*.cdn.schooltube.com/	http://thumb4.cdn.schooltube.com/77/0...
2011/01/12 11:16:30	192.168.30.92	IPGROUP	TRSTRFR	Pass	Wildcard		http://*.cdn.schooltube.com/	http://thumb4.cdn.schooltube.com/54/c...
2011/01/12 11:16:30	192.168.30.92	IPGROUP	TRSTRFR	Pass	Wildcard		http://*.cdn.schooltube.com/	http://thumb4.cdn.schooltube.com/54/c...
2011/01/12 11:16:30	192.168.30.92	IPGROUP	TRSTRFR	Pass	Wildcard		http://*.cdn.schooltube.com/	http://thumb2.cdn.schooltube.com/e9/0...
2011/01/12 11:16:30	192.168.30.92	IPGROUP	TRSTRFR	Pass	Wildcard		http://*.cdn.schooltube.com/	http://thumb2.cdn.schooltube.com/e9/0...
2011/01/12 11:16:31	192.168.30.92	IPGROUP	TRSTRFR	Pass	Wildcard		http://*.cdn.schooltube.com/	http://thumb4.cdn.schooltube.com/f0/f3...
2011/01/12 11:16:31	192.168.30.92	IPGROUP	TRSTRFR	Pass	Wildcard		http://*.cdn.schooltube.com/	http://thumb4.cdn.schooltube.com/f0/f3...
2011/01/12 11:16:31	192.168.30.92	IPGROUP	TRSTRFR	Pass	Wildcard		http://*.cdn.schooltube.com/	http://thumb1.cdn.schooltube.com/08/5...
2011/01/12 11:16:31	192.168.30.92	IPGROUP	TRSTRFR	Pass	Wildcard		http://*.cdn.schooltube.com/	http://thumb1.cdn.schooltube.com/08/5...
2011/01/12 11:16:31	192.168.30.92	IPGROUP	Edge Content Servers/Infrastructure	Pass	Wildcard		http://*.GOOGLE-ANALYTICS.COM/	http://www.google-analytics.com/__ut...
2011/01/12 11:16:31	192.168.30.92	IPGROUP	Edge Content Servers/Infrastructure	Pass	Wildcard		http://*.GOOGLE-ANALYTICS.COM/	http://www.google-analytics.com/__ut...
2011/01/12 11:16:31	192.168.30.92	IPGROUP	Banner/Web Ads	Pass	URL		http://PIXEL.QUANTSERVE.COM/	http://pixel.quantserve.com/pixel;r=197...
2011/01/12 11:16:31	192.168.30.92	IPGROUP	Banner/Web Ads	Pass	URL		http://PIXEL.QUANTSERVE.COM/	http://pixel.quantserve.com/pixel;r=197...
2011/01/12 11:16:33	192.168.30.92	IPGROUP	Information Technology	Pass	Wildcard		http://*.CHARTBEAT.NET/	http://ping.chartbeat.net/ping?h=school...
2011/01/12 11:16:33	192.168.30.92	IPGROUP	Information Technology	Pass	Wildcard		http://*.CHARTBEAT.NET/	http://ping.chartbeat.net/ping?h=school...
2011/01/12 11:16:37	192.168.30.92	IPGROUP	Search Engines	Pass	Wildcard		http://*.GOOGLE.COM/	http://safebrowsing.clients.google.com...
2011/01/12 11:16:37	192.168.30.92	IPGROUP	Search Engines	Pass	Wildcard		http://*.GOOGLE.COM/	http://safebrowsing.clients.google.com...

Fig. 2:4-11 Real Time Information window

This window displays the number of minutes left for the probe to run (Run Time Left), and user details for each record in the grid: Date & Time (in the YYYY/MM/DD HH:MM:SS format); IP Address; User Name; library Category (PASSED for any uncategorized sites allowed to pass, and Approved Content if the Approved Content feature is enabled and the record pertains to an approved video), Filter Action set up in the profile (Pass, Block, reserved for ER/SR, 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.

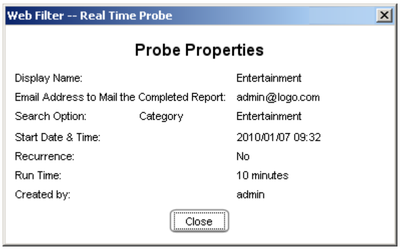
The following actions can be performed in this window:

- 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 window.

Properties option

Clicking **Properties** opens the Probe Properties pop-up box:



Web Filter -- Real Time Probe

Probe Properties

Display Name:		Entertainment
Email Address to Mail the Completed Report:		admin@logo.com
Search Option:	Category	Entertainment
Start Date & Time:		2010/01/07 09:32
Recurrence:		No
Run Time:		10 minutes
Created by:		admin

Fig. 2:4-12 Probe Properties pop-up box

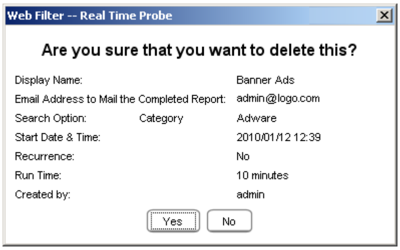
This pop-up box includes the following information for the probe: Display Name; Email Address to Mail the Completed Report; Search Option criteria; Start Date & Time; Run Time; and User ID of the creator of the probe (Created by).

Click **Close** to close this pop-up 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:



Are you sure that you want to delete this?

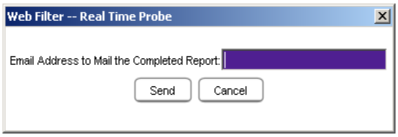
Display Name:		Banner Ads
Email Address to Mail the Completed Report:		admin@logo.com
Search Option:	Category	Adware
Start Date & Time:		2010/01/12 12:39
Recurrence:		No
Run Time:		10 minutes
Created by:		admin

Fig. 2:4-13 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:



Email Address to Mail the Completed Report:

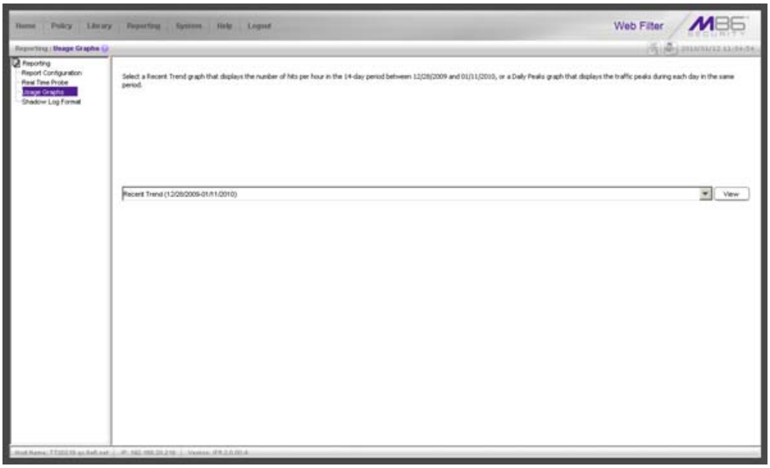
Fig. 2:4-14 Email Address box

Enter the **Email Address to Mail the Completed Report** and click **Send** to send the completed report to the designated email address.

Usage Graphs

Usage Graphs window

The Usage Graphs window displays when Usage Graphs is selected from the navigation panel. This window is used for viewing and analyzing Internet usage data for a specified time period within the past 14 days. The following data can be analyzed for the given time period: number of URLs accessed by end users, number of machine IP addresses accessing the Internet, and number of end users who have been authenticated (if using the authentication feature).



Select a Recent Trend graph that displays the number of hits per hour in the 14-day period between 12/28/2009 and 01/11/2010, or a Daily Peaks graph that displays the traffic peaks during each day in the same period.

Recent Trend (12/28/2009-01/11/2010)

Fig. 2:4-15 Usage Graphs window

Select a Graph to View

1. From the available menu choices, select either “Recent Trend” or one of the “Daily Peaks” dates.
2. Click **View** to open a separate browser window containing the specified graph.

Recent Trend

The Recent Trend graph includes the following information: date range, and Number of Hits per Hour for a given date:

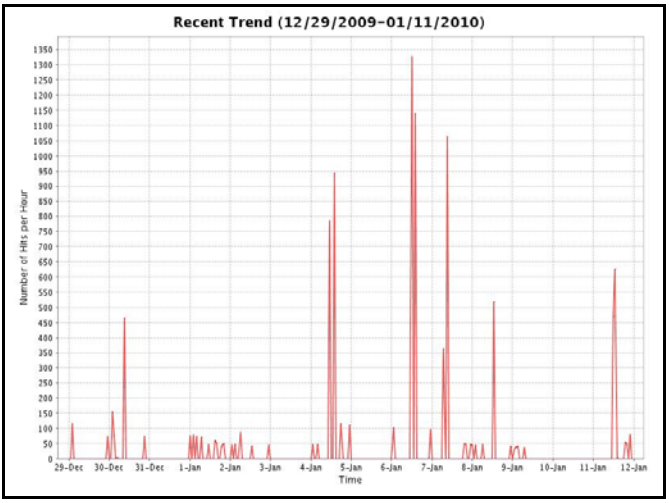


Fig. 2:4-16 Recent Trend graph

Click the “X” in the upper right corner to close this window.

Daily Peaks

The Daily Peaks graph includes the following information: date, and Number of Hits per Second at Peak Time for a given Time using the HH:MM format:

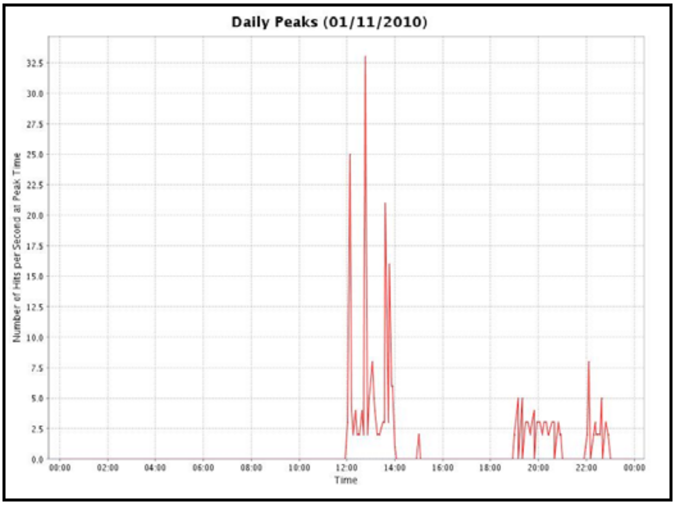


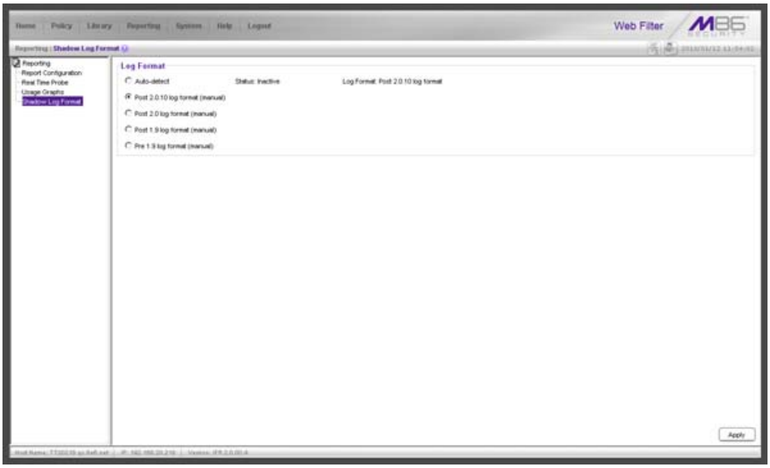
Fig. 2:4-17 Daily Peaks graph

Click the “X” in the upper right corner to close this window.

Shadow Log Format

Shadow Log Format window

The Shadow Log Format window displays when Shadow Log Format is selected from the navigation panel.This window is used for specifying the log format the Web Filter will use for sending logs to the SR.



Log Format

○ Auto-detect   Status: Inactive   Log Format: Post 2.0.10 log format

● Post 2.0.10 log format (manual)

○ Post 2.0 log format (manual)

○ Post 1.9 log format (manual)

○ Pre 1.9 log format (manual)

Fig. 2:4-18 Shadow Log Format window

Specify the Shadow Log Format

The window is comprised of the Log Format frame containing radio buttons corresponding to the following options: “Auto-detect”, “Post 2.0.10 log format (manual)”, Post 2.0 log format (manual)”, “Post 1.9 log format (manual)”, and “Pre 1.9 log format (manual)”.

***NOTE**: For the WFR Web Filter, the only selection that should be made in this window is “Auto-detect” or “Post 2.0.10 log format (manual)”.*

Auto-detect option

By default, “Auto-detect” is selected. Using this option, the Web Filter will search for a connection to the SR and identify the software version applied to the SR.

Status:

- Active - displays by default
- Inactive - displays if the SR is not connected to the Web Filter

Log Format:

- Post 1.9 log format - not applicable in this software release
- Post 2.0 log format - not applicable in this software release
- Post 2.0.10 log format - displays by default

Post 2.0.10 log format option

If this Web Filter currently has the 2.0.10 or higher software version applied, the Post 2.0.10 log format option should be selected.

Apply Setting

Click **Apply** to apply the setting for the shadow log format.

WF GROUP ADMINISTRATOR SECTION

Introduction

The WF Group Administrator Section of this portion of the user guide is comprised of two chapters that include information on functions performed by the group administrator.

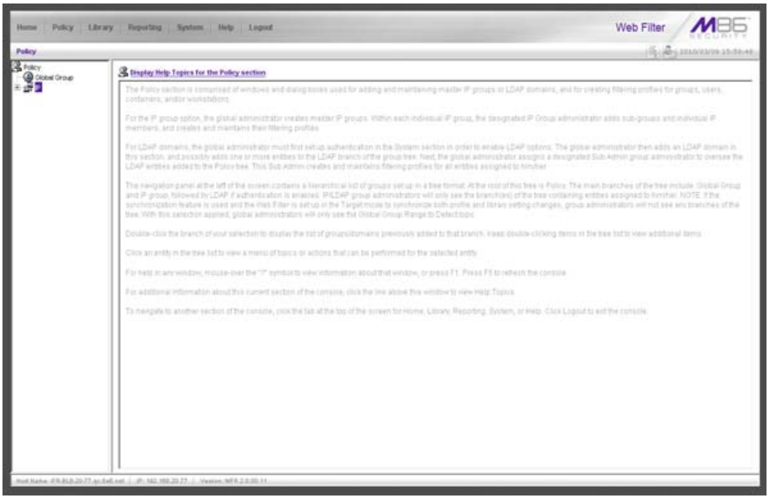
Chapter 1 includes information on setting up and maintaining master IP groups and group members. Chapter 2 includes information on creating and maintaining Custom Categories for libraries.

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
- creates and maintains customized library categories
- uses the lookup tool to remove URLs or search engine keywords from customized libraries

Chapter 1: Policy screen

Group administrators use Policy 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 or MAC address (the latter when using the mobile mode) and may contain a netmask within a valid IP address range.



The Policy section is comprised of windows and dialog boxes used for adding and maintaining master IP groups or LDAP domains, and for creating filtering profiles for groups, users, containers, and/or workstations.

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

For LDAP domains, the global administrator must first set up authentication in the System section in order to enable LDAP options. The global administrator then adds an LDAP domain in this section, and possibly adds one or more entities to the LDAP branch of the group tree. Next, the global administrator assigns a designated Sub Admin group administrator to oversee the LDAP entities added to the Policy tree. This Sub Admin creates and maintains filtering profiles for all entities assigned to him/her.

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 Policy. The main branches of the tree include: Global Group and IP group, followed by LDAP if authentication is enabled. IP/LDAP group administrators will only see the branch(es) of the tree containing entities assigned to him/her. NOTE: If the synchronization feature is used and the Web Filter is set up in the Target mode to synchronize both profile and library setting changes, group administrators will not see any branches of the tree. With this selection applied, global administrators will only see the Global Group Range to Detect topic.

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 the selected entity.

For help in any window, mouse-over the "?" symbol to view information about that window, or press F1. Press F5 to refresh the console.

For additional information about this current section of the console, click the link above this window to view Help Topics.

To navigate to another section of the console, click the tab at the top of the screen for Home, Library, Reporting, System, or Help. Click Logout to exit the console.

Fig. 3:1-1 Policy screen

The navigation panel at the left of the screen contains the IP branch of the Policy tree.

***NOTE**: If the synchronization feature is used, a server set up in the Target mode to synchronize both profile and library setting changes will not have branches of the tree accessible.*

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.

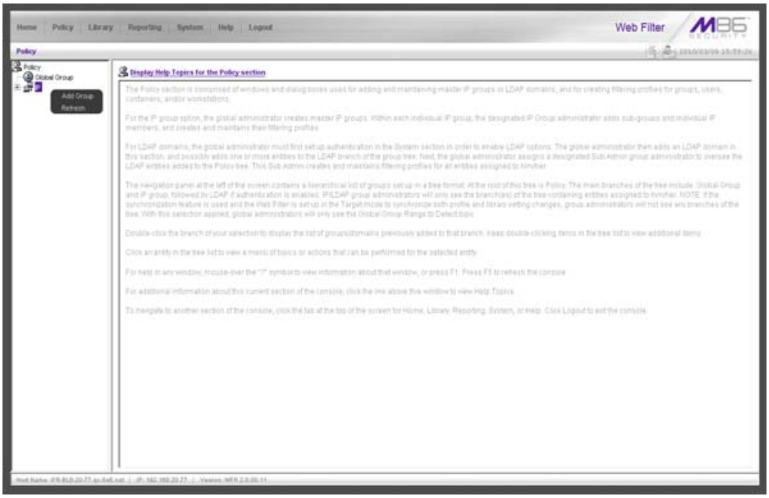
Click an entity in the tree list to view a menu of topics or actions that can be performed for that entity.

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.



The Policy section is comprised of windows and dialog boxes used for adding and maintaining master IP groups or LDAP domains, and for creating filtering profiles for groups, users, containers, and/or workstations.

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

For LDAP domains, the global administrator must first set up authentication in the System section in order to enable LDAP options. The global administrator then adds an LDAP domain in this section, and possibly adds one or more entities to the LDAP branch of the group tree. Next, the global administrator assigns a designated Sub Admin group administrator to oversee the LDAP entities added to the Policy tree. This Sub Admin creates and maintains filtering profiles for all entities assigned to him/her.

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 Policy. The main branches of the tree include: Global Group and IP group, followed by LDAP if authentication is enabled. IP/LDAP group administrators will only see the branch(es) of the tree containing entities assigned to him/her. NOTE: If the synchronization feature is used and the Web Filter is set up in the Target mode to synchronize both profile and library setting changes, group administrators will not see any branches of the tree. With this selection applied, global administrators will only see the Global Group Range to Detect topic.

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 the selected entity.

For help in any window, mouse-over the "i" symbol to view information about that window, or press F1. Press F5 to refresh the console.

For additional information about this current section of the console, click the link above this window to view Help Topics.

To navigate to another section of the console, click the tab at the top of the screen for Home, Library, Reporting, System, or Help. Click Logout to exit the console.

Host Name: [illegible] | IP: [illegible] | Version: [illegible]

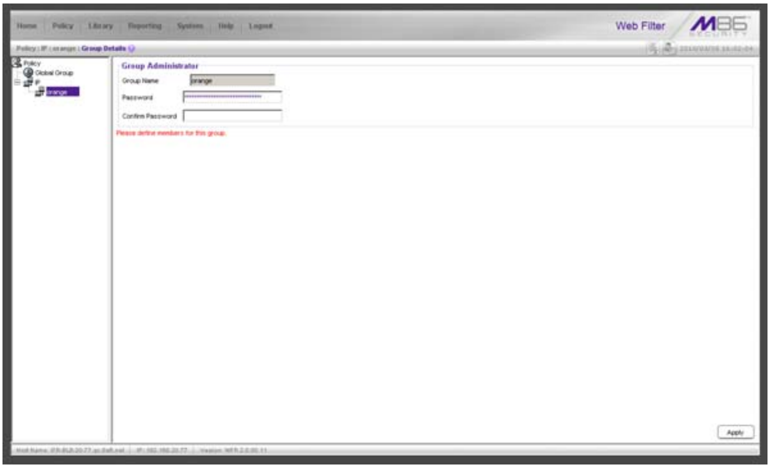
Fig. 3:1-2 Policy screen, IP menu

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, Approved Content (incl. VuSafe), Upload/Download IP Profile, Add Sub Group, Add Individual IP, Delete Group, and Paste Sub Group.

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.



Group Administrator

Group Name: orange

Password: ••••••••••••••••••••••••

Confirm Password:

Please define members for this group.

Fig. 3:1-3 Group Details window

Change the Group Administrator Password

In the Group Administrator frame, the **Group Name** displays.

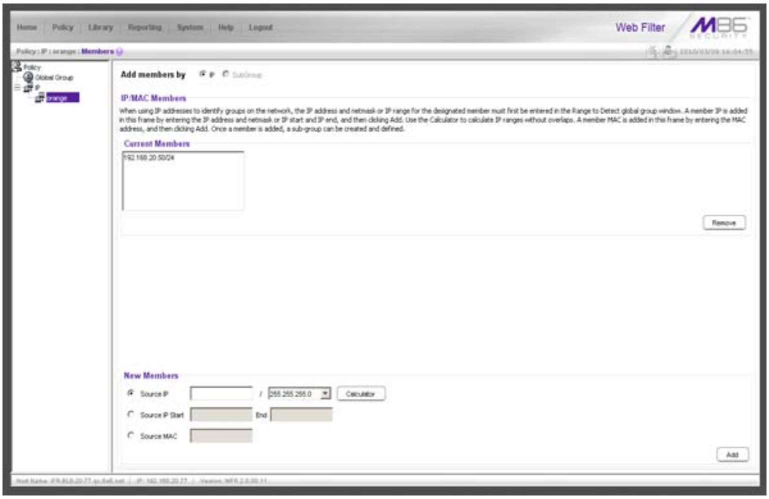
To change the password for this group:

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. For the invisible and router modes, a member is comprised of an associated IP address, and a sub-group may also contain a netmask. For the mobile mode, a member's MAC address is used for obtaining the end user's filtering profile.

***NOTE**: See Appendix D: Mobile Client for information on adding members when using the mobile mode.*



Home | Policy | Library | Reporting | System | Help | Logout
Web Filter
M86 SECURITY
Policy : IP : orange : Members
Policy
Global Group
IP
orange
Remove
Calculator
Add

Add members by ● IP ○ SubGroup

IP/MAC Members

When using IP addresses to identify groups on the network, the IP address and netmask or IP range for the designated member must first be entered in the Range to Detect global group window. A member IP is added in this frame by entering the IP address and netmask or IP start and IP end, and then clicking Add. Use the Calculator to calculate IP ranges without overlaps. A member MAC is added in this frame by entering the MAC address, and then clicking Add. Once a member is added, a sub-group can be created and defined.

Current Members

192.168.20.50/24

New Members

● Source IP ____ / 255.255.255.0

○ Source IP Start ____ End ____

○ Source MAC ____

Fig. 3:1-4 Members window

Add the IP Address of the Member

If using the invisible or router mode:

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.

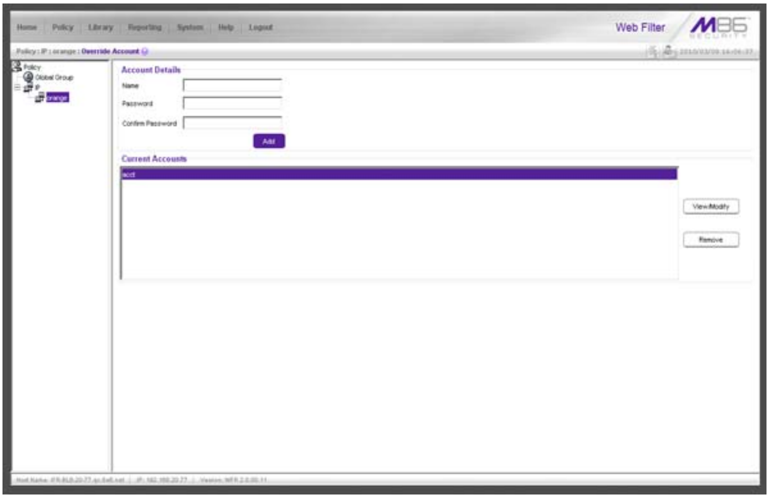


Fig. 3:1-5 Override Account window

***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 WF Global Administrator Section for information on setting up a global group user's override account.

See Appendix C: 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.

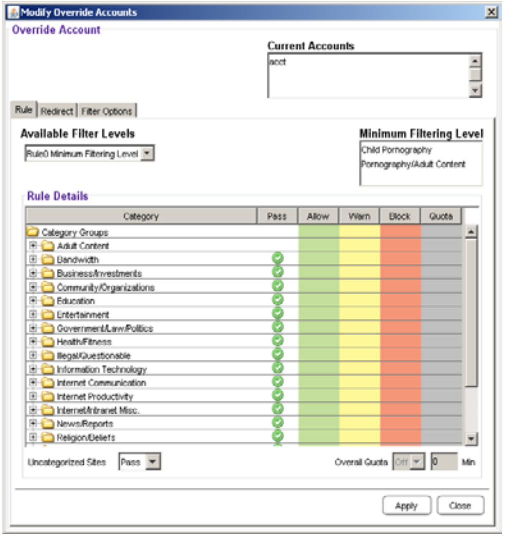
Add an Override Account

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.



Current Accounts: acct

Available Filter Levels: Rule0 Minimum Filtering Level

Minimum Filtering Level: Child Pornography, Pornography/Adult Content

Category	Pass	Allow	Warn	Block	Quota
Category Groups					
Adult Content					
Bandwidth	✓				
Business/Investments	✓				
Community/Organizations	✓				
Education	✓				
Entertainment	✓				
Government/Law/Politics	✓				
Health/Fitness	✓				
Illegal/Questionable	✓				
Information Technology	✓				
Internet Communication	✓				
Internet Productivity	✓				
Internet/Intranet Misc.	✓				
News/Reports	✓				
Religion/Beliefs	✓				

Uncategorized Sites: Pass

Overall Quota: Off 0 Min

Fig. 3:1-6 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.*

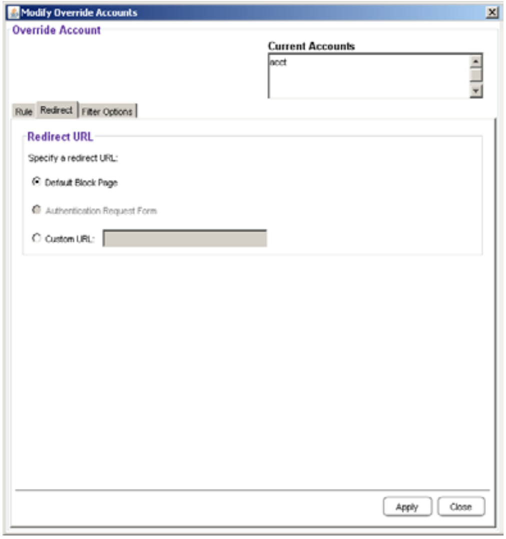
- The **Overall Quota** field becomes enabled if a quota is entered for any library group/category. By default, the enabled Overall Quota is turned “Off”. If turned “On”, enter the number of minutes in the **Min** field to indicate when the end user’s access to passed library groups/ categories with 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.



Current Accounts: acct

Specify a redirect URL:

● Default Block Page

○ Authentication Request Form

○ Custom URL:

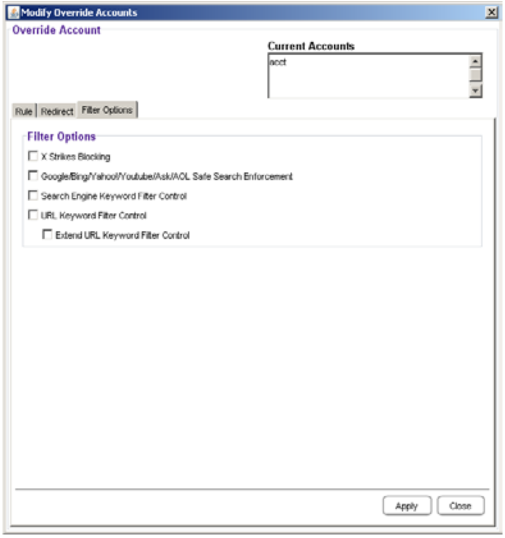
Fig. 3:1-7 Override Account pop-up window, Redirect tab

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.



acct

Filter Options

□ X Strikes Blocking
□ Google/Bing/Yahoo!/Youtube/Ask/AOL Safe Search Enforcement
□ Search Engine Keyword Filter Control
□ URL Keyword Filter Control
  □ Extend URL Keyword Filter Control

Fig. 3:1-8 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 WF Global Administrator Section for information on setting up the X Strikes Blocking feature.*

- “Google/Bing/Yahoo!/Youtube/Ask/AOL Safe Search Enforcement” - With the Google/Bing/Yahoo!/Youtube/Ask/AOL Safe Search Enforcement option enabled, Google, Bing.com, Yahoo!, YouTube, Ask.com, and

AOL's "strict" SafeSearch Filtering option will be used whenever the end user performs a Google, Bing.com, Yahoo!, YouTube, 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, Bing.com, Yahoo!, YouTube, 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, Bing.com, Yahoo!, YouTube, 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**.

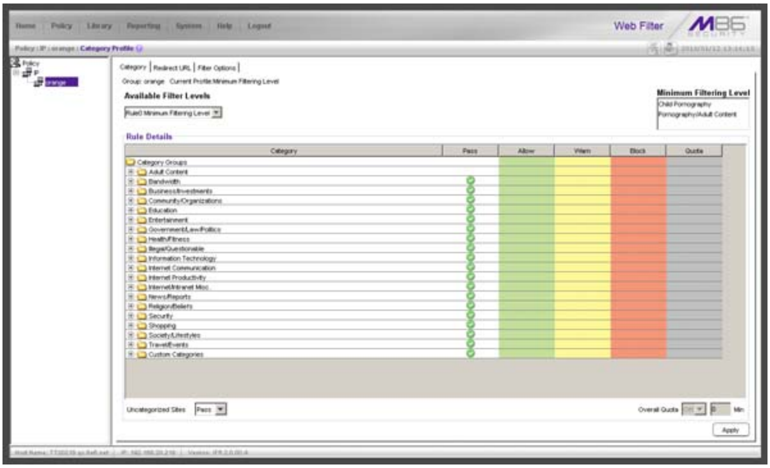
Group Profile window

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.

NOTE*: The Group Profile window is similar to the Sub Group Profile window and the Individual IP Profile window, except the latter windows are configured and maintained by the group administrator.*

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.



Group: orange Current Profile:Minimum Filtering Level

Available Filter Levels

Rule0 Minimum Filtering Level

Minimum Filtering Level

Child Pornography
Pornography/Adult Content

Category	Pass	Allow	Warn	Block	Quota
Category Groups					
Adult Content					
Bandwidth	✓				
Business/Investments	✓				
Community/Organizations	✓				
Education	✓				
Entertainment	✓				
Government/Law/Politics	✓				
Health/Fitness	✓				
Illegal/Questionable	✓				
Information Technology	✓				
Internet Communication	✓				
Internet Productivity	✓				
Internet/Intranet Misc.	✓				
News/Reports	✓				
Religion/Beliefs	✓				
Security	✓				
Shopping	✓				
Society/Lifestyles	✓				
Travel/Events	✓				
Custom Categories	✓				

Uncategorized Sites: Pass

Overall Quota: Off 0 Min

Fig. 3:1-9 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 M86 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.*

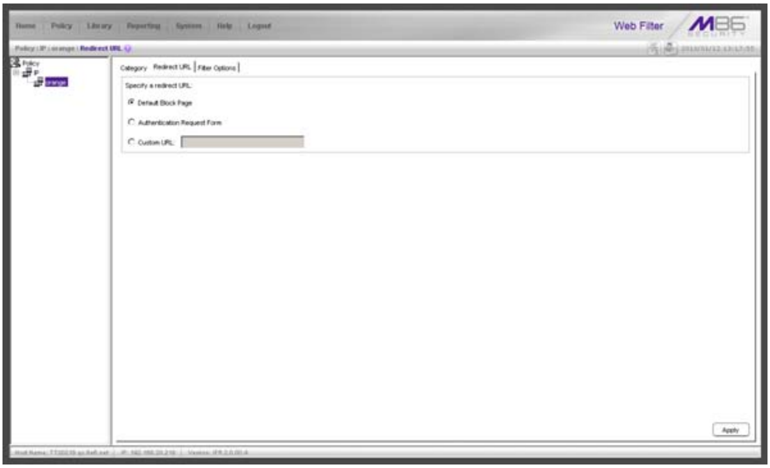
NOTE*: See the Quota Settings window in Chapter 1: System screen for more information on configuring quota settings and resetting quotas for end users currently blocked by quotas.*

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.



Specify a redirect URL:

● Default Block Page

○ Authentication Request Form

○ Custom URL:

Fig. 3:1-10 Group Profile window, Redirect URL tab

Create, Edit the Redirect URL

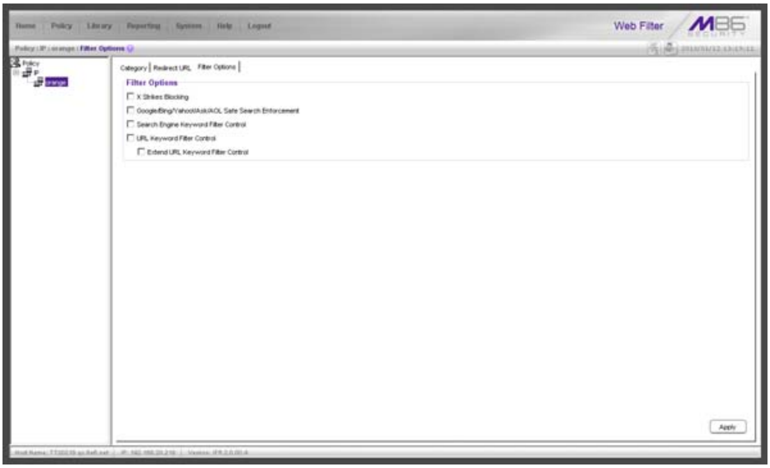
1. Specify the type of redirect URL to be used: “Default Block Page”, “Authentication Request Form”, or “Custom URL”.

   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.



Filter Options

□ X Strikes Blocking
□ Google/Bing/Yahoo!/Ask/AOL Safe Search Enforcement
□ Search Engine Keyword Filter Control
□ URL Keyword Filter Control
  □ Extend URL Keyword Filter Control

Fig. 3:1-11 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!/Youtube/Ask/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 WF Global Administrator Section for information on setting up the X Strikes Blocking feature.*

Google/Bing/Yahoo!/Youtube/Ask/AOL Safe Search Enforcement

With the Google/Bing/Yahoo!/Youtube/Ask/AOL Safe Search Enforcement option enabled, Google, Bing.com, Yahoo!, YouTube, Ask.com, and AOL's "strict" SafeSearch Filtering option will be used whenever end users perform a Google, Bing.com, Yahoo!, YouTube, 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 M86's library or is blocked by Google, Bing.com, Yahoo!, YouTube, 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, Bing.com, Yahoo!, YouTube, 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, Bing.com, Yahoo!, YouTube, 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.

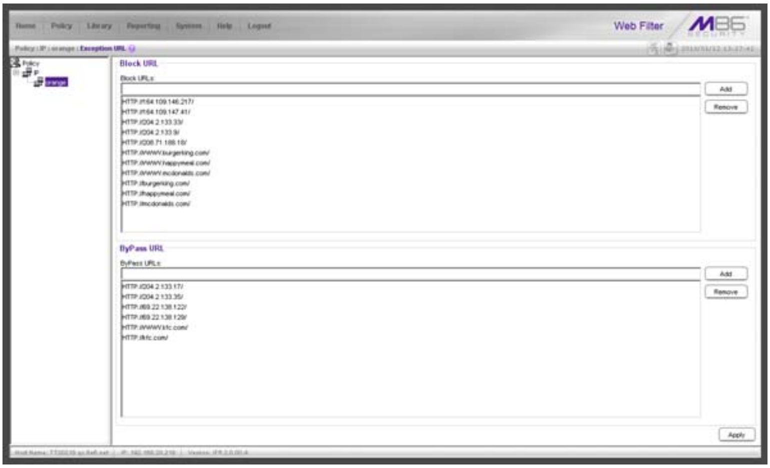
***NOTE**: To set up URL keywords in a URL Keywords window for Custom Categories, see Chapter 2: Library screen, URL Keywords window.*

***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.

***NOTE**: This window is identical to the window by the same name in the Sub Group and Individual IP sections of the Policy tree.*



Block URL

Block URLs:

HTTP://64.109.146.217/
HTTP://64.109.147.41/
HTTP://204.2.133.33/
HTTP://204.2.133.9/
HTTP://208.71.188.18/
HTTP://WWW.burgerking.com/
HTTP://WWW.happymeal.com/
HTTP://WWW.mcdonalds.com/
HTTP://burgerking.com/
HTTP://happymeal.com/
HTTP://mcdonalds.com/

ByPass URL

ByPass URLs:

HTTP://204.2.133.17/
HTTP://204.2.133.35/
HTTP://69.22.138.122/
HTTP://69.22.138.129/
HTTP://WWW.kfc.com/
HTTP://kfc.com/

Fig. 3:1-12 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.)*

Valid URL entries

The following types of URL entries are accepted in this window:

- formats such as: **http://www.coors.com**, **www.coors.com**, or **coors.com**
- 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
- query string - e.g. http://www.youtube.com/watch?v=3_Wfnj1IlMU

NOTE*: The pound sign (#) character is not allowed in this entry.*

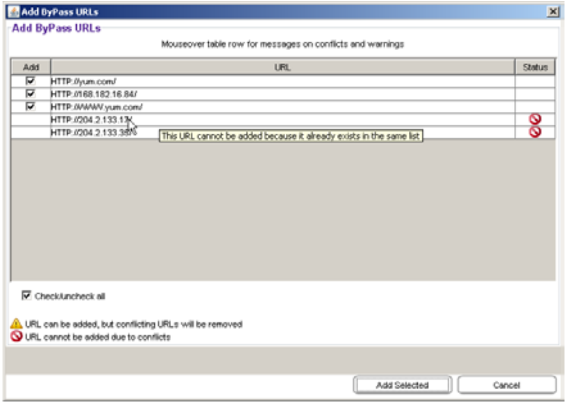
- wildcard entry format that uses an asterisk (*) followed by a period (.) and then the URL, such as: ***.coors.com**

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

Add URLs to Block URL or ByPass URL frame

To block or bypass specified URLs, in the Block URL or the ByPass URL frame:

1. Type the URL to be blocked in the **Block URLs** field, or the URL to be bypassed in the **ByPass URLs** field.
2. Click **Add** to open the Add Block URLs / Add Bypass URLs pop-up window to view all corresponding URLs found by the query:



Add ByPass URLs

Mouseover table row for messages on conflicts and warnings

Add	URL	Status
☑	HTTP://yum.com/	
☑	HTTP://168.182.16.84/	
☑	HTTP://WWW.yum.com/	
	HTTP://204.2.133.1[illegible]	🚫
	HTTP://204.2.133.3[illegible]	🚫

This URL cannot be added because it already exists in the same list

☑ Check/uncheck all

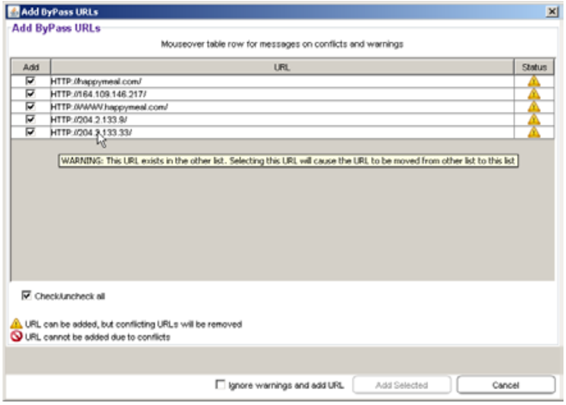
⚠ URL can be added, but conflicting URLs will be removed
🚫 URL cannot be added due to conflicts

Fig. 3:1-13 Add ByPass URLs pop-up window

This window includes a pre-populated checkbox preceding each URL found by the query. Uncheck any checkbox corresponding to a URL you do not want to include in your list. Click the “Check/uncheck all” checkbox at the bottom of this window to toggle between selecting or de-selecting all checkboxes in this window.

***NOTES**: The following messages display in this pop-up window if any URL found by the query is already included in either frame of the Exception URL window: “URL can be added, but conflicting URLs will be removed” (this message is preceded by a yellow warning triangle icon), and “URL cannot be added due to conflicts” (this message is preceded by a red circle icon with a line through it). Mousing over this URL in the table provides details about the status of the URL in the Exception URL window.*

The message "URL can be added, but conflicting URLs will be removed" applies to any URL that the query found included in the opposite frame of the Exception URL window. When this scenario occurs, for each conflicting URL a yellow warning triangle icon displays in the Status column of the pop-up window. At the bottom of this window, the "ignore warnings and add URL" field displays to the left of the Add Selected button:



Add ByPass URLs

Add ByPass URLs

Mouseover table row for messages on conflicts and warnings

Add	URL	Status
☑	HTTP://happymeal.com/	⚠
☑	HTTP://164.109.146.217/	⚠
☑	HTTP://WWW.happymeal.com/	⚠
☑	HTTP://204.2.133.9/	⚠
☑	HTTP://204.2.133.33/	⚠

WARNING: This URL exists in the other list. Selecting this URL will cause the URL to be moved from other list to this list

☑ Check/uncheck all

⚠ URL can be added, but conflicting URLs will be removed
🚫 URL cannot be added due to conflicts

☐ Ignore warnings and add URL

Fig. 3:1-14 Conflicting URLs found by query

Clicking the checkbox for the "ignore warnings and add URL" field activates the Add Selected button. Clicking Add Selected closes the pop-up window and moves the selected URLs to the opposite frame in the Exception URL window.

The message "URL cannot be added due to conflicts" applies to any URL that the query found already included in the same target frame. When this scenario occurs, for each URL already included in the frame, a red circle icon with a line through it displays in the Status column of the pop-up window (see Fig. 3:1-13). The URL cannot be added since it is already included in the list.

***TIP**: Click Cancel to close this pop-up window without making any selections.*

3. Click **Add Selected** to close the pop-up window and to add your selection(s) in the appropriate URL list box.

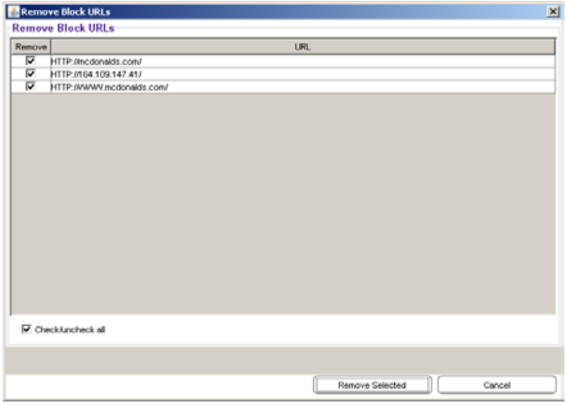
Remove URLs from Block URL or ByPass URL frame

To remove URLs from the Block URL or the ByPass URL frame:

1. Select a URL to be removed from the Block URL / ByPass URL list box; your selection populates the Block URLs field / ByPass URLs field.

***TIP**: Choose a non-IP address URL to maximize results to be returned by the URL query.*

2. Click **Remove** to open the Remove Block URLs / Remove ByPass URLs pop-up window to view all corresponding URLs found by the query:



Remove	URL
☑	HTTP://mcdonalds.com/
☑	HTTP://164.109.147.41/
☑	HTTP://WWW.mcdonalds.com/

☑ Check/uncheck all

Fig. 3:1-15 Remove Block URLs pop-up window

This window includes a pre-populated checkbox preceding each URL found by the query. Uncheck any checkbox corresponding to a URL you do not want to remove from your list. Clicking the “Check/uncheck all” checkbox at the bottom of this window toggles between selecting or de-selecting all checkboxes in this window.

***TIP**: Click Cancel to close this pop-up window without making any selections.*

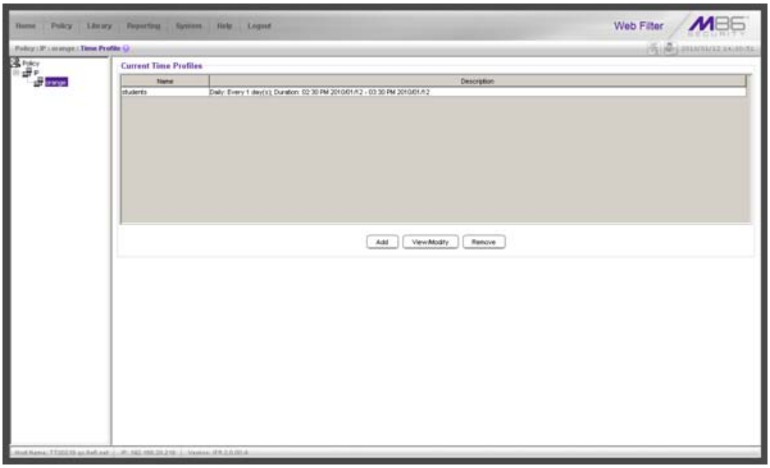
3. Click **Remove Selected** to close the pop-up window and to remove your selection(s) from the appropriate URL list box.

Apply Settings

Click **Apply** to apply your settings after adding or removing any URLs.

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.



Current Time Profiles

Name	Description
students	Daily: Every 1 day(s); Duration: 02:30 PM 2010/01/12 - 03:30 PM 2010/01/12

Fig. 3:1-16 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.

***NOTE**: This window is similar to the one used for Sub Group and Individual IP profiles.*

Add a Time Profile

To create a time profile:

1. Click **Add** to open the Adding Time Profile pop-up box:

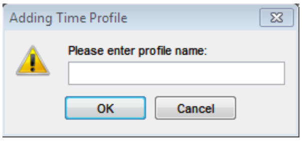
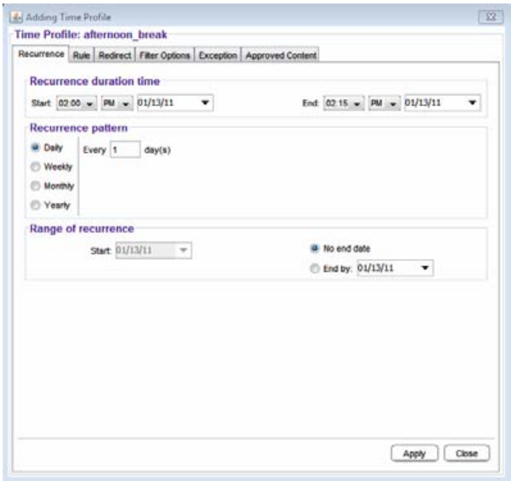


Fig. 3:1-17 Adding Time Profile

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:



Time Profile: afternoon_break

Recurrence duration time

Start: 02:00 PM 01/13/11 End: 02:15 PM 01/13/11

Recurrence pattern

● Daily Every 1 day(s)
○ Weekly
○ Monthly
○ Yearly

Range of recurrence

Start: 01/13/11 ● No end date
○ End by: 01/13/11

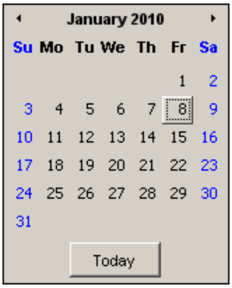
Fig. 3:1-18 Time Profile window Recurrence tab

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:



Su	Mo	Tu	We	Th	Fr	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

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 2010, the first Monday in June this year would be the 7th. The next time this profile would be used will be in June 2012.

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.)

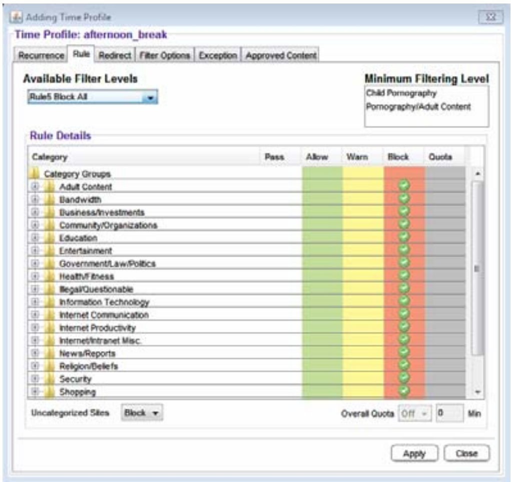
8. Click **Apply** to activate the time profile for the IP group at the specified time.

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.



Adding Time Profile

Time Profile: afternoon_break

Available Filter Levels: Rule5 Block All

Minimum Filtering Level: Child Pornography, Pornography/Adult Content

Rule Details

Category	Pass	Allow	Warn	Block	Quota
Category Groups					
Adult Content				✓	
Bandwidth				✓	
Business/Investments				✓	
Community/Organizations				✓	
Education				✓	
Entertainment				✓	
Government/Law/Politics				✓	
Health/Fitness				✓	
Illegal/Questionable				✓	
Information Technology				✓	
Internet Communication				✓	
Internet Productivity				✓	
Internet/Intranet Misc.				✓	
News/Reports				✓	
Religion/Beliefs				✓	
Security				✓	
Shopping				✓	

Uncategorized Sites: Block

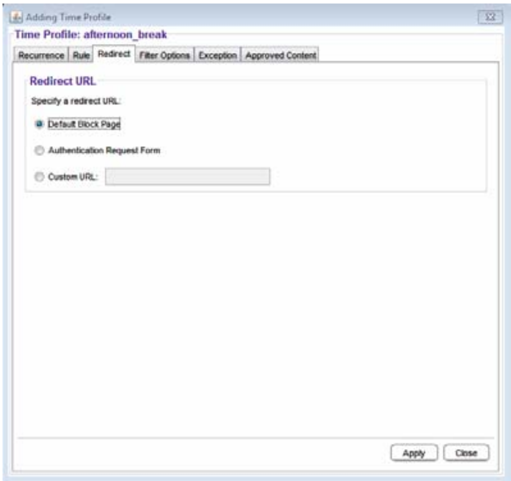
Overall Quota: Off 0 Min

Fig. 3:1-19 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.



Specify a redirect URL:

● Default Block Page

○ Authentication Request Form

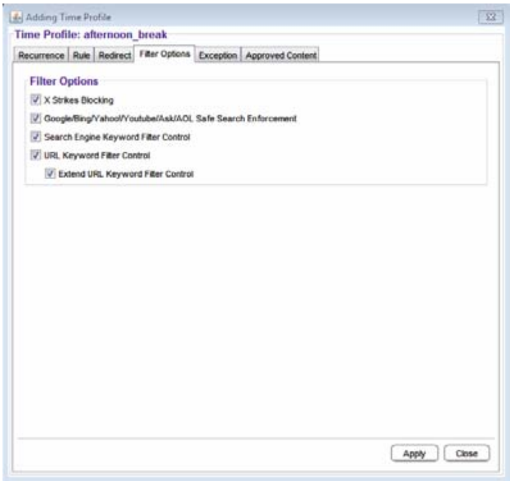
○ Custom URL:

Fig. 3:1-20 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.



Time Profile: afternoon_break

Filter Options

☑ X Strikes Blocking

☑ Google/Bing/Yahoo!/Youtube/Ask/AOL Safe Search Enforcement

☑ Search Engine Keyword Filter Control

☑ URL Keyword Filter Control

☑ Extend URL Keyword Filter Control

Fig. 3:1-21 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.

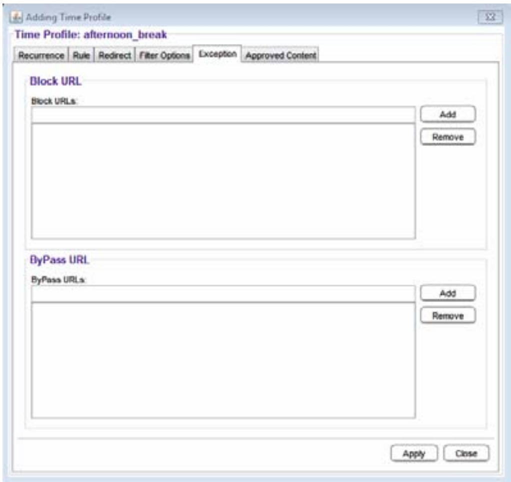


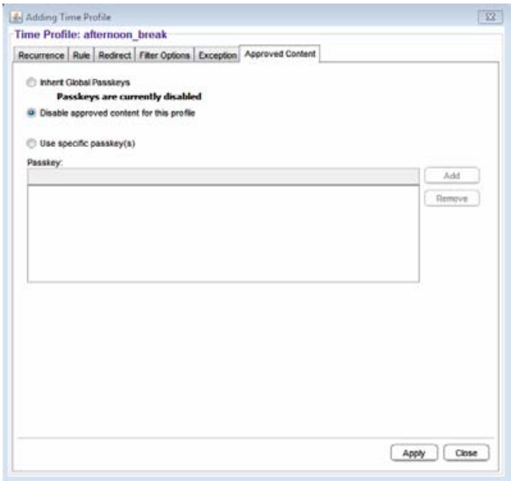
Fig. 3:1-22 Time Profile pop-up window, Exception tab

***NOTES**: See the Exception URL window sub-section in this chapter for information about entries that can be made for this component of the filtering profile.*

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.)

Approved Content

The Approved Content tab is used for enabling/disabling the Approved Content feature for users to view specific YouTube or SchoolTube videos from a designated portal or from VuSafe. If this feature is enabled for this profile, passkeys for approved videos are entered in the Passkey list box.



○ Inherit Global Passkeys

Passkeys are currently disabled

● Disable approved content for this profile

○ Use specific passkey(s)

Passkey:

Fig. 3:1-23 Time Profile pop-up window, Approved Content tab

NOTE: See the Approved Content Settings window sub-section in this chapter for information about entries that can be made for this component of the filtering profile.

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, Approved Content).
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.

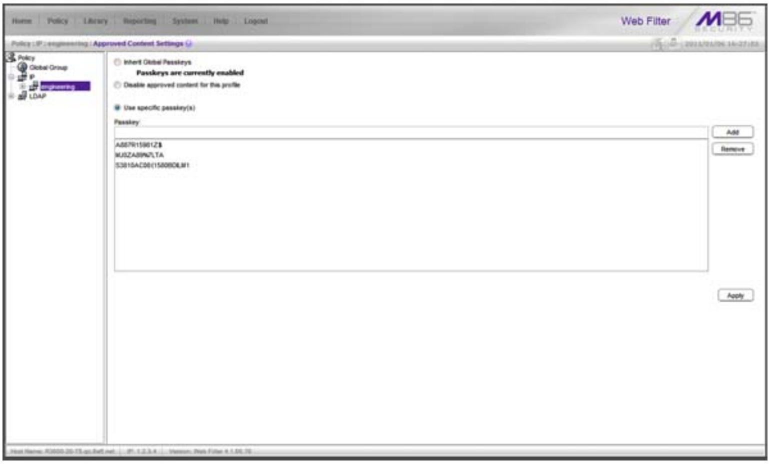
Delete a Time Profile

To delete a time profile:

1. Select the time profile from the Current Time Profiles list box.
2. Click **Remove**.

Approved Content Settings window

The Approved Content Settings window displays when Approved Content (incl. VuSafe) is selected from the group menu. This window is used for granting users access to a specified set of approved YouTube or SchoolTube videos—via a portal managed by someone within the organization—or videos posted to VuSafe.



○ Inherit Global Passkeys

Passkeys are currently enabled

○ Disable approved content for this profile

● Use specific passkey(s)

Passkey

A887R15981Z$
MJSZA89N7LTA
S3810AC00(1580BDL81

Fig. 3:1-24 Approved Content Settings window

NOTE*: See Approved Content Settings window from Chapter 2 of the WF Global Administrator Section for information about the Approved Content feature and VuSafe.*

Approved Content setup and configuration

There are two parts to set up in order to use the Approved Content feature:

- A portal for viewing videos must be created
- The passkey of each approved video must be entered in the Approved Content Settings window for the user's profile

NOTE*: If Pattern Blocking is enabled (System > Control > Filter > Service Control frame), then the filtering profile must "Allow" the Flash Video (FLV) pattern (Category Groups > Bandwidth > Streaming Media > Flash Video).*

Approved Content portal setup

To create a portal for users to view approved YouTube and/or SchoolTube videos, you will need the following:

- Online Web page or intranet page that you or someone in your organization will maintain for users to view approved videos
- Text editor tool such as Notepad or TextPad
- MD5 checksum calculator tool

NOTE*: See the M86 Approved Content Portal Setup document at* ***http://www.m86security.com/software/8e6/docs/ug/misc/wf.ac.4.1.00.pdf*** *for instructions on setting up a portal and passkeys for users to view YouTube or SchoolTube videos.*

Approved Content Settings entries

1. Choose one of the following options by clicking its corresponding radio button:
   - **Inherit Global Passkeys** - If the Global Group’s Approved Content Settings window has the “Enable Approved Content (incl. VuSafe)” option selected, the message “Passkeys are currently enabled” displays in this window. Choosing this option grants this profile access to all videos that have passkeys set up in the Global Group’s Passkey list box.

If the Global Group has the "Enable Approved Content (incl. VuSafe)" option disabled, the message "Passkeys are currently disabled" displays, and any passkeys listed for the Global Group will not be inherited by this profile. In this scenario, select either of the other two options, based on whether the Approved Content feature should be disabled or enabled for this profile.

- **Disable approved content for this profile** - Choosing this option disables the Approved Content feature for this profile.
- **Use specific passkey(s)** - Choosing this option lets the profile use passkeys added to the Passkey list box.

  To add a passkey to the Passkey list box:

  a. Enter the case-sensitive, eight to 20 character code in the **Passkey** field.

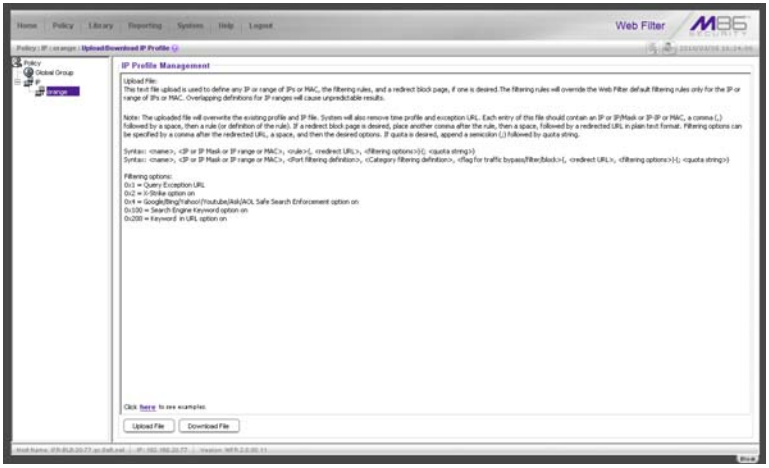
  b. Click **Add**.

***TIP**: To remove a passkey from the list box, select it and then click **Remove**.*

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

Upload/Download IP Profile window

The IP Profile Management 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.



Upload File:
This text file upload is used to define any IP or range of IPs or MAC, the filtering rules, and a redirect block page, if one is desired. The filtering rules will override the Web Filter default filtering rules only for the IP or range of IPs or MAC. Overlapping definitions for IP ranges will cause unpredictable results.

Note: The uploaded file will overwrite the existing profile and IP file. System will also remove time profile and exception URL. Each entry of this file should contain an IP or IP/Mask or IP-IP or MAC, a comma (,) followed by a space, then a rule (or definition of the rule). If a redirect block page is desired, place another comma after the rule, then a space, followed by a redirected URL in plain text format. Filtering options can be specified by a comma after the redirected URL, a space, and then the desired options. If quota is desired, append a semicolon (;) followed by quota string.

Syntax: <name>, <IP or IP Mask or IP range or MAC>, <rule>[, <redirect URL>, <filtering options>][; <quota string>]
Syntax: <name>, <IP or IP Mask or IP range or MAC>, <Port filtering definition>, <Category filtering definition>, <flag for traffic bypass/filter/block>[, <redirect URL>, <filtering options>][; <quota string>]

Filtering options:
0x1 = Query Exception URL
0x2 = X-Strike option on
0x4 = Google/Bing/Yahoo!/Youtube/Ask/AOL Safe Search Enforcement option on
0x100 = Search Engine Keyword option on
0x200 = Keyword in URL option on

Click here to see examples.

Fig. 3:1-25 IP Profile Management window

Upload IP Profiles

1. Click **Upload File** to open both the refresh message page (see Fig. 3:1-27) and the Upload IP Profiles pop-up window:

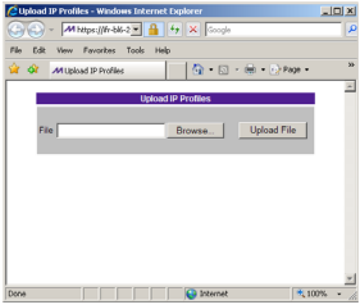


Fig. 3:1-26 Upload IP Profiles pop-up window

***NOTE**: Leave the refresh page open until the file containing the profile has been uploaded.*

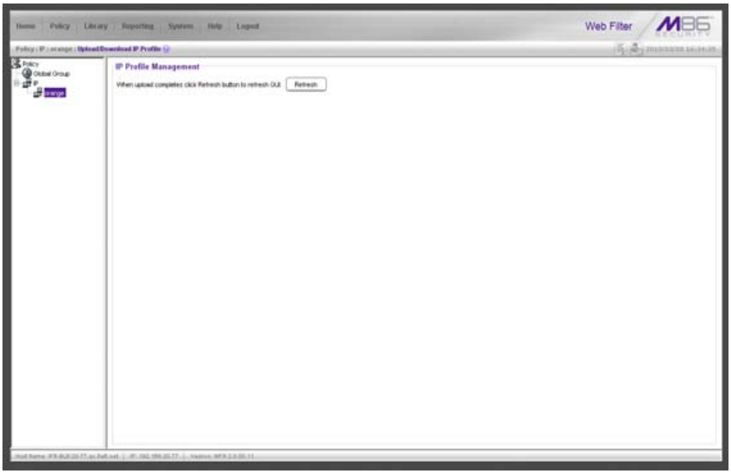
2. Click **Browse...** to open the Choose file window in which you find and select the file containing the IP profiles to be uploaded. This text file of user/group profiles must be entered in a specific format.

NOTE**: For examples of entries to include in a profile file, go to **http://www.m86security.com/software/8e6/hlp/ifr/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 **Refresh** in the refresh page to refresh the IP groups branch of the tree:



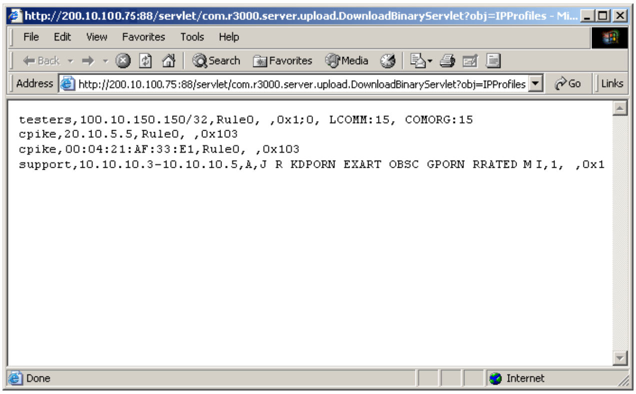
When upload completes click Refresh button to refresh GUI.

Fig. 3:1-27 Upload IP Profiles refresh page

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:


http://200.10.100.75:88/servlet/com.r3000.server.upload.DownloadBinaryServlet?obj=IPProfiles - Mi...
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Media
Address
http://200.10.100.75:88/servlet/com.r3000.server.upload.DownloadBinaryServlet?obj=IPProfiles
Go
Links
Done
Internet

```
testers,100.10.150.150/32,Rule0, ,0x1;0, LCOMM:15, COMORG:15
cpike,20.10.5.5,Rule0, ,0x103
cpike,00:04:21:AF:33:E1,Rule0, ,0x103
support,10.10.10.3-10.10.10.5,A,J R KDPORN EXART OBSC GPORN RRATED M I,1, ,0x1
```

Fig. 3:1-28 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:

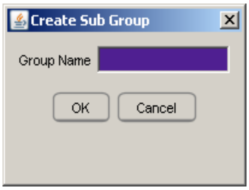


Fig. 3:1-29 Create Sub Group box

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” 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 in the Policy 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:

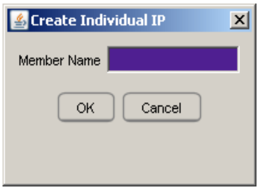


Fig. 3:1-30 Create Individual IP box

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” 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 in the Policy 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:

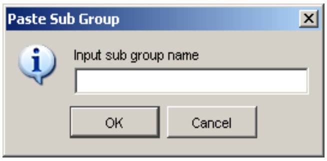


Fig. 3:1-31 Paste Sub Group dialog box

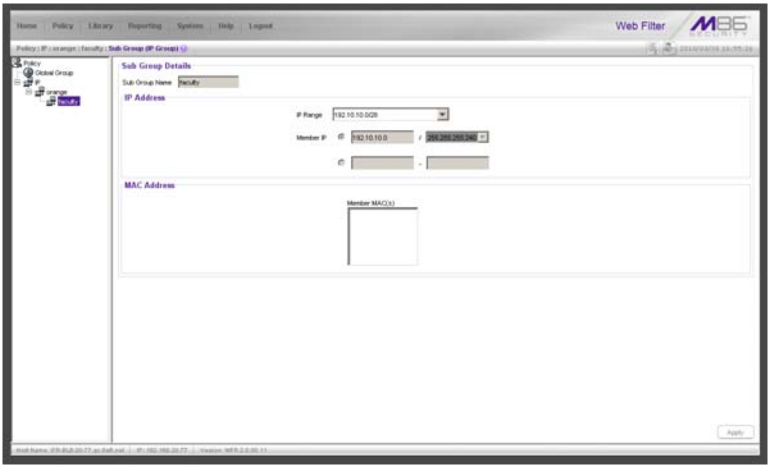
2. In the **Input sub group name** field, enter the name of the sub-group.
3. Click **OK** to add the sub-group to the group in the Policy tree.

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, Approved Content (incl. VuSafe), Delete Sub Group, and Copy Sub Group.

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.



Sub Group Details

Sub Group Name: faculty

IP Address

IP Range: 192.10.10.0/28

Member IP: ● 192.10.10.0 / 255.255.255.240

○ -

MAC Address

Member MAC(s)

Fig. 3:1-32 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:

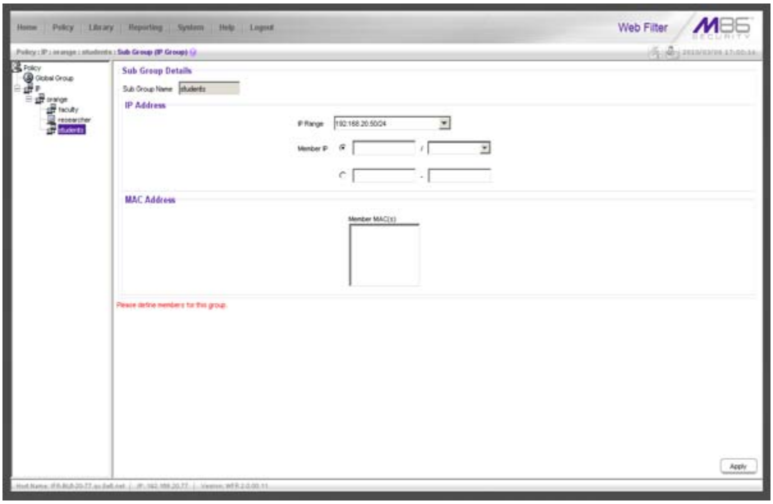
- Sub Group Name

- IP Range
- Member IP address and netmask or IP address range, and MAC Address(es) if using the mobile mode.

***NOTE**: See Appendix D: Mobile Client for information on using the mobile mode.*

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.



Sub Group Name: students

IP Range: 192.168.20.50/24

Member IP ● / ○ -

Please define members for this group.

Fig. 3:1-33 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

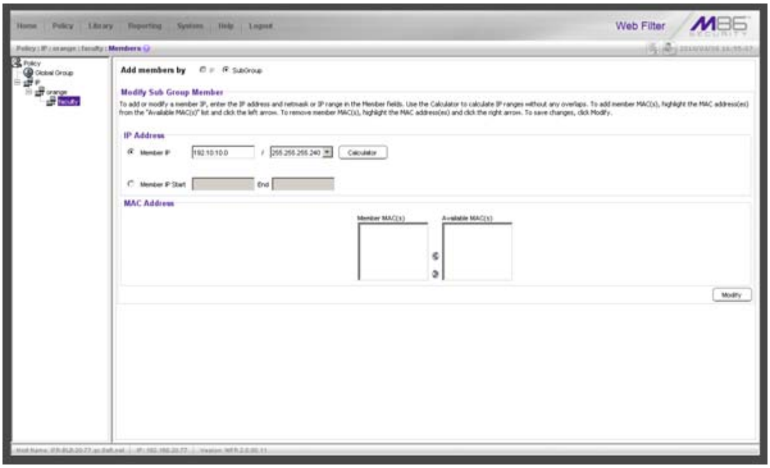
- enter the IP address range in the text boxes.

3. Click **Apply** to save your entries. Once applied, the Member fields become greyed-out and the Apply button becomes deactivated (see Fig. 3:1-32).

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, if using the invisible or router mode. If using the mobile mode, MAC address(es) can be selected for inclusion in the sub-group.

***NOTE**: See Appendix D: Mobile Client for information on modifying members when using the mobile mode.*



Add members by ○ IP ● SubGroup

Modify Sub Group Member

To add or modify a member IP, enter the IP address and netmask or IP range in the Member fields. Use the Calculator to calculate IP ranges without any overlaps. To add member MAC(s), highlight the MAC address(es) from the "Available MAC(s)" list and click the left arrow. To remove member MAC(s), highlight the MAC address(es) and click the right arrow. To save changes, click Modify.

IP Address

● Member IP 192.10.10.0 / 255.255.255.240

○ Member IP Start End

MAC Address

Member MAC(s)

Available MAC(s)

Fig. 3:1-34 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 Master IP Group sub-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 Master IP Group sub-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, Approved Content.*

Approved Content Settings window

The Approved Content Settings window displays when Approved Content (incl. VuSafe) is selected from the sub-group menu. This window is used for granting access to a specified set of approved online videos posted to YouTube or SchoolTube—via a portal managed by someone within the organization—or videos posted to VuSafe.

***NOTES**: See the Approved Content Settings window in Chapter 2 of the WF Global Administrator Section of this user guide for information about the Approved Content feature and VuSafe.*

*See the M86 Approved Content Portal Setup document at **http://www.m86security.com/software/8e6/docs/ug/misc/wf.ac.4.1.00.pdf** for information on setting up a portal and pass-keys for viewing online YouTube and/or SchoolTube videos. See the Approved Content Settings window in the Master IP Group sub-section of this chapter for information on entries that can be made in this window.*

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.)

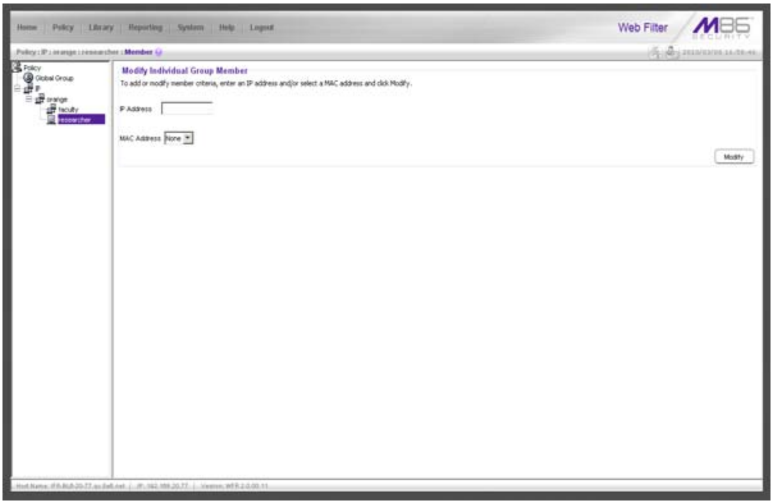
Individual IP

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, Approved Content (incl. VuSafe), Delete Individual IP.

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, if using the invisible or router mode. If using the mobile mode, the member's MAC address can be selected for inclusion in the sub-group.

***NOTE**: See Appendix D: Mobile Client for information on modifying members when using the mobile mode.*



Modify Individual Group Member

To add or modify member criteria, enter an IP address and/or select a MAC address and click Modify.

IP Address

MAC Address: None

Fig. 3:1-35 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 Master IP Group sub-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 Master IP Group sub-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, Approved Content.*

Approved Content Settings window

The Approved Content Settings window displays when Approved Content (incl. VuSafe) is selected from the individual IP member menu. This window is used for granting access to a specified set of approved online videos posted to YouTube or SchoolTube—via a portal managed by someone within the organization—or videos posted to VuSafe.

***NOTES**: See the Approved Content Settings window in Chapter 2 of the WF Global Administrator Section of this user guide for information about the Approved Content feature and VuSafe.*

*See the M86 Approved Content Portal Setup document at **http://www.m86security.com/software/8e6/docs/ug/misc/wf.ac.4.1.00.pdf** for information on setting up a portal and pass-keys for viewing online YouTube and/or SchoolTube videos. See the Approved Content Settings window in the Master IP Group sub-section of this chapter for information on entries that can be made in this window.*

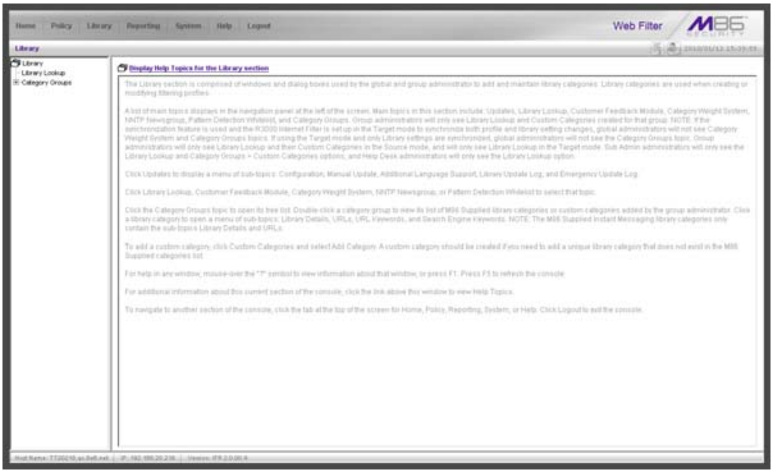
Delete Individual IP

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 and to add and maintain custom library categories for a group. Library categories are used when creating or modifying filtering profiles.



The Library section is comprised of windows and dialog boxes used by the global and group administrator to add and maintain library categories. Library categories are used when creating or modifying filtering profiles.

A list of main topics displays in the navigation panel at the left of the screen. Main topics in this section include: Updates, Library Lookup, Customer Feedback Module, Category Weight System, NNTP Newsgroup, Pattern Detection Whitelist, and Category Groups. Group administrators will only see Library Lookup and Custom Categories created for that group. NOTE: If the synchronization feature is used and the R3000 Internet Filter is set up in the Target mode to synchronize both profile and library setting changes, global administrators will not see Category Weight System and Category Groups topics. If using the Target mode and only Library settings are synchronized, global administrators will not see the Category Groups topic. Group administrators will only see Library Lookup and their Custom Categories in the Source mode, and will only see Library Lookup in the Target mode. Sub Admin administrators will only see the Library Lookup and Category Groups > Custom Categories options, and Help Desk administrators will only see the Library Lookup option.

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, Customer Feedback Module, Category Weight System, NNTP Newsgroup, or Pattern Detection Whitelist to select that topic.

Click the Category Groups topic to open its tree list. Double-click a category group to view its list of M86 Supplied library categories or custom categories added by the group administrator. Click a library category to open a menu of sub-topics: Library Details, URLs, URL Keywords, and Search Engine Keywords. NOTE: The M86 Supplied Instant Messaging library categories only contain the sub-topics Library Details and URLs.

To add a custom category, click Custom Categories and select Add Category. A custom category should be created if you need to add a unique library category that does not exist in the M86 Supplied categories list.

For help in any window, mouse-over the "?" symbol to view information about that window, or press F1. Press F5 to refresh the console.

For additional information about this current section of the console, click the link above this window to view Help Topics.

To navigate to another section of the console, click the tab at the top of the screen for Home, Policy, Reporting, System, or Help. Click Logout to exit the console.

Fig. 3:2-1 Library screen

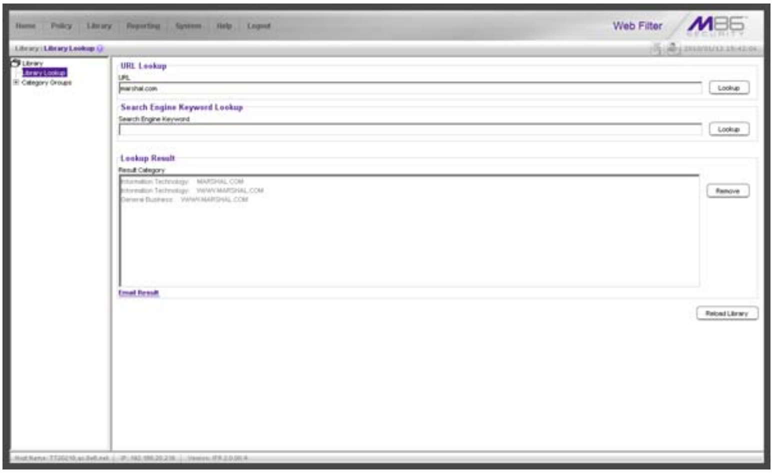
A list of main topics displays in the navigation panel at the left of the screen. Main topics in this section include the following: Library Lookup and Category Groups, the latter topic containing the Custom Categories sub-topic.

***NOTE**: If the synchronization feature is used, a server set up in the Target mode will only have the Library Lookup topic available.*

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.



URL: marshal.com

Search Engine Keyword:

Result Category:
Information Technology: MARSHAL.COM
Information Technology: WWW.MARSHAL.COM
General Business: WWW.MARSHAL.COM

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.coors.com**, **coors.com**, or use a wildcard by entering ***.coors.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
   - query string - e.g. http://www.youtube.com/watch?v=3_Wfnj1llMU

***NOTES**: The pound sign (#) character is not allowed in this entry. 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.

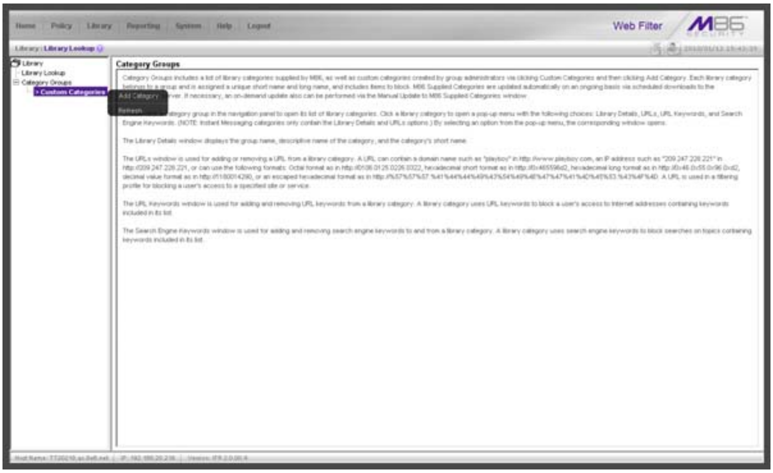
Look up a Search Engine Keyword

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 options for adding a custom category to the tree list and to refresh the menu. Click the Custom Categories link to view a menu of topics: Add Category, and Refresh.



Category Groups

Category Groups includes a list of library categories supplied by M86, as well as custom categories created by group administrators via clicking Custom Categories and then clicking Add Category. Each library category belongs to a group and is assigned a unique short name and long name, and includes items to block. M86 Supplied Categories are updated automatically on an ongoing basis via scheduled downloads to the [illegible]ver. If necessary, an on-demand update also can be performed via the Manual Update to M86 Supplied Categories window.

[illegible] category group in the navigation panel to open its list of library categories. Click a library category to open a pop-up menu with the following choices: Library Details, URLs, URL Keywords, and Search Engine Keywords. (NOTE: Instant Messaging categories only contain the Library Details and URLs options.) By selecting an option from the pop-up menu, the corresponding window opens.

The Library Details window displays the group name, descriptive name of the category, and the category's short name.

The URLs window is used for adding or removing a URL from a library category. A URL can contain a domain name such as "playboy" in http://www.playboy.com, an IP address such as "209.247.228.221" in http://209.247.228.221, or can use the following formats: Octal format as in http://0106.0125.0226.0322, hexadecimal short format as in http://0x465596d2, hexadecimal long format as in http://0x46.0x55.0x96.0xd2, decimal value format as in http://1180014290, or an escaped hexadecimal format as in http://%57%57%57.%41%44%44%49%43%54%49%4E%47%47%41%4D%45%53.%43%4F%4D. A URL is used in a filtering profile for blocking a user's access to a specified site or service.

The URL Keywords 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.

The Search Engine Keywords window is used for adding and removing search engine keywords to and from a library category. A library category uses search engine keywords to block searches on topics containing keywords included in its list.

Fig. 3:2-3 Custom Categories menu

***NOTE**: Since custom categories are not created by M86, updates cannot be provided. Maintaining the list of URLs and keywords is the responsibility of the global or group administrator.*

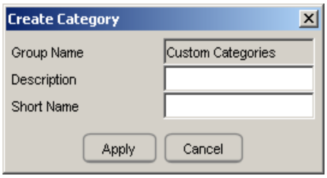
***WARNING**: The maximum number of categories that can be saved is 512. This figure includes both M86 supplied categories and custom categories.*

Add Category

A unique custom library category should be created only if it does not exist in the Category Groups tree, and if any sub-group needs to use that library category. Custom library categories for a group must be maintained by the group administrator.

Add a Custom Library Category

1. Select Add Category to open the Create Category dialog box:



Create Category

Group Name: Custom Categories

Description:

Short Name:

Fig. 3:2-4 Create Category dialog box

The **Group Name** field displays Custom Categories greyed-out.

2. In the **Description** field, enter from three to 20 characters for the long name of the new category.

3. In the **Short Name** field, enter up to seven characters without any spaces for the short name of the new category.

***NOTE**: Once the short name has been saved it cannot be edited.*

4. Click **Apply** to add the category to the Custom Categories tree list. Upon saving this entry, the long name displays in the tree list. For group administrators adding a

new custom category, the group name displays in parentheses after the long name.

***TIP**: If this is the first custom category you are adding, you may need to double-click “Custom Categories” to open the tree list.*

***NOTE**: The category must have URLs, URL keywords, and/or search keywords added to its profile in order for it to be effective.*

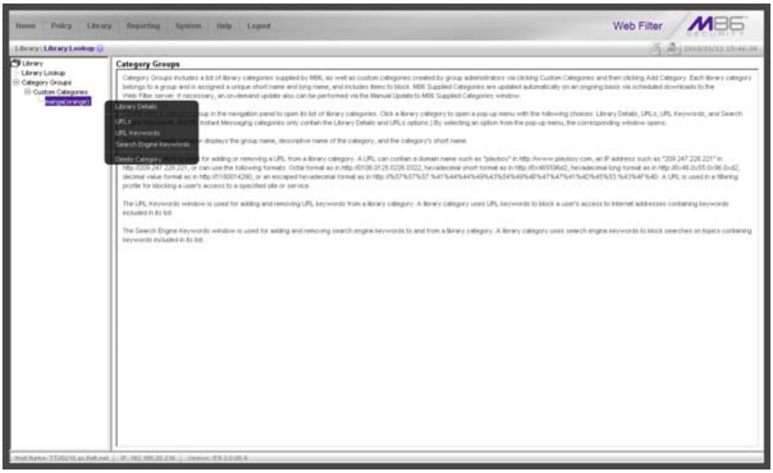
Refresh

Refresh the Library

Click Refresh after uploading a file to a customized library category.

Custom library category

When a custom library category is created, its long name displays in the Custom Categories tree list. Click the custom library category link to view a menu of sub-topics: Library Details, URLs, URL Keywords, Search Engine Keywords, and Delete Category.



Category Groups

Category Groups includes a list of library categories supplied by M86, as well as custom categories created by group administrators via clicking Custom Categories and then clicking Add Category. Each library category belongs to a group and is assigned a unique short name and long name, and includes items to block. M86 Supplied Categories are updated automatically on an ongoing basis via scheduled downloads to the Web Filter server. If necessary, an on-demand update also can be performed via the Manual Update to M86 Supplied Categories window.

oup in the navigation panel to open its list of library categories. Click a library category to open a pop-up menu with the following choices: Library Details, URLs, URL Keywords, and Search Instant Messaging categories only contain the Library Details and URLs options.) By selecting an option from the pop-up menu, the corresponding window opens.

w displays the group name, descriptive name of the category, and the category's short name.

for adding or removing a URL from a library category. A URL can contain a domain name such as "playboy" in http://www.playboy.com, an IP address such as "209.247.228.221" in http://209.247.228.221, or can use the following formats: Octal format as in http://0106.0125.0226.0322, hexadecimal short format as in http://0x465596d2, hexadecimal long format as in http://0x46.0x55.0x96.0xd2, decimal value format as in http://1180014290, or an escaped hexadecimal format as in http://%57%57%57.%41%44%44%49%43%54%49%4E%47%47%41%4D%45%53.%43%4F%4D. A URL is used in a filtering profile for blocking a user's access to a specified site or service.

The URL Keywords 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.

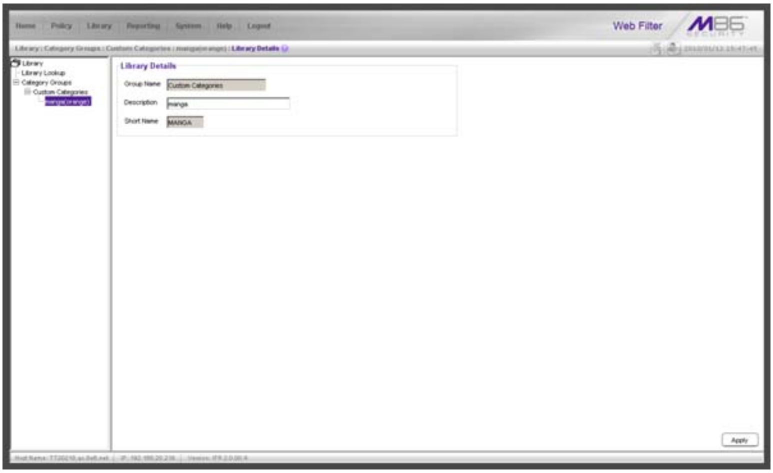
The Search Engine Keywords window is used for adding and removing search engine keywords to and from a library category. A library category uses search engine keywords to block searches on topics containing keywords included in its list.

