



M86 Security Reporter **USER GUIDE**

Software Version: 2.0.00
Document Version: 03.03.10

M86 SECURITY REPORTER USER GUIDE

© 2010 M86 Security
All rights reserved.

Version 1.01, published March 2010

Printed in the United States of America

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form without prior written consent from M86 Security.

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/sr/documentation.asp>

Trademarks

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

CONTENTS

| | |
|--|-----------|
| SR OVERVIEW | 1 |
| How to Use this User Guide | 2 |
| Organization | 2 |
| Conventions | 3 |
| Components and Environment | 4 |
| Components | 4 |
| Hardware | 4 |
| Software | 4 |
| Environment | 5 |
| Network Requirements | 5 |
| Administrator Workstation Requirements | 5 |
| End User Workstation Requirements | 6 |
| How to Use the SR on the Web | 7 |
| Initial Setup | 7 |
| Access the SR Welcome Window | 8 |
| Single Sign-On Access | 10 |
| Access all applications from the TAR UI | 10 |
| Default Usernames and Passwords | 10 |
| ENTERPRISE REPORTER OVERVIEW | 11 |
| Operations | 11 |
| About this Portion of the User Guide | 12 |
| Organization | 12 |
| Terminology | 13 |
| ER ADMINISTRATOR SECTION | 17 |
| Introduction | 17 |
| Chapter 1: Access the ER Admin Module | 18 |
| Procedures for Logging On, Off | 18 |
| Access the ER Administrator Login window | 18 |

| | |
|--|-----------|
| Access ER Admin Module from the SR Portal | 18 |
| Enter ER Admin Module's URL in Address field | 19 |
| Log On | 19 |
| Logging on the First Time | 21 |
| Set up an Administrator Login ID | 21 |
| Log Off | 22 |
| Chapter 2: Configuring the Server | 23 |
| Administrator Console | 23 |
| Network Menu | 23 |
| Box Mode screen | 24 |
| Live Mode | 25 |
| Archive Mode | 25 |
| Change the Box Mode | 25 |
| Add/Edit/Delete Administrators screen | 27 |
| View a List of Administrators | 28 |
| Add an Administrator | 28 |
| Edit an Administrator's Login ID | 28 |
| Delete an Administrator | 29 |
| Locked-out Accounts and IPs screen | 30 |
| View Locked Accounts, IP addresses | 31 |
| Unlock Accounts, IP addresses | 31 |
| Network Settings screen | 32 |
| Set up/Edit IP Addresses | 33 |
| Routing Table screen | 34 |
| View a List of Routers | 34 |
| Add a Router | 35 |
| Delete a Router | 35 |
| Regional Setting screen | 36 |
| Specify the Time Zone | 37 |
| Specify the Language Set | 37 |
| Specify Network Time Protocol Servers | 37 |
| Update the Time on the Server | 38 |
| Network Diagnostics screen | 39 |
| Ping | 40 |
| Trace Route | 41 |
| SNMP screen | 43 |
| Enable SNMP | 44 |
| Set up Community Token for Public Access | 44 |
| Create, Build the Access Control List | 44 |
| Maintain the Access Control List | 44 |

| | |
|--|----|
| Server Menu | 45 |
| Backup screen | 45 |
| Backup and Recovery Procedures | 46 |
| Set up/Edit External Backup FTP Password | 48 |
| Execute a Manual Backup | 48 |
| Perform a Remote Backup | 49 |
| Perform a Restoration to the ER Server Module | 50 |
| Self Monitoring screen | 51 |
| View a List of Contact E-Mail Addresses..... | 52 |
| Set up and Activate Self-Monitoring | 52 |
| Remove Recipient from E-mail Notification List..... | 52 |
| Deactivate Self-Monitoring..... | 52 |
| SMTP Server Setting screen | 53 |
| Enter, Edit SMTP Server Settings | 53 |
| Verify SMTP Settings..... | 54 |
| Server Status screen..... | 55 |
| View the Status of the ER Server | 56 |
| Secure Access screen | 57 |
| Activate a Port to Access the ER Server | 57 |
| Terminate a Port Connection..... | 58 |
| Terminate All Port Connections | 58 |
| Software Update screen | 59 |
| View Installed Software Updates..... | 60 |
| Uninstall the Most Recently Applied Software Update .. | 60 |
| View Available Software Updates..... | 60 |
| Install a Software Update..... | 60 |
| Software Update Setting screen | 64 |
| Specify Proxy Settings..... | 65 |
| Save Settings..... | 65 |
| Shut Down screen | 66 |
| Server Action Selections..... | 66 |
| Perform a Server Action | 67 |
| Web Client Server Management screen | 68 |
| Restart the Web Client Server | 68 |
| Enable/Disable the Web Client Scheduler..... | 69 |
| Hardware Failure Detection screen | 70 |
| View the Status of the Hard Drives..... | 71 |
| Database Menu | 73 |
| User Name Identification screen | 73 |
| View the User Name Identification screen..... | 76 |
| Configure the Server to Log User Activity..... | 76 |

- Deactivate User Name Identification 77
- Username Display Setting screen 78
 - View the Current Username Display Setting 79
 - Modify the Username Display Setting..... 79
- Page View Elapsed Time screen 81
 - Establish the Unit of Elapsed Time for Page Views..... 81
 - Elapsed Time Rules..... 82
- Page Definition screen 83
 - View the Current Page Types 83
 - Remove a Page Type 84
 - Add a Page Type 84
- Tools screen 85
 - View Diagnostic Reports..... 86
 - View Database Status Logs..... 86
- Expiration screen 89
 - Expiration Screen Terminology..... 90
 - Expiration Rules..... 91
 - View Data Storage Statistics 92
 - Change Data Storage Settings 95
- Optional Features screen 96
 - Enable Search String Reporting 98
 - Enable Block Request Count..... 98
 - Enable Blocked Searched Keywords..... 98
 - Enable Wall Clock Time..... 99
 - Enable Page and/or Object Count..... 99
 - Enable, Configure Password Security Option..... 100
- User Group Import screen 103
 - Import User Groups 104

ER SERVER APPENDIX SECTION 105

- Appendix A 105**
 - Evaluation Mode 105
 - Administrator Console 106
 - Use the Server in the Evaluation Mode 107
 - Expiration screen 107
 - Change the Evaluation Mode 109
 - Activation Page..... 109

WEB CLIENT INTRODUCTORY SECTION 1

| | |
|--|-----------|
| Enterprise Reporter | 1 |
| Operations | 1 |
| About this Portion of the User Guide | 2 |
| Terminology | 3 |
| Getting Started | 7 |
| Procedures for Logging On, Off | 8 |
| Access the ER Web Client Login window | 8 |
| Access ER Web Client from the SR Portal | 8 |
| Enter ER Web Client's URL in Address field..... | 9 |
| Log In | 10 |
| Client Screen Navigation | 14 |
| Links in the Navigation Toolbar..... | 14 |
| Using the Client | 15 |
| Log Out | 15 |
| Re-login | 16 |
| WEB CLIENT ADMINISTRATOR SECTION | 17 |
| Introduction | 17 |
| Chapter 1: Installation and Maintenance | 18 |
| Environment Requirements | 18 |
| Client Updates | 19 |
| Chapter 2: Configuring the Client | 20 |
| Settings | 20 |
| Category Descriptions | 21 |
| View Details for a Filter Category | 22 |
| Category Groupings | 23 |
| Group Information frame | 24 |
| Add a Category Group..... | 24 |
| Rename a Category Group..... | 24 |
| Delete a Category Group..... | 25 |
| Group Definitions frame | 26 |
| Add Categories to a Category Group | 26 |
| Delete a Category from a Category Group..... | 27 |
| User Groupings | 28 |
| Group Definitions frame | 29 |

- View a List of Users in a User Group..... 29
- Define a User Group..... 31
- Disable a User Group 33
- Delete User(s) from User Group..... 34
- Group Information frame 35
 - Add a User Group..... 35
 - Rename a User Group..... 35
 - Copy a User Group..... 36
 - Delete a User Group..... 36
- User and Group Permissions 37
 - Add User 38
 - Sub-Admin Information frame 40
 - Add User Group to a Sub-Admin 40
 - Remove User Group from a Sub-Admin 40
 - Group Information frame 41
 - Update User Group by Adding a Sub-Admin..... 41
 - Update User Group by Removing a Sub-Admin..... 41
 - Edit Password, Change Permissions, Delete User 42
 - Change a User’s Password 42
- Database Process List 43
 - View Details on a Process 43
 - Terminate a Process 44

WEB CLIENT USER SECTION 45

Introduction 45

Chapter 1: Installation Requirements 46

Chapter 2: Customizing the Client 47

- Settings 47
 - My Account 48
 - View Users in a User Group..... 48
 - Change Password..... 49
 - ER Server Information 50
 - Date Scopes 51
 - Web Client Server Startup Time 51
 - Server Info..... 51
 - ER Activity 52
 - Expiration Info 55
 - Default Options 56

| | |
|---|-----------|
| Set New Defaults | 56 |
| Chapter 3: Executive Reports | 58 |
| Generate an Executive Report | 60 |
| Executive Report in the PDF format | 61 |
| Executive Report in the CSV format | 64 |
| Executive Report in the PNG format | 65 |
| Export an Executive Report | 66 |
| Chapter 4: Summary and Detail Reports | 67 |
| Summary Drill Down Report View | 68 |
| Detail Drill Down Report View | 69 |
| Report View Tools and Usage Tips | 71 |
| Navigation Tips | 71 |
| Back button | 71 |
| Record navigation field..... | 71 |
| Summary Report View Tools and Tips | 72 |
| Filter columns and buttons | 72 |
| Count columns and column arrows | 73 |
| Column sorting tips | 75 |
| Record exportation | 76 |
| Detail Report View Tools and Tips | 77 |
| Page link navigation | 77 |
| Report Type columns | 77 |
| Column sorting tips | 79 |
| Page/Object viewing tip..... | 79 |
| Truncated data viewing tip | 79 |
| Using escape characters in an NT domain query | 80 |
| Header Buttons for Customization Options | 81 |
| New Report button | 81 |
| Set Result Limit button | 82 |
| Modify Report button | 83 |
| Drill Down Report option..... | 83 |
| Detail Custom Report option..... | 83 |
| Export Report button | 84 |
| Export Drill Down Report option | 84 |
| Export Custom Report option | 85 |
| Save Report button | 86 |
| Summary Drill Down Report option | 86 |
| Detail Drill Down Report option..... | 87 |
| Report View Components | 88 |

| | |
|---|------------|
| Report Fields and Usage | 88 |
| Type field..... | 88 |
| Date Scope and Date fields | 89 |
| Display and # Records fields..... | 91 |
| Search and Filter String fields..... | 91 |
| Sort by and Order fields | 92 |
| Result Set Limit fields..... | 92 |
| Break type field | 93 |
| Format field | 93 |
| Data to export field | 93 |
| For double-break reports only | 94 |
| Amount shown field | 94 |
| # Records field..... | 94 |
| For pie and bar charts only | 95 |
| Generate using field..... | 95 |
| Output type field | 95 |
| Hide Un-Identified IPs checkbox..... | 95 |
| For E-Mail output only / Email Report fields..... | 96 |
| Detailed Info field | 96 |
| Exporting a Report | 98 |
| View and Print Options | 101 |
| View and Print Tools | 101 |
| Sample Report File Formats | 102 |
| MS-DOS Text | 103 |
| PDF | 104 |
| Rich Text Format | 105 |
| HTML | 106 |
| Comma-Delimited Text | 107 |
| Excel (English) | 108 |
| Chapter 5: Drill Down Reports | 109 |
| Generate a Drill Down Report | 110 |
| Generate a Single User Group Report | 111 |
| Chapter 6: Custom Reports | 112 |
| Custom Report Wizard | 114 |
| Step 1: Specify Report Option | 115 |
| Step 2: Specify Report Selection | 117 |
| Summary report | 117 |
| Detail report..... | 117 |
| Batch user report..... | 117 |