Fig. 3:2-5 Library screen, custom library category menu

***NOTE**: Since custom categories are not created by M86, updates cannot be provided. Maintaining the list of URLs and keywords is the responsibility of the global or group administrator.*

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 used for editing the long name of the custom library category, and for viewing name criteria previously entered.



Library Details

Group Name: Custom Categories

Description: manga

Short Name: MANGA

Fig. 3:2-6 Library Details window

View, Edit Library Details

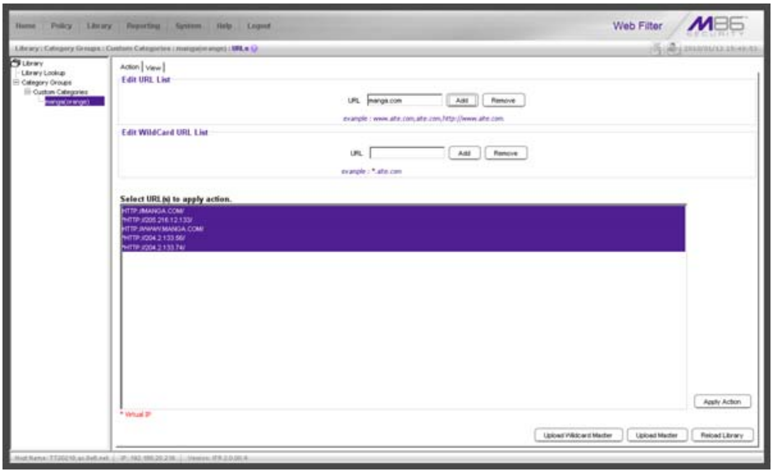
The following display and cannot be edited: Custom Categories **Group Name** and library category **Short Name**.

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 is used in a filtering profile for blocking a user's access to a specified site or service.

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 query string can be entered to block access to a specific URL.



URL manga.com

URL

Select URL(s) to apply action.

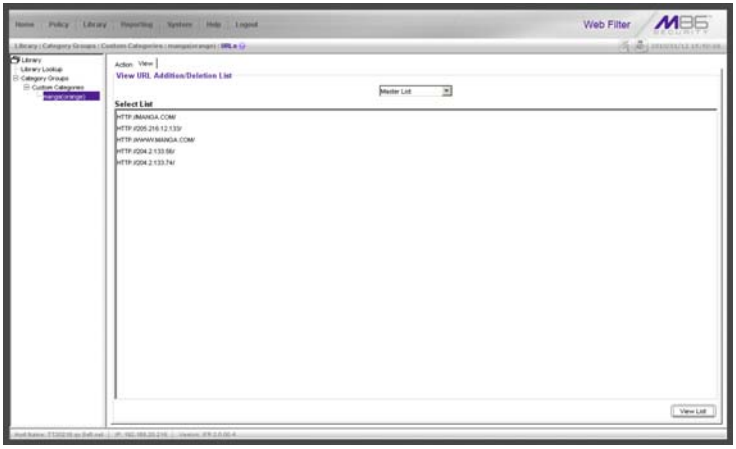
HTTP://MANGA.COM/
*HTTP://205.216.12.133/
HTTP://WWW.MANGA.COM/
*HTTP://204.2.133.56/
*HTTP://204.2.133.74/

Fig. 3:2-7 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:



HTTP://MANGA.COM/
HTTP://205.216.12.133/
HTTP://WWW.MANGA.COM/
HTTP://204.2.133.58/
HTTP://204.2.133.74/

Fig. 3:2-8 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.coors.com**, **www.coors.com**, or **coors.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
   - query string - e.g. http://www.youtube.com/watch?v=3_Wfnj1IlMU

NOTE*: The pound sign (#) character is not allowed in this entry.*

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 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 *.beer.com would find a URL such as http://virtualbartender.beer.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.cnn.com is added to a category that is not set up to be blocked, and *.cnn.com is added to a category set up to be blocked, the end user will be able to access http://www.cnn.com since it is a direct match, but will not be able to access http://www.sports.cnn.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:

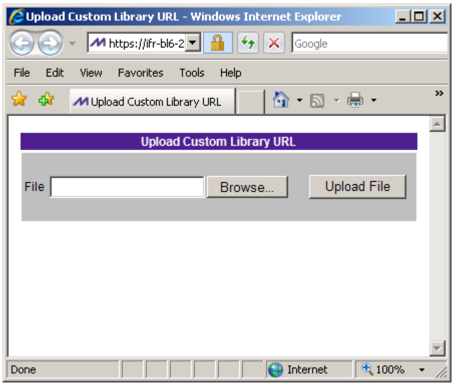

Upload Custom Library URL - Windows Internet Explorer
https://ifr-bl6-2
Google
File Edit View Favorites Tools Help
Upload Custom Library URL
Upload Custom Library URL
File
Browse...
Upload File
Done
Internet
100%

Fig. 3:2-9 Upload Custom Library URL window

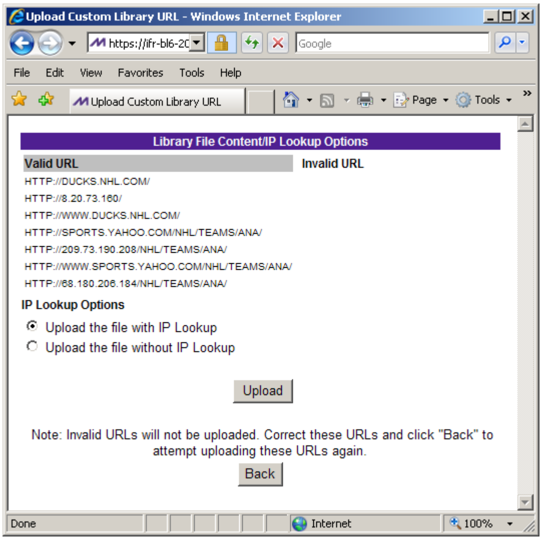
2. Click **Browse...** to open the Choose file pop-up window.
3. Select the file to be uploaded.

***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:



Library File Content/IP Lookup Options

Valid URL	Invalid URL
HTTP://DUCKS.NHL.COM/	
HTTP://8.20.73.160/	
HTTP://WWW.DUCKS.NHL.COM/	
HTTP://SPORTS.YAHOO.COM/NHL/TEAMS/ANA/	
HTTP://209.73.190.208/NHL/TEAMS/ANA/	
HTTP://WWW.SPORTS.YAHOO.COM/NHL/TEAMS/ANA/	
HTTP://68.180.206.184/NHL/TEAMS/ANA/	

IP Lookup Options

● Upload the file with IP Lookup

○ Upload the file without IP Lookup

Upload

Note: Invalid URLs will not be uploaded. Correct these URLs and click "Back" to attempt uploading these URLs again.

Back

Fig. 3:2-10 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:

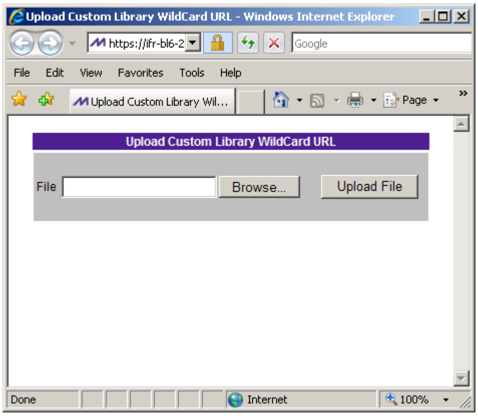

Upload Custom Library WildCard URL - Windows Internet Explorer
https://ifr-bl6-2
Google
File
Edit
View
Favorites
Tools
Help
Upload Custom Library Wil...
Page
Upload Custom Library WildCard URL
File
Browse...
Upload File
Done
Internet
100%

Fig. 3:2-11 Upload Custom Library WildCard URL window

2. Click **Browse...** to open the Choose file pop-up window.

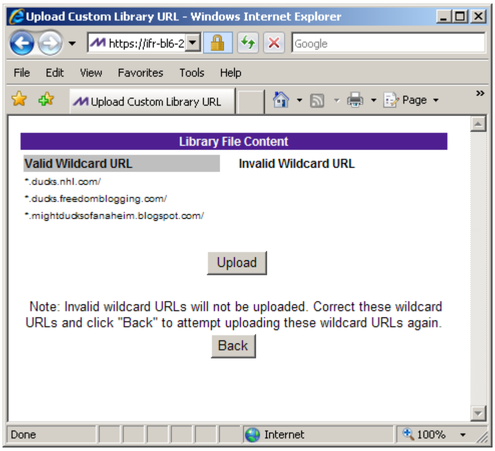
3. Select the file to be uploaded.

***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:


Upload Custom Library URL - Windows Internet Explorer
https://ifr-bl6-2
Google
File
Edit
View
Favorites
Tools
Help
Upload Custom Library URL
Page
Done
Internet
100%

Library File Content

Valid Wildcard URL	Invalid Wildcard URL
*.ducks.nhl.com/	
*.ducks.freedomblogging.com/	
*.mightducksofanaheim.blogspot.com/	

Upload

Note: Invalid wildcard URLs will not be uploaded. Correct these wildcard URLs and click "Back" to attempt uploading these wildcard URLs again.

Back

Fig. 3:2-12 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.*

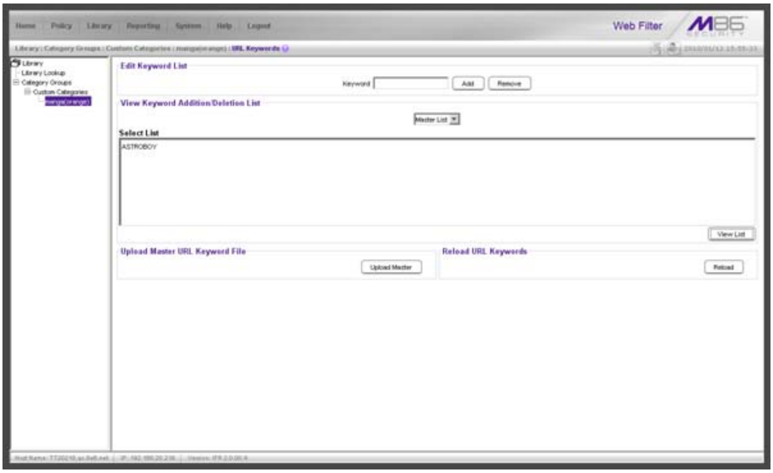
Reload the Library

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 Web Filter, M86 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 custom 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.


Library : Category Groups : Custom Categories : manga(orange) : URL Keywords

Select List: ASTROBOY

View Keyword Addition/Deletion List: Master List

Fig. 3:2-13 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 Policy 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:

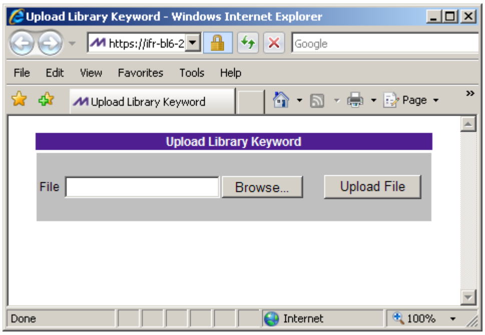


Fig. 3:2-14 Upload Library Keyword pop-up window

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.*

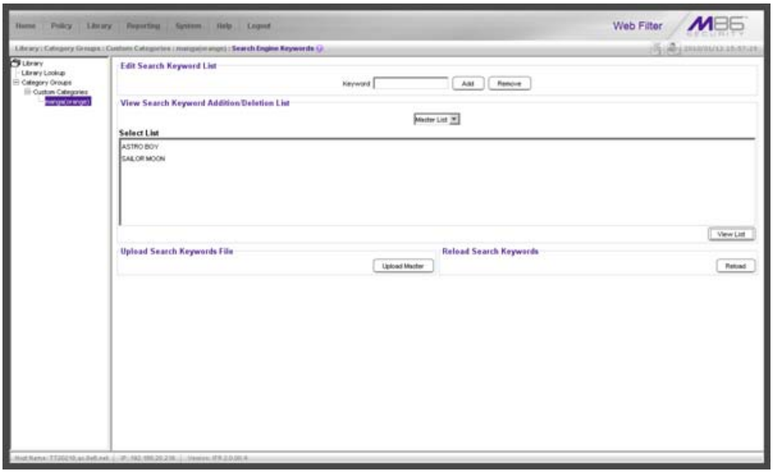
Reload the Library

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 Web Filter, M86 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 custom 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.



Master List

ASTRO BOY
SAILOR MOON

Fig. 3:2-15 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 Policy 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. 3:2-14).
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 Web Filter, M86 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.

WEB FILTER 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 or MAC 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.m86security.com/software/8e6/hlp/ifr/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.m86security.com/resources/database-categories.asp***

- **Filter Option codes:**

  - 0x1 = Exception URL Query (always enabled)
  - 0x2 = X Strikes Blocking
  - 0x4 = Google/Bing/Yahoo!/Youtube/Ask/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.m86security.com/software/8e6/hlp/ifr/files/2group_ipprofiles.html** for examples of filtering profile entries.*

Appendix B

Create a Custom Block Page

M86 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 M86’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 Web Filter

1. Enable block page redirection

Set up for each sub-group

1. Make modifications in one of the redirect URL tabs:
   - Go to: Policy > IP > “Group Name” > “Sub-Group Name” > Sub Group Profile > Redirect URL
   - Go to: Policy > 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 Web Filter console 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 Web Filter 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: Policy > Global Group > Range to Detect
2. Input the IP address under “Destination IP” > ”Exclude IP”

   Without excluding this IP address, the Web Filter 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 M86'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 M86's default block page. If used, the <block page> needs to provide a link back to Web Filter'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 <Web Filter IP> with the real IP in the HTML/CGI before using these samples.*

Part III: Restart the Web Filter

You must restart the Web Filter to make your changes effective.

Reference

HTML

```
<!-- Description: Sample HTML for Web Filter customized block page
-->
<!-- Replace <Web Filter 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://<Web Filter 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>Web Filter 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 Web Filter customized block
page
# Replace the <Web Filter 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>Web Filter 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: $user<br>\n";
print "<br>For further options, <a href=\"http://<Web Filter IP>:81/
cgi/
block.cgi?URL=$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 Web Filter customized
block page
# Replace the <Web Filter 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://<Web Filter 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>Web Filter 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

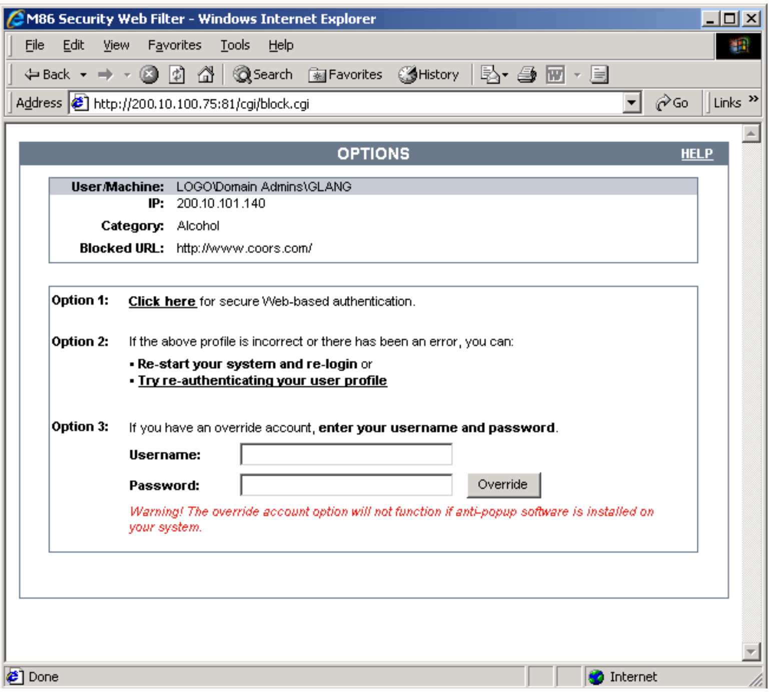
```
/*
 * cusc_block.c
 * Description: sample C source code of CGI for customized block page
 * Replace <Web Filter IP> with real IP and recompile before using
 * Revision: 1
 * Date: 03/08/2004
 */
#include <stdio.h>

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://<Web Filter 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>Web Filter 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 C

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:


M86 Security Web Filter - Windows Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://200.10.100.75:81/cgi/block.cgi
Go Links
Done
Internet

OPTIONS HELP

User/Machine:	LOGO\Domain Admins\GLANG
IP:	200.10.101.140
Category:	Alcohol
Blocked URL:	http://www.coors.com/

Option 1: **Click here** for secure Web-based authentication.

Option 2: If the above profile is incorrect or there has been an error, you can:

- **Re-start your system and re-login** or
- **Try re-authenticating your user profile**

Option 3: If you have an override account, **enter your username and password**.

Username:

Password: Override

Warning! The override account option will not function if anti-popup software is installed on your system.

Fig. C-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. C-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:

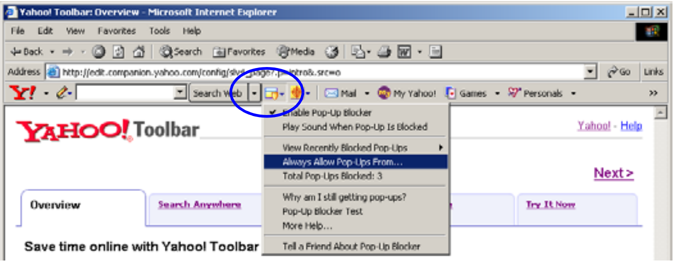
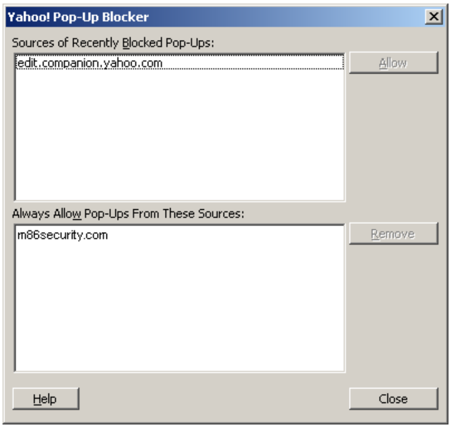

Yahoo! Toolbar: Overview - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://edit.companion.yahoo.com/config/slv4_page?.p=intro&.src=o
Go Links
Y! Search Web Mail My Yahoo! Games Personals
✓ Enable Pop-Up Blocker
Play Sound When Pop-Up Is Blocked
View Recently Blocked Pop-Ups
Always Allow Pop-Ups From...
Total Pop-Ups Blocked: 3
Why am I still getting pop-ups?
Pop-Up Blocker Test
More Help...
Tell a Friend About Pop-Up Blocker
YAHOO! Toolbar
Yahoo! - Help
Next >
Overview
Search Anywhere
Try It Now
Save time online with Yahoo! Toolbar

Fig. C-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:



Yahoo! Pop-Up Blocker

Sources of Recently Blocked Pop-Ups:

edit.companion.yahoo.com

Always Allow Pop-Ups From These Sources:

m86security.com

Fig. C-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.

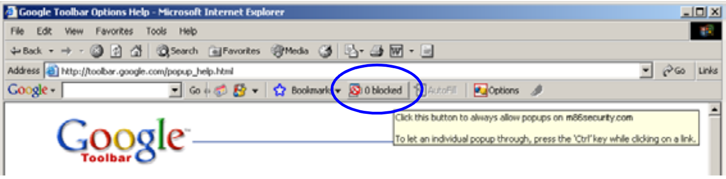
Google Toolbar Pop-up Blocker

If Pop-up Blocking is Enabled

1. In the Options page (see Fig. C-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 Pop-up blocker button:



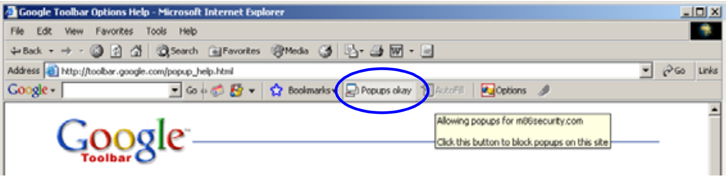
http://toolbar.google.com/popup_help.html

Click this button to always allow popups on m86security.com

To let an individual popup through, press the 'Ctrl' key while clicking on a link.

Fig. C-4 Pop-up blocker button enabled

Clicking this button toggles to the Pop-ups okay button, adding the override account window to your white list:



http://toolbar.google.com/popup_help.html

Allowing popups for m86security.com

Click this button to block popups on this site

Fig. C-5 Pop-ups okay button enabled

AdwareSafe Pop-up Blocker

If Pop-up Blocking is Enabled

1. In the Options page (see Fig. C-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

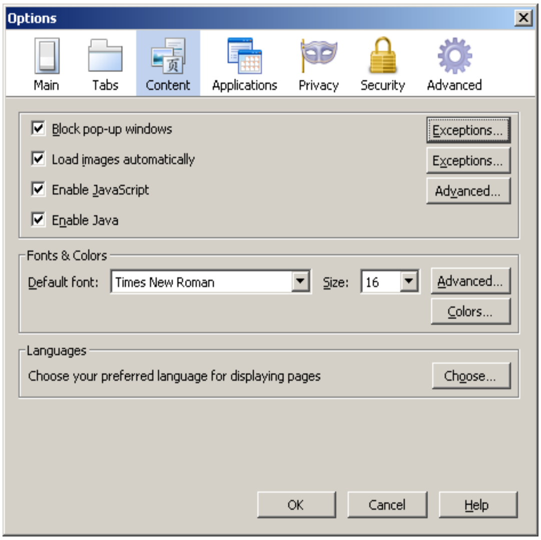
AdwareSafe's SearchSafe toolbar lets you toggle between enabling pop-up blocking (# popups blocked) and disabling pop-up blocking (Popup protection off) by clicking the pop-up icon.

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. C-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 Firefox browser, go to the toolbar and select **Tools > Options** to open the Options dialog box.
2. Click the Content tab at the top of this box to open the Content section:



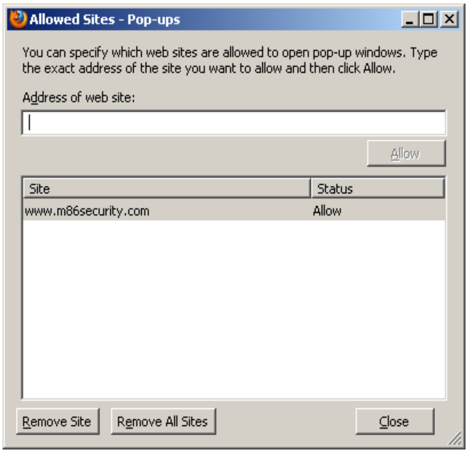
☑ Block pop-up windows
☑ Load images automatically
☑ Enable JavaScript
☑ Enable Java

Fonts & Colors
Default font: Times New Roman
Size: 16

Languages
Choose your preferred language for displaying pages

Fig. C-6 Mozilla Firefox Pop-up Windows Options

3. With the “Block pop-up windows” checkbox checked, click the **Exceptions...** button at right to open the Allowed Sites - Pop-ups box:



You can specify which web sites are allowed to open pop-up windows. Type the exact address of the site you want to allow and then click Allow.

Address of web site:

Site	Status
www.m86security.com	Allow

Fig. C-7 Mozilla Firefox Pop-up Window Exceptions

4. Enter the **Address of the web site** to let the override account window pass.
5. Click **Allow** to add the URL to the list box section below.
6. Click **Close** to close the Allowed Sites - Pop-ups box.
7. Click **OK** to close the Options dialog box.

Windows XP SP2 Pop-up Blocker

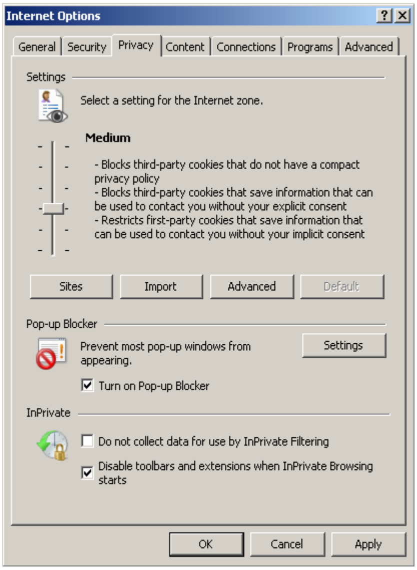
Set up Pop-up Blocking

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:



Select a setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that save information that can be used to contact you without your explicit consent
- Restricts first-party cookies that save information that can be used to contact you without your implicit consent

Prevent most pop-up windows from appearing.

☑ Turn on Pop-up Blocker

☐ Do not collect data for use by InPrivate Filtering

☑ Disable toolbars and extensions when InPrivate Browsing starts

Fig. C-8 Enable pop-up blocking

3. In the Pop-up Blocker frame, check “Turn on Pop-up Blocker”.

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

Use the IE Toolbar

In the IE browser, go to the toolbar and select **Tools > Pop-up Blocker > Turn On Pop-up Blocker**:

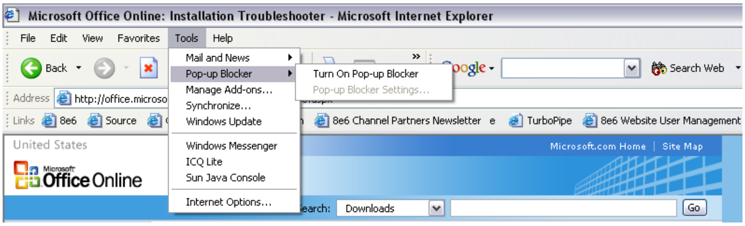


Fig. C-9 Toolbar setup

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

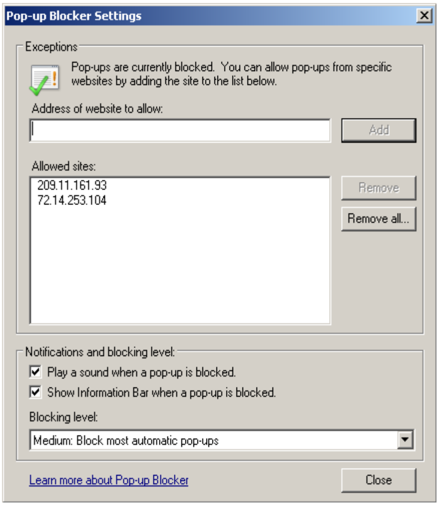
1. In the Options page (see Fig. C-1), enter your **Username** and **Password**.
2. Press and hold the **Ctrl** key on your keyboard while simultaneously clicking the **Override** button—this action opens the override account pop-up window.

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:



Pop-up Blocker Settings

Exceptions

Pop-ups are currently blocked. You can allow pop-ups from specific websites by adding the site to the list below.

Address of website to allow:

Allowed sites:
209.11.161.93
72.14.253.104

Notifications and blocking level:

☑ Play a sound when a pop-up is blocked.

☑ Show Information Bar when a pop-up is blocked.

Blocking level:
Medium: Block most automatic pop-ups

Fig. C-10 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. C-1), enter your **Username** and **Password**.
4. Click the **Override** button to open the override account pop-up window.

Use the Information Bar

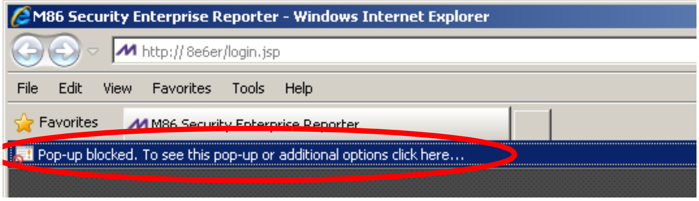
With pop-up blocking enabled, the Information Bar can be set up and used for viewing information about blocked pop-ups or allowing pop-ups from a specified site.

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. C-10).
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. C-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...":

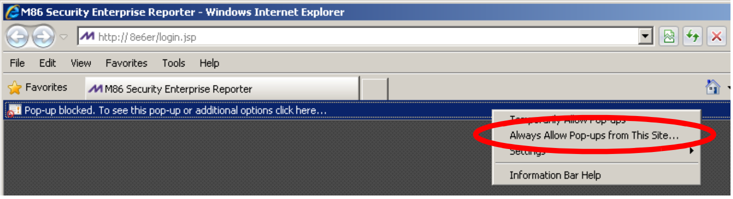


M86 Security Enterprise Reporter - Windows Internet Explorer

Pop-up blocked. To see this pop-up or additional options click here...

Fig. C-11 Information Bar showing blocked pop-up status

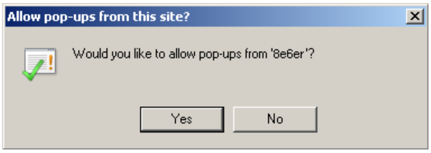
3. Click the Information Bar for settings options:


M86 Security Enterprise Reporter - Windows Internet Explorer
http://8e6er/login.jsp
File
Edit
View
Favorites
Tools
Help
Favorites
M86 Security Enterprise Reporter
Temporarily Allow Pop-ups
Always Allow Pop-ups from This Site...
Settings
Information Bar Help

Pop-up blocked. To see this pop-up or additional options click here...

Fig. C-12 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:



Would you like to allow pop-ups from '8e6er'?

Fig. C-13 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. C-10) 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 D

Mobile Client

Mobile Client performs Internet filtering and blocking on mobile PCs physically located outside your organization. This product is comprised of a Web Filter configured to use the mobile mode, profiles of end users—working at home or on the road—uploaded to the Web Filter configured to use the mobile mode, and Mobile Client software installed on end users' workstations. Mobile Client ensures Internet activity of all end users located outside the organization will be tracked and filtered in the same manner as end users on the Web Filter used in house, thereby giving you, the administrator, assurance that your organization will be protected against lost productivity, network bandwidth issues, Internet security threats, and possible legal problems that can result from the misuse of Internet resources on an unfiltered, remote, laptop computer.

Environment Requirements

Workstation Requirements

System requirements for the administrator include the following:

- Web Filter must be configured to use the Mobile mode option
- Session cookies from the Web Filter must be allowed in order for the Administrator console to function properly
- Pop-up blocking software, if installed, must be disabled
- JavaScript enabled
- Java Virtual Machine
- Java Plug-in (use the version specified for the Web Filter software version)

System requirements for the end user include the following:

- Windows XP, Vista (32-bit), or 7 (32-bit) operating system running:
  - Internet Explorer (IE) 7.0 or 8.0
  - Firefox 3.5 or 3.6
- Macintosh OS X Version 10.4, 10.5, or 10.6 running:
  - Safari 4.0
  - Firefox 3.5 or 3.6

⚠ ***WARNING**: The filtered end user must be set up with standard user rights only—these users should **not** have Power User, Administrator, or root level access.*

Network Requirement

- High speed connection from the Web Filter to mobile PCs

Remote Filtering Components

- Mobile Client software installed on each end user’s mobile PC

Work Flow Overview

Mobile Client Installed on a Mobile PC

For mobile PCs located outside of the organization:

- a Web Filter set up for filtering in the mobile mode is used for obtaining the end user’s profile and for logging his/her Internet activity
- the Mobile Client application is used on the remote PC for filtering the end user’s Internet activity

When these two components are installed, the following scenario occurs on the network:

1. The end user logs into his/her mobile PC located outside of the organization, and then makes a URL request.
2. The Mobile Client detects the Web Filter, and the Web Filter grants the URL request or blocks the request, based on the end user’s profile supplied by the Mobile Client.
3. If the end user comes into the organization, logs into his/her workstation and is authenticated on the internal network, the end user’s profile now comes from the Web Filter, and not the Mobile Client.

Network Operations Overview

Mobile Client on the Network

1. A URL request is made from an end user’s mobile PC to access inappropriate content on the Internet.
2. The Mobile Client installed on the end user’s workstation sends a parallel request to the Web Filter.
3. The Web Filter searches its M86 database for a match to the request. If a match to the requested URL is found and the site is disallowed, the Mobile Client software blocks the connection to the Web server.

***NOTE**: If using Mobile Client software version 2.0 or higher in a Macintosh environment, and the Web Filter is configured to use the “High” HTTPS Filtering Level, Macintosh end users will be blocked from accessing any HTTPS URL. (See the Filter window in the WF Global Administrator Section of this User Guide for information about setting the HTTPS Filtering Level.)*

Mobile Server Section

The Mobile Server Section of this portion of the user guide contains information on how to set up and configure the WFR server’s hardware and Web Filter software to be used with the Mobile Client.

Initial Setup

Basic requirements for initial network setup are as follows:

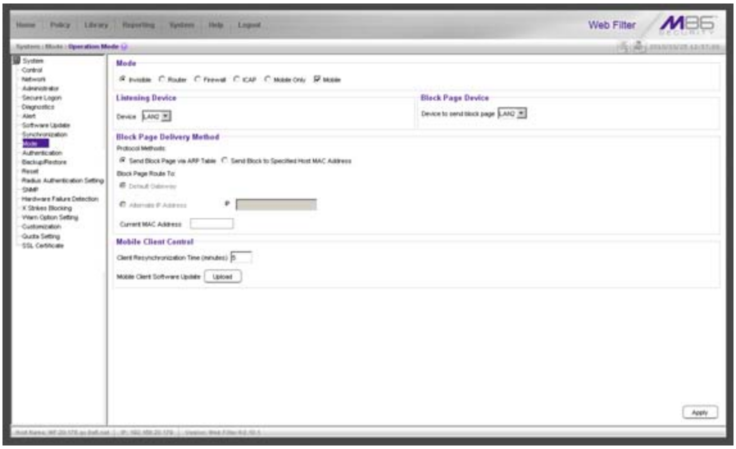
- Port 81 must be open on the network for block page requests
- Port 443 must be open on the network for the Mobile Client to communicate with the Web Filter.

***NOTE**: The WFR server can be set up on the WAN network’s DMZ for extra security purposes.*

Configure the Web Filter to use the Mobile Mode

The Operation Mode window is used for setting up the Web Filter to use the mobile mode for filtering mobile PCs.

1. In the Mode frame, choose either “Mobile Only” or one of the filtering modes (Invisible, Router, FIrewall) with the “Mobile” option added to display the Mobile Client Control frame, used for configuring the Web Filter to use the mobile mode:



Mode

● Invisible ○ Router ○ Firewall ○ ICAP ○ Mobile Only ☑ Mobile

Listening Device

Device LAN2

Block Page Device

Device to send block page LAN2

Block Page Delivery Method

Protocol Methods:

● Send Block Page via ARP Table ○ Send Block to Specified Host MAC Address

Block Page Route To:

● Default Gateway

○ Alternate IP Address IP

Current MAC Address

Mobile Client Control

Client Resynchronization Time (minutes) 5

Mobile Client Software Update

Fig. D-1 Operation Mode window, mobile mode

2. In the **Client Resynchronization Time** field, specify the interval of minutes for the Web Filter to resynchronize the profile on the end user's workstation with the profile set up for him/her on the Web Filter. By default, *60* minutes displays.

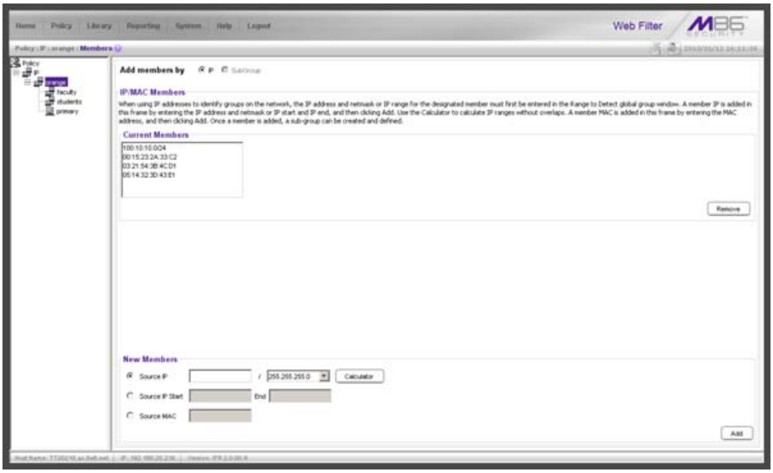
NOTES*: The Mobile Client Software Update field is used if you wish to update end user workstations automatically with the latest configuration files and will be using the Web Filter to host and deploy these files. More information about using this feature is provided in subsequent pages in this section of the user guide.*

The following features are not available when using the mobile mode: Minimum Filtering Level, Time Profile, Override Account, *Exception URL, LDAP Authentication, and Warn and Quota filter settings. (An end user with categories blocked in his/her profile will be blocked from categories with a Warn or Quota setting instead of receiving a warning or quota page. If his/her profile does not contain blocked categories but instead contains categories with Warn or Quota settings, the Global Group Profile will be assigned instead.)*

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

Add MAC Addresses to the Master IP Group

In the mobile mode, the master IP group Members window is used for adding mobile PC MAC addresses. MAC addresses are used for obtaining mobile PC members' filtering profiles.



When using IP addresses to identify groups on the network, the IP address and netmask or IP range for the designated member must first be entered in the Range to Detect global group window. A member IP is added in this frame by entering the IP address and netmask or IP start and IP end, and then clicking Add. Use the Calculator to calculate IP ranges without overlaps. A member MAC is added in this frame by entering the MAC address, and then clicking Add. Once a member is added, a sub-group can be created and defined.

```
100.10.10.0/24
00:15:23:2A:33:C2
03:21:54:3B:4C:D1
05:14:32:3D:43:E1
```

● Source IP [ ] / 255.255.255.0

○ Source IP Start [ ] End [ ]

○ Source MAC [ ]

Fig. D-2 Members window, master IP group with MAC addresses

1. In the New Members frame, select "Source MAC".

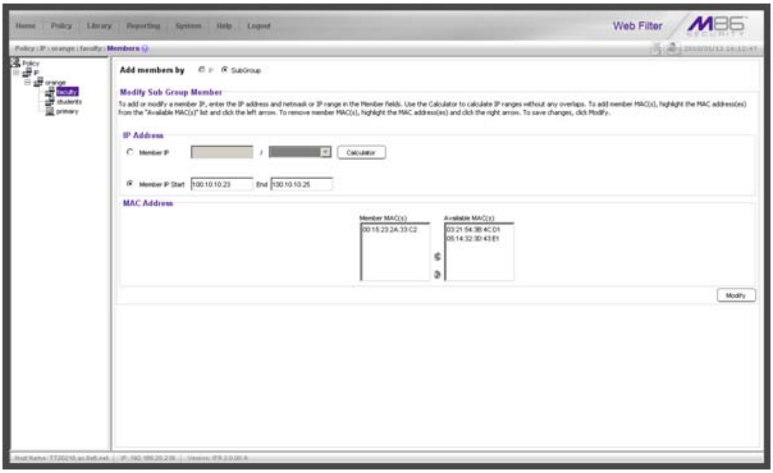
2. Enter the member's MAC address.

3. Click **Add** to include the MAC address entry in the Current Members list box.

***NOTES**: Follow steps 2-3 for each MAC address to be added. To remove a member from the Current Members list box, select the MAC address from the list box, and then click **Remove**.*

Select MAC Addresses for a Sub Group

In the mobile mode, the sub-group Members window is used for selecting MAC addresses for inclusion in the sub-group.



Add members by ○ IP ● SubGroup

Modify Sub Group Member

To add or modify a member IP, enter the IP address and netmask or IP range in the Member fields. Use the Calculator to calculate IP ranges without any overlaps. To add member MAC(s), highlight the MAC address(es) from the "Available MAC(s)" list and click the left arrow. To remove member MAC(s), highlight the MAC address(es) and click the right arrow. To save changes, click Modify.

IP Address

○ Member IP

● Member IP Start 100.10.10.23 End 100.10.10.25

MAC Address

Member MAC(s): 00:15:23:2A:33:C2

Available MAC(s): 03:21:54:3B:4C:D1, 05:14:32:3D:43:E1

Fig. D-3 Members window, sub-group with MAC addresses

The Modify Sub Group Member frame is comprised of the IP Address and MAC Address frames.

1. In the MAC Address frame, Source MAC addresses previously added in the master IP group's Members window display in the Available MAC(s) and/or Member MAC(s) list box(es). Specify whether or not to add/remove MAC addresses to/from the sub-group:
    - To add MAC addresses to the sub-group, select each sub-group by highlighting it in the Available MAC(s) list box, and then clicking the left arrow to move the item(s) to the Member MAC(s) list box.

- To remove MAC addresses from the sub-group, select each sub-group by highlighting it in the Member MAC(s) list box, and then clicking the right arrow to move the item(s) to the Available MAC(s) list box.

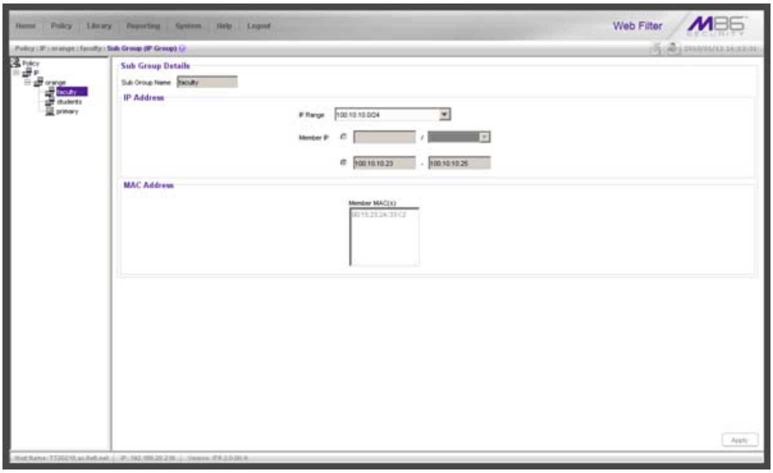
***TIPS**: Multiple MAC addresses can be moved to a list box by clicking each MAC address while pressing the Ctrl key on your keyboard, and then clicking the arrow key pointing to that list box.*

Blocks of MAC addresses can be moved to a list box by clicking the first MAC address, and then pressing the Shift key on your keyboard while clicking the last MAC address, and then clicking the arrow key pointing to that list box.

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

View Sub Group MAC Addresses

When using the mobile mode, the Sub Group (IP Group) window is used for viewing this sub-group's MAC addresses previously added in the sub-group's Members window.



Sub Group Details

Sub Group Name: faculty

IP Address

IP Range: 100.10.10.0/24

Member IP: ○ /

● 100.10.10.23 - 100.10.10.25

MAC Address

Member MAC(s): 00:15:23:2A:33:C2

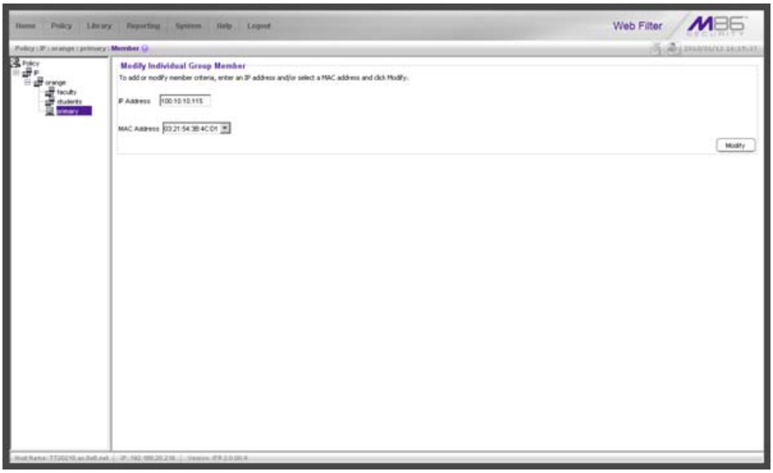
Fig. D-4 Sub Group (IP Group) window, view MAC Addresses

MAC addresses display in the Member MAC(s) list box in the MAC Address frame.

If the sub-group has been completely defined, IP address criteria was entered in the IP Address frame and saved in this window.

Add a MAC Address to an Individual Member

When using the mobile mode, the Individual IP's Member window is used for selecting the member's MAC address for inclusion in the sub-group.



Modify Individual Group Member

To add or modify member criteria, enter an IP address and/or select a MAC address and click Modify.

IP Address 100.10.10.115

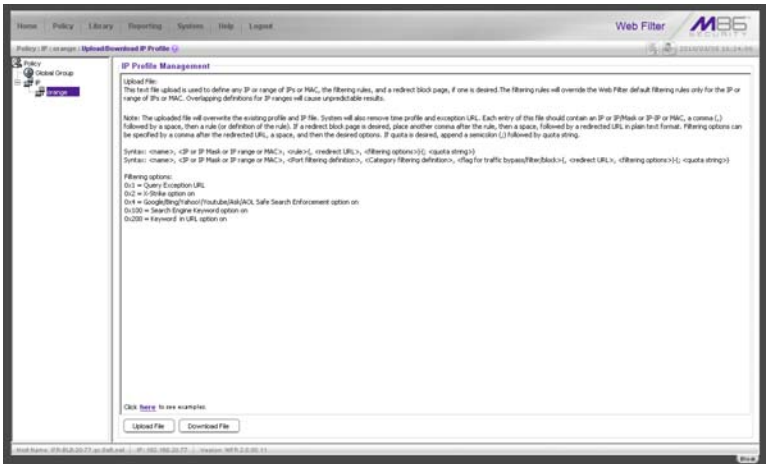
MAC Address 03:21:54:3B:4C:D1

Fig. D-5 Member window with MAC Address

1. In the Modify Individual Group Member frame, select the member's **MAC Address** from the pull-down menu.
2. Click **Modify** to apply your changes.

Upload MAC Address File for IP Group

A file containing multiple MAC addresses can be uploaded to the master IP group using the Upload/Download IP Profile window.



Upload File:
This text file upload is used to define any IP or range of IPs or MAC, the filtering rules, and a redirect block page, if one is desired. The filtering rules will override the Web Filter default filtering rules only for the IP or range of IPs or MAC. Overlapping definitions for IP ranges will cause unpredictable results.

Note: The uploaded file will overwrite the existing profile and IP file. System will also remove time profile and exception URL. Each entry of this file should contain an IP or IP/Mask or IP-IP or MAC, a comma (,) followed by a space, then a rule (or definition of the rule). If a redirect block page is desired, place another comma after the rule, then a space, followed by a redirected URL in plain text format. Filtering options can be specified by a comma after the redirected URL, a space, and then the desired options. If quota is desired, append a semicolon (;) followed by quota string.

Syntax: <name>, <IP or IP Mask or IP range or MAC>, <rule>[, <redirect URL>, <filtering options>][; <quota string>]
Syntax: <name>, <IP or IP Mask or IP range or MAC>, <Port filtering definition>, <Category filtering definition>, <flag for traffic bypass/filter/block>[, <redirect URL>, <filtering options>][; <quota string>]

Filtering options:
0x1 = Query Exception URL
0x2 = X-Strike option on
0x4 = Google/Bing/Yahoo!/Youtube/Ask/AOL Safe Search Enforcement option on
0x100 = Search Engine Keyword option on
0x200 = Keyword in URL option on

Click here to see examples.

Fig. D-6 Master IP group's Upload/Download IP Profile window

WARNING: *Any existing profiles will be overwritten by the contents of the uploaded file.*

If the end user has both an IP address and a MAC address, each profile should be entered on a separate line in the file.

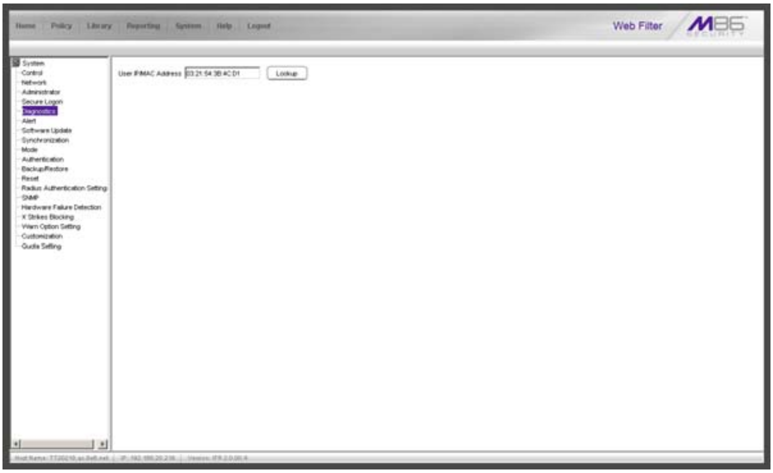
For example, if end user "tlind" has the IP address 150.100.30.2 and MAC address 00:04:21:AF:33:E1, the following entries for that user's profile would be made on two separate lines in the master IP group's profile file:

tlind,150.100.30.2,A,J CHAT R GPORN M I,1, ,0x103
tlind, 00:04:21:AF:33:E1,A,J CHAT R GPORN M I,1, ,0x103

NOTE: *For other examples of entries to include in the profile file, go to* ***http://www.m86security.com/software/8e6/hlp/ifr/files/2group_ipprofiles.html****.*

Troubleshoot MAC Addresses

When using the mobile mode, the Active Profile Lookup is used for verifying whether an entity has an active filtering profile for his/her MAC address. This window also is used for troubleshooting synchronization on "target" Web Filters, to verify whether settings for user profiles match the ones synced over from the "source" Web Filter.



User IP/MAC Address: 03:21:54:3B:4C:D1

Fig. D-7 Active Profile Lookup window with MAC Address

***NOTE**: See Active Profile Lookup window in Chapter 1: System screen from the WF Global Administrator Section for information on using the Active Profile Lookup window.*

Mobile Client Section

The Mobile Client Section of this user guide contains information on how the Windows network administrator uses the Mobile Client Deployment Kit to install the Mobile Client on a Windows or Macintosh network, configure the Mobile Client via the Package Editor, deploy the Mobile Client to Windows or Macintosh OS X end user workstations, and uninstall the Mobile Client.

The Mobile Client Deployment Kit is comprised of the following resources:

- Unconfigured packages containing the Mobile Client software (8e6client.msi for Windows, and 8e6clientInstaller.mpkg.tar for Macintosh OS X)

***NOTE**: The unconfigured 8e6clientInstaller.mpkg.tar package in this kit contains Mobile Client software for Macintosh OS X and should be used in a “Macintosh only” environment.*

- A tool for setting or modifying Mobile Client packages (the “package editor,” Mc_tool.exe)
- The optional Mobile Client Updater (MCU) component that updates Mobile Client binaries from your Mobile Server running M86 Web Filter software version 4.0 or higher, or from your own Web server (the “updater,” 8e6winmcu.msi for Windows, and 8e6osxmcu.pkg.tar for Macintosh OS X)
- An .msi package that can be assigned via Group Policy to workstations to remove a previously-installed Mobile Client package (the "remover," 8e6purge.msi)
- Online help instructions for configuring, deploying, and removing the Mobile Client.

Download and Install the Deployment Kit

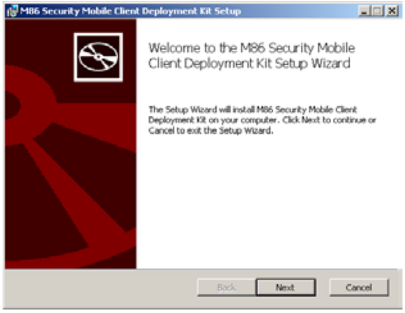
To download the Mobile Client Deployment Kit to your machine:

1. Launch the M86 Mobile Client Web page, and then find and click the link for the Mobile Client Deployment Kit Installer (.msi file) you wish to download to your machine.

***NOTES**: Please contact technical support if you need the link to the M86 Mobile Client Web page.*

***WARNING**: If a prior version of the Mobile Client is installed on your workstation (i.e. software version 1.x or 2.x), you must uninstall that software before installing software version 3.0. (See Mobile Client Removal from Computers for information about using 8e6purge.msi to uninstall the Mobile Client.)*

2. Once the .msi file is downloaded to your machine, click that file to launch the Mobile Client Deployment Kit Setup Wizard:

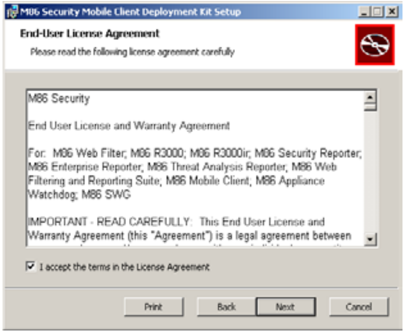


Welcome to the M86 Security Mobile Client Deployment Kit Setup Wizard

The Setup Wizard will install M86 Security Mobile Client Deployment Kit on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Fig. D-8 Mobile Deployment Kit Setup Wizard

3. Click **Next** to read the End User License Agreement and to accept its terms by clicking the checkbox corresponding to “I accept the terms in the License Agreement”:



M86 Security Mobile Client Deployment Kit Setup

End-User License Agreement

Please read the following license agreement carefully

M86 Security

End User License and Warranty Agreement

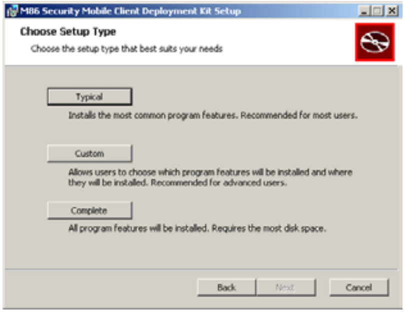
For: M86 Web Filter; M86 R3000; M86 R3000ir; M86 Security Reporter; M86 Enterprise Reporter; M86 Threat Analysis Reporter; M86 Web Filtering and Reporting Suite; M86 Mobile Client; M86 Appliance Watchdog; M86 SWG

IMPORTANT - READ CAREFULLY: This End User License and Warranty Agreement (this "Agreement") is a legal agreement between

☑ I accept the terms in the License Agreement

Fig. D-9 End User License Agreement

4. Click **Next** to go to the Choose Setup Type step, and select the setup option for installing the Mobile Client: “Typical”, “Custom”, “Complete”:



M86 Security Mobile Client Deployment Kit Setup

Choose Setup Type

Choose the setup type that best suits your needs

Typical

Installs the most common program features. Recommended for most users.

Custom

Allows users to choose which program features will be installed and where they will be installed. Recommended for advanced users.

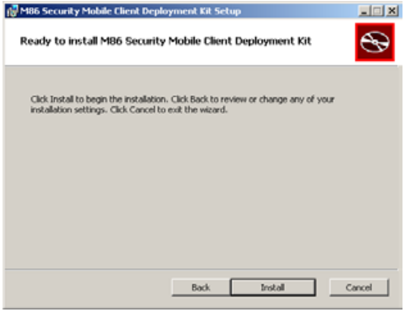
Complete

All program features will be installed. Requires the most disk space.

Fig. D-10 Choose Setup Type

5. Click **Next** to proceed with the option you selected for installing the application. If you chose the Custom option, you will need to specify where or how the main executable and support files will be installed on your machine, and/or where or how Windows and Macintosh packages for the Mobile Client will be installed for distribution to user workstations.

   When your machine is ready to install the Deployment Kit, the page that confirms the installation process is ready to begin displays:



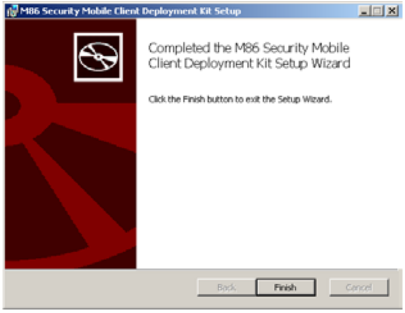
M86 Security Mobile Client Deployment Kit Setup

Ready to install M86 Security Mobile Client Deployment Kit

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Fig. D-11 Installation process ready to begin

6. Click **Install** to begin the installation process. The following page displays when the installation process is complete:



M86 Security Mobile Client Deployment Kit Setup

Completed the M86 Security Mobile Client Deployment Kit Setup Wizard

Click the Finish button to exit the Setup Wizard.

Fig. D-12 Installation complete

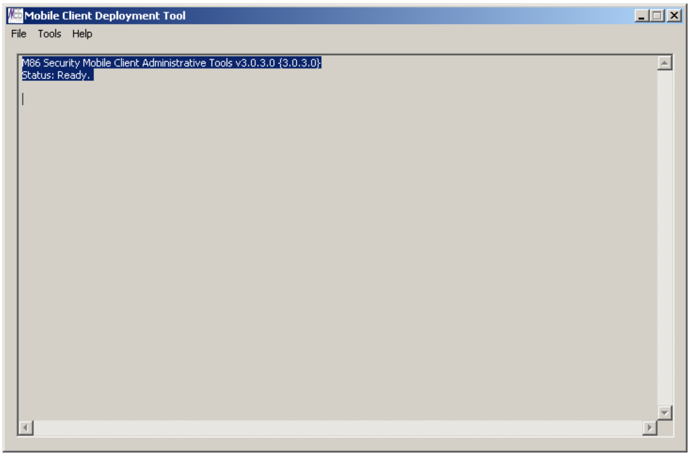
7. Click **Finish** to close the wizard dialog box.

Access the Mobile Client Deployment Tool window

Once the Mobile Client Deployment Kit is installed on your machine, the Mobile Client Deployment Tool window (see Fig. D-13) and Package Configuration window (see Fig. D-15) are used for configuring packages for Windows or Macintosh.

***NOTE**: Refer to the instructions in this section of the user guide or consult the help topics via the **Help** link in the Mobile Client Deployment Tool for instructions on using these windows.*

The Mobile Client Deployment Tool window is accessible via **Start > All Programs > M86 Security Mobile Client Deployment Kit > Package Editor**:



```
M86 Security Mobile Client Administrative Tools v3.0.3.0 {3.0.3.0}
Status: Ready.
```

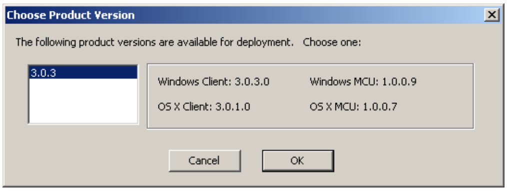
Fig. D-13 Mobile Client Deployment Tool window

The Mobile Client Deployment Tool's package editor log window displays the operations performed when creating and configuring packages.

***NOTES**: Before exiting the Mobile Client Deployment Tool and Package Configuration windows, be sure to save all entries you intend to save for packages you've configured. To exit the Mobile Client Deployment Tool window, with the Package Configuration window closed, go to **File > Exit**.*

Configure a New Package Set

1. In the Mobile Client Deployment Tool window, go to **File > New Package...** to open the Choose Product Version dialog box:



Choose Product Version

The following product versions are available for deployment. Choose one:

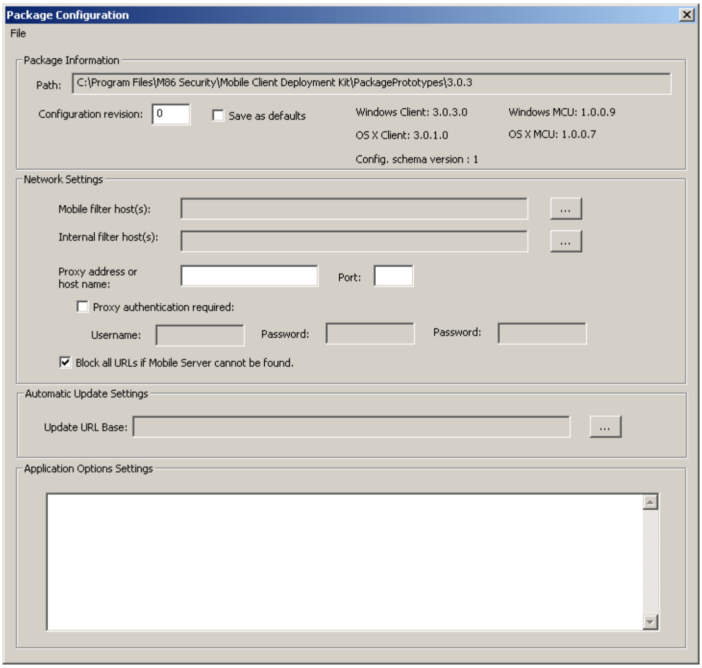
3.0.3

Windows Client: 3.0.3.0 Windows MCU: 1.0.0.9

OS X Client: 3.0.1.0 OS X MCU: 1.0.0.7

Fig. D-14 Choose Product Version dialog box

2. Select the Mobile Client software version from the available choices, and then click **OK** to close the Choose Product Version dialog box and to open the Package Configuration window:



Package Configuration

File

Package Information

Path: C:\Program Files\M86 Security\Mobile Client Deployment Kit\PackagePrototypes\3.0.3

Configuration revision: 0 □ Save as defaults

Windows Client: 3.0.3.0 Windows MCU: 1.0.0.9

OS X Client: 3.0.1.0 OS X MCU: 1.0.0.7

Config. schema version : 1

Network Settings

Mobile filter host(s):

Internal filter host(s):

Proxy address or host name: Port:

□ Proxy authentication required:

Username: Password: Password:

☑ Block all URLs if Mobile Server cannot be found.

Automatic Update Settings

Update URL Base:

Application Options Settings

Fig. D-15 Package Configuration window

The Package Configuration window is comprised of the following frames: Package Information, Network Settings, Automatic Update Settings, and Application Options Settings.

***NOTE**: To exit the Package Configuration window at any time before saving your edits, select **File > Cancel** from the menu.*

Specify Package criteria

The Package Information frame includes the following information: Path on the system where the current package is located, Configuration revision number, Configuration schema version number, and package version numbers.

The following fields are editable:

- **Configuration revision**: This number is automatically incremented by “1” each time changes made to the package configuration are saved. When deploying the Mobile Client to end user workstations, the installer uses this revision number to determine whether a newer configuration is already installed on the workstation.

***TIP**: To ensure updates to end user workstations are properly applied, if you are making configuration-only changes, it is better to edit the previous package rather than create a new one.*

- **Save as defaults**: By checking this box, your configuration will be saved in a central defaults file for use in the next “Save” command.

***TIP**: By enabling this feature, if creating a new package you can apply these saved default settings to the new package by choosing **File > Apply Defaults** from the menu.*

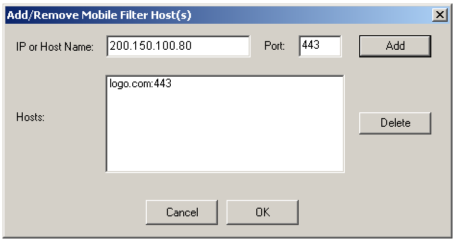
***NOTE**: To edit the default settings, from the Mobile Client Deployment Tool window select **Tools > Edit default configuration...** (see Edit a Package Configuration: Edit default configuration settings for information about making edits to default settings).*

Configure Network Settings

The Network Settings frame includes fields for entering IP addresses of host servers used for filtering mobile workstations and in-house workstations, and proxy server criteria—the latter, if a proxy server is used with filtering servers on your network.

Add, remove mobile filter host server

1. Click the ellipses (...) button to the right of the **Mobile filter host(s)** field to open the Add/Remove Mobile Filter Host(s) dialog box:



IP or Host Name: 200.150.100.80

Port: 443

Hosts: logo.com:443

Fig. D-16 Add/Remove Mobile Filter Host(s)

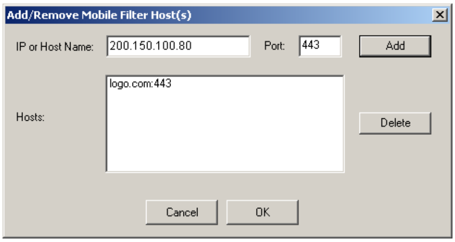
2. In the **IP or Host Name** field, enter the public IP address or hostname of your mobile filter host server.
3. By default, *443* displays in the **Port** field and should not be modified unless the mobile filter host server is on another port.
4. Click **Add** to include the entry in the list box below.
5. After entering host criteria for each mobile filter, click **OK** to close the dialog box and to display your entries in the Mobile filter host(s) field of the Package Configuration window.

***NOTE**: To remove a mobile filter from the list, select the entry from the Hosts list box, click **Delete**, and then click **OK**.*

Add, remove internal filter host server

***NOTE**: Entries made in this portion of the user interface are optional. If you have one filter host server on your network, the IP address would be the same IP address you entered for the mobile filter host server.*

1. Click the ellipses (...) button to the right of the **Internal filter host(s)** field to open the Add/Remove Internal Filter Host(s) dialog box:



Add/Remove Mobile Filter Host(s)

IP or Host Name: 200.150.100.80

Port: 443

Hosts: logo.com:443

Fig. D-17 Add/Remove Internal Filter Host(s)

2. In the **IP or Host Name** field, enter the public IP address or hostname of your internal filter host server.
3. By default, *81* displays in the **Port** field and should not be modified unless the internal filter host server is using a different port.
4. Click **Add** to include the entry in the list box below.
5. After entering host criteria for each internal filter, click **OK** to close the dialog box and to display your entries in the Internal filter host(s) field of the Package Configuration window.

***NOTE**: To remove an internal filter from the list, select the entry from the Hosts list box, click **Delete**, and then click **OK**.*

Add proxy address or host name

1. If your organization is using a proxy server on the network, in the **Proxy address or host name** field, enter the IP address or host name of your proxy server.
2. In the **Port** field, enter the port number for this proxy server.
3. If authentication is required for the Mobile Client to communicate with this proxy server, do the following:

   a. Click the “Proxy authentication required” checkbox; this action activates the Username and Password fields.

   b. Enter the proxy server **Username**.

   c. Enter the proxy server **Password** twice.

Optional: Block all URLs if Mobile Server cannot be found

The “Block all URLs if Mobile Server cannot be found.” checkbox is checked by default. This setting indicates that if the Mobile Client cannot detect the mobile filter host server, all URLs requested by the end user will be blocked.

Uncheck this box if the end user’s workstation should be permitted unrestricted Internet access when the mobile filter host server is unavailable.

⚠ ***WARNING****: By deselecting this option, technically savvy end users may be able to bypass filtering permanently by disrupting communications between the workstation and the mobile filter host server.*

Optional: Specify URL for Mobile Client Updates

NOTES*: A URL directory entry is required in the Automatic Update Settings frame only if the Mobile Client Updater will be installed on end user workstations and a Web server will be used for deploying updated Mobile Client package configuration updates to these workstations.*

You do not need to specify a URL directory entry if you wish to use the Web Filter (running software version 4.0 or higher) to deploy updates to end user workstations. However, please note that using the Web Filter to deploy updates could impact the performance of the server.

For more information about using a host server for the Mobile Client Updater, see MCU file preparations: Choose a deployment host for updates.

1. In the Automatic Update Settings frame, click the ellipses (...) button to the right of the **Update URL Base** field to open the Add/Remove Update URL(s) dialog box:

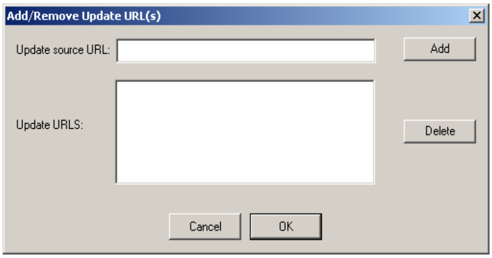


Fig. D-18 Add/Remove Update URL(s)

2. In the **Update source URL** field, enter the URL of the directory to be used for deploying Mobile Client package configuration updates to mobile workstations with the Mobile Client installed. The URL format should include the protocol (e.g. “http”), the port number (if a port other than port 80 is used), the host name, and directory name. For example: **http://www.mycompany.com/ mobile_client_updates**

NOTE*: Only the HTTP protocol is supported at this time.*

3. Click **Add** to include the entry in the list box below.
4. After entering the URL, click **OK** to close the dialog box and to display your entries in the Update URL Base field of the Package Configuration window.

***NOTE**: To remove a URL from the list, select the entry from the Update URLS list box, click **Delete**, and then click **OK**.*

Optional: Set up Application Options

***NOTE**: Entries in the Application Options Settings frame are only required if you need to modify the behavior of the Mobile Client in order to accommodate specific applications on your network.*

Both Windows and Macintosh OS X share a single set of Applications Options Settings. This is not a problem as long as you qualify the application(s) sufficiently to avoid any chance of ambiguity (e.g. “wget” is too short of a qualifier if you want to block it on Macintosh OS X but allow it on Windows).

Types of scenarios in which entries would be made in the Applications Options Settings frame for the Mobile Client include the following:

- Your organization uses a custom application which should never be filtered
- There are specific applications you would like to permanently and unconditionally block from accessing the Internet
- You wish to enable special log-verbosity settings for one or more applications—i.e. to troubleshoot possible conflicts between the Mobile Client and other network applications.

Step 1: First line entry

By default, the Application Options Settings field is empty. If you wish to add any options, you must first type in ***Mode 0*** on the first line. For example:

```
Mode 0
{option #1}
{option #2}
…
```

Step 2: Identify the name and path of the application

Determine the name and path of the executable program for which network access should be blocked or granted unrestricted network access. For example: Program Files\Mozilla Firefox\Firefox.exe

Step 3: Add an option line for the application

Enter an option line for each application to be blocked or bypassed.

To block an application, for example:

```
block_firefox  -c  “c:\Program Files\Mozilla Firefox\Firefox.exe” -k
```

To bypass an application, for example:

```
bypass_myapp  -c  “c:\Program Files\MyCorporation\MyCus-
    tomApp\MyApp.exe” -b
```

To enabling verbose logging for an application, for example:

```
logall_IE  -c  “c:\Program Files\Internet Explorer\iexplore.exe”
    -xt *,0 -xl *,0
```

Here’s an example of the entire set of entries to enable verbose logging for all applications, block Firefox for Windows, and grant unfiltered access to Myapp.exe:

```
Mode0
logall -c * -xl *,0 -xt *,0
block_firefox  -c  *\Program Files\Mozilla Firefox\Firefox.exe* -k
pass_myapp -c *\Program Files\MyCompany\MyApp\Myappl.exe* -b
```

***NOTES**: The first word of each option is an arbitrary “label”; you can use any name containing characters [a-z],[A-Z],[0-9], or an underscore (‘_’).*

The -c option specifies a partial command line match. You could, therefore, just specify “Firefox.exe” instead of listing the entire path. However, doing so could also make it easier for a sophisticated end user to exploit a bypass setting.

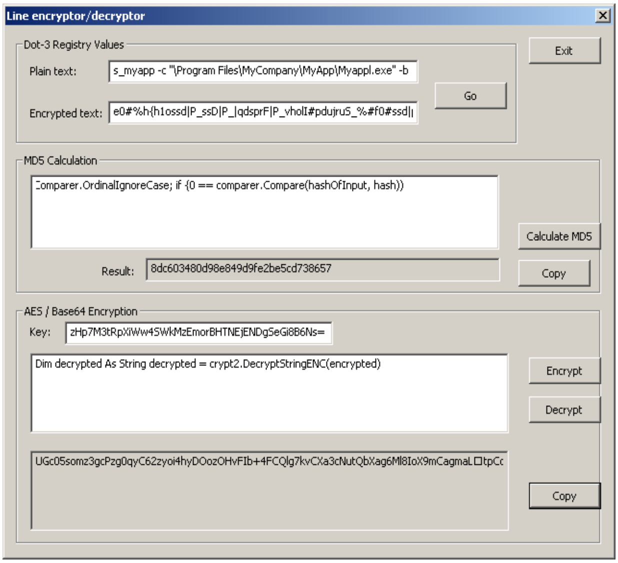
Line encryptor/decryptor...

Other types of application qualifying arguments exist in addition to the examples provided in the previous paragraphs of this user guide. It is also possible to encrypt the Application Options Settings if you wish to obfuscate them from your users.

***NOTE**: Contact M86 Technical Support for advanced information about Applications Options Settings.*

To encrypt or decrypt commands to be included in the Application Options Settings frame of the Package Configuration window:

1. From the Mobile Client Deployment Tool window, go to **Tools > Line encryptor/decryptor...** to open the **Line encryptor/decryptor** window:



Plain text: s_myapp -c "\Program Files\MyCompany\MyApp\Myappl.exe" -b

Encrypted text: e0#%h{h1ossd|P_ssD|P_|qdsprF|P_vholI#pdujruS_%#f0#ssd||

```
Comparer.OrdinalIgnoreCase; if (0 == comparer.Compare(hashOfInput, hash))
```

Result: 8dc603480d98e849d9fe2be5cd738657

Key: zHp7M3tRpXiWw4SWkMzEmorBHTNEjENDgSeGi8B6Ns=

```
Dim decrypted As String decrypted = crypt2.DecryptStringENC(encrypted)
```

UGc05somz3gcPzg0qyC62zyoi4hyDOozOHvFIb+4FCQlg7kvCXa3cNutQbXag6Ml8IoX9mCagmaL□tpCc

Fig. D-19 Line encryptor/decryptor window

The following frames are included in this window:

- Dot-3 Registry Values - use the tools in this frame to modify .3 registry entries.

- MD5 Calculation - use the tools in this frame to generate an MD5 “digital thumbprint” for a file.
- AES / Base64 Encryption - use the tools in this frame to generate Advanced Encryption Standard (AES) base64 encryption:

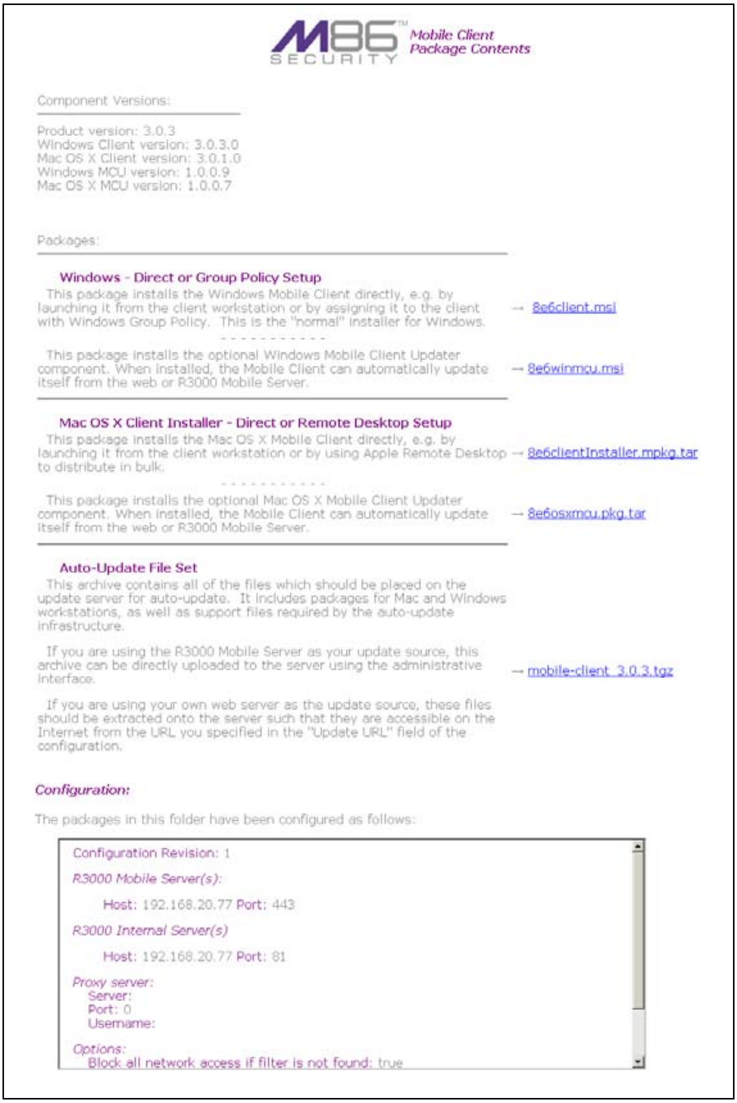
2. Click **Exit** to close this window.

Save configuration settings, download files

In the Package Configuration window, the following options are available from the File menu for saving the package configuration:

- **Save** - Saves the current package
- **Save as...** - Launches the Save Package window in which you specify the **Package Name**, click **OK** and then **Yes** in a dialog box to close both the box and window
- **Save and Quit** - Saves your edits and closes the Package Configuration window

When the package is saved the Configuration revision number in the Package Configuration window is automatically incremented to the next sequential number, and the Mobile Client Package Contents local Web page launches, providing a summary of package contents with links to various components generated in the package:



Mobile Client Package Contents

Component Versions:

Product version: 3.0.3
Windows Client version: 3.0.3.0
Mac OS X Client version: 3.0.1.0
Windows MCU version: 1.0.0.9
Mac OS X MCU version: 1.0.0.7

Packages:

Windows - Direct or Group Policy Setup

This package installs the Windows Mobile Client directly, e.g. by launching it from the client workstation or by assigning it to the client with Windows Group Policy. This is the "normal" installer for Windows. → 8e6client.msi

This package installs the optional Windows Mobile Client Updater component. When installed, the Mobile Client can automatically update itself from the web or R3000 Mobile Server. → 8e6winmcu.msi

Mac OS X Client Installer - Direct or Remote Desktop Setup

This package installs the Mac OS X Mobile Client directly, e.g. by launching it from the client workstation or by using Apple Remote Desktop to distribute in bulk. → 8e6clientInstaller.mpkg.tar

This package installs the optional Mac OS X Mobile Client Updater component. When installed, the Mobile Client can automatically update itself from the web or R3000 Mobile Server. → 8e6osxmcu.pkg.tar

Auto-Update File Set

This archive contains all of the files which should be placed on the update server for auto-update. It includes packages for Mac and Windows workstations, as well as support files required by the auto-update infrastructure.

If you are using the R3000 Mobile Server as your update source, this archive can be directly uploaded to the server using the administrative interface. → mobile-client_3.0.3.tgz

If you are using your own web server as the update source, these files should be extracted onto the server such that they are accessible on the Internet from the URL you specified in the "Update URL" field of the configuration.

Configuration:

The packages in this folder have been configured as follows:

Configuration Revision: 1

R3000 Mobile Server(s):

Host: 192.168.20.77 Port: 443

R3000 Internal Server(s)

Host: 192.168.20.77 Port: 81

Proxy server:
Server:
Port: 0
Username:

Options:
Block all network access if filter is not found: true

Fig. D-20 Mobile Client Package Contents page

The Mobile Client Package Contents page includes the following information:

- **Component Versions** - The Mobile Client Windows and Macintosh version numbers and MCU version numbers
- **Packages** - Links to downloadable components for:
  - Windows - Direct or Group Policy Setup links for downloading the following components:
    - 8e6client.msi - download the Mobile Client application installer file for installation on Windows end user workstations
    - 8e6winmcu.msi - if using the optional Mobile Client Updater feature, download the MCU installer file for installation on Windows end user workstations
  - Mac OS X Client Installer - Direct or Remote Desktop Setup links for accessing the following components:
    - 8e6clientInstaller.mpkg.tar - download the compressed Mobile Client application installer package file and uncompress for installation on Macintosh end user workstations
    - 8e6osxmcu.pkg.tar - if using the optional Mobile Client Updater feature, download the compressed MCU installer package file and uncompress for installation on Macintosh end user workstations
  - Auto-Update File Set - if using the optional MCU feature on a Web Filter running software version 4.0 or higher, download the mobile-client_{version}.tgz compressed set of Mobile Client files, uncompress and extract files to the designated update server

***NOTE**: More information about these tools is provided in subsequent pages in this section of the user guide.*

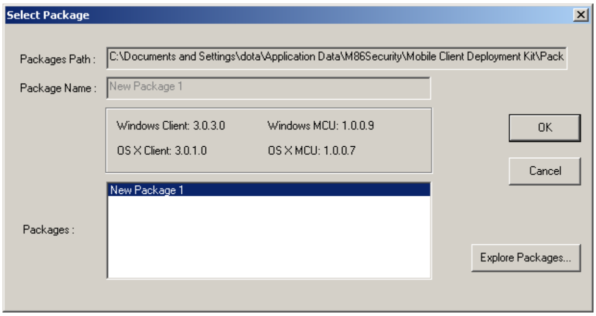
- **Configuration** - Mobile Client and server settings:
  - Configuration Revision number
  - Mobile Server Host IP address(es) and Port number(s)
  - Internal Server Host IP address(es) and Port number(s)
  - Proxy server - Server host name or IP address, Port number, and Username if a proxy server was specified
  - Options - Block all network access if filter is not found: true or false, and Update URL if using the Mobile Client Updater and a Web server was specified
  - AppOptions - Application Options Settings entries, if any were made and saved

When you are finished reviewing the contents of the Mobile Client Package Contents page, click the “X’ in the upper right corner to close the page.

NOTE*: If you need to find the Mobile Client Package Contents page after you close it, from the Mobile Client Deployment Tool window, go to* ***File > Explore Packages...*** *and then locate “Packages-View.html” inside the directory for the corresponding package.*

Edit a Package Configuration

1. From the Mobile Client Deployment Tool window, select **File > Edit Package...** to open the Select Package window:


Select Package

Packages Path : C:\Documents and Settings\dota\Application Data\M86Security\Mobile Client Deployment Kit\Pack

Package Name : New Package 1

Windows Client: 3.0.3.0 Windows MCU: 1.0.0.9

OS X Client: 3.0.1.0 OS X MCU: 1.0.0.7

Packages : New Package 1

Fig. D-21 Select Package window

2. From the Packages list box, choose the package to be edited; this action populates the Packages Path and Package Name fields with pertinent criteria about the package. The Mobile Client Windows and Macintosh version numbers and MCU version numbers also display.

TIP: *Click **Explore Packages...** to open the Mobile Client Deployment Kit's Packages folder and choose the package to be edited from the available selections.*

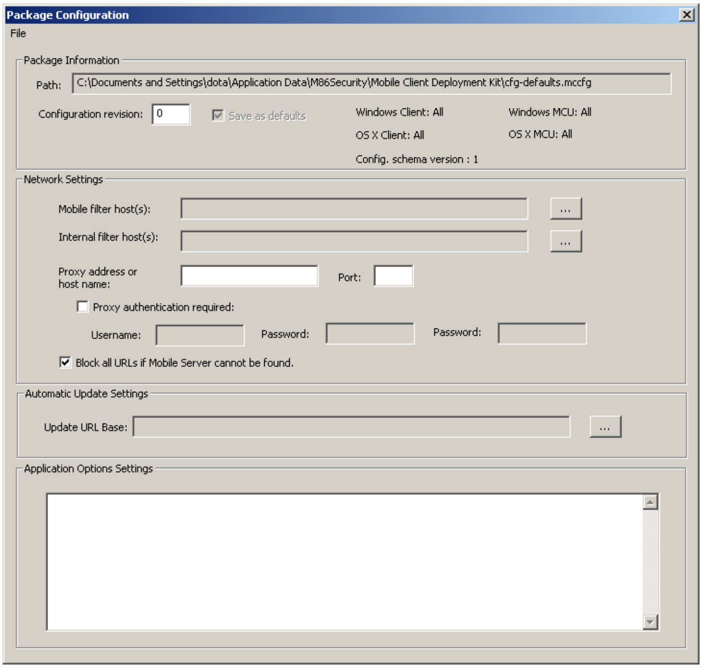
3. Click **OK** to close the Select Package window and to launch the Package Configuration window displaying the last saved edits made for the package.

NOTE: *The "Configuration revision" is incremented to the next sequential revision number.*

4. After making your edits, choose a Save option for saving the configuration package.

Edit default configuration settings

1. From the Mobile Client Deployment Tool window, select **Tools > Edit default configuration...** to open the Package Configuration window for default settings:



Path: C:\Documents and Settings\dota\Application Data\M86Security\Mobile Client Deployment Kit\cfg-defaults.mccfg

Configuration revision: 0

☑ Save as defaults

Windows Client: All

Windows MCU: All

OS X Client: All

OS X MCU: All

Config. schema version : 1

Mobile filter host(s):

Internal filter host(s):

Proxy address or host name:

Port:

☐ Proxy authentication required:

Username:

Password:

Password:

☑ Block all URLs if Mobile Server cannot be found.

Update URL Base:

Fig. D-22 Package Configuration window for default settings

This window is similiar in appearance to the Package Configuration window used for adding a new package or editing an existing package, except the Package Information frame includes the following differences:

- a different Path is used with the filename “cfg-defaults.mccfg” specified
- “Save as defaults” is greyed-out
- Mobile Client and MCU components for Windows and Macintosh OS X show "All" instead of software version numbers.

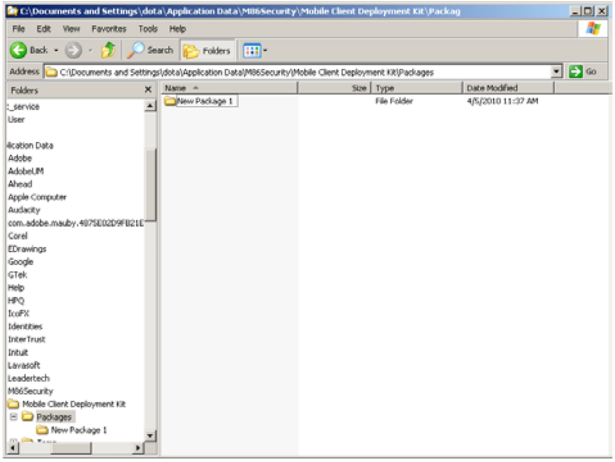
__TIP__: Select __File > Cancel__ to exit without saving your edits.

2. Make your edits in this window and then select from the following options to save the default configuration: **File > Save** or **File > Save and Quit**.

__NOTE__: See Save configuration settings, download files in Configure a New Package Set for information about these Save options.

View Package Configuration contents

1. From the Mobile Client Deployment Tool, select **File > Explore Packages...** to open the Packages window:



Address: C:\Documents and Settings\dota\Application Data\M86Security\Mobile Client Deployment Kit\Packages

Name	Size	Type	Date Modified
New Package 1		File Folder	4/5/2010 11:37 AM

Fig. D-23 Packages window

__TIP__: The Packages window is also accessible from the Select Package window (see Fig. D-21) by clicking the __Explore Packages...__ button.

2. Double-click the selected package to display its contents.

3. When you are finished, click the “X” in the upper right corner of the window to close it.

MCU file preparations

In order to use the optional Mobile Client Updater (MCU) component to distribute product or configuration updates to end users, you must first install the MCU on end user workstations. Then you must select the host server to deploy updates to end user workstations.

Step 1: Install MCU on end user workstations

1. Access the appropriate MCU installer (8e6winmcu.msi for Windows and 8e6osxmcu.pkg.tar for Macintosh OS X) and copy it to respective user workstations.

TIP*: You might want to copy the installers to a master CD-ROM to simplify the installation process.*

2. Install the installer as you would any other program. No configuration is required for the MCU component.

NOTE*: This is a one time operation; after this procedure the MCU will update itself when a new version is deployed.*

Step 2: Choose a deployment host for updates

Decide where to host Mobile Client update files:

- A Web server you maintain
- Mobile Server Web Filter

Host MC file on your Web server

This choice is advantageous for environments with multiple Mobile Server appliances, since update files need to be copied to only one server instead of each Web Filter appliance.

***NOTES**: If you choose to host update packages on your own Web server:*

- *The Web server's URL must be specified in the Package Configuration window. If this URL changes at any point in time, before using the "new" server, you must first update the "old" server with the package containing the "new" URL, so that clients know where to get current updates. Thereafter, any newer packages should be uploaded to the "new" server.*
- *The MIME types map may need to be modified in order to support custom file extensions for .mcxml (text/xml) and .mccfg (text/xml).*

Host MC files on the Mobile Server (Web Filter)

This choice is convenient for hosting Mobile Client updates since this Web Filter is already accessible by the Mobile Client application. However, performance issues may arise when a new version of the Mobile Client is available and is being requested by multiple end user workstations simultaneously.