| | |
|---|-----|
| URL sub-string, keyword report | 118 |
| Step 3: Specify Date Scope | 119 |
| Step 4: Specify Order Criteria | 119 |
| Summary report | 119 |
| Detail report..... | 119 |
| Step 5: Specify when to Generate the Report | 119 |
| Save Custom Report | 121 |
| Wizard Reporting Tips | 124 |
| Detail page Break report by Users, Category | 124 |
| Use wildcards in a Specific Search query | 124 |
| Sample Custom Reports | 126 |
| Report Format | 127 |
| Top 20 Categories by Page Count | 128 |
| Top 20 IPs by Category/IP | 129 |
| Top 20 Users by Category/User | 130 |
| Top 20 Users by Page Count | 131 |
| Top 20 Categories by User/Category | 132 |
| Top 20 Sites by User/Site | 133 |
| By User/Category/Site | 134 |
| Top 20 Sites by Category/Site | 135 |
| By Category/Site/IP | 136 |
| By Category/User/Site | 137 |
| Wall Clock Time Report | 138 |
| Generate a Wall Clock Time Report | 139 |
| View the Wall Clock Time Report | 142 |
| Wall Clock Time algorithm | 143 |
| Use wildcards in a Specific Search query | 144 |
| Blocked Request Report | 145 |
| Generate a Blocked Request Report | 145 |
| View the Blocked Request Report | 148 |
| Saved Custom Reports | 149 |
| View Information in a Saved Custom Report | 150 |
| Edit a Custom Report | 151 |
| Add a Username | 153 |
| Copy a Custom Report | 154 |
| Run a Custom Report | 154 |
| Delete a Custom Report | 155 |
| Event Schedules | 156 |
| View Details or Edit a Scheduled Event | 157 |
| View Details for a Scheduled Event | 158 |
| Edit a Scheduled Event..... | 158 |

- Add an Event to the Schedule 159
- Delete a Scheduled Event 160
- Scheduling a Report to Run 161
- Executive Internet Usage Summary 162
 - Specify category groups for the report 163
 - Add category groups to the Selected list box..... 163
 - Remove category groups from the Selected list box..... 163
 - Hide Unidentified IP addresses 164
 - Specify E-Mail Subject 164
 - Specify how the report will be accessed 164
 - Maintain a list of users to receive reports 165
 - Save your settings 165
 - Sample Executive Internet Usage report 166

WEB CLIENT APPENDICES SECTION 173

Appendix A 173

- Evaluation Mode 173
 - Client 174
 - Evaluation Mode alert box..... 174
 - ER Server Information window 175

Appendix B 176

- Lotus Notes Configuration 176
 - Steps for Former MS Outlook / Express Users 176
 - Steps for Installing, Configuring Lotus Notes 177
 - Step 1: Install Lotus Notes 177
 - Step 2: Configure Microsoft Mail Client..... 177
 - Step 3: Verify Internet Explorer Settings 177

Appendix C 178

- Glossary 178

TAR INTRODUCTORY SECTION 179

Threat Analysis Reporter 179

About this Portion of the User Guide 180

- Terminology 181

Getting Started 185

| | |
|--|------------|
| Procedures for Logging On, Off | 185 |
| Access the TAR Administrator Login window | 185 |
| Access TAR Administrator Console from SR Portal | 185 |
| Enter TAR's URL in the Address field | 186 |
| Log in | 186 |
| Navigation toolbar menu links and topics | 188 |
| Exit the user interface | 188 |
| Navigation Tips and Conventions | 189 |
| TAR PRELIMINARY SETUP SECTION | 191 |
| Introduction | 191 |
| Chapter 1: User Groups Setup | 192 |
| View User Group Information | 194 |
| User group status key | 194 |
| View a list of members in a user group | 194 |
| Add a User Group | 196 |
| Patterns frame | 197 |
| Add a new pattern | 197 |
| View users resolved by the pattern | 198 |
| Remove a pattern..... | 198 |
| IP Ranges frame | 199 |
| Specify an IP range | 200 |
| Remove an IP address range | 201 |
| Single Users frame | 202 |
| Add one or more individual users | 203 |
| Use the filter to narrow Available Users results | 203 |
| Select users to add to the Assigned Users list | 203 |
| Remove users from the Add tab | 204 |
| Edit a User Group | 205 |
| Rebuild the User Group | 206 |
| Delete a User Group | 206 |
| Chapter 2: Admin Groups Setup | 207 |
| Add a Group | 208 |
| View, Edit an Admin Group's Permissions | 210 |
| View Admin Group settings | 210 |
| Edit Admin Group settings | 211 |
| Delete an Administrator Group | 211 |

- Add an Administrator Profile 213
- View, Edit Admin Detail 216
 - View Admin Details 216
 - Edit Account Info 217
- Delete Admin 218

TAR CONFIGURATION SECTION 219

Introduction 219

Chapter 1: Gauge Components 220

- Types of Gauges 220
- Anatomy of a Gauge 221
- How to Read a Gauge 222
- Bandwidth Gauge Components 223
- Gauge Usage Shortcuts 225

Chapter 2: Custom Gauge Setup, Usage 227

- Add a Gauge 229
 - Specify Gauge Information 230
 - Define Gauge Components 231
 - Assign user groups 232
 - Save gauge settings 233
- Modify a Gauge 234
 - Edit gauge settings 234
- Hide, Disable, Delete, Rearrange Gauges 236
 - Hide a gauge 238
 - Disable a gauge 238
 - Show a gauge 238
 - Rearrange the gauge display in the dashboard 238
 - Delete a gauge 239
- View End User Gauge Activity 240
 - View Overall Ranking 240
 - View a Gauge Ranking table 242
- Monitor, Restrict End User Activity 244
 - View User Summary data 244
 - Access the Threat View User panel 246
 - URL Gauges tab selection 246
 - Bandwidth Gauges tab selection..... 247
 - Manually lock out an end user 248
 - Low severity lockout..... 249

| | |
|---|------------|
| Medium and High severity lockout | 250 |
| End user workstation lockout | 250 |
| Low severity URL lockout | 250 |
| Medium severity URL and bandwidth lockout..... | 251 |
| Low/high bandwidth, high severity URL lockout | 252 |
| Chapter 3: Alerts, Lockout Management | 253 |
| Add an Alert | 255 |
| Email alert function | 256 |
| Configure email alerts | 256 |
| Receive email alerts..... | 257 |
| System Tray alert function | 257 |
| Lockout function | 258 |
| View, Modify, Delete an Alert | 259 |
| View alert settings | 260 |
| Modify an alert | 261 |
| Delete an alert | 262 |
| View the Alert Log | 263 |
| Manage the Lockout List | 265 |
| View a specified time period of lockouts | 266 |
| Unlock workstations | 267 |
| Access User Summary details | 267 |
| Chapter 4: Analyze Usage Trends | 268 |
| View Trend Charts | 269 |
| View activity for an individual gauge | 269 |
| View overall gauge activity | 271 |
| Navigate a trend chart | 272 |
| View gauge activity for a different time period | 273 |
| Analyze gauge activity in a pie chart | 274 |
| Analyze gauge activity in a line chart | 275 |
| View In/Outbound bandwidth gauge activity | 277 |
| Print a trend chart from an IE browser window | 277 |
| Access Web Filter, ER Applications | 278 |
| Access the Web Filter | 278 |
| Access the ER Web Client application | 278 |
| Access the ER Administrator console | 278 |
| Chapter 5: Identify Users, Threats | 279 |
| Perform a Custom Search | 279 |
| Specify Search Criteria | 280 |

| | |
|--|------------|
| View URLs within the accessed category | 282 |
| TAR ADMINISTRATION SECTION | 283 |
| Introduction | 283 |
| Chapter 1: View the User Profiles List | 284 |
| Search the User Database | 285 |
| View End User Activity | 286 |
| Chapter 2: View Administrator Activity | 287 |
| Perform a Search on a Specified Activity | 288 |
| Search results | 290 |
| Chapter 3: Maintain the Device Registry | 291 |
| Generate SSL Certificate | 292 |
| Generate an SSL Certificate for the SR | 292 |
| Web Filter Device Maintenance | 293 |
| View, edit Web Filter device criteria | 293 |
| Add a Web Filter to the device registry | 294 |
| Delete a Web Filter from the device registry | 295 |
| Threat Analysis Reporter Maintenance | 296 |
| View TAR device criteria | 296 |
| Add, remove a bandwidth range | 297 |
| View Other Device Criteria | 298 |
| View SMTP device criteria | 298 |
| View Patch Server device criteria | 299 |
| View NTP Server device criteria | 299 |
| View Proxy Server device criteria | 299 |
| Sync All Devices | 300 |
| Chapter 4: Perform Backup, Restoration | 301 |
| Execute a Backup on Demand | 303 |
| Restore User Settings | 304 |
| Restore to Factory Default Settings | 305 |
| Reset to Factory Default Settings frame | 305 |
| Wizard Login window | 307 |
| TAR APPENDICES SECTION | 309 |
| Appendix A | 309 |

| | |
|---|------------|
| System Tray Alerts: Setup, Usage | 309 |
| LDAP server configuration | 309 |
| Create the System Tray logon script..... | 309 |
| Assign System Tray logon script to administrators | 313 |
| Administrator usage of System Tray | 315 |
| Use the TAR Alert icon's menu | 315 |
| Status of the TAR Alert icon..... | 316 |
| View System Tray alert messages..... | 317 |
| Appendix B | 318 |
| Glossary | 318 |
| | |
| SR TECHNICAL SUPPORT / PRODUCT WARRANTIES | 321 |
| | |
| Technical Support | 321 |
| Hours | 321 |
| Contact Information | 321 |
| Domestic (United States) | 321 |
| International | 321 |
| E-Mail | 321 |
| Office Locations and Phone Numbers | 322 |
| M86 Corporate Headquarters (USA)..... | 322 |
| M86 Taiwan..... | 322 |
| Support Procedures | 323 |
| | |
| Product Warranties | 324 |
| Standard Warranty | 324 |
| Technical Support and Service | 325 |
| Extended Warranty (optional) | 326 |
| Extended Technical Support and Service | 326 |
| | |
| SR APPENDICES SECTION | 327 |
| | |
| Appendix I | 327 |
| Disable Pop-up Blocking Software | 327 |
| Yahoo! Toolbar Pop-up Blocker | 327 |
| Add the Client to the White List | 327 |
| Google Toolbar Pop-up Blocker | 329 |
| Add the Client to the White List | 329 |
| AdwareSafe Pop-up Blocker | 330 |
| Disable Pop-up Blocking | 330 |

| | |
|--|------------|
| Mozilla Firefox Pop-up Blocker | 331 |
| Add the Client to the White List | 331 |
| Windows XP SP2 Pop-up Blocker | 333 |
| Set up Pop-up Blocking | 333 |
| Use the Internet Options dialog box..... | 333 |
| Use the IE Toolbar | 334 |
| Add the Client to the White List | 335 |
| Use the IE Toolbar | 335 |
| Use the Information Bar | 335 |
| Set up the Information Bar..... | 336 |
| Access the Client..... | 336 |
| Appendix II | 337 |
| RAID and Hardware Maintenance | 337 |
| Part 1: Hardware Components | 337 |
| Part 2: Server Interface | 338 |
| Front Control Panel on a 300 Series Unit | 338 |
| Front control panels on 500 and 700 series units | 338 |
| Rear panel on the 700 series unit | 340 |
| Part 3: Troubleshooting | 341 |
| Hard drive failure..... | 341 |
| Step 1: Review the notification email..... | 341 |
| Step 2: Verify the failed drive in the Admin console ... | 341 |
| Step 3: Replace the failed hard drive..... | 343 |
| Step 4: Rebuild the hard drive | 344 |
| Step 5: Contact Technical Support..... | 344 |
| Power supply failure..... | 344 |
| Step 1: Verify the power supply has failed..... | 344 |
| Step 2: Contact Technical Support..... | 344 |
| Step 3: Unplug the power cord | 345 |
| Step 4: Replace a failed hot swap power supply | 345 |
| Fan failure | 346 |
| Identify a fan failure | 346 |
| INDEX | 347 |

SR OVERVIEW

The Security Reporter (SR) from M86 Security consists of the best in breed of the M86 Professional Edition reporting software, consolidated into one unit.