The MCU checks for Mobile Client updates after each successful synchronization attempt. By default, synchronization attempts occur once per hour (unless you have modified the Mobile Server configuration to specify otherwise). When a new Mobile Client version is detected, the MCU immediately attempts to download it. Because the clients do not coordinate their synchronization attempts with each other, the timing of download attempts will follow a random statistical distribution. Nevertheless, it is conceivable that if you have 4,000 client workstations, they might all attempt to download the update within the first hour after it is posted, although the starting times of each download will vary.

NOTE*: A full Mobile Client update file size is about 1.5 MB for Windows and 1.4 MB for Macintosh OS X (as of software version 3.0.5).*

Step 3: Post the latest files for MCU

Next you must post the Mobile Client configuration files to the host server. After this initial posting, whenever changes are made to the client configuration, or whenever a new software version of the Mobile Client becomes available, you need to post the updated files to this designated host server.

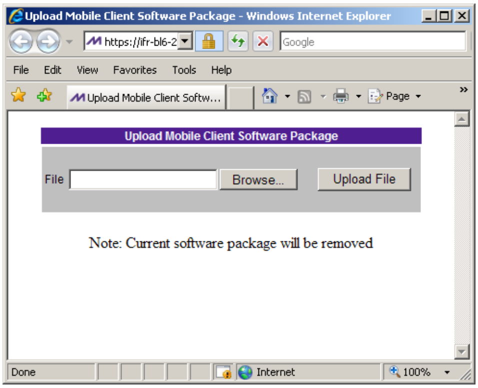
Post MC configuration files to a Web server

If you are using your own Web server as an update host, extract the .tgz file into the host directory associated with the Update URL Base field entry made in the Package Configuration window for that package.

Post MC configuration files to the Mobile Server

If you are using the Mobile Server (Web Filter) as an update host:

1. With the Web Filter user interface launched, go to **System > Mode > Operation Mode** (see Fig. D1).
2. In the Mobile Client Control frame, at the Mobile Client Software Update field click **Upload** to open the Upload Mobile Client Software Package pop-up window:


Upload Mobile Client Software Package - Windows Internet Explorer
https://ifr-bl6-2
Google
File
Edit
View
Favorites
Tools
Help
Upload Mobile Client Softw...
Page
Upload Mobile Client Software Package
File
Browse...
Upload File
Done
Internet
100%

Note: Current software package will be removed

Fig. D-24 Upload Mobile Client Software Package window

3. Click **Browse...** to open the File Upload window and search for the .tgz file to be uploaded to the server.

***WARNING**: Uploading subsequent packages of the Mobile Client to the server will overwrite the current file configuration.*

4. Once you have found the file, click **Upload File** to upload the file to the server. After the file has been uploaded a confirmation message displays.
5. Click the “X” in the upper right window of the message window to close it.

How MCU updates clients

The server will unpack the files into the default update location so that clients can find the update as expected. The default location is **http://{mobile_server_address}:81/ mobile_client_updates**. To verify that your update files have been posted, go to the file **latest-manifest.mcxml** in this directory. Clients read this file to determine if applicable updates are available.

When the MCU reads available update information, it gives priority to new versions of the software. If a new version of the Mobile Client is available, it is downloaded and installed. Since the updated package contains an embedded copy of the latest configuration, this is adequate to ensure both the software and the configuration are updated. However, if the MCU finds no new software available, it checks to see if a new configuration is available. If the latter is available, that is downloaded and applied. Such updates are much smaller in size than updating an entire new version of the Mobile Client.

MC Deployment to Windows Computers

Deployment to a group

The modified 8e6client.msi file is distributed to multiple Windows workstations by creating a Group Policy Object (GPO) which assigns this software to the required computers on the network.

***NOTE**: The procedure suggested below presumes that you are using the free add-on Group Policy Management Console (GPMC) provided by Microsoft.*

1. Make the distribution .msi file available to the target workstations on a network share (e.g. \\{server-name}\8e6MobileClient\8e6client.msi) .

2. Create a new Group Policy Object (GPO):

   a. in the GPMC, select **Group Policy Management > Forest > Domains > {domain name} > Group Policy Objects**.

   b. Right-click and choose "New", then create a name for the policy (suggested name: "M86 Mobile Client Deployment"). Click **OK**.

   c. In the Group Policy Object Editor, open the **{policy name} > Computer Configuration > Software Settings > Software installation node**.

   d. Click the right panel and choose **New > Package**. Navigate to the distribution .msi file you shared in step 1, and then click “Open”. When prompted, select "Assigned" for the deployment method. Click **OK**.

   e. Right-click the new package and choose **Properties > Deployment**, and then check the "Uninstall this application when it falls out of the scope of management" box. Click **OK**.

   f. Close the Group Policy Object Editor.

3. Link the new policy:

   a. In the GPMC, select the domain or organizational unit for which the policy should be applied.

   b. Right-click, choose "Link an existing GPO", and then select the new policy you created in step 2. Click **OK**.

   c. Right-click the new policy in the tree, and then de-select the "Link Enabled" menu checkmark. (The link will be re-enabled later in this procedure.)

4. Create a filter for the policy:

   A GPO filter limits the scope of the policy so that the Mobile Client is only installed on the appropriate computers. For example, you may want to install it on all workstations but not servers. There are two types of filters: Security filters and WMI filters.

   To create a Security filter:

   a. Select the new policy link. Note the "Security Filtering" section in the Scope panel to the right.

   b. Click "Authenticated Users" and then "Remove".

   c. Click "Add...", and then click "Object Types". Check the "Computers" type and uncheck the "Users" type. Click **OK**.

   d. Enter the names of all the computers to receive the Mobile Client installation, separated by semicolons. (Alternatively, you can select a User or Computer group created previously—details of group creation are beyond the scope of this procedure. Click **OK**.

   To create a WMI filter:

   WMI filters are capable of applying very sophisticated selection criteria to set the scope of a policy. See Microsoft Knowledgebase article #555253 for details on creating WMI filters: ***http://support.microsoft.com/kb/555253***

5. Enable the policy link:

   Return to the new policy link in the GPMC for the target domain or Organizational Unit, right-click, and then choose "Link Enabled".

6. Test the deployment:

   a. Select one of the workstations within the scope of the policy and refresh its policies by running gpupdate.exe.

NOTE*: By default, Windows periodically refreshes the group policy automatically. Using gpupdate allows you to force an immediate refresh for test purposes—this is not something all users on the network should be required to do.*

   b. Reboot the workstation and log in.

NOTE*: In some cases involving Windows XP workstations, it may be necessary to reboot twice for Group Policy processing to occur.*

   c. Verify the Mobile Client is blocking access to unauthorized Web sites, and is allowing access to other sites.

Installation on a single computer

The Mobile Client is manually installed on a single Windows workstation by following these procedures:

1. Go to the folder in which the modified 8e6client.msi file was downloaded, and click the .msi file icon to launch the automatic installation process on the current workstation:

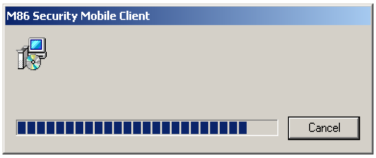
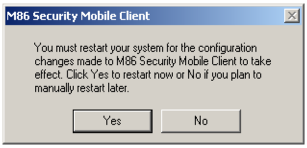


Fig. D-25 Begin Mobile Client installation

After the application has been installed, a dialog box opens asking if you wish to complete the installation process now or later:



You must restart your system for the configuration changes made to M86 Security Mobile Client to take effect. Click Yes to restart now or No if you plan to manually restart later.

Fig. D-26 Finish installation process

2. To complete the installation process now, save any applications—if necessary, and then click **Yes** to shut down and restart the computer. Or, click **No** to complete the installation process later.

MC Deployment to Macintosh OS X Computers

Apple Computer provides a product called Apple Remote Desktop (http://www.apple.com/remotedesktop/) that can be used to deploy Macintosh OS X Mobile Client software version in bulk to many users simultaneously. Contact Apple for additional information about this product.

Mobile Client Removal from Computers

Uninstallation from a Windows group

If the Group Policy that was used for installing the Mobile Client on workstations is removed, the Mobile Client will still remain installed on target workstations. In order to use the Group Policy framework to uninstall the Mobile Client, the Mobile Client Remover (8e6purge.msi) must be deployed using the Group Policy, just as the installer was deployed. Follow the instructions for deploying the Mobile Client, but substitute 8e6purge.msi as the package to be deployed. When the Remover is deployed on the workstation, the Mobile Client will be uninstalled from end users' machines.

NOTE*: The Remover does not require configuration prior to distribution.*

You will probably want to change the name of the policy (e.g. "Remove M86 Mobile Client"). Once the new policy has been processed on all target machines and the Mobile Client has been removed, you can delete or unlink the removal policy with GPMC.

Uninstallation from an individual computer

The Mobile Client can be removed from individual Windows or Macintosh OS X workstations.

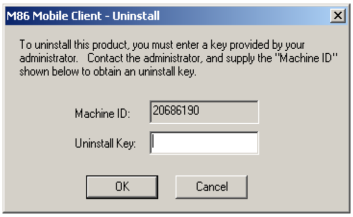
To remove the Mobile Client from a Windows computer, follow these procedures:

1. On the Windows workstation that needs to have the Mobile Client removed, go to the taskbar and do the following, based on the type of Windows operating system:

   - Windows Vista / Windows 7: **Start icon > Control Panel > Programs > Programs and Features > {program} > Uninstall**

- Windows XP: **Start > Control Panel > Add or Remove Programs**

2. Find the Mobile Client program and click **Remove** to open the M86 Mobile Client - Uninstall dialog box:



M86 Mobile Client - Uninstall

To uninstall this product, you must enter a key provided by your administrator. Contact the administrator, and supply the "Machine ID" shown below to obtain an uninstall key.

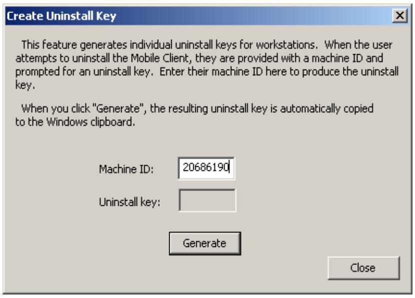
Machine ID: 20686190

Uninstall Key:

Fig. D-27 Mobile Client Uninstall dialog box

3. Copy the eight-digit number displayed in the **Machine ID** field. In this example: *20686190*

4. Access the Mobile Client Deployment Tool window, and go to **Tools > Create uninstall key...** to open the Create Uninstall Key pop-up window:



Create Uninstall Key

This feature generates individual uninstall keys for workstations. When the user attempts to uninstall the Mobile Client, they are provided with a machine ID and prompted for an uninstall key. Enter their machine ID here to produce the uninstall key.

When you click "Generate", the resulting uninstall key is automatically copied to the Windows clipboard.

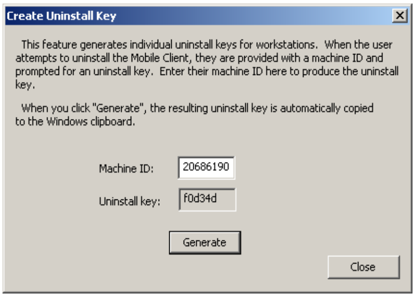
Machine ID: 20686190

Uninstall key:

Fig. D-28 Create Uninstall Key pop-up window

In the **Machine ID** field, enter or paste the eight-digit ID number from the Uninstall dialog box. In this example: *20686190*

5. Click **Generate** to display the generated six-character Uninstall key:



Create Uninstall Key

This feature generates individual uninstall keys for workstations. When the user attempts to uninstall the Mobile Client, they are provided with a machine ID and prompted for an uninstall key. Enter their machine ID here to produce the uninstall key.

When you click "Generate", the resulting uninstall key is automatically copied to the Windows clipboard.

Machine ID: 20686190

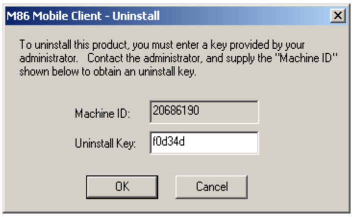
Uninstall key: f0d34d

Fig. D-29 Generate a key

Copy this Uninstall key. In this example: *f0d34d*

***NOTE**: Click **Close** to close the Create Uninstall Key pop-up window.*

6. Access the M86 Mobile Client - Uninstall dialog box again, and enter the generated password key in the **Key** field. In this example: *f0d34d*



M86 Mobile Client - Uninstall

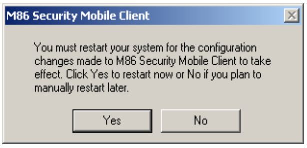
To uninstall this product, you must enter a key provided by your administrator. Contact the administrator, and supply the "Machine ID" shown below to obtain an uninstall key.

Machine ID: 20686190

Uninstall Key: f0d34d

Fig. D-30 Uninstall the Mobile Client

7. Click **OK** to begin the uninstallation process. When the Mobile Client has been uninstalled, a message displays asking you to restart the machine:



M86 Security Mobile Client

You must restart your system for the configuration changes made to M86 Security Mobile Client to take effect. Click Yes to restart now or No if you plan to manually restart later.

Fig. D-31 Restart message

8. Click **Yes** to restart the machine now, or **No** to restart the machine later.

Appendix E

Glossary

This glossary includes definitions for terminology used in this user guide.

always allowed - A filter category or port given this designation in a profile will be included in the white list. However, this setting in a library category is overridden if the minimum filtering level is set up to block that category.

Approved Content - A feature that lets users view only the videos posted to YouTube or SchoolTube that are approved for their profile. This feature requires the setup and maintenance of a Web portal, and/or access to VuSafe's portal.

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 - A unique library category that is created by an administrator, and can include URLs, URL keywords, and search engine keywords to be blocked. Group administrators create and manage 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, warn, or always allow settings) to determine whether users should be denied or allowed access to that port.

firewall mode - A Web Filter set up in the firewall mode will filter all requests. If the request is appropriate, the original packet will pass unchanged. If the request is inappropriate, the original packet will be blocked from being routed through.

global administrator - An authorized administrator of the network who maintains all aspects of the Web Filter, except for managing master IP groups and their members, and their associated filtering profiles. The global administrator configures the Web Filter, 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.

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 Web Filter, groups and/or individual client machines can be set up to block the use of IM services specified in the library category.

invisible mode - A Web Filter set up in the invisible mode 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.

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 Web Filter. Lightweight Directory Access Protocol

(LDAP) is a directory service protocol based on entries (Distinguished Names).

M86 supplied category - A library category that was created by M86, and includes a list of URLs, URL keywords, and search engine keywords to be blocked.

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 Policy 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. If the minimum filtering level is set up to block a library category, this setting will override an always allowed setting for that category in a user's profile. Minimum filtering level settings can be overridden by profile settings made in override accounts, exception URL settings, and use of the "bypass all" Rule setting.

mobile mode - The operations mode used on a Web Filter configured for filtering end users on machines located outside of the in-house network.

name resolution - A process that occurs when the Web Filter 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. An override account will bypass settings made in the minimum filtering level.

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 Web Filter, 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

Radius - This feature is used for controlling the filtering levels of dial-up users. The Radius accounting server determines which accounts will be filtered and how they will be filtered. The user profile in the Radius accounting server holds the filter definition for the user.

Real Time Probe - On the Web Filter, 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.

router mode - A Web Filter set up in the router mode will act as an Ethernet router, filtering IP packets as they pass from one card to another. While all original packets from client PCs are allowed to pass, if the Web Filter determines that a request is inappropriate, a block page is returned to the client to replace the actual requested Web page or service.

rule - A filtering component comprised of library categories set up to be blocked, opened, always allowed, or set up with a warning and/or a time quota. 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 Web Filter, a Simple Network Management Protocol is a third party product used for monitoring and managing the working status of the Web Filter's filtering on a network.

sub-group - An entity of a master IP group with an associated member IP address, and filtering profile.

synchronization - A process by which two or more machines run in parallel to each other. User filtering profiles and library configurations can be set up to be synchronized between multiple Web Filters. The clock on the Web Filter can be set up to be synchronized with a server on the Internet running Network Time Protocol (NTP) software.

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

Traveler - M86's executable program that downloads updates to your Web Filter 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 "m86security.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.

SR INTRODUCTORY SECTION

Security Reporter Overview

M86's Security Reporter (SR) application is comprised of the System Configuration administrator console and Report Manager.

Using System Configuration screens, the global administrator configures the SR to accept log files from the M86 Web Filter—and the M86 Secure Web Gateway, if this filtering device is added to the device registry—"normalize" the transferred data, and insert them into a MySQL database the Report Manager accesses to provide snapshots of end user Internet and/or network activity.

Using the Report Manager, the global administrator sets up group administrator accounts and grants these users access to designated sections in the Report Manager and System Configuration console, as applicable.

Administrators consult Report Manager dashboards for a high level picture of real time network Internet traffic, and then drill down into the URL categories or bandwidth gauges to quickly identify the source of user-generated Web threats. For further investigation of end user Internet usage, administrators generate productivity report views and interrogate massive datasets until the desired view is obtained. This "view" can be memorized and saved to a user-defined report menu for repetitive, scheduled execution and distribution.

If using an M86 Secure Web Gateway (SWG) appliance with the WFR, security reports show potentially harmful end user Internet/network activity that was halted by the SWG.

The SR targets threats to your network, thus arming you with the capability to take immediate action for terminating the source and securing your network.

About this Portion of the User Guide

The Security Reporter portion of the user guide primarily addresses the administrator designated to configure and manage the Security Reporter on the network. This administrator is referred to as the “global administrator” throughout this portion of the 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.

This portion of the user guide is organized into the following sections:

- **SR Introductory Section** - This section introduces the SR product, explains how to access and use the SR and this user guide, and provides information on how to contact M86 Security technical support.
- **SR System Configuration Section** - This section pertains to information on configuring and maintaining the SR administration module.
- **SR Report Manager Administration Section** - This section pertains to configuring and maintaining the administration side of the SR’s Report Manager application.
- **SR Productivity Reports Section** - Refer to this section for productivity reporting information.
- **SR Real Time Reports Section** - Refer to this section for real time report configuration and usage.
- **SR Security Reports Section** - Refer to this section for security report configuration and usage, if using a Secure Web Gateway appliance with the SR application in this WFR.

NOTE*: See the M86 Secure Web Gateway User Guide at* ***http://www.m86security.com/support/Secure-Web-Gateway/Documentation.asp*** *for information on the SWG.*

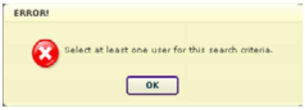
- **SR Appendices Section -** Appendix A of this section explains how to use the SR in the evaluation mode, and how to switch to the registered mode. Appendix B provides details on setting up and using the System Tray feature for real time gauge alerts. Appendix C features a glossary of technical terminology used in this portion of the user guide.

Terminology

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

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

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



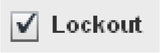
ERROR!

Select at least one user for this search criteria.

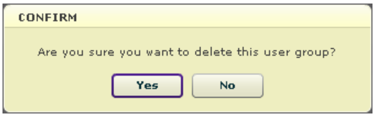
- **arrow** - a triangular-shaped object or button that displays in a window or on a screen. When displayed as a non-stationary object, the arrow points to the item that was selected in a list. When displayed as a button, the arrow is static. By clicking on this button, depending on the direction of the arrow, the previous item or the next item in a list displays or is selected.

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

- **checkbox** - a small square in a dialog box, window, or panel used for 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.

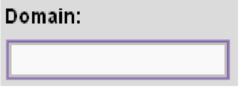

☑ Lockout

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

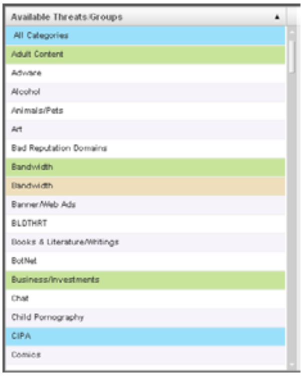

CONFIRM

Are you sure you want to delete this user group?

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


Domain:

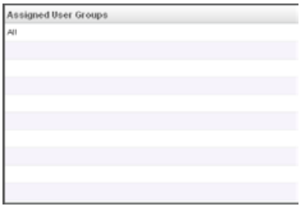
- **frame** - a boxed-in area in a dialog box, window, or panel that includes a group of objects such as fields, text boxes, list boxes, buttons, radio buttons, checkboxes, accordions, tables, tabs, and/or tables. Objects within a frame belong to a specific function or group. A frame often is labeled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


Available Threats/Groups

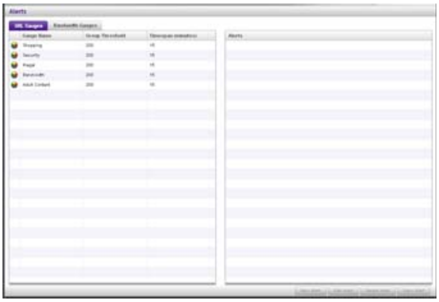
All Categories
Adult Content
Adware
Alcohol
Animals/Pets
Art
Bad Reputation Domains
Bandwidth
Bandwidth
Banner/Web Ads
BLDTHRT
Books & Literature/Writings
BotNet
Business/Investments
Chat
Child Pornography
CIPA
Comics

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

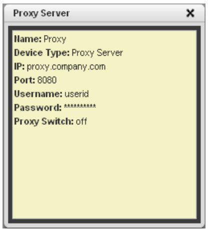
- **list box** - an area in a dialog box, window, or panel that accommodates and/or displays entries of items that can be added or removed.



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

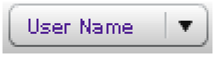


- **pop-up box** or **pop-up window** - a box or window that opens after you click a button in a dialog box, window, or panel. This box or window may display information, or may require you to make one or more entries. Unlike a dialog box, you do not need to choose between options.

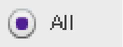

Proxy Server ✕

Name: Proxy
Device Type: Proxy Server
IP: proxy.company.com
Port: 8080
Username: userid
Password: *********
Proxy Switch: off

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

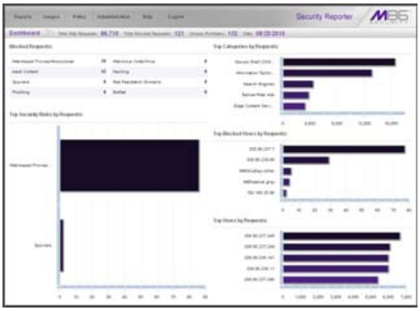


- **radio button** - a small, circular object in a dialog box, window, or screen used for selecting an option. This object allows you to toggle between two choices. By clicking a radio button, a dot is placed in the circle, indicating that you selected the option. When the circle is empty, the option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

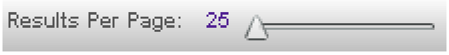


- **re-size button** - positioned between two frames, this button enlarges a frame or makes the frame narrower when clicked and dragged in a specific direction.

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

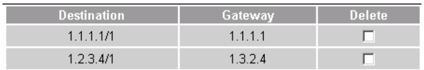


- **slider** - a small, triangular-shaped object—positioned on a line—that when clicked and dragged to the left or right decreases or increases the number of records displayed in the grid to which it pertains.


Results Per Page: 25

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

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

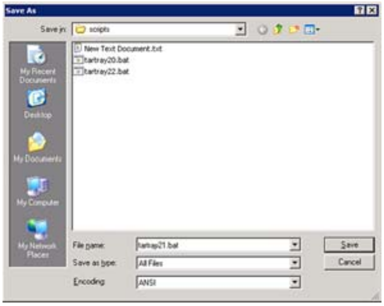


Destination	Gateway	Delete
1.1.1.1/1	1.1.1.1	□
1.2.3.4/1	1.3.2.4	□

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

- **thumbnail** - a small image in a window or on a screen that when clicked displays the same image enlarged within a window or on the screen.

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



Save in: scripts

New Text Document.txt
tartray20.bat
tartray22.bat

File name: tartray21.bat
Save as type: All Files
Encoding: ANSI

Getting Started

Procedures for Logging In, Out

Access the Security Reporter Login window

The SR Report Manager user interface is accessible in one of two ways:

- by clicking the SR icon in the WFR Welcome window (see Access SR Report Manager from the WFR Portal)
- by launching an Internet browser window supported by the Security Reporter and then entering SR's URL in the Address field (see Enter Report Manager's URL in the Address field)

Access SR Report Manager from the WFR Portal

Click the SR icon in the WFR Welcome window:

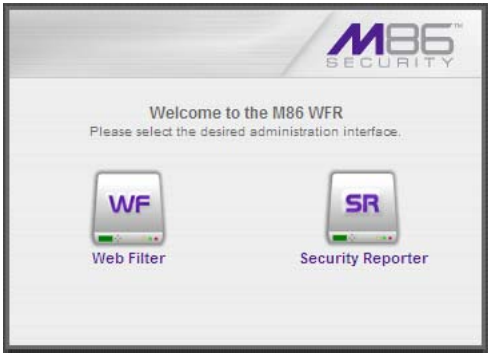


Fig. 1:1-1 Security Reporter icon in WFR Welcome window

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

Clicking the SR icon launches a separate browser window/ tab containing the Security Reporter Login window (see Fig. 1:1-2).

Enter Report Manager’s URL in the Address field

1. Launch an Internet browser window supported by the SR.
2. In the address line of the browser window, type in “https://” and the SR’s IP address or host name, and use port number “:8443” for a secure network connection, appended by “/SR/”.

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

   With a secure connection, the first time you attempt to access the Report Manager user interface in your browser you will be prompted to accept the security certificate. In order to accept the security certificate, follow the instructions at: ***http://www.m86security.com/software/8e6/docs/ig/misc/sec-cert-sr3.1.pdf***
3. After accepting the security certificate, click **Go** to open the Security Reporter Login window (see Fig. 1:1-2).

Log In

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

To log in the application:

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

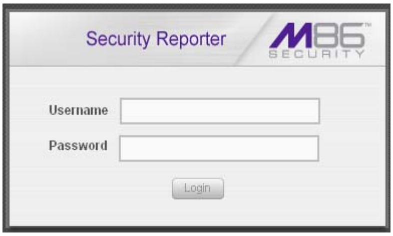


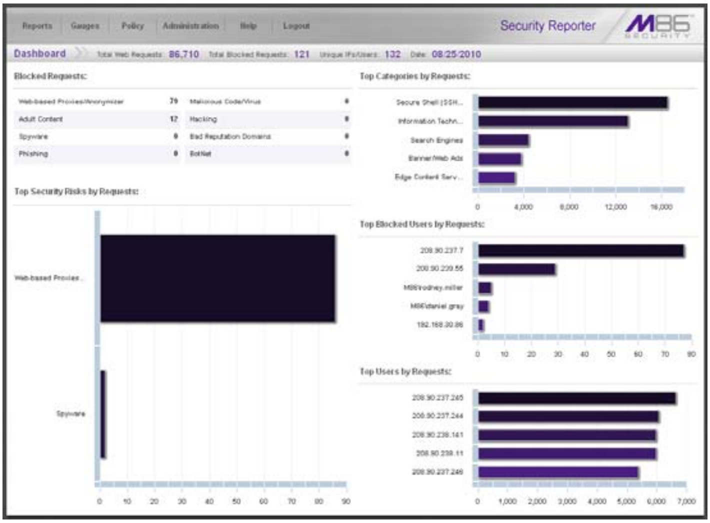
Fig. 1:1-2 Security Reporter Login window

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

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

TIP*: M86 Security recommends administrators who access this application for the first time should change their account password. Administrator usernames and passwords are modified in Administration > Admin Profiles.*

3. Click **Login** to display the Reports Dashboard of the Report Manager user interface:



Dashboard Total Web Requests: 86,710 Total Blocked Requests: 121 Unique IPs/Users: 132 Date: 08/25/2010

Blocked Requests:

Web-based Proxies/Anonymizer	79	Malicious Code/Virus	0
Adult Content	17	Hacking	0
Spyware	0	Bad Reputation Domains	0
Phishing	0	BotNet	0

Fig. 1:1-3 Default Report Manager panel

NOTES: *On a newly installed unit, SR reporting data is inaccessible and will not display in the dashboard until the server is configured, logs are transferred to the SR, and the database is built—the latter process could take about 24 hours. If a software update was recently applied on an existing server, it could take several hours before data is available.*

A maximum of eight users can use the SR user interface simultaneously. However, for optimum results, M86 Security recommends no more than four users generate reports at the same time.

Re-login

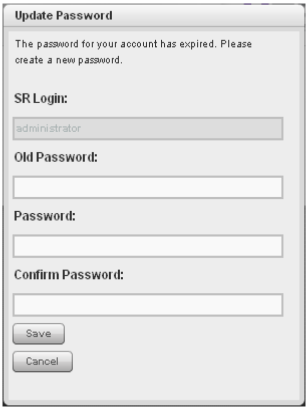
Each session is timed so that it remains active as long as there is activity in the user interface within an eight hour period. You need to log into the application again after an eight hour period of inactivity, or in the event that the SR server was restarted.

If your session in the application is timed out, when you click a button, thumbnail, or menu item in the Report Manager, an alert box opens with the message: “Session Timed out!” In the System Configuration administrator console, the following message displays: “Your session has ended, please login.”

To log in again, click **OK** to close the alert box; this action displays the Security Reporter login window where you will need to log in again.

Expired Passwords

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



Update Password

The password for your account has expired. Please create a new password.

SR Login: administrator

Old Password:

Password:

Confirm Password:

Fig. 1:1-4 Update Password window

1. Beneath your username displayed in the **SR Login** field, enter your **Old Password**.
2. In the **Password** and **Confirm Password** fields, enter eight to 20 characters for the new password, including at least one alpha character, one numeric character, and one special character. The password is case sensitive.
3. Click **Save** to close the pop-up window.
4. In the Security Reporter login window (see Fig. 1:1-2), enter your **Username** and new **Password**, and then click **Login** to access the user interface.

User Interface Navigation

Once you have logged into the Report Manager, use the navigation toolbar at the top of the screen to navigate to the section of the user interface you wish to use.

This toolbar provides a menu link to access the System Configuration administrator console (if permissions are granted by the global administrator to access this feature). A link to Web Filter is also available via a menu link.

Links in the Report Manager Navigation Toolbar

The navigation toolbar at the top of the Report Manager screen consists of the following links and menu topics for configuring and using the Report Manager:

- **Reports** - mouse over this link to open the Reports menu. Global and group administrators can click any Report menu item to view or generate a report, or schedule a report to run.
- **Gauges** - mouse over this link to open the Gauges menu. These menu options let you set up and manage URL and bandwidth gauges, and end user Internet activity.
- **Policy** - mouse over this link to open the Policy menu. These menu options let you set up and maintain policies used for triggering warnings when gauges approach their upper threshold limits.
- **Administration** - mouse over this link to open the Administration menu. These menu options let you set up and maintain administrator profiles and groups, maintain the Report Manager, and manage the SR.
- **Help** - click this link to launch a separate browser window or tab displaying the page containing links to the latest user guides (in the .pdf format) for this application.

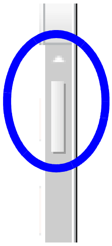
- **Logout** - click this link to log out of the SR (see Log Out for details on log out procedures).

Navigation Tips and Conventions

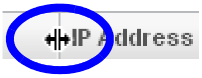
The following tips and list of conventions will help you navigate the Report Manager user interface:

- **Move a pop-up window** - Click the toolbar of a pop-up window and simultaneously move your mouse to relocate the pop-up window to another area in the current browser window.
- **Scroll up and down, and across a list** - If available, use the scrollbar to the right or along the bottom of a frame or list box to view an entire list.

  An extensive list can be viewed in its entirety by clicking the Previous and Next buttons.



- **Tab to the next field** - Press the Tab key on your keyboard to advance to the next field in a panel.
- **Expand, contract a column** - Columns can be expanded or contracted by first mousing over the divider in the column header to display the arrow and double line characters (<-II->). A column is then expanded or contracted by left-clicking the mouse and dragging the column bar to the right or left.



- **Browser back button, refresh button** - Clicking either the back button in the browser window or the refresh button in your browser will refresh the SR user interface and log you out of the application.
- **Select multiple items in specified windows** - In specified panels, when moving several items from one list box to another, or when deleting several items, the Ctrl and Shift keys can be used to expedite this task.

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

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

- **Sort records by another column header** - Records can often be sorted by a different column header by clicking the header for that column. This action sorts the records that display in descending order by that column. Clicking the same column header again sorts the records in ascending order by that column.
- **View tooltip information** - To view information about any object that has a circled "i" icon beside it, mouse over the icon to display tooltips that explain how to use that button or field.

Wildcard Searches

1. When performing a search with wildcard(s), enter text in the following format: **%X%**, **%X**, or **X%** (in which "X" represents a partial or complete user IP address, username, site URL, or other specified search query item).

   Examples:

   - User IP: **%200.10.100.51%**, **%100**, or **192.168.%**
   - Username: **%jsmith%**, **%t**, or **%qa**
   - Site: **%yahoo%**, **%z**, or **cnn%**
2. Click the designated button to perform the wildcard search.
3. Make your selection from records returned by the search.

Links in the System Configuration Navigation Toolbar

The navigation toolbar at the top of the System Configuration screen consists of the following menu topics and selections for configuring and using the SR:

- **Network** - select a menu item to access its corresponding page used for creating and maintaining network configuration settings on the SR.
- **Server** - select a menu item to access its corresponding page used for managing the SR administration module's software.
- **Database** - select a menu item to access its corresponding page used for maintaining the SR database and Report Manager.
- **Help** - click this link to launch a separate browser window or tab displaying the page containing links to the latest user guides (in the .pdf format) for this application.
- **Logout** - click this link to log out of the SR (see Log Out for details on log out procedures).

Log Out

To log out of the SR, click the **Logout** button in the navigation toolbar; this action re-displays the login window.

Click the “X” in the upper right corner of the logout window or tab to close the window/tab.

Exiting the SR application will log you out of the user interface, but will not log you out of the WFR server, nor turn off the server.

⚠ ***WARNING****: If you need to turn off the WFR server, follow the shut down procedures outlined in ShutDown window sub-section from the WF Global Administrator Section of the Web Filter portion of this user guide. Failure to properly shut down the server can result in data being lost or corrupted.*

SR SYSTEM CONFIGURATION SECTION

Introduction

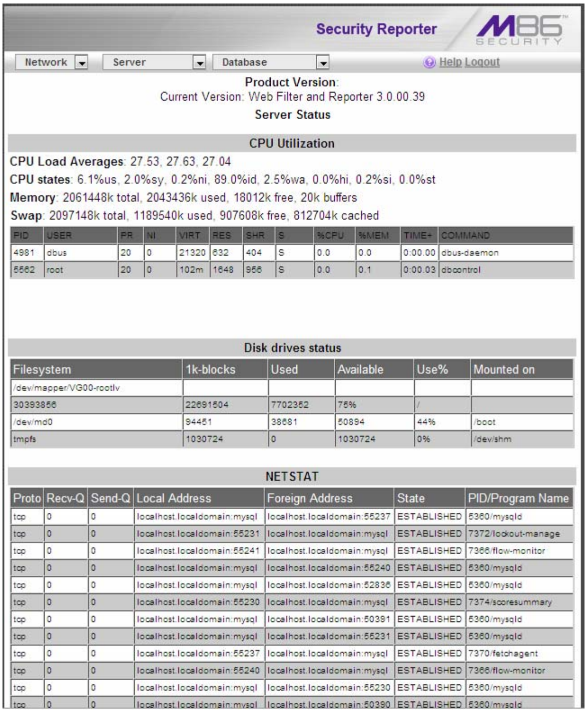
The SR System Configuration Section of this portion of the user guide provides instructions to the global administrator on configuring and maintaining the SR.

The global administrator performs the following tasks:

- provides a suitable environment for the SR, including a high speed access to authorized client workstations
- adds new administrators
- sets up administrators for receiving automatic alerts
- analyzes SR statistics
- utilizes diagnostics for monitoring the SR status to ensure optimum functioning of the SR
- establishes and implements backup and restoration procedures for the SR

Chapter 1: Access System Configuration

If your account profile is set up with privileges to access the System Configuration administrator console, its user interface is accessible by navigating in the Report Manager to **Administration > System Configuration**:



Product Version:
Current Version: Web Filter and Reporter 3.0.00.39
Server Status

CPU Utilization

CPU Load Averages: 27.53, 27.63, 27.04
CPU states: 6.1%us, 2.0%sy, 0.2%ni, 89.0%id, 2.5%wa, 0.0%hi, 0.2%si, 0.0%st
Memory: 2061448k total, 2043436k used, 18012k free, 20k buffers
Swap: 2097148k total, 1189540k used, 907608k free, 812704k cached

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
4981	dbus	20	0	21320	632	404	S	0.0	0.0	0:00.00	dbus-daemon
5562	root	20	0	102m	1648	956	S	0.0	0.1	0:00.03	dbcontrol

Disk drives status

Filesystem	1k-blocks	Used	Available	Use%	Mounted on
/dev/mapper/VG00-rootlv					
30393856	22691504	7702352	75%	/	
/dev/md0	94451	38681	50894	44%	/boot
tmpfs	1030724	0	1030724	0%	/dev/shm

NETSTAT

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program Name
tcp	0	0	localhost.localdomain:mysql	localhost.localdomain:55237	ESTABLISHED	5360/mysqld
tcp	0	0	localhost.localdomain:55231	localhost.localdomain:mysql	ESTABLISHED	7372/lockout-manage
tcp	0	0	localhost.localdomain:55241	localhost.localdomain:mysql	ESTABLISHED	7366/flow-monitor
tcp	0	0	localhost.localdomain:mysql	localhost.localdomain:55240	ESTABLISHED	5360/mysqld
tcp	0	0	localhost.localdomain:mysql	localhost.localdomain:52836	ESTABLISHED	5360/mysqld
tcp	0	0	localhost.localdomain:55230	localhost.localdomain:mysql	ESTABLISHED	7374/scoresummary
tcp	0	0	localhost.localdomain:mysql	localhost.localdomain:50391	ESTABLISHED	5360/mysqld
tcp	0	0	localhost.localdomain:mysql	localhost.localdomain:55231	ESTABLISHED	5360/mysqld
tcp	0	0	localhost.localdomain:55237	localhost.localdomain:mysql	ESTABLISHED	7370/fetchagent
tcp	0	0	localhost.localdomain:55240	localhost.localdomain:mysql	ESTABLISHED	7366/flow-monitor
tcp	0	0	localhost.localdomain:mysql	localhost.localdomain:55230	ESTABLISHED	5360/mysqld
tcp	0	0	localhost.localdomain:mysql	localhost.localdomain:50390	ESTABLISHED	5360/mysqld

Fig. 2:1-1 Server Status screen

The System Configuration user interface launches in a separate window/tab (using port 8843), displaying the Server Status screen.

***NOTES**: See Server Status screen in this Section of the user guide for information about this screen.*

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

Chapter 2: Configuring the Server

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

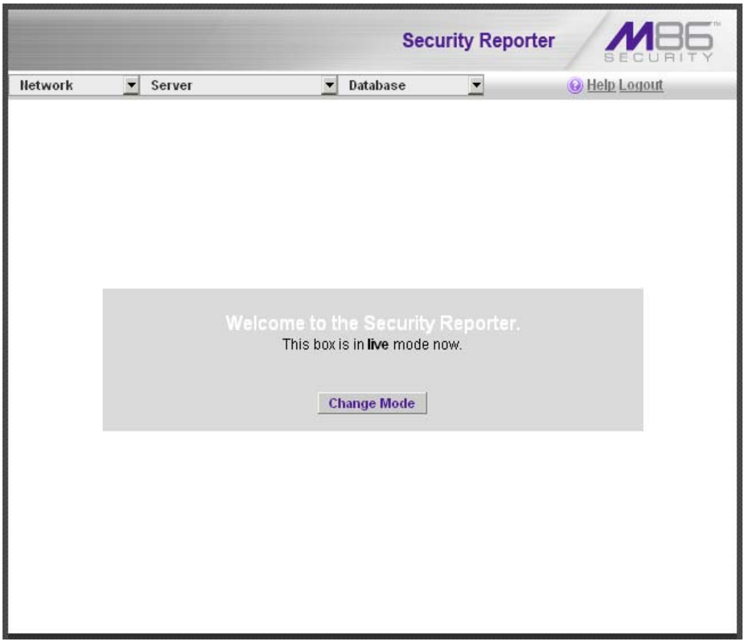
TIP*: When making a complete configuration in the System Configuration administrator console, M86 Security recommends you navigate from left to right (Network to Server to Database) in choosing your menu options.*

Network Menu

The Network pull-down menu includes options for setting up and maintaining components to be used on the server's network. These options are: Box Mode, and Lockouts.

Box Mode screen

The Box Mode screen displays when the Box Mode option is selected from the Network menu. The box mode indicates whether the server box is functioning in the “live” mode, or in the “archive” mode. When the box mode displays on the screen, you can view the current mode set for the server, and can change this setting, if necessary.



Welcome to the Security Reporter.
This box is in **live** mode now.

Fig. 2:2-1 Box Mode screen

Live Mode

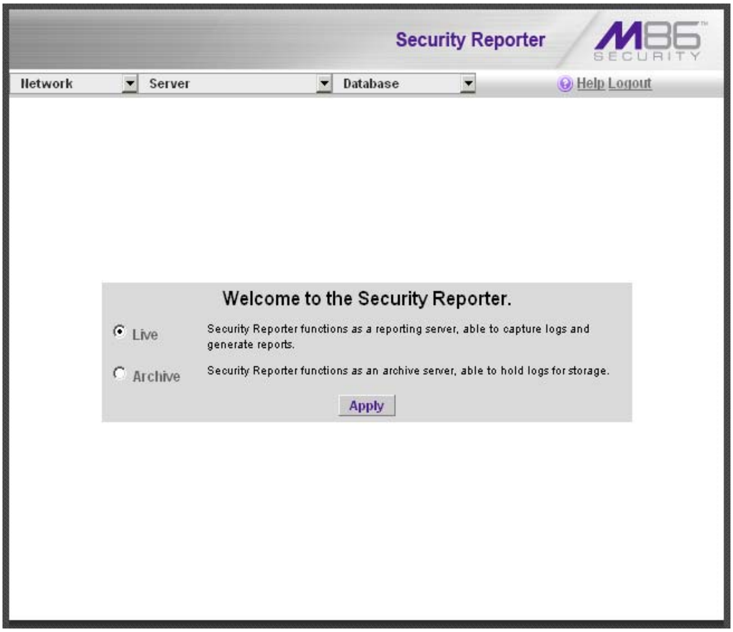
Once your server is configured and the server is set in the “live” mode, it will receive and process real time data from the Web Filter. The Report Manager can then be used to capture data and create views.

Archive Mode

In the “archive” mode, the server solely functions as a receptacle in which historical, archived files are placed. In this mode, “old” files placed on the server can be viewed using the Report Manager.

Change the Box Mode

1. Click the **Change Mode** button to display the two server box mode options on the screen:



Welcome to the Security Reporter.

● Live — Security Reporter functions as a reporting server, able to capture logs and generate reports.

○ Archive — Security Reporter functions as an archive server, able to hold logs for storage.

Fig. 2:2-2 Change Box Mode

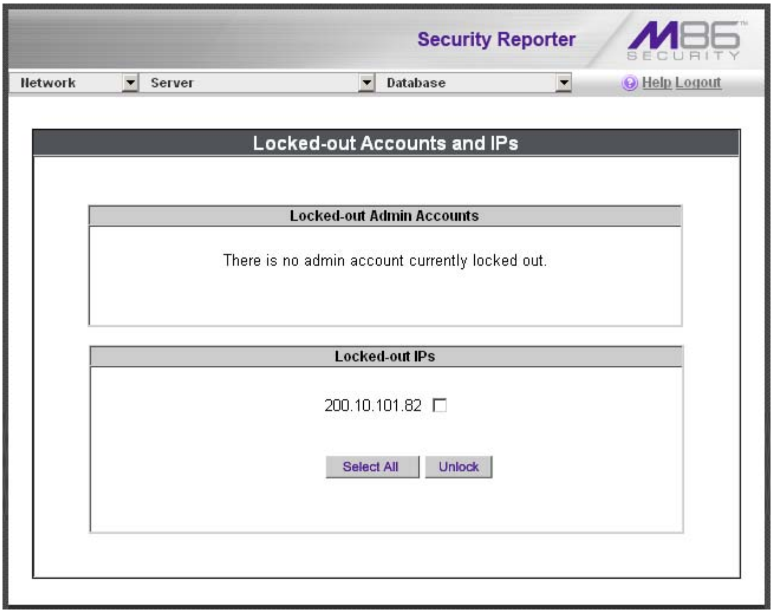
2. Click the radio button corresponding to **Live** or **Archive** to specify the mode in which the server should function:
   - choose **Live** if you wish the server to function in the “live” mode, receiving and processing real time data from the Web Filter.

- choose **Archive** if you wish the server to function in the “archive” mode, solely as a receptacle for historical, archived files.

3. Click **Apply** to confirm your selection. The mode you specify will immediately be in effect.

Locked-out Accounts and IPs screen

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



There is no admin account currently locked out.

200.10.101.82 □

Fig. 2:2-3 Locked-out Accounts and IPs screen

***NOTE**: An account or IP address becomes locked if the Password Security Options feature is enabled in the Optional Features screen, and a user is unable to log into the Report Manager or*

System Configuration administrator console due to a password expiration, or having met the specified number of failed password attempts within the designated timespan.

View Locked Accounts, IP addresses

The frames in this screen display the following messages if there are no users currently locked out:

- **Locked-out Admin Accounts** - There is no administrator account currently locked out.
- **Locked-out IPs** - There is no IP currently locked out.

If there are any locked accounts/IP addresses in a frame, each locked username/IP address displays on a separate line followed by a checkbox. The Select All and Unlock buttons display at the bottom of the frame.

Unlock Accounts, IP addresses

To unlock an account/IP address in a frame:

1. Click the checkbox corresponding to the username/IP address.

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

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

NOTE*: In the text above, ‘xxx’ and ‘x.x.x.x’ represents the unlocked username/IP address.*

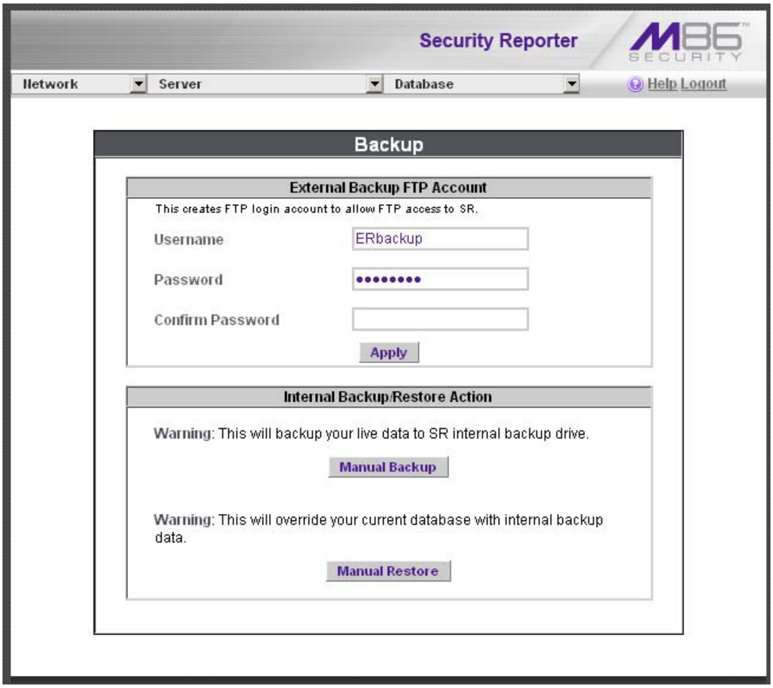
3. Click **OK** to return to the Locked-out Accounts and IPs screen that no longer shows the accounts/IPs that have been unlocked.

Server Menu

The Server pull-down menu includes options for setting up processes for maintaining the server. These options are: Backup, Self-Monitoring, Server Status, Secure Access, Shut Down, and Report Manager.

Backup screen

The Backup screen displays when the Backup option is selected from the Server menu. This screen is used for setting up the password for the remote server's FTP account, for executing an immediate backup on the SR, and for performing a restoration to the database from the previous backup run.



Backup

External Backup FTP Account

This creates FTP login account to allow FTP access to SR.

Username: ERbackup

Password: ••••••••

Confirm Password:

Internal Backup/Restore Action

Warning: This will backup your live data to SR internal backup drive.

Warning: This will override your current database with internal backup data.

Fig. 2:2-4 Backup screen

Backup and Recovery Procedures

***IMPORTANT**: M86 Security recommends establishing backup and recovery procedures when you first begin using the SR. Please follow the advice in this section to ensure your SR is properly maintained in the event that data is lost and back up procedures need to be performed to recover data.*

Although automatic backups to a local SR hard drive are scheduled weekly by default, it is important that the SR administrator implements a backup policy to ensure data integrity and continuity in the event of any possible failure scenario. This policy should include frequent, remote backups, such that raw logs and SR database files are available for restoration without relying on the SR's hard drives.

In general, recovery plans involve (i) restoring the most recent backup of the database, and (ii) restoring raw logs to fill in the gap between the most recent backup of the database, and the current date and time.

Some scenarios and action plans to consider include the following:

- **The SR database becomes corrupted** - Correct the root problem. Restore the database from the most recent SR backup, and reprocess raw logs up to the current date and time.
- **The data drive fails** - Replace the data drive. Restore the database from the SR backup drive, and reprocess raw logs up to the current date and time.
- **The backup drive fails** - Replace the backup drive, and perform a manual backup.
- **Both data and backup drives are damaged** - Restore the database from the most recent remote backup, and reprocess raw logs up to the current date and time.

As you can see, it is critical that raw logs are available to bridge the gap between the last database backup and the present time, and more frequent backups (local and remote) result in less “catch-up” time required for reprocessing raw logs.

Set up/Edit External Backup FTP Password

In order to back up the SR’s database to a remote server, an FTP account must be established for the remote server.

***NOTE**: In the External Backup FTP Account frame, the login name that will be used to access the remote server displays in the Username field. This field cannot be edited.*

1. In the **Password** field, enter up to eight characters for the password. The entry in this field is alphanumeric and case sensitive.
2. In the **Confirm Password** field, re-enter the password in the exact format used in the Password field.
3. Click the **Apply** button to save your entries. The updated Account ID will be activated after two minutes.

Execute a Manual Backup

In addition to performing on demand backups in preparation for a disaster recovery, you may wish to execute a manual backup under the following circumstances:

- **Power outage** - If there is a power outage at your facility and your system uses a backup battery, you might want to back up data before the battery fails.
- **Rolling blackout** - If your facility is subjected to rolling blackouts, and a blackout is scheduled during the time of your daily backup, you should back up your data before the blackout period, when the SR will be down.
- **Expiration about to occur** - If a data expiration is about to occur, you might want to back up your data before

losing the oldest data on the SR, prior to the daily backup process.

⚠ ***WARNING**: If corrupted data is detected on the SR, do not backup your data, as you may back up and eventually restore a corrupted database.*

When performing a manual backup, the SR's database is immediately saved to the internal backup drive. From the remote server, the backup database can be retrieved via FTP, and then stored off site.

***TIP**: M86 Security recommends executing an on demand backup during the lightest period of system usage, so the server will perform at maximum capacity.*

1. Click the **Manual Backup** button in the Internal Backup/ Restore Action frame to specify that you wish to back up live data to the SR's internal backup drive.
2. On the Confirm Backup/Restore screen, click the **Yes** button to back up the database tables and indexes.

⚠ ***WARNING**: M86 Security recommends that you do not perform other functions on the SR until the backup is complete. The time it will take to complete the backup depends on the size of all tables being saved.*

Perform a Remote Backup

After executing the manual backup, a remote backup can be performed on your remote server.

***NOTE**: Before beginning this FTP process, be sure you have enough space on the remote server for storing backup data. The required space can be upwards of 200 gigabytes.*

1. Log in to your FTP account.
2. Use FTP to download the SR's backup database to the remote server. When you are in the DAILY, WEEKLY, or MONTHLY sub-directory, be sure to get all the *.gz data files to include in your backup. You can then go to the

archive directory to get all the raw logs to include in your backup.

3. Store this backup data in a safe place off the remote server. If this backup database needs to be restored, it can be uploaded to the SR via FTP. (See Perform a Restoration to the SR.)

Perform a Restoration to the SR

There are two parts in performing a restoration of data to your SR. Part one requires data to be loaded on the remote server and then FTPed to the SR. Part two requires the FTPed data to be restored on the SR.

***NOTE**: Before restoring backup data to the SR, be sure you have enough space on the SR. Data that is restored to the SR will automatically include indexes.*

Perform these steps on the remote server:

1. Load the *.gz file backup data on your remote server.
2. Log in to your FTP account.
3. FTP the backup data to the SR's internal backup drive in the appropriate sub-directory: DAILY, WEEKLY, or MONTHLY.

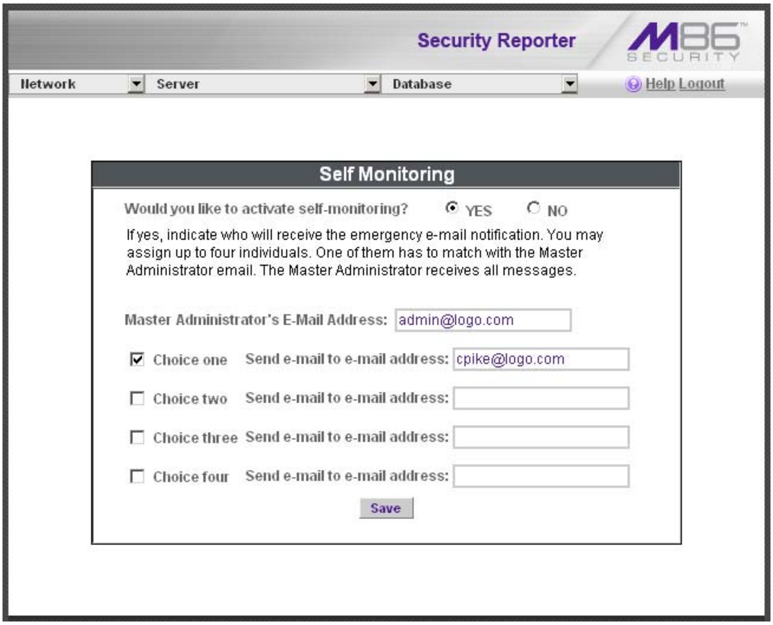
On the SR Server's Backup screen:

1. Click the **Manual Restore** button in the Internal Backup/ Restore Action frame to specify that you wish to over-write data on the live SR with data from the previous, internal backup run.
2. On the Confirm Backup/Restore screen, click the **Yes** button to restore database tables and indexes to the SR.

***NOTE**: The amount of time it will take to restore data to the SR depends on the combined size of all database tables being restored. M86 Security recommends that you do not perform other functions on the SR until the restoration is complete.*

Self Monitoring screen

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



Self Monitoring

Would you like to activate self-monitoring? ● YES ○ NO

If yes, indicate who will receive the emergency e-mail notification. You may assign up to four individuals. One of them has to match with the Master Administrator email. The Master Administrator receives all messages.

Master Administrator's E-Mail Address: admin@logo.com

☑ Choice one Send e-mail to e-mail address: cpike@logo.com

□ Choice two Send e-mail to e-mail address:

□ Choice three Send e-mail to e-mail address:

□ Choice four Send e-mail to e-mail address:

Fig. 2:2-5 Self Monitoring screen

As the administrator of the SR, you have the option to either activate or deactivate this feature. When the self-monitoring feature is activated, an automated e-mail message is dispatched to designated recipients if the SR identifies a failed process during its hourly check for new data.

View a List of Contact E-Mail Addresses

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

Set up and Activate Self-Monitoring

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

Remove Recipient from E-mail Notification List

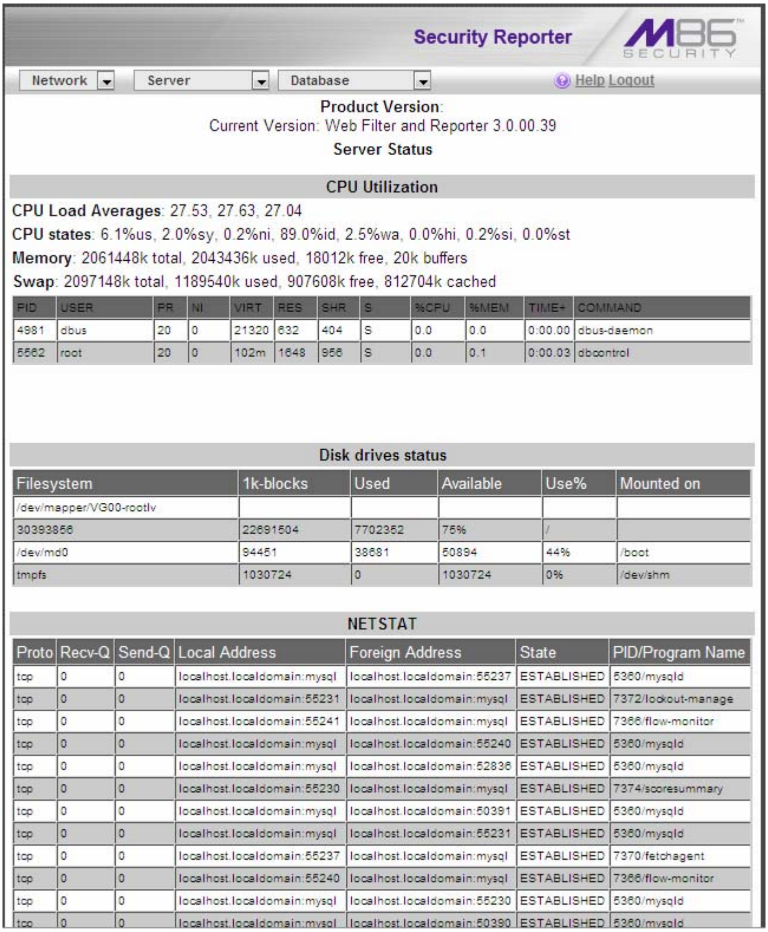
1. To stop sending emergency notifications to an e-mail address set up in the list, remove the check mark from the checkbox corresponding to the appropriate e-mail address.
2. Click the **Save** button to remove the recipient's name from the e-mail list. The Master Administrator and any remaining e-mail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

Deactivate Self-Monitoring

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

Server Status screen

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



Product Version:
Current Version: Web Filter and Reporter 3.0.00.39
Server Status

CPU Utilization

CPU Load Averages: 27.53, 27.63, 27.04
CPU states: 6.1%us, 2.0%sy, 0.2%ni, 89.0%id, 2.5%wa, 0.0%hi, 0.2%si, 0.0%st
Memory: 2061448k total, 2043436k used, 18012k free, 20k buffers
Swap: 2097148k total, 1189540k used, 907608k free, 812704k cached

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
4981	dbus	20	0	21320	632	404	S	0.0	0.0	0:00.00	dbus-daemon
5562	root	20	0	102m	1648	956	S	0.0	0.1	0:00.03	dbcontrol

Disk drives status

Filesystem	1k-blocks	Used	Available	Use%	Mounted on
/dev/mapper/VG00-rootlv					
30393856	22691504	7702352	75%	/	
/dev/md0	94451	38681	50894	44%	/boot
tmpfs	1030724	0	1030724	0%	/dev/shm

NETSTAT

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program Name
tcp	0	0	localhost.localdomain:mysql	localhost.localdomain:55237	ESTABLISHED	5360/mysqld
tcp	0	0	localhost.localdomain:55231	localhost.localdomain:mysql	ESTABLISHED	7372/lockout-manage
tcp	0	0	localhost.localdomain:55241	localhost.localdomain:mysql	ESTABLISHED	7366/flow-monitor
tcp	0	0	localhost.localdomain:mysql	localhost.localdomain:55240	ESTABLISHED	5360/mysqld
tcp	0	0	localhost.localdomain:mysql	localhost.localdomain:52836	ESTABLISHED	5360/mysqld
tcp	0	0	localhost.localdomain:55230	localhost.localdomain:mysql	ESTABLISHED	7374/scoresummary
tcp	0	0	localhost.localdomain:mysql	localhost.localdomain:50391	ESTABLISHED	5360/mysqld
tcp	0	0	localhost.localdomain:mysql	localhost.localdomain:55231	ESTABLISHED	5360/mysqld
tcp	0	0	localhost.localdomain:55237	localhost.localdomain:mysql	ESTABLISHED	7370/fetchagent
tcp	0	0	localhost.localdomain:55240	localhost.localdomain:mysql	ESTABLISHED	7366/flow-monitor
tcp	0	0	localhost.localdomain:mysql	localhost.localdomain:55230	ESTABLISHED	5360/mysqld
tcp	0	0	localhost.localdomain:mysql	localhost.localdomain:50390	ESTABLISHED	5360/mysqld

Fig. 2:2-6 Server Status screen

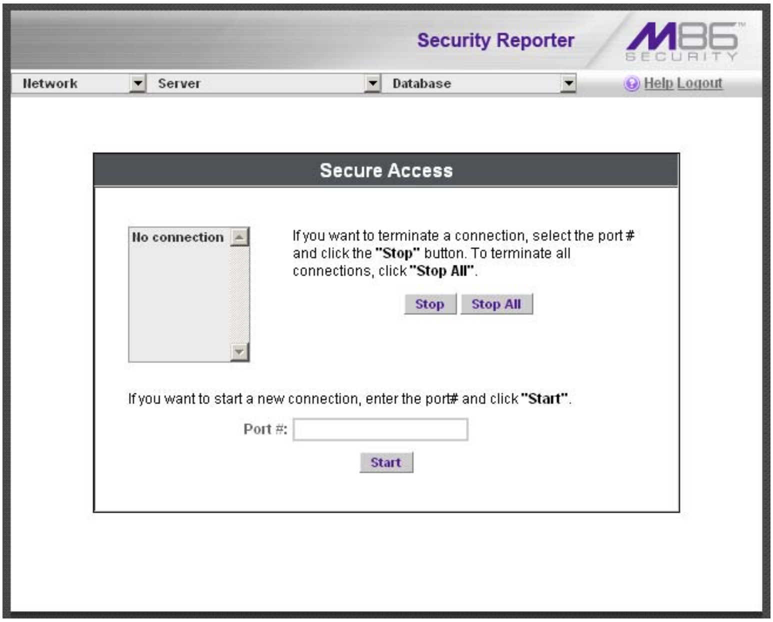
View the Status of the Server

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

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

Secure Access screen

The Secure Access screen displays when the Secure Access option is selected from the Server menu. This screen is primarily used by M86 Security technical support representatives to perform maintenance on your server, if your system is behind a firewall that denies access to your server.



Secure Access

No connection

If you want to terminate a connection, select the port # and click the **"Stop"** button. To terminate all connections, click **"Stop All"**.

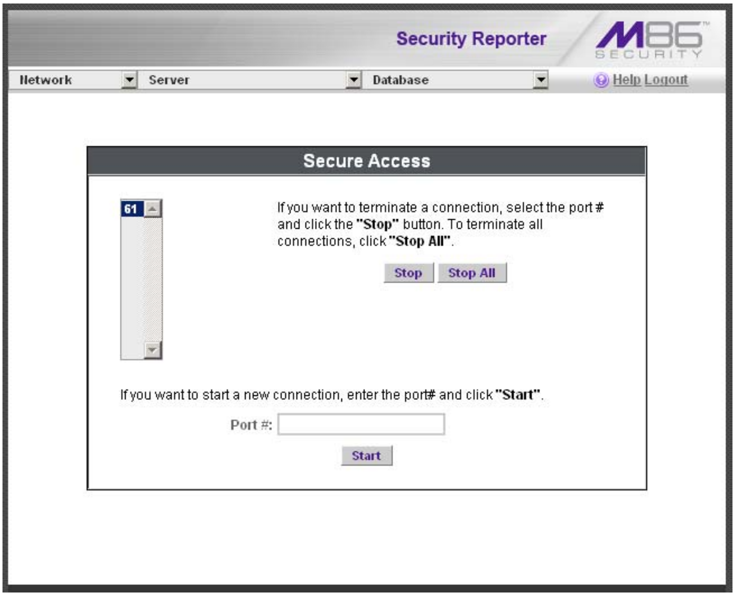
If you want to start a new connection, enter the port# and click **"Start"**.

Port #:

Fig. 2:2-7 Secure Access screen

Activate a Port to Access the SR

1. After the administrator at the customer’s site authorizes you to use a designated port to access their server, enter that number at the **Port #** field.
2. Click the **Start** button to activate the port. This action enters the port number in the list box above, replacing the text: “No connection”.



If you want to terminate a connection, select the port # and click the **"Stop"** button. To terminate all connections, click **"Stop All"**.

If you want to start a new connection, enter the port# and click **"Start"**.

Fig. 2:2-8 Port entries

Terminate a Port Connection

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

Terminate All Port Connections

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

Shut Down screen

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

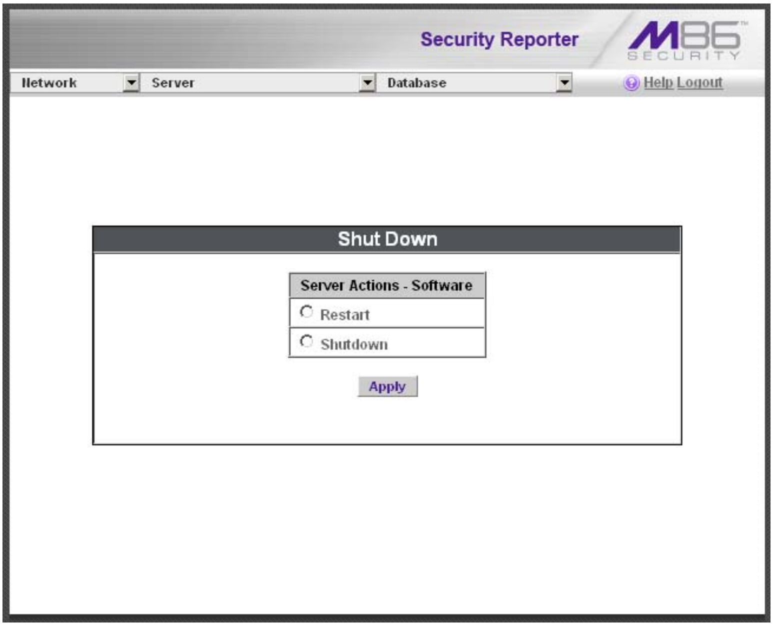


Fig. 2:2-9 Shut Down screen

SR Action Selections

- **Restart the SR's Software** - The Restart Software option should be selected if daemons fail to run and/or the database needs to be started again. When this option is selected, the MySQL database is rebooted.
- **Shut Down the SR's Software** - The Shutdown Software option should be selected if a software update needs to be installed on the server. When the Shutdown Software option is selected, the MySQL database shuts off and no files are FTPed to the server.

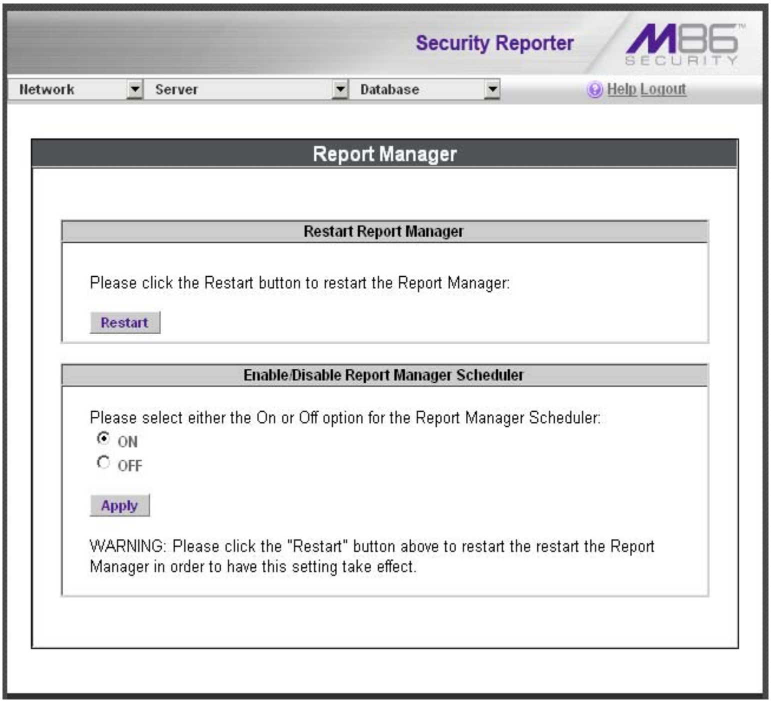
Perform a Server Action

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

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

Report Manager screen

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



Report Manager

Restart Report Manager

Please click the Restart button to restart the Report Manager:

Restart

Enable/Disable Report Manager Scheduler

Please select either the On or Off option for the Report Manager Scheduler:

● ON
○ OFF

Apply

WARNING: Please click the "Restart" button above to restart the restart the Report Manager in order to have this setting take effect.

Fig. 2:2-10 Report Manager screen

Restart the Report Manager

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

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

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

Enable/Disable the Report Manager Scheduler

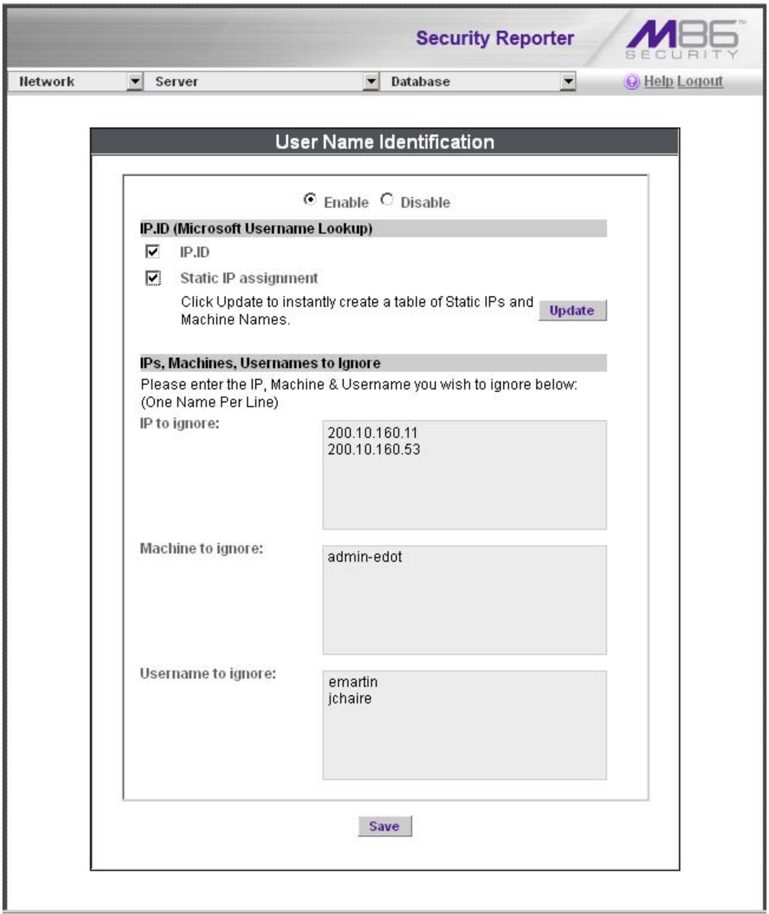
1. In the Enable/Disable Report Manager Scheduler frame, click the appropriate radio button to specify whether or not to automatically run scheduled reports:
   - “ON” - Choose this option to let the Report Manager automatically run scheduled reports.
   - “OFF” - Choose this option if you do not want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

Database Menu

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

User Name Identification screen

The User Name Identification screen displays when the IP.ID option is selected from the Database menu. This screen is used for configuring the SR to identify users based on the IP addresses of their machines, their usernames, and/or their machine names. Information set up on this screen is used by the Report Manager when logging a user’s Internet activity.



User Name Identification

● Enable ○ Disable

IP.ID (Microsoft Username Lookup)

☑ IP.ID

☑ Static IP assignment

Click Update to instantly create a table of Static IPs and Machine Names.

IPs, Machines, Usernames to Ignore

Please enter the IP, Machine & Username you wish to ignore below: (One Name Per Line)

IP to ignore:
200.10.160.11
200.10.160.53

Machine to ignore:
admin-edot

Username to ignore:
emartin
jchaire

Fig. 2:2-11 User Name Identification screen with IP.ID activated

As the administrator of the SR, you have the option to either enable or disable this feature for logging users’ activities by usernames, machine names, and/or IP addresses of machines.

Warnings

⚠ *The SR will generate NetBIOS requests outside the network if IP.ID is activated **and** if no segment settings have been specified in the configuration of the Web access logging device—causing it to log external traffic. To resolve this issue, the Web access logging device should be modified to log activity only within the network. If a firewall is used, it should be set up to prevent logging NetBIOS requests outside the network.*

***NOTE**: Depending on the type of Web access logging device you are using, there may not be a configuration parameter for segment settings.*

⚠ *Be sure the time zone specified for the SR is the same for each Web access logging device the SR uses. Failure in executing this setup will cause inconsistencies when users' logging times are reported, especially if IP.ID is activated. If multiple Web access logging devices are used, be sure to identify the subnets assigned to each of these devices, as users cannot be tracked solely by IP address.*

⚠ *If using IP.ID, note that user login times are established for set periods of 15 minutes, and if more than one user logs onto the same machine during that time period, the activity on that machine will be identified with the first user who logged onto that machine. For example, the first user logs on a machine for three minutes and then logs off. The second user logs on the same machine for 11 minutes and then logs off. The first user logs back on that machine for 16 minutes. All 30 minutes are logged as the first user's activity.*

View the User Name Identification screen

If user name identification is enabled, specified IP.ID criteria displays, and IP, Machine, and Username frames will be populated if entries were previously made in them.

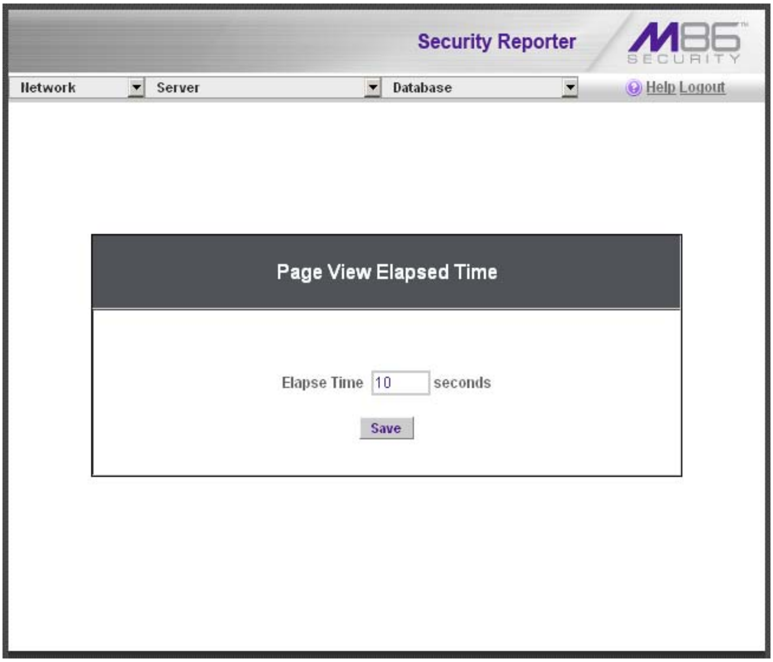
***NOTE**: If this feature is disabled, checkboxes in the IP.ID (Microsoft Username Lookup) section display greyed-out.*

Configure the Server to Log User Activity

1. In the area above the IP.ID (Microsoft Username Lookup) section of the screen, click the radio button corresponding to **Enable**. This action opens an alert box informing you that if usernames are enabled, these usernames will overwrite those that are being imported from the shadow log.
2. Click **OK** to close the alert box, and to activate the IP.ID and Static IP assignment checkboxes.
3. in the IP.ID (Microsoft Username Lookup) section of the screen, select one or both of the following options by clicking in the designated checkbox(es):
   - **IP.ID -** this option logs a user’s activity by username (login ID).
   - **Static IP assignment** - this option logs a user’s activity by the IP address of the machine used. When selecting this option, the Update button becomes activated.
     a. Click the **Update** button to automatically generate a table of static IP addresses and machine names. After this table is created, the message screen displays to confirm the successful execution of this task.
     b. Click the **Back** button to return to the User Name Identification screen.

Page View Elapsed Time screen

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



Elapse Time 10 seconds

Fig. 2:2-12 Page View Elapsed Time screen

Establish the Unit of Elapsed Time for Page Views

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

Elapsed Time Rules

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

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

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

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

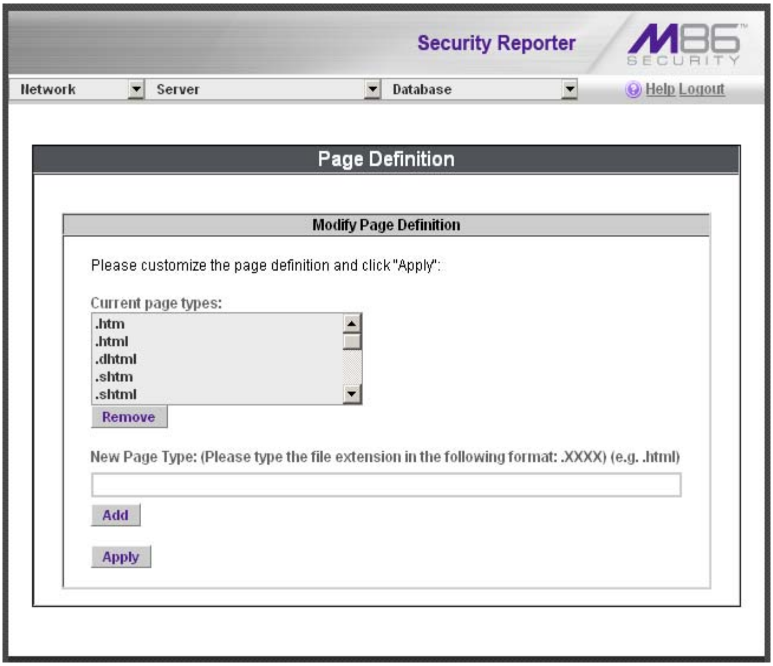
  For example, if the value entered at the Elapse Time field is 10 seconds and the user remains at a Web site for 12 seconds, two visits to that site will be logged for him/her.

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

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

Page Definition screen

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



Please customize the page definition and click "Apply":

Current page types:

.htm
.html
.dhtml
.shtm
.shtml

New Page Type: (Please type the file extension in the following format: .XXXX) (e.g. .html)

Fig. 2:2-13 Page Definition screen

View the Current Page Types

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

Remove a Page Type

To remove a page type from the detail report:

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

Add a Page Type

To add a page type in the detail report:

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

Tools screen

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

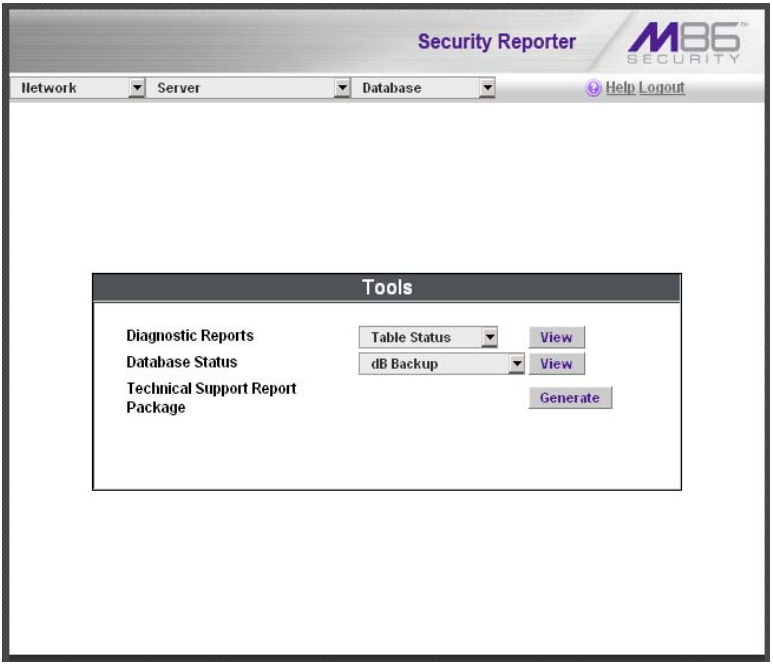


Fig. 2:2-14 Tools screen

The following options are available on this screen:

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

View Diagnostic Reports

1. Choose a report from the pull-down menu (Table Status, Process List, Full Process List, Tables, or Daily Summary).
2. Click the **View** button to view the selected diagnostic report in a pop-up window:
   - **Table Status** - This report contains a list of Client table names, and columns of statistics on each table, such as type, size, number of rows, and time created and updated.
   - **Process List** - This report shows a list of current SQL queries in the database, in an abbreviated format.
   - **Full Process List** - This report shows a list of current SQL queries in the database, in the full format that includes all columns of data.
   - **Tables** - This report contains a list of the names of tables currently in the database.
   - **Daily Summary** - This report shows the date range of summary tables currently in the database.
3. Click the “X” in the upper right corner of the pop-up window to close the window.

View Database Status Logs

1. Choose a database status log from the pull-down menu.
2. Click the **View** button to view the selected database status log in a pop-up window:
   - **db Active** - This log indicates when client tables were last updated with hits_objects and hits_pages.
   - **db Backup** - This log provides information about the MySQL backup/restore operation.
   - **db Control** - This log shows a list of actions performed by the SR process when processing log files.

- **db Identify** - This log provides information about the server's action of obtaining user/machine names from name log files and populating the database with these names.
- **db Ipgroups** - This log lists individual and group IP records that were added to—and deleted from—the client group lookup table.
- **db Logloader** - This log provides information about log file parsing and the number of valid and invalid records that are processed.
- **db Nbtlookup** - This log provides a list of user/ machine IP addresses from the NetBIOS lookup.
- **db Split** - This log contains information pertaining to the formation of the hits_objects/hits_pages tables.
- **db Staticip** - This log provides information about settings on the server for the static IP assignment option.
- **db Summary** - This log shows a summarization of activities from the dbsummary database tool.
- **db Support** - This log includes a list of temporary tables that were created for the formation of the hits tables.
- **db Tool** - This log shows information about system checks performed on disk usage, free memory, unprocessed files, and daemons.
- **db Traffic** - This log provides information about the daily traffic table.
- **Error Entry - Web Filter** - This log displays a list of Web Filter query errors.
- **File Watch Log** - This log shows a list of records that were imported from one machine to another.
- **MYSQL Log** - This log provides information pertaining to the MySQL server.

- **Partitioner Log** - This displays results of server partitioning for database expiration.
- **Software Update Log** - This log gives information about applied software updates.
- **Vsimporter** - If using an SWG, this log displays results of SWG archive log importation.

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

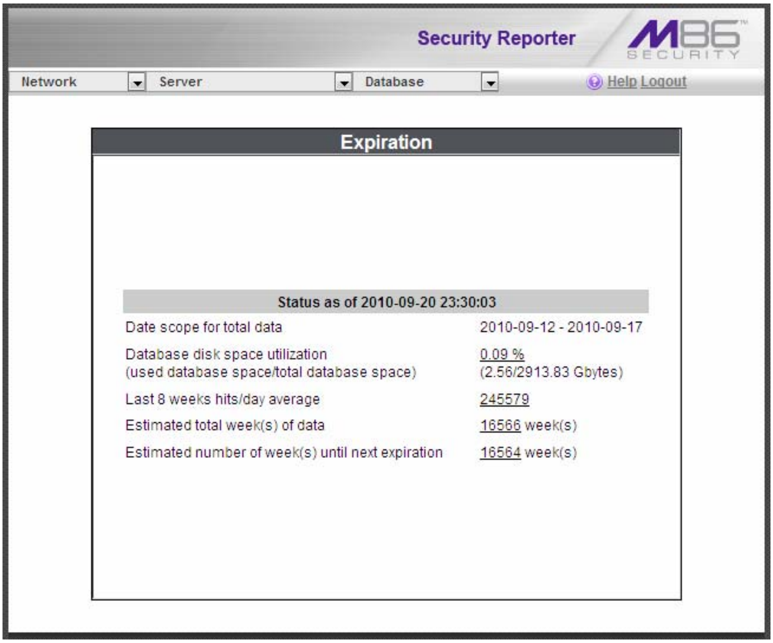
Generate Technical Support Report Package

When troubleshooting the SR unit with M86 Security Technical Support, a diagnostic report can be generated and submitted to M86 Security for further analysis. This report contains files with information about the ‘health’ of the unit.

1. At the **Techncal Support Report Package** field, click **Generate** to begin generating the report package.
2. After the package has generated, the “Successfully generated tech support log” pop-up window opens with the message: “Please download the file to email to M86 tech support.” Click **Download** to download the .tgz package to your machine.
3. Email the package to M86 Technical Support as instructed by your M86 technical support representative.

Expiration screen

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



Status as of 2010-09-20 23:30:03

Date scope for total data	2010-09-12 - 2010-09-17
Database disk space utilization (used database space/total database space)	0.09 % (2.56/2913.83 Gbytes)
Last 8 weeks hits/day average	245579
Estimated total week(s) of data	16566 week(s)
Estimated number of week(s) until next expiration	16564 week(s)

Fig. 2:2-15 Expiration screen

***NOTES**: Though the database is backed up automatically each week, under certain circumstances you may need to perform a manual backup to the internal backup drive, and then save this data off site. (See the Server Menu Backup screen section for information on establishing backup procedures, and backing up and restoring data on the SR.)*

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

Expiration Rules

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

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

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

Once data expires, it cannot be recovered.

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

View Data Storage Statistics

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

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

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

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

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

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

- **Estimated total week(s) of data** - the estimated number of weeks of data the server will store. This number is affected by end user hits/day and the storage capacity of the server.

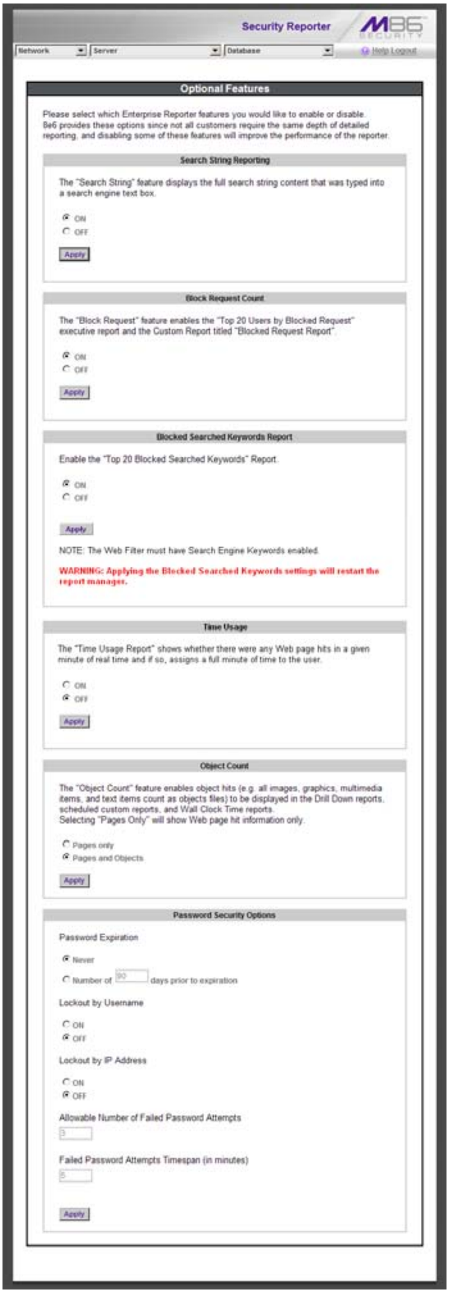
- **Estimated number of week(s) until next expiration** - the estimated number of weeks from this week that data on the server will expire, based on the hits/day and storage capacity of the server.

***NOTE**: See Appendix A: Evaluation Mode for information about viewing the Expiration screen in the evaluation mode.*

Optional Features screen

The Optional Features screen displays when Optional Features is selected from the Database menu. This screen is used for specifying any of the following options to be available in the Report Manager when generating specified types of reports: Search String Reporting, Block Request Count, Blocked Searched Keywords, Time Usage, Object Count. This screen also is used for enabling and configuring the password security feature to be used for the System Configuration administrator console and Report Manager (see Fig. 2-2:16).

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



Optional Features

Please select which Enterprise Reporter features you would like to enable or disable. 8e6 provides these options since not all customers require the same depth of detailed reporting, and disabling some of these features will improve the performance of the reporter.

Search String Reporting

The "Search String" feature displays the full search string content that was typed into a search engine text box.

● ON
○ OFF

Apply

Block Request Count

The "Block Request" feature enables the "Top 20 Users by Blocked Request" executive report and the Custom Report titled "Blocked Request Report".

● ON
○ OFF

Apply

Blocked Searched Keywords Report

Enable the "Top 20 Blocked Searched Keywords" Report.

● ON
○ OFF

Apply

NOTE: The Web Filter must have Search Engine Keywords enabled.

WARNING: Applying the Blocked Searched Keywords settings will restart the report manager.

Time Usage

The "Time Usage Report" shows whether there were any Web page hits in a given minute of real time and if so, assigns a full minute of time to the user.

○ ON
● OFF

Apply

Object Count

The "Object Count" feature enables object hits (e.g. all images, graphics, multimedia items, and text items count as objects files) to be displayed in the Drill Down reports, scheduled custom reports, and Wall Clock Time reports.
Selecting "Pages Only" will show Web page hit information only.

○ Pages only
● Pages and Objects

Apply

Password Security Options

Password Expiration

● Never
○ Number of 90 days prior to expiration

Lockout by Username

○ ON
● OFF

Lockout by IP Address

○ ON
● OFF

Allowable Number of Failed Password Attempts
3

Failed Password Attempts Timespan (in minutes)
5

Apply

Fig. 2:2-16 Optional Features screen

Enable Search String Reporting

If Search String Reporting is enabled, detail drill down reports display the full search string content typed into a search engine text box for search sites such as Google, Bing, Yahoo!, MSN, AOL, Ask.com, YouTube.com, and MySpace.com.

1. Click the radio button corresponding to “ON” to let search string entries display in drill down reports.
2. Click **Apply** to apply your setting.

Enable Block Request Count

If Block Request Count is enabled, the Top 20 Users by Blocked Requests Summary Report can be generated by the administrator.

1. Click the radio button corresponding to “ON” to make the Top 20 Users by Blocked Request report selection available in an administrator’s Summary Reports menu.
2. Click **Apply** to apply your setting.

NOTE: *Since Summary Reports are processed each night, any changes made to settings today will not effective until the following day.*

Enable Blocked Searched Keywords

If Blocked Seached Keywords is enabled, the Top 20 Blocked Searched Keywords Summary Report can be generated by the administrator.

1. Click the radio button corresponding to “ON” to make the Top 20 Users by Blocked Request report selection available in an administrator’s Summary Reports menu.
2. Click **Apply** to apply your setting.

⚠ ***WARNING***: *Applying this setting restarts the Report Manager.*

***NOTE**: Since Summary Reports are processed each night, any changes made to settings today will not effective until the following day.*

Enable Time Usage reports

If Time Usage Report is enabled, Time Usage reports can be generated by the administrator. These reports use the time usage algorithm to calculate the amount of time an end user spent accessing a given page or object—disregarding the number of seconds from each hit and counting each unique minute of Web time as one minute. Using this algorithm, an end user could never have more than 24 hours of Web time within a given 24-hour period.

1. Click the radio button corresponding to “ON” to make the Time Usage Report selection available in an administrator’s Custom Reports menu.
2. Click **Apply** to apply your setting.

***NOTE**: Since Time Usage reports are processed each night, any changes made to settings today will not effective until the following day.*

Enable Page and/or Object Count

In the Object Count frame, indicate whether drill down, Time Usage reports, and scheduled custom reports will include Web page hits only, or both Web page and object hits. Objects include images, graphics, multimedia items, and text item object files.

***WARNING**: If “Pages only” is selected, **all** records of objects accessed by end users will be lost for the time period in which this option was enabled. Even if there were objects accessed by end users during that time period, zeroes (“0”) will display for object activity in generated reports.*

1. Select one of two radio buttons to specify the type of hits to be included in drill down, Time Usage reports, and scheduled custom reports:

- “Pages only” - Choose this option to include *only* Web page hits in reports.
- “Pages and Objects” - Choose this option to include *both* Web page and object hits in reports.

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

Enable, Configure Password Security Option

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

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

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

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

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

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

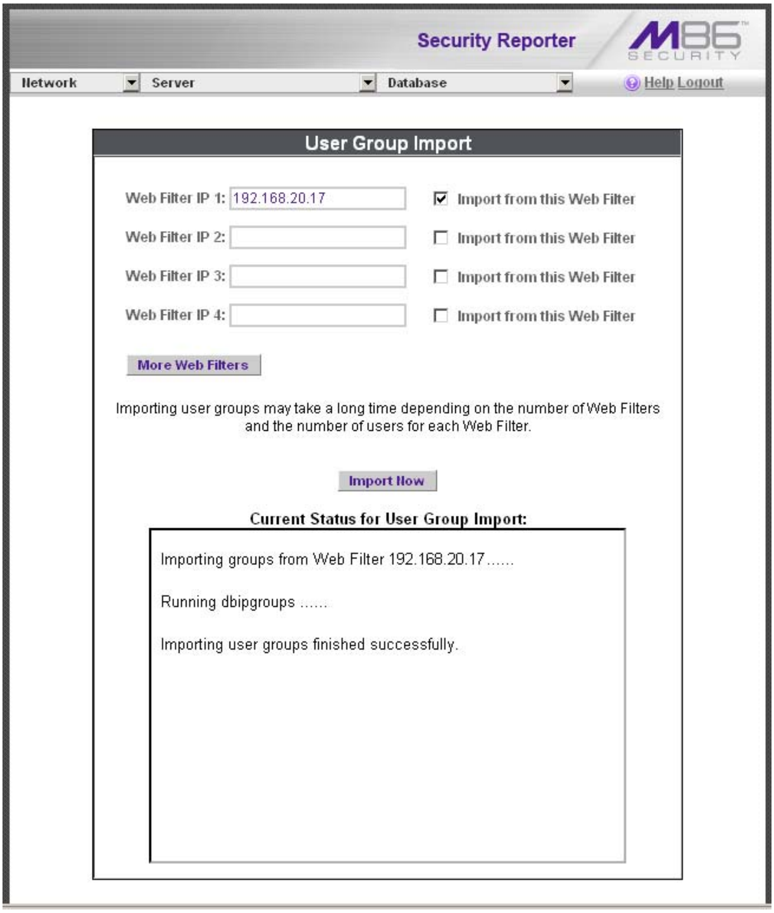
- **Failed Password Attempts Timespan (in minutes)** - With the Lockout by Username and/or Lockout by IP Address option(s) enabled, enter the number of minutes that defines the interval in which a user can enter an incorrect password—as specified in the Allowable Number of Failed Password Attempts field—before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

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

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

User Group Import screen

The User Group Import screen displays when the User Group Import option is selected from the Database menu. This screen is used for specifying the Web Filter(s) to send LDAP user group membership information to this SR, for performing a user group import on demand, and for viewing on demand user group import criteria.



User Group Import

Web Filter IP 1: 192.168.20.17 ☑ Import from this Web Filter

Web Filter IP 2: □ Import from this Web Filter

Web Filter IP 3: □ Import from this Web Filter

Web Filter IP 4: □ Import from this Web Filter

Importing user groups may take a long time depending on the number of Web Filters and the number of users for each Web Filter.

Current Status for User Group Import:

```
Importing groups from Web Filter 192.168.20.17......

Running dbipgroups ......

Importing user groups finished successfully.
```

Fig. 2:2-17 User Group Import screen

Import User Groups

NOTE*: Web Filter IP fields are populated by default if one or more Web Filter servers are connected to this SR.*

1. Specify the **Web Filter IP** address of each Web Filter to send LDAP user group membership data to this SR.
2. Click the checkbox corresponding to “Import from this Web Filter”.

NOTE*: If additional Web Filter servers need to be specified, click* ***More Web Filters*** *to display the next four sets of entry fields.*

3. After specifying all Web Filter servers from which to import user group data, click **Import Now** to begin the data importation process. The status of this process displays in the Current Status for User Group Import box that opens at the bottom of this screen when the Import Now button is clicked.

NOTE*: User groups will be imported in the exact format defined on the Web Filter.*

SR REPORT MANAGER ADMINISTRATION SECTION

Introduction

This section of the user guide provides instructions to the global administrator on configuring and managing the administration portion of the Report Manager for use with the Web Filter—and an SWG appliance, if applicable—and to the group administrator on using the SR to manage end user Internet and network activity.

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

The Report Manager’s Administration menu consists of the following options described in these chapters:

- Chapter 1: Group, Profile Management - This chapter explains how to set up user groups whose Internet activity will be monitored by group administrators; how to set up permissions so that an administrator in your group will only be able to access areas of the SR console that you specify; and how to set up a group administrator account.
- Chapter 2: Database Management - This chapter explains how to configure the server to use a secure network connection; view a list of user profiles; view administrator activity; manage the profiles of devices connected to the server; maintain Report Manager processes; analyze data storage on the server; and remove all profiles and configuration settings in the Report Manager.

- Chapter 3: Report Configuration - This chapter explains how to create and manage Custom Category Groups used for monitoring end user Internet activity, and configure general report settings.

Chapter 1: Group, Profile Management

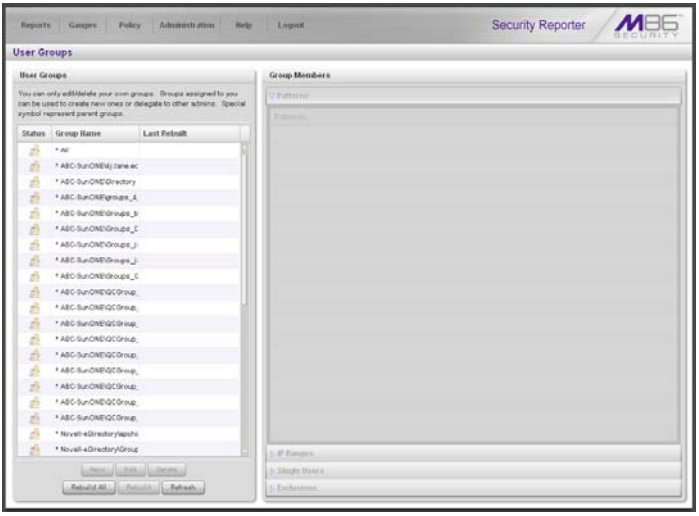
The following panels from the Administration menu of the Report Manager are described in this chapter: User Groups, Admin Groups, and Admin Profiles.

User Groups panel

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

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

1. In the navigation toolbar, mouse over the Administration menu link to display topics available to you.
2. Click **User Groups** to display the User Groups panel, which is comprised of the User Groups frame to the left and its Group Members target frame to the right:



You can only edit/delete your own groups. Groups assigned to you can be used to create new ones or delegate to other admins. Special symbol represent parent groups.

Status	Group Name	Last Rebuilt
	* All	
	* ABC-SunONE\uj.Jane.ec	
	* ABC-SunONE\Directory	
	* ABC-SunONE\groups_A	
	* ABC-SunONE\Groups_b	
	* ABC-SunONE\Groups_C	
	* ABC-SunONE\Groups_j	
	* ABC-SunONE\Groups_j	
	* ABC-SunONE\Groups_C	
	* ABC-SunONE\QCGroup_	
	* ABC-SunONE\QCGroup_	
	* ABC-SunONE\QCGroup_	
	* ABC-SunONE\QCGroup_	
	* ABC-SunONE\QCGroup_	
	* ABC-SunONE\QCGroup_	
	* ABC-SunONE\QCGroup_	
	* ABC-SunONE\QCGroup_	
	* ABC-SunONE\QCGroup_	
	* Novell-eDirectory\apshi	
	* Novell-eDirectory\Group	

Fig. 3:1-1 User Groups panel

Names of user groups previously added by the administrator display in black text in the User Groups frame. Imported user groups display preceded by an up arrow. For the global administrator, “All” displays as the first record in the list by default.

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

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

***NOTES**: This version of SR will import user groups from a source Web Filter or SWG using IP group authentication or the following LDAP server types:*

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

For the Web Filter:

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

View User Group Information

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

***NOTE**: User groups are automatically rebuilt daily.*

User group status key

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

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

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

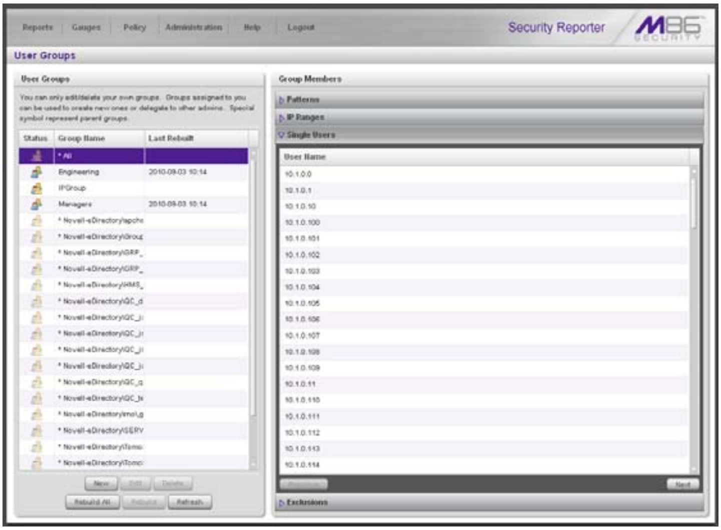
View a list of members in a user group

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

1. Select the user group from the User Groups frame by clicking its Group Name to highlight that record. Based on this selection, the Group Members frame to the right becomes activated along with the following buttons in the section below, based on the status of the user group:
   - If the selected user group is ready to be rebuilt, this action activates all buttons (New, Edit, Delete, Rebuild, Rebuild All, Refresh).
   - If the selected user group was not imported and cannot be rebuilt on demand, this action activates the New, Edit, Delete, Rebuild All, and Refresh buttons.
   - If the selected user group was imported and cannot be rebuilt on demand, this action activates the New, Rebuild All, and Refresh buttons only.

***NOTE**: A user group name preceded by an asterisk (*) indicates that user group is a parent group.*

2. Click an accordion in the Group Members frame to open it and view pertinent information:
   - Patterns accordion - view patterns previously set up for that user group.
   - IP Ranges accordion - view Starting IP and Ending IP ranges previously added for that user group.
   - Single Users accordion - view a list of User Names and IP Addresses for individual users previously selected from the Available Users list for that user group.
   - Exclusions accordion - view a list of User Names and IP Addresses for individual users previously selected from the Available Users list to be excluded from that user group.



You can only edit/delete your own groups. Groups assigned to you can be used to create new ones or delegate to other admins. Special symbol represent parent groups.

Status	Group Name	Last Rebuilt
	* All	
	Engineering	2010-09-03 10:14
	IPGroup	
	Managers	2010-09-03 10:14
	* Novell-eDirectory\apche	
	* Novell-eDirectory\Grou	
	* Novell-eDirectory\GRP_	
	* Novell-eDirectory\GRP_	
	* Novell-eDirectory\HMS_	
	* Novell-eDirectory\QC_d	
	* Novell-eDirectory\QC_j	
	* Novell-eDirectory\QC_j	
	* Novell-eDirectory\QC_j	
	* Novell-eDirectory\QC_j	
	* Novell-eDirectory\QC_q	
	* Novell-eDirectory\QC_b	
	* Novell-eDirectory\mol_g	
	* Novell-eDirectory\SERV	
	* Novell-eDirectory\Tomc	
	* Novell-eDirectory\Tomc	

User Name
10.1.0.0
10.1.0.1
10.1.0.10
10.1.0.100
10.1.0.101
10.1.0.102
10.1.0.103
10.1.0.104
10.1.0.105
10.1.0.106
10.1.0.107
10.1.0.108
10.1.0.109
10.1.0.11
10.1.0.110
10.1.0.111
10.1.0.112
10.1.0.113
10.1.0.114

Fig. 3:1-2 View user group information, Single Users accordion

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

Add a User Group

To add a new user group:

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

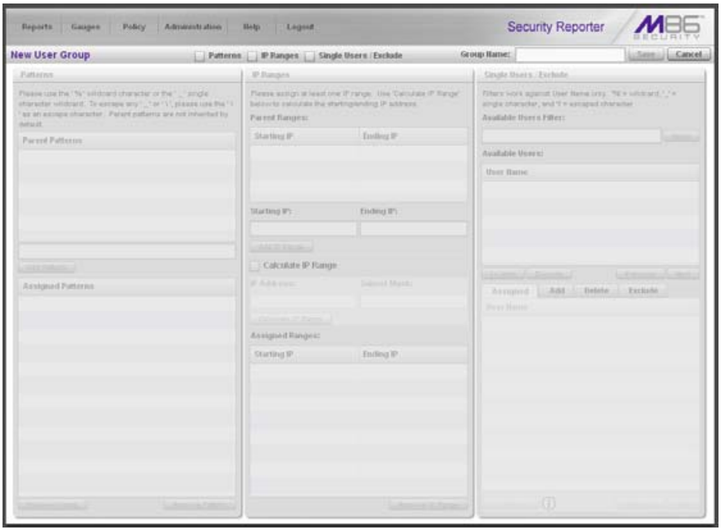


Fig. 3:1-3 New User Group panel

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

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

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

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

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

Patterns frame

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

Add a new pattern

To add a pattern to the new user group:

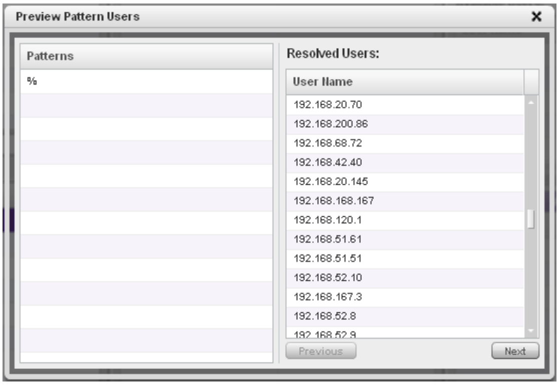
1. Do one of the following:
   - To add a pattern included in the base group, select the pattern from the Parent Patterns box to display that pattern in the field below.
   - To add a new pattern, enter the pattern in the field beneath the Parent Patterns box. For example: Enter *200.10.100.3%* to include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

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

View users resolved by the pattern

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

1. Select the pattern from the Assigned Patterns list box.
2. Click **Preview Users** to open the Preview Pattern Users pop-up window that shows the Patterns frame to the left and the Resolved Users frame to the right:



Preview Pattern Users

Patterns
%

Resolved Users:

User Name
192.168.20.70
192.168.200.86
192.168.68.72
192.168.42.40
192.168.20.145
192.168.168.167
192.168.120.1
192.168.51.61
192.168.51.51
192.168.52.10
192.168.167.3
192.168.52.8
192.168.52.9

Fig. 3:1-4 Add user group Patterns, Preview Pattern Users

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

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

Remove a pattern

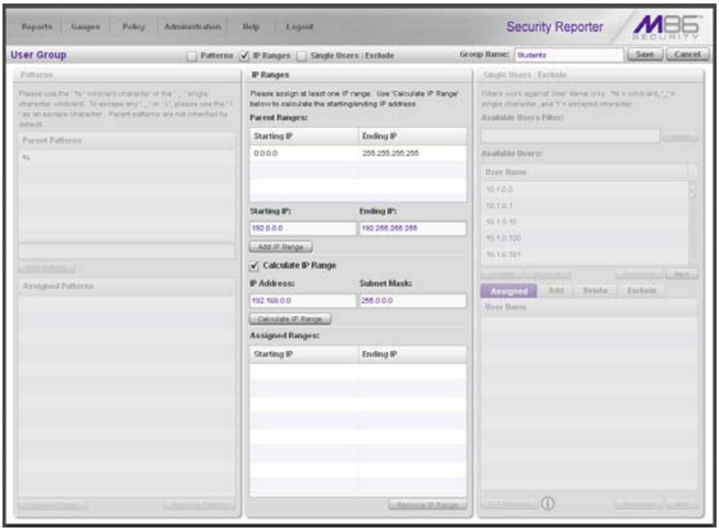
To remove a pattern in the Assigned Patterns list box:

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

IP Ranges frame

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

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



User Group □ Patterns ☑ IP Ranges □ Single Users / Exclude Group Name: Students

IP Ranges

Please assign at least one IP range. Use 'Calculate IP Range' below to calculate the starting/ending IP address.

Parent Ranges:

Starting IP	Ending IP
0.0.0.0	255.255.255.255

Starting IP: 192.0.0.0 Ending IP: 192.255.255.255

☑ Calculate IP Range

IP Address: 192.168.0.0 Subnet Mask: 255.0.0.0

Assigned Ranges:

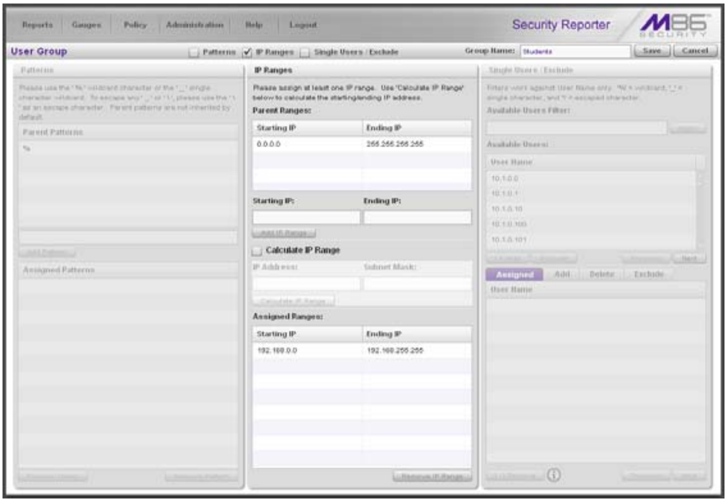
Starting IP	Ending IP

Fig. 3:1-5 Add user group, IP Ranges frame

Specify an IP range

To add an IP address range:

1. Do one of the following:
   - To make a selection from Parent Ranges, click the row in the Parent Ranges box to highlight and select that row, and also to add that Starting IP and Ending IP range in the Starting IP and Ending IP fields below. If necessary, edits can be made to these fields.
   - To add an IP address range without selecting from the Parent Ranges frame:
     a. Enter the **Starting IP** address.
     b. Enter the **Ending IP** address.
   - To calculate an IP address range:
     a. Click the **Calculate IP Range** checkbox to activate the IP Address and Subnet Mask fields below.
     b. Enter the **IP Address**.
     c. Enter the **Netmask** which activates the Calculate Range button.
     d. Click **Calculate IP Range** to display the Starting IP and Ending IP in the fields above.
2. Click **Add IP Range** to include that IP range in the Assigned Ranges list box below:



User Group

□ Patterns ☑ IP Ranges □ Single Users / Exclude

Group Name: Students

IP Ranges

Please assign at least one IP range. Use 'Calculate IP Range' below to calculate the starting/ending IP address.

Parent Ranges:

Starting IP	Ending IP
0.0.0.0	255.255.255.255

Starting IP: Ending IP:

□ Calculate IP Range

IP Address: Subnet Mask:

Assigned Ranges:

Starting IP	Ending IP
192.168.0.0	192.168.255.255

Single Users / Exclude

Available Users Filter:

Available Users:

User Name
10.1.0.0
10.1.0.1
10.1.0.10
10.1.0.100
10.1.0.101

Fig. 3:1-6 Add user group, IP range added

Remove an IP address range

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

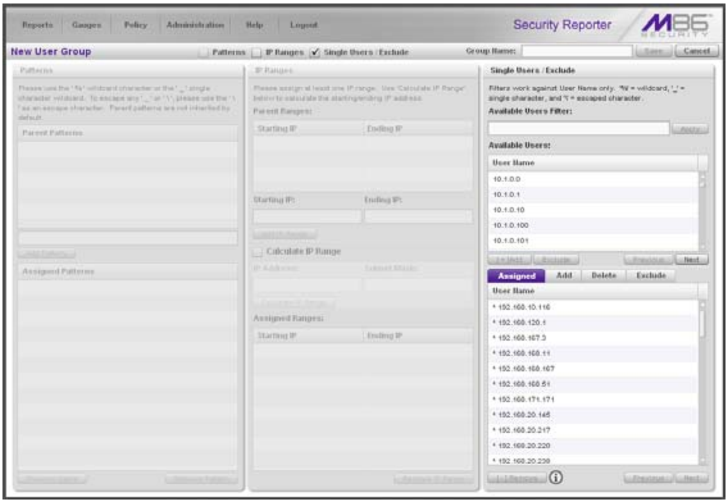
1. Click the row to highlight and select it; this action activates the Remove IP Range button below.
2. Click **Remove IP Range** to remove the IP address range from the list box.

Single Users/Exclude frame

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

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

*A user name preceded by an asterisk (*) indicates an auto-assigned user that can only be removed by adjusting the pattern or IP range for that user's group.*



Filters work against User Name only. '%' = wildcard, '_' = single character, and '\' = escaped character.

User Name
10.1.0.0
10.1.0.1
10.1.0.10
10.1.0.100
10.1.0.101

User Name
* 192.168.10.116
* 192.168.120.1
* 192.168.167.3
* 192.168.168.11
* 192.168.168.167
* 192.168.168.51
* 192.168.171.171
* 192.168.20.145
* 192.168.20.217
* 192.168.20.220
* 192.168.20.230

Fig. 3:1-7 Add user group, Single Users frame

Add one or more individual users

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

Use the filter to narrow Available Users results

To use the **Available Users Filter**:

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

Select users to add to the Assigned Users list

To make selections from the Available Users box:

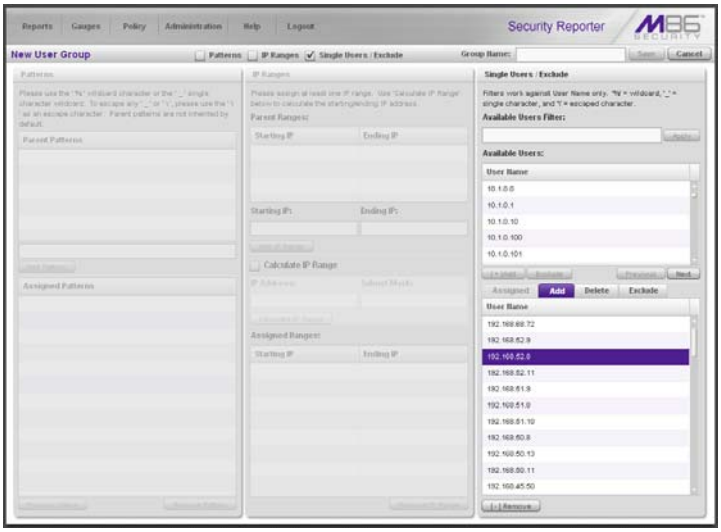
1. Select one or more IPs from the list to highlight the record(s).
2. Click **[+] Add** to include the selected user(s) in the Add tab.

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

Remove users from the Add tab

To remove users from this user group:

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



Please use the '%' wildcard character or the '_' single character wildcard. To escape any '_' or '\', please use the '\' as an escape character. Parent patterns are not inherited by default.

Please assign at least one IP range. Use 'Calculate IP Range' below to calculate the starting/ending IP address.

Filters work against User Name only. '%' = wildcard, '_' = single character, and '\' = escaped character.

Available Users: 10.1.0.0, 10.1.0.1, 10.1.0.10, 10.1.0.100, 10.1.0.101

Add: 192.168.68.72, 192.168.62.9, 192.168.52.8, 192.168.52.11, 192.168.61.9, 192.168.51.8, 192.168.51.10, 192.168.60.8, 192.168.50.13, 192.168.50.11, 192.168.45.50

Fig. 3:1-8 Add user group, remove user from Add tab

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

Edit a User Group

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

To edit a user group:

1. From the main User Groups panel, select the user group from the list in the User Groups frame.
2. Click **Edit** to display the User Group panel showing activated frames—i.e. if the Patterns frame had settings made in it, that frame is activated; if the Single Users frame was the only frame with settings made in it, that frame is activated. Any frame without settings made in it displays greyed-out.
3. Make any of these edits:
   - To make entries in a frame that is not yet activated, click the available checkbox to activate that frame: **Patterns**, **IP Ranges**, **Single Users/Exclude**.
   - Make any of these edits in a frame:
     - Patterns frame - add or remove a pattern.
     - IP Ranges frame - add or remove an IP address range.
     - Single Users/Exclude frame - add or remove one or more users.

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

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

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

Rebuild the User Group

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

1. In the User Groups panel, select the user group to be rebuilt.
2. Click **Rebuild** to initiate the rebuild process for that user group.
3. After a few minutes, click the **Refresh** button to refresh the display in the panel. Note that the Last Rebuilt column for user group you rebuilt now displays the date and time of the rebuild.

Delete a User Group

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

To delete a user group:

1. In the User Groups panel, select the user group from the User Groups list.
2. Click **Delete** to open the Confirm dialog box with the message: "Are you sure you want to delete this user group?"

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

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

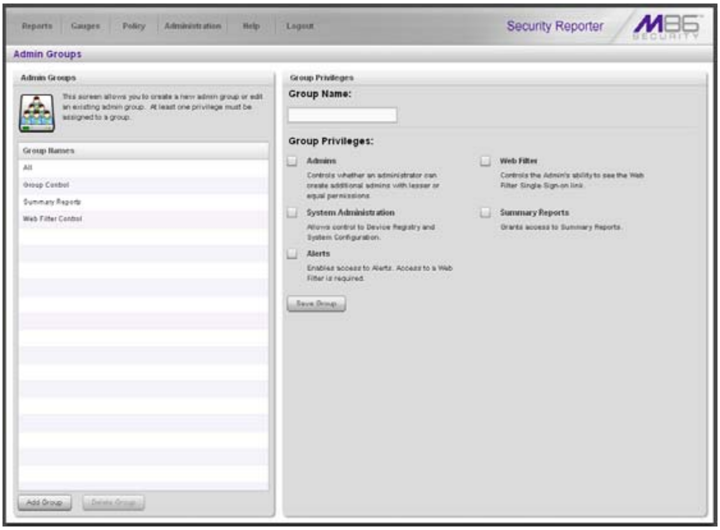
3. Click **Yes** to close the dialog box, and to remove the user group from the User Groups list.

Admin Groups panel

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

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

In the navigation toolbar, mouse over the Administration menu link and select **Admin Groups** to open the Admin Groups panel, comprised of the Admin Groups frame to the left and the Group Privileges frame to the right:



This screen allows you to create a new admin group or edit an existing admin group. At least one privilege must be assigned to a group.

□ Admins
Controls whether an administrator can create additional admins with lesser or equal permissions.

□ System Administration
Allows control to Device Registry and System Configuration.

□ Alerts
Enables access to Alerts. Access to a Web Filter is required.

□ Web Filter
Controls the Admin's ability to see the Web Filter Single Sign-on link.

□ Summary Reports
Grants access to Summary Reports.

Fig. 3:1-9 Admin Groups panel

***NOTE**: Any administrator groups previously set up display in the Group Names list box in the Admin Groups frame.*

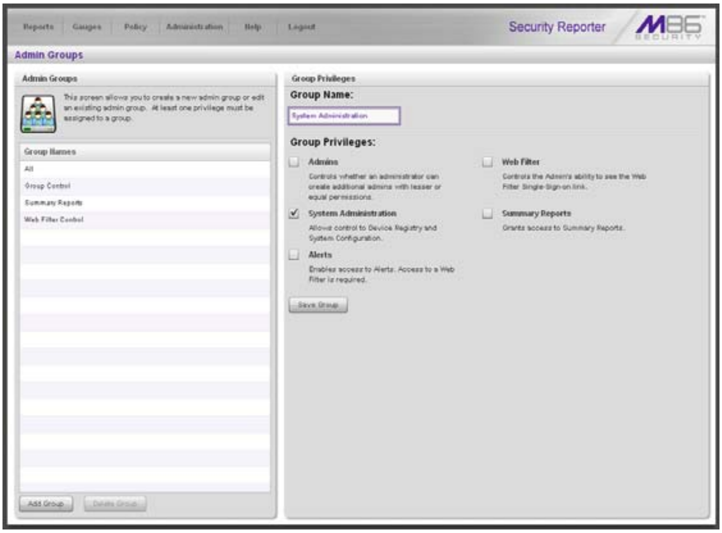
In this panel, you can add an administrator group, view information for an existing administrator group, and modify or delete that group, as necessary.

Add a Group

1. At the bottom of the Admin Groups frame, Click **Add Group**.
2. At the top of the Group Privileges frame, type in up to 32 characters for the **Group Name**.

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

3. In the Group Privileges section, click the appropriate checkbox(es) to specify the type of access the administrator group will be granted on the SR console or its related devices:



This screen allows you to create a new admin group or edit an existing admin group. At least one privilege must be assigned to a group.

Group Name: System Administration

Group Privileges:

□ Admins
Controls whether an administrator can create additional admins with lesser or equal permissions.

☑ System Administration
Allows control to Device Registry and System Configuration.

□ Alerts
Enables access to Alerts. Access to a Web Filter is required.

□ Web Filter
Controls the Admin's ability to see the Web Filter Single-Sign-on link.

□ Summary Reports
Grants access to Summary Reports.

Fig. 3:1-10 Add a new Group

- **Admins** - This privilege lets the administrator create another administrator account with equal or lesser privileges as that administrator.
- **System Administration** - This privilege gives the administrator access to the Device Registry and System Configuration administrator console.
- **Alerts** - This privilege lets the administrator manage alerts that indicate if URL or bandwidth gauges (driven by end user Internet/network activity) are close to—or have reached—their established upper thresholds.
- **Web Filter** - This privilege gives the administrator access to the Web Filter via a link in the Administration menu.
- **Summary Reports** - This privilege lets the administrator access Summary Reports from the Report menu.

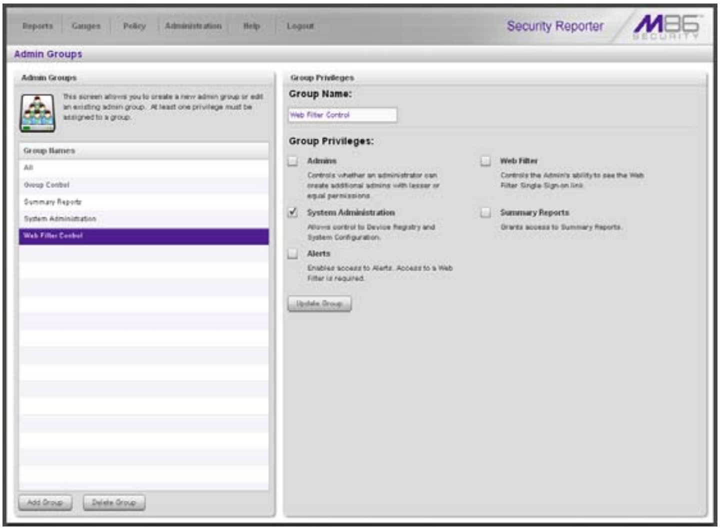
TIP*: To remove a checkmark from any active checkbox containing a checkmark, click the checkbox.*

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

View, Edit an Admin Group’s Permissions

View Admin Group settings

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



Admin Groups

Admin Groups

This screen allows you to create a new admin group or edit an existing admin group. At least one privilege must be assigned to a group.

Group Names
- All
- Group Control
- Summary Reports
- System Administration
- Web Filter Control

Group Privileges

Group Name: Web Filter Control

Group Privileges:

□ Admins
Controls whether an administrator can create additional admins with lesser or equal permissions.

☑ System Administration
Allows control to Device Registry and System Configuration.

□ Alerts
Enables access to Alerts. Access to a Web Filter is required.

□ Web Filter
Controls the Admin's ability to see the Web Filter Single Sign-on link.

□ Summary Reports
Grants access to Summary Reports.

Fig. 3:1-11 Admin Groups group selections

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

Edit Admin Group settings

1. In the Group Privileges frame, perform any of the following actions:
   - Modify the **Group Name**
   - Add functions to be monitored by the administrator group
   - Remove functions to be monitored by the administrator group
2. Click **Update Group** to save your settings and to clear all selections in the Group Privileges frame.

Delete an Administrator Group

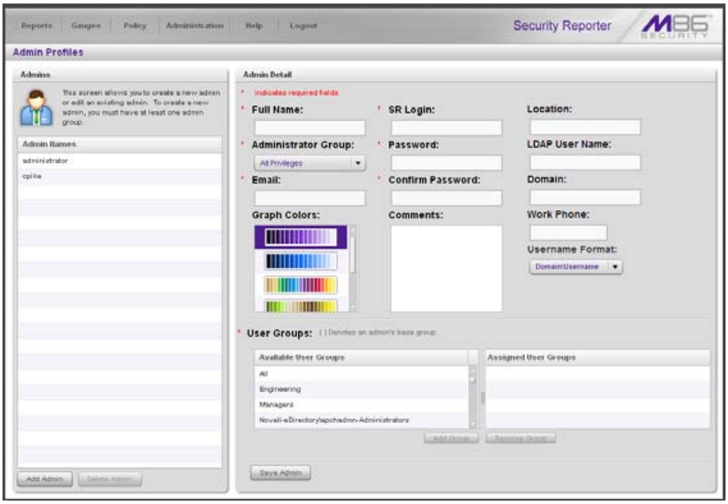
1. In the Group Names list box, click the name of the administrator group to highlight the group name, activate all buttons, and to populate the Group Privileges frame with previously-saved settings.
2. Click **Delete Group** to open the Confirm dialog box with the message: “Are you sure you want to delete this admin group?”
3. Click **Yes** to close the dialog box and to remove the administrator group from the Group Names list box.

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

Admin Profiles panel

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

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



This screen allows you to create a new admin or edit an existing admin. To create a new admin, you must have at least one admin group.

Admin Names: administrator, cpike

Administrator Group: All Privileges

Username Format: Domain\Username

User Groups: ( ) Denotes an admin's base group

Available User Groups: All, Engineering, Managers, Novell-eDirectory/apchadmin-Administrators

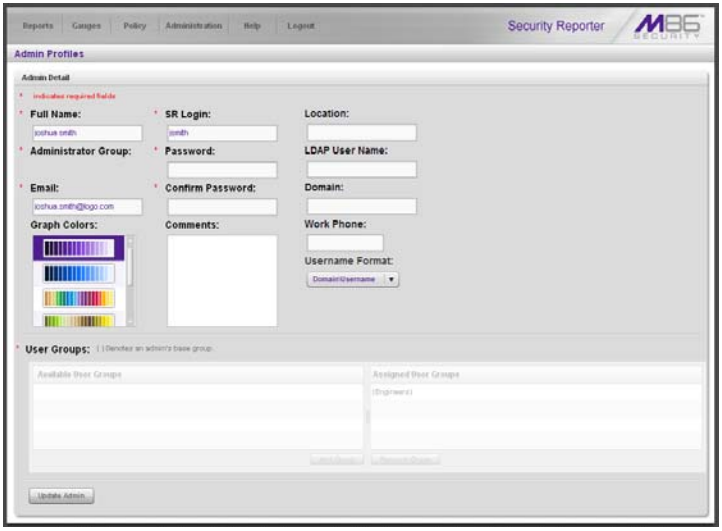
Fig. 3:1-12 Admin Profiles panel, global administrator view

If logged in as the global administrator, or as a group administrator with privileges to create other administrator profiles, at the left side of this panel, the Admin Names list box in the Admins frame displays SR Login IDs of administrator accounts previously set up in this panel (see Fig. 3:2-4).

NOTE*: In addition to seeing account IDs set up and saved by the administrator in this panel, a global administrator will also see the SR Login ID established during the wizard hardware installation process.*

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

If logged in as a group administrator without privileges to create other administrator profiles, only the Admin Detail panel displays, as in the sample screen below:



* indicates required fields

* Full Name: joshua smith

* SR Login: jsmith

Location:

* Administrator Group:

* Password:

LDAP User Name:

* Email: joshua.smith@logo.com

* Confirm Password:

Domain:

Graph Colors:

Comments:

Work Phone:

Username Format: Domain\Username

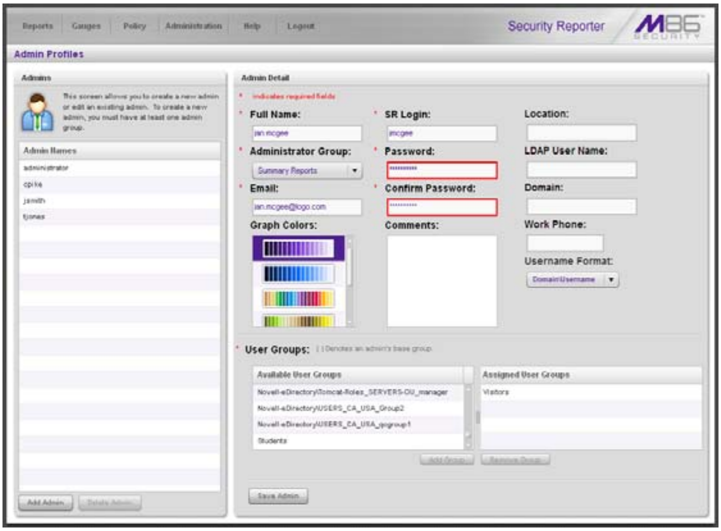
* User Groups: ( ) Denotes an admin's base group.

Available User Groups	Assigned User Groups
	(Engineers)

Fig. 3:1-13 Admin Profiles panel, group administrator view

Add an Administrator Profile

1. If privileges are granted for you to create a group administrator profile, at the bottom of the Admins frame, click **Add Admin** to clear and reset the Admin Detail frame.
2. In the Admin Detail frame, make the following entries or selections as appropriate:



Admin Profiles

Admins

This screen allows you to create a new admin or edit an existing admin. To create a new admin, you must have at least one admin group.

Admin Names
administrator
cpike
jsmith
tjones

Admin Detail

* indicates required fields

* Full Name: jan mcgee

* Administrator Group: Summary Reports

* Email: jan.mcgee@logo.com

Graph Colors:

* SR Login: jmcgee

* Password: **********

* Confirm Password: **********

Comments:

Location:

LDAP User Name:

Domain:

Work Phone:

Username Format: Domain\Username

* User Groups: [ ] Denotes an admin's base group.

Available User Groups	Assigned User Groups
Novell-eDirectory\Tomcat-Roles_SERVERS-OU_manager	Visitors
Novell-eDirectory\USERS_CA_USA_Group2	
Novell-eDirectory\USERS_CA_USA_qpgroup1	
Students	

Fig. 3:1-14 New administrator information entered but not yet saved

- Type in the group administrator’s **Full Name**.
- Select the **Administrator Group** (previously set up in the Admins Group panel) from the available choices in the pull-down menu.
- Type in the group administrator’s **Email** address.
- Optional: Select another report color scheme from the available **Graph Colors** choices.
- Type in the **SR Login** ID the group administrator will use to access the SR user interface. This entry will display in the Admin Names list when the record is saved.
- Type in the **Password** the group administrator will use in conjunction with the SR Login ID, and enter that same password again in the **Confirm Password** field. These entries display as asterisks for security purposes.
- Optional: Type in any **Comments** to be associated with the group administrator’s account.

- Optional: Type in identifying information about the group administrator's physical office **Location**.
- Optional: If the administrator has an Active Directory LDAP account, user name, and domain, type in the alphanumeric group administrator's **LDAP User Name** exactly as set up on the Active Directory domain in which he/she is registered.
- Optional: If an entry was made in the LDAP User Name field, type in the exact characters for the LDAP Active Directory **Domain** name in which the group administrator is registered.

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

- Optional: Type in the group administrator's **Work Phone** number, without entering special characters such as parentheses ( ), a hyphen (-), a period (.), or a left slash (/).
- Optional: If necessary, specify the **Username Format** used on the LDAP server by making a selection from the available choices—Domain\Username, Username\Domain, Username, Domain.

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

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

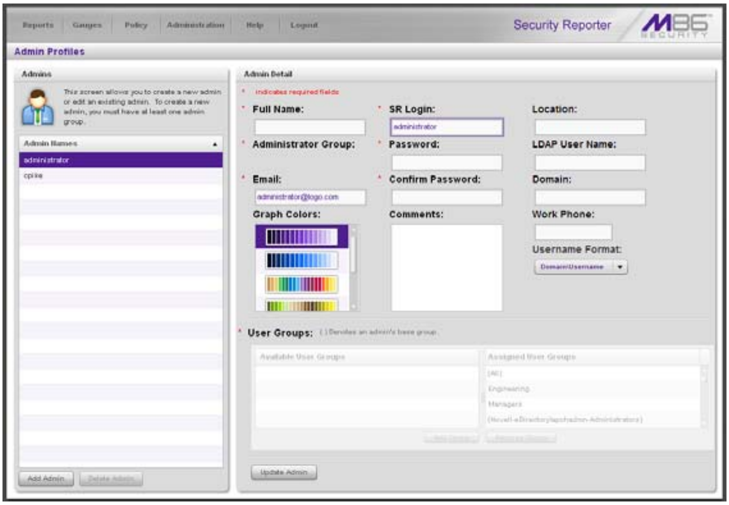
***TIP**: To remove any user group from the Assigned User Groups list box, select the user group(s), and then click Remove Group to remove the user group(s).*

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

View, Edit Admin Detail

View Admin Details

For an account with permissions to create other administrator profiles, in the Admin Names list box, select the administrator's SR Login ID to populate that user's profile information in the Admin Detail frame:



This screen allows you to create a new admin or edit an existing admin. To create a new admin, you must have at least one admin group.

Admin Names: administrator, cpike

* indicates required fields

* Full Name:

* SR Login: administrator

Location:

* Administrator Group:

* Password:

LDAP User Name:

* Email: administrator@logo.com

* Confirm Password:

Domain:

Work Phone:

Username Format: Domain\Username

* User Groups: ( ) Denotes an admin's base group.

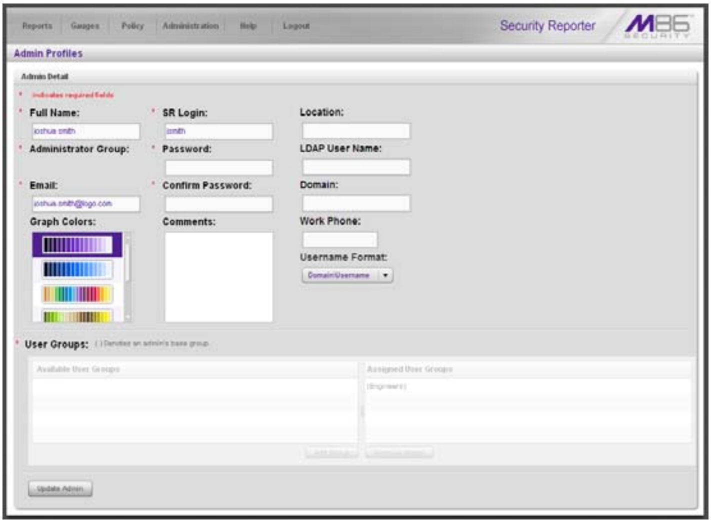
Available User Groups

Assigned User Groups: [All], Engineering, Managers, (Novell-eDirectory/ldapadmin-Administrators)

Fig. 3:1-15 Admin Names selection

***NOTE**: Administrator accounts with permissions to create other user profiles display at minimum the Email address, SR Login ID, LDAP Username, and—greyed-out in the Assigned User Groups list box—all user groups that would be available in the Available User Groups box.*

For an account without permission to create other user profiles, the Admin Detail frame displays at minimum the Full Name, Email address, SR Login ID, and User Groups selection greyed-out:



* Indicates required fields

* Full Name: joshua smith

* SR Login: jsmith

Location:

* Administrator Group:

* Password:

LDAP User Name:

* Email: joshua.smith@logo.com

* Confirm Password:

Domain:

Graph Colors:

Comments:

Work Phone:

Username Format: Domain\Username

* User Groups: ( ) Denotes an admin's base group

Available User Groups

Assigned User Groups: (Engineers)

Fig. 3:1-16 Admin Detail frame

Edit Account Info

1. In the populated Admin Detail frame:

   - The following information can be updated: Full Name, Email address, Graph Colors, SR Login ID, and Password and Confirm Password entries.
   - The following information can be added, modified, or deleted: Comments, Location information, and LDAP User Name or Domain name—the latter two fields are available if using LDAP—Work Phone number, and Username Format.
   - An administrator account with permissions to create other user accounts also has the ability to modify the Administrator Group selection, and User Groups selections.

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

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

Delete Admin

Only an administrator with privileges to create another user profile can delete a user profile he/she created.

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

1. In the Admin Names list box, select the group administrator’s SR Login ID.
2. Click **Delete Admin** to open the Confirm dialog box with the message: “Are you sure you want to delete this admin?”

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

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

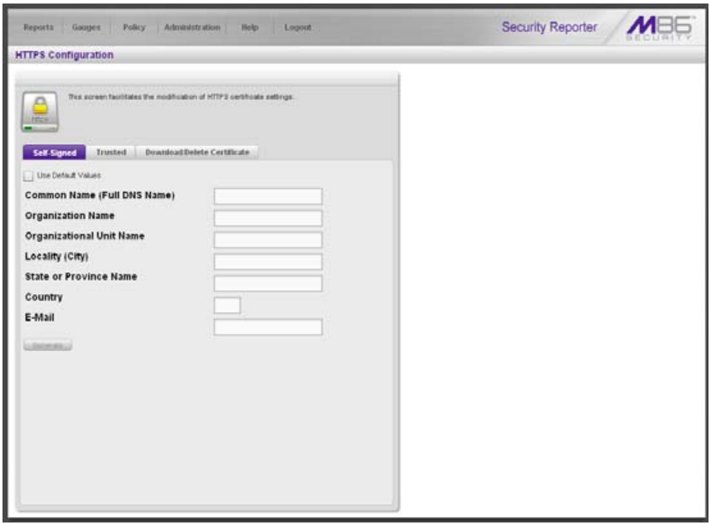
Chapter 2: Database Management

The following panels from the Administration menu of the Report Manager are described in this chapter: HTTPS Configuration, User Profiles, Activity View, Device Registry, Database Processes List, Server Information, and Reset to Factory Defaults.

HTTPS Configuration panel

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

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



This screen facilitates the modification of HTTPS certificate settings.

□ Use Default Values

Common Name (Full DNS Name)

Organization Name

Organizational Unit Name

Locality (City)

State or Province Name

Country

E-Mail

Fig. 3:2-1 HTTPS Configuration panel, Self-Signed tab

Generate a Self-Signed Certificate for the SR

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

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

1. Do the following:
   - click the checkbox corresponding to **Use Default Values** to grey-out the tab, or
   - make entries in these fields:

     a. **Common Name (Full DNS Name)** - Host name of the server, such as ***logo.com***.

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

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

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

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

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

     g. **E-Mail** - Your email address.
2. Click **Create** to generate the SSL certificate to be stored on the SR, and to restart the Report Manager. Hereafter, group administrators must accept the security certificate on their workstations in order for their machines to communicate with the Report Manager and/or System Configuration administrator console.

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

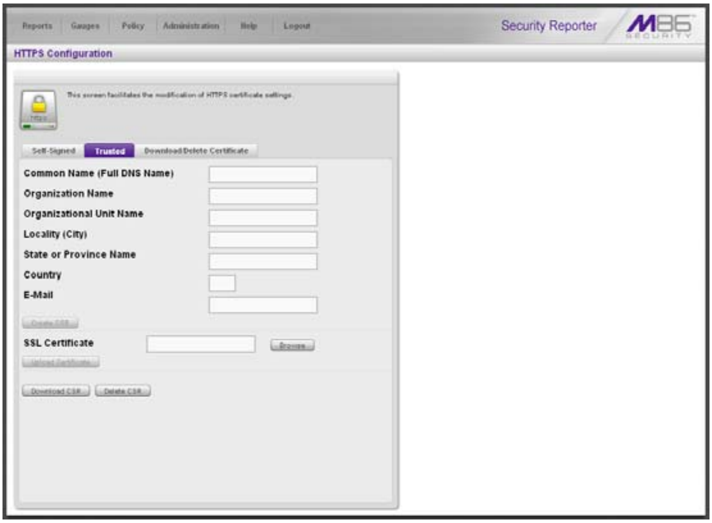
Create, Upload a Third Party Certificate

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

Step A: Create a CSR

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

1. Click the Trusted tab:



This screen facilitates the modification of HTTPS certificate settings.

Common Name (Full DNS Name)

Organization Name

Organizational Unit Name

Locality (City)

State or Province Name

Country

E-Mail

SSL Certificate

Fig. 3:2-2 HTTPS Configuration panel, Trusted tab

2. Make entries in these fields:

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

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

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

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

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

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

g. **E-Mail** - Your email address.

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

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

Step B: Download the CSR, Submit to Agency

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

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

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

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

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

Step C: Upload the Signed SSL Certificate to SR

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

1. Launch Notepad on your machine.
2. Copy and paste the contents of the certificate into Notepad in the following order:

   a. SSL certificate

   b. Intermediate certificate(s)—this step is not required if you have a Single Root SSL Certificate

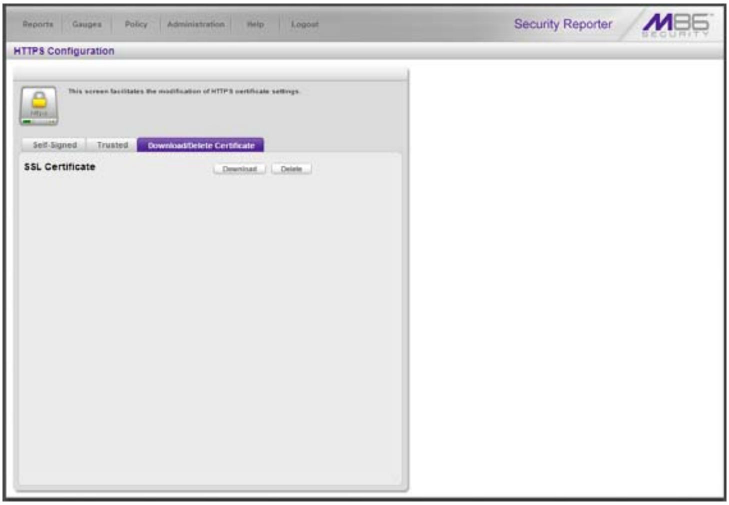
   c. Root certificate
3. Save the contents of the Notepad file with a .cer extension.
4. In the Trusted tab, go to the **SSL certificate** field and click **Browse** to find the .cer file you just saved.
5. Click **Upload** to load the certificate on the SR.

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

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

Download, Delete a Third Party Certificate

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



This screen facilitates the modification of HTTPS certificate settings.

Fig. 3:2-3 HTTPS Configuration panel, Trusted tab

Download the SSL Certificate

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

The certificate can now be distributed to group administrator workstations.

Delete the SSL Certificate

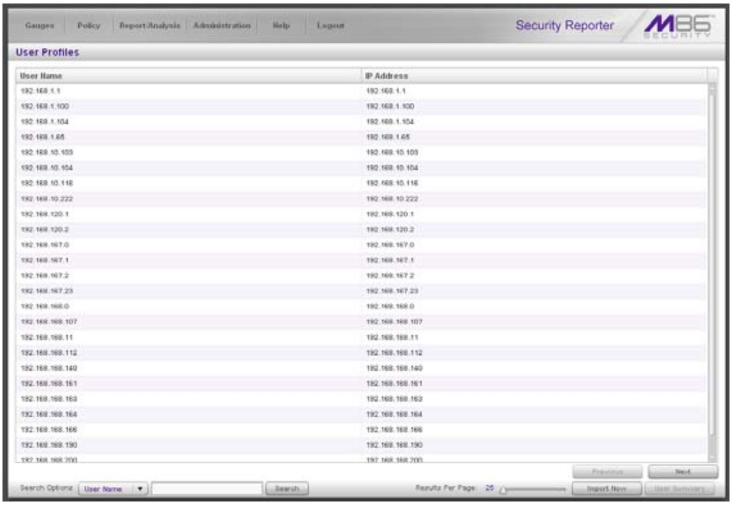
To delete the third party certificate from the SR, go to the Download/Delete Certificate tab and click **Delete** to remove the certificate from the SR.

User Profiles panel

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

***NOTE**: The User Profiles panel is available to a group administrator only if permissions were granted by the administrator who set up his/her account.*

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



User Profiles

User Name	IP Address
192.168.1.1	192.168.1.1
192.168.1.100	192.168.1.100
192.168.1.104	192.168.1.104
192.168.1.65	192.168.1.65
192.168.10.103	192.168.10.103
192.168.10.104	192.168.10.104
192.168.10.118	192.168.10.116
192.168.10.222	192.168.10.222
192.168.120.1	192.168.120.1
192.168.120.2	192.168.120.2
192.168.167.0	192.168.167.0
192.168.167.1	192.168.167.1
192.168.167.2	192.168.167.2
192.168.167.23	192.168.167.23
192.168.168.0	192.168.168.0
192.168.168.107	192.168.168.107
192.168.168.11	192.168.168.11
192.168.168.112	192.168.168.112
192.168.168.140	192.168.168.140
192.168.168.161	192.168.168.161
192.168.168.163	192.168.168.163
192.168.168.164	192.168.168.164
192.168.168.166	192.168.168.166
192.168.168.190	192.168.168.190
192.168.168.200	192.168.168.200

Search Options: User Name ▾

Results Per Page: 25

Fig. 3:2-4 User Profiles panel

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

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

Search the User Database

1. Specify search criteria by making a selection from the **Search Options** pull-down menu:
   - **User Name -** This selection performs a search by an end user's user name.
   - **IP Address -** This selection performs a search by an end user's IP address.
2. Make an entry in the blank field to the right:
   - If User Name was selected, enter a user name
   - If IP Address was selected, enter an IP address.
3. Click **Search** to display a record that matches your criteria.

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

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

View End User Activity

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

Activity View panel

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

In the navigation toolbar, mouse over the Administration menu link and select **Activity View** to display the Activity View panel:

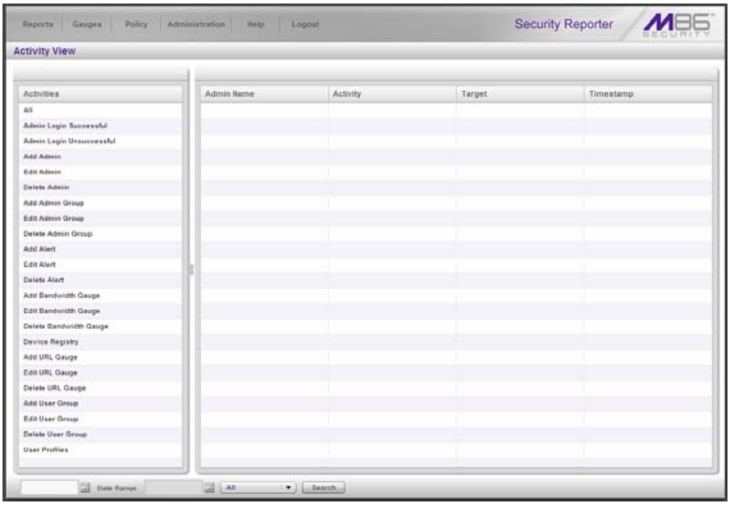


Fig. 3:2-5 Activity View panel

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

Perform a Search on a Specified Activity

To perform a search on a specified activity:

1. Select the type of Activity from available choices in the list: All, Admin Login Successful, Admin Login Unsuccessful, Add Admin, Edit Admin, Delete Admin, Add Admin Group, Edit Admin Group, Delete Admin Group,

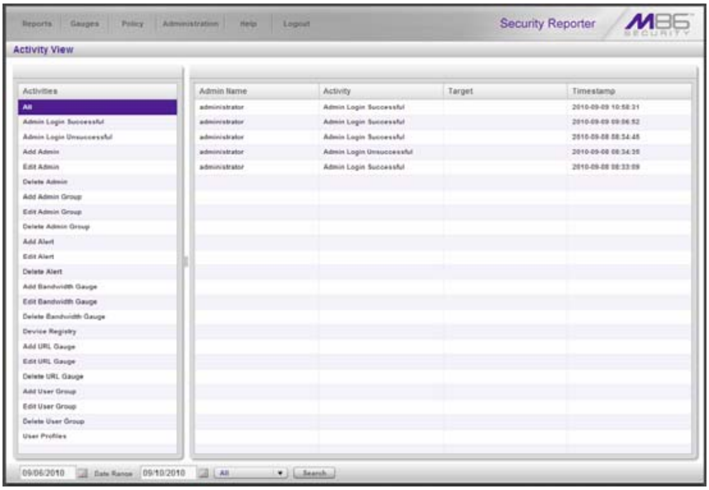
Add Alert, Edit Alert, Delete Alert, Add Bandwidth Gauge, Edit Bandwidth Gauge, Delete Bandwidth Gauge, Device Registry, Add URL Gauge, Edit URL Gauge, Delete URL Gauge, Add User Group, Edit User Group, Delete User Group, User Profiles.

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

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

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

3. Click the starting date to select it and to close the calendar pop-up window. This action populates the field to the left of the calendar icon with the selected date.
4. Click the 📅 calendar icon on the right to open the larger calendar for the current month, with today's date highlighted.
5. Click the ending date to select it and to close the calendar pop-up window. This action populates the field to the left of the calendar icon with the selected date.
6. To view the activity of a specified administrator, select the user name from the pull-down menu.
7. Click **Search** to display the specified records for the selected dates in the results list:



Admin Name	Activity	Target	Timestamp
administrator	Admin Login Successful		2010-09-09 10:58:31
administrator	Admin Login Successful		2010-09-09 09:06:52
administrator	Admin Login Successful		2010-09-08 08:34:45
administrator	Admin Login Unsuccessful		2010-09-08 08:34:35
administrator	Admin Login Successful		2010-09-08 08:33:09

Fig. 3:2-6 Activity View results

Search results

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

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

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

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

Device Registry panel

The Device Registry panel is used for viewing information about devices connected to the SR, synchronizing the SR with user groups and libraries from the source Web Filter, editing M86 appliance criteria, and adding or deleting an additional Web Filter, or adding/deleting an SWG or LDAP server from the registry.

This function is available to a group administrator only if permissions were granted by the administrator who set up his/her account, as detailed in Admins Group panel in Chapter 1.

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

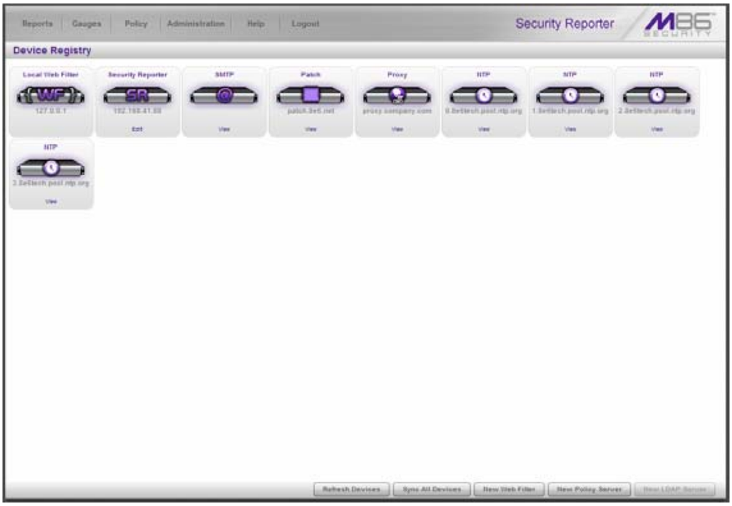


Fig. 3:2-7 Device Registry

This panel is comprised of icons representing devices set up to communicate with the WFR. Except for the source Web Filter device, all other device icons include at least one link describing the action(s) that can be performed on that device: View, Edit, Delete.

At the bottom of the panel the following buttons display:

- **Refresh Devices** - Click this button if any icon representing a device does not properly display in the user interface.
- **Sync All Devices -** Click this button to synchronize Web Filter library Categories, and/or User Groups.
- **New Web Filter** - Click this button to add a Web Filter to the device registry.
- **New Policy Server** (enabled only if an SWG has not already been added) **-** Click this button to add an SWG server to the device registry.
- **New LDAP Server** (enabled only if an SWG has been added) **-** Click this button to add an LDAP server to the device registry.

Removing/adding Web Filter, SWG devices

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

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

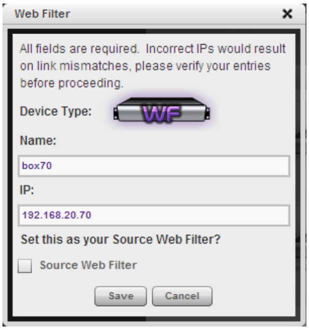
⚠ ***WARNING**: For any scenario specified above that would result in data being purged from the Security Reporter, M86 recommends backing up and saving current SR data off the server before adding or removing the designated device from the Device Registry. Please refer to the Backup screen sub-section from Chapter 2 of the SR System Configuration Section of this portion of the User Guide for information about backing up data.*

Web Filter Device Maintenance

***NOTE**: Web Filter device criteria is only accessible on a Web Filter added after the wizard hardware installation process.*

View, edit Web Filter device criteria

1. Go to the Web Filter server icon in the Device Registry panel and click **Edit** to open the Web Filter pop-up window:



Web Filter

All fields are required. Incorrect IPs would result on link mismatches, please verify your entries before proceeding.

Device Type: WF

Name: box70

IP: 192.168.20.70

Set this as your Source Web Filter?

□ Source Web Filter

Fig. 3:2-8 Web Filter pop-up window

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

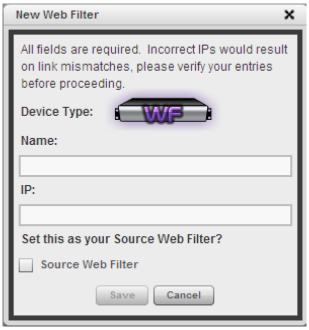
2. Edit any of the following:
   - **Name** - Name of the application.
   - **IP** - IP address of the server.
   - **Source Web Filter** - If this checkbox is not populated and the Web Filter will now be the source Web Filter, click in the checkbox to place a check mark here.

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

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

Add a Web Filter to the device registry

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



All fields are required. Incorrect IPs would result on link mismatches, please verify your entries before proceeding.

Fig. 3:2-9 New Web Filter pop-up window

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

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

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

Delete a Web Filter from the device registry

1. Go to the Web Filter server icon in the Device Registry panel and click **Delete** to open the CONFIRM dialog box with the message: “Are you sure you want to delete this device?”

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

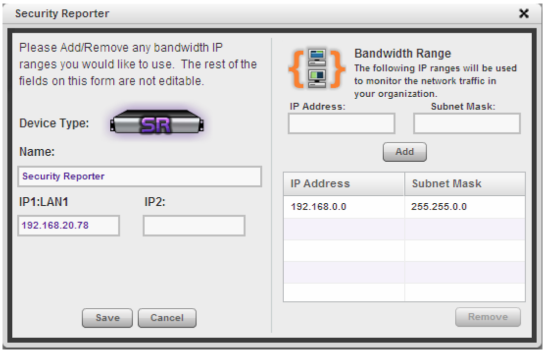
2. Click **Yes** to delete the Web Filter device from the registry, and to remove the Web Filter server icon from the Device Registry panel.

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

Security Reporter Maintenance

View SR device criteria

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



Security Reporter

Please Add/Remove any bandwidth IP ranges you would like to use. The rest of the fields on this form are not editable.

Device Type: SR

Name: Security Reporter

IP1:LAN1: 192.168.20.78

IP2:

Bandwidth Range

The following IP ranges will be used to monitor the network traffic in your organization.

IP Address:

Subnet Mask:

IP Address	Subnet Mask
192.168.0.0	255.255.0.0

Fig. 3:2-10 Security Reporter pop-up window

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

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

Add, remove a bandwidth range

1. Do the following in the Bandwidth Range section:
   - To add a bandwidth IP address range:
     a. Type in the **IP Address**.
     b. Type in the **Subnet Mask**.
     c. Click **Add** to add the bandwidth IP range in the list box.
   - To remove a bandwidth IP address range:
     a. Select the IP address range from the list box; this action activates the Remove button.
     b. Click **Remove** to remove the IP address range.

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

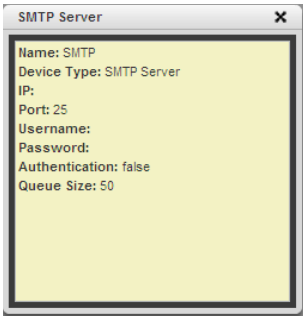
2. After making all modifications in this window, click **Save** to save your edits and to close the pop-up window.

View Other Device Criteria

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

View SMTP device criteria

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



SMTP Server

Name: SMTP
Device Type: SMTP Server
IP:
Port: 25
Username:
Password:
Authentication: false
Queue Size: 50

Fig. 3:2-11 SMTP window

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

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

View Patch Server device criteria

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

View Proxy Server device criteria

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

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

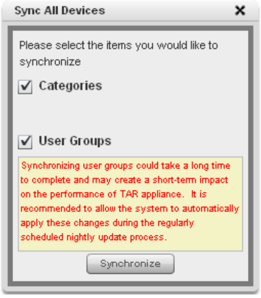
View NTP Server device criteria

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

Sync All Devices

A forced synchronization should be performed on the SR unit if any of the source Web Filter’s related devices listed in the Device Registry are updated.

1. Click **Sync All Devices** to open the Sync All Devices pop-up window:



Sync All Devices ✕

Please select the items you would like to synchronize

☑ Categories

☑ User Groups

Synchronizing user groups could take a long time to complete and may create a short-term impact on the performance of TAR appliance. It is recommended to allow the system to automatically apply these changes during the regularly scheduled nightly update process.

Fig. 3:2-12 Sync All Devices

2. Check the checkbox(es) pertaining to information to be synchronized between the Web Filter and SR devices, and to activate the Synchronize button:
   - **Categories** - Make this selection to synchronize M86 supplied library category updates and custom library categories from the source Web Filter to the SR.

- **User Groups** - Make this selection to synchronize LDAP user group information on the source Web Filter to the SR.

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

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

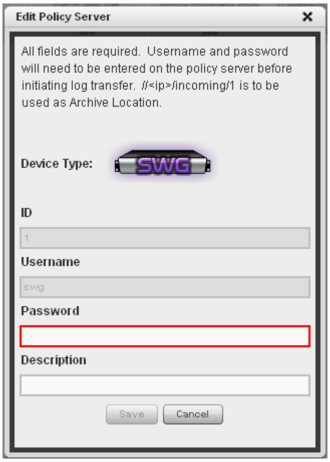
3. Click Synchronize to close the pop-up window and to begin the synchronization process.

New Policy Server Device Maintenance

NOTE: *For this software release, only one SWG can be added to the SR’s Device Registry to receive logs. However, multiple SWG policy servers can be set up to send logs to the SR, by entering the SR’s IP address in each SWG policy server’s Log Properties.*

View, edit Policy Server device criteria

1. Go to the SWG server icon in the Device Registry panel and click **Edit** to open the Edit Policy Server pop-up window:



Edit Policy Server

All fields are required. Username and password will need to be entered on the policy server before initiating log transfer. //<ip>/incoming/1 is to be used as Archive Location.

Device Type: SWG

ID

1

Username

swg

Password

Description

Fig. 3:2-13 Edit Policy Server pop-up window

The following information displays and cannot be edited: Device Type (SWG), ID, Username.

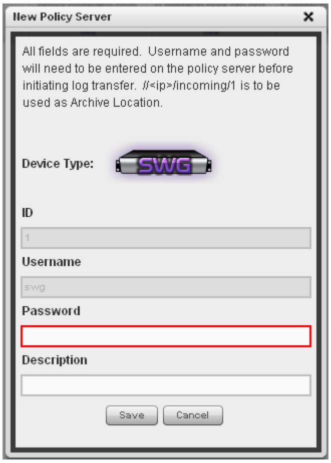
2. Edit any of the following fields:
   - **Password** - Password used to access the application.
   - **Description** - Description of the SWG server.

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

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

Add a Policy Server to the device registry

1. At the bottom of the Device Registry panel, click **New Policy Server** to open the New Policy Server pop-up window:



All fields are required. Username and password will need to be entered on the policy server before initiating log transfer. //<ip>/incoming/1 is to be used as Archive Location.

Device Type:

ID

1

Username

swg

Password

Description

Fig. 3:2-14 Add Policy Server

The following information displays and cannot be edited: Device Type (SWG), ID, Username.

2. Edit any of the following fields:
   - **Password** - Password used to access the application.
   - **Description** - Description of the SWG server.

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

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

Delete a Policy Server from the device registry

1. Go to the SWG server icon in the Device Registry panel and click **Delete** to open the CONFIRM dialog box with the message: “Are you sure you want to delete this device? This will result in all data being purged.”

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

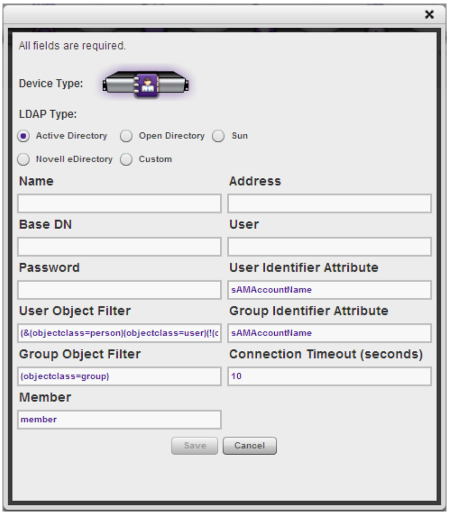
2. Click **Yes** to delete the SWG device from the registry, and to remove the SWG server icon from the Device Registry panel.

LDAP Server Device Management

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

Add an LDAP Server to the device registry

1. At the bottom of the Device Registry panel, click **New LDAP Server** to open the LDAP server pop-up window:



All fields are required.

Device Type:

LDAP Type:

● Active Directory ○ Open Directory ○ Sun

○ Novell eDirectory ○ Custom

Name

Address

Base DN

User

Password

User Identifier Attribute

sAMAccountName

User Object Filter

(&(objectclass=person)(objectclass=user)(!(c

Group Identifier Attribute

sAMAccountName

Group Object Filter

(objectclass=group)

Connection Timeout (seconds)

10

Member

member

Fig. 3:2-15 Add LDAP server

The Device Type image displays.

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

cn=Administrator,cn=Users,dc=qa,dc=local

or

cn=admin,o=logo-org

- **User Identifier Attribute** - Specify attributes used for identifying a user, if necessary
- **Group Identifier Attribute** - Specify attributes used for identifying a group, if necessary
- **Connection Timeout (seconds)** - Default is 10 seconds for connecting to the LDAP server

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

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

Import LDAP Group profiles

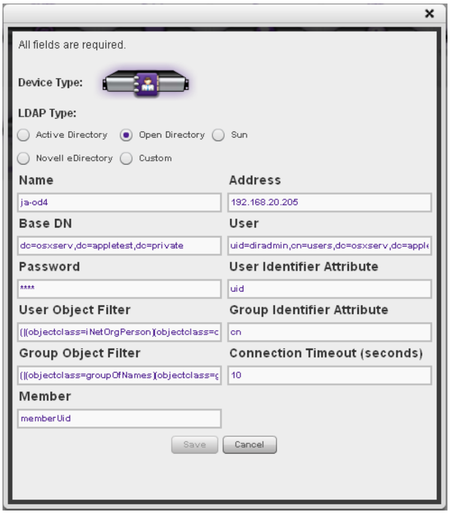
1. Go to the LDAP server icon in the Device Registry panel and click **Import** to begin importing group profiles from the LDAP server.

2. After the alert box opens to specify whether or not the LDAP group importation process was successful, click **OK** to close the pop-up box.

***TIP**: If the importation process failed, make edits in the LDAP server pop-up window and run the import process again.*

View, edit LDAP Server device criteria

1. Go to the LDAP server icon in the Device Registry panel and click **Edit** to open the pop-up window:



All fields are required.

Device Type:

LDAP Type:

○ Active Directory ● Open Directory ○ Sun

○ Novell eDirectory ○ Custom

Name: ja-od4	Address: 192.168.20.205
Base DN: dc=osxserv,dc=appletest,dc=private	User: uid=diradmin,cn=users,dc=osxserv,dc=appl
Password: ****	User Identifier Attribute: uid
User Object Filter: (|(objectclass=iNetOrgPerson)(objectclass=c	Group Identifier Attribute: cn
Group Object Filter: (|(objectclass=groupOfNames)(objectclass=g	Connection Timeout (seconds): 10
Member: memberUid	

Fig. 3:2-16 LDAP Server pop-up window

The Device Type image for the LDAP server displays, along with entries previously made and saved in this window.

2. Edit any of the fields in this pop-up window.

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

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

Delete an LDAP Server from the device registry

1. Go to the LDAP server icon in the Device Registry panel and click **Delete** to open the CONFIRM dialog box with the message: “Are you sure you want to delete this device?”

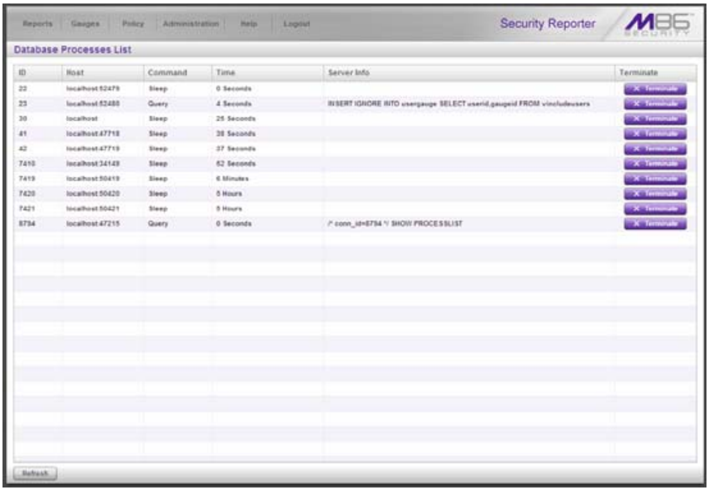
***NOTE**: Click **No** to close the dialog box.*

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

Database Processes List panel

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

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



Database Processes List

ID	Host	Command	Time	Server Info	Terminate
22	localhost:52479	Sleep	0 Seconds		X Terminate
23	localhost:52480	Query	4 Seconds	INSERT IGNORE INTO usergauge SELECT userid,gaugeid FROM vincludeusers	X Terminate
30	localhost	Sleep	25 Seconds		X Terminate
41	localhost:47718	Sleep	38 Seconds		X Terminate
42	localhost:47719	Sleep	37 Seconds		X Terminate
7410	localhost:34149	Sleep	62 Seconds		X Terminate
7419	localhost:50419	Sleep	6 Minutes		X Terminate
7420	localhost:50420	Sleep	5 Hours		X Terminate
7421	localhost:50421	Sleep	5 Hours		X Terminate
8794	localhost:47215	Query	0 Seconds	/* conn_id=8794 */ SHOW PROCESSLIST	X Terminate

Fig. 3:2-17 Database Processes List window

View Details on a Process

Each row in the list includes the following information: process identification number (ID) on the MySQL server; Host name or IP address of the server, and port connected to the database; the state of the last Command issued by the user (“Query” or “Sleep”); the amount of Time in seconds the process has remained in its current state, and SQL statement for a process currently running (Server Info). At the end of each row is the Terminate option.

***TIP**: Click the **Refresh** button to refresh the list of records.*

Terminate a Process

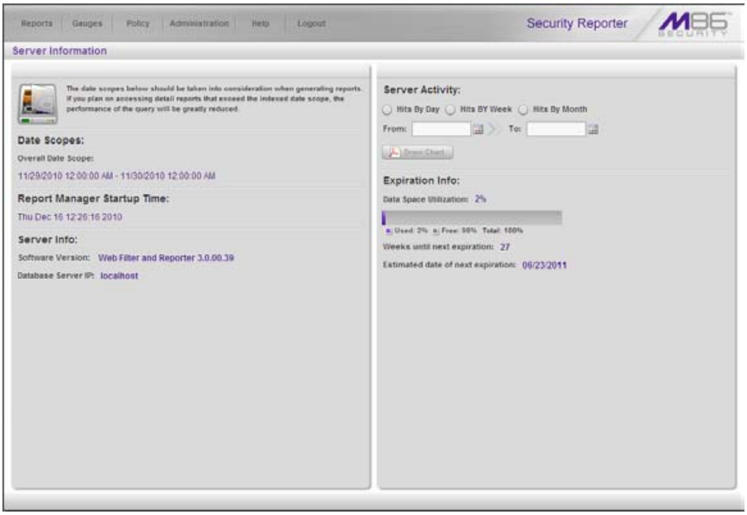
Select the process to be terminated and click **Terminate**.

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

Server Information panel

The global administrator uses the Server Information panel to obtain details about data storage on the SR Server, the time the Report Manager was last restarted, and the WFR Server’s IP address and current software version number.

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



Server Information

The date scopes below should be taken into consideration when generating reports. If you plan on accessing detail reports that exceed the indexed date scope, the performance of the query will be greatly reduced.

Date Scopes:

Overall Date Scope:

11/29/2010 12:00:00 AM - 11/30/2010 12:00:00 AM

Report Manager Startup Time:

Thu Dec 16 12:26:16 2010

Server Info:

Software Version: Web Filter and Reporter 3.0.00.39

Database Server IP: localhost

Server Activity:

○ Hits By Day ○ Hits BY Week ○ Hits By Month

From: To:

Expiration Info:

Data Space Utilization: 2%

Used: 2% Free: 98% Total: 100%

Weeks until next expiration: 27

Estimated date of next expiration: 06/23/2011

Fig. 3:2-18 Server Information panel

The panel is comprised of six sections: Mode, Date Scopes, Report Manager Startup Time, Server Info, Server Activity, and Expiration Info.

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

Mode

The Mode section displays information about the current mode in which the SR is operating: “EVALUATION” or “REGISTERED” followed by the maximum number of weeks of data storage (“MAX DATA STORAGE ‘X’ WEEKS”—in which ‘X’ represents the number of weeks).

Evaluation mode is used during the evaluation period of an SR. Since data is expired from the server in full weekly increments—from Sunday through Saturday—an evaluation period lasts three weeks by default. That is, if a newly installed SR is up and running on any day of the week after a Sunday (i.e. on a Monday through a Saturday)—and therefore would not fully cover a 14-day period—the evaluation period would be extended to the Saturday of the current week, and data would not expire until after that time period. For example, if the SR was installed on Friday, September 3, 2010, the evaluation period would run from that day until Saturday, September 18, 2010.

Registered mode pertains to an SR server that has been activated online and registered by M86 Security. An SR in registered mode will store as much data as allocated for data storage on its hard drive—and on its attached storage device, if applicable to the hardware model of the SR server. When the SR is close to reaching its maximum capacity of data storage—as determined by the SR when making its routine 30-minute check of available storage space—the oldest week of data (from Sunday through Saturday) is dropped from the database.

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

Date Scopes

The Date Scopes section displays the Overall Date Scope of data stored on the SR. This date scope includes the range for the period of stored data, using the MM/DD/YYYY HH:MM:SS AM/PM format. the number of week(s) of data stored on the SR, and the date and time range display for the following date scopes:

Report Manager Startup Time

The Report Manager Startup Time section contains the following information pertaining to the last time the Report Manager was restarted: Day of the week and month name abbreviation, day, military time (HH:MM:SS), and year (YYYY).

***NOTE**: This information is useful for troubleshooting manually generated reports. If your reports are not displaying, it may be that the Report Manager has restarted and terminated the report generation process.*

Server Info

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

Server Activity

In the Server Activity section, specify the type of chart you wish to generate that provides details on the number of hits within a designated time period. A “hit” is any page and/or object an end user accesses as the result of entering a URL in his/her browser window.

1. Specify the time period for the chart you wish to draw by doing the following:

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

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

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

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

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

2. Click the **Draw Chart** button to open a window that displays the chart of your selection in the PDF file format.

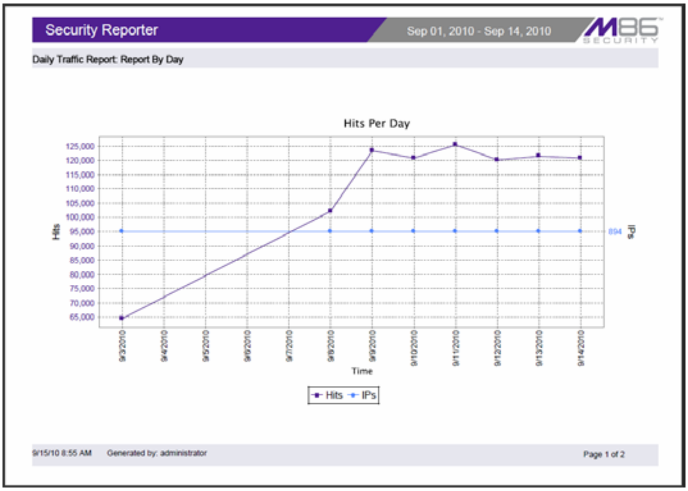
   The header section includes the title of the chart and date range. The footer section includes the date and time the chart was generated (shown in the MM/DD/YYYY HH:MM AM/PM format), the login ID of the person who generated the chart (Generated by) and the Page number and page range.

   The chart image includes a graph illustrating the general Number of Hits (in purple) and Number of IPs that generated those hits (in blue) for each unit of Time in the specified period.