M86's Threat Analysis Reporter (TAR) provides administrators or management personnel dynamic, real time graphical snapshots of network Internet traffic, supported by remediation tools to manage and control user-generated Web threats. Working in conjunction with M86's Web Filter that tracks users' online activity, TAR interprets end user Internet activity from the Web Filter's logs and supplies data that can be viewed via an easy-to-read dashboard of gauges the administrator can drill down into, thereby identifying the source of the threat.

Data from the Web Filter is fed into M86 Security's Enterprise Reporter (ER), 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.

Using the SR, threats to your network are quickly identified, thus arming you with the capability to take immediate action to halt the source, secure your network, and protect your organization against lost productivity, network bandwidth issues, and possible legal problems that can result from the misuse of Internet resources.

How to Use this User Guide

Organization

This User Guide is organized into the following sections:

- **SR Overview** - This section introduces the SR product and explains how to use the SR console and this user guide.
- **ER Administrator Section** - Refer to this section for information on configuring and maintaining the ER Administration module via the ER Administrator console.
- **ER Web Client Section** - Refer to this section for information on configuring and maintaining the ER Web Client application.
- **TAR Section** - Refer to this section for information on configuring and maintaining the Threat Analysis Reporter application.
- **SR Technical Support/Product Warranties Section** - This section includes information about how to contact M86 Security technical support for assistance, and what is covered in your warranty for the SR unit.
- **SR Appendices** - Appendix I of this section explains how to disable pop-up blocking software. Appendix II provides information on how to perform hardware maintenance and troubleshoot RAID on the SR chassis.
- **Index Section** - This section includes an index of 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 SR 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 Graphical User Interface (GUI) console utilized by an authorized administrator to configure and maintain the SR server
- MySQL database

Environment

Network Requirements

- Power connection protected by an Uninterruptible Power Supply (UPS)
- HTTPS connection to M86 Security's software update server
- High speed access to the SR server by authorized client workstations

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 3.5
- Macintosh OS X Version 10.5 or 10.6 running:
 - Safari 4.0
 - Firefox 3.5
- JavaScript enabled
- Pop-up blocking software, if installed, must be disabled
- Session cookies from the SR 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 SR 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 3.5
- Macintosh OS X Version 10.5 or 10.6 running:
 - Safari 4.0
 - Firefox 3.5
- JavaScript enabled
- Pop-up blocking software, if installed, must be disabled

How to Use the SR on the Web

Initial Setup

To initially set up your M86 Security Reporter (SR) server, the administrator installing the unit should follow the instructions in the M86 Security Reporter Installation Guide, the booklet packaged with your SR 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 Security Reporter 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 SR server is running, the server should be connected to a UPS or other battery backup system. Once you turn on the SR 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 SR Welcome Window

After the SR 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 TAR wizard hardware installation procedures.

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 server’s IP address or host name, and use port number “:8443” for a secure network connection.

For example, if your IP address is 210.10.131.34, type in **https://210.10.131.34:8443**. Using a host name example, if the host name is logo.com, type in **https://logo.com:8443**.

With a secure connection, the first time you attempt to access the SR’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-sr.pdf>***

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



Fig. 1:1-1 SR Welcome window

Using this portal you can click any of the icons (ER Reporter, ER Reporter Administration Module, or Threat Analysis Reporter) to access the user interface of the corresponding application (ER Web Client, ER Administrator, or TAR) as described in the following sections of this user guide.

However, by logging into the TAR application as the global administrator—as described on the next page—you will have access to all applications on the SR server without needing to use the SR Welcome portal to log into each application.

Single Sign-On Access

Access all applications from the TAR UI

By logging in to the Threat Analysis Reporter using the TAR Wizard username and password set up during the installation process, the ER Web Client and ER Administrator console are accessible to the global administrator user account via the TAR user interface. This single sign-on access eliminates the process of choosing each application from the SR Welcome window and then logging in to each one separately.

To use the single sign-on option:

1. Log in to TAR using the TAR Wizard username and password.
2. Go to the navigation links at the top of the screen and select:
 - **Report/Analysis > Enterprise Reporter > Web Client** to access the Web Client user interface
 - **Report/Analysis > Enterprise Reporter > Admin GUI** to access the ER Administrator console

Default Usernames and Passwords

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

| Application | Username | Password |
|--------------------------|----------|-----------|
| ER Web Client | manager | 8e6ReporT |
| ER Administration Module | admin | reporter |
| Threat Analysis Reporter | admin | testpass |

ENTERPRISE REPORTER OVERVIEW

Though many companies have Internet filtering solutions to prevent employees from accessing inappropriate, non-work related Web sites, simply blocking these sites is not enough. Administrators want the ability to know who is accessing which site, the duration of each site visit, and the frequency of these visits. This data can help administrators identify abusers, develop policies, and target sites to be filtered, in order to maximize bandwidth utilization and productivity.

The Enterprise Reporter (ER) from M86 Security is designed to readily obtain this information, giving the user 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.

Operations

In simplified terms, the ER operates as follows: the ER Server module accepts log files (text files containing Web access data) from a source device such as the M86 Web Filter. M86 Security’s proprietary programs “normalize” the transferred data and insert them into a MySQL database. The ER Web Client reporting application accesses this database to generate a virtually unlimited number of queries and reports.

About this Portion of the User Guide

Organization

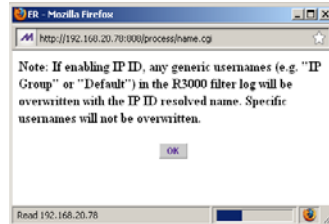
The Enterprise Reporter Administrator Console portion of the user guide is organized into the following sections:

- **Enterprise Reporter Overview** - This section provides information on how to use this portion of the user guide to help you configure the ER Server module.
- **ER Administrator Section** - Refer to this section for information on configuring and maintaining the ER Server module via the Administrator console.
- **ER Server Appendix Section** - Appendix A provides information on how to use the ER in the evaluation mode, and how to switch to the activated mode.

Terminology

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

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



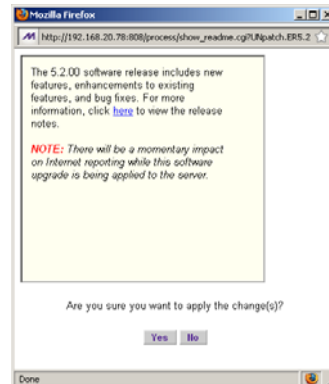
- **button** - an object in a dialog box, window, or screen that can be clicked with your mouse to execute a command.



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



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



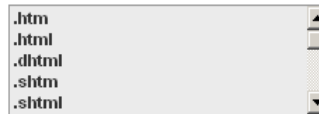
- **field** - an area in a dialog box, window, or screen that either accommodates your data entry, or displays pertinent information. A text box is a type of field.



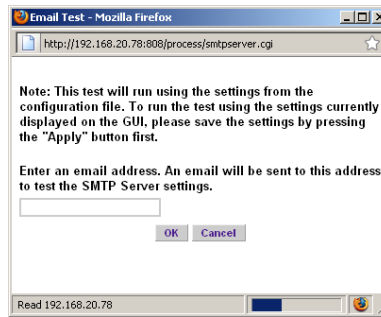
- **frame** - a boxed-in area in a dialog box, window, or screen that includes a group of objects such as fields, text boxes, list boxes, buttons, radio buttons, and/or tables. Objects within a frame belong to a specific function or group. A frame often is labeled to indicate its function or purpose.



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



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



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



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



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



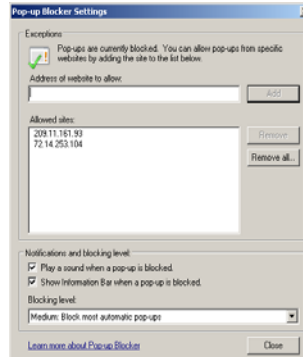
- **table** - an area in a window or screen that contains items previously entered or selected.

| Destination | Gateway | Delete |
|-------------|---------|--------------------------|
| 1.1.1.1/1 | 1.1.1.1 | <input type="checkbox"/> |
| 1.2.3.4/1 | 1.3.2.4 | <input type="checkbox"/> |

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

Activation Code:

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



ER ADMINISTRATOR SECTION

Introduction

The authorized administrator of the ER Server application is responsible for configuring and maintaining the SR server—which includes the ER and Threat Analysis Reporter modules. To attain this objective, the administrator performs the following tasks:

- executes Installation procedures defined in the Installation Guide booklet packaged with the SR server
- provides a suitable environment for the server, including:
 - high speed, HTTPS link to the current logging device
 - power connection protected by an Uninterruptible Power Supply (UPS)
 - high speed access to the server by authorized ER Web Client workstations
- adds new administrators
- sets up administrators for receiving automatic alerts
- updates the server with software updates supplied by M86 Security
- analyzes server statistics
- utilizes diagnostics for monitoring the server status to ensure optimum functioning of the server
- establishes and implements backup and restoration procedures for the server

Instructions on configuring and maintaining the server are documented in this section.



NOTE: Click the **Help** link beneath the banner in any screen of the ER Administrator console to access a page with links to .pdf files of the latest user guides (in the .pdf format) for this product.

Chapter 1: Access the ER Admin Module

Procedures for Logging On, Off

Access the ER Administrator Login window

The ER Administrator user interface is accessible in one of two ways:

- by clicking the ER Administrator Module icon in the SR Welcome window (see Access ER Admin Module from the SR Portal)
- by launching an Internet browser window supported by the ER Administrator Module and then entering the ER Administrator Module's URL in the Address field (see Enter ER Admin Module's URL in Address field)

Access ER Admin Module from the SR Portal

Click the ER Administrator Module icon in the SR Welcome window:



Fig. 1:1-1 ER Administration Module icon in SR 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 SR Appendix I: Disable Pop-up Blocking Software.