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

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

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



Security Reporter

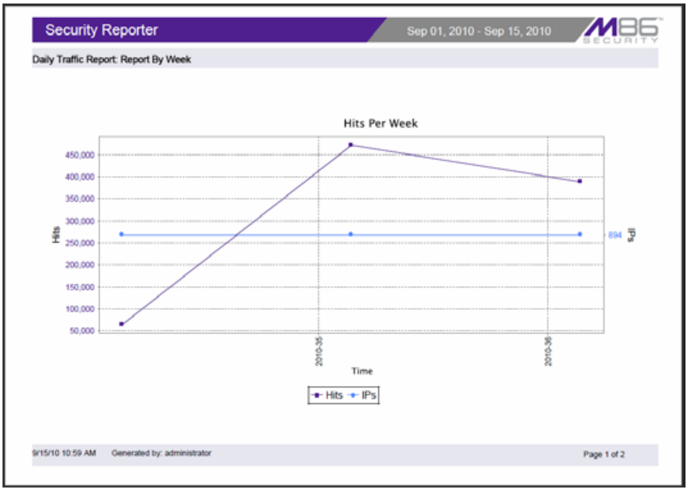
Sep 01, 2010 - Sep 14, 2010

Daily Traffic Report: Report By Day

9/15/10 8:55 AM Generated by: administrator Page 1 of 2

Fig. 3:2-19 Hits Per Day chart

- **Hits Per Week** - If you selected Hits By Week, each week within the date range is plotted on the graph. The summary shows the general Number of Hits (in purple) and Number of IPs that generated those hits (in blue) for a specified Week (YYYY-WW). Weeks are numbered 1-52.



Security Reporter

Sep 01, 2010 - Sep 15, 2010

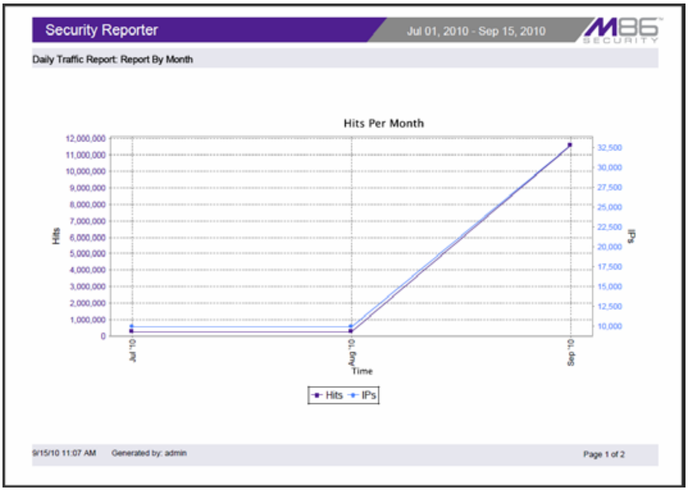
Daily Traffic Report: Report By Week

9/15/10 10:59 AM Generated by: administrator

Page 1 of 2

Fig. 3:2-20 Hits Per Week chart

- **Hits Per Month -** If you selected Hits By Month, each month within the date range is plotted on the graph. The summary shows the general Number of Hits (in red) and Number of IPs that generated those hits (in green) for a specified Month (Month ’YY). Month names are abbreviated.



Security Reporter

Jul 01, 2010 - Sep 15, 2010

Daily Traffic Report: Report By Month

9/15/10 11:07 AM Generated by: admin

Page 1 of 2

Fig. 3:2-21 Hits Per Month chart

3. You now have the option to do any of the following:

   - print the chart - click the print 🖨 icon to open the Print dialog box, and proceed with standard print procedures.
   - save the chart - click the save 💾 icon to open the Save a Copy dialog box, and proceed with standard save procedures.
   - close the chart window - click the “X” in the upper right corner to close the chart window.
   - generate a new chart - make new entries in the Server Information panel.

Expiration Info

In the Expiration Info section, the following data displays:

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

***NOTE**: If using the SR in evaluation mode, the text “(IF REGISTERED)” is included in the label to indicate the number of weeks of data that would be stored on the SR if the server was activated and running in registered mode.*

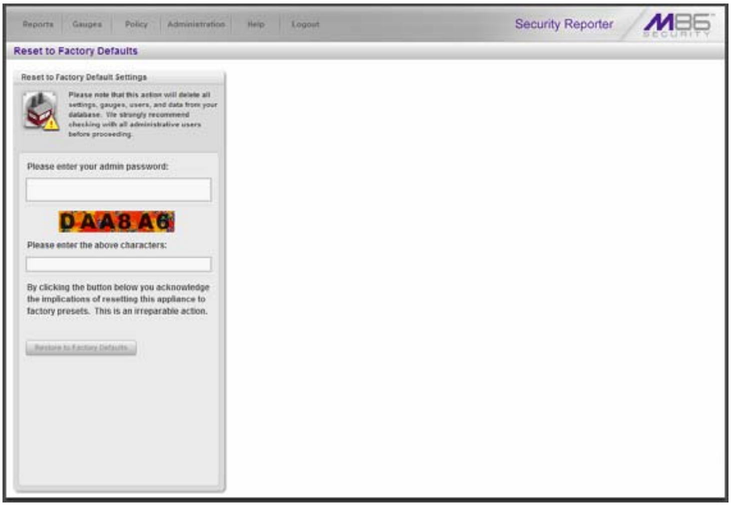
- **Estimated date of next expiration** - the date scheduled for the next automatic database expiration (MM/DD/YYYY format).

***NOTE**: If using the SR in evaluation mode, the text "(IF REGISTERED)" is included in the label to indicate the date (MM/DD/YYYY) that data would expire on the SR if the server was activated and running in registered mode.*

Reset to Factory Defaults panel

The global administrator uses the Reset to Factory Defaults panel, if necessary, to restore the SR to default settings for the current software update level of the application.

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


Reports
Gauges
Policy
Administration
Help
Logout
Security Reporter
M86 SECURITY
Reset to Factory Defaults
Reset to Factory Default Settings
DAA8A6
Restore to Factory Defaults

Please note that this action will delete all settings, gauges, users, and data from your database. We strongly recommend checking with all administrative users before proceeding.

Please enter your admin password:

Please enter the above characters:

By clicking the button below you acknowledge the implications of resetting this appliance to factory presets. This is an irreparable action.

Fig. 3:2-22 Reset to Factory Defaults panel

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

Reset to Factory Default Settings frame

1. In the Reset to Factory Default Settings panel, **Please enter your admin password** that was created during the WFR wizard hardware installation process.
2. Beneath the security characters, **Please enter the above characters**.
3. Click **Restore to Factory Defaults** to reset the SR application and to display the WFR's End User License Agreement window:

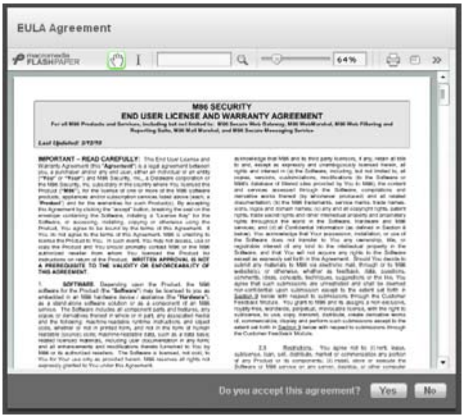
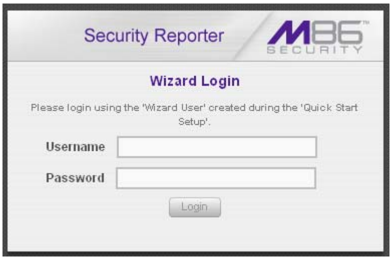

EULA Agreement
macromedia FLASHPAPER
64%
M86 SECURITY
END USER LICENSE AND WARRANTY AGREEMENT
IMPORTANT – READ CAREFULLY:
Do you accept this agreement?
Yes
No

Fig. 3:2-23 End User License Agreement

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



Wizard Login

Please login using the 'Wizard User' created during the 'Quick Start Setup'.

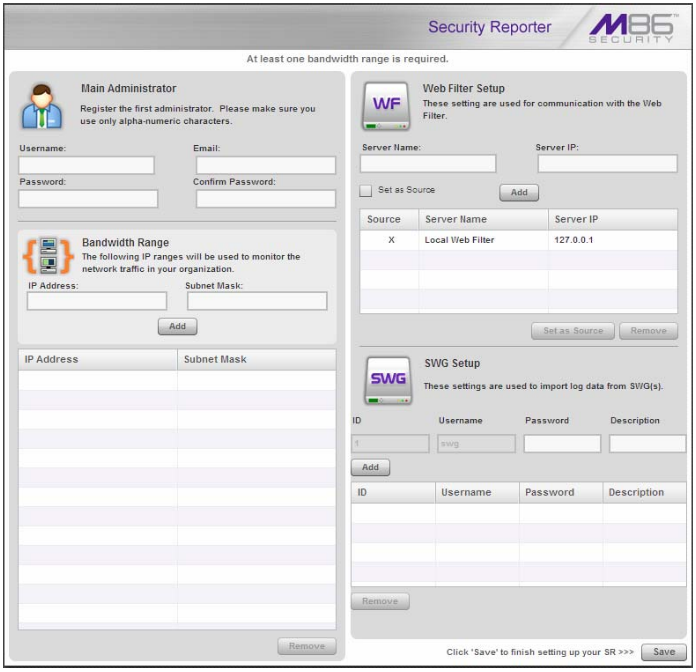
Username

Password

Fig. 3:2-24 Wizard Login window

Wizard panel

1. In the Wizard Login window, type in the **Username** created during the wizard hardware installation process.
2. Type in the **Password** created for the Username during the wizard hardware installation process.
3. Click **Login** to display the wizard panel:



At least one bandwidth range is required.

Register the first administrator. Please make sure you use only alpha-numeric characters.

The following IP ranges will be used to monitor the network traffic in your organization.

IP Address	Subnet Mask

These setting are used for communication with the Web Filter.

Source	Server Name	Server IP
X	Local Web Filter	127.0.0.1

These settings are used to import log data from SWG(s).

ID	Username	Password	Description
1	swg		

ID	Username	Password	Description

Click 'Save' to finish setting up your SR >>>

Fig. 3:2-25 Wizard panel

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

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

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

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

6. By default, the table in the Web Filter Setup section should be populated with an "X" in the Source column and the Server Name and Server IP address for the Source Web Filter.

   To add another Web Filter in the Web Filter Setup section, type in the **Server Name** and **Server IP** address, and then click **Add** to include the server criteria in the list box below.

***TIPS**: To remove a Web Filter from the list box, select it and then click **Remove**. To make a Web Filter the Source server—if the Source server IP address has changed—select the Web Filter from the list box and then click **Set as Source**.*

7. If using an SWG with the SR, in the SWG Setup section the "ID" and "Username" display greyed-out. Type in the **Password** and **Server Description**, and then click **Add** to include the server criteria in the list box below.

***NOTE**: For this software release, only one SWG can be added in this section, even though multiple SWG policy servers can be set up to send logs to the SR.*

8. Click **Save** to save your entries and to go to the Security Reporter login window:

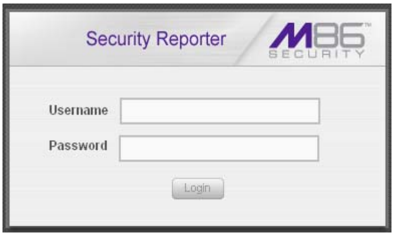


Fig. 3:2-26 SR Login window

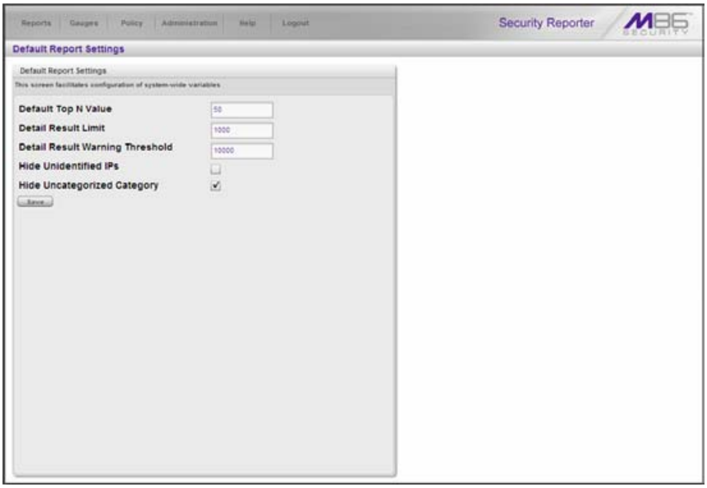
Chapter 3: Report Configuration

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

Default Report Settings panel

The global administrator uses the Default Report Settings panel for specifying various settings to be used in reports.

In the navigation toolbar, mouse over the Administration menu link and select **Default Report Settings** to display the Default Report Settings panel:



Default Report Settings

Default Report Settings

This screen facilitates configuration of system-wide variables

Default Top N Value	50
Detail Result Limit	1000
Detail Result Warning Threshold	10000
Hide Unidentified IPs	□
Hide Uncategorized Category	☑

Fig. 3:3-1 Default Report Settings panel

Set New Defaults

1. Enter the **Default Top N Value** of records that will be generated for summary reports. The default is “50” records.
2. Enter the maximum number of records that will be included in a detail report’s **Detail Result Limit**. If the number of records from a query exceeds the limit established in this field, the overflow will be included in the next set of records. The default is “1000” records per set.
3. Enter the maximum number of records that can be returned by a detail report query before triggering the **Detail Result Warning Threshold** message. This warning message indicates that the number of records exceeds the number specified in this field. The default is “10000” records.
4. By default, the **Hide Unidentified IPs** checkbox is deselected. This indicates that activity on machines not assigned to specific users will be included in reports.

   If you wish to exclude activity from machines not assigned to specific users, click in the checkbox to enter a check mark.
5. By default, the **Hide Uncategorized Category** checkbox is selected. This indicates that uncategorized sites will not be displayed or counted in drill down reports.

   If you wish to include uncategorized sites in drill down reports, click in the checkbox to remove the check mark.

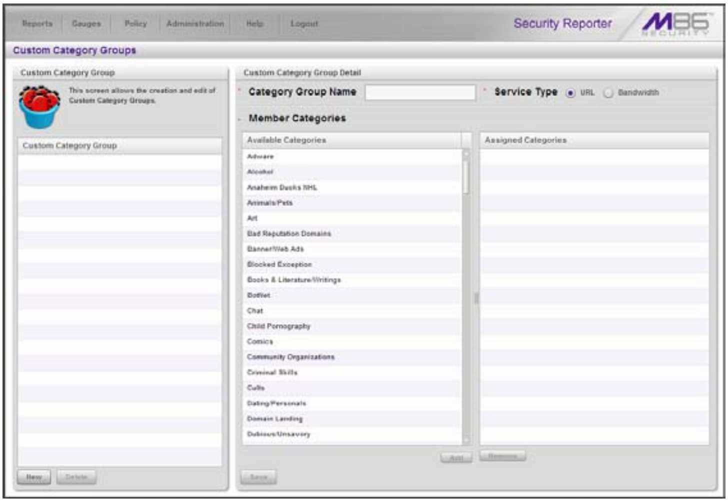
TIP: *Click Cancel to exit without saving your entries.*

6. Click the **Save** button to save your settings and to exit the Default Report Settings panel.

Custom Category Groups panel

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

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



This screen allows the creation and edit of Custom Category Groups.

Service Type ● URL ○ Bandwidth

Fig. 3:3-2 Custom Category Groups panel

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

Add a Custom Category Group

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

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

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

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

Modify a Custom Category Group

1. Select the Custom Category Group name from the list box by clicking on your choice to highlight it.
2. Make your edits:
   - To modify the Custom Category Group name, edit the **Category Group Name** in the Custom Category Group Detail frame.
   - To update the assigned selections in the list box, select the item to select it, and then click **Remove** to remove it.
3. Click **Update** to save your modification(s).

Delete a Category Group

1. Select the Custom Category Group name from the list box by clicking on your choice to highlight it.
2. Click **Delete** to remove the Custom Category Group name from the list box.

SR PRODUCTIVITY REPORTS SECTION

Introduction

This section of the user guide provides instructions to administrators on how to utilize the Report Manager to generate productivity report views and interpret results. Productivity report views are generated via selections made from the Reports menu.

The Reports menu consists of the following options described in these chapters:

- Chapter 1: A High Level Overview - This chapter shows you how to view productivity report data in the Dashboard, canned Summary Reports, and Sample Reports that provide a high level overview of end user Internet and network activity.
- Chapter 2: Drill Down Reports - This chapter provides instructions on using tools to generate summary and detail Drill Down Reports that give you more information on specific end user activity.
- Chapter 3: Customize, Maintain Reports - This chapter tells you how to generate customized reports using the Report Wizard, maintain Saved Reports for ongoing usage, and set up a Report Schedule for running reports on a regular basis.
- Chapter 4: Specialized Reports - This chapter informs you of three specialized types of reports you can generate: Executive Internet Usage Summary Reports, Blocked Request Reports, and Time Usage Reports.

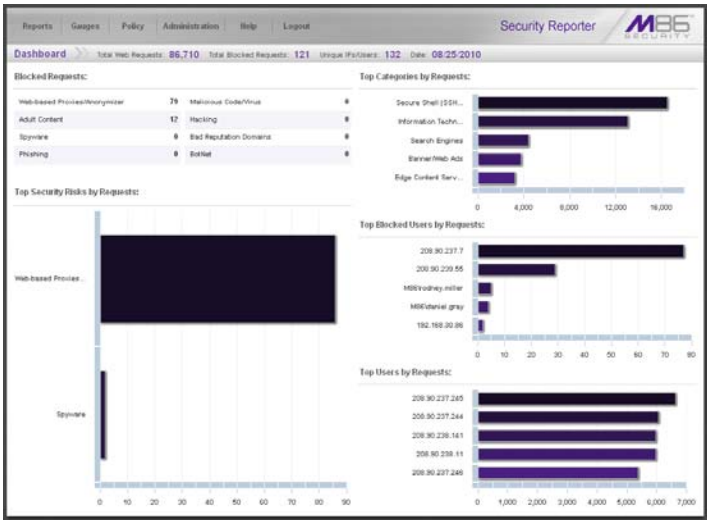
Chapter 1: A High Level Overview

The following productivity reporting topics from the Reports menu of the Report Manager are described in this chapter: Dashboard, Summary Reports, and Sample Reports. These tools give you a high level overview of how end users are currently using the Internet and network resources.

Dashboard

The Dashboard provides statistics and bar charts depicting the top end user requests in various productivity report categories.

The Dashboard displays by default after you log in to the Security Reporter user interface, or when you use the navigation toolbar to navigate to **Reports > Dashboard**:



Total Web Requests: 86,710 Total Blocked Requests: 121 Unique IPs/Users: 132 Date: 08/25/2010

Blocked Requests:

Web-based Proxies/Anonymizer	79	Malicious Code/Virus	0
Adult Content	12	Hacking	0
Spyware	0	Bad Reputation Domains	0
Phishing	0	BotNet	0

Fig. 4:1-1 Dashboard panel

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

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

The following information displays in the center of the panel:

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

***TIP**: Mouse over each bar in the bar graph to view the name of graph entry and number of requests for that entry.*

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

Summary Reports

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

Summary Reports are available to group administrators assigned the privilege to access the **Reports > Summary Reports** menu selection. By default, yesterday’s report view showing the Top 20 Users by Blocked Request displays in the panel:

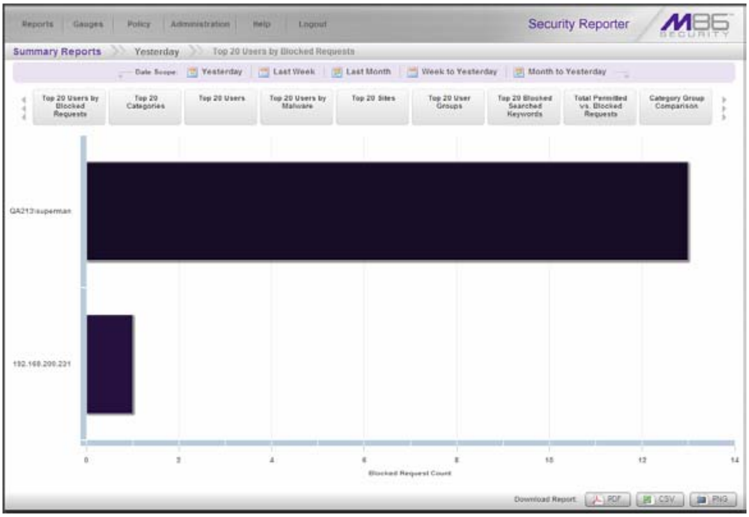


Fig. 4:1-2 Yesterday’s Top 20 Users by Blocked Requests Report

***NOTES**: On a newly installed SR unit, the panel will not show any thumbnail images or bar chart report. If there was no activity for a given report type, the message “No Data to display.” displays in the panel.*

***TIPS**: Click the left arrows or right arrows at the edges of the dashboard to display thumbnail images that are currently hidden. Mouse over each bar in the bar graph to view the name of graph entry and number of requests for that entry.*

Summary Report types

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

- **Top 20 Users by Blocked Requests** - Bar chart report depicting each top end user's total Page Count for Blocked and Warn Blocked requests. If using a Web Filter only, this report is available if the Block Request Count feature is enabled in the Optional Features screen in the System Configuration administrator console.
- **Top 20 Users by Bandwidth Consumption** (for SWG only) - Bar chart depicting each top end user's total Mega Bytes for bandwidth requests.
- **Top 20 Users by Virus Hit Count** (for SWG only) - Bar chart report depicting each top end user's total Virus Count detected by the anti-virus engine.
- **Top 20 Categories** - Bar chart report depicting the total Page Count in the top requested filtering library categories.
- **Top 20 Users** - Bar chart report depicting each top end user's total Page Count.
- **Top 20 Viruses Detected by** (for SWG only) - Bar chart report depicting the top viruses and Virus Count detected by the anti-virus engine.
- **Top 20 Users by Malware** - Bar chart report depicting each top end user's total "Blocked" and "Permitted" Hit Count from the following categories in the Security, Internet Productivity, and Internet Communication (Instant Messaging) category groups: BotNet, Malicious Code/Virus, Bad Reputation Domains, Spyware, Adware, and IRC.

***NOTE**: For SWG users, results that display in the Top 20 Users by Malware report reflect library contents mapped to the M86 Supplied Categories.*

- **Top 20 Sites** - Bar chart report depicting the total Page Count for the most popular sites accessed by end users.
- **Top 20 User Groups** - Bar chart report depicting the total Page Count for the top scoring user groups.
- **Top 20 Blocked Searched Keywords** - Bar chart report depicting the total blocked keyword requests Page Count. For Web Filter users, this report is only available if the Block Searched Keywords Report feature is enabled in the Optional Features screen in the System Configuration administrator console.
- **Total Permitted vs. Blocked Requests** - Pie chart report depicting the total Page Count for all filtering categories Permitted to pass and all filtering categories set up to be Blocked.
- **Category Group Comparison** - Pie chart report depicting the total Page Count in each top scoring filtering category group.
- **Category Comparison** - Pie chart report depicting the total Page Count in each top scoring filtering category.
- **User Group Comparison** - Pie chart report depicting the total Page Count in each top scoring user group.

Modify the Summary Report view

The report view displays either a bar chart or pie chart graph based on the selected report type.

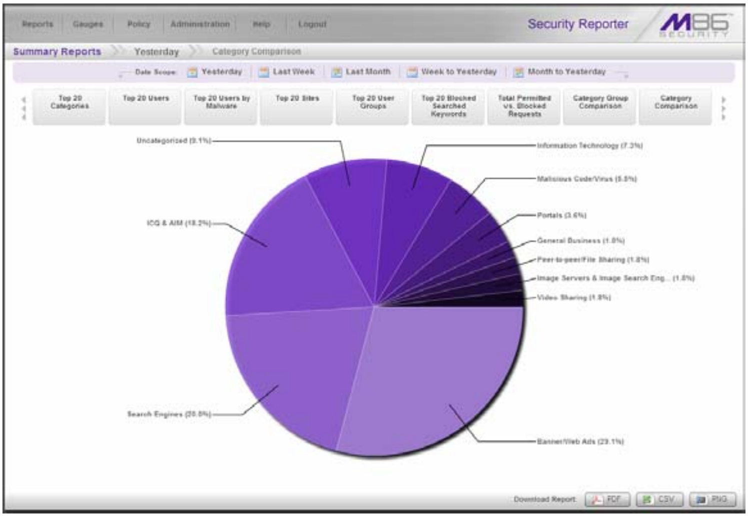


Fig. 4:1-3 Yesterday's Category Comparison Report

Use any the following tools to modify the report view:

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

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

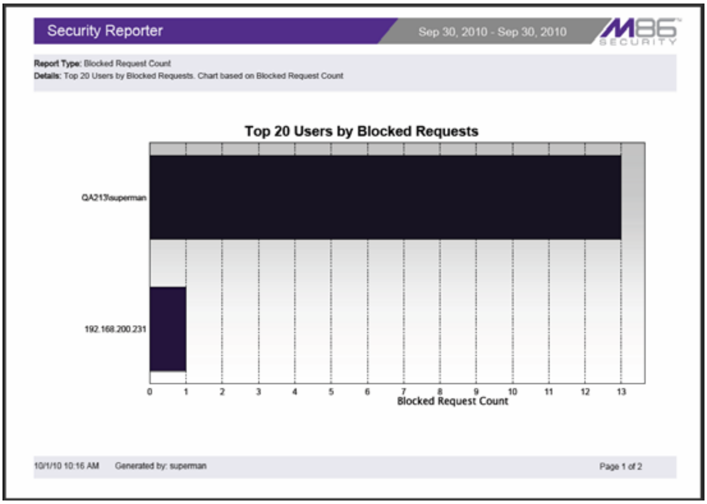
Download, Export a Summary Report

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

PDF format

Download the report in the PDF format

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



Security Reporter

Sep 30, 2010 - Sep 30, 2010

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

10/1/10 10:16 AM Generated by: superman

Page 1 of 2

Fig. 4:1-4 Sample Summary Report in the PDF format

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

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

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

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

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

- Top 20 Users by Blocked Request report - User NAME and corresponding BLOCKED REQUEST COUNT—which includes Blocked and Warn Blocked requests. Total Records and Total Number of Blocked Requests for this Date Scope display at the end of the report.
- Top 20 Blocked Searched Keywords report - Blocked Keywords and corresponding Blocked Count. A Grand Total of Blocked Count displays at the end of the report.
- All other reports - Count columns and corresponding totals for all reports. Grand Total and Count display at the end of the report.

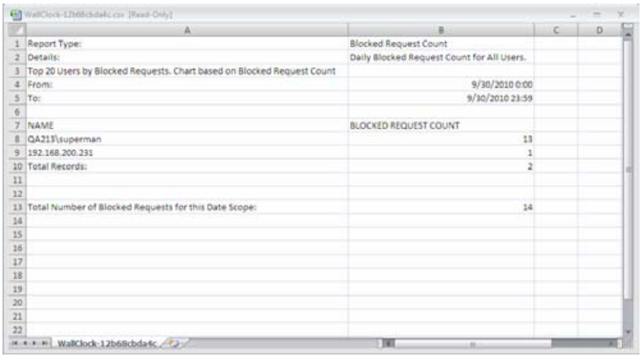
Export the PDF format report

- print the report - Click the print 🖨 icon to open the Print dialog box, and proceed with standard print procedures.
- save the report - Navigate to **File > Save a Copy** to open the Save a Copy dialog box, and proceed with standard save procedures.

CSV format

Download the report in the CSV format

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



	A	B	C	D
1	Report Type:	Blocked Request Count		
2	Details:	Daily Blocked Request Count for All Users.		
3	Top 20 Users by Blocked Requests. Chart based on Blocked Request Count			
4	From:	9/30/2010 0:00		
5	To:	9/30/2010 23:59		
6				
7	NAME	BLOCKED REQUEST COUNT		
8	QA213\superman	13		
9	192.168.200.231	1		
10	Total Records:	2		
11				
12				
13	Total Number of Blocked Requests for this Date Scope:	14		
14				
15				
16				
17				
18				
19				
20				
21				
22				

Fig. 4:1-5 Sample Summary Report in the CSV format

The header of the generated report includes the Report Type, Details criteria, and From/To date and time range (MM/D/YYYY HH:MM:SS AM/PM format).

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

Totals display after the last row of user data.

The footer of the report includes the date and time the report was generated (MM/D/YYYY HH:MM), product name, Filter specifications, and the login ID of the user who generated the report.

Export the CSV format report

- print the report - Navigate to **File > Print** to open the Print dialog box, and proceed with standard print procedures.

- save the report - Navigate to **File > Save As** to open the Save As dialog box, and proceed with standard save procedures.

PNG format

Download the report in the PNG format

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

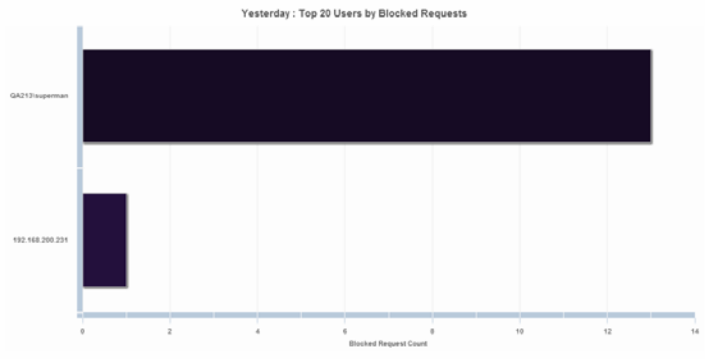


Fig. 4:1-6 Sample Summary Report in the PNG format

The generated report includes the report title followed by a graphical chart image:

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

Export the PNG format report

- print the report - Navigate to **File > Print** to open the Print dialog box, and proceed with standard print procedures.
- save the report - Right-click the image and choose Save Image As... to open the Save Image dialog box, and proceed with standard save procedures.

Sample Reports

Sample Reports are productivity reports in the PDF format that contain today's data for a specified reporting topic. These types of reports are accessible by navigating to **Reports > Sample Reports** and clicking one of the thumbnails in the panel:

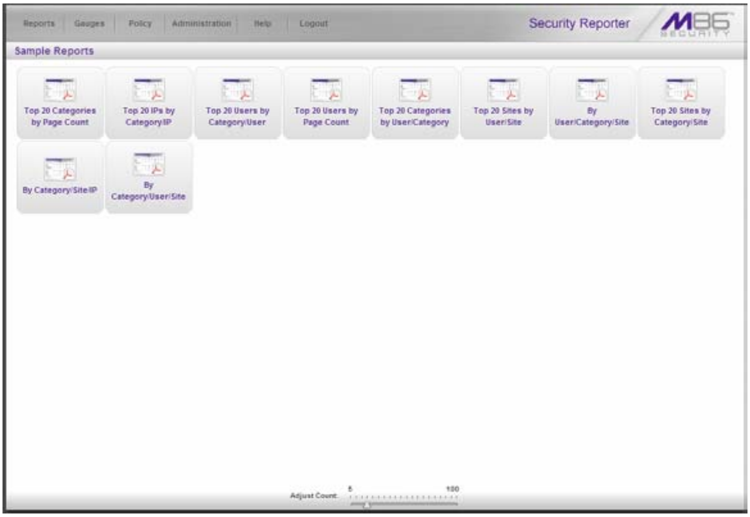

Reports
Gauges
Policy
Administration
Help
Logout
Security Reporter
M86 SECURITY
Sample Reports
Top 20 Categories by Page Count
Top 20 IPs by Category/IP
Top 20 Users by Category/User
Top 20 Users by Page Count
Top 20 Categories by User/Category
Top 20 Sites by User/Site
By User/Category/Site
Top 20 Sites by Category/Site
By Category/Site/IP
By Category/User/Site
Adjust Count:
5
100

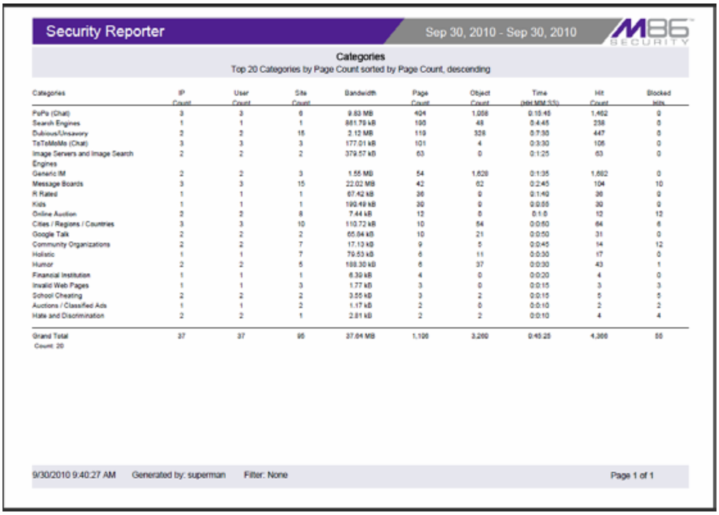
Fig. 4:1-7 Sample Reports

Sample Report types

Available Sample Report types are as follows:

- **Top 20 Categories by Page Count -** Top library categories end users accessed
- **Top 20 IPs by Category/IP** - Top end user IP addresses in each library category
- **Top 20 Users by Category/User -** Top usernames in each library category
- **Top 20 Users by Page Count -** Top end users who accessed library categories
- **Top 20 Categories by User/Category** - Top library categories each end user accessed
- **Top 20 Sites by User/Site -** Top sites each end user accessed
- **By User/Category/Site -** For each end user, the sites he/she visited in each library category
- **Top 20 Sites by Category/Site** - Top sites end users accessed in each library category
- **By Category/Site/IP -** For each library category, the sites end users accessed, and IP address of each end user
- **By Category/User/Site** - For each library category, the end users with activity in that library category, and the sites each end user accessed

View, Export a Sample Report



Security Reporter Sep 30, 2010 - Sep 30, 2010

Categories

Top 20 Categories by Page Count sorted by Page Count, descending

Categories	IP Count	User Count	Site Count	Bandwidth	Page Count	Object Count	Time (HH:MM:SS)	Hit Count	Blocked Hits
PoPo (Chat)	3	3	6	9.83 MB	404	1,008	0:15:45	1,462	0
Search Engines	1	1	1	881.79 kB	190	48	0:4:45	238	0
Dubious/Unsavory	2	2	15	2.12 MB	119	328	0:7:30	447	0
TeTeMoMo (Chat)	3	3	3	177.01 kB	101	4	0:3:30	106	0
Image Servers and Image Search Engines	2	2	2	379.57 kB	63	0	0:1:25	63	0
Generic IM	2	2	3	1.55 MB	54	1,628	0:1:35	1,682	0
Message Boards	3	3	15	22.02 MB	42	62	0:2:45	104	10
R Rated	1	1	1	67.42 kB	36	0	0:1:40	36	0
Kids	1	1	1	190.49 kB	30	0	0:0:55	30	0
Online Auction	2	2	8	7.44 kB	12	0	0:1:0	12	12
Cities / Regions / Countries	3	3	10	110.72 kB	10	54	0:0:50	64	6
Google Talk	2	2	2	65.04 kB	10	21	0:0:50	31	0
Community Organizations	2	2	7	17.13 kB	9	5	0:0:45	14	12
Holistic	1	1	7	79.53 kB	6	11	0:0:30	17	0
Humor	2	2	5	188.30 kB	6	37	0:0:30	43	1
Financial Institution	1	1	1	6.39 kB	4	0	0:0:20	4	0
Invalid Web Pages	1	1	3	1.77 kB	3	0	0:0:15	3	3
School Cheating	2	2	2	3.55 kB	3	2	0:0:15	5	5
Auctions / Classified Ads	1	1	2	1.17 kB	2	0	0:0:10	2	2
Hate and Discrimination	2	2	1	2.81 kB	2	2	0:0:10	4	4
Grand Total Count: 20	37	37	95	37.04 MB	1,100	3,200	0:45:25	4,300	55

9/30/2010 9:40:27 AM Generated by: superman Filter: None Page 1 of 1

Fig. 4:1-8 Sample Categories report

View Sample Report contents

The report header contains the following information: “Security Reporter” and date range for today’s date (MM/DD/YYYY format); report name; description for that report type, including the sort order and **Page Count, descending**

The body of the report contains rows of records and is comprised of one or more sections.

For each record, end user statistics display in columns such as: Category Count, IP Count, Site Count, Bandwidth (kB or MB amounts display for SWG only), Page Count, Object Count, Time (HH:MM:SS), Hit Count, and Blocked Hits.

Total counts display at the end of each section.

The Grand Total and total Count for all sections display at the end of the report.

The footer on each page contains the following information: today’s date (MM/DD/YYYY) and time (HH:MM:SS AM/PM) the report was generated; **Generated by**: manager’s login ID; **Filter: None**; **Page** number.

Export the Sample Report

1. From the open PDF file window, the Sample Report can be exported in some of the following ways:

   - print the report - click the print 🖨 icon to open the Print dialog box, and proceed with standard print procedures.
   - save the report - navigate to **File > Save a Copy** to open the Save a Copy dialog box, and proceed with standard save procedures.

2. Click the “X” in the upper right corner of the PDF file window to close it.

Chapter 2: Drill Down Reports

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

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

The following types of reports can be generated from the **Reports > Drill Down Reports** menu:

- **Categories** - Includes data in each filter category that was set up for monitoring user activity.
- **IPs** - Includes Internet activity by user IP address.
- **Users** - Includes Internet activity by username.
- **Sites** - Includes activity on Web sites users accessed.
- **Category Groups** - Includes activity by Category Groups.
- **User Groups** - Includes activity by User Groups.

***NOTE**: The Report Wizard feature for drill down reports is discussed in detail in Chapter 3: Customize, Maintain Reports.*

Once you have generated a drill down report view, you can customize your view, save the view, export the view, and/or schedule the report to run at a designated time.

***NOTE**: Before you begin generating report views for these reports, we recommend that you review this chapter in order to become familiar with the organization of these report views, and how report view tools and components are used in creating summary drill down reports and detail drill down reports customized to your specifications.*

Generate a Drill Down Report

To generate a drill down productivity report:

1. Choose one of the following topics from the **Reports > Drill Down Reports** menu for the type of summary drill down report you wish to view: Categories, IPs, Users, Sites, Category Groups, User Groups.

***NOTES**: As the report is generating, the “Processing...” message displays. After the report has finished being generated, if no records are available an alert box opens displaying the message “No records returned!”*

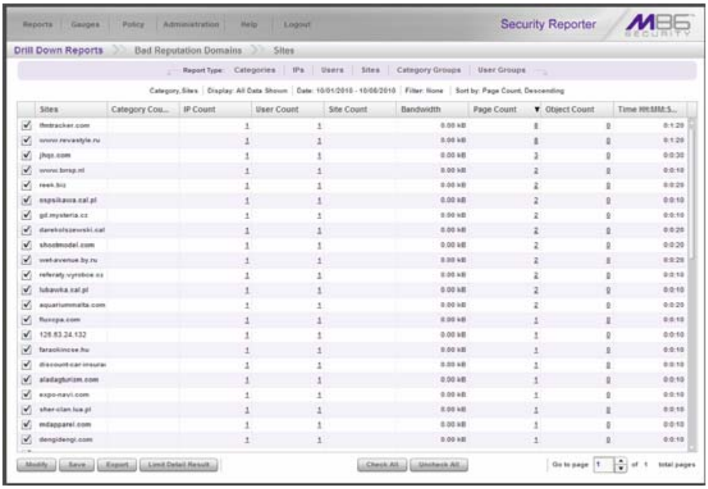
2. Once the generated summary drill down report has loaded in the panel, use the tools in the panel to create the desired drill down view.

***NOTE**: A detail drill down report view is generated by clicking a link in the Page Count or Object Count column corresponding to a specific record displayed in the current summary drill down report view.*

3. The drill down view can be exported, saved, and/or scheduled to run at a specified time.

Summary Drill Down Report View

The summary drill down productivity report view provides a snapshot of end user activity for a specified report type and defined date of activity recorded by the SR, and is horizontally organized into three sections:



Drill Down Reports >> Bad Reputation Domains >> Sites

Report Type: Categories | IPs | Users | Sites | Category Groups | User Groups

Category,Sites | Display: All Data Shown | Date: 10/01/2010 - 10/06/2010 | Filter: None | Sort by: Page Count, Descending

	Sites	Category Cou...	IP Count	User Count	Site Count	Bandwidth	Page Count ▼	Object Count	Time HH:MM:S...
☑	ifmtracker.com		1	1		0.00 kB	8	0	0:1:20
☑	www.revastyle.ru		1	1		0.00 kB	8	0	0:1:20
☑	jhqs.com		1	1		0.00 kB	3	0	0:0:30
☑	www.brsp.nl		1	1		0.00 kB	2	0	0:0:10
☑	reek.biz		1	1		0.00 kB	2	0	0:0:20
☑	ospsikawa.cal.pl		1	1		0.00 kB	2	0	0:0:10
☑	gd.mysteria.cz		1	1		0.00 kB	2	0	0:0:10
☑	darekolszewski.cal		1	1		0.00 kB	2	0	0:0:20
☑	shoolmodel.com		1	1		0.00 kB	2	0	0:0:20
☑	wet-avenue.by.ru		1	1		0.00 kB	2	0	0:0:20
☑	referaty.vyroboe.cz		1	1		0.00 kB	2	0	0:0:10
☑	lubawka.cal.pl		1	1		0.00 kB	2	0	0:0:10
☑	aquariummalta.com		1	1		0.00 kB	2	0	0:0:20
☑	flunopa.com		1	1		0.00 kB	1	0	0:0:10
☑	126.83.24.132		1	1		0.00 kB	1	0	0:0:10
☑	faraokincse.hu		1	1		0.00 kB	1	0	0:0:10
☑	discount-car-insura		1	1		0.00 kB	1	0	0:0:10
☑	aladagturizm.com		1	1		0.00 kB	1	0	0:0:10
☑	expo-navi.com		1	1		0.00 kB	1	0	0:0:10
☑	sher-clan.lua.pl		1	1		0.00 kB	1	0	0:0:10
☑	mdapparel.com		1	1		0.00 kB	1	0	0:0:10
☑	dengidengi.com		1	1		0.00 kB	1	0	0:0:10

Fig. 4:2-1 Summary Drill Down Report view

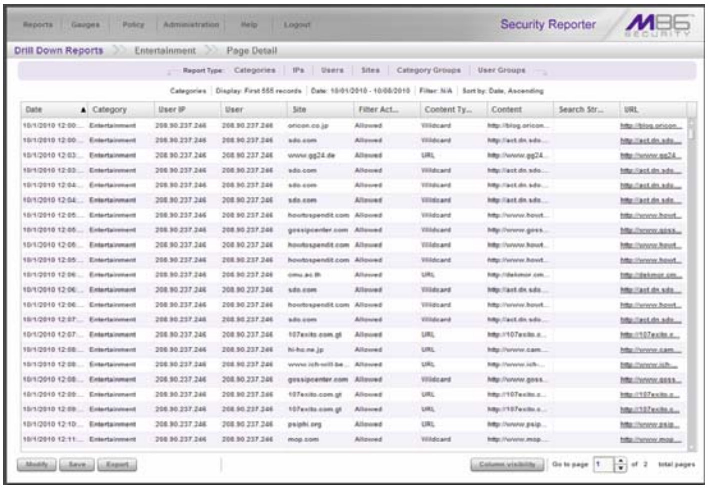
- Top section - includes navigational links in the row beneath the navigation toolbar. Beneath this row, **Report Type** tabs let you generate another summary drill down report by clicking that tab (Categories, IPs, Users, Sites, Category Groups, or User Groups). The following information displays beneath this row of tabs: report type, Display criteria, Date, Filter criteria, and Sort by criteria.
- Main section - includes rows of records returned by the reporting query. Each row is preceded by a checkbox. For each record, filter columns with statistics display (such as Category Count, IP Count, User Count, Site Count, Bandwidth, Page Count, and Object Count), and the Time HH:MM:SS column. Each filter column populated with statistics includes links that if clicked will generate a different report view. Clicking a link in the

Page Count or Object Count column will generate a detail drill down report view.

- Bottom section - includes buttons for customizing the current report view: **Modify**, **Save**, **Export**, **Limited Detail Result**, **Check All**, and **Uncheck All**. The **Go to page** navigation field at far right lets you navigate to a specific page and includes the total pages in the report view.

Detail Drill Down Report View

The detail drill down productivity report view provides information on pages or objects accessed by end users within a specific time period and is horizontally organized into three sections:


Reports
Gauges
Policy
Administration
Help
Logout
Security Reporter
M86 SECURITY
Drill Down Reports >> Entertainment >> Page Detail
Report Type: Categories | IPs | Users | Sites | Category Groups | User Groups
Modify
Save
Export
Column visibility

Categories | Display: First 555 records | Date: 10/01/2010 - 10/08/2010 | Filter: N/A | Sort by: Date, Ascending

Date ▲	Category	User IP	User	Site	Filter Act...	Content Ty...	Content	Search Str...	URL
10/1/2010 12:00:...	Entertainment	208.90.237.246	208.90.237.246	oricon.co.jp	Allowed	Wildcard	http://blog.oricon...		http://blog.oricon...
10/1/2010 12:00:...	Entertainment	208.90.237.246	208.90.237.246	sdo.com	Allowed	Wildcard	http://act.dn.sdo...		http://act.dn.sdo...
10/1/2010 12:03:...	Entertainment	208.90.237.246	208.90.237.246	www.gg24.de	Allowed	URL	http://www.gg24...		http://www.gg24...
10/1/2010 12:03:...	Entertainment	208.90.237.246	208.90.237.246	sdo.com	Allowed	Wildcard	http://act.dn.sdo...		http://act.dn.sdo...
10/1/2010 12:04:...	Entertainment	208.90.237.246	208.90.237.246	sdo.com	Allowed	Wildcard	http://act.dn.sdo...		http://act.dn.sdo...
10/1/2010 12:04:...	Entertainment	208.90.237.246	208.90.237.246	sdo.com	Allowed	Wildcard	http://act.dn.sdo...		http://act.dn.sdo...
10/1/2010 12:05:...	Entertainment	208.90.237.246	208.90.237.246	howtospendit.com	Allowed	Wildcard	http://www.howt...		http://www.howt...
10/1/2010 12:05:...	Entertainment	208.90.237.246	208.90.237.246	gossipcenter.com	Allowed	Wildcard	http://www.goss...		http://www.goss...
10/1/2010 12:06:...	Entertainment	208.90.237.246	208.90.237.246	howtospendit.com	Allowed	Wildcard	http://www.howt...		http://www.howt...
10/1/2010 12:05:...	Entertainment	208.90.237.246	208.90.237.246	howtospendit.com	Allowed	Wildcard	http://www.howt...		http://www.howt...
10/1/2010 12:06:...	Entertainment	208.90.237.246	208.90.237.246	cmu.ac.th	Allowed	URL	http://dekmor.cm...		http://dekmor.cm...
10/1/2010 12:06:...	Entertainment	208.90.237.246	208.90.237.246	sdo.com	Allowed	Wildcard	http://act.dn.sdo...		http://act.dn.sdo...
10/1/2010 12:06:...	Entertainment	208.90.237.246	208.90.237.246	howtospendit.com	Allowed	Wildcard	http://www.howt...		http://www.howt...
10/1/2010 12:07:...	Entertainment	208.90.237.246	208.90.237.246	sdo.com	Allowed	Wildcard	http://act.dn.sdo...		http://act.dn.sdo...
10/1/2010 12:07:...	Entertainment	208.90.237.246	208.90.237.246	107exito.com.gt	Allowed	URL	http://107exito.c...		http://107exito.c...
10/1/2010 12:08:...	Entertainment	208.90.237.246	208.90.237.246	hi-ho.ne.jp	Allowed	URL	http://www.cam...		http://www.cam...
10/1/2010 12:08:...	Entertainment	208.90.237.246	208.90.237.246	www.ich-will.be...	Allowed	URL	http://www.ich-...		http://www.ich-...
10/1/2010 12:08:...	Entertainment	208.90.237.246	208.90.237.246	gossipcenter.com	Allowed	Wildcard	http://www.goss...		http://www.goss...
10/1/2010 12:09:...	Entertainment	208.90.237.246	208.90.237.246	107exito.com.gt	Allowed	URL	http://107exito.c...		http://107exito.c...
10/1/2010 12:09:...	Entertainment	208.90.237.246	208.90.237.246	107exito.com.gt	Allowed	URL	http://107exito.c...		http://107exito.c...
10/1/2010 12:10:...	Entertainment	208.90.237.246	208.90.237.246	psiphi.org	Allowed	URL	http://www.psip...		http://www.psip...
10/1/2010 12:11:...	Entertainment	208.90.237.246	208.90.237.246	mop.com	Allowed	Wildcard	http://www.mop...		http://www.mop...

Go to page 1 of 2 total pages

Fig. 4:2-2 Detail Drill Down Report view

- Top section - same content as in the summary detail drill down report view.
- Main section - includes rows of records returned by the reporting query. The Date and URL columns display for each record, along with any of the following columns specified via the Column visibility pop-up window: Category, User IP, User name, Site, Filter Action, Content Type, Content criteria, Search String.
- Bottom section - includes buttons for customizing the current report view: **Modify**, **Save**, **Export**, **Column visibility**. The **Go to page** navigation field at far right lets you navigate to a specific page and includes the total pages in the report view.

Report View Tools and Usage Tips

Understanding report view tools and their functions is paramount to generating a report containing relevant content, since the usage of these tools determines the results of your query.

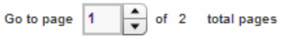
As you will learn from the rest of this chapter, report view tools along with report view components help you create the desired report view. This report view can then be exported, saved, and/or scheduled to run at a specified time.

Navigation Tips

Report view breadcrumb trail links

When generating a report view and modifying that report view to create another report view, a trail of breadcrumb links remain in the row beneath the navigation toolbar. Clicking a link returns you to that prior report view.

Page navigation

At the bottom right of the panel, the **Go to page** field displays: 

Go to page 1 of 2 total pages

If more than one page of records displays for the total pages returned, enter a page number within that range to navigate to that page of records, or use the up/down arrow(s) to specify the page you want displayed.

Summary Report View Tools and Tips

Count columns and links

In a summary drill down report view, Count columns (Category Count, IP Count, User Count, Site Count, Page Count, Object Count) display after the column containing the record name. Clicking a specific link in a record's Count column gives more in-depth analysis on a given record displayed in the current view.

- **Category Count** - Displays the number of categories a user has visited, or the number of categories included within a given site. It is possible for a site to be listed in more than one category, so even if a user has visited only one site, this column may count the user's visit in two or three categories.
- **IP Count** - Displays the number of sites or categories visited by the IP address for a user's machines.
- **User Count** - Displays the number of individuals who have visited a specific site or category.
- **Site Count** - Displays the number of sites a user has visited, or the number of sites in a category. This figure is based on the root name of the site. For example, if a user visits www.espn.com, www.msn.com, and www.foxsports.com, that user will have visited three pages. If that same user additionally visits www.espn.com/scores, the total number of sites visited would still count as three—and not as four—because the latter page is on the original ESPN site that was already counted.
- **Page Count** - displays the total number of pages visited. A user may visit only one site, but visit 20 pages on that site. If a user visits a page with pop-up ads, these items would add to the page count. If a page has banner ads that link to other pages, these items also would factor into the page count. In categories that use a lot of pop-up

ads—porn, gambling, and other related sites—the page count usually exceeds the number of objects per page.

By clicking the link in this column, the detail report view displays data for all pages accessed, including hyperlinks to those pages. In the detail report view, you have the option to exclude Information columns for Category, User IP, User name, Site, Filter Action, Content Type, Content criteria, and Search String by deselecting the corresponding checkboxes via the Column visibility option.

- **Object Count** - displays the number of objects on a Web page. All images, graphics, multimedia items, and text items count as objects. The number of objects on a page is generally higher than the number of pages a user visits.

  However, if an advertisement or banner ad (an object on the page) is actually a page from another site, this item would not be classified as an object but as a page, since it comes from a different server.

  By clicking the link in this column, the detail report view displays data for all objects accessed, including hyperlinks to those objects. In the detail report view, you have the option to include Information columns for Category, User IP, User name, Site, Filter Action, Content Type, Content criteria, and Search String by deselecting the corresponding checkboxes via the Column visibility option.

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

Bandwidth and Time columns

In a summary drill down report view, the Bandwidth and Time columns provide additional information about a record.

- **Bandwidth** - Displays the amount of bandwidth in kB or MB used for each record, if using an SWG only with this SR.
- **Time HH:MM:SS** - Displays the amount of time a user spent at a given site. Each page detected by a user's machine adds to the count. If a browser window is opened to a certain page and left there for an extended time period, and that page is refreshed by either the user or a banner ad, the counter starts again and continues as long as Web activity is detected. If that Web page contains an active banner ad that refreshes the page every 10 to 30 seconds, a user could show an incredibly high page count and many minutes, even though only one page was opened by that user.

Column sorting tips

To sort summary report view records in ascending/ descending order by a specified column, click that column's header: Category Count, IP Count, User Count, Site Count, Bandwidth, Page Count, Object Count, or Time HH:MM:SS.

Click the same column header again to sort records for that column in the reverse order.

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

Record exportation

In a summary drill down report view, each record is preceded by a checkbox that is populated (selected) by default.

When exporting a report, only selected records are included. To de-select a record, click the checkbox to remove the check mark from that checkbox.

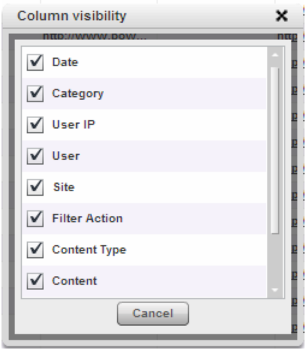
To de-select all records, click **Uncheck All** at the bottom of the panel.

To select all records, click **Check All** at the bottom of the panel.

Detail Report View Tools and Tips

Page/Object Detail columns

In the detail report view, by default all Page/Object Detail column(s) display. Any of these columns can be hidden from view by clicking the **Column visibility** button at the bottom of the panel to open the Column visibility pop-up window, and de-selecting the checkbox corresponding to that column:



☑ Date
☑ Category
☑ User IP
☑ User
☑ Site
☑ Filter Action
☑ Content Type
☑ Content

- **Date** - Displays the date in the M/D/YYYY H:M:S AM/PM format
- **Category** - Displays the category name (e.g. “Alcohol”).
- **User IP** - Displays the IP address of the user’s machine (e.g. “200.10.101.80”).
- **User** - Displays any of the following information: username, user IP address, or the path and username (e.g. “logo\admin\jsmith”).
- **Site** - Displays the URL the user attempted to access (e.g. “coors.com”).
- **Filter Action -** Displays the type of filter action used by the Web Filter in creating the record: "Allowed", "Blocked", "Warn Blocked" (for the first warning page that displayed for the end user), "Warn Allowed" (for any subsequent warning page that displayed for the end user), “Quota Blocked” (if a quota blocked the end user), "X-Strike", or "N/A" if the filter action was unclassified at the time the log file was created.
- **Content Type -** Displays the method used by the Web Filter in creating the record: “Search KW” (Search Engine Keyword), “URL KW” (URL Keyword), “URL”, “Wildcard”, “Https High” (HTTPS Filtering Level set at High), “X-strike” (X Strikes Blocking), “Pattern” (Proxy Pattern Blocking), “File Type”, “Https Medium” (HTTPS Filtering Level set at Medium), or “N/A” if the content was unclassified at the time the log file was created.
- **Content** - Displays criteria used for determining the categorization of the record, or “N/A” if unclassified.
- **Search String** - Displays the full search string the end user typed into a search engine text box in search sites such as Google, Bing, Yahoo!, MSN, AOL, Ask.com, YouTube.com, and MySpace.com—if the Search Engine Reporting option is enabled in the Optional Features

screen of the System Configuration administrator console user interface.

***NOTE**: Refer to the Optional Features screen sub-section of the SR System Configuration Section for information about the Search String feature.*

Column sorting tips

To sort detail report view records in ascending/descending order by a specified column, click that column's header: Date, Category, User IP, User name, Site, Filter Action, Content Type, Content criteria, Search String, or URL.

Click the same column header again to sort records for that column in the reverse order.

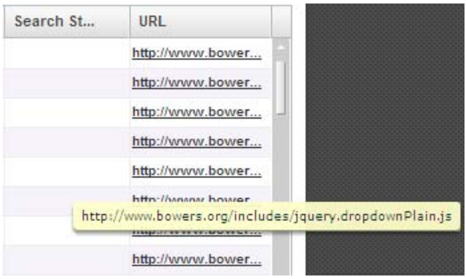
Click another column header to sort records by that specified column.

Page/Object viewing tip

Click the URL for a specified record to view the page or object currently indexed in the SR's memory.

Truncated data viewing tip

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



Search St...	URL
	http://www.bower...
	http://www.bower...
	http://www.bower...
	http://www.bower...
	http://www.bower...
	http://www.bower
	http://www.bower...
	http://www.bower...

http://www.bowers.org/includes/jquery.dropdownPlain.js

Customization Buttons

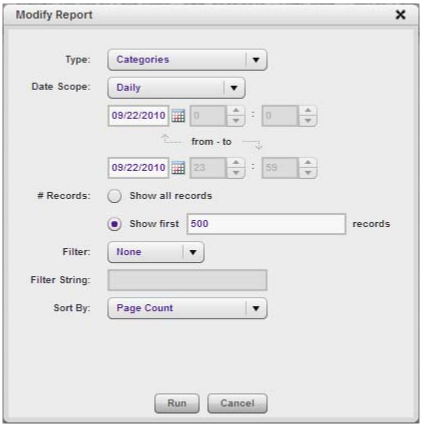
Clicking a button at the bottom of a report view panel opens a pop-up box that lets you customize the current report view. The following buttons are available in the summary and detail report views: Modify, Save, and Export. The Limit Detail Result button is additionally available in summary report views.

***NOTES**: Information on using the fields in these pop-up boxes can be found in the Report View Components sub-section. Information on using Check All and Uncheck All for summary reports can be found in the Record exportation sub-section of Summary Report View Tools and Tips, and information about Column visibility can be found in Detail Report View Tools and Tips.*

Modify button

The Modify Report option lets you modify the current report view by changing any of the following: Date Scope, maximum number of Records to be included other than the number entered in Default Report Settings, or sort column.

For summary drill down reports, if specifying a Sort By the first column, summary results must be limited to the top count for another designated column.



Modify Report

Type: Categories

Date Scope: Daily

09/22/2010 0 : 0

from - to

09/22/2010 23 : 59

Records: ○ Show all records

● Show first 500 records

Filter: None

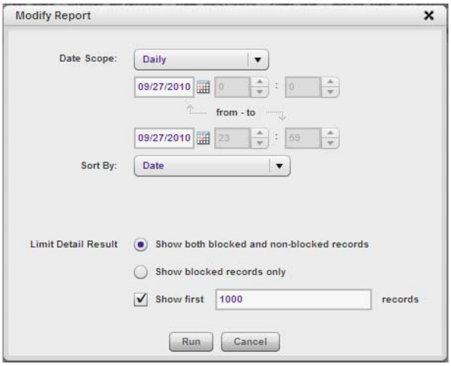
Filter String:

Sort By: Page Count

Fig. 4:2-3 Summary drill down Modify Report pop-up box

Selection of a different report Type or execution of a search for specific text can also be performed for summary drill down reports.

For detail drill down reports, you have the additional option to specify whether blocked records or all returned records—both blocked and non-blocked—will display.



Modify Report ✕

Date Scope: Daily

09/27/2010 0 : 0

from - to

09/27/2010 23 : 59

Sort By: Date

Limit Detail Result ● Show both blocked and non-blocked records

○ Show blocked records only

☑ Show first 1000 records

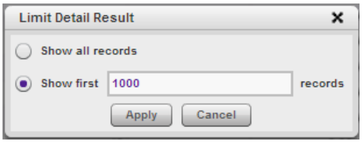
Run Cancel

Fig. 4:2-4 Detail drill down Modify Report pop-up box

***NOTE**: After all modifications are made, click **Run** to generate the new report view and to close the pop-up box.*

Limit Detail Result button

The Limit Detail Result option lets you specify the maximum number of records to be included in a detail drill down report view, instead of the default number entered in Default Report Settings.



Limit Detail Result ✕

○ Show all records

● Show first 1000 records

Apply Cancel

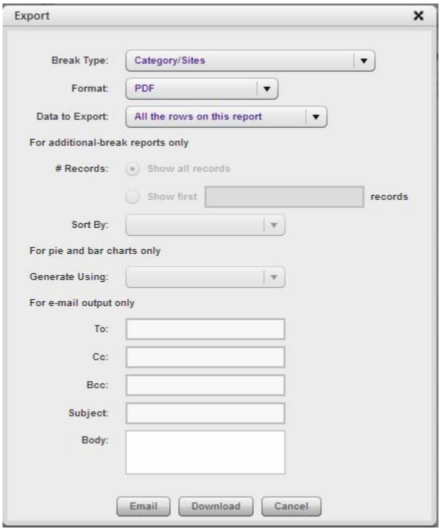
Fig. 4:2-5 Limit Detail Result pop-up box

***NOTE**: After all modifications are made, click **Apply** to save your settings and to close the pop-up box. If generating a detail drill down report, the number of records specified in this box will display.*

Export button

The Export option lets you Email or Download the current report view in the specified Break Type and output Format.

For summary drill down reports, if specifying a Break Type, indicate the records to be exported, and the Count column to be used for sorting these records.



Export

Break Type: Category/Sites

Format: PDF

Data to Export: All the rows on this report

For additional-break reports only

Records: ● Show all records

○ Show first records

Sort By:

For pie and bar charts only

Generate Using:

For e-mail output only

To:

Cc:

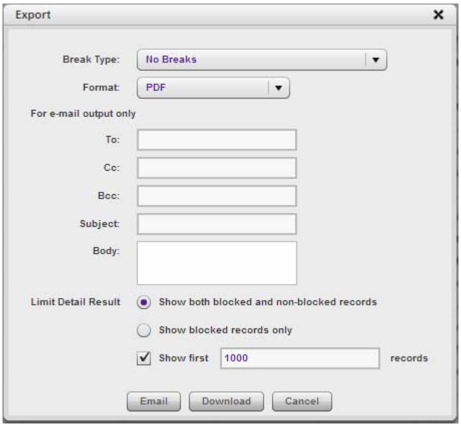
Bcc:

Subject:

Body:

Fig. 4:2-6 Summary drill down Export pop-up box

For detail drill down reports, you have the option to specify the quantity of records, and whether blocked records or all returned records—both blocked and non-blocked—will be included.



Export ✕

Break Type: No Breaks ▾

Format: PDF ▾

For e-mail output only

To:

Cc:

Bcc:

Subject:

Body:

Limit Detail Result ● Show both blocked and non-blocked records

○ Show blocked records only

☑ Show first 1000 records

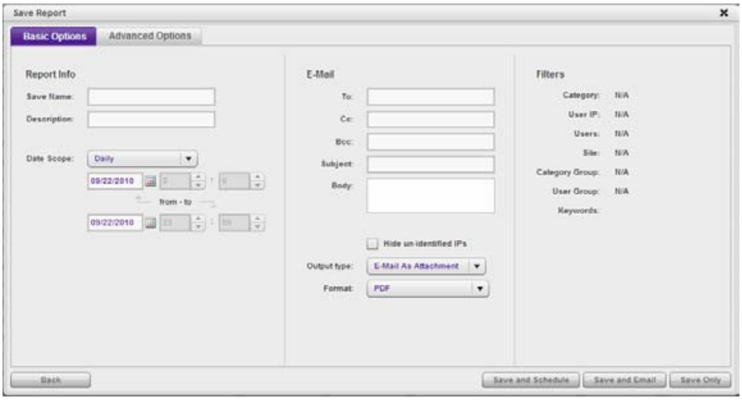
Fig. 4:2-7 Detail drill down Export pop-up box

***NOTES**: After all modifications are made, click **Email** to dispatch the report to the email recipient, or click **Download** to launch a separate browser window containing the generated report in the specified format.*

- *See Exporting a Report in this chapter for information about using the Email option to email a report.*
- *See View and Print Options in this chapter for information about using the View option to view and print a generated report, and for sample reports.*

Save button

The Save Report option lets you save the current report view so a report using these customizations can be run again later at a designated time. Basic Options requirements include a report Name, Description, Date Scope, Email and Output criteria, and whether unidentified IPs should be included.



Save Name:
Description:
Date Scope: Daily
09/22/2010 0 : 0
from - to
09/22/2010 23 : 59

To:
Cc:
Bcc:
Subject:
Body:
□ Hide un-identified IPs
Output type: E-Mail As Attachment
Format: PDF

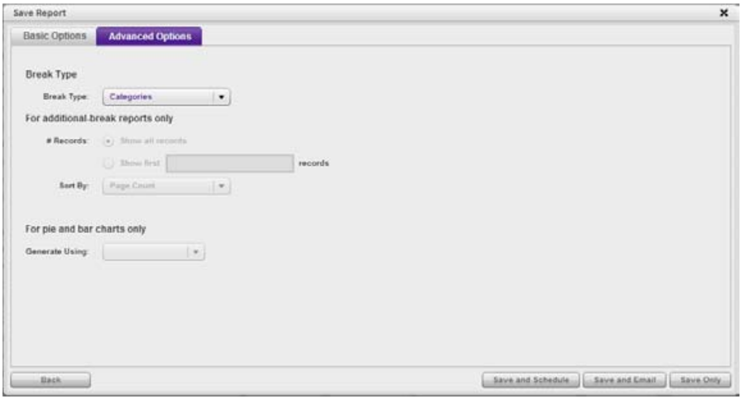
Category: N/A
User IP: N/A
Users: N/A
Site: N/A
Category Group: N/A
User Group: N/A
Keywords:

Fig. 4:2-8 Save Report pop-up window for summary reports

TIP*: The Copy (Ctrl+C) and Paste (Ctrl+V) functions can be used in the fields in the Save Report pop-up window.*

The Advanced Options tab lets you specify additional criteria for the report.

For a summary drill down report, Advanced Options include Break Type criteria.



Break Type

Break Type: Categories

For additional break reports only

# Records: ● Show all records

○ Show first records

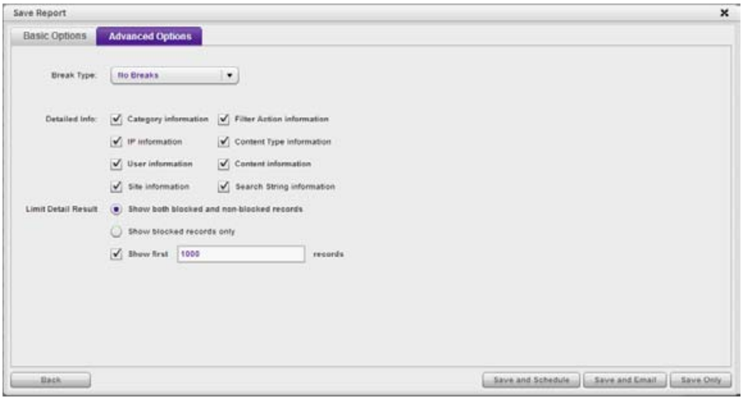
Sort By: Page Count

For pie and bar charts only

Generate Using:

Fig. 4:2-9 Save Report, Advanced Options tab for summary reports

For a detail drill down report, Advanced Options include Break Type criteria, column selections, and record types.



Break Type: No Breaks

Detailed Info: ☑ Category information ☑ Filter Action information

☑ IP information ☑ Content Type information

☑ User information ☑ Content information

☑ Site information ☑ Search String information

Limit Detail Result ● Show both blocked and non-blocked records

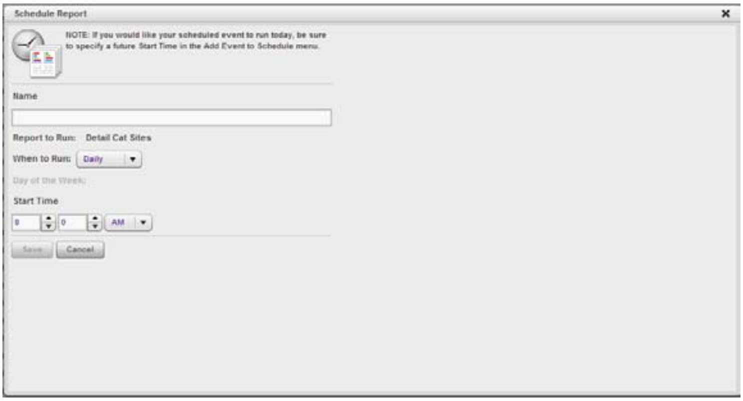
○ Show blocked records only

☑ Show first 1000 records

Fig. 4:2-10 Save Report, Advanced Options tab for detail reports

After all modifications are made, click one of the save option buttons:

- **Save and Schedule** to open the Schedule Report pop-up window where a schedule can be set up for running the report:



Schedule Report

NOTE: If you would like your scheduled event to run today, be sure to specify a future Start Time in the Add Event to Schedule menu.

Name

Report to Run: Detail Cat Sites

When to Run: Daily

Day of the Week:

Start Time

0 0 AM

Fig. 4:2-11 Save Report, Schedule Report option

- **Save and Email** to save the report in the specified format and then email it to the designated email address(es).
- **Save Only** to save the report.

NOTE*: See Report Wizard and Report Schedule in Chapter 3 for information about using these report options.*

Report View Components

Report Fields and Usage

The following fields are used in the summary and detail drill down productivity Report Wizard, Save Report, and/or summary or detail report views and pop-up boxes linked to report views.

Type field

The Type field is used for specifying the report type for the summary report to be generated.

At the **Type** field, make a selection from the pull-down menu for one of the following report types:

- **Categories** - This option performs a query on filter categories accessed by end users.
- **IPs** - This option performs a query on Internet activity by end user IP address.
- **Users** - This option performs a query on end user Internet activity by username.
- **Sites** - This option performs a query on Web sites visited by end users.
- **Category Groups** - This option performs a query on end user Internet activity in Category Groups and Custom Category Groups, the latter which are set up using the Custom Category Groups option from the Administration menu.
- **User Groups** - This option performs a query on Internet activity of User Groups. User Groups are set up using the User Groups option from the Administration menu.

Date Scope and date fields

The Date Scope field is used for specifying the period of time to be included in the generated report view. Reports can be run for any data saved in the SR's memory.

At the **Date Scope** field, make a selection from the pull-down menu for the time frame you wish to use in your query (depending on the scope selected, the from and to date fields are used in conjunction with this field):

- **Today** - This option generates the report view for today only, if logs from the Web Filter have been received and processed.
- **Month to Date** - This option generates the report view for the range of days that includes the first day of the current month through today.
- **Monthly** - Selecting this option activates the **from** and **to** date fields where you specify the date range using the calendar icons.
- **Year to Date** - This option generates the report view for the range of days that includes the first day of the current year through today.
- **Daily** - Selecting this option activates the **from** and **to** date fields where you specify the date range using the calendar icons. The generated report view includes data for the specified days only, if the data for these days are stored on the SR.
- **Yesterday** - This option generates the report view for yesterday only.
- **Month to Yesterday** - This option generates the report view for the range of days that includes the first day of the current month through yesterday.

- **Year to Yesterday** - This option generates the report view for the range of days that includes the first day of the current year through yesterday.
- **Last Week** - This option generates the report view for all days in the past week, beginning with Sunday and ending with Saturday.
- **Last Weekend** - This option generates the report view for the past Saturday and Sunday.
- **Current Week** - This option generates the report view for today and all previous days in the current week, beginning with Sunday and ending with Saturday.
- **Last Month** - This option generates the report view for all days within the past month.

For detail reports, the following fields are additionally available:

- **Part of Today** - This option generates the report view for today within a specified time range. Make a selection for the hour (1-24) and minutes (0-59).
- **Part of Yesterday** - This option generates the report view for yesterday, within a specified time range. Make a selection for the hour (1-24) and minutes (0-59).
- **Part of Specific Day** - This option generates the report view for the date specified via the calendar icon. In the time fields, make a selection for the hour (1-24) and minutes (0-59).
- **User Defined** - This option generates the report view for the specified time range within the specified date range. In the **from** and **to** fields, use the calendar icons to make selections for the date range. In the time fields, specify the hour (1-24) and minute (0-59) time ranges.

# Records fields

The # Records fields are used for specifying the number of records from the query you wish to include in the summary drill down report view, and how these records will be sorted.

In the **# Records** field, indicate whether the report view should “Show all records” or “Show first ‘x’ records”. If the latter selection is made, the value that displays in this field may have come from the Default Report Settings panel and can be modified.

***NOTE**: The Default Top N Value entry is modified in the Default Report Settings panel, accessible via the Administration menu. See the Default Report Settings panel sub-section in Chapter 3: Report Configuration from the SR Report Manager Administration Section for information about the Default Top N Value.*

Filter and Filter String fields

The filter fields are used for narrowing results that display in the current summary drill down report view.

At the **Filter** field, make a selection from the pull-down menu for the filter term to be used: “None”, “Contains”, “Starts with”, “Ends with”.

The **Filter String** field displays greyed-out if “None” was selected at the Filter field. If any other selection was made at that field, enter text in this field corresponding to the type of filter term to be used.

Sort By and Limit summary result to fields

The sort fields are used for specifying the report view column by which the generated report will be sorted.

For summary drill down reports, at the **Sort By** field, make a selection from the pull-down menu for one of the available sort options: “Name of ‘x’”, “Category Count”, “IP Count”, “User Count”, “Site Count”, “Page Count”, “Object Count”, “Time”, “Hit Count”, “Bandwidth”.

If the “Name of ‘x’” option is selected, the **Limit summary result to field** displays. Make a selection from the pull-down menu for one of the available choices for which the summary report results will be limited: “Top Category Count”, “Top IP Count”, “Top User Count”, “Top Site Count”, “Top Page Count”, “Top Object Count”, “Top Time”, “Top Hit Count”, “Top Bandwidth”.

For detail drill down reports, at the **Sort By** field, make a selection from the pull-down menu for one of the available sort options: "Date", "Category", "User IP", "User", "Site", "Filter Action", "Content Type", "Content", "Search String", "URL".

Order field

For detail drill down reports, at the **Order** field, make a selection from the pull-down menu for the order in which to display the selected sort option column: “Ascending”, “Descending”.

Limit Detail Results fields

Limit Detail Results fields are used for specifying the maximum number of records to be included in the report view.

Select the appropriate radio button:

- **Show all records** - If using the Report Wizard to create a summary drill down report, click this radio button to include all records returned by the report query. In a summary drill down report view, click this button to include all records if generating a detail drill down report view from the current report view.
- **Show first** ‘x’ **records** - Click this radio button to only include the first set of records returned by the report query, and make an entry to specify the maximum number of records. This logic applies when using the Report Wizard to create a summary drill down report, and when generating a detail drill down report view from the current summary drill down report view.
- **Show both blocked and non-blocked records** - For a detail drill down report, click this radio button to include records for URLs that were blocked, as well as those that were not blocked.
- **Show blocked records only** - For a detail drill down report, click this radio button to only include records for URLs that were blocked.

Break Type field

The Break Type field is used for indicating the manner in which records will display for the specified report view when exported.

Choose from the available report selections at the **Break Type** pull-down menu. Based on the current report view displayed, the selections in this menu might include the main report type such as “Sites”, double-break report types such as “Users/Sites”, triple-break report types such as “User/Category/IPs”, or pie or bar charts.

Format field

The Format field is used for specifying the manner in which text from the report view will be outputted.

At the **Format** pull-down menu, choose the format for the report: “MS-DOS Text”, “PDF”, “Rich Text Format”, “HTML”, “Comma-Delimited Text”, “Excel (Chinese)”, “Excel (English)”.

Data to Export field

The Data to Export field is used for specifying which records will be exported when the generated summary drill down report is emailed or viewed.

At the **Data to Export** field pull-down menu, specify the amount of data to be exported: “All the rows on this report”, “Only rows on this page”, or “Only selected rows on this page”.

For additional-break reports only

The # Records and Sort By fields are used when exporting double-break and triple-break summary drill down reports and are deactivated by default.

Records field

The # Records field is used for specifying the number of records that will display for the selected sort option. By default, this field displays greyed-out and becomes activated when a different Break Type is selected.

In the activated **# Records** field, indicate whether to “Show all records” or “Show first ‘x’ records”.

Sort By field

The Sort By field is used for specifying the report view column by which the generated report will be sorted.

For summary drill down reports, at the **Sort By** field, make a selection from the pull-down menu for one of the available sort options: “Category Count”, “IP Count”, “User Count”, “Site Count”, “Page Count”, “Object Count”, “Time”, “Hit Count”, “Bandwidth”.

For pie and bar charts only

Generate Using field

The Generate Using field is used when exporting a drill down Categories, Category Group, or User Group pie chart or bar chart report, and determines by which column the report will be sorted. By default, the field displays greyed-out and becomes activated when a pie or bar chart report is selected from the Break type pull-down menu.

At the activated **Generate Using** field, make a selection from the pull-down menu for the sort option to be used:

“Category Count”, IP Count”, “User Count”, “Site Count”, “Page Count”, “Object Count”, “Time”, “Hit Count”, “Bandwidth”.

Output type field

The Output type field is used for specifying how the generated report will be sent to the recipient(s).

At the **Output type** field, choose either “E-Mail As Attachment”, or “E-Mail As Link”.

Hide un-Identified IPs checkbox

The Hide un-Identified IPs checkbox is used for specifying whether or not IP addresses of workstations that are not assigned to a designated end user will be included in reports. This checkbox is deselected by default if the checkbox by this same name was de-selected in the Default Report Settings panel.

NOTE*: The Default Report Settings panel is accessible via the Administration menu. See the Default Report Settings panel subsection in Chapter 3 of the Report Manager Administration Section for more information about the Hide Unidentified IPs option.*

To change the selection in this field, click the **Hide un-identified IPs** checkbox to remove—or add—a check mark in the checkbox. By entering a check mark in this checkbox, activity on machines not assigned to specific end users will not be included in report views. Changing this selection will not affect the setting previously saved in the Default Report Settings panel.

E-Mail / For e-mail output only fields

E-Mail fields are used for entering email criteria pertinent to the report to be sent to the designated addressee(s).

Specify the following in the **E-Mail** or **For E-Mail output only** fields:

- **To** - Enter the email address of each intended report recipient, separating each address by a comma (,) and a space.
- **Subject** - Type in a brief description about the report.
- **Cc** (optional) - Enter the email address of each intended recipient of a carbon copy of this message, separating each address by a comma (,) and a space.
- **Bcc** (optional) - Enter the email address of each intended recipient of a blind carbon copy of this message, separating each address by a comma (,) and a space.
- **Body** - Type in text pertaining to the report.

Detailed Info fields

Detailed Info fields are used for specifying which columns of data will be excluded from detail drill down reports.

In the **Detailed Info** fields, by default all checkboxes corresponding to detail drill down report columns are selected. Click the checkbox corresponding to any of the following options to remove the check marks and thereby exclude those columns of information from displaying in the report:

- **Category information** - Click this checkbox to exclude the column that displays the library category name.
- **IP information** - Click this checkbox to exclude the column that displays the end user IP address.
- **User information** - Click this checkbox to exclude the column that displays the username.

- **Site information** - Click this checkbox to exclude the column that displays the IP addresses or URLs of sites.
- **Filter Action information** - Click this checkbox to exclude the column that displays the type of filter action used by the Web Filter in creating the record: "Allowed", "Blocked", "Warn Blocked" (for the first warning page that displayed for the end user), "Warn Allowed" (for any subsequent warning page that displayed for the end user), “Quota Blocked” (if a quota blocked the end user), "X-Strike", or "N/A" if the filter action was unclassified at the time the log file was created.
- **Content Type information** - Click this checkbox to exclude the column that displays the method used by the Web Filter in creating the record: “Search KW” (Search Engine Keyword), “URL KW” (URL Keyword), “URL”, “Wildcard”, “Https High” (HTTPS Filtering Level set at High), “X-strike” (X Strikes Blocking), “Pattern” (Proxy Pattern Blocking), or “N/A” if the content was unclassified at the time the log file was created.
- **Content information** - Click this checkbox to exclude the column that displays criteria used for determining the categorization of the record, or “N/A” if unclassified.
- **Search String information** - Click this checkbox to exclude the column that displays the full search string the end user typed into a search engine text box. This column displays pertinent information only if the Search Engine Reporting option is enabled in the Optional Features screen of the System Configuration administrator console user interface.

***NOTE**: Refer to the Optional Features screen sub-section of the System Configuration Section for information about the Search String feature.*

Exporting a Report

The email option for exporting productivity reports lets you electronically send the report in the specified file format to designated personnel.

WARNING*: If using a spam filter on your mail server, email messages or attachments might not be delivered if these messages contain keywords that are set up to be blocked. Consult with the administrator of the mail server for work around solutions between the spam filter and mail server.*

1. In the Export pop-up box, enter the following information:
   - **To** field - Type in the email address of each intended report recipient, separating each address by a comma (,) and a space.
   - **Subject** field (optional) - Type in a brief description about the report.
   - **Cc** field (optional) - Type in the email address of each intended recipient of a carbon copy of this message, separating each address by a comma (,) and a space.
   - **Bcc** field (optional) - Type in the email address of each intended recipient of a blind carbon copy of this message, separating each address by a comma (,) and a space.
   - **Body** field (optional) - Type in text pertaining to the report.
2. Click **Email** to send the report to the designated recipient(s).

WARNING*: Large reports might not be sent due to email size restrictions on your mail server. The maximum size of an email message is often two or three MB. Please consult your mail server administrator for more information about email size restrictions.*

View and Print Options

The view and print options for exporting productivity reports let you view/print the report in the specified file format. The view option lets you make any necessary adjustments to your report file settings prior to printing the report. To print the report, you must have a printer configured for your workstation.

In the Export pop-up box, click the **Download** button to generate and download the report in the specified file format.

NOTE: *Reports generated in the format for MS-DOS Text, Comma-Delimited Text, or Excel (Chinese or English) will display a single row of text for each record. Reports generated in all other formats (PDF, Rich Text Format, HTML) will display any lengthy string of text wrapped around below.*

View and Print Tools

In the browser window containing the report, the tools available via the toolbar let you perform some of the following actions on the open report file:

File:

- **Save** (Ctrl+S) or **Save As** - Save the report file to your local drive
- **Print** (Ctrl+P) - Open the Print dialog box where specifications can be made before printing the report file, such as changing the orientation of the printed page by selecting **Portrait** (vertical) or **Landscape** (horizontal).

Edit:

- **Select All** - Hghlight the entire text (Ctrl+A), and then Copy (Ctrl+C) and Paste (Ctrl+V) this text in an open file
- Perform a search for text > **Find** - Search for specific text in the file (Ctrl+F)

Sample Report File Formats

The following report file formats are available for emailing and viewing productivity reports: MS-DOS Text, PDF, Rich Text Format, HTML, Comma-Delimited Text, Excel (Chinese), Excel (English).

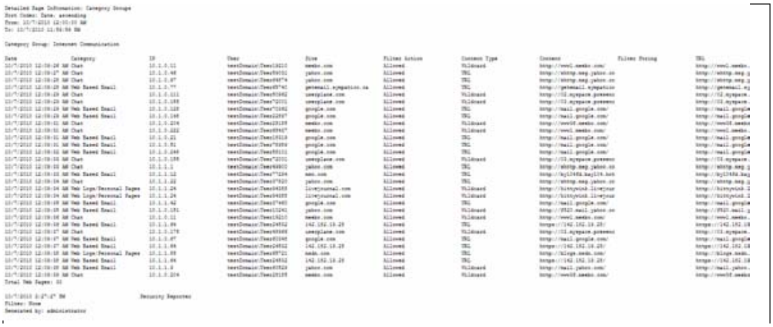
NOTES*: M86 Security recommends using the PDF and HTML file formats over other file format selections—in particular for detail reports—since these files display and print in a format that is easiest to read. Lengthy text in PDF, HTML, and Rich Text Format files wraps around within the column so all text is captured without displaying truncated.*

Comma-Delimited Text and Excel report columns may display with truncated text, but an entire column can be viewed by manipulating the column width in the generated report file. These reports can then be printed at a smaller percentage than normal size in order to accommodate all text.

For MS-DOS Text reports, text may display truncated—in particular for lengthy usernames and URLs in detail reports—but an entire column can be viewed by scrolling to the right. Since there is no way to manipulate text in the generated report file, the printed report may display with truncated text. However, the maximum amount of text can be captured by printing the report in the landscape format.