Clicking the ER Administration Module icon launches a separate browser window/tab containing the ER Administrator console Login window (see Fig. 1:1-2).

Enter ER Admin Module's URL in Address field

1. Launch an Internet browser window supported by the ER Administrator Module.
2. In the address line of the browser window, type in "https://" and the ER Administrator Module's IP address or host name, and use port number ":8843" for a secure network connection.

For example, if your IP address is 210.10.131.34, type in **https://210.10.131.34:8843**. Using a host name example, if the host name is logo.com, type in **https://logo.com:8843**.

With a secure connection, the first time you attempt to access the ER Administrator Module'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-sr.pdf>**

3. After accepting the security certificate, click **Go** to open the ER Administrator Login window (see Fig. 1:1-2).

Log On

1. In the Login window, type in the generic Username **admin**, and Password **reporter**, if you have not yet set up your own user name and password. Otherwise, enter your personal **Username** and **Password**:



Fig. 1:1-2 Login window

2. Click **Login** to go to the default Server Status screen in the ER Administrator console:

Product Version:
Current Version: Security Reporter 2.0.00.3

Server Status

CPU Utilization

CPU Load Averages: 0.00, 0.00, 0.00
 CPU states: 0.5%us, 1.9%sy, 0.0%ni, 95.8%id, 1.7%wa, 0.0%hi, 0.1%si, 0.0%st
 Memory: 2055832k total, 1990232k used, 65600k free, 300k buffers
 Swap: 2097144k total, 170488k used, 1926656k free, 1760096k cached

| PID | USER | PR | NI | VIRT | RES | SHR | S | %CPU | %MEM | TIME+ | COMMAND |
|-------|------|----|----|-------|------|------|---|------|------|---------|-------------|
| 3160 | dbus | 20 | 0 | 21268 | 452 | 448 | S | 0.0 | 0.0 | 0:00.00 | dbus-daemon |
| 19016 | root | 20 | 0 | 7184 | 1320 | 1204 | S | 0.0 | 0.1 | 0:00.29 | dbcontrol |

Disk drives status

| Filesystem | 1k-blocks | Used | Available | Use% | Mounted on |
|-----------------------------|-----------|-----------|-----------|----------------|------------|
| /dev/mapper/V900-rootlv | | | | | |
| 28297728 | 4782900 | 23514628 | 17% | / | /boot |
| /dev/md0 | 108765 | 55690 | 47466 | 54% | /boot |
| tmpfs | 1027916 | 0 | 1027916 | 0% | /dev/shm |
| /dev/mapper/V900-8e6lv | | | | | |
| 36682240 | 1142748 | 35539492 | 4% | /usr/local/8e6 | |
| /dev/mapper/V900-backuplv | | | | | |
| 136248320 | 7688 | 136240632 | 1% | /backup | |
| /dev/mapper/V900-recoverylv | | | | | |
| 2064208 | 977184 | 982188 | 50% | /recovery | |
| /dev/mapper/V900-dblv1 | | | | | |
| 253631488 | 35133788 | 218497700 | 14% | /database/d1 | |

NETSTAT

| Proto | Recv-Q | Send-Q | Local Address | Foreign Address | State | PID/Program Name |
|-------|--------|--------|-----------------------------|---------------------------|-------------|------------------|
| tcp | 0 | 0 | R3000T64.qc.opression-proxy | R3000T64.qc.8e6.net:54224 | ESTABLISHED | 3374/mysqld |
| tcp | 0 | 0 | R3000T64.qc.opression-proxy | R3000T64.qc.8e6.net:54223 | ESTABLISHED | 3374/mysqld |

Fig. 1:1-3 Server Status screen

The Server Status screen displays the current status of the SR server.



NOTES: See *Server Status* screen in the *Server* section of this document for information about the contents and usage of this screen.

If using this product in the *Evaluation Mode* the *ER Status* pop-up window opens after logging into this application. Please see *Appendix A: Evaluation Mode* for information about the *Evaluation Mode*.

Logging on the First Time

Set up an Administrator Login ID



NOTE: If you have already set up your user name and password, you can skip this section.

1. At the *Network* pull-down menu, choose **Administrators** to display the *Add/Edit/Delete Administrators* screen where you set up your user name and password:

The screenshot displays the 'Add/Edit/Delete Administrators' screen within the Enterprise Reporter application. The interface includes a top navigation bar with the 'Enterprise Reporter' title and 'M86 SECURITY' logo. Below the navigation bar are dropdown menus for 'Network', 'Server', and 'Database', along with a 'Help Logout' link. The main content area features a form titled 'Add/Edit/Delete Administrators' with a 'New Administrator' dropdown menu. The form contains three input fields: 'User Name' (containing 'admin'), 'Password' (masked with dots), and 'Confirm Password'. At the bottom of the form are 'Save' and 'Delete' buttons.

Fig. 1:1-4 Add/Edit/Delete Administrators screen

2. Select **New Administrators** from the pull-down menu.
3. In the **User Name** field, enter up to 20 characters—this may include upper- and/or lowercase alphanumeric characters, and special characters.
4. 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.
5. In the **Confirm Password** field, re-enter the password in the exact format used at the Password field.
6. Click the **Save** button.

Log Off

To log off the Administrator console, click the **Logout** link beneath the banner in any screen to display the logout window:

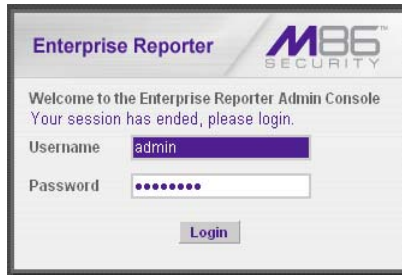


Fig. 1:1-5 Logout window

Click the “X” in the upper right corner of the browser window/tab to close the logout window. Exiting the Administrator console will log you out of the ER Server module, but will not log you out of the SR server, nor turn off the server.



WARNING: *If you need to turn off the SR server, follow the shut down procedures outlined in the Shut Down screen sub-section under the Server Menu section in Chapter 2. Failure to properly shut down the server can result in data being lost or corrupted.*

Chapter 2: Configuring the Server

Administrator Console

The Administrator console is used for configuring and maintaining the SR server. Settings made in the Administrator console affect the ER Web Client reporting application and Threat Analysis Reporter application. The Administrator console includes three menus: Network, Server, and Database. Each menu contains options from which you make selections to access screens used for configuring the server.



TIP: *When making a complete configuration using the ER Server module, 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, Administrators, Lockouts, Network Setting, Routing Table, Regional Setting, Diagnostics, and SNMP.

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.

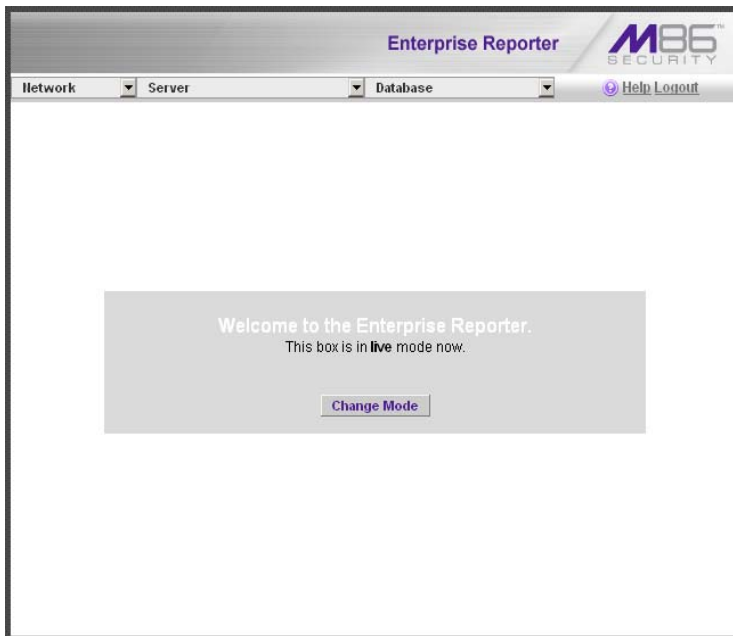


Fig. 1:2-1 Box Mode screen

Live Mode

Once your server is configured and the server box is set in the “live” mode, it will receive and process real time data from the Web access logging device. The ER Web Client reporting application can then be used to capture data and create views.

Archive Mode

In the “archive” mode, the server box 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 ER Web Client reporting application.

Change the Box Mode

1. Click the **Change Mode** button to display the two box mode options on the screen:



Fig. 1:2-2 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 access logging device.

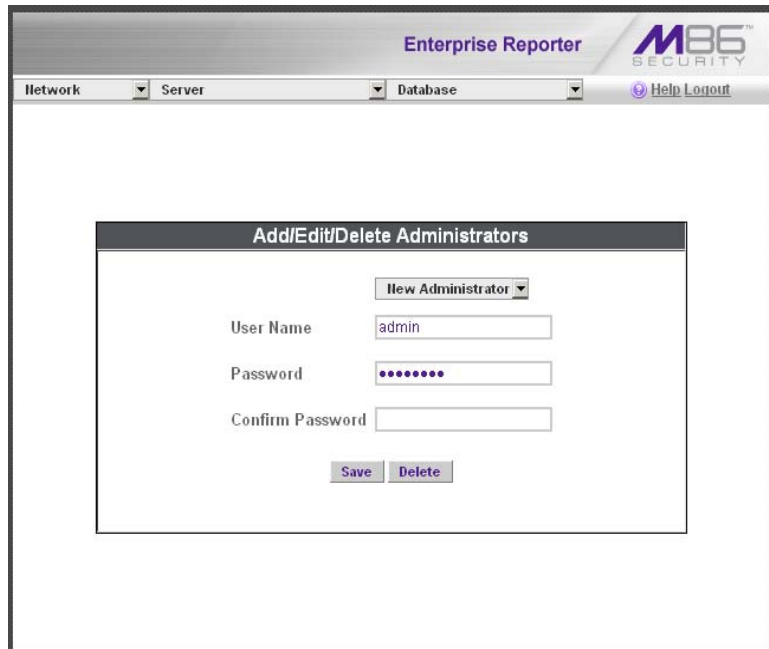
- choose **Archive** if you wish the server to function in the “archive” mode, solely as a receptacle for historical, archived files.
3. Click **Apply** to confirm your selection. The mode you specify will immediately be in effect.



NOTE: After applying the box mode setting, you must restart the server by selecting the **Restart Hardware** option on the Shut Down screen. (See the Shut Down sub-section under the Server menu section in this chapter.)


Add/Edit/Delete Administrators screen

The Add/Edit/Delete Administrators screen displays when the Administrators option is selected from the Network menu. This screen is used for viewing, adding, editing, and deleting the login ID of personnel authorized to configure the server. For security purposes, administrators should be the first users set up in the ER Server application.



The screenshot shows the 'Enterprise Reporter' application interface. At the top, there is a navigation bar with 'Enterprise Reporter' and the 'M86 SECURITY' logo. Below this, there are three dropdown menus: 'Network', 'Server', and 'Database'. A 'Help Logout' link is also present. The main content area displays a modal window titled 'Add/Edit/Delete Administrators'. Inside this window, there is a dropdown menu labeled 'New Administrator' with a downward arrow. Below it are three input fields: 'User Name' containing the text 'admin', 'Password' filled with ten dots, and 'Confirm Password' which is currently empty. At the bottom of the modal window, there are two buttons: 'Save' and 'Delete'.

Fig. 1:2-3 Add/Edit/Delete Administrators screen

 **TIP:** M86 Security recommends adding an alternate login ID prior to editing or deleting the default login ID. By doing so, if one login ID fails, you have another you can use.

View a List of Administrators

To view a list of administrator user names, click the down arrow at the **New Administrator** field. If no administrator has yet been assigned to the server, no selections display except for the default “admin” user name.

Add an Administrator

1. Select **New Administrator** from the pull-down menu.
2. In the **User Name** field, enter up to 20 characters—this may include upper- and/or lowercase alphanumeric characters, and special characters.
3. 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.
4. In the **Confirm Password** field, re-enter the password in the exact format used in the Password field.
5. Click the **Save** button to add the administrator to the choices in the pull-down menu.

Edit an Administrator’s Login ID

1. Select the administrator’s user name from the pull-down menu.
2. Edit either of the following fields:
 - User Name
 - Password (if this field is edited, the Confirm Password field must be edited in tandem)
3. Click the **Save** button.

Delete an Administrator

1. Select the administrator's user name from the pull-down menu.
2. After the administrator's login ID information populates the fields, click the **Delete** button to remove the administrator's user name from the choices in the pull-down menu.

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 and sub-administrators that are currently locked out of the Administrator console or Web Client.

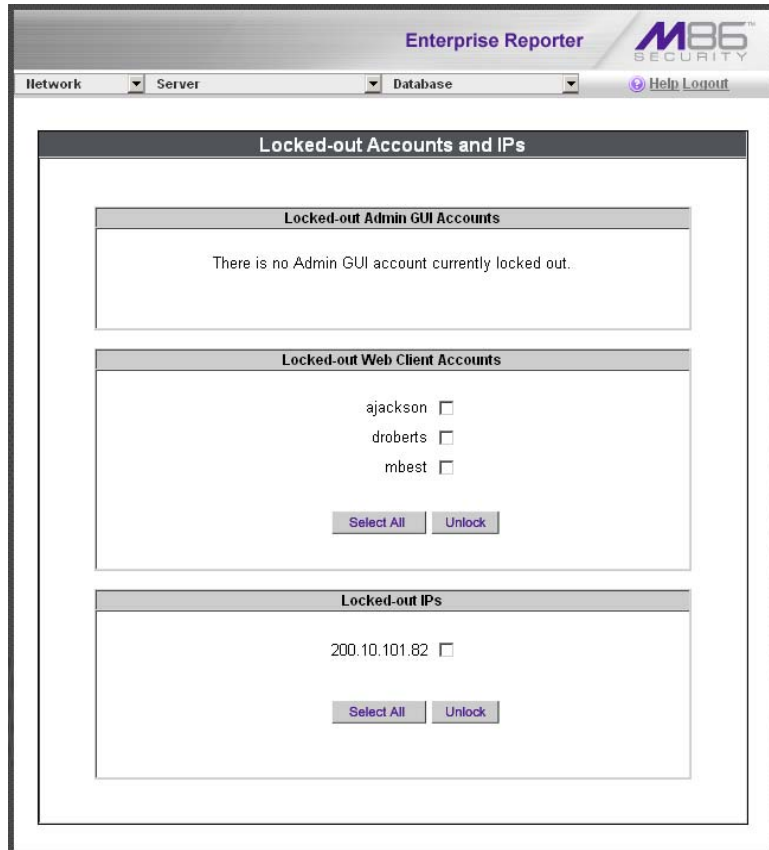


Fig. 1:2-4 Locked-out Accounts and IPs screen



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 Administrator console or Web Client 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 GUI Accounts** - There is no Admin GUI account currently locked out.
- **Locked-out Web Client Accounts** - There is no Web Client 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.
 - Web client 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.

Network Settings screen

The Network Settings screen displays when the Network Setting option is selected from the Network menu. This screen is used for setting up IP addresses so the server can communicate with your system.

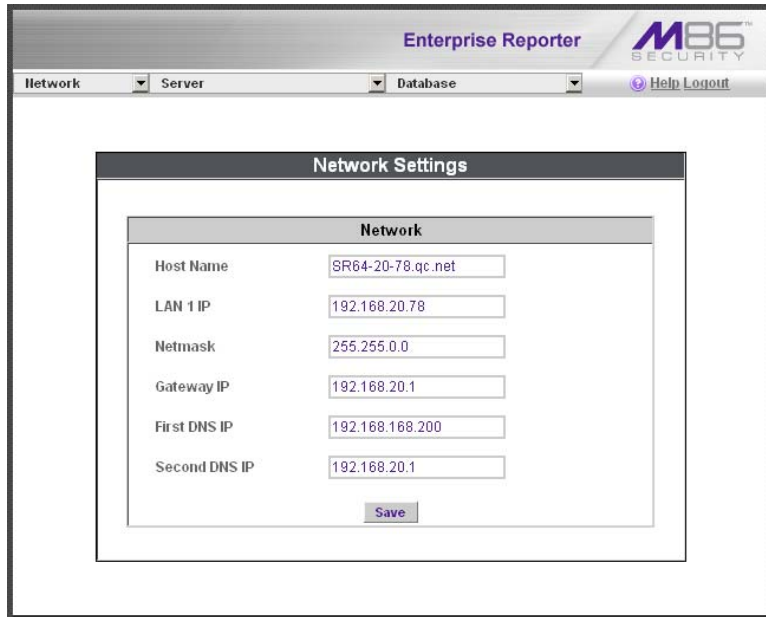


Fig. 1:2-5 Network Settings screen

Set up/Edit IP Addresses



TIP: In order for the server to effectively communicate with your system, be sure all fields contain accurate information before saving your settings.

1. Enter or edit an IP address in each appropriate field:
 - In the **Host Name** field, enter the address or URL that will be used for accessing the Administrator console. This entry should include the full, qualified domain name, and the “host” name for the box (i.e. reporter.myserver.com).
 - In the **LAN 1 IP** field, enter the IP address of the SR server on your Local Area Network (LAN 1).
 - In the **Netmask** field, enter the netmask that will define the traffic designated for the LAN.
 - In the **Gateway IP** field, enter the IP address for the default router that will be the main gateway for the entire network segment.
 - In the **First DNS IP** field, enter the IP address of the primary Domain Name System (name server). The server will use this IP address to identify other IP addresses on the system, including its own IP address.
 - In the **Second DNS IP** field, enter the IP address of the fallback DNS.
2. Be sure each IP address is correct, and then click **Save**.



NOTE: After appropriate entries have been made in these fields and saved, you must restart the server to activate the IPs. To restart the server, select the **Restart Hardware** option on the Shut Down screen. (See the Shut Down sub-section under the Server menu section in this chapter.)

Routing Table screen

The Routing Table screen displays when the Routing Table option is selected from the Network menu. This screen is used for viewing, building, and maintaining a list of routers—network destination and gateway IP addresses—the server will use for communicating with other segments of the network. You will only need to set up a routing table if your local network is interconnected with another network.

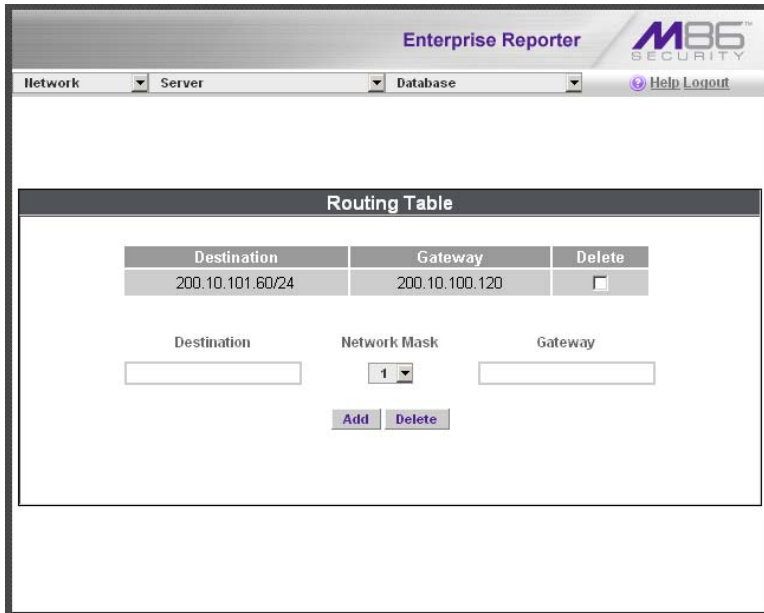


Fig. 1:2-6 Routing Table screen

View a List of Routers

Each router that was configured in the routing table displays as a separate row in the table. The IP address and subnet mask to receive data packets display in the Destination column, and the IP address of the portal that will transfer data packets to and from the Internet displays in the Gateway column.

Add a Router

1. In the **Destination** field, enter the IP address of the network to which data packets will be forwarded.
2. At the **Network Mask** pull-down menu, specify the number (1-32) of the subnet mask that will be used for grouping IP addresses on the same local network.
3. In the **Gateway** field, enter the IP address of the portal to which data packets will be transferred to and from the Internet.
4. Click the **Add** button to include your entry in the table. If you have another router to add, follow steps 1-4.
5. Click the **Back** button on the confirmation screen to return to the Routing Table screen.

Delete a Router

1. Click in the **Delete** checkbox of the row corresponding to the router you wish to remove from the routing table.
2. Click the **Delete** button.
3. Click the **Back** button on the confirmation screen to return to the Routing Table screen.

Regional Setting screen

The Regional Setting screen displays when the Regional Setting option is selected from the Network menu. This screen is used for specifying the time zone and network time to be used by the server when generating reports via the Web Client application, and setting the language set type to be displayed in the Administrator console, if necessary.

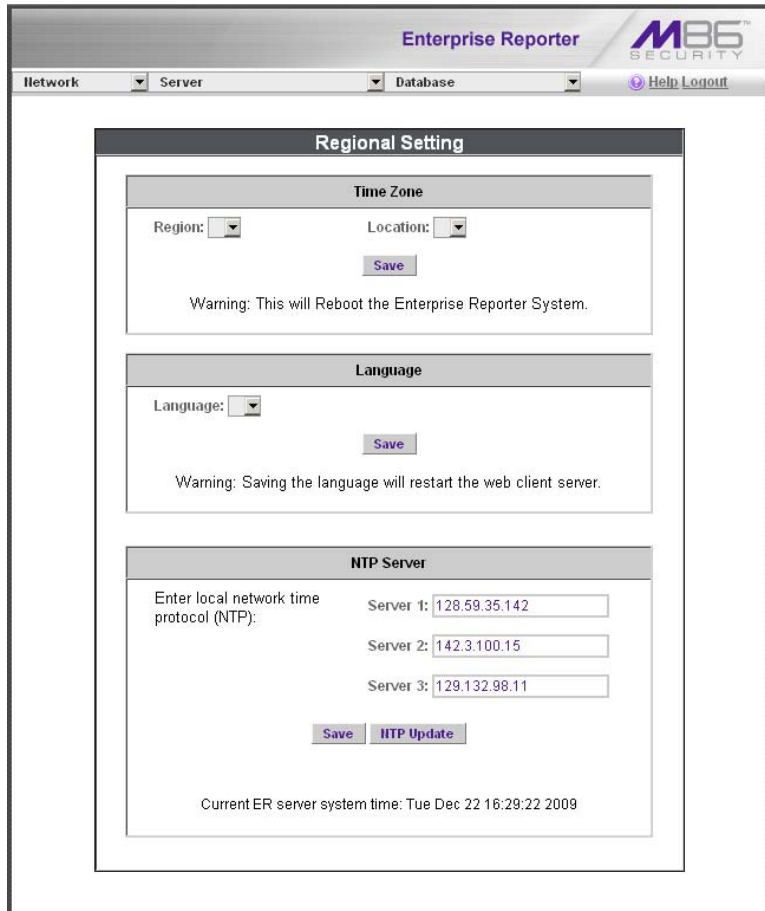


Fig. 1:2-7 Regional Setting screen

Specify the Time Zone

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.
3. Click **Save** to apply your settings, and to restart the Web Client Server.