MS-DOS Text

This is a sample of the Category Groups report in the MS-DOS Text format, saved with a .txt file extension:

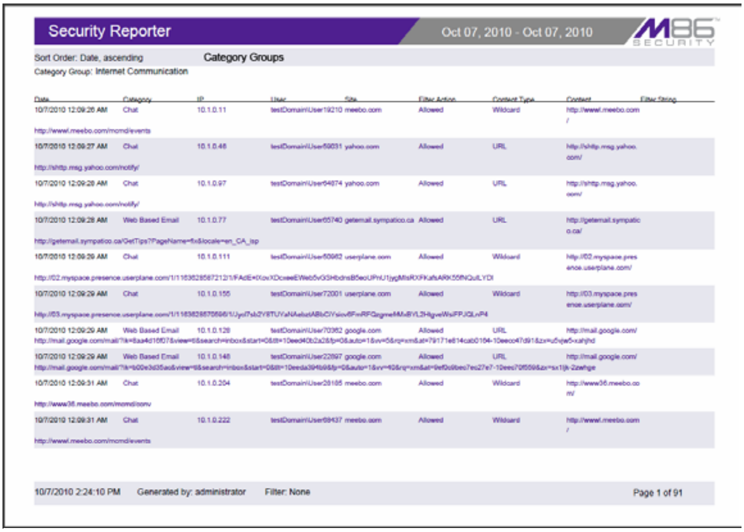


```
Detailed Page Information: Category Groups
Sort Order: Date, ascending
From: 10/7/2010 12:00:00 AM
To: 10/7/2010 11:59:59 PM

Category Group: Internet Communication

Date                   Category                IP           User                   Site                   Filter Action   Content Type   Content                    Filter String   URL
10/7/2010 12:09:26 AM Chat                     10.1.0.11    testDomain\User19210   meebo.com              Allowed         Wildcard       http://www1.meebo.com/                     http://www1.meebo..
10/7/2010 12:09:27 AM Chat                     10.1.0.48    testDomain\User59031   yahoo.com              Allowed         URL            http://shttp.msg.yahoo.co                  http://shttp.msg.y
10/7/2010 12:09:28 AM Chat                     10.1.0.97    testDomain\User64874   yahoo.com              Allowed         URL            http://shttp.msg.yahoo.co                  http://shttp.msg.y
10/7/2010 12:09:28 AM Web Based Email          10.1.0.77    testDomain\User65740   getemail.sympatico.ca  Allowed         URL            http://getemail.sympatico                  http://getemail.sy
10/7/2010 12:09:29 AM Chat                     10.1.0.111   testDomain\User50962   userplane.com          Allowed         Wildcard       http://02.myspace.presenc                  http://02.myspace.
10/7/2010 12:09:29 AM Chat                     10.1.0.155   testDomain\User72001   userplane.com          Allowed         Wildcard       http://03.myspace.presenc                  http://03.myspace.
10/7/2010 12:09:29 AM Web Based Email          10.1.0.128   testDomain\User70362   google.com             Allowed         URL            http://mail.google.com/                    http://mail.google
10/7/2010 12:09:29 AM Web Based Email          10.1.0.148   testDomain\User22897   google.com             Allowed         URL            http://mail.google.com/                    http://mail.google
10/7/2010 12:09:31 AM Chat                     10.1.0.204   testDomain\User28185   meebo.com              Allowed         Wildcard       http://www36.meebo.com/                    http://www36.meebo
10/7/2010 12:09:31 AM Chat                     10.1.0.222   testDomain\User69437   meebo.com              Allowed         Wildcard       http://www1.meebo.com/                     http://www1.meebo..
10/7/2010 12:09:31 AM Web Based Email          10.1.0.21    testDomain\User19319   google.com             Allowed         URL            http://mail.google.com/                    http://mail.google
10/7/2010 12:09:31 AM Web Based Email          10.1.0.81    testDomain\User73359   google.com             Allowed         URL            http://mail.google.com/                    http://mail.google
10/7/2010 12:09:32 AM Web Based Email          10.1.0.246   testDomain\User55111   google.com             Allowed         URL            http://mail.google.com/                    http://mail.google
10/7/2010 12:09:33 AM Chat                     10.1.0.155   testDomain\User72001   userplane.com          Allowed         Wildcard       http://03.myspace.presenc                  http://03.myspace.
10/7/2010 12:09:33 AM Chat                     10.1.1.1     testDomain\User69900   yahoo.com              Allowed         URL            http://shttp.msg.yahoo.co                  http://shttp.msg.y
10/7/2010 12:09:33 AM Web Based Email          10.1.1.12    testDomain\User77104   msn.com                Allowed         URL            http://by124fd.bay124.hot                  http://by124fd.bay
10/7/2010 12:09:34 AM Chat                     10.1.1.22    testDomain\User87920   yahoo.com              Allowed         URL            http://shttp.msg.yahoo.co                  http://shttp.msg.y
10/7/2010 12:09:34 AM Web Logs/Personal Pages  10.1.1.24    testDomain\User04183   livejournal.com        Allowed         Wildcard       http://kittywink.livejour                  http://kittywink.l
10/7/2010 12:09:34 AM Web Logs/Personal Pages  10.1.1.24    testDomain\User04183   livejournal.com        Allowed         Wildcard       http://kittywink.livejour                  http://kittywink.l
10/7/2010 12:09:35 AM Web Based Email          10.1.1.42    testDomain\User07465   google.com             Allowed         URL            http://mail.google.com/                    http://mail.google
10/7/2010 12:09:35 AM Web Based Email          10.1.0.181   testDomain\User13241   yahoo.com              Allowed         Wildcard       http://f523.mail.yahoo.co                  http://f523.mail.y
10/7/2010 12:09:36 AM Chat                     10.1.0.11    testDomain\User19210   meebo.com              Allowed         Wildcard       http://www1.meebo.com/                     http://www1.meebo..
10/7/2010 12:09:36 AM Web Based Email          10.1.1.99    testDomain\User24532   142.182.19.29          Allowed         URL            https://142.182.19.29/                     https://142.182.19
10/7/2010 12:09:37 AM Chat                     10.1.0.176   testDomain\User65369   userplane.com          Allowed         Wildcard       http://03.myspace.presenc                  http://03.myspace.
10/7/2010 12:09:37 AM Web Based Email          10.1.0.87    testDomain\User63198   google.com             Allowed         URL            http://mail.google.com/                    http://mail.google
10/7/2010 12:09:37 AM Web Based Email          10.1.1.99    testDomain\User24532   142.182.19.29          Allowed         URL            https://142.182.19.29/                     https://142.182.19
10/7/2010 12:09:38 AM Web Logs/Personal Pages  10.1.1.88    testDomain\User88721   msdn.com               Allowed         URL            http://blogs.msdn.com/                     http://blogs.msdn.
10/7/2010 12:09:38 AM Web Based Email          10.1.1.99    testDomain\User24532   142.182.19.29          Allowed         URL            https://142.182.19.29/                     https://142.182.19
10/7/2010 12:09:39 AM Web Based Email          10.1.1.8     testDomain\User63829   yahoo.com              Allowed         Wildcard       http://mail.yahoo.com/                     http://mail.yahoo.
10/7/2010 12:09:39 AM Chat                     10.1.0.204   testDomain\User28185   meebo.com              Allowed         Wildcard       http://www36.meebo.com/                    http://www36.meebo
Total Web Pages: 30

10/7/2010 2:27:27 PM                    Security Reporter
Filter: None
Generated by: administrator
```

Fig. 4:2-12 Category Groups report, MS-DOS Text file format

PDF

This is a sample of the Category Groups report in the PDF format, saved with a .pdf file extension:



Security Reporter Oct 07, 2010 - Oct 07, 2010

Sort Order: Date, ascending   Category Groups

Category Group: Internet Communication

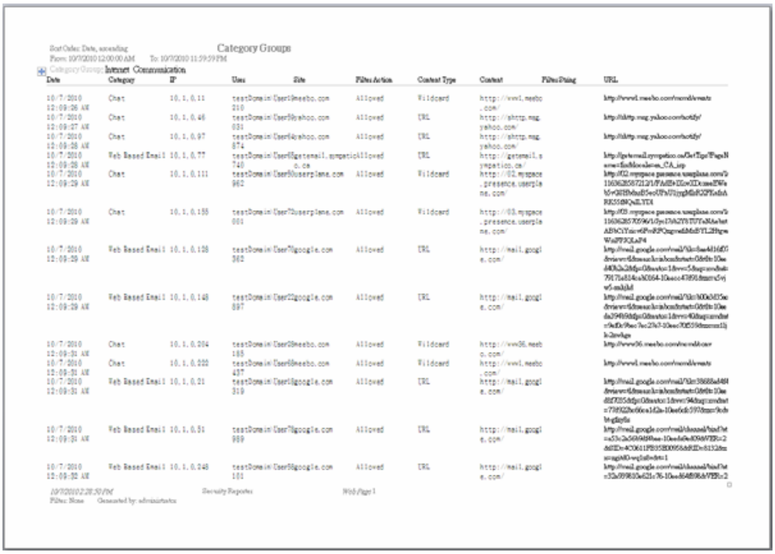
Date	Category	IP	User	Site	Filter Action	Content Type	Content	Filter String
10/7/2010 12:09:26 AM	Chat	10.1.0.11	testDomain\User19210	meebo.com	Allowed	Wildcard	http://www1.meebo.com/	
http://www1.meebo.com/mcmd/events								
10/7/2010 12:09:27 AM	Chat	10.1.0.48	testDomain\User59031	yahoo.com	Allowed	URL	http://shttp.msg.yahoo.com/	
http://shttp.msg.yahoo.com/notify/								
10/7/2010 12:09:28 AM	Chat	10.1.0.97	testDomain\User64874	yahoo.com	Allowed	URL	http://shttp.msg.yahoo.com/	
http://shttp.msg.yahoo.com/notify/								
10/7/2010 12:09:28 AM	Web Based Email	10.1.0.77	testDomain\User65740	getemail.sympatico.ca	Allowed	URL	http://getemail.sympatico.ca/	
http://getemail.sympatico.ca/GetTips?PageName=fx&locale=en_CA_isp								
10/7/2010 12:09:29 AM	Chat	10.1.0.111	testDomain\User50962	userplane.com	Allowed	Wildcard	http://02.myspace.presence.userplane.com/	
http://02.myspace.presence.userplane.com/1/1163828587212/1/FAdE=lXovXDcwwEWeb5vG3HbdnsB5eoUPnU1jygMlsRXFKafsARK55fNQuLYDI								
10/7/2010 12:09:29 AM	Chat	10.1.0.155	testDomain\User72001	userplane.com	Allowed	Wildcard	http://03.myspace.presence.userplane.com/	
http://03.myspace.presence.userplane.com/1/1163828875696/1/Jyd7sb2Y8TUYaNAebzlABbCIYsiov6FmRFQagmeMMxBVL2HlgveWsiFPJQLnP4								
10/7/2010 12:09:29 AM	Web Based Email	10.1.0.128	testDomain\User70362	google.com	Allowed	URL	http://mail.google.com/	
http://mail.google.com/mail/?ik=8aa4d16f07&view=tl&search=inbox&start=0&tlt=10eed40b2a2&fp=0&auto=1&vv=5&rq=xm&at=79171e814cab0164-10eeco47d91&zx=u5vjw5-xahjhd								
10/7/2010 12:09:29 AM	Web Based Email	10.1.0.148	testDomain\User22897	google.com	Allowed	URL	http://mail.google.com/	
http://mail.google.com/mail/?ik=b00e3d35ac&view=tl&search=inbox&start=0&tlt=10eeda394b9&fp=0&auto=1&vv=40&rq=xm&at=9ef0c9bec7ec27e7-10eec70f5598&zx=sx1ljk-2zwhge								
10/7/2010 12:09:31 AM	Chat	10.1.0.204	testDomain\User28185	meebo.com	Allowed	Wildcard	http://www36.meebo.com/	
http://www36.meebo.com/mcmd/conv								
10/7/2010 12:09:31 AM	Chat	10.1.0.222	testDomain\User69437	meebo.com	Allowed	Wildcard	http://www1.meebo.com/	
http://www1.meebo.com/mcmd/events								

10/7/2010 2:24:10 PM   Generated by: administrator   Filter: None   Page 1 of 91

Fig. 4:2-13 Category Groups report, PDF format

Rich Text Format

This is a sample of the Category Groups report in the Rich Text file Format, saved with a .rtf file extension:



Sort Order: Date, ascending   Category Groups
From: 10/7/2010 12:00:00 AM   To: 10/7/2010 11:59:59 PM
Category Group: Internet Communication

Date	Category	IP	User	Site	Filter Action	Content Type	Content	Filter Rating	URL
10/7/2010 12:09:26 AM	Chat	10.1.0.11	testDomain\User19 210	meebo.com	Allowed	Wildcard	http://www1.meebo.com/		http://www1.meebo.com/mcmd/events
10/7/2010 12:09:27 AM	Chat	10.1.0.46	testDomain\User59 031	yahoo.com	Allowed	URL	http://shttp.msg.yahoo.com/		http://shttp.msg.yahoo.com/notify/
10/7/2010 12:09:28 AM	Chat	10.1.0.97	testDomain\User64 874	yahoo.com	Allowed	URL	http://shttp.msg.yahoo.com/		http://shttp.msg.yahoo.com/notify/
10/7/2010 12:09:28 AM	Web Based Email	10.1.0.77	testDomain\User65 740	getemail.sympatico.ca	Allowed	URL	http://getemail.sympatico.ca/		http://getemail.sympatico.ca/GetTips?PageName=findlocale=en_CA.jsp
10/7/2010 12:09:29 AM	Chat	10.1.0.111	testDomain\User50 962	userplane.com	Allowed	Wildcard	http://02.myspace.presence.userplane.com/		http://02.myspace.presence.userplane.com/[illegible]
10/7/2010 12:09:29 AM	Chat	10.1.0.155	testDomain\User72 001	userplane.com	Allowed	Wildcard	http://03.myspace.presence.userplane.com/		http://03.myspace.presence.userplane.com/[illegible]
10/7/2010 12:09:29 AM	Web Based Email	10.1.0.128	testDomain\User70 362	google.com	Allowed	URL	http://mail.google.com/		http://mail.google.com/mail/?ik=[illegible]
10/7/2010 12:09:29 AM	Web Based Email	10.1.0.148	testDomain\User22 897	google.com	Allowed	URL	http://mail.google.com/		http://mail.google.com/mail/?ik=[illegible]
10/7/2010 12:09:31 AM	Chat	10.1.0.204	testDomain\User28 185	meebo.com	Allowed	Wildcard	http://www36.meebo.com/		http://www36.meebo.com/mcmd/core
10/7/2010 12:09:31 AM	Chat	10.1.0.222	testDomain\User68 437	meebo.com	Allowed	Wildcard	http://www1.meebo.com/		http://www1.meebo.com/mcmd/events
10/7/2010 12:09:31 AM	Web Based Email	10.1.0.21	testDomain\User18 319	google.com	Allowed	URL	http://mail.google.com/		http://mail.google.com/mail/?ik=[illegible]
10/7/2010 12:09:31 AM	Web Based Email	10.1.0.51	testDomain\User78 989	google.com	Allowed	URL	http://mail.google.com/		http://mail.google.com/mail/channel/bind?at=[illegible]
10/7/2010 12:09:32 AM	Web Based Email	10.1.0.248	testDomain\User58 101	google.com	Allowed	URL	http://mail.google.com/		http://mail.google.com/mail/channel/bind?at=[illegible]

10/7/2010 2:28:50 PM   Security Reports   Web Page 1
Filter: None   Generated by: administrator

Fig. 4:2-14 Category Groups report, RTF format

HTML

This is a sample of the Category Groups report in the HTML format, saved with a .html file extension:

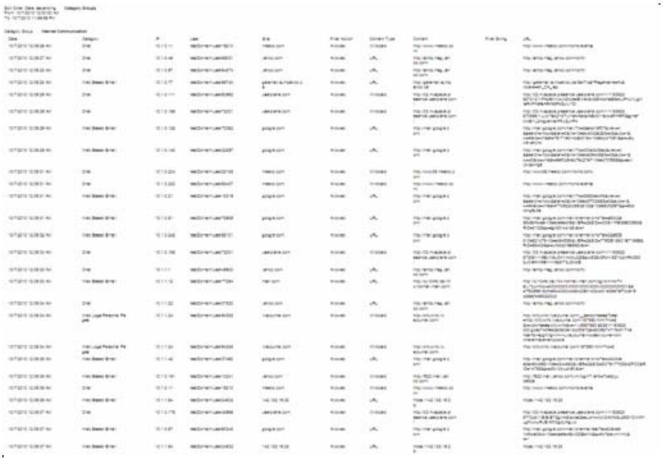


Fig. 4:2-15 Category Groups report, HTML file format

Comma-Delimited Text

This is a sample of the Category Groups report in the Comma-Delimited Text format, saved with a .csv file extension:

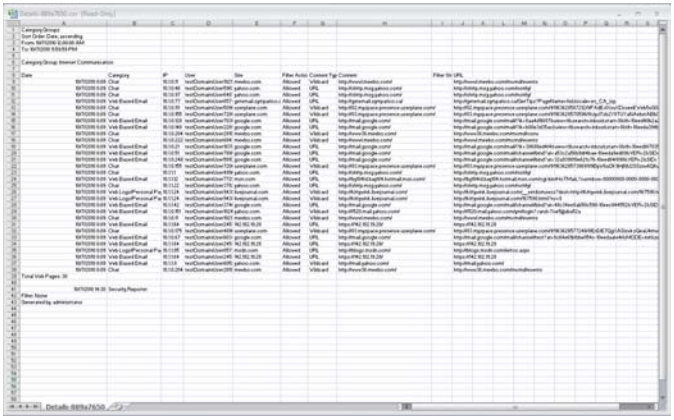
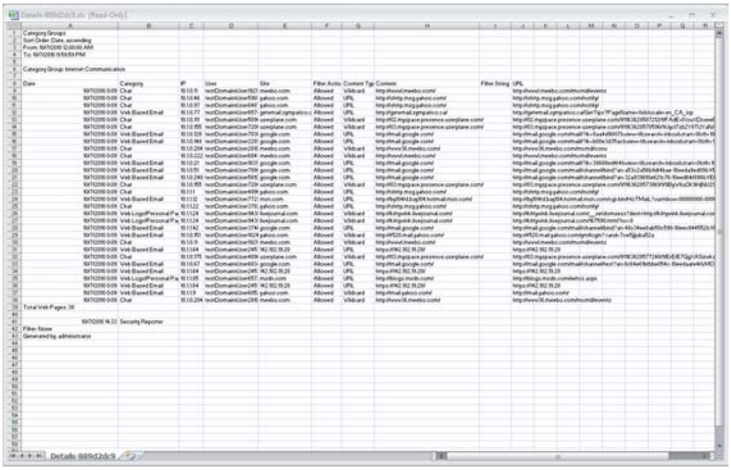


Fig. 4:2-16 Category Groups report, Comma-Delimited Text file

Excel (English)

This is a sample of the Category Groups report in the Excel (English) format, saved with a .xls file extension:



Category Groups
Sort Order: Date, ascending
From: [illegible] 12:00:00 AM
To: [illegible] 11:59:59 PM

Category Group: Internet Communication

Date	Category	IP	User	Site	Filter Action	Content Type	Content	Filter String	URL
[illegible]	Chat	[illegible]	[illegible]	meebo.com	Allowed	Wildcard	http://www.meebo.com/		[illegible]
[illegible]	Chat	[illegible]	[illegible]	yahoo.com	Allowed	URL	http://shttp.msg.yahoo.com/		[illegible]
[illegible]	Chat	[illegible]	[illegible]	yahoo.com	Allowed	URL	http://shttp.msg.yahoo.com/		[illegible]
[illegible]	Web Based Email	[illegible]	[illegible]	genemail.sympatico.c	Allowed	URL	http://genemail.sympatico.ca/		[illegible]
[illegible]	Chat	[illegible]	[illegible]	userplane.com	Allowed	Wildcard	http://r02.myspace.presence.userplane.com/		[illegible]
[illegible]	Chat	[illegible]	[illegible]	userplane.com	Allowed	Wildcard	http://r03.myspace.presence.userplane.com/		[illegible]
[illegible]	Web Based Email	[illegible]	[illegible]	google.com	Allowed	URL	http://mail.google.com/		[illegible]
[illegible]	Web Based Email	[illegible]	[illegible]	google.com	Allowed	URL	http://mail.google.com/		[illegible]
[illegible]	Chat	[illegible]	[illegible]	meebo.com	Allowed	Wildcard	http://www36.meebo.com/		[illegible]
[illegible]	Chat	[illegible]	[illegible]	meebo.com	Allowed	Wildcard	http://www.meebo.com/		[illegible]
[illegible]	Web Based Email	[illegible]	[illegible]	google.com	Allowed	URL	http://mail.google.com/		[illegible]
[illegible]	Web Based Email	[illegible]	[illegible]	google.com	Allowed	URL	http://mail.google.com/		[illegible]
[illegible]	Web Based Email	[illegible]	[illegible]	google.com	Allowed	URL	http://mail.google.com/		[illegible]
[illegible]	Chat	[illegible]	[illegible]	userplane.com	Allowed	Wildcard	http://r03.myspace.presence.userplane.com/		[illegible]
[illegible]	Chat	[illegible]	[illegible]	yahoo.com	Allowed	URL	http://shttp.msg.yahoo.com/		[illegible]
[illegible]	Web Based Email	[illegible]	[illegible]	msn.com	Allowed	URL	http://by304fd.bay304.hotmail.msn.com/		[illegible]
[illegible]	Chat	[illegible]	[illegible]	yahoo.com	Allowed	URL	http://shttp.msg.yahoo.com/		[illegible]
[illegible]	Web Logs/Personal Pa	[illegible]	[illegible]	livejournal.com	Allowed	Wildcard	http://kittypink.livejournal.com/		[illegible]
[illegible]	Web Logs/Personal Pa	[illegible]	[illegible]	livejournal.com	Allowed	Wildcard	http://kittypink.livejournal.com/		[illegible]
[illegible]	Web Based Email	[illegible]	[illegible]	google.com	Allowed	URL	http://mail.google.com/		[illegible]
[illegible]	Web Based Email	[illegible]	[illegible]	yahoo.com	Allowed	Wildcard	http://f520.mail.yahoo.com/		[illegible]
[illegible]	Chat	[illegible]	[illegible]	meebo.com	Allowed	Wildcard	http://www.meebo.com/		[illegible]
[illegible]	Web Based Email	[illegible]	[illegible]	162.182.19.28	Allowed	URL	https://162.182.19.28/		[illegible]
[illegible]	Chat	[illegible]	[illegible]	userplane.com	Allowed	Wildcard	http://r03.myspace.presence.userplane.com/		[illegible]
[illegible]	Web Based Email	[illegible]	[illegible]	google.com	Allowed	URL	http://mail.google.com/		[illegible]
[illegible]	Web Based Email	[illegible]	[illegible]	162.182.19.28	Allowed	URL	https://162.182.19.28/		[illegible]
[illegible]	Web Logs/Personal Pa	[illegible]	[illegible]	msdn.com	Allowed	URL	http://blogs.msdn.com/		[illegible]
[illegible]	Web Based Email	[illegible]	[illegible]	162.182.19.28	Allowed	URL	https://162.182.19.28/		[illegible]
[illegible]	Web Based Email	[illegible]	[illegible]	yahoo.com	Allowed	Wildcard	http://mail.yahoo.com/		http://mail.yahoo.com/
[illegible]	Chat	[illegible]	[illegible]	meebo.com	Allowed	Wildcard	http://www36.meebo.com/		[illegible]

Total Web Pages: 30

[illegible] Security Reporter
Filter: None
Generated by: administrator

Fig. 4:2-17 *Category Groups report, Excel (English) file format*

NOTES*: The Excel (English) option supports up to 65,000 rows of exported data. If exporting more than 65,000 rows of data, M86 Security recommends using another format.*

The Excel (Chinese) option supports up to 10,000 rows of exported data. If exporting more than 10,000 rows of data, M86 Security recommends using the PDF format option.

The number of rows that can be exported varies with each file format.

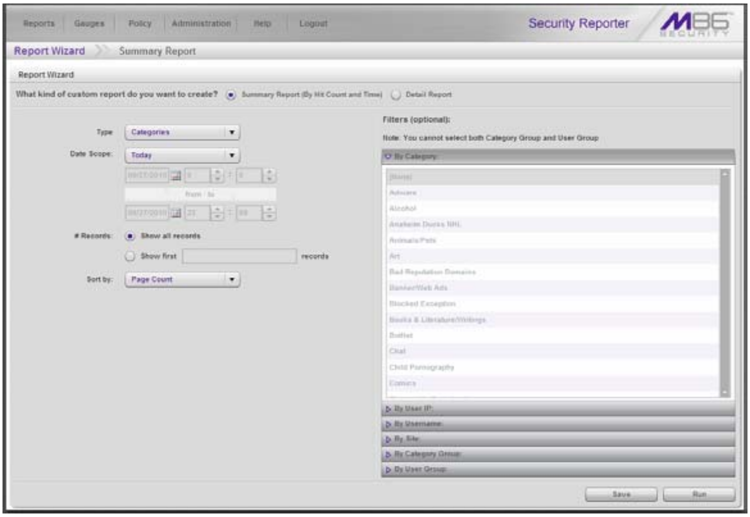
Chapter 3: Customize, Maintain Reports

The following report topics from the Reports menu of the Report Manager are described in this chapter: Report Wizard, Saved Reports, and Report Schedule.

Report Wizard

Report Wizard lets you generate a customized productivity report, querying the database for hits, pages, or objects viewed by end users.

In the navigation toolbar, mouse over the Reports menu link and select **Report Wizard** to display the productivity Report Wizard panel:



Report Wizard

What kind of custom report do you want to create? ● Summary Report (By Hit Count and Time) ○ Detail Report

Type: Categories

Date Scope: Today

Records: ● Show all records

○ Show first records

Sort by: Page Count

Filters (optional):

Note: You cannot select both Category Group and User Group

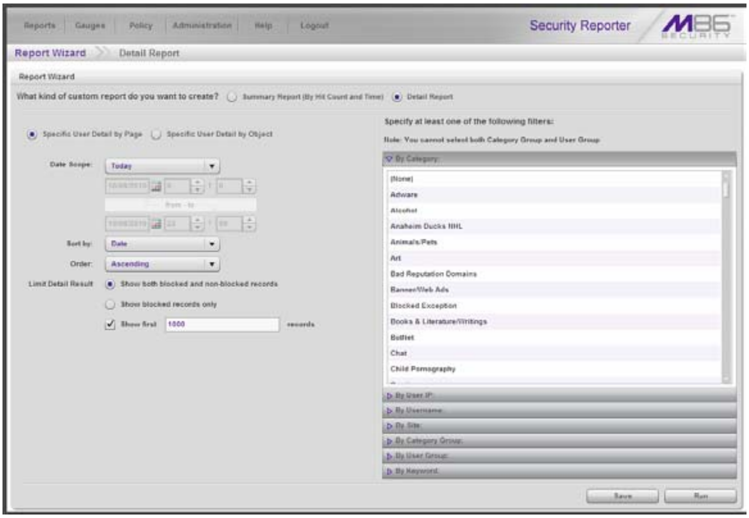
Fig. 4:3-1 Report Wizard panel for summary reports

Step A: Select the Report Option

Select one of two available custom productivity report options:

- **Summary Report (By Hit Count and Time) -** This report provides a synopsis of specified end user Internet activity by hit count and time for a designated period.
- **Detail Report -** This report provides information about end user Web page or Web object access for a specified time period.

The fields that display in this panel depend upon whether a summary report or a detail report is selected.



Report Wizard

What kind of custom report do you want to create? ○ Summary Report (By Hit Count and Time) ● Detail Report

● Specific User Detail by Page ○ Specific User Detail by Object

Date Scope: Today

from - to

Sort by: Date

Order: Ascending

Limit Detail Result ● Show both blocked and non-blocked records

○ Show blocked records only

☑ Show first 1000 records

Specify at least one of the following filters:

Note: You cannot select both Category Group and User Group

By Category:

(None)
Adware
Alcohol
Anaheim Ducks NHL
Animals/Pets
Art
Bad Reputation Domains
Banner/Web Ads
Blocked Exception
Books & Literature/Writings
Botnet
Chat
Child Pornography

By User IP:
By Username:
By Site:
By Category Group:
By User Group:
By Keyword:

Fig. 4:3-2 Report Wizard panel for detail reports

Step B: Specify the Report Type

Summary report

Make a choice for the **Type** of report to be generated: “Categories”, “IPs”, “Users”, “Sites”, “Category Groups”, “User Groups”.

To narrow your results, use the appropriate **Filters (optional)** accordions to the right, described in Step C.

Detail report

1. Choose the type of detail report to use in the query:
    - **Specific User Detail by Page -** Includes viewed page results
    - **Specific User Detail by Object** - Includes viewed object results
2. **Specify at least one of the following filters** in the accordions at right to narrow your search, described in Step C.

Step C: Specify Filters

This step is optional for summary reports, but required for detail reports.

- **By Category -** If selecting this filter, choose the category to filter your report query results.

TIP*: To de-select a Category choose “(None)” from the list.*

- **By User IP** - If selecting this filter, enter the end user IP address for filtering your results—using the ‘%’ wildcard to return multiple IP addresses—and then click **Search** to display query results in the list box below.

TIP*: Click* ***Reset*** *to remove the IP address(es) from the list box.*

- **By Username -** If selecting this filter, enter the end user name to filter your results—using the '%' wildcard to return multiple usernames—and then click **Search** to display query results in the list box below.

  For a detail report, select the username and click the right arrow (>) to move the username into the Added user names list box. Additional searches can be performed to include other usernames in the list box.

***TIP**: For a summary report, click **Reset** to remove the username from the list box. For a detail report, use the left arrow (<) to remove the username from the list box.*

***NOTE**: If more than one username is entered, the following message displays at the bottom of this panel: 'NOTE: This report is very processor and time intensive and may take several minutes to complete.' The report must now be saved and run at a later time.*

- **By Site -** If selecting this filter, enter the site name to filter your results—using the '%' wildcard to return multiple site names—and then click **Search** to display query results in the list box below.

***TIP**: Click **Reset** to remove the site(s) from the list box.*

- **By Category Group -** If selecting this filter, choose the Category Group to filter your report query results.

***TIP**: To de-select a Category Group, choose "(None)" from the list.*

- **By User Group -** If selecting this filter, choose the User Group to filter your report query results.

***TIP**: To de-select a User Group, choose "(None)" from the list.*

- **By Keyword -** This selection is available for detail reports only. If selecting this filter, enter a keyword from three to 255 characters to filter your results, and then click **Add** to include your keyword term in the list box below. More than one keyword can be included in the list box.

***TIP**: To remove a keyword, select the keyword from the list box and click **Remove**.*

***NOTE**: If a keyword is entered, the following message displays at the bottom of this panel: 'NOTE: This report is very processor and time intensive and may take several minutes to complete.' The report must now be saved and run at a later time.*

Step D: Specify Other Report Components

Specify criteria for the remaining components to be used in the report:

- **Date Scope -** Choose the date scope to be included in the results.

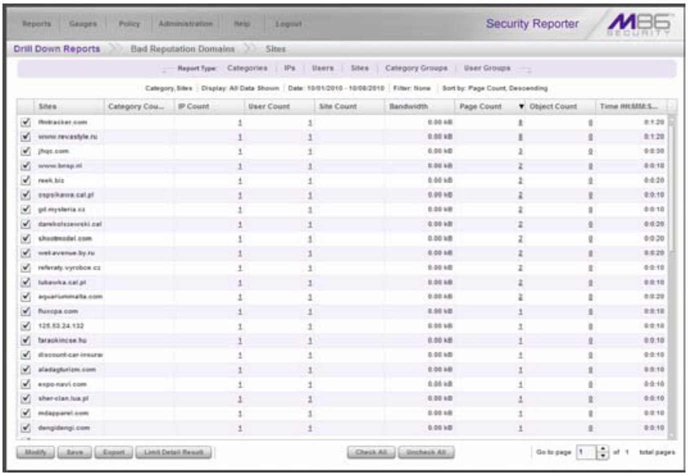
***NOTE**: For detail reports, if more than one username or if any keyword is entered in this panel, the following Date Scope choices are the only choices available: "Yesterday" (default), "Previous 7 Days", selections for Previous 6, 5, 4, 3, or 2 Days, and "Daily".*

- **# Records -** For a summary report, specify the number of records to be returned in the results.
- **Sort by** - Select column by which the results will be sorted and displayed in the report.
- **Order** - For a detail report, indicate whether results will be sorted in "Ascending" or "Descending" order.
- **Limit Detail Result -** For a detail report, specify the number of records to be returned in the results, and if these records will only include records of blocked end user queries, or also records of non-blocked end user queries.

Step E: Specify when to Generate the Report

Indicate the next step in the wizard by selecting one of two choices that specify when the report will be generated:

- **Run** - Click this button to generate and view the drill down report now in the specified report view format.

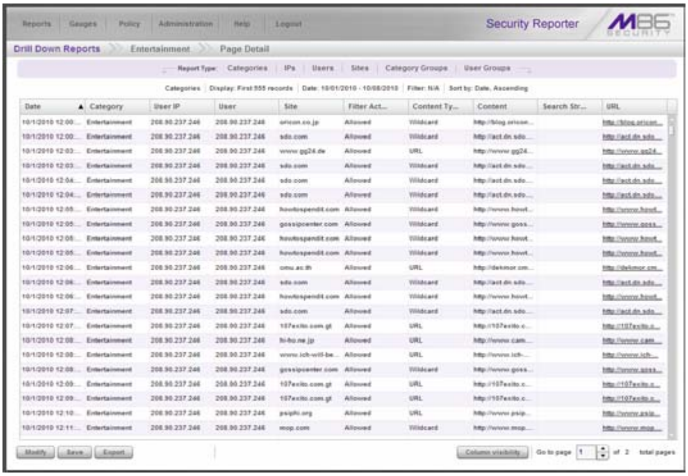


Category, Sites | Display: All Data Shown | Date: 10/01/2010 - 10/08/2010 | Filter: None | Sort by: Page Count, Descending

	Sites	Category Cou...	IP Count	User Count	Site Count	Bandwidth	Page Count ▼	Object Count	Time HH:MM:S...
☑	ifmtracker.com		1	1		0.00 kB	8	0	0:1:20
☑	www.revastyle.ru		1	1		0.00 kB	8	0	0:1:20
☑	jhqc.com		1	1		0.00 kB	3	0	0:0:30
☑	www.bnsp.nl		1	1		0.00 kB	2	0	0:0:10
☑	reek.biz		1	1		0.00 kB	2	0	0:0:20
☑	czpsikawa.cal.pl		1	1		0.00 kB	2	0	0:0:10
☑	gd.mysteria.cz		1	1		0.00 kB	2	0	0:0:10
☑	darekolszewski.cal		1	1		0.00 kB	2	0	0:0:20
☑	shootmodel.com		1	1		0.00 kB	2	0	0:0:20
☑	wet.avenue.by.ru		1	1		0.00 kB	2	0	0:0:20
☑	referaty.vyrobce.cz		1	1		0.00 kB	2	0	0:0:10
☑	lubawka.cal.pl		1	1		0.00 kB	2	0	0:0:10
☑	aquariummalta.com		1	1		0.00 kB	2	0	0:0:20
☑	fluxcpa.com		1	1		0.00 kB	1	0	0:0:10
☑	125.83.24.132		1	1		0.00 kB	1	0	0:0:10
☑	faraokincse.hu		1	1		0.00 kB	1	0	0:0:10
☑	discount-car-insurai		1	1		0.00 kB	1	0	0:0:10
☑	aladagturizm.com		1	1		0.00 kB	1	0	0:0:10
☑	expo-navi.com		1	1		0.00 kB	1	0	0:0:10
☑	sher-clan.lua.pl		1	1		0.00 kB	1	0	0:0:10
☑	mdapparel.com		1	1		0.00 kB	1	0	0:0:10
☑	dengidengi.com		1	1		0.00 kB	1	0	0:0:10

Go to page 1 of 1 total pages

Fig. 4:3-3 Summary drill down report



Categories | Display: First 555 records | Date: 10/01/2010 - 10/08/2010 | Filter: N/A | Sort by: Date, Ascending

Date ▲	Category	User IP	User	Site	Filter Act...	Content Ty...	Content	Search Str...	URL
10/1/2010 12:00:...	Entertainment	208.90.237.246	208.90.237.246	oricon.co.jp	Allowed	Wildcard	http://blog.oricon...		http://blog.oricon...
10/1/2010 12:00:...	Entertainment	208.90.237.246	208.90.237.246	sdo.com	Allowed	Wildcard	http://act.dn.sdo...		http://act.dn.sdo...
10/1/2010 12:03:...	Entertainment	208.90.237.246	208.90.237.246	www.gg24.de	Allowed	URL	http://www.gg24...		http://www.gg24...
10/1/2010 12:03:...	Entertainment	208.90.237.246	208.90.237.246	sdo.com	Allowed	Wildcard	http://act.dn.sdo...		http://act.dn.sdo...
10/1/2010 12:04:...	Entertainment	208.90.237.246	208.90.237.246	sdo.com	Allowed	Wildcard	http://act.dn.sdo...		http://act.dn.sdo...
10/1/2010 12:04:...	Entertainment	208.90.237.246	208.90.237.246	sdo.com	Allowed	Wildcard	http://act.dn.sdo...		http://act.dn.sdo...
10/1/2010 12:05:...	Entertainment	208.90.237.246	208.90.237.246	howtospendit.com	Allowed	Wildcard	http://www.howt...		http://www.howt...
10/1/2010 12:05:...	Entertainment	208.90.237.246	208.90.237.246	gossipcenter.com	Allowed	Wildcard	http://www.goss...		http://www.goss...
10/1/2010 12:05:...	Entertainment	208.90.237.246	208.90.237.246	howtospendit.com	Allowed	Wildcard	http://www.howt...		http://www.howt...
10/1/2010 12:05:...	Entertainment	208.90.237.246	208.90.237.246	howtospendit.com	Allowed	Wildcard	http://www.howt...		http://www.howt...
10/1/2010 12:06:...	Entertainment	208.90.237.246	208.90.237.246	cmu.ac.th	Allowed	URL	http://dekmor.cm...		http://dekmor.cm...
10/1/2010 12:06:...	Entertainment	208.90.237.246	208.90.237.246	sdo.com	Allowed	Wildcard	http://act.dn.sdo...		http://act.dn.sdo...
10/1/2010 12:06:...	Entertainment	208.90.237.246	208.90.237.246	howtospendit.com	Allowed	Wildcard	http://www.howt...		http://www.howt...
10/1/2010 12:07:...	Entertainment	208.90.237.246	208.90.237.246	sdo.com	Allowed	Wildcard	http://act.dn.sdo...		http://act.dn.sdo...
10/1/2010 12:07:...	Entertainment	208.90.237.246	208.90.237.246	107exito.com.gt	Allowed	URL	http://107exito.c...		http://107exito.c...
10/1/2010 12:08:...	Entertainment	208.90.237.246	208.90.237.246	hi-ho.ne.jp	Allowed	URL	http://www.cam...		http://www.cam...
10/1/2010 12:08:...	Entertainment	208.90.237.246	208.90.237.246	www.ich-will-be...	Allowed	URL	http://www.ich-...		http://www.ich-...
10/1/2010 12:08:...	Entertainment	208.90.237.246	208.90.237.246	gossipcenter.com	Allowed	Wildcard	http://www.goss...		http://www.goss...
10/1/2010 12:09:...	Entertainment	208.90.237.246	208.90.237.246	107exito.com.gt	Allowed	URL	http://107exito.c...		http://107exito.c...
10/1/2010 12:09:...	Entertainment	208.90.237.246	208.90.237.246	107exito.com.gt	Allowed	URL	http://107exito.c...		http://107exito.c...
10/1/2010 12:10:...	Entertainment	208.90.237.246	208.90.237.246	psiphi.org	Allowed	URL	http://www.psip...		http://www.psip...
10/1/2010 12:11:...	Entertainment	208.90.237.246	208.90.237.246	mop.com	Allowed	Wildcard	http://www.mop...		http://www.mop...

Go to page 1 of 2 total pages

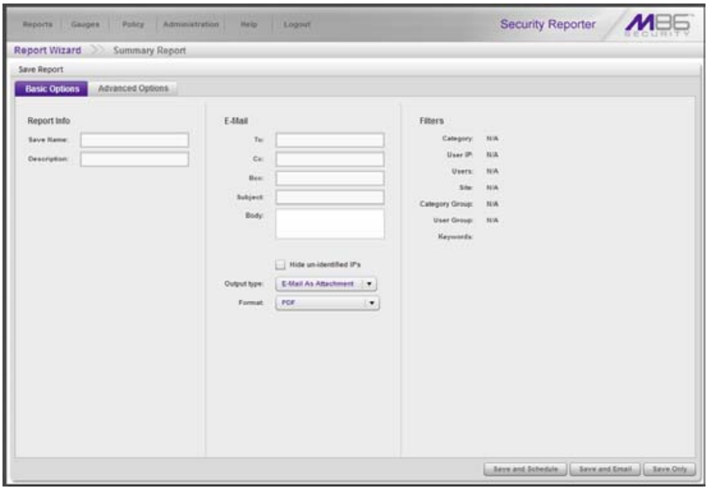
Fig. 4:3-4 Detail by page drill down report

- **Save** - Click this button to go to the Save Report panel where you save your report criteria now but generate your report later (see Save Custom Report).

NOTE*: See Save Custom Report in this chapter for information on using the Save Custom Report window, and Chapter 2: Drill Down Reports for information about drill down reports.*

Step F: Save Report panel

1. Click the **Save** button to display the Basic Options tab of the Report Wizard > Save Report panel:



Report Info
Save Name:
Description:

E-Mail
To:
Cc:
Bcc:
Subject:
Body:
□ Hide un-identified IP's
Output type: E-Mail As Attachment
Format: PDF

Filters
Category: N/A
User IP: N/A
Users: N/A
Site: N/A
Category Group: N/A
User Group: N/A
Keywords:

Fig. 4:3-5 Report Wizard's Save Report panel Basic Options tab

This panel is similar in design to the Save Report pop-up window that displays when saving a drill down report (see Chapter 2: Drill Down Reports). However, the Date Scope does not display in this panel.

2. In the **Save Name** field, enter a name for the report. This name will display in the Reports > Saved Reports list box.

***TIP**: The Copy (Ctrl+C) and Paste (Ctrl+V) functions can be used in the fields in this screen.*

3. In the **Description** field, enter the report description.
4. Specify **E-Mail** criteria:
   - **To** and **Subject**, and optional fields for Body, Cc, and Bcc.
   - **Hide un-identified IPs** checkbox is de-selected by default if the “Hide Unidentified IPs” checkbox is de-selected in the Default Report Settings panel.

***NOTE**: The Default Report Settings panel is accessible via Administration > Default Report Settings. See the Default Report Settings sub-section in Chapter 3 of the Report Manager Administration Section for more information about the Hide Unidentified IPs option.*

- **Output type** - Choose either “E-Mail As Attachment”, or “E-Mail As Link”.
- **Format** - Choose from available output format selections in the pull-down menu.

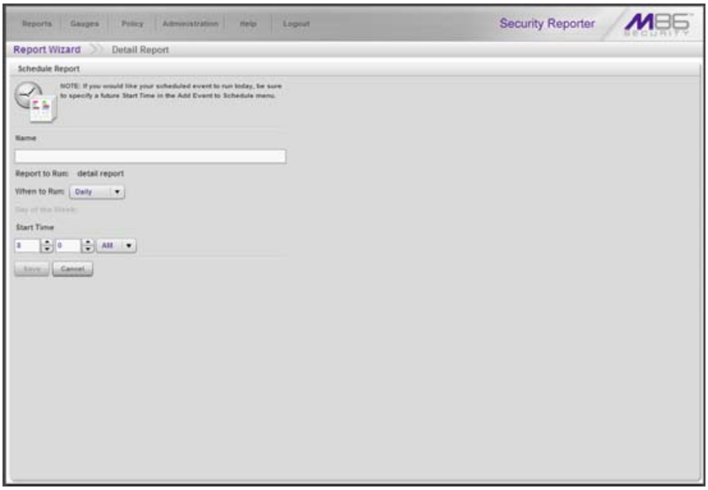
***NOTE**: Any selected filter options display to the right.*

5. Click the Advanced Options tab for additional options:
   - **Break Type** - Available selections are based on the type of report specified.
   - For summary reports, at the **For additional-break reports only** field, if a selection was made in the Break Type field, specify the top count option to be used in the **# Records** and **Sort By** fields.
   - For a summary report, **For pie and bar charts only**, the activated **Generate using** field lets you select the count column sort option.

- For detail reports, specify any of the following options:
  - **Detailed Info** - Uncheck any checkbox corresponding to a column that should not be included in the report.
  - **Limit Detail Result** - Indicate the maximum number of records to be included in the report, and whether these records will only include blocked end user queries, or also records of non-blocked end user queries.

6. Specify the next—or final—step in the wizard by selecting one of three choices:

   - **Save and Schedule -** Click this button to save your entries and to go to the Schedule Report panel where you set up a schedule for running the productivity report:



NOTE: If you would like your scheduled event to run today, be sure to specify a future Start Time in the Add Event to Schedule menu.

Name

Report to Run: detail report

When to Run: Daily

Day of the Week:

Start Time

8 0 AM

Fig. 4:3-6 Report Wizard’s Schedule Report panel

a. Enter a **Name** for the event.

b. Select the **Report to Run** from the list.

c. Select the frequency **When to Run** from the pull-down menu (Daily, Weekly, or Monthly).

If Weekly, specify the **Day of the Week** from the pull-down menu (Sunday - Saturday).

If Monthly, specify the **Day of the Month** from the pull-down menu (1 - 31).

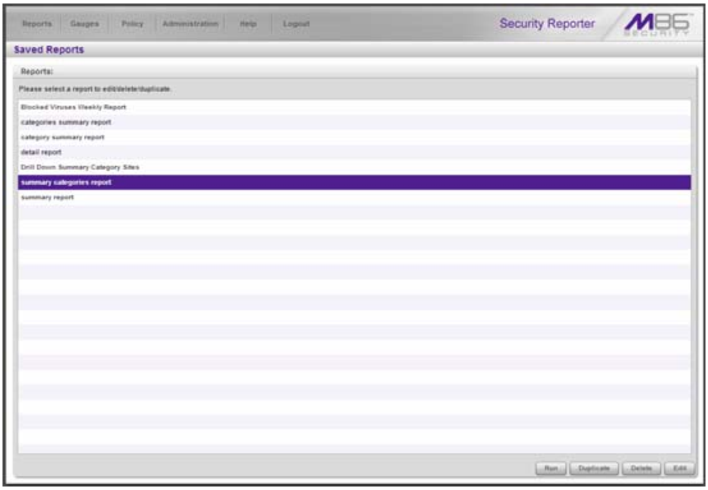
d. Select the **Start Time** for the report: 1 - 12 for the hour, 0 - 59 for the minutes, and AM or PM.

***NOTE**: The default Start Time is 8:00 AM. If you wish to run a report today and this time has already passed, be sure to select a future time.*

e. Click **Save** to save your report schedule settings and to go to the Report Schedule panel where the report is now included in the list (see Fig. 4:3-11).

***TIP**: Click **Cancel** to save the report and to return to the Report Wizard panel without scheduling a time for running the report.*

- **Save and Email** - Click this button to save your entries and to email the generated report to the designated recipient(s). After the report is emailed, the Saved Reports panel displays if you need to run this report again or another report.



Saved Reports

Reports:

Please select a report to edit/delete/duplicate.

Blocked Viruses Weekly Report
categories summary report
category summary report
detail report
Drill Down Summary Category Sites
summary categories report
summary report

Fig. 4:3-7 Saved Reports panel

***NOTE**: If more than one username or if any keyword was entered in the Report Wizard for a detail report, the Save and Email button is greyed-out.*

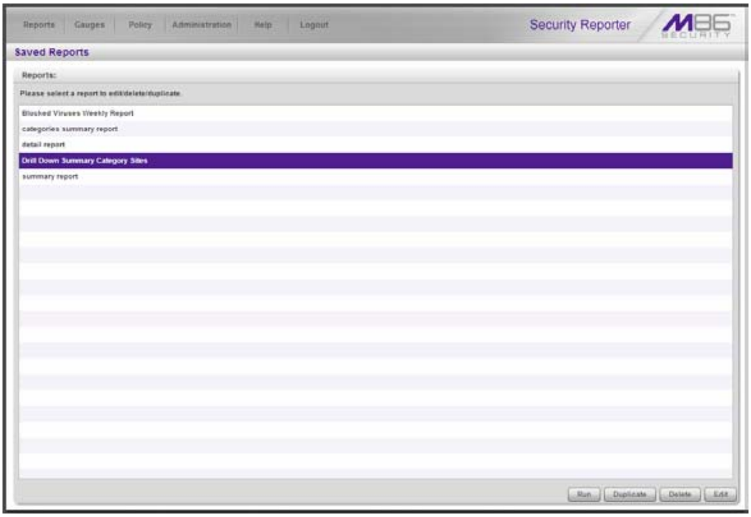
- **Save Only** - Click this button to save your entries and to go to the Saved Reports panel where you can delete, edit, or run this report or another report.

***NOTE**: See Report Schedule and Saved Reports in this chapter for information on using these options.*

Saved Reports

The Saved Reports option lets you view, copy, or edit data in a report you created, run a report, or delete a report.

In the navigation toolbar, mouse over the Reports menu link and select **Saved Reports** to display the Saved Reports panel that displays any productivity drill down reports or security reports you saved:



Saved Reports

Reports:

Please select a report to edit/delete/duplicate

Blocked Viruses Weekly Report
categories summary report
detail report
Drill Down Summary Category Sites
summary report

Fig. 4:3-8 Saved Reports panel

To perform any action in this panel, select the report name from the list to activate the buttons at the bottom right corner.

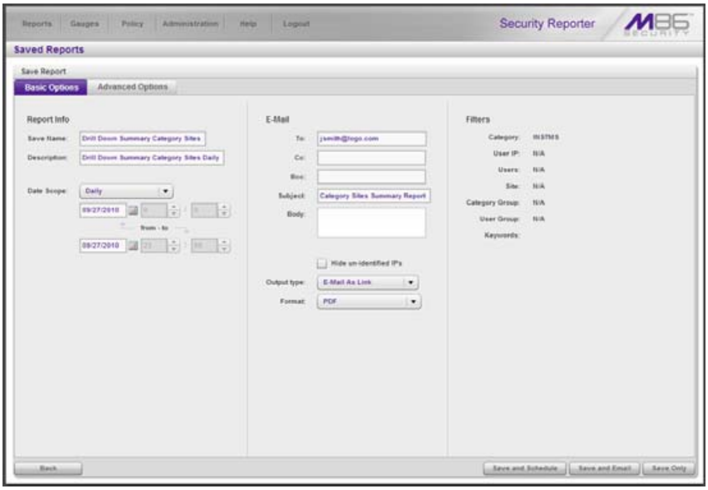
TIP: *On the Save Report panel, click* ***Back*** *to return to the Saved Reports panel without saving your edits or performing any other action.*

NOTES: *Refer to Report View Components in Chapter 2: Drill Down Reports for information on using the fields in the Save Report panel discussed on the following pages in this sub-section. Refer to the Security Reports Section for information on security reports.*

Edit a Report

Edit a Summary or Detail Report

1. To edit a summary or detail productivity report, click **Edit** to display the Save Report panel where you edit report settings for a saved report:



Report Info

Save Name: Drill Down Summary Category Sites

Description: Drill Down Summary Category Sites Daily

Date Scope: Daily

09/27/2010

from - to

09/27/2010

E-Mail

To: jsmith@logo.com

Cc:

Bcc:

Subject: Category Sites Summary Report

Body:

☐ Hide un-identified IPs

Output type: E-Mail As Link

Format: PDF

Filters

Category: INSTMS

User IP: N/A

Users: N/A

Site: N/A

Category Group: N/A

User Group: N/A

Keywords:

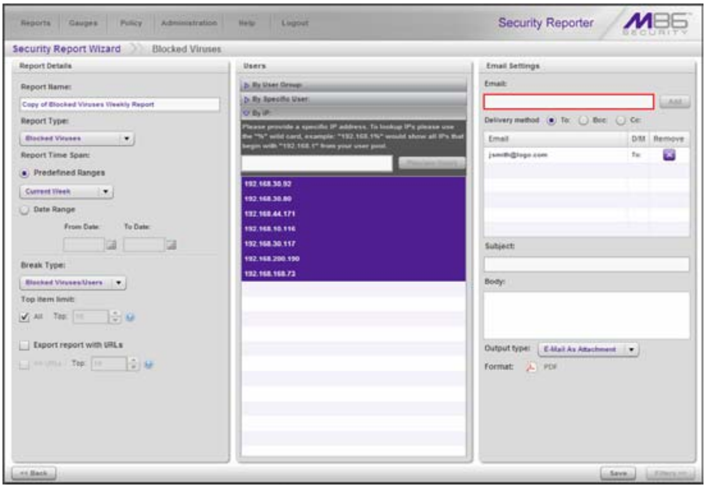
Fig. 4:3-9 Save Report, edit summary report

***TIP**: The Copy (Ctrl+C) and Paste (Ctrl+V) functions can be used in the fields in the Save Report panel.*

2. After making your selections and entries on the Basic Options tab and Advanced Options tab (as described in Save Report panel in this chapter, and for the Save button option in Chapter 2), click **Save Only**.

Edit a Security Report

1. To edit a security report, click **Edit** to display the Security Report Wizard panel where you edit report settings for a saved report:



Report Name: Copy of Blocked Viruses Weekly Report

Report Type: Blocked Viruses

Report Time Span:

● Predefined Ranges: Current Week

○ Date Range — From Date: To Date:

Break Type: Blocked Viruses/Users

Top item limit: ☑ All Top: 10

☐ Export report with URLs

☐ All URLs Top: 10

Please provide a specific IP address. To lookup IP's please use the "%" wild card, example: "192.168.1%" would show all IPs that begin with "192.168.1" from your user pool.

192.168.30.92
192.168.30.80
192.168.44.171
192.168.10.116
192.168.30.117
192.168.200.190
192.168.168.73

Email:

Delivery method ● To: ○ Bcc: ○ Cc:

Email	D/M	Remove
jsmith@logo.com	To:	☒

Subject:

Body:

Output type: E-Mail As Attachment

Format: PDF

Fig. 4:3-10 Save Report, edit Security Report

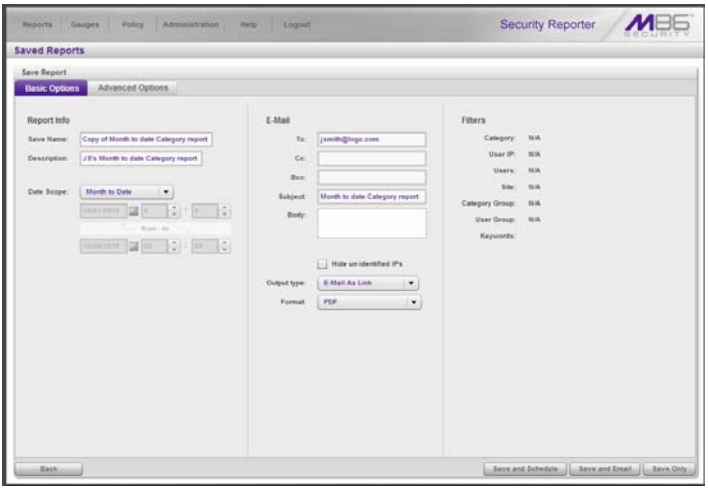
***TIP**: The Copy (Ctrl+C) and Paste (Ctrl+V) functions can be used in the fields in this panel.*

2. After making your selections and entries in the Report Details, Users, and Email Settings frames—and Filters panel, if available for use—(as described in Chapter 2: Security Report Wizard from the Security Reports Section), click **Save**.

Copy a Saved Report

The copy feature is a great time saver, letting you use settings from a saved summary or detail report.

1. In the Saved Reports panel, select the report from the list.
2. Click **Duplicate** to display the panel for the specified report:
    - Save Report panel for a summary or detail productivity report:



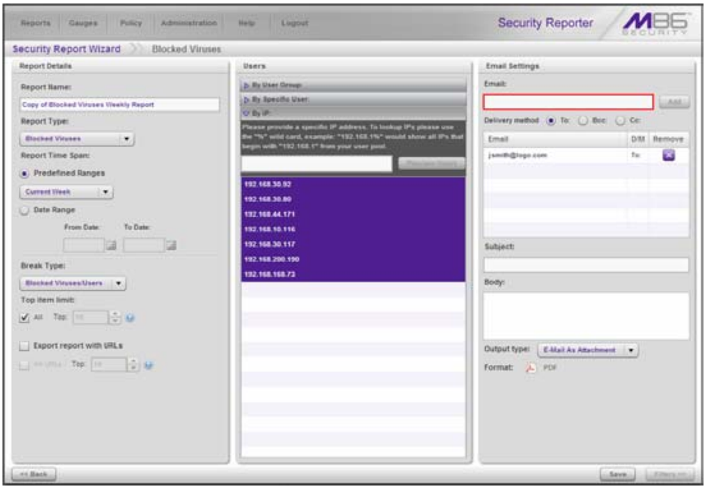
Save Name: Copy of Month to date Category report
Description: J.B's Month to date Category report
Date Scope: Month to Date

To: jsmith@logo.com
Cc:
Bcc:
Subject: Month to date Category report
Body:
Output type: E-Mail As Link
Format: PDF

Category: N/A
User IP: N/A
Users: N/A
Site: N/A
Category Group: N/A
User Group: N/A
Keywords:

Fig. 4:3-11 Save Report, duplicate report

- Security Report Wizard panel for a security report:



Report Name: Copy of Blocked Viruses Weekly Report

Report Type: Blocked Viruses

Report Time Span:

● Predefined Ranges: Current Week

○ Date Range From Date: To Date:

Break Type: Blocked Viruses/Users

Top item limit: ☑ All Top: 10

□ Export report with URLs

□ All URLs Top: 10

Please provide a specific IP address. To lookup IPs please use the "%" wild card, example: "192.168.1%" would show all IPs that begin with "192.168.1" from your user pool.

192.168.30.92
192.168.30.80
192.168.44.171
192.168.10.116
192.168.30.117
192.168.200.190
192.168.168.73

Email:

Delivery method ● To: ○ Bcc: ○ Cc:

Email	D/M	Remove
jsmith@logo.com	To:	☒

Subject:

Body:

Output type: E-Mail As Attachment

Format: PDF

Fig. 4:3-12 Security Report Wizard, duplicate report

***NOTE**: The Report Name field displays the text “Copy of ‘X’”, in which ‘X’ represents the report name of the report being copied. Edit this text if you wish to modify this report name.*

3. After making your selections and entries in the panel:
   - Click **Save Only** in the Save Report panel.
   - Click **Save** in the Security Report Wizard panel.

Run a Saved Report

1. In the Saved Reports panel (see Fig. 4:3-8), select the report from the list.
2. Click **Run** to generate the report view and email the report to the specified recipient(s).

Delete a Report

To remove the report from choices available in the Report Name list, and the list in the Report Schedule panel:

1. In the Saved Reports panel (see Fig. 4:3-8), select the report from the list.
2. Click **Delete** to open the Confirmation dialog box with the message: “Are you sure you wish to delete the report? Event schedules associated will also be deleted.”
3. Click **Yes** to close the dialog box and delete the report.

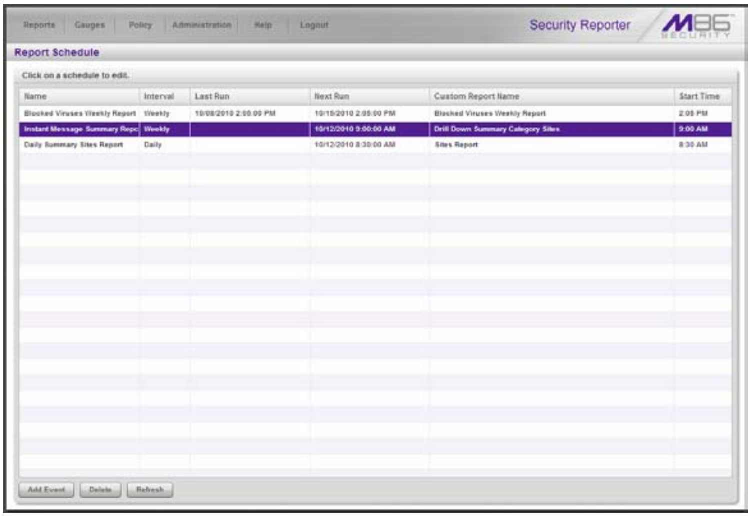
***TIP**: Click **No** to close the dialog box without deleting the report.*

***NOTE**: If a report is scheduled to run via the Report Schedule option, deleting the report removes it from the Report Schedule list.*

Report Schedule

The Report Schedule option is used for maintaining a schedule for generating a customized productivity or security report.

In the navigation toolbar, mouse over the Reports menu link and select **Report Schedule** to display the Report Schedule panel:



Report Schedule

Click on a schedule to edit.

Name	Interval	Last Run	Next Run	Custom Report Name	Start Time
Blocked Viruses Weekly Report	Weekly	10/08/2010 2:00:00 PM	10/15/2010 2:05:00 PM	Blocked Viruses Weekly Report	2:05 PM
Instant Message Summary Repc	Weekly		10/12/2010 9:00:00 AM	Drill Down Summary Category Sites	9:00 AM
Daily Summary Sites Report	Daily		10/12/2010 8:30:00 AM	Sites Report	8:30 AM

Fig. 4:3-13 Report Schedule panel

In the Report Schedule panel, reports scheduled to be run display as rows of records. The following information is included for each record: Name assigned to the scheduled report, Interval when the report is scheduled to run, date and time of the Last Run, date and time of the Next Run, Custom Report Name, and Start Time for the report to run.

NOTES: *Records in this panel may include summary productivity reports, detail productivity reports, and security reports. Security reports are scheduled to run via the Schedule Settings option in the Security Report Wizard (see the Security Reports Section for more information about the Security Report Wizard).*

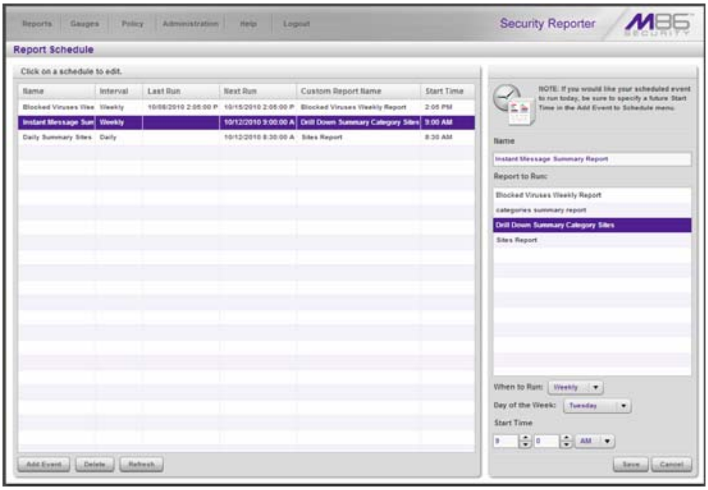
Click the **Refresh** button to refresh the list of records and to scroll to the top of the list.

***NOTE**: Refer to these sub-sections for information about the following topics:*

- *To save summary and detail productivity reports, see the Saved Reports sub-section and the Save Report panel from the Report Wizard sub-section in this chapter, and the Save button sub-section in Chapter 2: Drill Down Reports.*
- *To save security reports, see the Security Reports Section—Save a Security Report in Chapter 1, and Chapter 2: Security Report Wizard.*
- *To enable or disable the Report Manager to run scheduled reports, see the Report Manager screen sub-section of the System Configuration Section in this User Guide.*

View Details for a Scheduled Report Run Event

To view additional information on a scheduled report run event, select the record from the list to display the report schedule details frame to the right of the table of report records:



Report Schedule

Click on a schedule to edit.

Name	Interval	Last Run	Next Run	Custom Report Name	Start Time
Blocked Viruses Wee	Weekly	10/08/2010 2:05:00 P	10/15/2010 2:05:00 P	Blocked Viruses Weekly Report	2:05 PM
Instant Message Sum	Weekly		10/12/2010 9:00:00 A	Drill Down Summary Category Sites	9:00 AM
Daily Summary Sites	Daily		10/12/2010 8:30:00 A	Sites Report	8:30 AM

NOTE: If you would like your scheduled event to run today, be sure to specify a future Start Time in the Add Event to Schedule menu.

Name: Instant Message Summary Report

Report to Run:
Blocked Viruses Weekly Report
categories summary report
Drill Down Summary Category Sites
Sites Report

When to Run: Weekly

Day of the Week: Tuesday

Start Time: 9 : 0 AM

Fig. 4:3-14 View report schedule details

The following information displays in this frame: Name assigned to the scheduled event; selected Report to Run; interval When to Run the report; Day of the Week the report will run if the report is a daily report, or Day of the Month the report will run if the report is a monthly report, and Start Time to run.

TIP*: To remove a report from the Report to Run list, go to the Saved Reports panel and delete that report from the list.*

Edit a Scheduled Report Run Event

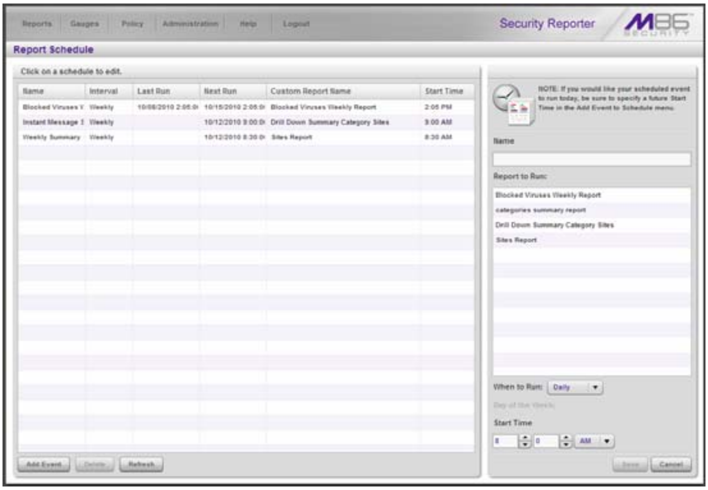
1. To edit criteria for a report scheduled to run, do the following in the report schedule details frame:
   - change the **Name** of the report
   - make different selections as necessary from the pull-down menus for **Report to Run**, **When to Run**, and/or **Day of the Week** or **Day of the Month**
   - change the **Start Time** for running the report

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

2. Click **Save** to display the updated criteria in the Report Schedule panel.

Add a Report Run Event to the Schedule

1. In the Report Schedule panel, click **Add Event** to display the report schedule details frame to the right side of the panel:



Report Schedule

Click on a schedule to edit.

Name	Interval	Last Run	Next Run	Custom Report Name	Start Time
Blocked Viruses V	Weekly	10/08/2010 2:05:0	10/15/2010 2:05:0	Blocked Viruses Weekly Report	2:05 PM
Instant Message 1	Weekly		10/12/2010 9:00:0	Drill Down Summary Category Sites	9:00 AM
Weekly Summary	Weekly		10/12/2010 8:30:0	Sites Report	8:30 AM

NOTE: If you would like your scheduled event to run today, be sure to specify a future Start Time in the Add Event to Schedule menu.

Name

Report to Run:

- Blocked Viruses Weekly Report
- categories summary report
- Drill Down Summary Category Sites
- Sites Report

When to Run: Daily

Day of the Week:

Start Time: 8 : 0 AM

Fig. 4:3-15 Add an event to the schedule

2. Enter a **Name** for the report run event you are scheduling.

3. Select the **Report to Run** from the list.

4. Select the frequency **When to Run** from the pull-down menu (Daily, Weekly, or Monthly).

   If Weekly, specify the **Day of the Week** from the pull-down menu (Sunday - Saturday).

   If Monthly, specify the **Day of the Month** from the pull-down menu (1 - 31).

5. Select the **Start Time** for the report: 1 - 12 for the hour, 0 - 59 for the minutes, and AM or PM.

***NOTE**: The default Start Time is 8:00 AM. If you wish to run a report today and this time has already passed, be sure to select a future time.*

***TIP**: Click **Cancel** to return to the Report Schedule panel without saving your edits.*

6. Click **Save** to add the scheduled event to the list of reports to run.

Delete a Scheduled Report Run Event

1. In the Report Schedule panel, select the report record from the list and click the **Delete**; this action opens a dialog box with the message: “Are you sure you want to delete this event?”
2. Click **Yes** to close the dialog box and remove the record from the list.

***TIP**: Click **Cancel** to return to the Report Schedule panel without deleting the record from the list of reports scheduled to run.*

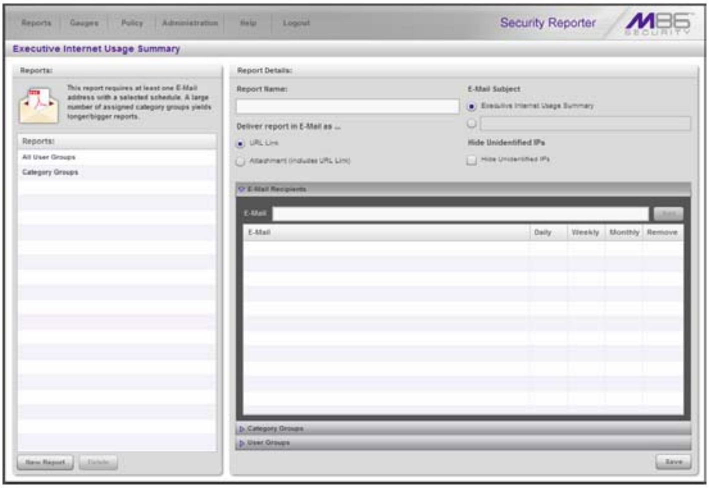
Chapter 4: Specialized Reports

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

Executive Internet Usage Summary

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

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



This report requires at least one E-Mail address with a selected schedule. A large number of assigned category groups yields longer/bigger reports.

Reports:
All User Groups
Category Groups

Report Name:

Deliver report in E-Mail as ...
● URL Link
○ Attachment (includes URL Link)

E-Mail Subject
● Executive Internet Usage Summary
○

Hide Unidentified IPs
□ Hide Unidentified IPs

E-Mail

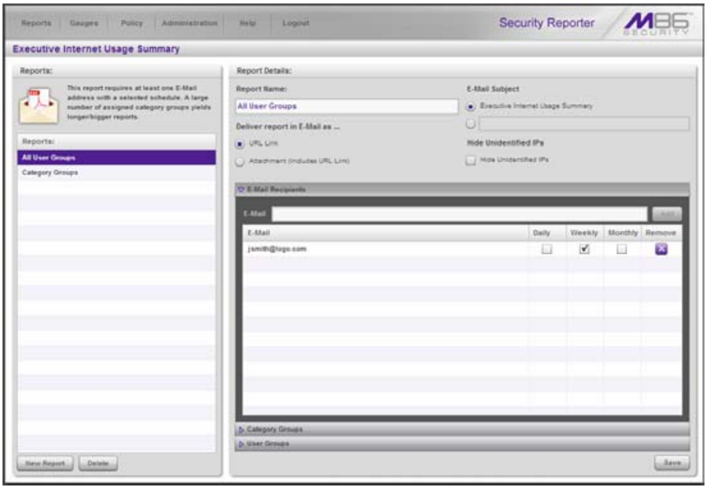
E-Mail	Daily	Weekly	Monthly	Remove

Fig. 4:4-1 Executive Internet Usage Summary panel

This panel contains the Reports frame listing saved report names, and the Report Details frame used for configuring reports.

View, Edit Report Settings

1. In the Reports frame, select the report name to display report setting criteria in the Report Details frame.



Executive Internet Usage Summary

Reports:

This report requires at least one E-Mail address with a selected schedule. A large number of assigned category groups yields longer/bigger reports.

Reports:
- All User Groups
- Category Groups

Report Details:

Report Name: All User Groups

Deliver report in E-Mail as ...
- ● URL Link
- ○ Attachment (includes URL Link)

E-Mail Subject
- ● Executive Internet Usage Summary
- ○

Hide Unidentified IPs
- □ Hide Unidentified IPs

▽ E-Mail Recipients

E-Mail

E-Mail	Daily	Weekly	Monthly	Remove
jsmith@logo.com	□	☑	□	☒

▷ Category Groups

▷ User Groups

Fig. 4:4-2 Executive Internet Usage Summary report details

The following information displays and can be viewed and edited: Report Name, E-Mail Subject criteria, Deliver report in E-Mail as... selection, Hide Unidentified IPs choice, E-Mail Recipients list and report delivery schedule, and Category Groups and/or User Groups selection(s).

2. Click **Save** to update any modifications made to these report settings.

Add a New Report

1. At the bottom of the Reports frame, click **New Report** to clear the panel.
2. At the top of the Report Details frame, enter the **Report Name** to be used.
3. In the **Deliver report in E-Mail as...** section, by default the “URL Link” option is selected, indicating the email will only include a URL link to the report.

   To specify that both a URL link to the report and an attachment of the report will be included in the email, choose the “Attachment (includes URL Link)” option.
4. In the **E-Mail Subject** section, by default the “Executive Internet Usage Summary” option is selected, indicating the subject line to be used in the email.

   To create a custom subject line for the email, select the radio button to the left of the blank field below, and make an entry in the text box for the subject line to be used in the email.
5. In the **Hide Unidentified IPs** section, by default the **Hide Unidentified IPs** checkbox is de-selected. This indicates that activity on machines not assigned to specific users will be included in reports.

   If you wish to exclude activity from machines not assigned to specific users, click in the checkbox to enter a check mark.

***NOTE**: If enabling this feature, the generated report will only hide hit counts for IP addresses in sections of the report labeled “Users.” IP hit counts **will be included** for all other sections of the report, such as those labeled “Categories”, “Category Groups”, etc.*

6. In the E-Mail Recipients accordion, specify the user(s) to receive the report and the frequency of delivery.

a. Click in the empty field and type in the **E-Mail** address.

b. Click **Add** to clear the field and to add the email address in the list box below.

c. By default, checkmarks populate the frequency checkboxes: **Daily**, **Weekly**, **Monthly**. This indicates reports will be emailed to the recipient at the specified intervals.

To change these settings, click the checkbox to remove the selection.

Follow the steps above to add additional recipients.

***TIP**: To remove a recipient from the list of users authorized to receive reports, click the 'X' in the **Remove** column.*

7. Click to open the Category Groups and/or User Groups accordion(s) and specify groups for inclusion in the report:

- In the Category Groups accordion, select the category group(s) from the Available M86 Category Groups and Custom Category Groups, and then click **Add Category Group** to move the selection(s) to the Selected list box.

  By default, the following categories are included in the Selected list box: Adult Content, Security, and Illegal/ Questionable.

***TIPS**: Multiple category groups can be selected by clicking each category group while pressing the Ctrl key on your keyboard. Blocks of category groups can be selected by clicking the first category group, and then pressing the Shift key on your keyboard while clicking the last category group.*

*To remove a category group from the Selected list box, select the category group and then click **Remove Category Group**.*

- In the User Groups accordion, select the user group(s) from the Available User Groups, and then click **Add User Group** to move the selection(s) to the Selected list box.

***TIPS**: Multiple user groups can be selected by clicking each user group while pressing the Ctrl key on your keyboard. Blocks of user groups can be selected by clicking the first user group, and then pressing the Shift key on your keyboard while clicking the last user group.*

*To remove a user group from the Selected list box, select the user group and then click **Remove User Group**.*

8. Click **Save** to save all settings made in this panel and to include the new report in the Reports list box.

Sample Executive Internet Usage report

The recipient of the Executive internet Usage Summary report receives an email containing a link to the report, and a .pdf attachment of the report, if specified (if the size of the .pdf file is within the limits).

Links are available for the following time frame:

- Daily reports (14 days)
- Weekly reports (30 days)
- Monthly reports (90 days)

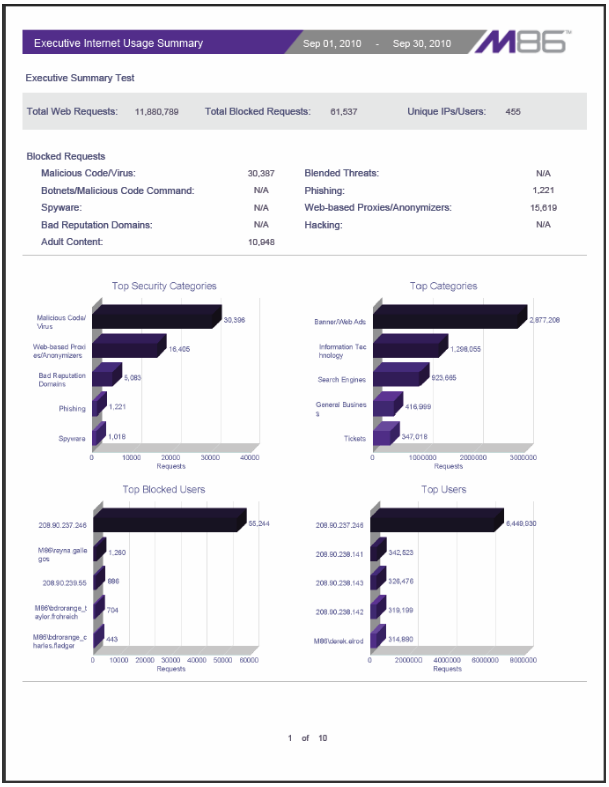
The header of the generated report includes the title and date range. The footer includes the page number and page range.

The first page includes statistics for the following: Total Web Requests, Total Blocked Requests, Unique IPs/Users.

Total Blocked Requests are given for the following library categories: Malicious Code/Virus, Botnets/Malicious Code Command, Spyware, Bad Reputation Domains, Adult Content, Blended Threats, Phishing, Web-based Proxies/ Anonymizers, Hacking.

***NOTE**: Blended Threats is not currently used and displays “N/A.”*

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



Executive Internet Usage Summary Sep 01, 2010 - Sep 30, 2010

Executive Summary Test

Total Web Requests: 11,880,789 Total Blocked Requests: 61,537 Unique IPs/Users: 455

Blocked Requests

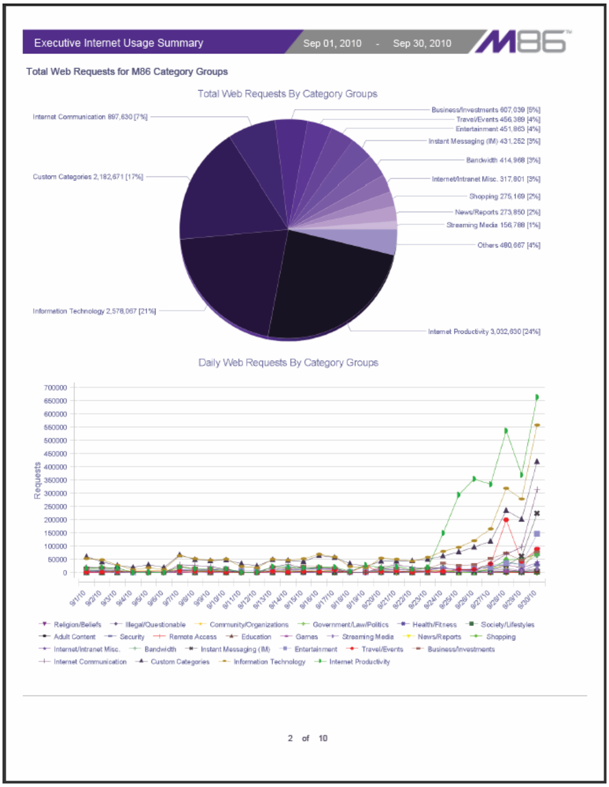
Malicious Code/Virus:	30,387	Blended Threats:	N/A
Botnets/Malicious Code Command:	N/A	Phishing:	1,221
Spyware:	N/A	Web-based Proxies/Anonymizers:	15,619
Bad Reputation Domains:	N/A	Hacking:	N/A
Adult Content:	10,948		

1 of 10

Fig. 4:4-3 Executive Internet Usage Summary monthly report, page 1

The second page includes a pie chart depicting Total Web Requests for M86 Category Groups. Each category group in the chart is represented by a pie slice and shows the number of requests and overall percentage for that pie slice.

For Weekly and Monthly reports, the bottom half of the second page includes a line chart for Daily Web Requests by Category Groups. Each category group in the chart is represented by a colored symbol that can be identified by the key at the bottom of the page. The range of Requests is shown to the left of the chart, and the days (M/D/YY) are shown beneath the chart.



Executive Internet Usage Summary Sep 01, 2010 - Sep 30, 2010

Total Web Requests for M86 Category Groups

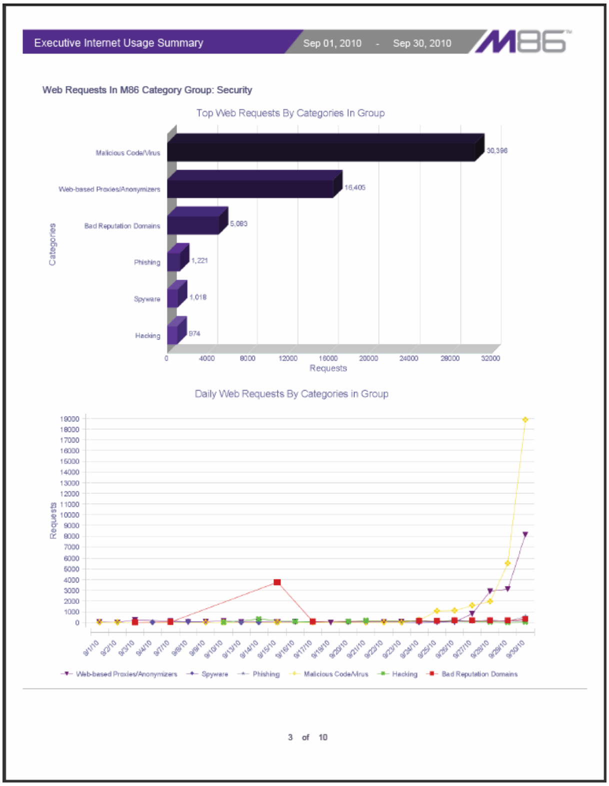
2 of 10

Fig. 4:4-4 Executive Internet Usage Summary monthly report, page 2

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

For Weekly and Monthly reports, the bottom half of the third page includes a line chart for Top Daily Web Requests by

Categories in Group. Each library category in the chart is represented by a colored symbol that can be identified by the key at the bottom of the page. The range of Requests is shown to the left of the chart, and the days (M/D/YY) are shown beneath the chart.


Executive Internet Usage Summary Sep 01, 2010 - Sep 30, 2010

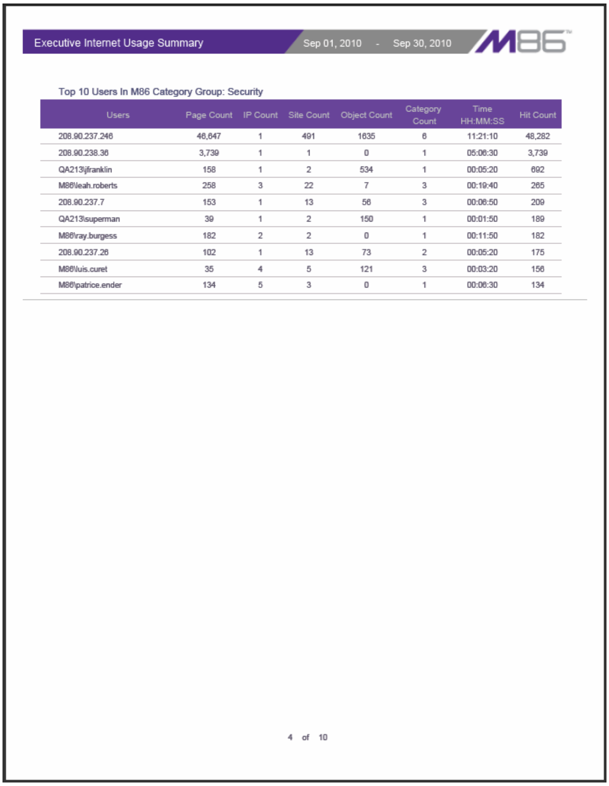
Web Requests In M86 Category Group: Security

3 of 10

Fig. 4:4-5 Executive Internet Usage Summary monthly report, page 3

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

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



Executive Internet Usage Summary Sep 01, 2010 - Sep 30, 2010

Top 10 Users In M86 Category Group: Security

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

4 of 10

Fig. 4:4-6 Executive Internet Usage Summary monthly report, page 4

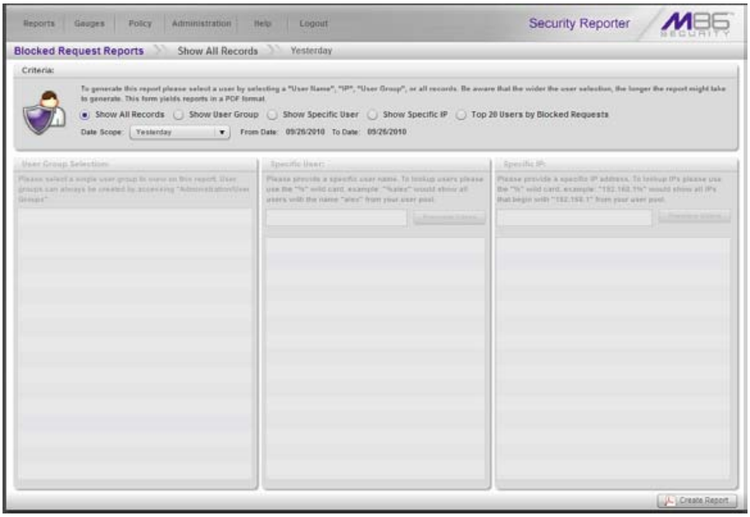
The balance of the report is comprised of statistics for each of the remaining category groups, represented by report page 3, and page 4 for Weekly and Monthly reports.

Blocked Request Reports

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

***NOTE**: If using a Web Filter only, the Blocked Request Reports option does not display if the Block Request Count feature is disabled in the System Configuration administrator console. Refer to the Optional Features screen sub-section of the System Configuration Section of this user guide for information about enabling or disabling the Block Request Count feature.*

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



To generate this report please select a user by selecting a "User Name", "IP", "User Group", or all records. Be aware that the wider the user selection, the longer the report might take to generate. This form yields reports in a PDF format.

● Show All Records ○ Show User Group ○ Show Specific User ○ Show Specific IP ○ Top 20 Users by Blocked Requests

Date Scope: Yesterday ▼ From Date: 09/26/2010 To Date: 09/26/2010

Please select a single user group to view on this report. User groups can always be created by accessing "Administration/User Groups"

Please provide a specific user name. To lookup users please use the "%" wild card, example: "%alex" would show all users with the name "alex" from your user pool.

Please provide a specific IP address. To lookup IPs please use the "%" wild card, example: "192.168.1%" would show all IPs that begin with "192.168.1" from your user pool.

Fig. 4:4-7 Blocked Request Reports panel

Generate a Blocked Request Report

To generate a Blocked Request Report:

1. In the Criteria frame, specify the type of report to be generated by clicking the radio button corresponding to that option, and—if necessary—making entries/selections in pertinent fields:

    - **Show All Records -** If choosing this option, the Date Scope field displays “Yesterday” and yesterday’s date.
    - **Show User Group -** If choosing this option, select the user group from the User Group Selection list box below. The Date Scope field displays “Yesterday” and yesterday’s date.
    - **Show Specific User -** If choosing this option, enter the username—or a portion of the username with the ‘%’ wildcard—in the Specific User frame, and then click **Preview Users** to display results in the list box below. Select the user, and then make a selection from the **Date Scope** field to display the date range for that time period: Yesterday, Last Week, Last Month, Week to Yesterday, Month to Yesterday.
    - **Show Specific IP -** If choosing this option, enter the IP address—or a portion of the IP address with the ‘%’ wildcard—in the Specific IP frame, and then click **Preview Users** to display results in the list box below. Select the user IP address, and then make a selection from the **Date Scope** field to display the date range for that time period: Yesterday, Last Week, Last Month, Week to Yesterday, Month to Yesterday.
    - **Top 20 Users by Blocked Requests -** If choosing this option, make a selection from the **Date Scope** field to display the date range for that time period: Yesterday, Last Week, Last Month, Week to Yesterday, Month to Yesterday.

2. Click **Create Report** to generate the report view in the PDF format.

   As with other reports exported in the PDF format, this report can be saved and/or printed.

NOTES*: If there is no data available—or if data is available for only a partial number of days within the date scope range—a message displays indicating that no records are available.*

If a new user group with existing usernames or IP addresses was added, data for that user group will not be available for viewing on the current day. Data for the following viewing options are available according to this schedule:

- *Yesterday, Week to Yesterday, and Month to Yesterday - available by the next day*
- *Last Week - available by the next Sunday*
- *Last Month - available by the first of next month.*

If a new user group with new users was added, by the next day only the "Yesterday" viewing option will contain data available for viewing. All other viewing options will not be available until the full length of time indicated by the viewing option has transpired.

View the Blocked Request Report

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

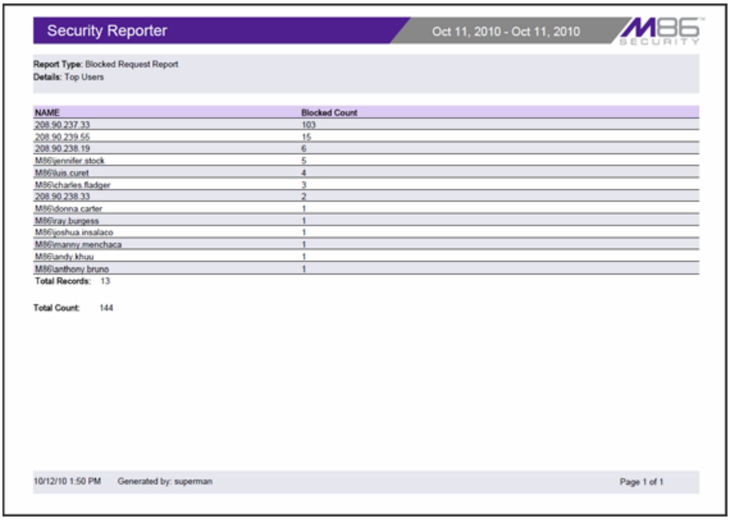
‘RESULTS FOR: the date’ displays above the NAME column header if the report criteria is other than “Top 20 Users by Blocked Requests”.