WARNING: *The time zone set for the SR should be the same one set for each Web access logging device to be used by the SR. These “like” settings ensure consistency when tracking the logging times of all users on the network.*

Specify the Language Set

1. If necessary, select a language set from the **Language** pull-down menu to specify that you wish to display that text in the console.
2. Click **Save** to apply your settings, and to restart the Web Client Server.

Specify Network Time Protocol Servers

IP addresses of servers running Network Time Protocol (NTP) software are entered in the Server fields, and the Current ER server system time (day, date, HH:MM:SS time format, and year) displays below. NTP is a time synchronization system for computer clocks throughout the Internet. Your SR server will use the actual time from clocks at the IP addresses you've specified.

For the Enter local network time protocol (NTP) server fields, by default, the following IP addresses display in these three fields: 128.59.35.142, 142.3.100.15, and 129.132.98.11. If you wish to use different NTP servers, follow these steps:

1. Enter or edit an IP address in each appropriate field:
 - In the **Server 1** field, enter the IP address of the primary NTP server to be used for clock settings on your server.
 - In the **Server 2** field, enter the IP address of the secondary NTP server. The time from this server will be used by your server if the IP address for the primary server fails to be accessed by your server.
 - In the **Server 3** field, enter the IP address of the tertiary NTP server. The time from this server will be used by your server if the IP addresses for the primary and secondary servers fail to be accessed by your server.
2. Click the **Save** button to save your entries.



NOTE: *When you click the Save button, the IP addresses you entered are saved, but the time on your server will not be synchronized with the NTP servers until you click the NTP Update button.*

Update the Time on the Server

After you have saved the IP addresses of NTP servers you wish your server to access, click the **NTP Update** button to synchronize the clock on your server with the NTP server clocks.

Network Diagnostics screen

The Network Diagnostics screen displays when the Diagnostics option is selected from the Network menu. This screen is used to help you identify and resolve problems with your network configuration, using the ping and trace route utility tools.

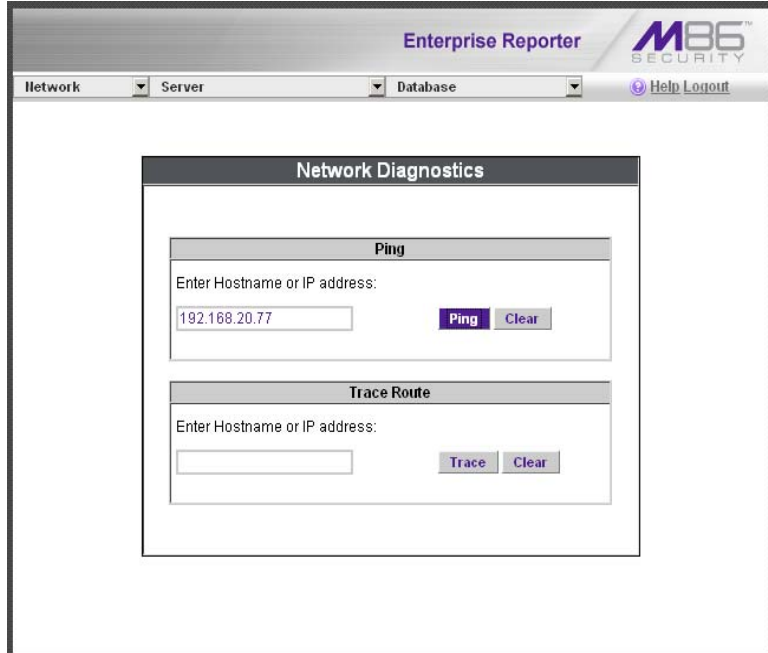


Fig. 1:2-8 Network Diagnostics screen, Ping entry

Ping

The ping utility is used for verifying whether the server can communicate with a machine at a given IP address within the network, and the speed of the network connection.

1. In the Ping frame, enter the IP address or host name of the specific Internet address to be contacted (pinged).
2. Click the **Ping** button to display the results found by the server, as shown on the sample screen:

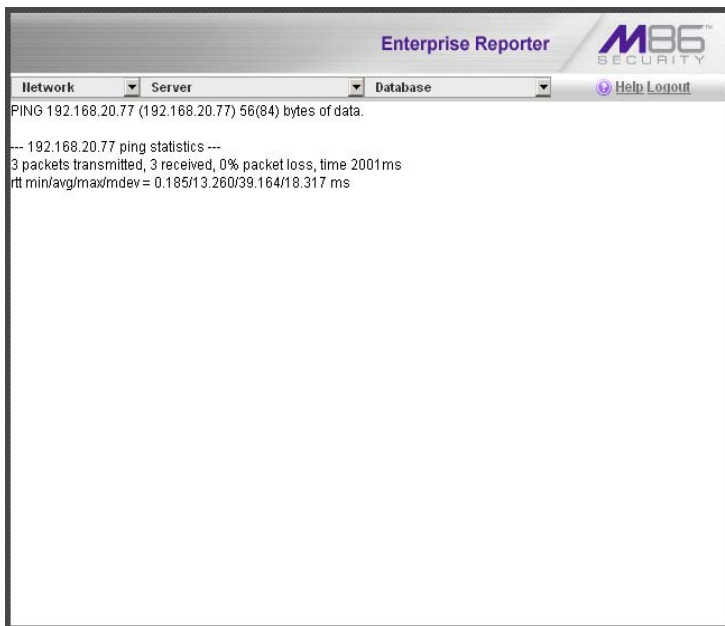


Fig. 1:2-9 Ping results

As indicated by the results for the sample entry, the server at 192.168.20.78 was able to communicate with the machine at the IP address 192.168.20.77. The statistics show that three (3) data packets were transmitted by the server, and three (3) packets were received by the designated machine, for a total of zero (0) percent packet loss.



TIP: *If the machine cannot be contacted, be sure the ping feature on that machine is turned on.*



NOTE: *To ping another IP address, click the Back button in your browser window, then click the Clear button in the Ping frame, and follow the procedures documented in this sub-section.*

Trace Route

If the ping utility was not able to help you diagnose the problem with your network configuration, you should use the trace route utility. This diagnostic tool records each “hop” (trip from one router to another) 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.



NOTE: *The trace route utility can be used after your routing table has been set up. To set up a routing table, see the Routing Table screen sub-section under the Network menu in this chapter.*

1. In the Trace Route frame, enter the IP address or host name of the specific Internet address to be validated.
2. Click the **Trace** button to display the results found by the server, as shown on the sample screen:

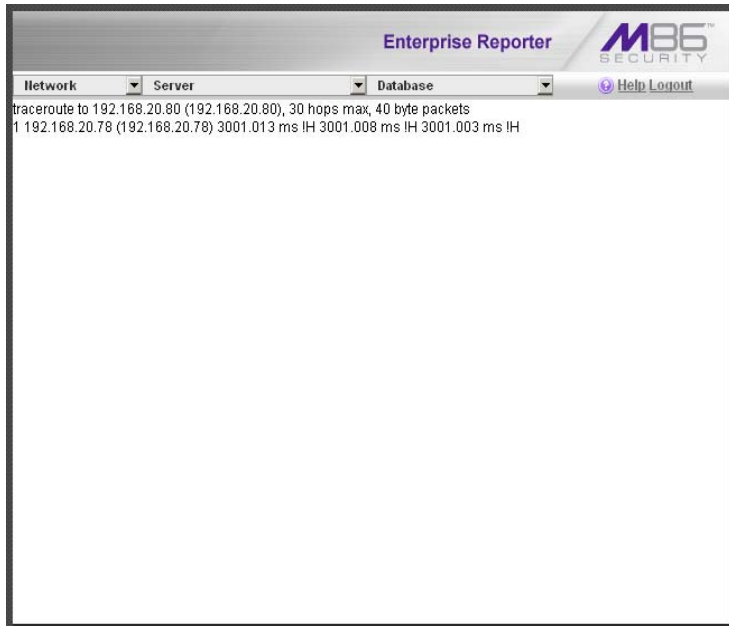



Fig. 1:2-10 Trace Route results

As indicated by the results for the sample entry, the packet made 30 hops. For each line in the report, the hop number displays, followed by the IP address or host name; the IP address in parentheses; and the maximum, minimum, and average response time in milliseconds.

 **TIP:** To “trace” another IP address, click the Back button in your browser window, then click the Clear button in the Trace Route frame, and follow the procedures documented in this sub-section.

SNMP screen

The SNMP screen displays when the SNMP option is selected from the Network menu. 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 ER's Internet reporting on a network.

The screenshot shows the 'Enterprise Reporter' web interface. At the top, there are navigation tabs for 'Network', 'Server', and 'Database', along with a 'Help Logout' link. The main content area is titled 'SNMP' and is divided into two sections: 'Monitoring Mode' and 'Monitoring Settings'. In the 'Monitoring Mode' section, the status is 'Monitoring mode: On', with 'Enable' and 'Disable' buttons. The 'Monitoring Settings' section includes a 'Community token for public access' text box containing 'public'. Below this is an 'Access control list' section with a text box containing '10.20.20.73' and a 'Delete' button. At the bottom of this section is an 'Enter new IP to add' text box and an 'Add' button. Finally, 'Save' and 'Cancel' buttons are located at the bottom right of the main content area.

Fig. 1:2-11 SNMP screen

The following aspects of the SR 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.

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 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**.

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**.

Server Menu

The Server pull-down menu includes options for setting up processes for maintaining the server. These options are: Backup, Self-Monitoring, SMTP Server Setting, Server Status, Secure Access, Software Update, Software Update Setting, Shut Down, Web Client Server Management, and Hardware Failure Detection.

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 ER, and for performing a restoration to the database from the previous backup run.