In the body of the report, rows of records display beneath the following column headers: end user NAME, IP address (if the report criteria is other than “Top 20 Users by Blocked Requests”), and Blocked Count quantity.

If the report was generated for any criteria other than “Top 20 Users by Blocked Requests”, the Total for Day count displays beneath each section.

The footer of the report includes the Date and Time the report was generated, and Page number.

The Total Count for all blocked requests displays at the end of the report.



Security Reporter Oct 11, 2010 - Oct 11, 2010

Report Type: Blocked Request Report
Details: Top Users

NAME	Blocked Count
208.90.237.33	103
208.90.239.55	15
208.90.238.19	6
M86\jennifer.stock	5
M86\luis.curet	4
M86\charles.fladger	3
208.90.238.33	2
M86\donna.carter	1
M86\ray.burgess	1
M86\joshua.insalaco	1
M86\manny.menchaca	1
M86\andy.khuu	1
M86\anthony.bruno	1

Total Records: 13

Total Count: 144

10/12/10 1:50 PM Generated by: superman Page 1 of 1

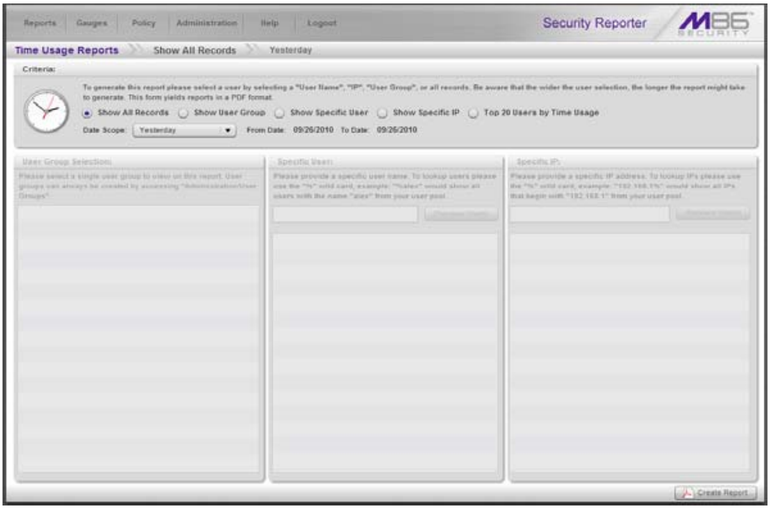
Fig. 4:4-8 Blocked Request Report for Top 20 Users

Time Usage Reports

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

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

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



To generate this report please select a user by selecting a "User Name", "IP", "User Group", or all records. Be aware that the wider the user selection, the longer the report might take to generate. This form yields reports in a PDF format.

● Show All Records ○ Show User Group ○ Show Specific User ○ Show Specific IP ○ Top 20 Users by Time Usage

Date Scope: Yesterday From Date: 09/26/2010 To Date: 09/26/2010

User Group Selection:

Please select a single user group to view on this report. User groups can always be created by accessing "Administration/User Groups".

Specific User:

Please provide a specific user name. To lookup users please use the "%" wild card, example: "%alex" would show all users with the name "alex" from your user pool.

Specific IP:

Please provide a specific IP address. To lookup IPs please use the "%" wild card, example: "192.168.1%" would show all IPs that begin with "192.168.1" from your user pool.

Fig. 4:4-9 Time Usage Reports panel

Generate a Time Usage Report

To generate a Time Usage report:

1. In the Criteria frame, specify the type of report to be generated by clicking the radio button corresponding to that option, and—if necessary—making entries/selections in pertinent fields:

   - **Show All Records** - If choosing this option, the Date Scope field displays “Yesterday” and yesterday’s date.
   - **Show User Group** - If choosing this option, select the user group from the User Group Selection list box below. The Date Scope field displays “Yesterday” and yesterday’s date.
   - **Show Specific User** - If choosing this option, enter the username—or a portion of the username with the ‘%’ wildcard—in the Specific User frame, and then click **Preview Users** to display results in the list box below. Select the user, and then make a selection from the **Date Scope** field to display the date range for that time period: Yesterday, Last Week, Last Month, Week to Yesterday, Month to Yesterday.
   - **Show Specific IP** - If choosing this option, enter the IP address—or a portion of the IP address with the ‘%’ wildcard—in the Specific IP frame, and then click **Preview Users** to display results in the list box below. Select the user IP address, and then make a selection from the **Date Scope** field to display the date range for that time period: Yesterday, Last Week, Last Month, Week to Yesterday, Month to Yesterday.
   - **Top 20 Users by Time Usage** - If choosing this option, make a selection from the **Date Scope** field to display the date range for that time period: Yesterday, Last Week, Last Month, Week to Yesterday, Month to Yesterday.

2. Click **Create Report** to generate the report view in the PDF format.

   As with other reports exported in the PDF format, this report can be saved and/or printed.

***NOTES**: If there is no data available—or if data is available for only a partial number of days within the date scope range—a message displays indicating that no records are available.*

If a new user group with existing usernames or IP addresses was added, data for that user group will not be available for viewing on the current day. Data for the following viewing options are available according to this schedule:

- *Yesterday, Week to Yesterday, and Month to Yesterday - available by the next day*
- *Last Week - available by the next Sunday*
- *Last Month - available by the first of next month.*

If a new user group with new users was added, by the next day only the “Yesterday” viewing option will contain data available for viewing. All other viewing options will not be available until the full length of time indicated by the viewing option has transpired.

View the Time Usage Report

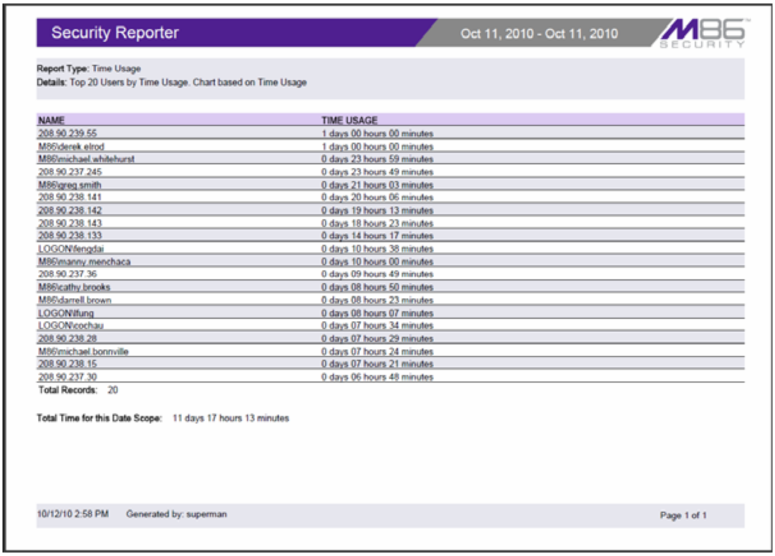
The header of the generated Time Usage report includes the date range, Report Type, and Details criteria.

The body of the report includes the end user NAME, TIME USAGE time totals in days, hours, and minutes, and any other relative criteria, such as username path or IP address.

The Total Records displays at the end of each section.

The footer of the report includes the Date and Time the report was generated, and Page number.

The Total Time for this Date Scope in days, hours, and minutes displays at the end of the report.



Security Reporter

Oct 11, 2010 - Oct 11, 2010

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

NAME	TIME USAGE
208.90.239.55	1 days 00 hours 00 minutes
M86\derek.elrod	1 days 00 hours 00 minutes
M86\michael.whitehurst	0 days 23 hours 59 minutes
208.90.237.245	0 days 23 hours 49 minutes
M86\greg.smith	0 days 21 hours 03 minutes
208.90.238.141	0 days 20 hours 06 minutes
208.90.238.142	0 days 19 hours 13 minutes
208.90.238.143	0 days 18 hours 23 minutes
208.90.238.133	0 days 14 hours 17 minutes
LOGON\fengdai	0 days 10 hours 38 minutes
M86\manny.menchaca	0 days 10 hours 00 minutes
208.90.237.36	0 days 09 hours 49 minutes
M86\cathy.brooks	0 days 08 hours 50 minutes
M86\darrell.brown	0 days 08 hours 23 minutes
LOGON\lfung	0 days 08 hours 07 minutes
LOGON\cochau	0 days 07 hours 34 minutes
208.90.238.28	0 days 07 hours 29 minutes
M86\michael.bonnville	0 days 07 hours 24 minutes
208.90.238.15	0 days 07 hours 21 minutes
208.90.237.30	0 days 06 hours 48 minutes

Total Records: 20

Total Time for this Date Scope: 11 days 17 hours 13 minutes

10/12/10 2:58 PM Generated by: superman Page 1 of 1

Fig. 4:4-10 Sample Time Usage Report for Top 20 Users

Time Usage algorithm

For each end user included in the report, the number of seconds from the log is dropped, and each unique minute within a given hour counts as one minute.

In the following example, the end user shows a total of seven minutes of Time Usage:

```
12:00:01    www.m86security.com
12:00:10    www.abc.com
12:01:00    www.m86security.com
12:02:04    www.whitepages.com
12:05:58    www.yellowpages.com
12:05:58    www.yellowpages.com/714.jsp
12:05:59    www.yellowpages.com/phone_number.gif
12:07:03    www.google.com
12:07:33    www.yahoo.com
12:08:23    www.news.com
12:08:30    www.usatoday.com
12:08:59    www.usatoday.com/usa.gif
12:09:00    www.usatoday.com/ca.gif
12:09:01    www.yahoo.com
12:09:02    http://200.100.10.65:88
12:09:03    www.abc.com
12:09:04    www.nbc.com
```

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

SR REAL TIME REPORTS SECTION

Introduction

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

- Chapter 1: Gauge Components - This chapter describes the types of gauges, the components of a gauge, how to read a gauge, and how to perform shortcuts using gauges.
- Chapter 2: Custom Gauge Setup, Usage - This chapter explains how gauges are configured and monitored.
- Chapter 3: Alerts, Lockout Management - This chapter explains how alerts are set up and used, and how to manage end user lockouts.
- Chapter 4: Analyze Usage Trends - This chapter explains how trend charts are used for assessing end user Internet/network activity.
- Chapter 5: Identify Users, Categories - This chapter explains how to perform a custom search on Internet/ network usage by a specified user, or for a specified category or category group.

Chapter 1: Gauge Components

Types of Gauges

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

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

URL gauges

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

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

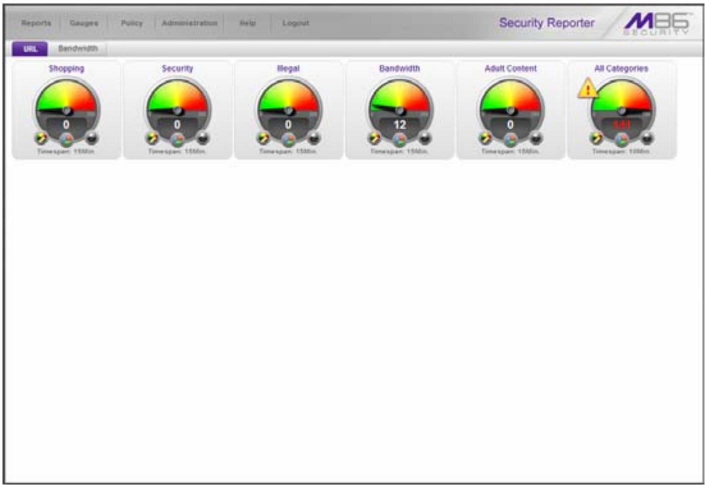


Fig. 5:1-1 URL gauges Dashboard

Bandwidth gauges

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

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

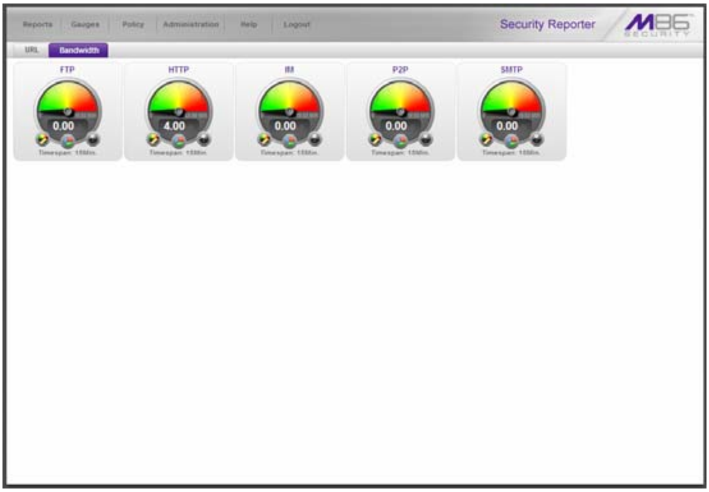


Fig. 5:1-2 Bandwidth gauges Dashboard

Anatomy of a Gauge

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

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

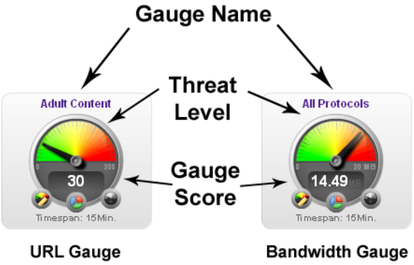


Fig. 5:1-3 URL and bandwidth gauge anatomy

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

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

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

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

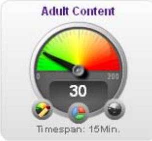
- URL gauge - score includes the total number of end user hits (page count plus blocked object count) for all library categories the gauge monitors.
- Bandwidth gauge - score includes the total number of bytes (kB, MB, GB) of inbound/outbound end user traffic for all protocols/ports the gauge monitors.

How to Read a Gauge

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

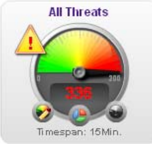
The score will always reflect activity from the most recent past number of specified minutes set up in the Timespan, unless gauge settings were manually changed and saved, at which point the gauge is reset.

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



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

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



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

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

Bandwidth Gauge Components

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

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

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

  - **80** - HTTP TCP port used for transferring and listening
  - **443** - HTTPS TCP/UDP port used for encrypted transmission over TLS/SSL
  - **8080** - HTTP Alternate (http-alt) TCP port used under the following conditions: when running a second Web server on the same machine (the other is using port 80), as a Web proxy and caching server, or when running a Web server as a non-root user. This port is used for Tomcat.
- **FTP** - File Transfer Protocol gauge monitors the protocol used for transferring files from one computer to another on the Internet or an intranet.

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

  - **20** - FTP TCP/UDP data port for file transfer
  - **21** - FTP TCP/UDP control (command) port for file transfer
- **SMTP** - Simple Mail Transfer Protocol gauge monitors the protocol used for transferring email messages from one server to another.

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

  - **25** - SMTP TCP/UDP port used for email routing between mail server email messages
  - **110** - POP3 (Post Office Protocol version 3) TCP port used for sending/retrieving email messages
- **P2P** - Peer-to-Peer gauge monitors the protocol used for communication between computing devices—desktops, servers, and other smart devices—that are linked directly to each other.

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

  - **1214** - TCP/UDP port for Kazaa, Morpheous, Grokster, etc.
  - **4662** - TCP/UDP port for eMule, eDonkey, etc.
  - **4665** - TCP/UDP port for eDonkey 2000
  - **6346** - TCP/UDP port for Gnutella file sharing (FrostWire, LimeWire, BearShare, etc.)
  - **6347** - TCP/UDP port for Gnutella
  - **6699** - UDP port for Napster
  - **6881** - TCP/UDP port for BitTorrent
- **IM** - Instant Messaging gauge monitors the protocol used for direct connections between workstations either locally or across the Internet.

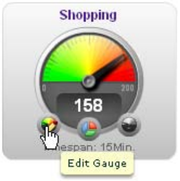
  This protocol gauge is comprised of gauges for monitoring the following ports by default:

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

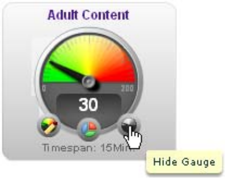
Gauge Usage Shortcuts

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

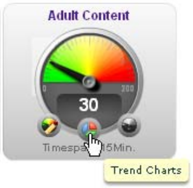
- **View Gauge Ranking** - Clicking a gauge or right-clicking a gauge and selecting this topic from the menu displays the Gauge Ranking panel. The table in this panel contains a list of library categories/protocols/ports that comprise the gauge, along with the list of current users driving the gauge's score. (See View End User Gauge Activity in Chapter 2.)
- **Edit Gauge** - Clicking the left icon at the bottom of a gauge—or right-clicking a gauge and then selecting this menu topic—displays the panel that lets you edit the gauge's components. This is a shortcut to use instead of going to the Add/Edit Gauges panel, selecting the gauge, and then clicking Edit Gauge. (See Modify a Gauge in Chapter 2.)



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



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

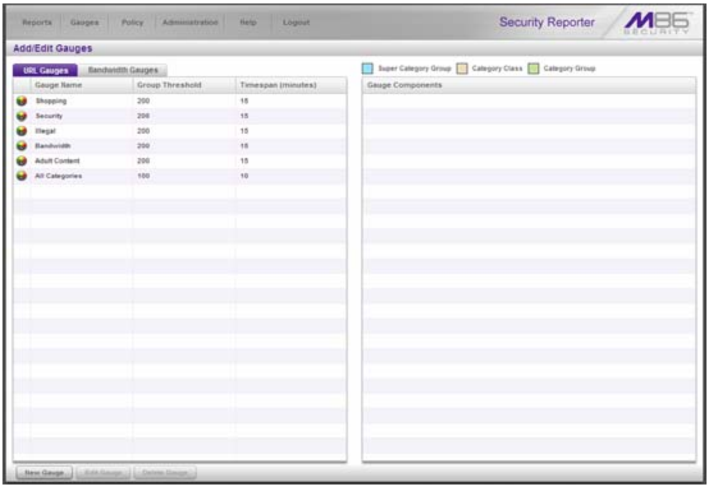


- **Disable Gauge** - Right-clicking a gauge and then selecting this menu topic lets you disable a gauge. This is a shortcut to use instead of going to Dashboard Settings, selecting the gauge from the list, and then clicking the Disable Gauge icon. (See Hide, Disable, Delete, Rearrange Gauges in Chapter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

Chapter 2: Custom Gauge Setup, Usage

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

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



	Gauge Name	Group Threshold	Timespan (minutes)
●	Shopping	200	15
●	Security	200	15
●	Illegal	200	15
●	Bandwidth	200	15
●	Adult Content	200	15
●	All Categories	100	10

Gauge Components

Fig. 5:2-1 Add/Edit Gauges panel

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

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

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

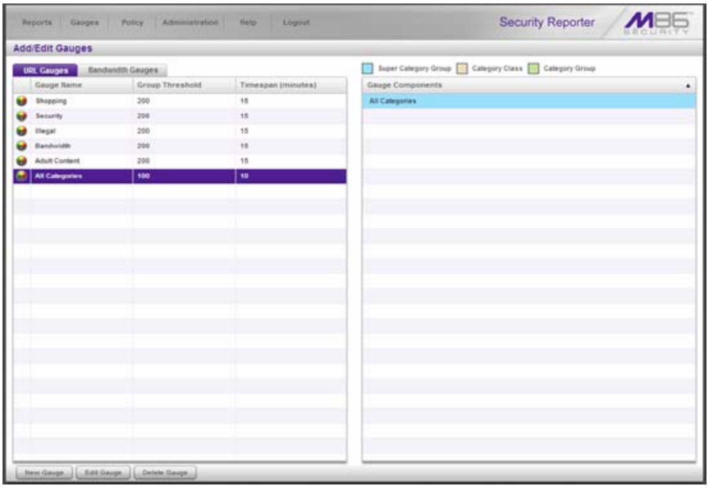
For each Gauge Name in this list, the following information displays: Group Threshold (*200*), Timespan (minutes)—*15* by default.

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

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

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

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



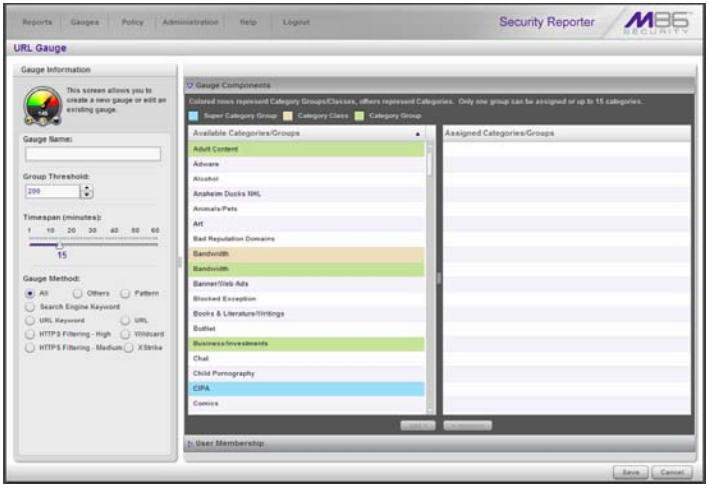
Gauge Name	Group Threshold	Timespan (minutes)
Shopping	200	15
Security	200	15
Illegal	200	15
Bandwidth	200	15
Adult Content	200	15
All Categories	100	10

Gauge Components
All Categories

Fig. 5:2-2 Gauge Components frame populated

Add a Gauge

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



This screen allows you to create a new gauge or edit an existing gauge.

Gauge Name:

Group Threshold: 200

Timespan (minutes): 1 10 20 30 40 50 60 — 15

Gauge Method: ● All ○ Others ○ Pattern ○ Search Engine Keyword ○ URL Keyword ○ URL ○ HTTPS Filtering - High ○ Wildcard ○ HTTPS Filtering - Medium ○ XStrike

Colored rows represent Category Groups/Classes, others represent Categories. Only one group can be assigned or up to 15 categories.

🟦 Super Category Group 🟧 Category Class 🟩 Category Group

Fig. 5:2-3 Add a new gauge

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

When adding a new gauge, do the following:

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

Specify Gauge Information

In the Gauge Information frame:

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

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

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

Define Gauge Components

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

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

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

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

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

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

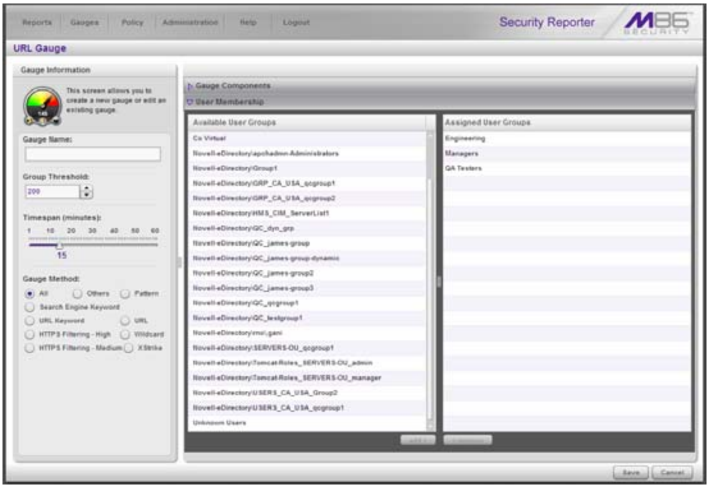
2. Click **add >** (for URL gauges) or **add port >** (for bandwidth gauges) to move the selection(s) to the Assigned Categories/Groups list box.

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

Assign user groups

To assign user groups to be monitored by the gauge:

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



This screen allows you to create a new gauge or edit an existing gauge.

Gauge Name:

Group Threshold: 200

Timespan (minutes): 1 10 20 30 40 50 60 — 15

Gauge Method:
● All ○ Others ○ Pattern
○ Search Engine Keyword
○ URL Keyword ○ URL
○ HTTPS Filtering - High ○ Wildcard
○ HTTPS Filtering - Medium ○ XStrike

Available User Groups	Assigned User Groups
Ca Virtual	Engineering
Novell-eDirectory/apchadmn-Administrators	Managers
Novell-eDirectory/Group1	QA Testers
Novell-eDirectory/GRP_CA_USA_qcgroup1	
Novell-eDirectory/GRP_CA_USA_qcgroup2	
Novell-eDirectory/HMS_CIM_ServerList1	
Novell-eDirectory/QC_dyn_grp	
Novell-eDirectory/QC_james-group	
Novell-eDirectory/QC_james-group-dynamic	
Novell-eDirectory/QC_james-group2	
Novell-eDirectory/QC_james-group3	
Novell-eDirectory/QC_qcgroup1	
Novell-eDirectory/QC_testgroup1	
Novell-eDirectory/mol.gani	
Novell-eDirectory/SERVERS-OU_qcgroup1	
Novell-eDirectory/Tomcat-Roles_SERVERS-OU_admin	
Novell-eDirectory/Tomcat-Roles_SERVERS-OU_manager	
Novell-eDirectory/USERS_CA_USA_Group2	
Novell-eDirectory/USERS_CA_USA_qcgroup1	
Unknown Users	

Fig. 5:2-4 User Membership accordion opened

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

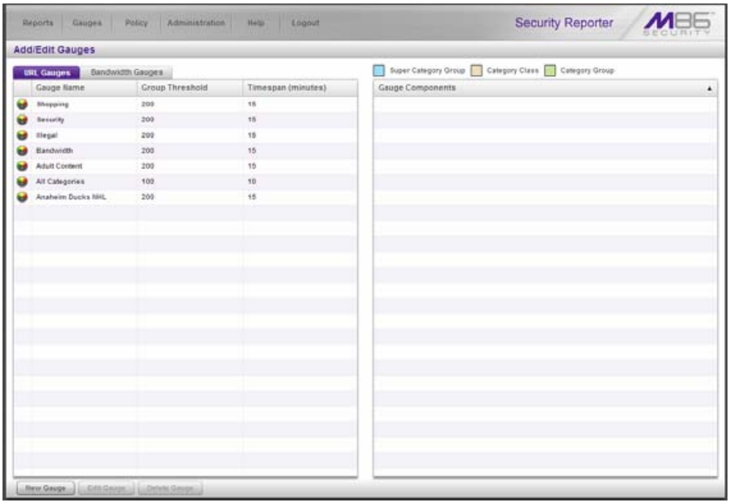
2. From the Available User Groups list, select the user group to highlight it.

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

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

Save gauge settings

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



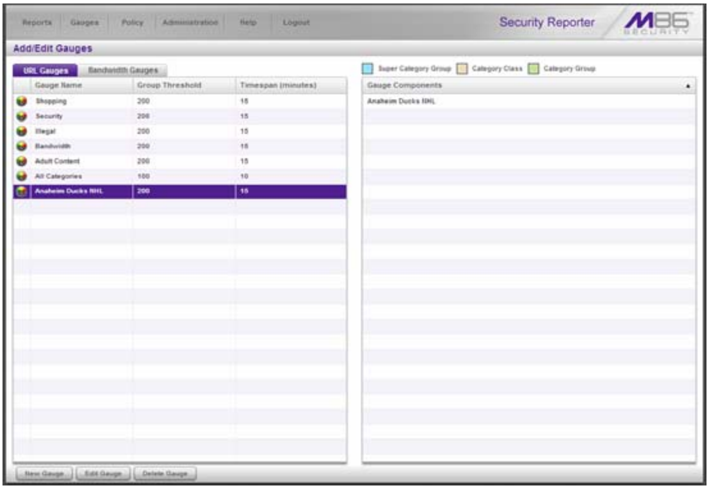
Gauge Name	Group Threshold	Timespan (minutes)
Shopping	200	15
Security	200	15
Illegal	200	15
Bandwidth	200	15
Adult Content	200	15
All Categories	100	10
Anaheim Ducks NHL	200	15

Fig. 5:2-5 New gauge added

Modify a Gauge

Edit gauge settings

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

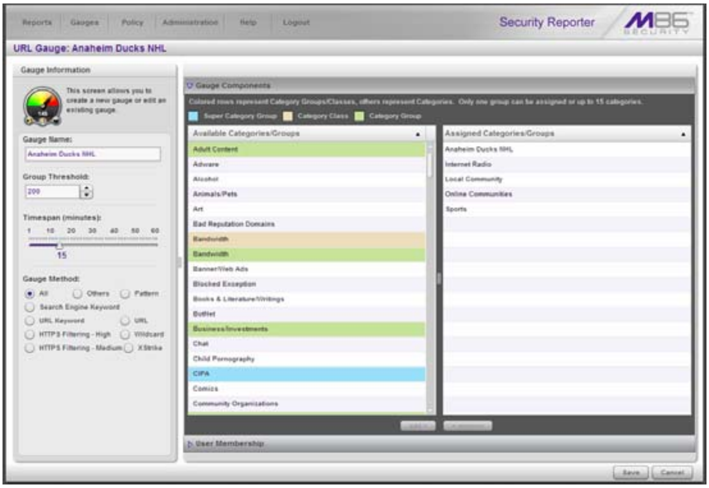


Gauge Name	Group Threshold	Timespan (minutes)
Shopping	200	15
Security	200	15
Illegal	200	15
Bandwidth	200	15
Adult Content	200	15
All Categories	100	10
Anaheim Ducks NHL	200	15

Gauge Components
Anaheim Ducks NHL

Fig. 5:2-6 Select the gauge to be edited

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



URL Gauge: Anaheim Ducks NHL

Gauge Information

This screen allows you to create a new gauge or edit an existing gauge.

Gauge Name: Anaheim Ducks NHL

Group Threshold: 200

Timespan (minutes): 1 10 20 30 40 50 60 — 15

Gauge Method:
● All ○ Others ○ Pattern
○ Search Engine Keyword
○ URL Keyword ○ URL
○ HTTPS Filtering - High ○ Wildcard
○ HTTPS Filtering - Medium ○ XStrike

Gauge Components

Colored rows represent Category Groups/Classes, others represent Categories. Only one group can be assigned or up to 15 categories.

Super Category Group   Category Class   Category Group

Available Categories/Groups	Assigned Categories/Groups
Adult Content	Anaheim Ducks NHL
Adware	Internet Radio
Alcohol	Local Community
Animals/Pets	Online Communities
Art	Sports
Bad Reputation Domains	
Bandwidth	
Bandwidth	
Banner/Web Ads	
Blocked Exception	
Books & Literature/Writings	
BotNet	
Business/Investments	
Chat	
Child Pornography	
CIPA	
Comics	
Community Organizations	

User Membership

Fig. 5:2-7 Edit gauge settings

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

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

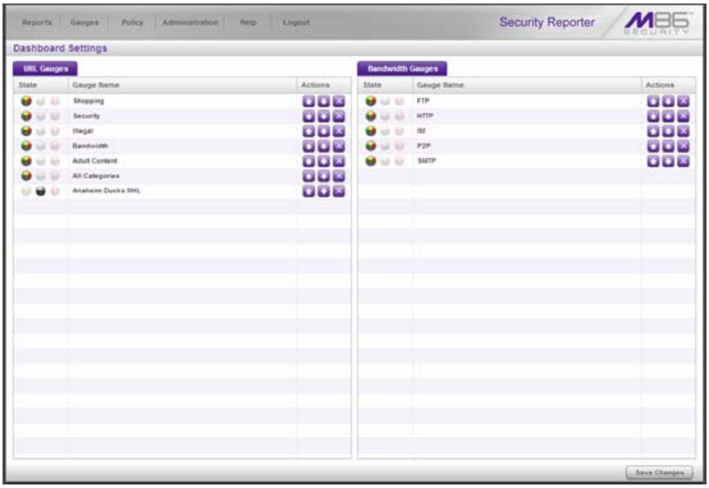
Hide, Disable, Delete, Rearrange Gauges

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

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

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

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



Dashboard Settings

URL Gauges

State	Gauge Name	Actions
● ○ ○	Shopping	▲ ▼ ✕
● ○ ○	Security	▲ ▼ ✕
● ○ ○	Illegal	▲ ▼ ✕
● ○ ○	Bandwidth	▲ ▼ ✕
● ○ ○	Adult Content	▲ ▼ ✕
● ○ ○	All Categories	▲ ▼ ✕
○ ● ○	Anaheim Ducks NHL	▲ ▼ ✕

Bandwidth Gauges

State	Gauge Name	Actions
● ○ ○	FTP	▲ ▼ ✕
● ○ ○	HTTP	▲ ▼ ✕
● ○ ○	IM	▲ ▼ ✕
● ○ ○	P2P	▲ ▼ ✕
● ○ ○	SMTP	▲ ▼ ✕

Fig. 5:2-8 Dashboard Settings panel

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

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

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

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

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

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

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

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

Hide a gauge

To hide a gauge from displaying in the dashboard:

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

Disable a gauge

To disable a gauge:

1. Select the gauge in the URL Gauges or Bandwidth Gauges tab.
2. In the State column, click the icon in the third column (Disable Gauge) to change the gauge’s status to “disabled.”

Show a gauge

To re-display a gauge in the dashboard again:

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

Rearrange the gauge display in the dashboard

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

1. Select the gauge in the URL Gauges or Bandwidth Gauges tab.
2. In the Actions column, perform any of the following actions:

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

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

Delete a gauge

To delete a gauge:

1. Select the gauge in the URL Gauges or Bandwidth Gauges tab.
2. In the Actions column, click the “X” icon in the far right column to open the Confirm dialogue box with the message: “Deleting this gauge will remove all alerts that are associated with this gauge. Are you sure you want to delete this gauge?”

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

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

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

View End User Gauge Activity

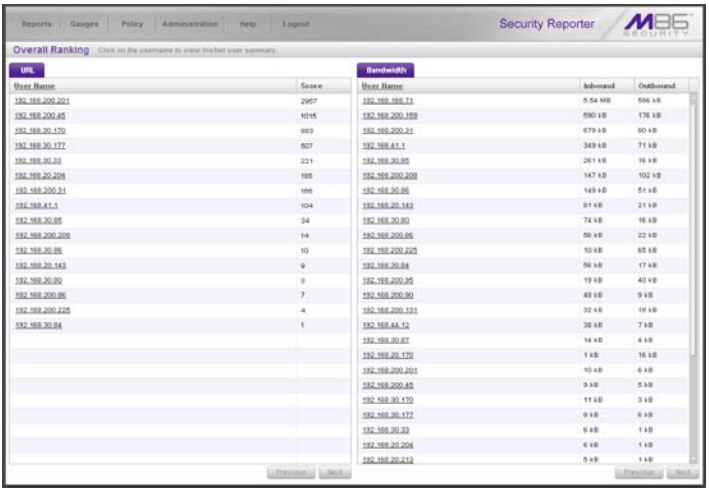
There are two types of gauge activity you will want to view and monitor:

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

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

View Overall Ranking

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



Overall Ranking Click on the username to view his/her user summary.

User Name	Score
192.168.200.201	2967
192.168.200.45	1015
192.168.30.170	883
192.168.30.177	607
192.168.30.33	221
192.168.20.204	185
192.168.200.31	166
192.168.41.1	104
192.168.30.85	34
192.168.200.208	14
192.168.30.86	10
192.168.20.143	9
192.168.30.80	8
192.168.200.86	7
192.168.200.225	4
192.168.30.84	1

User Name	Inbound	Outbound
192.168.168.71	5.54 MB	506 kB
192.168.200.169	590 kB	176 kB
192.168.200.31	679 kB	80 kB
192.168.41.1	349 kB	71 kB
192.168.30.85	261 kB	16 kB
192.168.200.208	147 kB	102 kB
192.168.30.86	149 kB	51 kB
192.168.20.143	81 kB	21 kB
192.168.30.80	74 kB	16 kB
192.168.200.86	56 kB	22 kB
192.168.200.225	10 kB	65 kB
192.168.30.84	66 kB	17 kB
192.168.200.95	19 kB	40 kB
192.168.200.90	48 kB	9 kB
192.168.200.131	32 kB	18 kB
192.168.44.12	38 kB	7 kB
192.168.30.87	14 kB	4 kB
192.168.20.170	1 kB	16 kB
192.168.200.201	10 kB	6 kB
192.168.200.45	9 kB	5 kB
192.168.30.170	11 kB	3 kB
192.168.30.177	9 kB	6 kB
192.168.30.33	6 kB	1 kB
192.168.20.204	6 kB	1 kB
192.168.20.213	5 kB	1 kB

Fig. 5:2-9 Overall Ranking panel

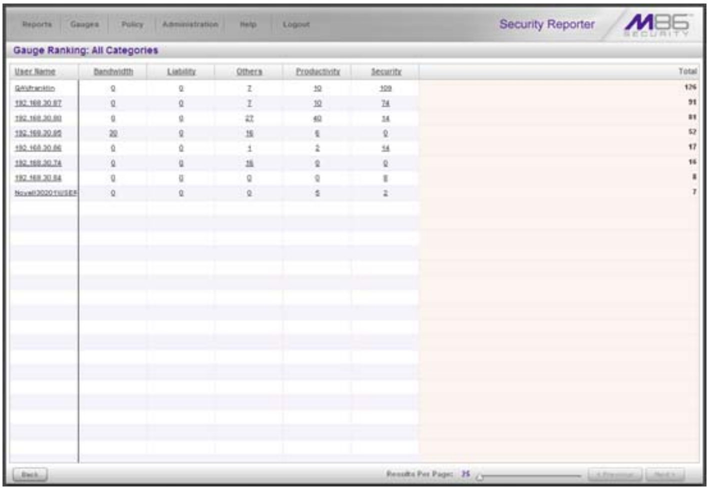
The URL frame displays to the left and the Bandwidth frame displays to the right, containing the User Name (or IP address) and Score for each user currently affecting one or more gauges.

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

2. To drill down and view additional information about an end user’s activity, click the **User Name** in the appropriate tab to access the User Summary panel (see Monitor, Restrict End User Activity).
3. In the User Summary panel, you can view URLs visited by the end user and lock out that user from accessing designated areas of the Internet/network.

View a Gauge Ranking table

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



Gauge Ranking: All Categories

User Name	Bandwidth	Liability	Others	Productivity	Security	Total
QA\tfranklin	0	0	7	10	109	126
192.168.20.87	0	0	7	10	74	91
192.168.20.80	0	0	27	40	14	81
192.168.20.85	30	0	16	6	0	52
192.168.20.86	0	0	1	2	14	17
192.168.20.74	0	0	16	0	0	16
192.168.20.84	0	0	0	0	8	8
Novell\2020\USE	0	0	0	5	2	7

Fig. 5:2-10 Gauge Ranking table

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

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

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

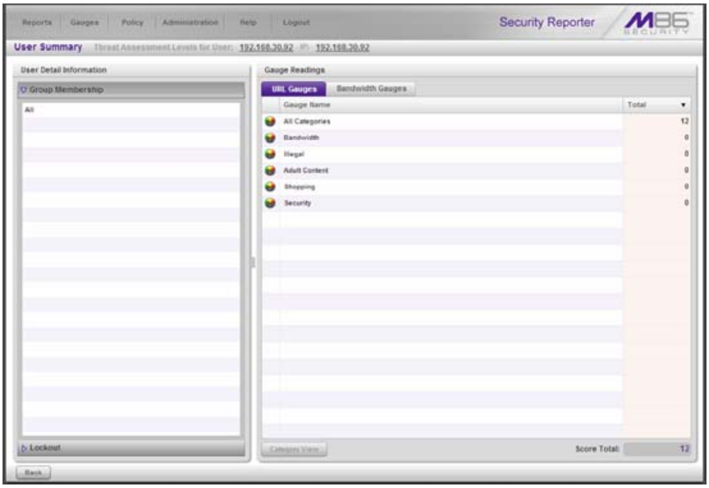
   - Access the User Summary panel by clicking the **User Name** (see Monitor, Restrict End User Activity: View User Summary data). In the User Summary panel, you can view URLs visited by the end user and lock out that user from accessing designated areas of the Internet/network.
   - Access the Category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

Monitor, Restrict End User Activity

View User Summary data

The User Summary panel contains the following frames:

- User Detail Information frame to the left that includes the Group Membership and Lockout accordions. The Group Membership accordion is expanded by default and displays a list of groups in which the end user belongs.
- Gauge Readings frame to the right that includes the URL Gauges and Bandwidth Gauges tabs, each showing the Gauge Name and end user's Total score for each gauge in the dashboard.



User Summary Threat Assessment Levels for User: 192.168.20.92 IP: 192.168.20.92

All

Gauge Name	Total
All Categories	12
Bandwidth	0
Illegal	0
Adult Content	0
Shopping	0
Security	0

Score Total: 12

Fig. 5:2-11 User Summary panel

In this panel you can perform the following actions:

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

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

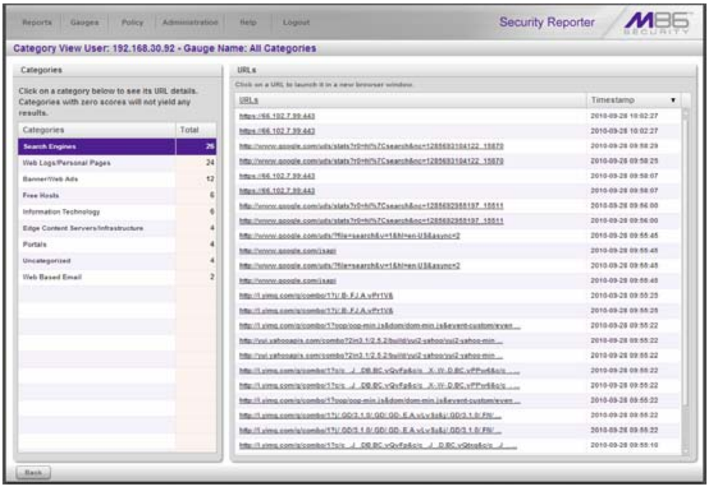
Access the Category View User panel

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

URL Gauges tab selection

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

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



Category View User: 192.168.30.92 - Gauge Name: All Categories

Categories

Click on a category below to see its URL details. Categories with zero scores will not yield any results.

Categories	Total
Search Engines	26
Web Logs/Personal Pages	24
Banner/Web Ads	12
Free Hosts	6
Information Technology	6
Edge Content Servers/Infrastructure	4
Portals	4
Uncategorized	4
Web Based Email	2

URLs

Click on a URL to launch it in a new browser window.

URLs	Timestamp ▼
https://66.102.7.99:443	2010-09-28 10:02:27
https://66.102.7.99:443	2010-09-28 10:02:27
http://www.google.com/uds/stats?r0=hl%7Csearch&nc=1285693104122_15870	2010-09-28 09:58:29
http://www.google.com/uds/stats?r0=hl%7Csearch&nc=1285693104122_15870	2010-09-28 09:58:25
https://66.102.7.99:443	2010-09-28 09:58:07
https://66.102.7.99:443	2010-09-28 09:58:07
http://www.google.com/uds/stats?r0=hl%7Csearch&nc=1285692958197_15511	2010-09-28 09:56:00
http://www.google.com/uds/stats?r0=hl%7Csearch&nc=1285692958197_15511	2010-09-28 09:56:00
http://www.google.com/uds/?file=search&v=1&hl=en-US&async=2	2010-09-28 09:55:45
http://www.google.com/jsapi	2010-09-28 09:55:45
http://www.google.com/uds/?file=search&v=1&hl=en-US&async=2	2010-09-28 09:55:45
http://www.google.com/jsapi	2010-09-28 09:55:45
http://l.yimg.com/q/combo/1?l/_B-_FJ.A.vPr1V&	2010-09-28 09:55:25
http://l.yimg.com/q/combo/1?l/_B-_FJ.A.vPr1V&	2010-09-28 09:55:25
http://l.yimg.com/q/combo/1?oop/oop-min.js&dom/dom-min.js&event-custom/even ...	2010-09-28 09:55:22
http://yui.yahooapis.com/combo?2in3.1/2.5.2/build/yui2-yahoo/yui2-yahoo-min ...	2010-09-28 09:55:22
http://yui.yahooapis.com/combo?2in3.1/2.5.2/build/yui2-yahoo/yui2-yahoo-min ...	2010-09-28 09:55:22
http://l.yimg.com/q/combo/1?c/c_J_DB.BC.vQvfg&c/c_X-W-D.BC.vPPw6&c/c ...	2010-09-28 09:55:22
http://l.yimg.com/q/combo/1?c/c_J_DB.BC.vQvfg&c/c_X-W-D.BC.vPPw6&c/c ...	2010-09-28 09:55:22
http://l.yimg.com/q/combo/1?oop/oop-min.js&dom/dom-min.js&event-custom/even ...	2010-09-28 09:55:22
http://l.yimg.com/q/combo/1?l/_GD/3.1.0/_GD/_GD-_E.A.vLv3s&l/_GD/3.1.0/_FN/ ...	2010-09-28 09:55:22
http://l.yimg.com/q/combo/1?l/_GD/3.1.0/_GD/_GD-_E.A.vLv3s&l/_GD/3.1.0/_FN/ ...	2010-09-28 09:55:22
http://l.yimg.com/q/combo/1?c/c_J_DB.BC.vQvfg&c/c_J_D.BC.vQtog&c/c_J ...	2010-09-28 09:55:10

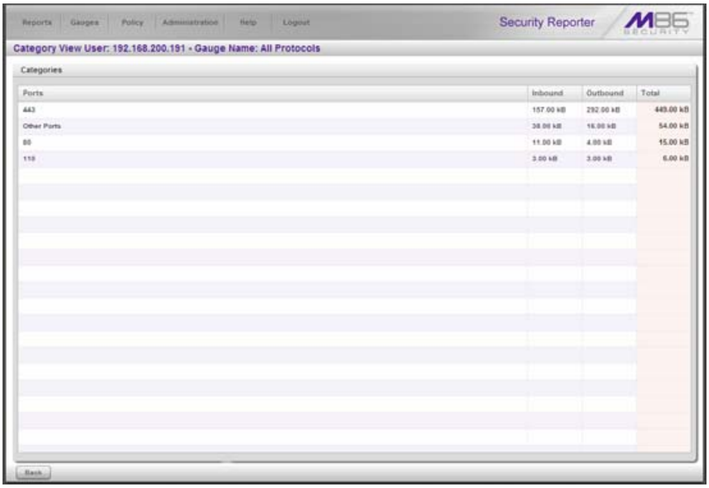
Fig. 5:2-12 Category View User panel for URL Gauges tab selection

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

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

Bandwidth Gauges tab selection

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



Category View User: 192.168.200.191 - Gauge Name: All Protocols

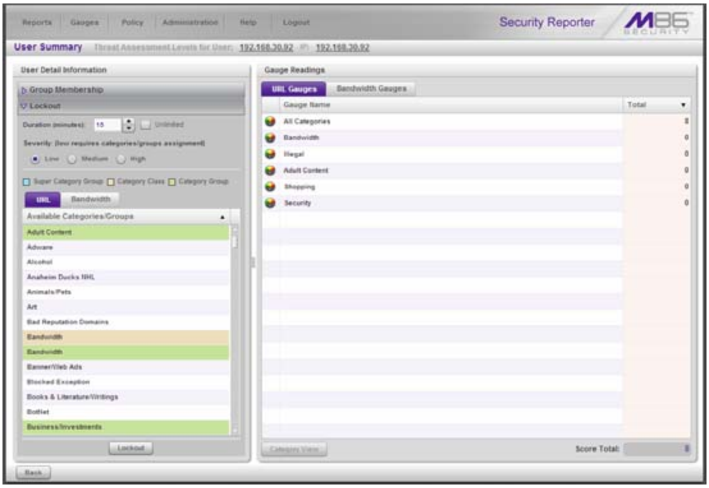
Categories

Ports	Inbound	Outbound	Total
443	157.00 kB	292.00 kB	449.00 kB
Other Ports	38.00 kB	16.00 kB	54.00 kB
80	11.00 kB	4.00 kB	15.00 kB
110	3.00 kB	3.00 kB	6.00 kB

Fig. 5:2-13 Category View User panel for Bandwidth tab selection

Manually lock out an end user

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



Duration (minutes): 15 □ Unlimited

Severity: (low requires categories/groups assignment)

● Low ○ Medium ○ High

□ Super Category Group □ Category Class □ Category Group

Adult Content
Adware
Alcohol
Anaheim Ducks NHL
Animals/Pets
Art
Bad Reputation Domains
Bandwidth
Bandwidth
Banner/Web Ads
Blocked Exception
Books & Literature/Writings
BotNet
Business/Investments

Gauge Name	Total
All Categories	0
Bandwidth	0
Illegal	0
Adult Content	0
Shopping	0
Security	0

Score Total: 0

Fig. 5:2-14 User Summary panel, Lockout accordion expanded

2. Specify the **Duration** (minutes) of the lockout (the default is “15” minutes), or click the “Unlimited” checkbox.

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

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

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

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

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

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

Low severity lockout

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

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

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

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

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

Medium and High severity lockout

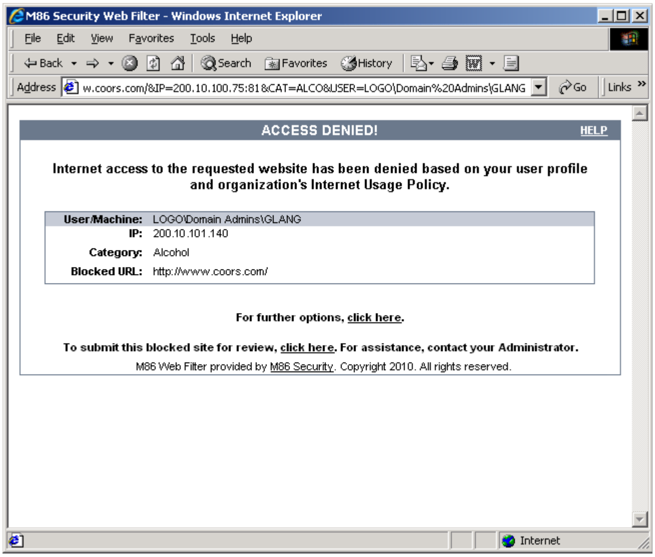
If a “Medium” or “High” Severity lockout was selected, the **Type** field displays. Click either “Medium” or “High” to select that lockout level.

End user workstation lockout

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

Low severity URL, medium URL/bandwidth lockout

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


M86 Security Web Filter - Windows Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address
Go
Links
Internet

w.coors.com/&IP=200.10.100.75:81&CAT=ALCO&USER=LOGO\Domain%20Admins\GLANG

ACCESS DENIED! HELP

Internet access to the requested website has been denied based on your user profile and organization's Internet Usage Policy.

User/Machine:	LOGO\Domain Admins\GLANG
IP:	200.10.101.140
Category:	Alcohol
Blocked URL:	http://www.coors.com/

For further options, click here.

To submit this blocked site for review, click here. For assistance, contact your Administrator.

M86 Web Filter provided by M86 Security. Copyright 2010. All rights reserved.

Fig. 5:2-15 Low, medium level URL, medium bandwidth lockout page

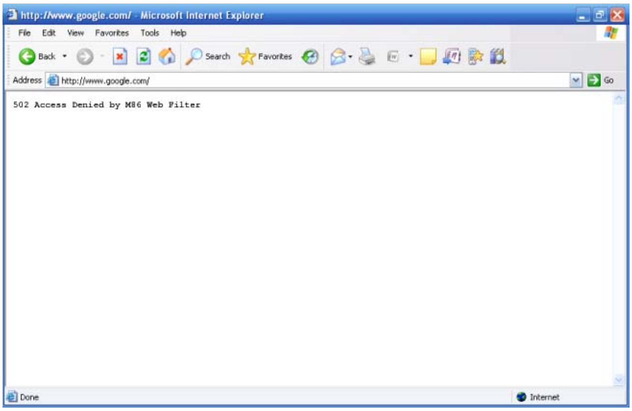
This page contains the following information: header "ACCESS DENIED!", User/Machine name for an LDAP user (blank for an IP group user), user's IP address, library Category in which the URL resides, and the Blocked URL the user attempted to access.

By default, the following standard links are included in the block page: HELP; M86 Security; For further options, click here; To submit this blocked site for review, click here.

NOTE*: Please refer to the WF Global Administrator Section of this user guide for information about fields in the block page and how to use them.*

High severity URL, low/high bandwidth lockout

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



```
502 Access Denied by M86 Web Filter
```

Fig. 5:2-16 High level URL, low and high bandwidth lockout page

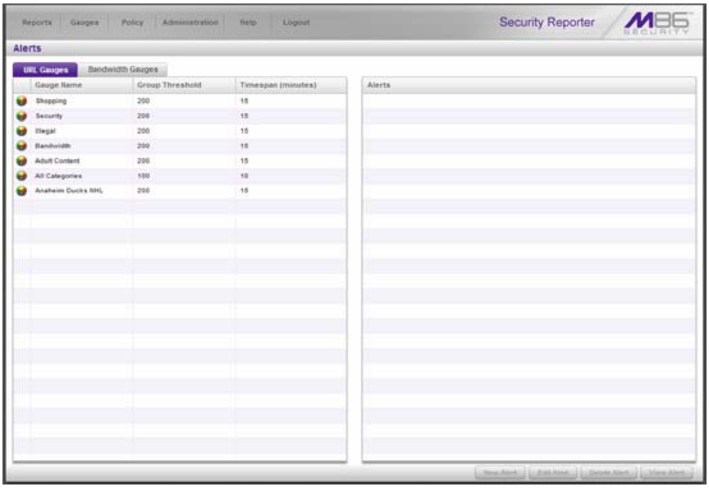
This page contains the following information: "502 Access Denied by M86 Web Filter".

Chapter 3: Alerts, Lockout Management

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

These functions are available to a group administrator only if permissions were granted by the administrator who set up his/her account.

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



Gauge Name	Group Threshold	Timespan (minutes)
Shopping	200	15
Security	200	15
Illegal	200	15
Bandwidth	200	15
Adult Content	200	15
All Categories	100	10
Anaheim Ducks NHL	200	15

Alerts

Fig. 5:3-1 Alerts panel

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

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

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

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

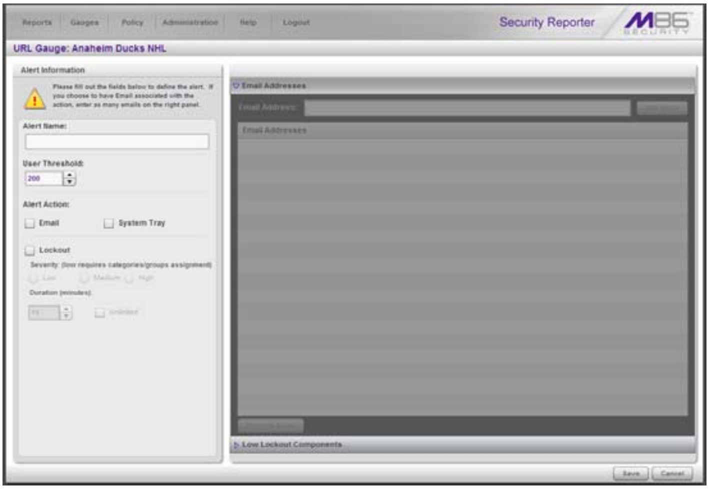
    - Click **Bandwidth Gauges** to view the contents of this tab. By default, this tab includes the following list of Gauge Names: FTP, HTTP, IM, P2P, SMTP.

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

Add an Alert

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

2. Click **New Alert** to open the panel for that gauge:



URL Gauge: Anaheim Ducks NHL

Alert Information

Please fill out the fields below to define the alert. If you choose to have Email associated with the action, enter as many emails on the right panel.

Alert Name:

User Threshold: 200

Alert Action:

□ Email □ System Tray

□ Lockout

Severity: (low requires categories/groups assignment)

○ Low ○ Medium ○ High

Duration (minutes):

15 □ Unlimited

Fig. 5:3-2 Add a new Alert

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

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

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

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

5. In the Alert Action section, specify the mode(s) to use when an alert is triggered:
   - **Email** - An email alert notifies a group administrator via email if an end user has reached the threshold limit set up in a gauge alert.
   - **System Tray** - An SR Alert message notifies a group administrator via his/her workstation’s System Tray if an end user has reached the threshold limit set up in a gauge alert.
   - **Lockout** - The Lockout function locks out an end user from Internet/network access if he/she reaches the threshold limit set up in a gauge alert.

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

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

Email alert function

Configure email alerts

To set up the email alert function:

1. In the Alert Action section of the Alert Information frame, click the checkbox corresponding to **Email** to open the Email Addresses accordion in the target frame to the right.
2. Type in the **Email Address**.
3. Click **Add Email** to include the address in the Email Addresses list box.

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

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

Receive email alerts

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

- Subject: Alert triggered by user (user name/IP address).
- Body of message: User (user name/IP address) has triggered the (Alert Name) alert with a threshold of ‘X’ (in which “X” represents the alert threshold) on the (gauge name) gauge.

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

System Tray alert function

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

***NOTE**: In order to use this feature, the LDAP User Name and Domain set up in the administrator’s profile account must be the same ones he/she uses when logging into his/her workstation.*

Lockout function

To set up the lockout function:

1. Click the checkbox corresponding to **Lockout** to activate the Severity and Duration (minutes) fields.
2. Specify the **Severity** of the end users' lockout:
    - **Low** - Choosing this option opens the Low Lockout Components accordion containing the Available Categories/Groups and Assigned Categories/Groups frames.

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

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

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

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

- **Medium** - Choosing this option will lock out an end user from World Wide Web access if he/she reaches the threshold limit set up for the gauge.
- **High** - Choosing this option will lock out an end user from network access via a TCP connection if he/she reaches the threshold limit set up for the gauge.

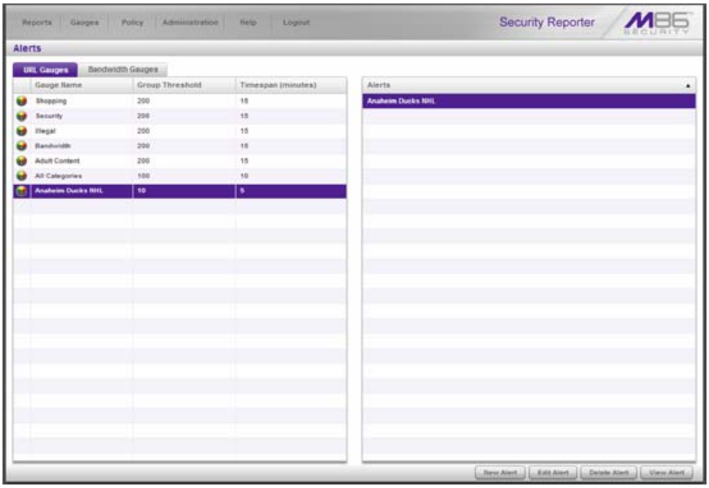
3. Specify the **Duration** (minutes) of the lockout (the default is “15” minutes), or click the “Unlimited” checkbox.

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

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

View, Modify, Delete an Alert

1. In the Alerts panel, select the URL Gauges or Bandwidth Gauges tab.
2. Select the gauge for which an alert will be viewed and/or modified. This action populates the Alerts frame list box with any existing alerts created for that gauge.
3. Select the alert to be viewed or modified by clicking on it to highlight it; this action activates all buttons below the Alerts frame (Add Alert, Edit Alert, Delete Alert, View Alert):



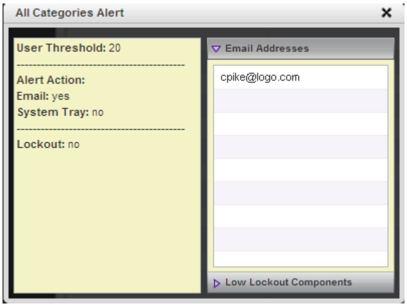
Gauge Name	Group Threshold	Timespan (minutes)
Shopping	200	15
Security	200	15
Illegal	200	15
Bandwidth	200	15
Adult Content	200	15
All Categories	100	10
Anaheim Ducks NHL	10	5

Alerts
Anaheim Ducks NHL

Fig. 5:3-3 Alert added

View alert settings

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



User Threshold: 20

Alert Action:
Email: yes
System Tray: no

Lockout: no

cpike@logo.com

Fig. 5:3-4 View an alert

The following information displays to the left of this window:

- User Threshold amount
- Alert Action criteria (yes/no): Email, System Tray
- Lockout (yes/no)

If a Lockout was set up for the alert, the following information displays below “Lockout”:

- Severity (Low, Medium, High)
- Duration (minutes)

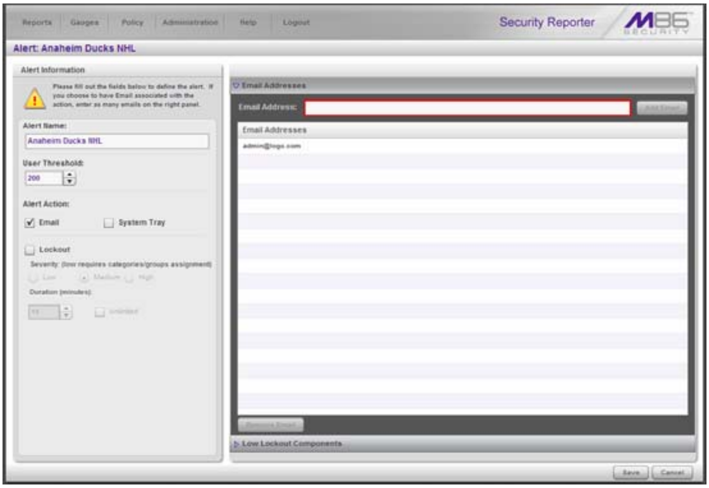
To the right of this window, the Email Addresses and Low Lockout Components accordions display. Click an accordion to expand it, and view the contents—if any—within that accordion.

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

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

Modify an alert

1. In the Alerts panel, click the URL Gauges or Bandwidth Gauges tab.
2. Select the gauge from the list to populate the Alerts frame with alerts for that gauge, and to activate all buttons beneath the frame.
3. Click **Edit Alert** to open the edit Alert panel:



Alert: Anaheim Ducks NHL

Alert Information

Please fill out the fields below to define the alert. If you choose to have Email associated with the action, enter as many emails on the right panel.

Alert Name: Anaheim Ducks NHL

User Threshold: 200

Alert Action:

☑ Email □ System Tray

□ Lockout

Severity: (low requires categories/groups assignment)

○ Low ● Medium ○ High

Duration (minutes): 15 □ Unlimited

Email Address:

Email Addresses

admin@logo.com

Fig. 5:3-5 Edit an alert

4. The following items can be edited:
   - Alert Name
   - User Threshold
   - Alert Action selections: Email, System Tray—the latter is only functional for Active Directory LDAP—and Lockout
   - Lockout Severity selection (Low, Medium, High)
   - Duration (minutes) selection
   - Email Addresses
   - Low Lockout Components

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

Delete an alert

1. In the Alerts panel, click the URL Gauges or Bandwidth Gauges tab.
2. Select the gauge from the list to populate the Alerts frame with alerts for that gauge, and to activate all buttons beneath the frame.
3. Click **Delete Alert** to open the Confirm dialog box with the message: “Are you sure you want to delete this alert?”

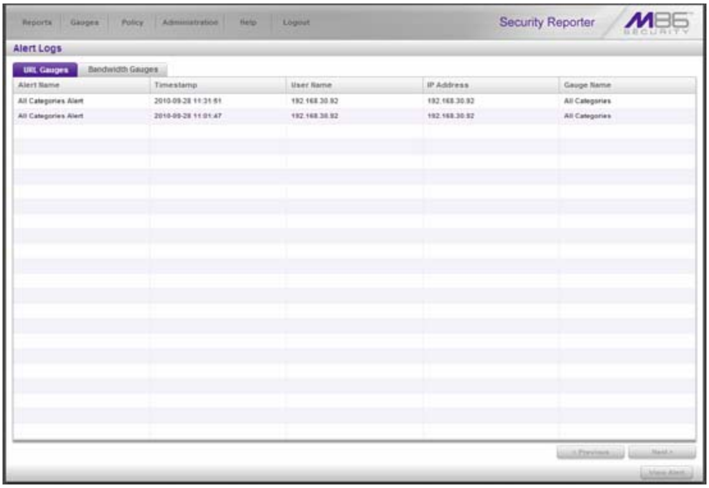
NOTE*: Clicking No closes the dialog box without removing the alert, and returns you to the main Alerts panel.*

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

View the Alert Log

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

1. In the navigation toolbar, mouse over the Policy menu link and select **Alert Logs** to open the Alert Logs panel.
2. Select the URL Gauges or Bandwidth Gauges tab to display its contents:



Alert Name	Timestamp	User Name	IP Address	Gauge Name
All Categories Alert	2010-09-28 11:31:51	192.168.30.92	192.168.30.92	All Categories
All Categories Alert	2010-09-28 11:01:47	192.168.30.92	192.168.30.92	All Categories

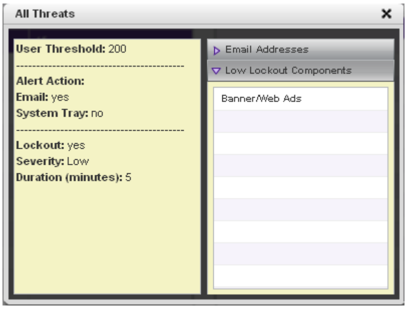
Fig. 5:3-6 Alert Logs panel

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

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

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

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



User Threshold: 200

Alert Action:
Email: yes
System Tray: no

Lockout: yes
Severity: Low
Duration (minutes): 5

Fig. 5:3-7 View an alert

The following information displays to the left of this window:

- User Threshold amount
- Alert Action criteria (yes/no): Email, System Tray
- Lockout (yes/no)

If a Lockout was set up for the alert, the following information displays below “Lockout”:

- Severity (Low, Medium, High)
- Duration (minutes)

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

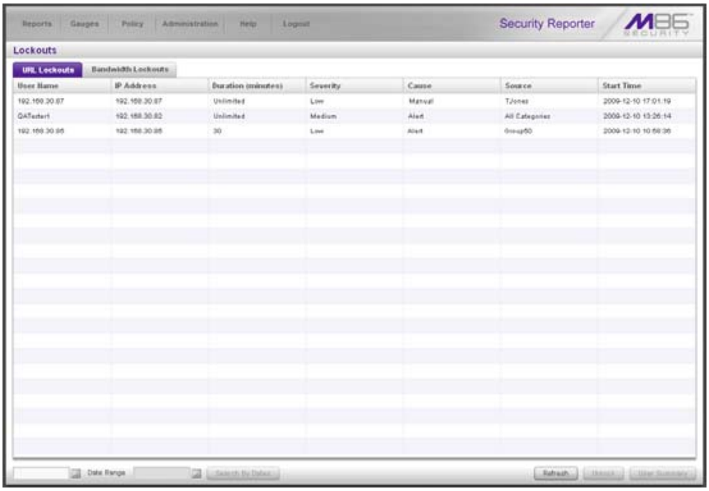
5. Click the “X” in the upper right corner of alert viewer pop-up window to close it.

Manage the Lockout List

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

To view the current lockout list:

1. In the navigation toolbar, mouse over the Gauges menu link and select **Lockouts** to open the Lockouts panel.
2. Select the URL Gauges or Bandwidth Gauges tab to display its contents:



User Name	IP Address	Duration (minutes)	Severity	Cause	Source	Start Time
192.168.30.87	192.168.30.87	Unlimited	Low	Manual	TJones	2009-12-10 17:01:19
QATester1	192.168.30.82	Unlimited	Medium	Alert	All Categories	2009-12-10 13:26:14
192.168.30.95	192.168.30.95	30	Low	Alert	Group50	2009-12-10 10:58:36

Fig. 5:3-8 View Lockouts

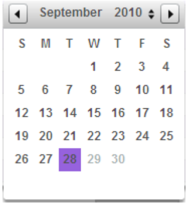
The lockout list contains records for all end users currently locked out of the Internet/network. Each end user’s record displays in a separate row. For each row in the list, the following information displays: User Name (or IP address); IP address; Duration (minutes); Severity of the lockout (Low, Medium,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

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

View a specified time period of lockouts

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

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



S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

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

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

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

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

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

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

Unlock workstations

1. In the populated Lockouts panel, click each record to highlight it.
2. Click **Unlock** to unlock the end user(s) and to remove the record(s) from the list.

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

Access User Summary details

1. To access details about an end user’s online activity, first click the user’s record to highlight it.
2. Next, click **User Summary** to display the User Summary panel where you can monitor that end user’s online activity and lock him/her out of designated areas of the Internet/network. (See Monitor, Restrict End User Activity for details about using the User Summary panel.)

Chapter 4: Analyze Usage Trends

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

If more information is required in your analysis, the Web Filter application, Report Manager tools, and System Configuration administrator console should be consulted so you can generate customized reports to run for a time period of your specifications.

View Trend Charts

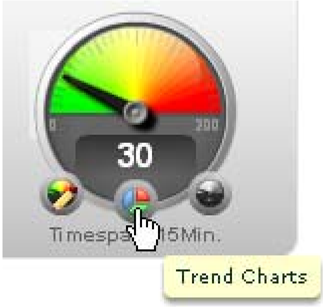
There are three basic types of trend charts that can be generated on demand to show total gauge score averages for a specified, limited time period:

- Pie trend chart for an individual URL or bandwidth gauge
- Pie trend chart for all collective URL or bandwidth gauges
- Line chart showing details for a pie chart

View activity for an individual gauge

To view activity for any individual URL or bandwidth gauge:

1. If the gauges dashboard does not currently display, choose **Dashboard** from the Gauges menu in the navigation toolbar.
2. Be sure the dashboard of your choice (URL or Bandwidth gauges) displays. If not, click the URL or Bandwidth button above the dashboard to display the dashboard of your choice.
3. Find the gauge for which the trend chart will be generated, and then click the Trend Charts icon at the bottom middle of that gauge:



This action of clicking the Trend Charts icon displays the Gauge Trend Chart panel:

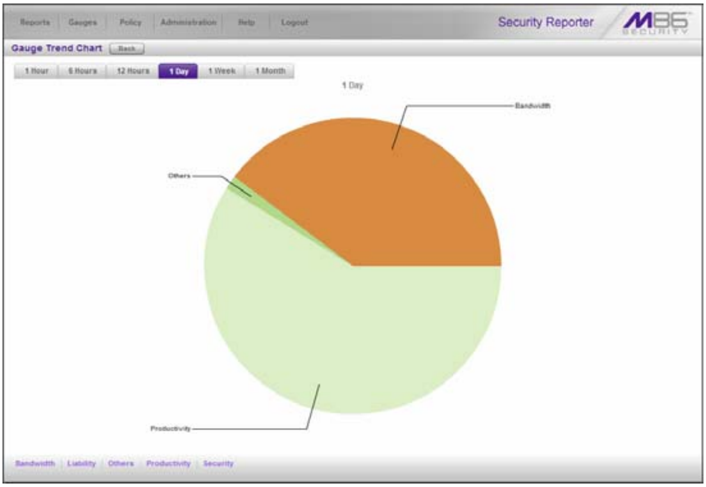


Fig. 5:4-1 Pie trend chart for an individual URL gauge

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

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

The top and bottom sections of this panel contain tabs.

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

View overall URL or bandwidth gauge activity

1. In the navigation toolbar, mouse over the Reports menu link and select either the **URL Trend Charts** to display the URL Trend Charts panel, or select **Bandwidth Trend Charts** to display the BandWidth Trend Charts panel:

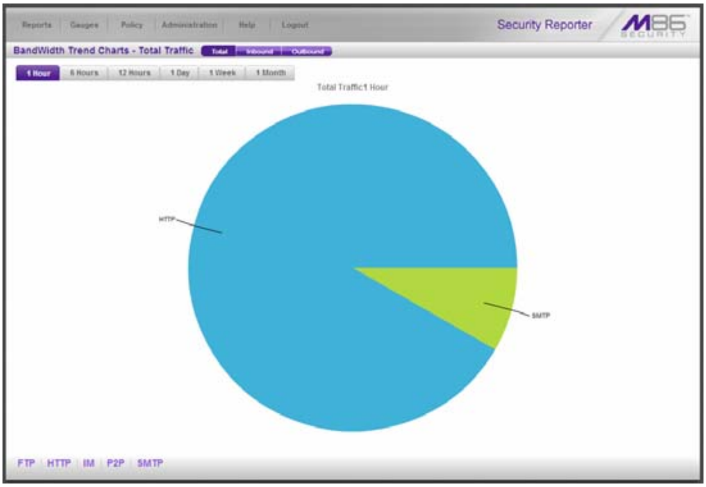


Fig. 5:4-2 Overall Bandwidth Trend Chart, Total Traffic

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

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

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

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

Navigate a trend chart

The following actions can be performed in this panel:

- View gauge activity for a different time period (1 Hour, 6 Hours, 12 Hours, 1 Day, 1 Week, 1 Month)
- Analyze gauge activity in a pie chart
- Analyze gauge activity in a line chart
- View Inbound, Outbound bandwidth gauge activity
- Print a trend chart from an IE browser window

View gauge activity for a different time period

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

- **1 Hour** - This selection displays the gauge URL/byte average score in 10 minute increments for the past 60-minute time period
- **6 Hours** - This selection displays the gauge URL/byte average score in 30 minute increments for the past six-hour time period
- **12 Hours** - This selection displays the gauge URL/byte average score in one hour increments for the past 12-hour time period
- **1 Day** - This selection displays the gauge URL/byte average score in one hour increments for the past 24-hour time period
- **1 Week** - This selection displays the gauge URL/byte average score in 12 hour increments for the past seven-day time period

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

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

Analyze gauge activity in a pie chart

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

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

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

Analyze gauge activity in a line chart

1. To view a line chart showing activity for a slice of the pie chart, do either of the following:
   - Click that slice of the pie chart
   - Click the specified tab beneath the pie chart

   Either action displays the line Trend Chart:

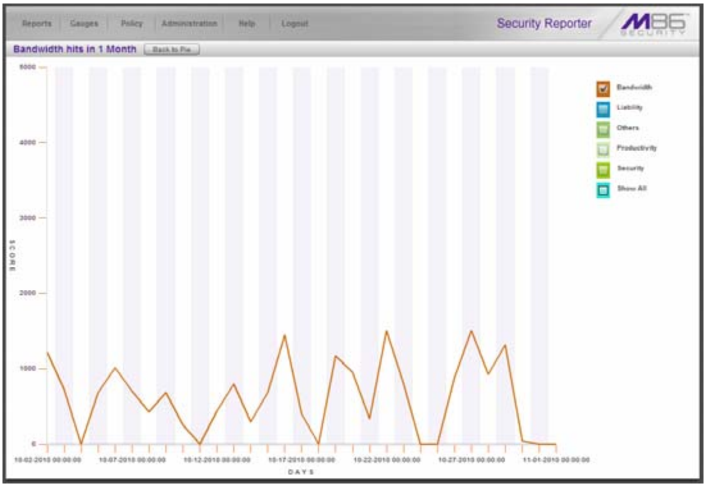


Fig. 5:4-3 Drill into a pie slice to display a line Trend Chart

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

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

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

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

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

   - To view information about a specific point in the line chart, mouse over that point in the chart:

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

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

- To return to the pie chart, click **Back to Pie** in the upper right portion of the panel.
- To print this trend chart, if using an IE browser, see Print a trend chart from an IE browser window.

View In/Outbound bandwidth gauge activity

By default, the total inbound and outbound bandwidth activity is included in the overall Bandwidth Trend Chart. To view only Inbound or Outbound activity, click the **Inbound** or **Outbound** button above the pie chart, to the right of the Total button.

Print a trend chart from an IE browser window

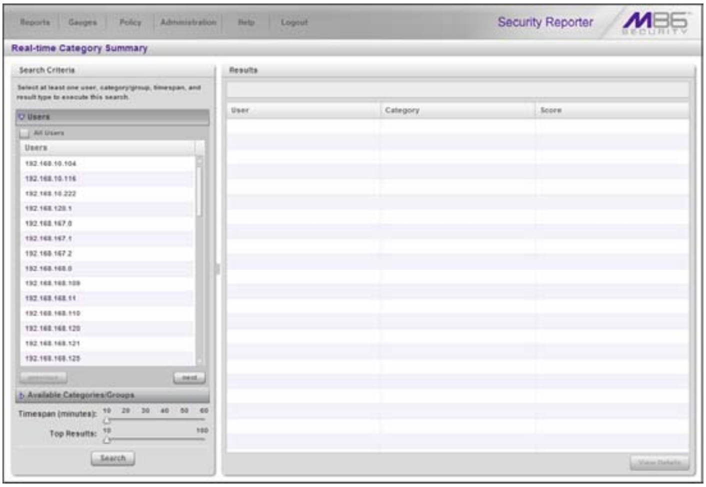
A trend chart can be printed from an IE browser window by using the browser window's toolbar and going to **File > Print** and proceeding with the print commands.

Chapter 5: Identify Users, Categories

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

Perform a Custom Search

In the navigation toolbar, mouse over the Reports menu link and select **Real-time Category Summary** to display the Real-time Category Summary panel:



Select at least one user, category/group, timespan, and result type to execute this search.

192.168.10.104
192.168.10.116
192.168.10.222
192.168.120.1
192.168.167.0
192.168.167.1
192.168.167.2
192.168.168.0
192.168.168.109
192.168.168.11
192.168.168.110
192.168.168.120
192.168.168.121
192.168.168.125

Fig. 5:5-1 Real-time Category Summary, Users accordion opened

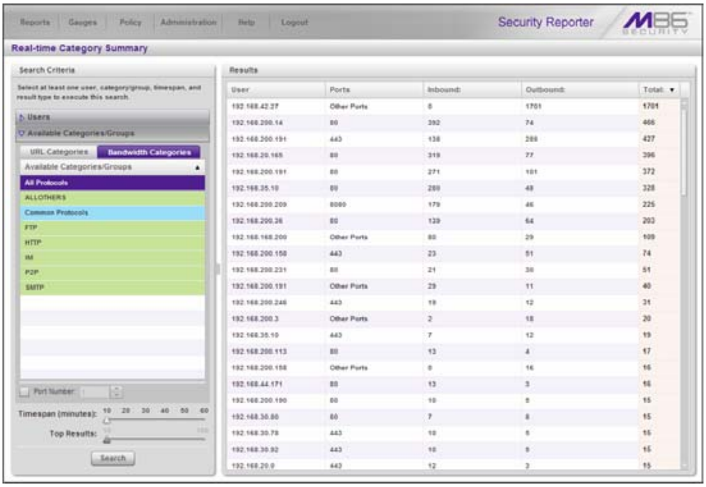
This panel displays the Search Criteria frame to the left with the open Users accordion and closed Available Categories/ Groups accordion, Timespan and Top Results sliders, Search button; and to the right, the empty Results target frame.

Specify Search Criteria

1. In the **Users** accordion, do one of the following:
   - To identify users with the highest scores - Click the **All Users** checkbox to select all users in the list and to grey-out the list.
   - To identify the activities of a specific user - Select the user name/IP address from the list to highlight it.
2. Click the Available Categories/Groups accordion to open it.
3. Select either the **URL Categories** or **Bandwidth Categories** tab to display its list of library categories/protocols, and do either of the following:
   - To identify library categories or protocols with the highest scores - Select a category group or protocol that includes as many of categories/ports as possible.
   - To identify activities for a specific class/group - Select that class or group.

     For bandwidth gauges, to query activities for a specific port number, click the **Port Number** checkbox to activate the port field and to deactivate the listed bandwidth protocol selections. Type a specific value in the pre-populated field, and/or use the up/down arrow buttons to increment/decrement the current value by one.
4. Use the **Timespan (Minutes)** slider to specify the time period in which the threat(s)/group(s) were accessed: last 10, 20, 30, 40, 50, 60 minutes.
5. If a user selection other than “All Users” was specified in the Users accordion, the **Top Results** slide becomes activated and you can make a selection for the maximum number of records to return in the results for that user: top 10, 20, 30, 40, 50, 60, 70, 80, 90, 100 records.

6. Click **Search** to display records returned by the query in the Results frame at the right side of the panel:



Select at least one user, category/group, timespan, and result type to execute this search.

User	Ports	Inbound:	Outbound:	Total: ▼
192.168.42.27	Other Ports	0	1701	1701
192.168.200.14	80	392	74	466
192.168.200.191	443	138	289	427
192.168.20.165	80	319	77	396
192.168.200.191	80	271	101	372
192.168.35.10	80	280	48	328
192.168.200.209	8080	179	46	225
192.168.200.26	80	139	64	203
192.168.168.200	Other Ports	80	29	109
192.168.200.158	443	23	51	74
192.168.200.231	80	21	30	51
192.168.200.191	Other Ports	29	11	40
192.168.200.246	443	19	12	31
192.168.200.3	Other Ports	2	18	20
192.168.35.10	443	7	12	19
192.168.200.113	80	13	4	17
192.168.200.158	Other Ports	0	16	16
192.168.44.171	80	13	3	16
192.168.200.190	80	10	5	15
192.168.30.80	80	7	8	15
192.168.30.78	443	10	5	15
192.168.30.92	443	10	5	15
192.168.20.0	443	12	3	15

Fig. 5:5-2 Search results for Bandwidth Categories

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

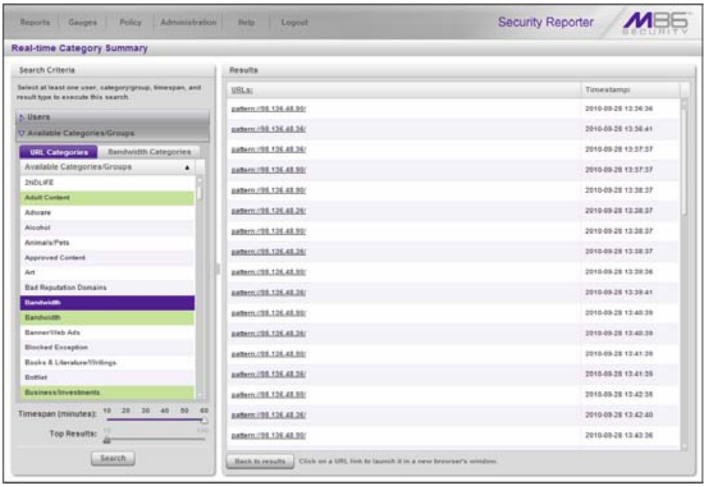
- For a URL search - User (user name/IP address), Category name, and the end user’s total Score for that record.
- For a bandwidth search - User (user name/IP address), Ports number, Inbound score, Outbound score, and the end user’s Total score for that record.

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

View URLs within the accessed category

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

1. Click the User name/IP address to highlight that user's record and to activate the View Details button.
2. Click **View Details** to display a list of URLs and corresponding Timestamp (using the YYYY-MM-DD HH:MM:SS format) for each URL in the library category accessed by the end user within the specified time period:



URLs:	Timestamp:
pattern://98.126.48.90/	2010-09-28 13:36:36
pattern://98.126.48.36/	2010-09-28 13:36:41
pattern://98.126.48.36/	2010-09-28 13:37:37
pattern://98.126.48.90/	2010-09-28 13:37:37
pattern://98.126.48.90/	2010-09-28 13:38:37
pattern://98.126.48.26/	2010-09-28 13:38:37
pattern://98.126.48.90/	2010-09-28 13:38:37
pattern://98.126.48.26/	2010-09-28 13:38:37
pattern://98.126.48.90/	2010-09-28 13:39:36
pattern://98.126.48.26/	2010-09-28 13:39:41
pattern://98.126.48.90/	2010-09-28 13:40:39
pattern://98.126.48.26/	2010-09-28 13:40:39
pattern://98.126.48.90/	2010-09-28 13:41:39
pattern://98.126.48.26/	2010-09-28 13:41:39
pattern://98.126.48.90/	2010-09-28 13:42:35
pattern://98.126.48.26/	2010-09-28 13:42:40
pattern://98.126.48.90/	2010-09-28 13:43:36

Click on a URL link to launch it in a new browser's window.

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

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

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

SR SECURITY REPORTS SECTION

Introduction

This section of the user guide provides instructions to administrators on how to utilize data from SWG logs for monitoring end user Internet and network usage via security reports.

- Chapter 1: Security Reports - This chapter explains how to use the four basic security reports: Blocked Viruses, Security Policy Violations, Traffic Analysis, and Rule Transactions.
- Chapter 2: Security Report Wizard - This chapter explains how to use the Report Wizard to create your own customized security reports.

NOTES*: If the SR is connected to an SWG running software version 9.2.X, reports may not be accurate since bypass transactions (e.g. streaming) are not logged for the SR to process.*

See the M86 Secure Web Gateway User Guide at ***http://www.m86security.com/support/Secure-Web-Gateway/Documentation.asp*** *for information on the SWG.*

Chapter 1: Security Reports

Security Reports are accessible by navigating to **Reports > Security Reports** and selecting the report type from the menu: Blocked Viruses, Security Policy Violations, Traffic Analysis, and Rule Transactions.

Security Report types

The four basic Security Report types include the following information:

- **Blocked Viruses** - This report displays details for each instance of each blocked virus detected from end user Internet/network activity.
- **Security Policy Violations** - This report provides information on each instance in which an end user breached a security policy.
- **Traffic Analysis** - This report shows activity for end user access of objects utilizing an excessive amount of network bandwidth.
- **Rule Transactions** - This report lists each instance in which an end user triggered a threshold in an SWG Security Policy.

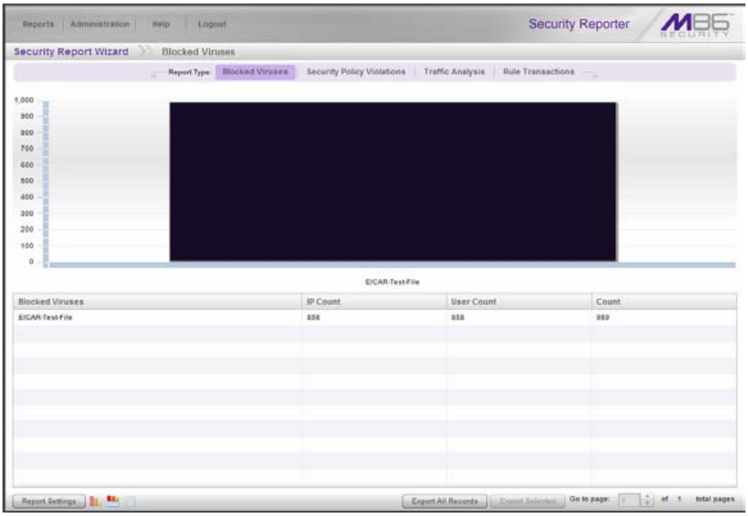
For each report type, by default the top portion of the report view includes tabs for all security Report Types. Beneath these tabs, a bar chart depicts the first six records for the current report type.

***NOTE**: Mousing over a bar in the chart displays the name of the record along with the total hit count or bandwidth used in that record. The Rule Transactions report also includes Actions and Policies information.*

By default, the bottom porton of the report view contains a table that includes rows of records. Columns of pertinent statistics display for each record.