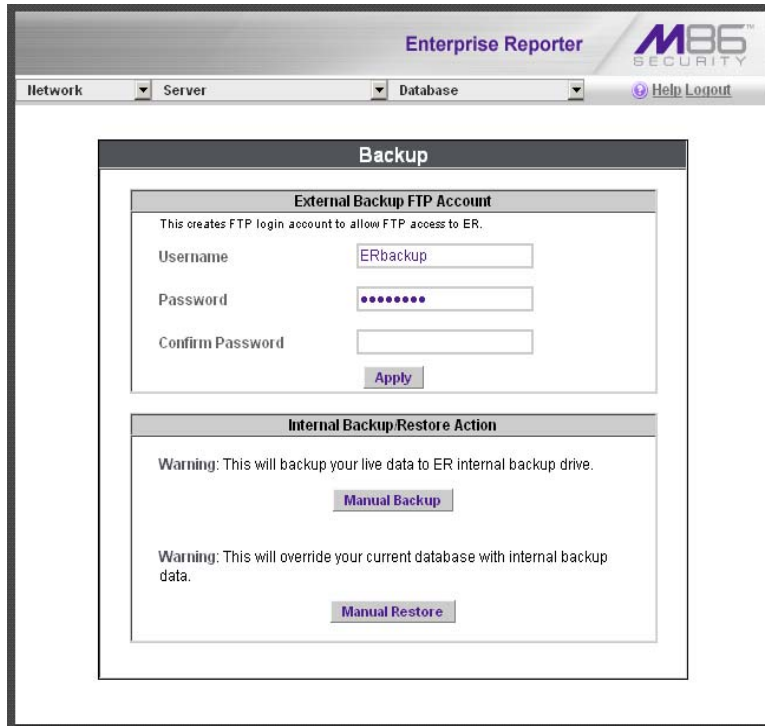


Fig. 1:2-12 Backup screen

Backup and Recovery Procedures

! **IMPORTANT:** M86 Security recommends establishing backup and recovery procedures when you first begin using the ER. Please follow the advice in this section to ensure your ER 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 nightly by default, it is important that the ER 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 ER 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 ER database becomes corrupted** - Correct the root problem. Restore the database from the most recent ER 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 ER 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 ER'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 ER, prior to the daily backup process.



WARNING: If corrupted data is detected on the ER, do not backup your data, as you may back up and eventually restore a corrupted database.

When performing a manual backup, the ER'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 ER'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 ER 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 ER's backup database to the remote server. When you are in the /backup/database/ directory, be sure to get all the *.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 ER via FTP. (See Perform a Restoration to the ER Server Module.)

Perform a Restoration to the ER Server Module

There are two parts in performing a restoration of data to your ER. Part one requires data to be loaded on the remote server and then FTPed to the ER. Part two requires the FTPed data to be restored on the ER.



NOTE: *Before restoring backup data to the ER, be sure you have enough space on the ER. Data that is restored to the ER will automatically include indexes.*

Perform these steps on the remote server:

1. Load the backup data on your remote server.
2. Log in to your FTP account.
3. FTP the backup data to the ER's internal backup drive.

On the ER Server's Backup screen:

1. Click the **Manual Restore** button in the Internal Backup/Restore Action frame to specify that you wish to overwrite data on the live ER 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 ER.



NOTE: *The amount of time it will take to restore data to the ER depends on the combined size of all database tables being restored. M86 Security recommends that you do not perform other functions on the ER 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.

The screenshot shows the 'Enterprise Reporter' application interface. At the top, there are navigation menus for 'Network', 'Server', and 'Database', along with a 'Help Logout' link. The main content area displays a 'Self Monitoring' dialog box. The dialog box contains the following elements:

- Header: **Self Monitoring**
- Question: **Would you like to activate self-monitoring?** with radio buttons for **YES** and **NO**.
- Text: **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.**
- Form fields:
 - Master Administrator's E-Mail Address:**
 - Choice one** **Send e-mail to e-mail address:**
 - 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:**
- Button: **Save**

Fig. 1:2-13 Self Monitoring screen

As the administrator of the server, 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 server 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

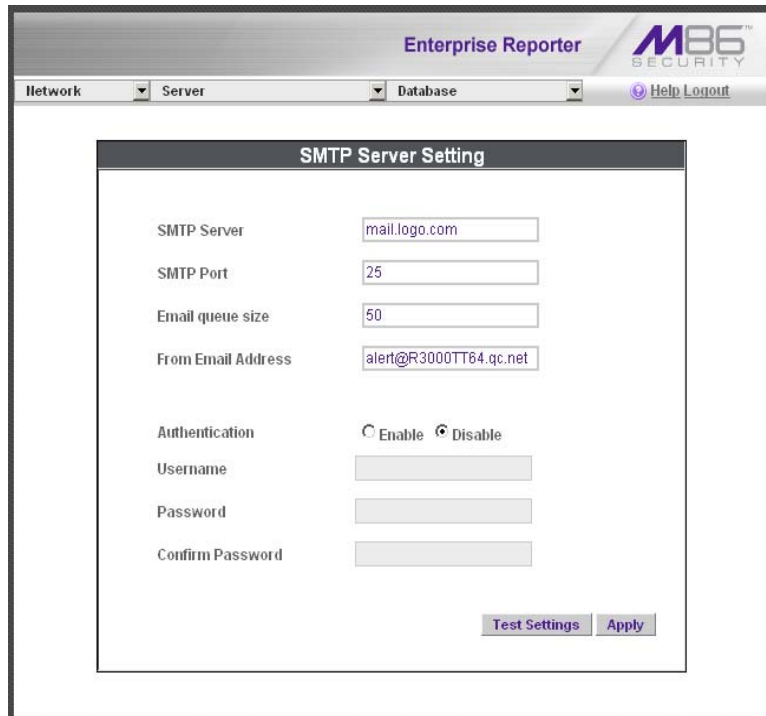
1. To stop sending emergency notifications to an e-mail address set up in the list, remove the check mark from the checkbox corresponding to the appropriate e-mail address.
2. Click the **Save** button to remove the recipient's name from the e-mail list. The Master Administrator and any remaining e-mail 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.

SMTP Server Setting screen

The SMTP Server Setting screen is used for entering settings for the Simple Mail Transfer Protocol that will be used for sending email alert messages to specified administrators.



The screenshot shows the 'SMTP Server Setting' screen within the 'Enterprise Reporter' application. The interface includes a navigation bar with 'Network', 'Server', and 'Database' dropdown menus, and a 'Help Logout' link. The main content area is titled 'SMTP Server Setting' and contains the following fields and options:

- SMTP Server:
- SMTP Port:
- Email queue size:
- From Email Address:
- Authentication: Enable Disable
- Username:
- Password:
- Confirm Password:

At the bottom right of the form, there are two buttons: 'Test Settings' and 'Apply'.

Fig. 1:2-14 SMTP Server Setting screen

Enter, Edit SMTP Server Settings

1. Enter the **SMTP Server** name, for example: **mail.logo.com**.
2. By default, the **SMTP 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. In the **From Email Address** field, enter the email address of the server that will be sending alert email messages to designated administrators.
5. 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.
6. Click **Apply** to apply your settings.

Verify SMTP Settings

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

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

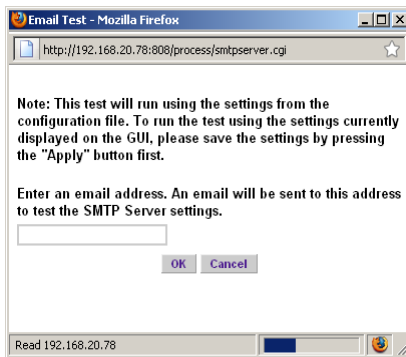


Fig. 1:2-15 SMTP Email Test box

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

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

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 server, and provides information on the amount of space and memory used by each process.

The screenshot displays the 'Enterprise Reporter' interface with the 'Server Status' section selected. It provides a comprehensive overview of the server's operational metrics.

Product Version:
Current Version: Security Reporter 2.0.00.3

Server Status

CPU Utilization

CPU Load Averages: 0.00, 0.00, 0.00
 CPU states: 0.5%us, 1.9%sy, 0.0%ni, 95.8%id, 1.7%wa, 0.0%hi, 0.1%st, 0.0%st

Memory: 2056832k total, 1990232k used, 65600k free, 300k buffers

Swap: 2097144k total, 170488k used, 1926656k free, 1760096k cached

| PID | USER | PR | NI | VIRT | RES | SHR | S | %CPU | %MEM | TIME+ | COMMAND |
|-------|------|----|----|-------|------|------|---|------|------|---------|-------------|
| 3160 | dbus | 20 | 0 | 21268 | 462 | 448 | S | 0.0 | 0.0 | 0:00.00 | dbus-daemon |
| 19916 | root | 20 | 0 | 7164 | 1320 | 1204 | S | 0.0 | 0.1 | 0:00.28 | dbcontrol |

Disk drives status

| Filesystem | 1k-blocks | Used | Available | Use% | Mounted on |
|-----------------------------|-----------|-----------|-----------|------|----------------|
| /dev/mapper/VG00-rootlv | | | | | / |
| 28297728 | 4782900 | 23514828 | 17% | | / |
| /dev/md0 | 108765 | 55690 | 47459 | 54% | /boot |
| tmpfs | 1027916 | 0 | 1027916 | 0% | /dev/shm |
| /dev/mapper/VG00-8e6lv | | | | | |
| 36682240 | 1142748 | 35539492 | 4% | | /usr/local/8e6 |
| /dev/mapper/VG00-backuplv | | | | | |
| 136248320 | 7688 | 136240632 | 1% | | /backup |
| /dev/mapper/VG00-recoverylv | | | | | |
| 2064208 | 977184 | 982168 | 50% | | /recovery |
| /dev/mapper/VG00-dblv1 | | | | | |
| 253631488 | 35133788 | 219497700 | 14% | | /database/d1 |

NETSTAT

| Proto | Recv-Q | Send-Q | Local Address | Foreign Address | State | PID/Program Name |
|-------|--------|--------|----------------------------|----------------------------|-------------|------------------|
| tcp | 0 | 0 | R3000TT64.qc.opsession-pny | R3000TT64.qc.8e6.net:54224 | ESTABLISHED | 3374/mysqld |
| tcp | 0 | 0 | R3000TT64.qc.opsession-pny | R3000TT64.qc.8e6.net:54223 | ESTABLISHED | 3374/mysqld |

Fig. 1:2-16 Server Status screen

View the Status of the ER 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.



Fig. 1:2-17 Secure Access screen

Activate a Port to Access the ER Server

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".

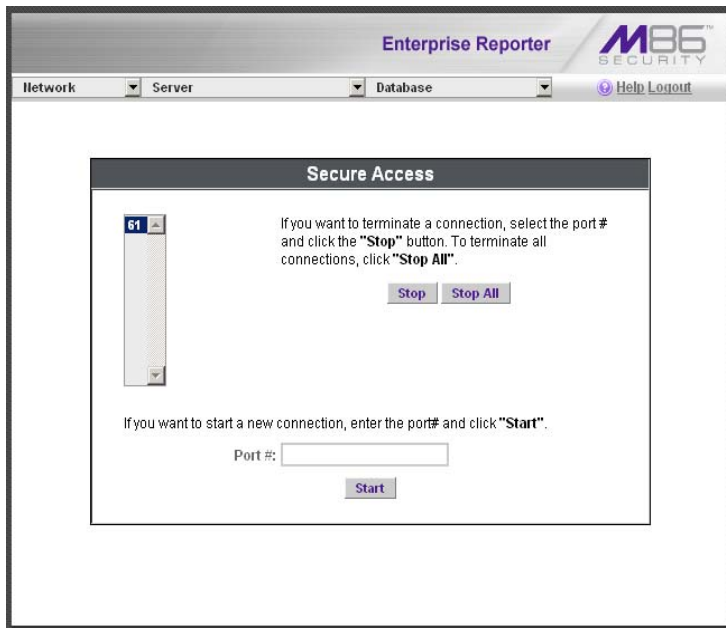


Fig. 1:2-18 Port entries

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.