Blocked Viruses report view

The Blocked Viruses report view is accessible via **Reports > Security Reports > Blocked Viruses**:



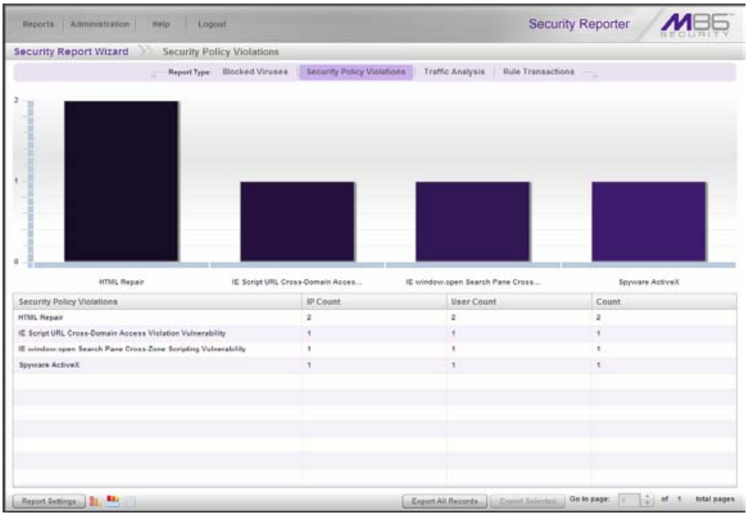
Blocked Viruses	IP Count	User Count	Count
EICAR-Test-File	808	808	989

Fig. 6:1-1 Blocked Viruses report view

The following statistics display for each Blocked Virus record in the table: IP Count and User Count of end users who encountered the blocked virus, and the total Count for all instances of this blocked virus encounter.

Security Policy Violations report view

The Security Policy Violations report view is accessible via **Reports > Security Reports > Security Policy Violations**:



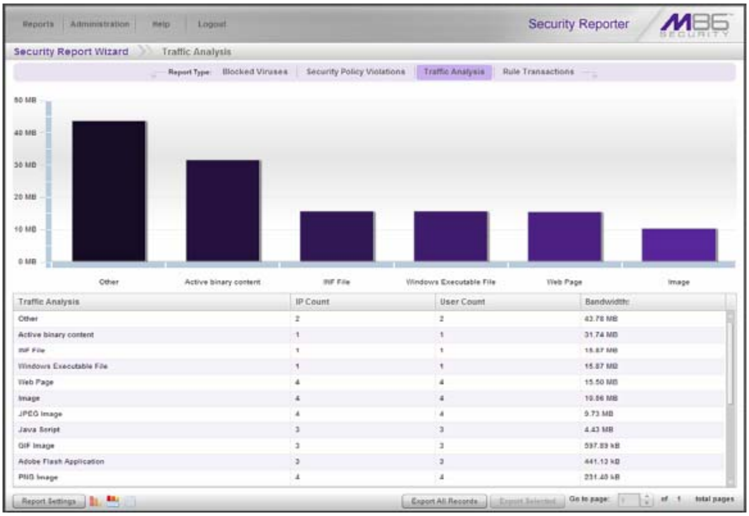
Security Policy Violations	IP Count	User Count	Count
HTML Repair	2	2	2
IE Script URL Cross-Domain Access Violation Vulnerability	1	1	1
IE window.open Search Pane Cross-Zone Scripting Vulnerability	1	1	1
Spyware ActiveX	1	1	1

Fig. 6:1-2 Security Policy Violations report view

The following statistics display for each Security Policy Violation record in the table: IP Count and User Count of end users who breached that security policy, and the total Count for all instances of this type of security breach.

Traffic Analysis report view

The Blocked Viruses report view is accessible via **Reports > Security Reports > Traffic Analysis**:



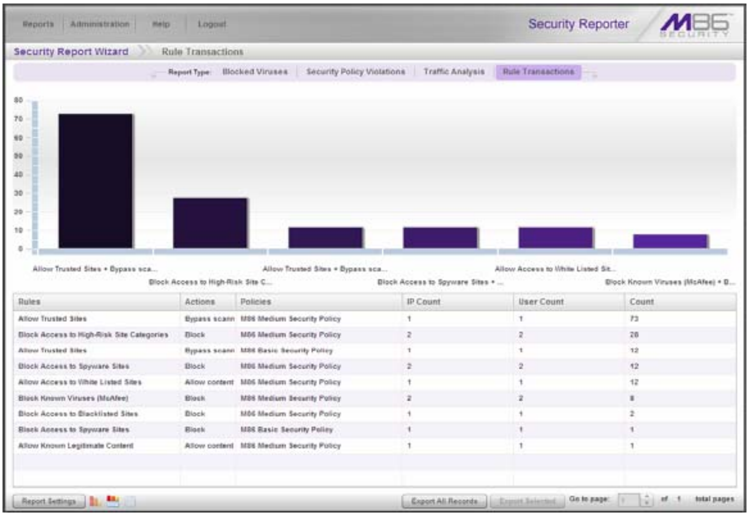
Traffic Analysis	IP Count	User Count	Bandwidth:
Other	2	2	43.78 MB
Active binary content	1	1	31.74 MB
INF File	1	1	15.87 MB
Windows Executable File	1	1	15.87 MB
Web Page	4	4	15.50 MB
Image	4	4	10.56 MB
JPEG Image	4	4	9.73 MB
Java Script	3	3	4.43 MB
GIF Image	3	3	597.89 kB
Adobe Flash Application	3	3	441.13 kB
PNG Image	4	4	231.40 kB

Fig. 6:1-3 Traffic Analysis report view

The following statistics display for each Traffic Analysis record in the table: IP Count and User Count of end users who accessed the high bandwidth usage object, and the total Bandwidth used in all occurrences of accessing this object.

Rule Transactions report view

The Blocked Viruses report view is accessible via **Reports > Security Reports > Rule Transactions**:



Rules	Actions	Policies	IP Count	User Count	Count
Allow Trusted Sites	Bypass scann	M86 Medium Security Policy	1	1	73
Block Access to High-Risk Site Categories	Block	M86 Medium Security Policy	2	2	28
Allow Trusted Sites	Bypass scann	M86 Basic Security Policy	1	1	12
Block Access to Spyware Sites	Block	M86 Medium Security Policy	2	2	12
Allow Access to White Listed Sites	Allow content	M86 Medium Security Policy	1	1	12
Block Known Viruses (McAfee)	Block	M86 Medium Security Policy	2	2	8
Block Access to Blacklisted Sites	Block	M86 Medium Security Policy	1	1	2
Block Access to Spyware Sites	Block	M86 Basic Security Policy	1	1	1
Allow Known Legitimate Content	Allow content	M86 Medium Security Policy	1	1	1

Fig. 6:1-4 Rule Transactions report view

The following statistics display for each Rule Transactions record in the table: In the Actions column, the action performed by the SWG regarding the rule applied to that transaction; in the Policies column, the policy from the SWG applied to that transaction; the IP Count and User Count of end users who triggered that rule, and the total Count of all user encounters for that record.

Security Report Tools

Report Type tabs (Blocked Viruses, Security Policy Violations, Traffic Analysis, and Rule Transactions) display at the top of the panel. Click one of these tabs to display the specified report view.

The following objects display at the bottom of the panel:

- **Report Settings** - Mouse over this object to display a menu of reporting options: Run, Save, Schedule (see Report Settings Options).
- Report View Option icons:
  - Click this icon to display only the top six bars (see Report View Options, Fig. 6:1-5).
  - Click this icon to display the top six bars and table of records (see Report View Options, Fig. 6:1-6).
  - Click this icon to display the table of records only (see Report View Options, Fig. 6:1-7).
- **Export All Records** - Click this button to open the Export Report pop-up window in which you specify criteria for the report to be generated and distributed (see Export a Security Report).
- **Export Selected** - After selecting one or more records in the table, clicking this button opens the Export Report pop-up window (see Export a Security Report).
- **Go to page ‘x’ of ‘x’ total pages** - If more than one page is included in the report, this field lets you specify the page number to display for the report, using the designated page range for reference.

TIP: *To refresh the report view displayed in the panel, select* ***Reports > Security Reports*** *and choose the report type again.*

Report View Options

The following report view displays as a result of clicking a report view icon at the bottom of a security reports panel:

Report View Graph Only

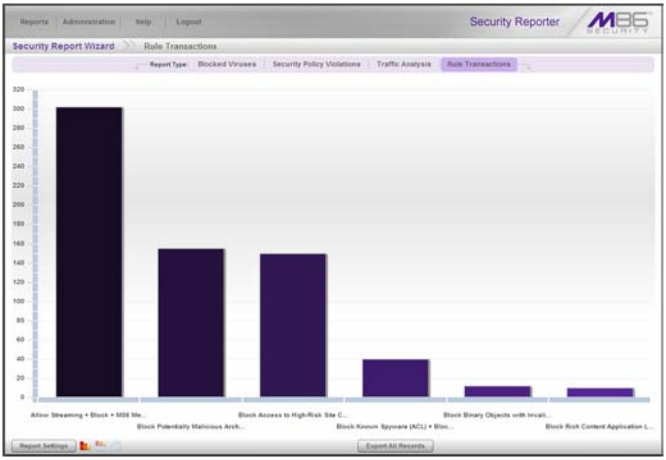
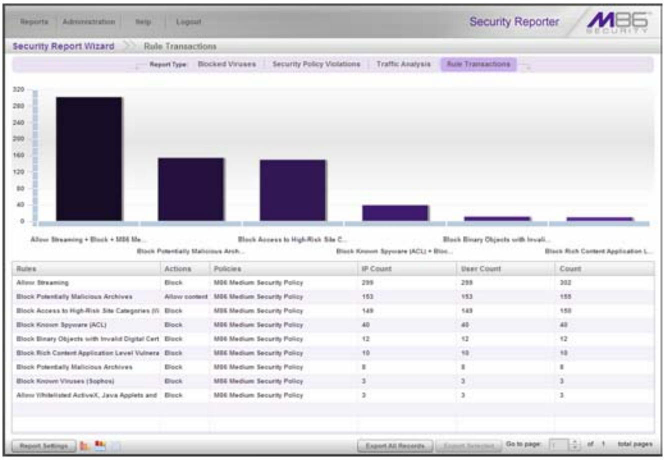


Fig. 6:1-5 Sample top six bars view

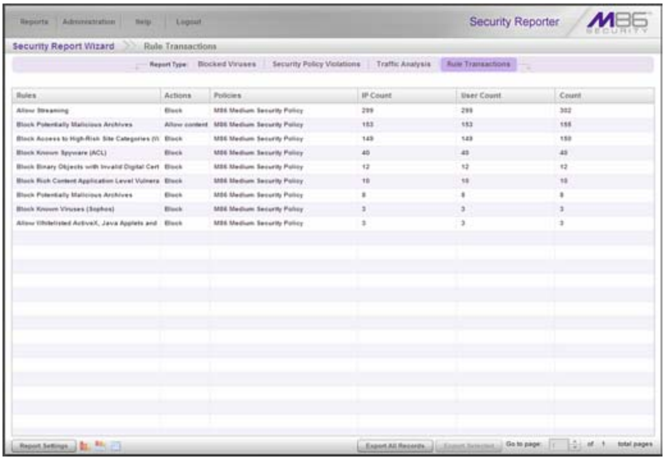
Report View Graph and Records



Rules	Actions	Policies	IP Count	User Count	Count
Allow Streaming	Block	M86 Medium Security Policy	299	299	302
Block Potentially Malicious Archives	Allow content	M86 Medium Security Policy	153	153	155
Block Access to High-Risk Site Categories (V	Block	M86 Medium Security Policy	149	149	150
Block Known Spyware (ACL)	Block	M86 Medium Security Policy	40	40	40
Block Binary Objects with Invalid Digital Cert	Block	M86 Medium Security Policy	12	12	12
Block Rich Content Application Level Vulnera	Block	M86 Medium Security Policy	10	10	10
Block Potentially Malicious Archives	Block	M86 Medium Security Policy	8	8	8
Block Known Viruses (Sophos)	Block	M86 Medium Security Policy	3	3	3
Allow Whitelisted ActiveX, Java Applets and	Block	M86 Medium Security Policy	3	3	3

Fig. 6:1-6 Sample top six bars and report records view (default view)

Report View Records Only



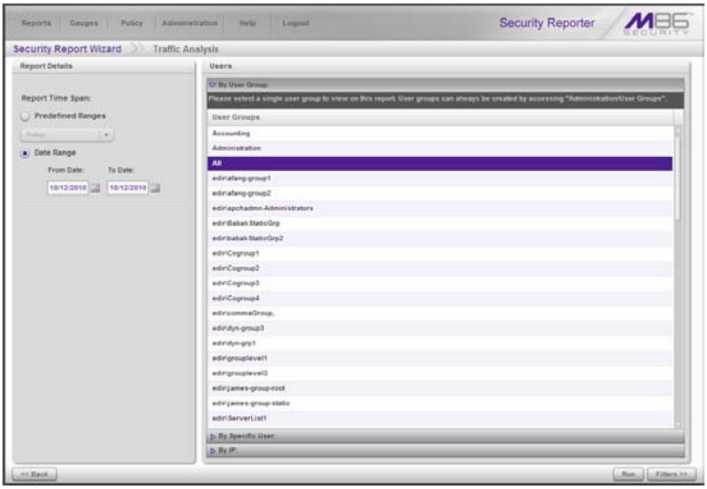
Rules	Actions	Policies	IP Count	User Count	Count
Allow Streaming	Block	M86 Medium Security Policy	299	299	302
Block Potentially Malicious Archives	Allow content	M86 Medium Security Policy	153	153	155
Block Access to High-Risk Site Categories (V	Block	M86 Medium Security Policy	149	149	150
Block Known Spyware (ACL)	Block	M86 Medium Security Policy	40	40	40
Block Binary Objects with Invalid Digital Cert	Block	M86 Medium Security Policy	12	12	12
Block Rich Content Application Level Vulnera	Block	M86 Medium Security Policy	10	10	10
Block Potentially Malicious Archives	Block	M86 Medium Security Policy	8	8	8
Block Known Viruses (Sophos)	Block	M86 Medium Security Policy	3	3	3
Allow Whitelisted ActiveX, Java Applets and	Block	M86 Medium Security Policy	3	3	3

Fig. 6:1-7 Sample records only view

Report Settings Options

Run a Security Report

1. In the security report view, mouse over **Report Settings** and choose **Run** to display the Security Report Wizard panel for that report:



Report Time Span:

○ Predefined Ranges

Today

● Date Range

From Date: 10/12/2010 To Date: 10/12/2010

Please select a single user group to view on this report. User groups can always be created by accessing "Administration/User Groups".

Accounting
Administration
All
edir\afang-group1
edir\afang-group2
edir\apchadmn-Administrators
edir\Babak StaticGrp
edir\babak StaticGrp2
edir\Cogroup1
edir\Cogroup2
edir\Cogroup3
edir\Cogroup4
edir\commaGroup,
edir\dyn-group3
edir\dyn-grp1
edir\grouplevel1
edir\grouplevel3
edir\james-group-root
edir\james-group-static
edir\ServerList1

Fig. 6:1-8 Report Settings Run option

2. In the Report Details frame, specify the **Report Time Span** by choosing one of two options:

   - **Predefined Ranges** - If selecting this option, make a choice from the pull-down menu: “Today” (default), “Month to Date”, “Year to Date”, “Yesterday”, “Month to Yesterday”, “Year to Yesterday”, “Last Week”, “Last Weekend”, “Current Week”, “Last Month”.
   - **Date Range** (default) - If selecting this option, use the calendar icons to set the date range.

***TIP**: At the bottom left of the panel, click **<< Back** at any time to return to the previous Security Report panel.*

3. In the Users frame, select one of the accordions and indicate criteria to include in the report to be generated:

   - **By User Group** - If selecting this option, choose the User Group for your report query results.
   - **By Specific User** - If selecting this option, enter the end user name—using the ‘%’ wildcard to return multiple usernames—and then click **Preview Users** to display query results in the list box below.
   - **By IP** - If selecting this option, enter the end user IP address for filtering your results—using the ‘%’ wildcard to return multiple IP addresses—and then click **Preview Users** to display query results in the list box below.

   For a Traffic Analysis or Rule Transactions report, you can narrow your search result by including filters:

   a. Click **>> Filters** at the bottom right of the panel to display the filter results panel:

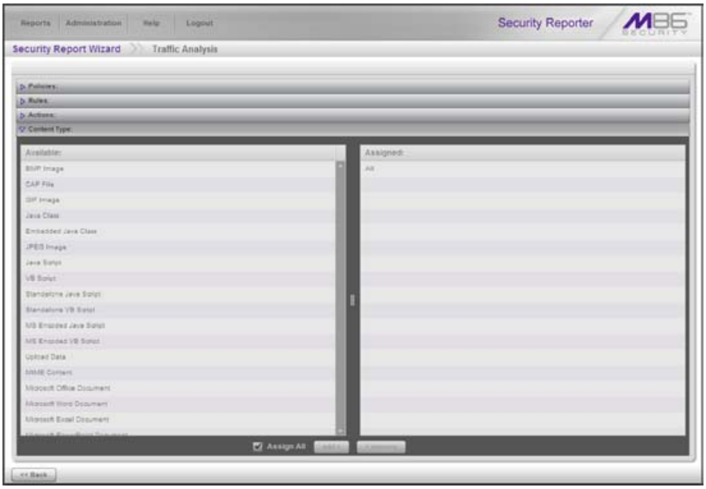


Fig. 6:1-9 Report Filters option

b. Choose a filter type from an available accordion (Policies, Rules, Action, Content Type) and indicate criteria to use in the filter:

- Select one or more records from the Available list box and click **add >** to move the record(s) to the Assigned list box.

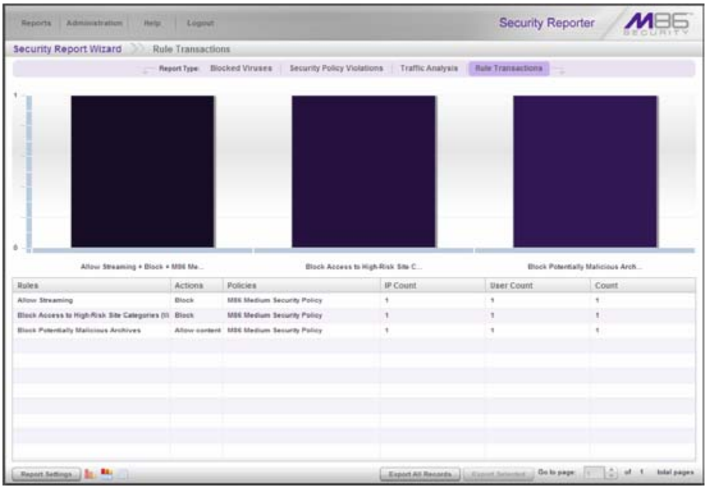
***TIPS**: Multiple records can be selected by clicking each record while pressing the Ctrl key on your keyboard. Blocks of records can be selected by clicking the first record, and then pressing the Shift key on your keyboard while clicking the last record.*

*To remove the record(s), select the record(s) from the Assigned list box and click **< remove**.*

- Click the "Assign All" checkbox to select all records and grey-out the panel.

c. Click **<< Back** to return to the Security Report Wizard panel.

4. Click **Run** to generate the security report view:



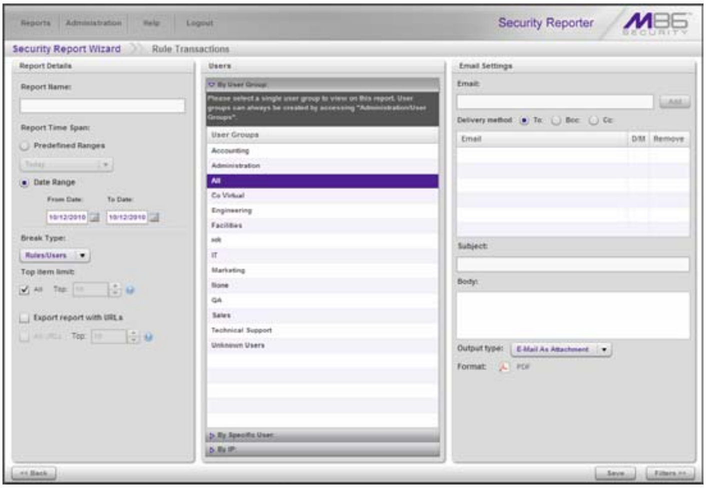
Rules	Actions	Policies	IP Count	User Count	Count
Allow Streaming	Block	M86 Medium Security Policy	1	1	1
Block Access to High-Risk Site Categories (II	Block	M86 Medium Security Policy	1	1	1
Block Potentially Malicious Archives	Allow content	M86 Medium Security Policy	1	1	1

Fig. 6:1-10 Generated Security Report view

The report can now be exported by selecting one of the export options (see Export a Security Report).

Save a Security Report

1. In the security report view, mouse over **Report Settings** and choose **Save** to display the Security Report Wizard panel for that report:



Please select a single user group to view on this report. User groups can always be created by accessing "Administration/User Groups".

Report Name:

Report Time Span: ○ Predefined Ranges (Today) ● Date Range

From Date: 10/12/2010 To Date: 10/12/2010

Break Type: Rules/Users

Top item limit: ☑ All Top: 10

□ Export report with URLs

□ All URLs Top: 10

User Groups: Accounting, Administration, All, Co Virtual, Engineering, Facilities, sdt, IT, Marketing, None, QA, Sales, Technical Support, Unknown Users

Email:

Delivery method: ● To: ○ Bcc: ○ Cc:

Subject:

Body:

Output type: E-Mail As Attachment

Format: PDF

Fig. 6:1-11 Report Settings Save option

2. In the Report Details frame:

   a. Type in the **Report Name**.

   b. Specify the **Report Time Span** by choosing one of two options:

   - **Predefined Ranges** - If selecting this option, make a choice from the pull-down menu: “Today” (default), “Month to Date”, “Year to Date”, “Yesterday”, “Month to Yesterday”, “Year to Yesterday”, “Last Week”, “Last Weekend”, “Current Week”, “Last Month”.
   - **Date Range** - If selecting this default option, use the calendar icons to set the date range.

   c. Specify the **Break Type** from the available choices in the pull-down menu.

d. Indicate the **Top item limit** to be included in the report; by default “All” is selected. To modify this selection, uncheck this box and specify the **Top** number of items.

e. By default, **Export report with URLs** is de-selected. Click this checkbox to select this option, and then specify the number of URLs to export:

- **All URLs** - Check this checkbox to export all URLs
- **Top** - Specify the number of top URLs to be exported

3. In the Users frame, select one of the accordions and indicate criteria to include in the report to be generated:

- **By User Group** - If selecting this option, choose the User Group for your report query results.
- **By Specific User** - If selecting this option, enter the end user name—using the ‘%’ wildcard to return multiple usernames—and then click **Preview Users** to display query results in the list box below.
- **By IP** - If selecting this option, enter the end user IP address for filtering your results—using the ‘%’ wildcard to return multiple IP addresses—and then click **Preview Users** to display query results in the list box below.

For a Traffic Analysis or Rule Transactions report, you can narrow your search result by including filters:

a. Click **>> Filters** at the bottom right of the panel to display the filter results panel (see Fig. 6:1-9).

TIP: *At the bottom left of the panel, click* ***<< Back*** *at any time to return to the Security Report Wizard panel.*

b. Choose a filter type from an available accordion (Policies, Rules, Action, Content Type) and indicate criteria to use in the filter:

- Select one or more records from the Available list box and click **add >** to move the record(s) to the Assigned list box.

***TIPS**: Multiple records can be selected by clicking each record while pressing the Ctrl key on your keyboard. Blocks of records can be selected by clicking the first record, and then pressing the Shift key on your keyboard while clicking the last record. To remove the record(s), select the record(s) from the Assigned list box and click **< remove**.*

- Click the “Assign All” checkbox to select all records and grey-out the panel.

c. Click **<< Back** to return to the Security Report Wizard panel.

4. In the Email Settings frame:

a. Enter at least one **Email** address and then click **Add** to include the email address in the list box below.

b. Specify the **Delivery method** for the email address: “To” (default), “Bcc”, or “Cc”.

***TIP**: To remove an email address, click the “**X**” in the **Remove** column of the list box.*

***NOTE**: Follow the above procedures for each email to be added.*

c. Type in the **Subject** for the email message.

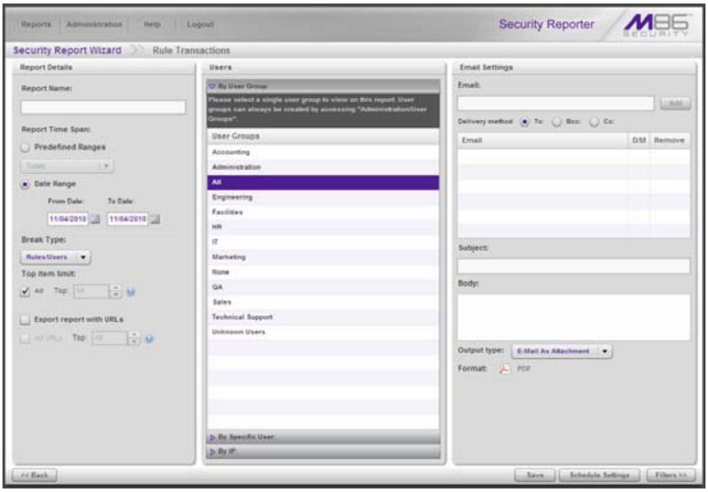
d. If you wish, enter text to be included in the **Body** of the message.

e. Specify the **Output type** for the email: “E-Mail As Attachment” or “E-Mail As Link”.

5. Click **Save** at the bottom of the Security Report Wizard panel to save your settings and to add the report to the Saved Reports panel (see Saved Reports in Chapter 3 from the SR Productivity Reports Section).

Schedule a Security Report to Run

1. In the security report view, click **Report Settings** and choose **Schedule** to display the Security Report Wizard panel for scheduling the report to run:



Report Name:

Report Time Span:
○ Predefined Ranges
● Date Range
From Date: 11/04/2010 To Date: 11/04/2010

Break Type: Rules/Users

Top item limit:
☑ All Top:

□ Export report with URLs
□ All URLs Top:

By User Group

Please select a single user group to view on this report. User groups can always be created by accessing "Administration/User Groups".

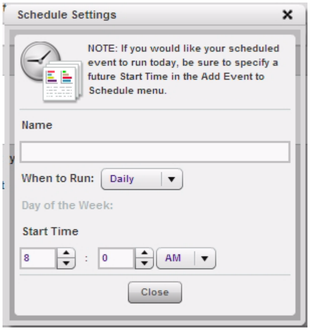
User Groups
Accounting
Administration
All
Engineering
Facilities
HR
IT
Marketing
None
QA
Sales
Technical Support
Unknown Users

By Specific User
By IP

Email:
Delivery method: ● To: ○ Bcc: ○ Cc:
Subject:
Body:
Output type: E-Mail As Attachment
Format: PDF

Fig. 6:1-12 Report Settings Schedule option

2. After specifying criteria for saving the report, go to the lower right corner of the panel and click **Schedule Settings** to open the Schedule Settings pop-up window:



NOTE: If you would like your scheduled event to run today, be sure to specify a future Start Time in the Add Event to Schedule menu.

Name

When to Run: Daily

Day of the Week:

Start Time
8 : 0 AM

Fig. 6:1-13 Schedule Settings

3. Enter a **Name** for the report run event you are scheduling.

4. Select the frequency **When to Run** from the pull-down menu (Daily, Weekly, or Monthly).

   If Weekly, specify the **Day of the Week** from the pull-down menu (Sunday - Saturday).

   If Monthly, specify the **Day of the Month** from the pull-down menu (1 - 31).

5. Select the **Start Time** for the report: 1 - 12 for the hour, 0 - 59 for the minutes, and AM or PM.

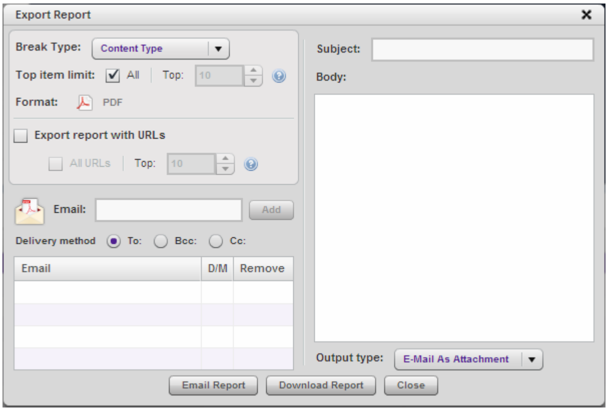
***NOTE**: The default Start Time is 8:00 AM. If you wish to run a report today and this time has already passed, be sure to select a future time.*

6. Click **Close** to save your settings and close the pop-up window.

7. Click **Save** at the bottom of the Security Report Wizard panel to save your settings and to add the report to the schedule to be run (see Report Schedule in Chapter 3 of the SR Productivity Reports Section).

Export a Security Report

At the bottom of the security report view panel, click either **Export All Records** or **Export Selected** to open the Export Report pop-up window:



Export Report

Break Type: Content Type

Top item limit: ☑ All Top: 10

Format: PDF

☐ Export report with URLs

☐ All URLs Top: 10

Email:

Delivery method ● To: ○ Bcc: ○ Cc:

Email	D/M	Remove

Subject:

Body:

Output type: E-Mail As Attachment

Fig. 6:1-14 Export Report pop-up window

***TIP**: Click **Close** to close the pop-up window without executing any of the export functions.*

1. Specify the **Break Type** from the available choices in the pull-down menu.

2. If the Export Selected option was specified, the **Top item limit** for “All” is selected. To modify this selection, uncheck this box and specify the **Top** number of items to be included in the exported report.

3. By default, **Export report with URLs** is de-selected. Click this checkbox to select this option, and then specify the number of URLs to export:

   - **All URLs** - Check this checkbox to export all URLs
   - **Top** - Specify the number of top URLs to be exported

4. To download the report without emailing it, click **Download Report**. To email the report, proceed to step 5.

5. If the report will be emailed instead of downloaded:

    a. Enter at least one **Email** address and then click **Add** to include the email address in the list box below.

    b. Specify the **Delivery method** for the email address: “To” (default), “Bcc”, or “Cc”.

__TIP__: To remove an email address, click the “__X__” in the __Remove__ column of the list box.

__NOTE__: Follow the above procedures in step 5 for each email to be added.

    c. Enter the **Subject** for the email message.

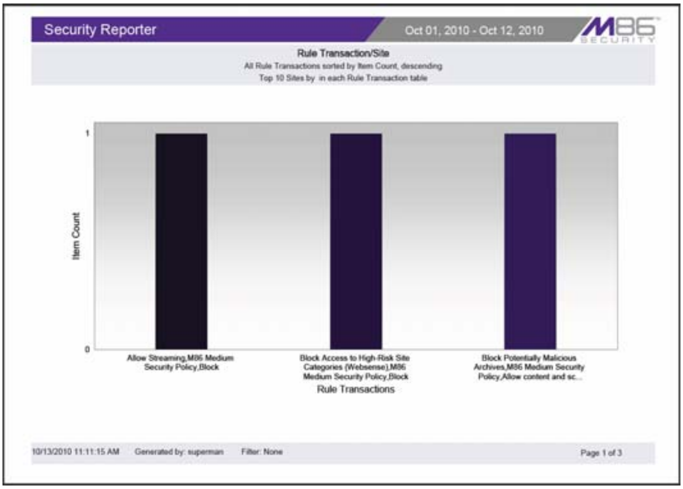
    d. If you wish, enter text to be included in the **Body** of the message.

    e. Specify the **Output type** for the email: “E-Mail As Attachment” or “E-Mail As Link”.

    f. Click **Email Report** to send the email to the specified recipient(s).

Security Report Format

The generated Security Report PDF file includes the following information:



Security Reporter

Oct 01, 2010 - Oct 12, 2010

Rule Transaction/Site

All Rule Transactions sorted by Item Count, descending

Top 10 Sites by in each Rule Transaction table

10/13/2010 11:11:15 AM Generated by: superman Filter: None

Page 1 of 3

M86 SECURITY
1
0
Item Count
Allow Streaming,M86 Medium Security Policy,Block
Block Access to High-Risk Site Categories (Websense),M86 Medium Security Policy,Block
Block Potentially Malicious Archives,M86 Medium Security Policy,Allow content and sc...
Rule Transactions

Fig. 6:1-15 Sample PDF for break type Security Report, page 1

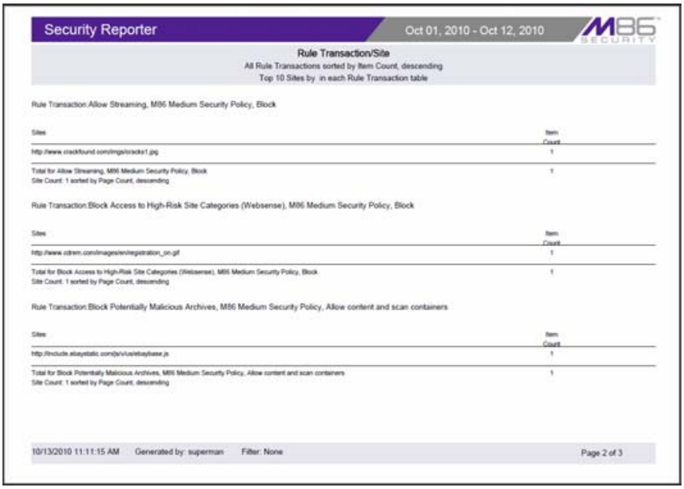
The header of the generated report includes the date range, report type, and criteria details.

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

The body of the first page of the report includes a bar chart showing the top six graphs with count indicators, and the report name.

The body of pages following the first page of the report includes the report name and list of records with the corresponding Item Count for each record. For break type reports, the Total displays at the end of each section.

For non-break type Rule Transaction reports, Policy and Action column data precede Item Count column data.



Security Reporter Oct 01, 2010 - Oct 12, 2010

Rule Transaction/Site
All Rule Transactions sorted by Item Count, descending
Top 10 Sites by in each Rule Transaction table

Rule Transaction:Allow Streaming, M86 Medium Security Policy, Block

Sites	Item Count
http://www.crackfound.com/imgs/cracks1.jpg	1
Total for Allow Streaming, M86 Medium Security Policy, Block Site Count: 1 sorted by Page Count, descending	1

Rule Transaction:Block Access to High-Risk Site Categories (Websense), M86 Medium Security Policy, Block

Sites	Item Count
http://www.cdrem.com/images/en/registration_on.gif	1
Total for Block Access to High-Risk Site Categories (Websense), M86 Medium Security Policy, Block Site Count: 1 sorted by Page Count, descending	1

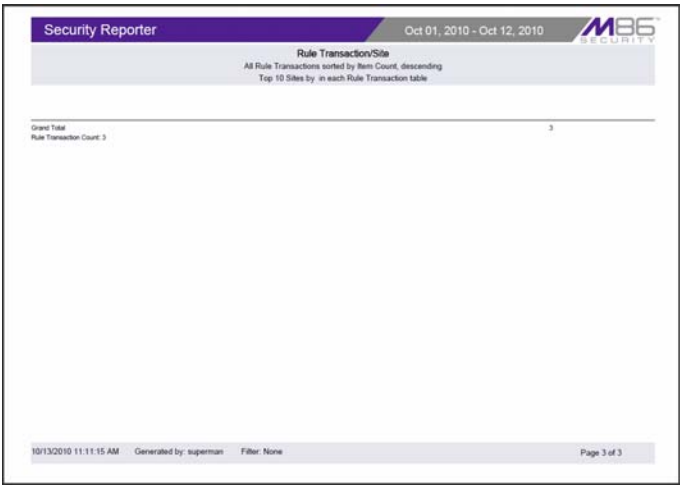
Rule Transaction:Block Potentially Malicious Archives, M86 Medium Security Policy, Allow content and scan containers

Sites	Item Count
http://include.ebaystatic.com/js/v/us/ebaybase.js	1
Total for Block Potentially Malicious Archives, M86 Medium Security Policy, Allow content and scan containers Site Count: 1 sorted by Page Count, descending	1

10/13/2010 11:11:15 AM Generated by: superman Filter: None Page 2 of 3

Fig. 6:1-16 Sample PDF for break type Security Report, page 2

At the end of the report, the Grand Total displays for all records. For Rule Transaction reports, the total Count displays beneath the Grand Total.



Security Reporter Oct 01, 2010 - Oct 12, 2010

Rule Transaction/Site
All Rule Transactions sorted by Item Count, descending
Top 10 Sites by in each Rule Transaction table

Grand Total Rule Transaction Count: 3	3

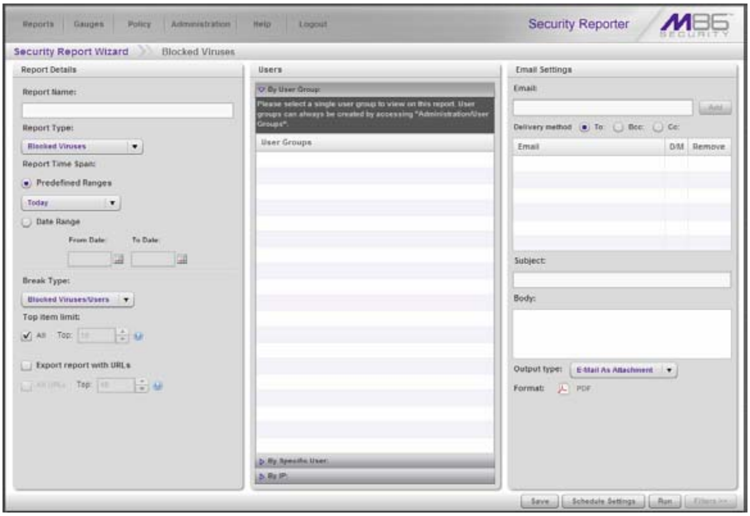
10/13/2010 11:11:15 AM Generated by: superman Filter: None Page 3 of 3

Fig. 6:1-17 Sample PDF for break type Security Report, page 3

Chapter 2: Security Report Wizard

The Security Report Wizard lets you customize any of the basic four Security Reports, and schedule these reports to run on a regular basis.

In the navigation toolbar, mouse over the Reports menu link, choose Security Reports, and then select **Report Wizard** to open the Security Report Wizard panel:



Report Name:

Report Type: Blocked Viruses

Report Time Span:

● Predefined Ranges

Today

○ Date Range

From Date: To Date:

Break Type: Blocked Viruses/Users

Top item limit:

☑ All Top: 10

□ Export report with URLs

□ All URLs Top: 10

▽ By User Group:

Please select a single user group to view on this report. User groups can always be created by accessing "Administration/User Groups".

User Groups

▷ By Specific User:

▷ By IP:

Email:

Delivery method ● To: ○ Bcc: ○ Cc:

Subject:

Body:

Output type: E-Mail As Attachment

Format: PDF

Fig. 6:2-1 Security Report Wizard panel

Create a Custom Security Report

Specify Report Details

In the Report Details frame, specify general information for the security report to be generated:

1. Type in the **Report Name**.
2. Choose the **Report Type** from the pull-down menu (“Blocked Viruses”, “Security Policy Violations”, “Traffic

Analysis", "Rule Transactions"); by default "Blocked Viruses" displays.

3. Specify the **Report Time Span** by choosing one of two options:
   - **Predefined Ranges** - If selecting this default option, make a choice from the pull-down menu: "Today" (default), "Month to Date", "Year to Date", "Yesterday", "Month to Yesterday", "Year to Yesterday", "Last Week", "Last Weekend", "Current Week", "Last Month".
   - **Date Range** - If selecting this option, use the calendar icons to set the date range.
4. Specify the **Break Type** from the available choices in the pull-down menu.
5. Indicate the **Top item limit** to be included in the report; by default "All" is selected. To modify this selection, uncheck this box and specify the **Top** number of items.
6. By default, **Export report with URLs** is de-selected. Click this checkbox to select this option, and then specify the number of URLs to export:
   - **All URLs** - Check this checkbox to export all URLs
   - **Top** - Specify the number of top URLs to be exported

Select Users

In the Users frame, select one of the accordions and indicate criteria to include in the report to be generated:

- **By User Group** - If selecting this option, choose the User Group for your report query results.
- **By Specific User** - If selecting this option, enter the end user name—using the '%' wildcard to return multiple usernames—and then click **Preview Users** to display query results in the list box below.

- **By IP** - If selecting this option, enter the end user IP address for filtering your results—using the ‘%’ wildcard to return multiple IP addresses—and then click **Preview Users** to display query results in the list box below.

  For a Traffic Analysis or Rule Transactions report, you can narrow your search result by including filters:

  a. Click **>> Filters** at the bottom right of the panel to display the filter results panel:

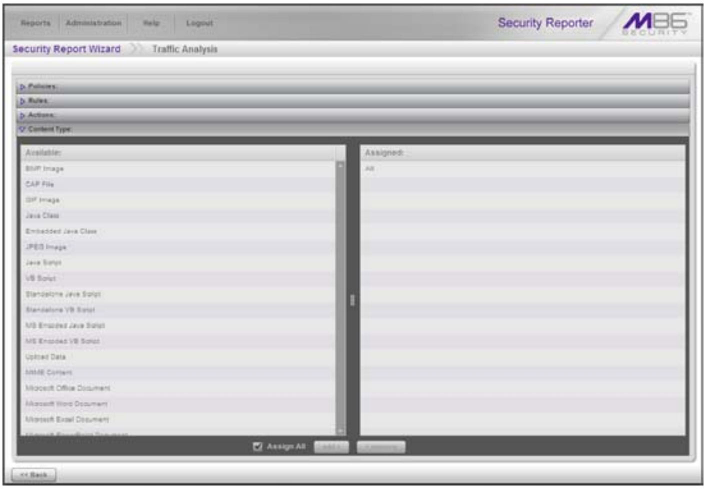


Fig. 6:2-2 Security Report Wizard Filters option

***TIP**: At the bottom left of the panel, click **<< Back** at any time to return to the Security Report Wizard panel.*

  b. Choose a filter type from an available accordion (Policies, Rules, Action, Content Type) and indicate criteria to use in the filter:

  - Select one or more records from the Available list box and click **add >** to move the record(s) to the Assigned list box.

***TIPS**: Multiple records can be selected by clicking each record while pressing the Ctrl key on your keyboard. Blocks of records can be selected by clicking the first record, and then pressing the Shift key on your keyboard while clicking the last record.*

*To remove the record(s), select the record(s) from the Assigned list box and click **< remove**.*

- Click the “Assign All” checkbox to select all records and grey-out the panel.

c. Click **<< Back** to return to the Security Report Wizard panel.

Specify Email Settings

In the Email Settings frame:

1. Enter at least one **Email** address and then click **Add** to include the email address in the list box below.
2. Specify the **Delivery method** for the email address: “To” (default), “Bcc”, or “Cc”.

***TIP**: To remove an email address, click the “**X**” in the **Remove** column of the list box.*

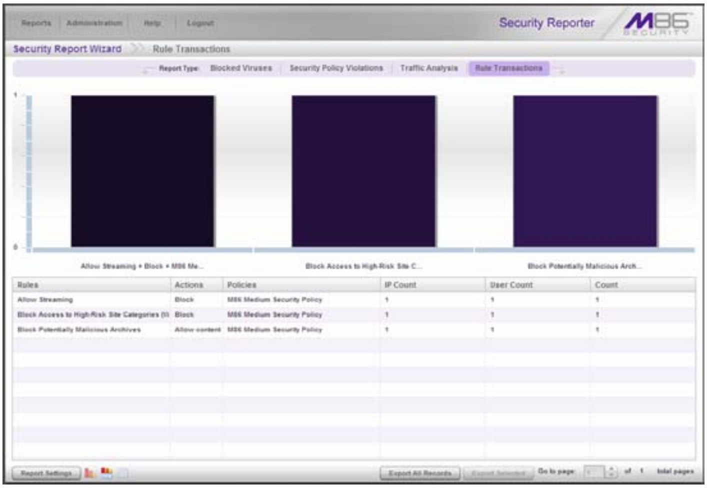
***NOTE**: Follow the above procedures for each email to be added.*

3. Type in the **Subject** for the email message.
4. If you wish, enter text to be included in the **Body** of the message.
5. Specify the **Output type** for the email: “E-Mail As Attachment” or “E-Mail As Link”.

Schedule, Run a Report using the Wizard

Once security report settings have been made using the Security Report Wizard, choose one of two reporting options by clicking the button at the bottom right of the panel:

- **Schedule Settings** - Click this button to open the Schedule Settings pop-up window (see Fig. 6:1-13) and follow the procedures in Report Settings Options: Schedule a Security Report to Run from Chapter 1.
- **Run** - Click this button to generate the security report. The finished report view displays in the panel:



Rules	Actions	Policies	IP Count	User Count	Count
Allow Streaming	Block	M86 Medium Security Policy	1	1	1
Block Access to High-Risk Site Categories (II)	Block	M86 Medium Security Policy	1	1	1
Block Potentially Malicious Archives	Allow content	M86 Medium Security Policy	1	1	1

Fig. 6:2-3 Generated Security Report view

The report can now be:

- Exported by selecting one of the export options (see Export a Security Report in Chapter 1), and a PDF of the report downloaded to your machine.
- Saved by going to the Report Settings menu and selecting the Save option (see Report Settings Options: Save a Security Report in Chapter 1).

SR APPENDICES SECTION

Appendix A

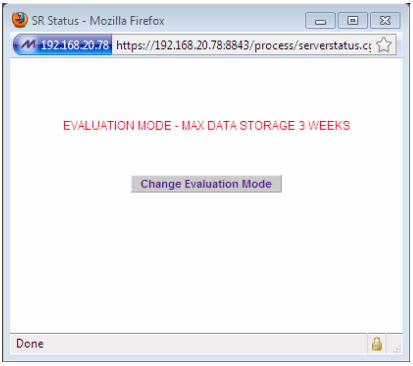
Evaluation Mode

By default, the SR is set to the evaluation mode. This appendix explains how to use the SR in the evaluation mode, and how to register the SR to function in the registered mode.

***NOTE**: Contact the administrator of the SR to enable the SR in the registered mode.*

System Configuration Console

When accessing the **Server > Server Status** screen for the first time, the SR Status pop-up box opens to inform you that the SR unit is currently in the evaluation mode:


SR Status - Mozilla Firefox
192.168.20.78
https://192.168.20.78:8843/process/serverstatus.cç
Change Evaluation Mode
Done

EVALUATION MODE - MAX DATA STORAGE 3 WEEKS

Fig. A-1 SR Status pop-up box

The SR will store data for the period specified in the pop-up box: “EVALUATION MODE - MAX DATA STORAGE ‘X’ WEEKS”—in which ‘X’ represents the maximum number of weeks in the SR’s data storage scope.

You have the option to either use the SR in the evaluation mode, or change the evaluation mode in one of two ways—by extending the evaluation period, or by registering the SR so that it can be used in the registered mode.

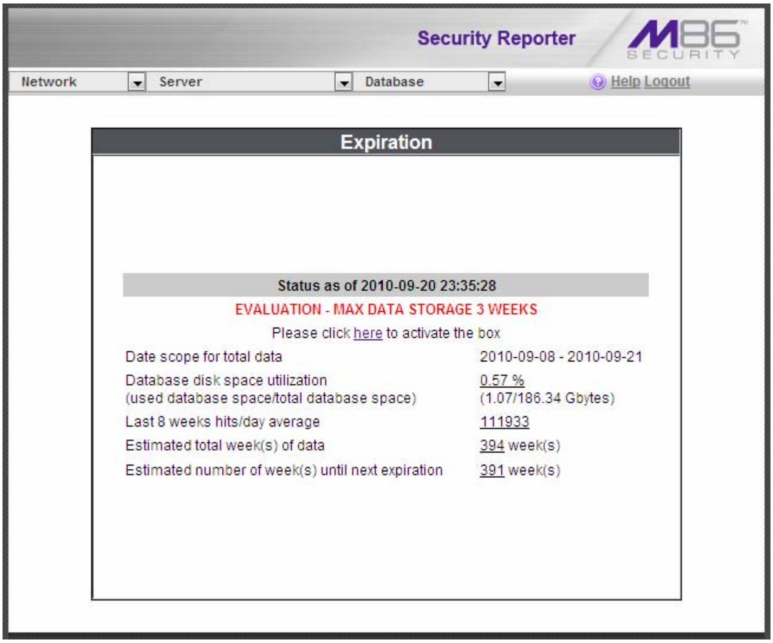
***NOTE**: The message: “EVALUATION MODE - MAX DATA STORAGE ‘X’ WEEKS” also displays at the top of the Expiration screen in the System Configuration console. Refer to the Expiration screen sub-section in Chapter 2 of the SR System Configuration Section for more information about data storage and expiration.*

Use the Server in the Evaluation Mode

To use the unit in the evaluation mode, click the "X" in the upper right corner of the SR Status pop-up box to close it.

Expiration screen

In the evaluation mode, the Expiration screen can only be used for viewing data storage statistics, and not for modifying data storage capacity criteria.



Expiration

Status as of 2010-09-20 23:35:28

EVALUATION - MAX DATA STORAGE 3 WEEKS

Please click here to activate the box

Date scope for total data	2010-09-08 - 2010-09-21
Database disk space utilization (used database space/total database space)	0.57 % (1.07/186.34 Gbytes)
Last 8 weeks hits/day average	111933
Estimated total week(s) of data	394 week(s)
Estimated number of week(s) until next expiration	391 week(s)

Fig. A-2 Expiration screen

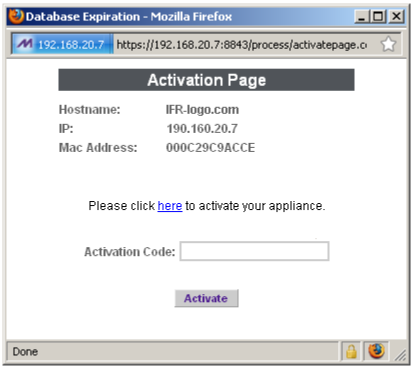
When the SR is in the evaluation mode, the following message displays at the top of the screen: “EVALUATION – MAX DATA STORAGE ‘X’ WEEKS” (in which ‘X’ represents the maximum number of weeks in the SR’s data storage scope).

Change the Evaluation Mode

After the designated evaluation period has expired, you may extend your evaluation period, or register the unit and use it in the registered mode. There are two ways to change the evaluation mode from the System Configuration console:

- in the SR Status pop-up box (see Fig. A-1), click **Change Evaluation Mode**
- in the Evaluation screen, click the link (“here”) in the message at the top of the screen: “Please click here to activate the box”.

By clicking the button or link, the Activation Page pop-up box opens:


Database Expiration - Mozilla Firefox
192.168.20.7
https://192.168.20.7:8843/process/activatepage.c
Activate
Done

Activation Page

Hostname: IFR-logo.com
IP: 190.160.20.7
Mac Address: 000C29C9ACCE

Please click here to activate your appliance.

Activation Code:

Fig. A-3 Activation Page pop-up box

Activation Page

1. In the Activation Page pop-up box, the **Hostname** of the Server, **IP** address, and **Mac Address** (Media Access Control address) display.
2. In the message “Please click here to activate your appliance.”, click the link ‘**here**’ to open the Product Activation page at the M86 Security Web site.
3. In this Web page:

a. Enter your following information: Contact Details, Company Information, and Security Reporter Information.

b. Choose the Activation Type: "Evaluation Extension" or "Full Activation."

4. Click **Send Information**. After M86 obtains your information, a technical support representative will issue you an activation code.
5. Return to the Activation Page (see Fig. A-3) and enter the activation code in the **Activation Code** field.
6. Click **Activate** to display the confirmation message in the Activation Page pop-up box:
   - If extending the evaluation period for the unit, the following message displays: “It is now in evaluation mode (‘X’ weeks)!” in which ‘X’ represents the number of weeks in the new evaluation period.
   - If registering the unit, the following message displays: “Your box has been activated!”
7. Click the ‘X’ in the upper right corner to close the Activation Page pop-up box.

Appendix B

System Tray Alerts: Setup, Usage

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

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

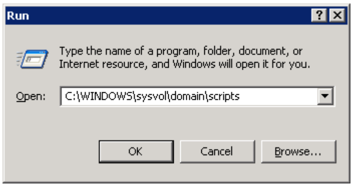
***NOTE**: In order to use this feature, the LDAP Username and Domain set up in the administrator's profile account (see Admin Profiles panel from Chapter 1 of the SR Report Manager Administrator Section) must be the same one he/she uses when logging into his/her workstation.*

LDAP server configuration

Create the System Tray logon script

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

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



Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: C:\WINDOWS\sysvol\domain\scripts

Fig. B-1 Run dialog box

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

3. Click **OK** to open the scripts folder:

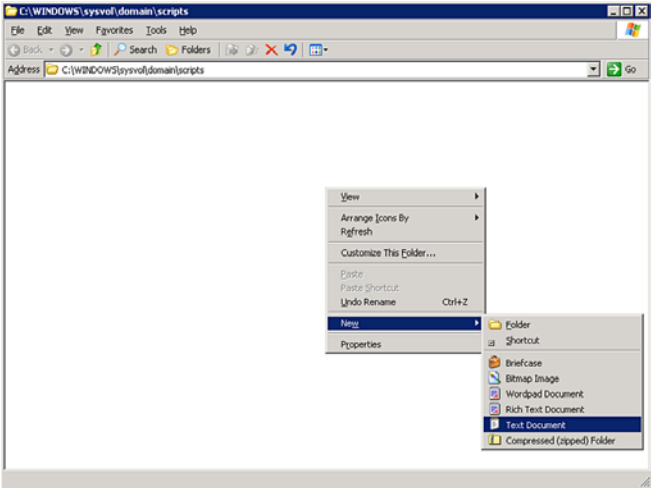
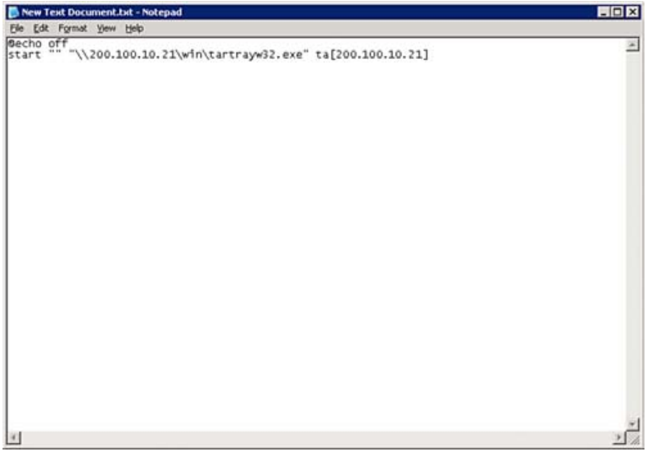


Fig. B-2 C:\WINDOWS\sysvol\domain\scripts window

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

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



```
@echo off
start "" "\\200.100.10.21\win\tartrayw32.exe" ta[200.100.10.21]
```

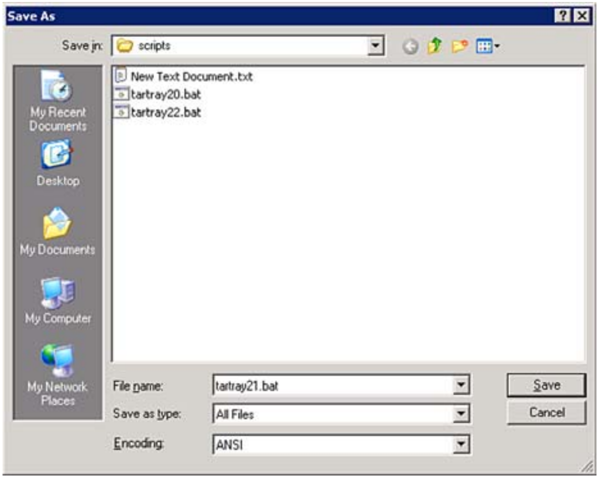
Fig. B-3 New Text Document

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

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

   in which “X.X.X.X” represents the IP address of the SR, and “\win\tartrayw32.exe” refers to the location of the SR Tray Alert executable file on the SR.

7. Go to: **File > Save As** to open the Save As window:



File name: tartray21.bat

Save as type: All Files

Encoding: ANSI

Fig. B-4 Save As dialog box

8. In the **File name** field, type in the name for the file using the “filename.bat” format. For example: ***tartray21.bat***.

NOTE: *Be sure that the Save as type field has “All Files” selected.*

9. Click **Save** to save your file and to close the window.

Assign System Tray logon script to administrators

With the ".bat" file created, the administrator with permissions on the LDAP server can now begin to assign the System Tray logon script to as many administrators as needed.

1. From the taskbar of the LDAP server, go to: **Start > Programs > Administrative Tools > Active Directory Users and Computers** to open the Active Directory Users and Computers folder:

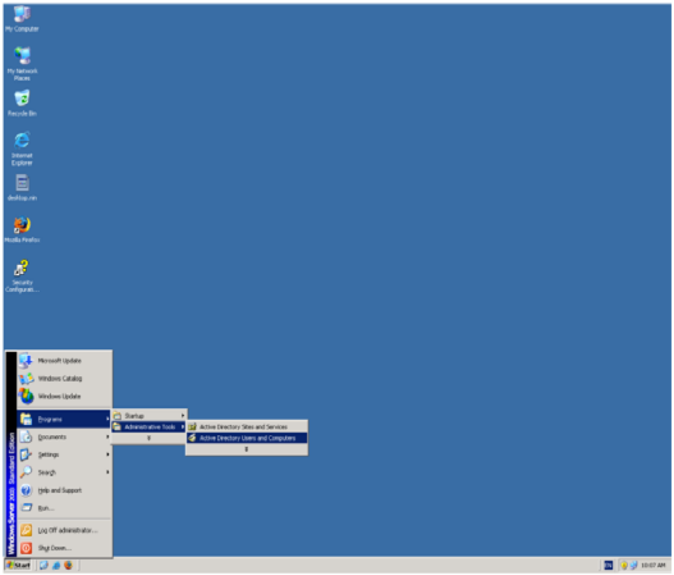
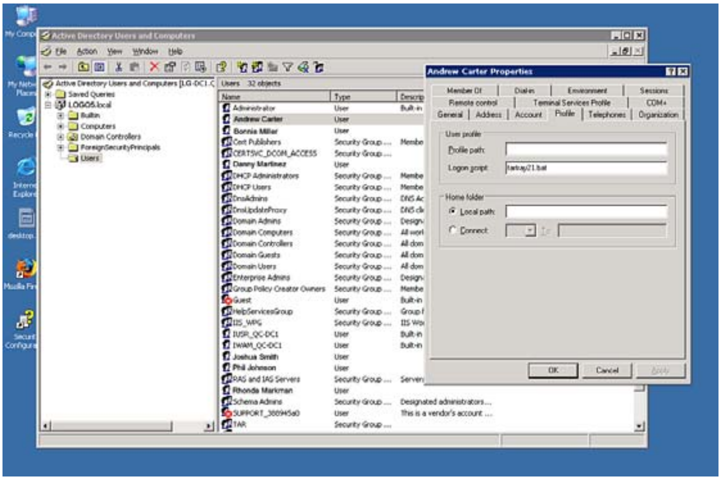


Fig. B-5 Programs > Administrative Tools > Active Directory Users

2. In the Active Directory Users and Computers folder, double-click the administrator's Name in the Users list to open the Properties dialog box for his/her profile:



Users 32 objects

Name	Type	Descrip
Administrator	User	Built-in
Andrew Carter	User	
Bonnie Miller	User	
Cert Publishers	Security Group	Membe
CERTSVC_DCOM_ACCESS	Security Group	
Danny Martinez	User	
DHCP Administrators	Security Group	Membe
DHCP Users	Security Group	Membe
DnsAdmins	Security Group	DNS Ac
DnsUpdateProxy	Security Group	DNS cli
Domain Admins	Security Group	Design
Domain Computers	Security Group	All worl
Domain Controllers	Security Group	All dom
Domain Guests	Security Group	All dom
Domain Users	Security Group	All dom
Enterprise Admins	Security Group	Design
Group Policy Creator Owners	Security Group	Membe
Guest	User	Built-in
HelpServicesGroup	Security Group	Group f
IIS_WPG	Security Group	IIS Wo
IUSR_QC-DC1	User	Built-in
IWAM_QC-DC1	User	Built-in
Joshua Smith	User	
Phil Johnson	User	
RAS and IAS Servers	Security Group	Servers
Rhonda Markman	User	
Schema Admins	Security Group	Designated administrators....
SUPPORT_388945a0	User	This is a vendor's account ....
TAR	Security Group	

User profile

Profile path:

Logon script: tartray21.bat

Home folder

● Local path:

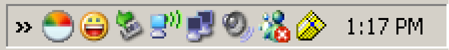
○ Connect: To:

Fig. B-6 Properties dialog box, Active Directory Users folder

3. In the Properties dialog box, click the Profile tab to display its contents.
4. In the **Login script** field, type in the ".bat" filename. For example: ***tartray21.bat***.
5. Click **Apply** to save your entry.
6. Click **OK** to close the dialog box.
7. Click the "X" in the upper right corner of the folder to close the window.

Administrator usage of System Tray

Once the System Tray logon script has been added to the administrator's profile, when the administrator logs on his/her workstation, the System Tray Alert icon (pictured to the far left in the image below) automatically loads in his/her System Tray:



***NOTE**: The System Tray Alert icon will not load in the System Tray if the SR is not actively running.*

Use the System Tray Alert icon's menu

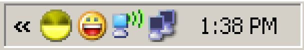
When right-clicking the System Tray Alert icon, the following pop-up menu items display:

- SR Admin Interface - clicking this menu selection launches a browser window containing the SR user interface's login window.
- Reconnect - clicking this menu selection re-establishes the System Tray Alert icon's connection to the SR, resetting the status of the System Tray Alert icon to the standard setting.
- Exit - clicking this menu selection removes the System Tray Alert icon from the System Tray.

Status of the System Tray Alert icon

If there are no alerts for any gauges set up by the administrator, the following message displays when mousing over the standard System Tray Alert icon: “Connected. No Alerts.”

However, if an alert is triggered, the System Tray Alert icon changes in appearance from the standard gauge to a yellow gauge (pictured to the far left in the image below):



The following message appears briefly above the yellow gauge: “New M86 SR Alert!” The following message displays whenever mousing over this icon: “New M86 SR Alert”.

If more than one alert is triggered for the administrator, the message reads: “New M86 SR Alert! (X Total)”, in which “X” represents the total number of new alerts. The following message displays whenever mousing over this icon: “X New M86 SR Alerts”, in which “X” represents the total number of new alerts.

View System Tray alert messages

1. Double-click the SR Tray Alert notification icon to open the SR Alert box:

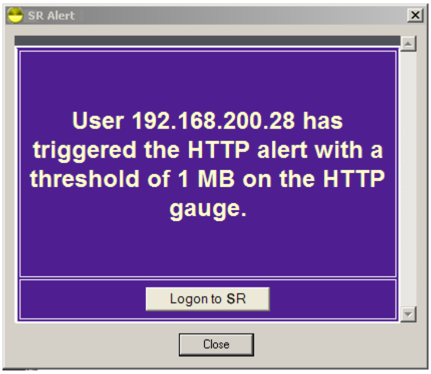

SR Alert
User 192.168.200.28 has triggered the HTTP alert with a threshold of 1 MB on the HTTP gauge.
Logon to SR
Close

Fig. B-7 SR Alert

This box contains the following message: “User (username/IP address) has triggered the (Alert Name) alert with a threshold of X (in which “X” represents the alert threshold) on the (URL dashboard gauge name) gauge.”

The Logon to SR button displays beneath this message, followed by the Close button.

If more than one alert was triggered, the alert box includes the following message and button to the right of the Close button: “X more alerts” (in which “X” represents the number of additional alerts), and the Next >> button.

2. Click **Logon to SR** to launch the SR login window (see Fig. 1:1-2).

If there are additional alerts, click **Next >>** to view the next SR Alert. Each time the Next >> button is clicked, the number of remaining alerts to be viewed decreases by one. The Next >> button no longer displays after the last alert is viewed.

3. Click **Close** to close the SR Alert box.

Appendix C

Glossary

This glossary includes definitions for terminology used in this user guide.

base group - A user group consisting of end users whose network activities are monitored by the designated group administrator(s). Only the creator of the base group can modify the base group, delegate the base group to another group administrator, or delete the base group.

canned report - A pre-processed report that includes statistics of end user Internet/network traffic prior to the current day.

custom category - A unique library category on the Web Filter that includes URLs, URL keywords, and/or search engine keywords to be blocked. On the SR, global administrators can create and manage custom library categories and sync them to the source Web Filter.

detail drill down report - One of two types of basic reports—the other report type being a “summary drill down report”—that provides information on objects or pages an end user viewed within the specified time period.

double-break report - A report that uses two sets of criteria, such as User/Sites or Category/IPs.

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

global administrator - An authorized administrator of the network who maintains all aspects of the SR. The global administrator configures the SR, sets up user groups, administrator groups and group administrators, and performs routine maintenance on the server.

group administrator - An authorized administrator of the SR who maintains user group, administrator groups, group administrator profiles, and gauges.

hit count - the number of pages and/or objects end users access as the result of entering URLs in a browser window.

HTTP - Hyper Text Transfer Protocol is used for transferring files via the World Wide Web or an intranet.

instant messaging - IM involves direct connections between workstations either locally or across the Internet.

library category - A list of URLs, URL keywords, and search engine keywords set up to be blocked.

LDAP - One of two authentication method protocols that can be used with the SR. Lightweight Directory Access Protocol (LDAP) is a directory service protocol based on entries (Distinguished Names). The other authentication method that can be used with the SR is IP groups.

object count - The number of objects end users access on a Web page, including images, graphics, multimedia items, and text items. The number of objects on a page is generally higher than the number of pages a user visits.

page count - The number of Web pages end users access, which can exceed the number of objects per page in categories that use a lot of pop-up ads (porn, gambling, and other related sites). A user may visit only one site, but visit 20 pages on that site if the page has pop-up ads or banner ads that link to other pages.

peer-to-peer - P2P involves communication between computing devices—desktops, servers, and other smart devices—that are linked directly to each other.

protocol - A type of format for transmitting data between two devices. LDAP is a type of authentication method protocol.

search engine - A program that searches Web pages for specified keywords and returns a list of the pages or services where the keywords were found.

SMTP - Simple Mail Transfer Protocol is used for transferring email messages between servers.

summary drill down report - One of two types of basic reports—the other report type being a “detail drill down report”—that provides a synopsis of end user Internet activity for the specified time period.

synchronization - A process by which two or more machines run in parallel to each other. User filtering profiles and library configurations on the source Web Filter can be set up to be synchronized between the source Web Filter and the SR.

TCP - An abbreviation for Transmission Control Protocol, one of the core protocols of the Internet protocol suite. Using TCP, applications on networked hosts can create connections to one another, over which streams of data can be exchanged.

time count - The amount of time end users spend on a given Web page, including the number of times that page is refreshed by either the user or a banner ad.

Time Usage Report count - The amount of time end users spend on the Internet, based on the Time Usage algorithm. For each user, the number of seconds from the log is dropped, and any unique minute within a given hour counts as one minute.

Traveler - M86 Security’s executable program that downloads updates to the WFR at a scheduled time.

UDP - An abbreviation for User Data Protocol, one of the core protocols of the Internet protocol suite. Using UDP, programs on networked computers can send short messages (sometimes known as datagrams) to one another.

URL - An abbreviation for Uniform Resource Locator, the global address of Web pages and other resources on the Internet. A URL is comprised of two parts. The first part of the address specifies which protocol to use (such as "http"). The second part specifies the IP address or the domain name where the resource is located (such as “203.15.47.23” or "m86security.com").

Web access logging device - The M86 Web Filter and possibly other filtering device (such as an M86 Secure Web Gateway) feeding logs to the SR.

WFR APPENDICES SECTION

Appendix I

Disable Pop-up Blocking Software

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

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

Yahoo! Toolbar Pop-up Blocker

Add the Client to the White List

If the Client was previously blocked by the Yahoo! Toolbar, it can be moved from the black list and added to the white list so that it will always be allowed to pass. To do this:

1. Go to the Yahoo! Toolbar and click the pop-up icon to open the pop-up menu:

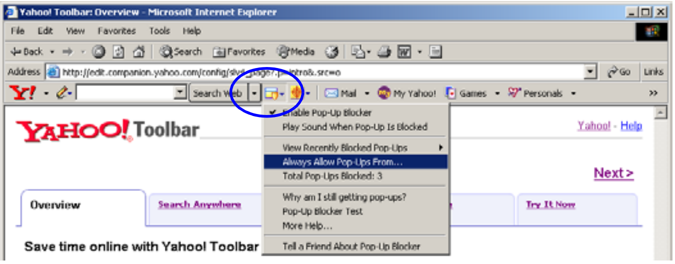

Yahoo! Toolbar: Overview - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://edit.companion.yahoo.com/config/slv_page?.p=intro&.src=o
Go Links
Y! Search Web Mail My Yahoo! Games Personals
YAHOO! Toolbar
Yahoo! - Help
✓ Enable Pop-Up Blocker
Play Sound When Pop-Up Is Blocked
View Recently Blocked Pop-Ups
Always Allow Pop-Ups From...
Total Pop-Ups Blocked: 3
Why am I still getting pop-ups?
Pop-Up Blocker Test
More Help...
Tell a Friend About Pop-Up Blocker
Next >
Overview
Search Anywhere
Try It Now
Save time online with Yahoo! Toolbar

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

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

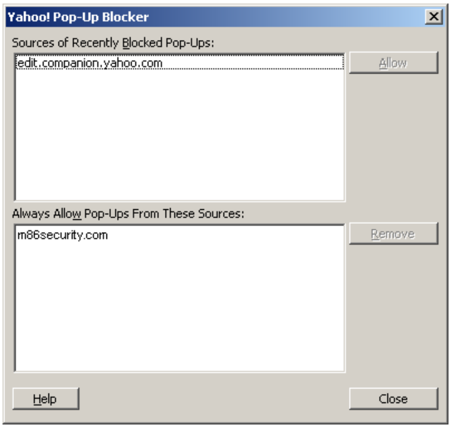


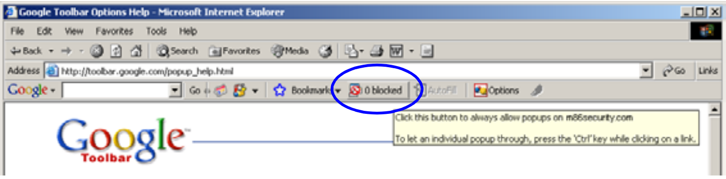
Fig. I-2 Allow pop-ups from source

3. Select the source from the Sources of Recently Blocked Pop-Ups list box to activate the Allow button.
4. Click **Allow** to move the selected source to the Always Allow Pop-Ups From These Sources list box.
5. Click **Close** to save your changes and to close the dialog box.

Google Toolbar Pop-up Blocker

Add the Client to the White List

To add the Client to the white list so that it will always be allowed to pass, go to the Google Toolbar and click the Pop-up blocker button:

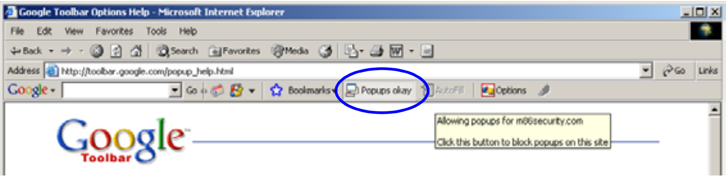

Google Toolbar Options Help - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://toolbar.google.com/popup_help.html
Go Links
Google Go Bookmarks 0 blocked AutoFill Options
Google Toolbar

Click this button to always allow popups on m86security.com

To let an individual popup through, press the 'Ctrl' key while clicking on a link.

Fig. I-3 Pop-up blocker button enabled

Clicking this icon toggles to the Pop-ups okay button, adding the Client to your white list:


Google Toolbar Options Help - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://toolbar.google.com/popup_help.html
Go Links
Google Go Bookmarks Popups okay AutoFill Options
Google Toolbar

Allowing popups for m86security.com

Click this button to block popups on this site

Fig. I-4 Pop-ups okay button enabled

AdwareSafe Pop-up Blocker

Disable Pop-up Blocking

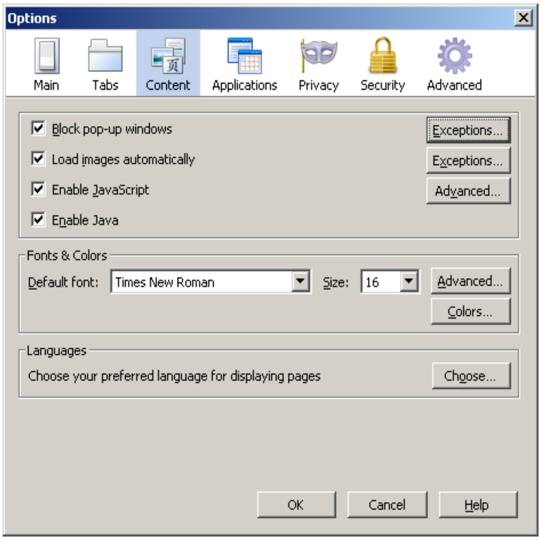
AdwareSafe's SearchSafe toolbar lets you toggle between enabling pop-up blocking (# popups blocked) and disabling pop-up blocking (Popup protection off) by clicking the pop-up icon.

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

Mozilla Firefox Pop-up Blocker

Add the Client to the White List

1. From the Firefox browser, go to the toolbar and select **Tools > Options** to open the Options dialog box.
2. Click the Content tab at the top of this box to open the Content section:



☑ Block pop-up windows

☑ Load images automatically

☑ Enable JavaScript

☑ Enable Java

Fonts & Colors

Default font: Times New Roman

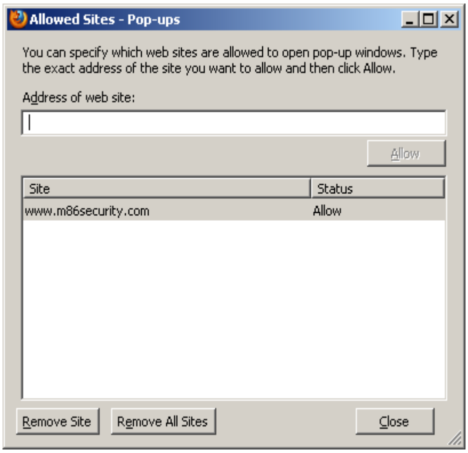
Size: 16

Languages

Choose your preferred language for displaying pages

Fig. I-5 Mozilla Firefox Pop-up Windows Options

3. With the “Block pop-up windows” checkbox checked, click the **Exceptions...** button at right to open the Allowed Sites - Pop-ups box:



Allowed Sites - Pop-ups

You can specify which web sites are allowed to open pop-up windows. Type the exact address of the site you want to allow and then click Allow.

Address of web site:

Site	Status
www.m86security.com	Allow

Fig. I-6 Mozilla Firefox Pop-up Window Exceptions

4. Enter the **Address of the web site** to let the client pass.
5. Click **Allow** to add the URL to the list box section below.
6. Click **Close** to close the Allowed Sites - Pop-ups box.
7. Click OK to close the Options dialog box.

Windows XP SP2 Pop-up Blocker

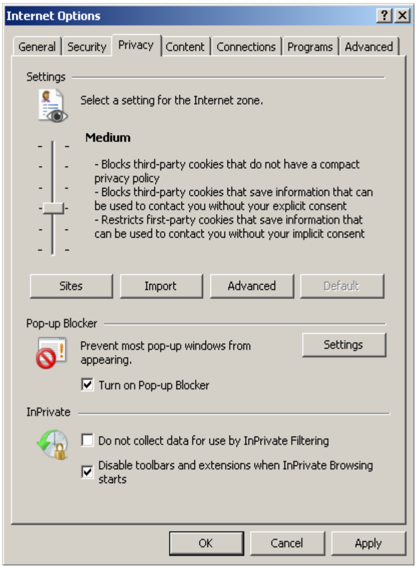
This sub-section provides information on setting up pop-up blocking and disabling pop-up blocking in Windows XP SP2.

Set up Pop-up Blocking

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

Use the Internet Options dialog box

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



Select a setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that save information that can be used to contact you without your explicit consent
- Restricts first-party cookies that save information that can be used to contact you without your implicit consent

Prevent most pop-up windows from appearing.

☑ Turn on Pop-up Blocker

☐ Do not collect data for use by InPrivate Filtering

☑ Disable toolbars and extensions when InPrivate Browsing starts

Fig. I-7 Enable pop-up blocking

3. In the Pop-up Blocker frame, check “Turn on Pop-up Blocker”.

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

Use the IE Toolbar

In the IE browser, go to the toolbar and select **Tools > Pop-up Blocker > Turn On Pop-up Blocker**:

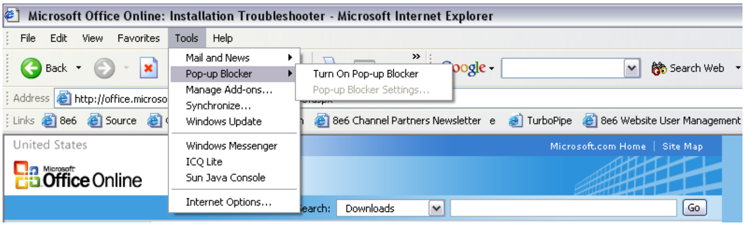


Fig. I-8 Toolbar setup

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.

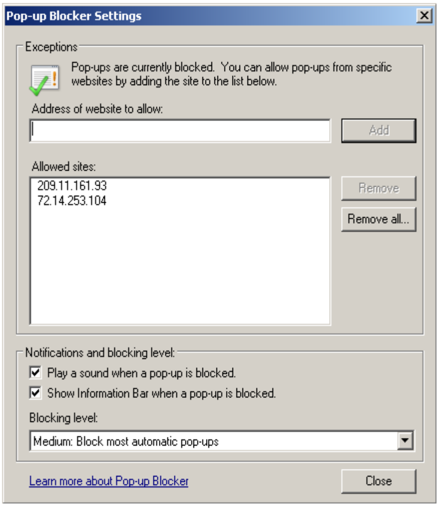
You can toggle between the On and Off settings to enable or disable pop-up blocking.

Add the Client to the White List

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

Use the IE Toolbar

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



Pop-up Blocker Settings

Exceptions

Pop-ups are currently blocked. You can allow pop-ups from specific websites by adding the site to the list below.

Address of website to allow:

Allowed sites:
209.11.161.93
72.14.253.104

Notifications and blocking level:

☑ Play a sound when a pop-up is blocked.

☑ Show Information Bar when a pop-up is blocked.

Blocking level:
Medium: Block most automatic pop-ups

Fig. I-9 Pop-up Blocker Settings

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

Use the Information Bar

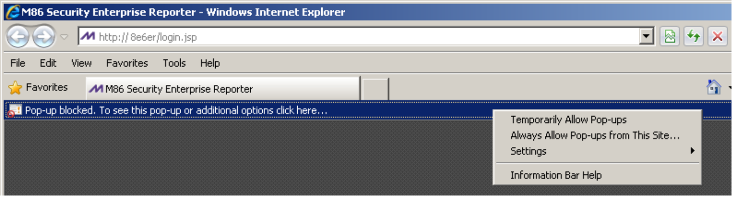
With pop-up blocking enabled, the Information Bar can be set up and used for viewing information about blocked pop-ups or allowing pop-ups from a specified site.

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. I-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 the Client

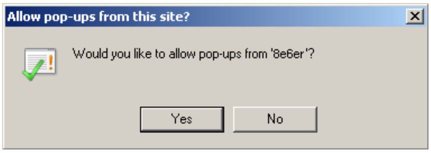
1. Click the Information Bar for settings options:


M86 Security Enterprise Reporter - Windows Internet Explorer
http://8e6er/login.jsp
File
Edit
View
Favorites
Tools
Help
Favorites
M86 Security Enterprise Reporter
Temporarily Allow Pop-ups
Always Allow Pop-ups from This Site...
Settings
Information Bar Help

Pop-up blocked. To see this pop-up or additional options click here...

Fig. I-10 Information Bar menu options

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



Would you like to allow pop-ups from '8e6er'?

Fig. I-11 Allow pop-ups dialog box

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

NOTE*: To view your white list, go to the Pop-up Blocker Settings dialog box (see Fig. I-9) and see the entries in the Allowed sites list box.*

Appendix II

RAID and Hardware Maintenance

This appendix is divided into three parts: Hardware Components, Server Interface, and Troubleshooting—in the event of a failure in one of the drives, power supplies, or fans.

***NOTE**: As part of the ongoing maintenance procedure for your RAID server, M86 recommends that you always have a spare drive and spare power supply on hand.*

Contact M86 Technical Support for replacement hard drives and power supplies.

Part 1: Hardware Components

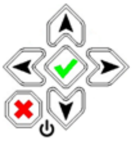
A 300 series model and 500 series model chassis consist of the following components:

300 Series Model	500 Series Model
2 hard drives	4 hard drives
1 power supply	1 power supply
1 cooling fan	3 cooling fans

Part 2: Server Interface

Front Control Panel on a 300 Series Unit

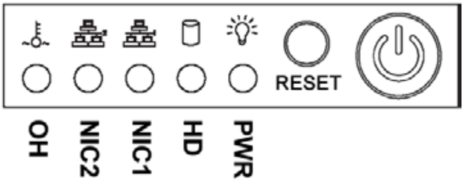
The keypad on the front of the server is used for performing basic server functions.



- **Boot up** - Depress and hold the check-mark key for 3 seconds.
- **Reboot** - Depress and hold the check-mark key for 10 seconds.
- **Shut down** - Depress and hold the ‘X’ key for 10 seconds.

Front control panel on the 500 series model

Control panel buttons, icons, and LED indicators display on the right side of the 500 series model front panel. The buttons let you perform a function on the unit, while an LED indicator corresponding to an icon alerts you to the status of that feature on the unit.



500 series model chassis front panel

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 a flashing amber LED in the control panel, and a flashing green LED on a drive carrier. An unlit LED on a drive carrier may indicate a hard drive failure. (See Hard drive failure in the Troubleshooting sub-section for information on detecting a hard drive failure and resolving this problem.)

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

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

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

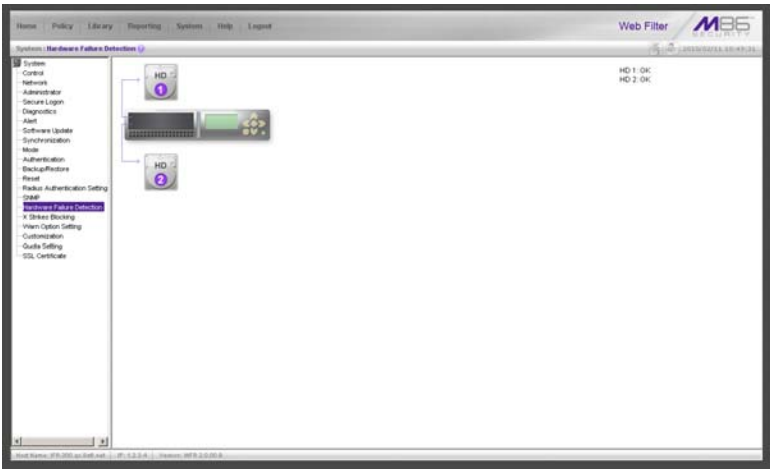
Step 1: Review the notification email

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 on a 300 series model, or HD 1 through HD 4 on a 500 series model). Upon receiving this alert, the administrator should verify the status of the drives by first going to the Hardware Failure Detection window in the Web Filter 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.*

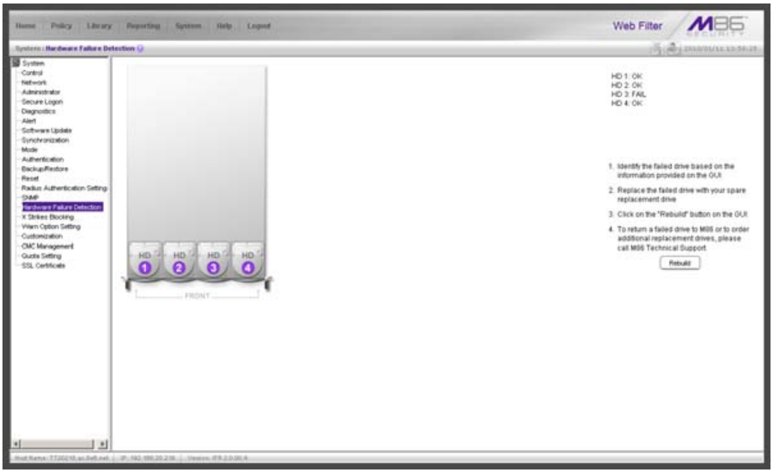
Step 2: Verify the failed drive in the Admin console

The Hardware Failure Detection window in the Web Filter Administrator console is accessible via the **System > Hardware Failure Detection** menu selection:



HD 1: OK
HD 2: OK

Fig. II-1 Hardware Failure Detection window on a 300 series model



HD 1: OK
HD 2: OK
HD 3: FAIL
HD 4: OK

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 M86 or to order additional replacement drives, please call M86 Technical Support

Fig. II-2 Hardware Failure Detection window on a 500 series model

The Hardware Failure Detection window displays the current RAID Array Status for all the hard drives (HD) at the right side of the window.

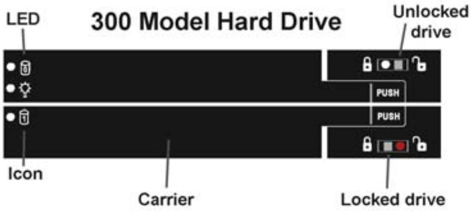
Normally, when all hard drives are functioning without failure, the text “OK” displays to the right of the hard drive number, and no other text displays in the window.

However, if a hard drive has failed, the message “FAIL” displays to the right of the hard drive number.

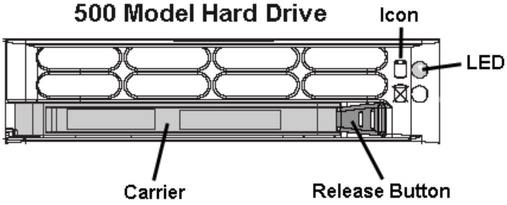
Before taking any action in this window, proceed to Step 3.

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.



300 series model hard drive carrier



500 series model hard drive carrier

On a 300 series model, be sure the carrier is unlocked, then press the section on the carrier handle labeled PUSH to release the carrier handle. On a 500 series model, press the red release button to release the carrier handle.

Extend the carrier handle fully by pulling it out towards you. Pull out the failed drive and replace it with your spare replacement drive. Push the drive into its slot, and press the carrier back in place.

NOTE*: Contact 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 M86.

Power supply failure

Step 1: Verify the power supply has failed

The administrator of the server is alerted to a power supply failure on the 500 series chassis by an audible alarm and an amber power supply LED—or an unlit LED—on the front of the chassis.

***NOTE**: A steady amber power supply LED on a 500 series chassis also may indicate a disconnected or loose power supply cord. Verify that the power supply cord is plugged in completely before removing a power supply.*

Step 2: Contact Technical Support

Contact Technical Support for assistance with installing the replacement power supply, or to order a new replacement power supply, or for instructions on returning your failed power supply to M86.

Fan failure

Identify a fan failure

A flashing red LED on a 500 series model 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 M86.

A steady red LED (on and not flashing) on a 500 series model indicates an overheating condition, which may be caused by cables obstructing the airflow in the system or the ambient room temperature being too warm. Check the routing of the cables and make sure all fans are present and operating normally. The LED will remain steady as long as the overheating condition exists.

INDEX