Software Update screen

The Software Update screen displays when the Software Update option is selected from the Server menu. This screen is used for updating the SR server with software updates supplied by M86 Security, and for viewing a list of software updates that are available and/or previously installed on the server.

The screenshot shows the 'Software Update' screen within the 'Enterprise Reporter' application. The interface includes a navigation bar with 'Network', 'Server', and 'Database' dropdown menus, and a 'Help Logout' link. The main content area is titled 'Software Update' and contains two tables:

| SR Software Updates | | |
|---------------------|---|----------------------------|
| Date | Name | Description |
| 2010/01/26 | SR.2.0.00.9.20100121 Undo README | Security Reporter 2.0.00.9 |

| SR Software Update History | | |
|----------------------------|---|-------------------|
| Date | Name | Description |
| 2010/01/21 | SR.2.0.00.6.20100107 Undo README | Security Reporter |

Please click [here](#) to view the Software Update Log.

Fig. 1:2-19 Software Update screen

View Installed Software Updates

Any software update previously installed on the server displays in the SR Software Update History frame. For each installed software update, the Date installed (YYYY/MM/DD), and software update Name and Description display.

Uninstall the Most Recently Applied Software Update

In the SR Software Update History frame, the most recently applied software update can be unapplied by clicking **Undo**. This action removes the software update from the server.

View Available Software Updates

Any software update available for installing on the SR server displays in the SR Software Updates frame. The following information is included for each software update: Date the software update was made available (YYYY/MM/DD), software update Name, and Description (software version number, and Prerequisite software version for installing the software update). The Apply Now and README buttons display beneath the software update name. (See Install a Software Update for information about these buttons.)

Install a Software Update



WARNING: Before installing a software update, you must shut off the server's software by selecting the **Shutdown Software** option on the Shut Down screen. (See the Shut Down subsection under the Server menu section in this chapter.) All software updates must be installed in numerical order on your server.



NOTES: Be sure to terminate all reports that are currently running or are scheduled to run before applying a software update, and that port 8084 is open on your network.

In the SR Software Updates frame, two buttons are available: README and Apply Now.

README:

1. Click **README** to open a pop-up box containing information about the software release:

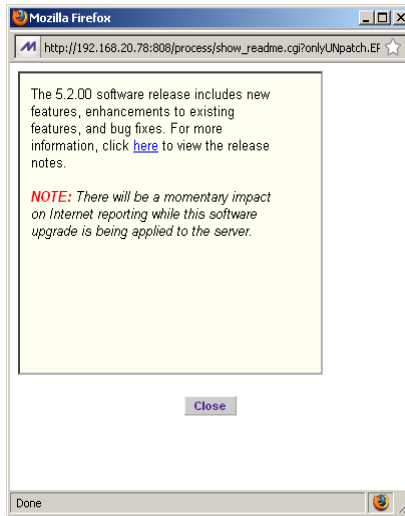


Fig. 1:2-20 Software update box

2. After reading the contents of the software release, click **Close** to close the pop-up box.

Apply Now:

1. Click **Apply Now** to open a dialog box containing information about the software release:

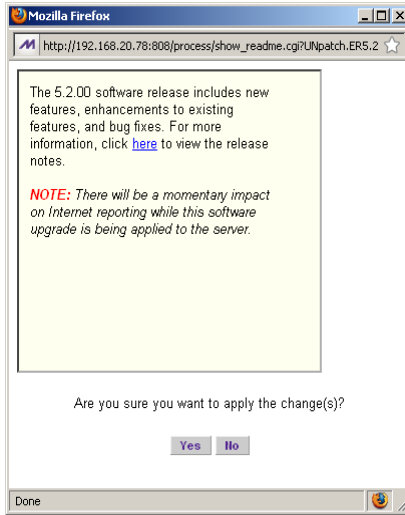


Fig. 1:2-21 Software update dialog box

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

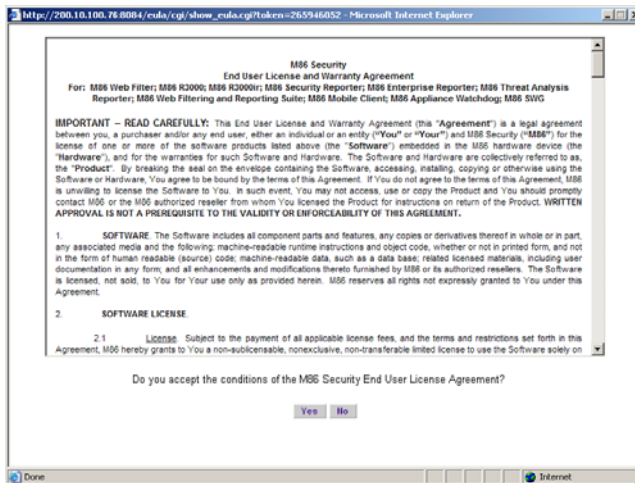


Fig. 1:2-22 EULA dialog box

3. 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 begins the software update application process.
4. To determine whether the software update has been successfully applied, click the hyperlink (“here”) beneath the SR Software Update History frame in the Software Update screen to open the Software Update Log window:

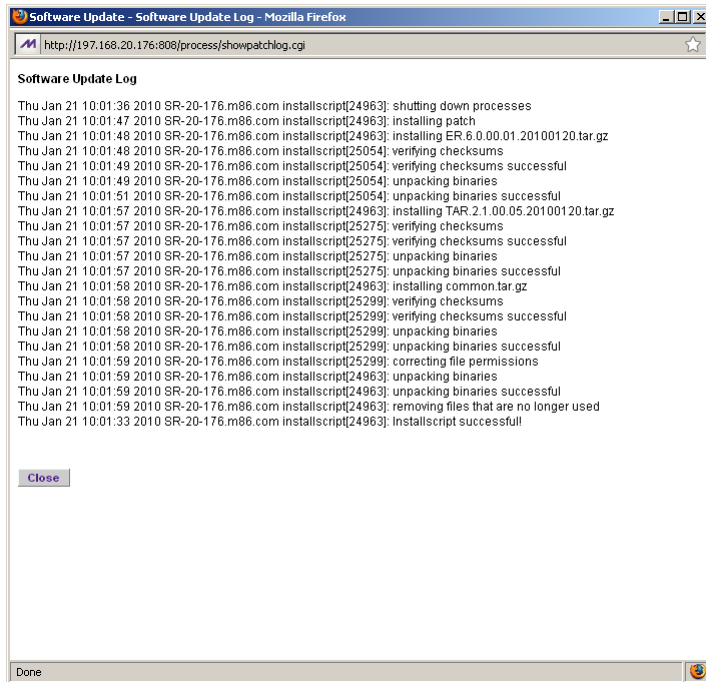



Fig. 1:2-23 Software Update Log window

5. After viewing the contents of this window, click **Close** to close this window.
6. After the software update has been successfully applied, refresh the Software Update screen by selecting Software Update from the Server pull-down menu. The soft-

ware update details should display in the SR Software Update History frame.

 **NOTE:** After installing the software update, if a message displays that informs you to reboot the server, you should select the **Restart Software** option on the Shut Down screen.

Software Update Setting screen

The Software Update Setting screen displays when the Software Update Setting option is selected from the Server menu. This screen is used for configuring the SR to receive software updates.

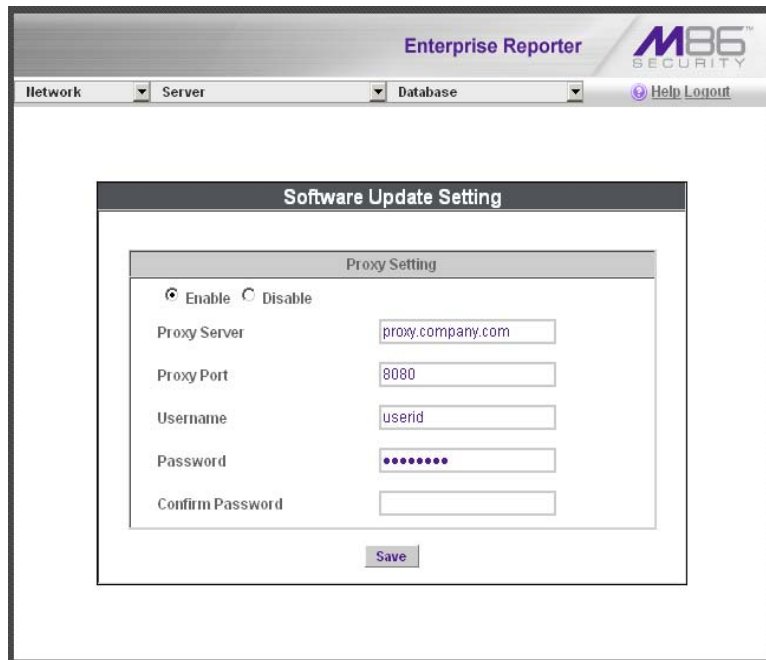


Fig. 1:2-24 Software Update Setting screen

Specify Proxy Settings

1. In the Proxy Setting frame, by default “Disable” is selected. Click “Enable” if the server is in a proxy server environment.
2. In the **Proxy Server** field, enter the host name of the proxy server.
3. In the **Proxy Port** field, enter the port number of the proxy server.
4. In the **Username** field, enter the username for the proxy account.
5. Enter the same password in the **Password** and **Confirm Password** fields.

Save Settings

Click **Save** to save your settings.

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 server’s software or hardware.

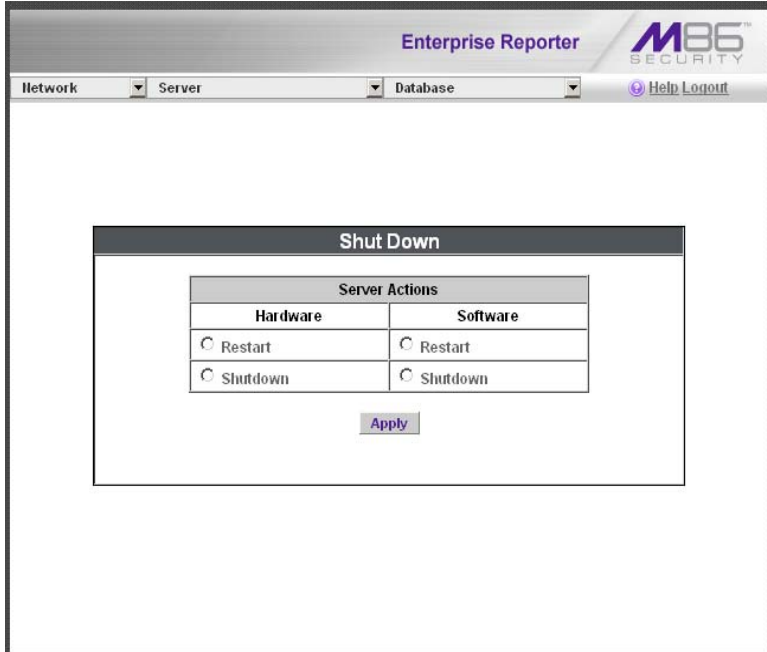


Fig. 1:2-25 Shut Down screen

Server Action Selections

- Restart the Server’s Hardware** - The Restart Hardware option should be selected if the server needs to be rebooted—for example, when applying certain hardware configurations. You will need to use this option if the box mode has been changed or after an IP address has been entered in the Network Settings screen. During the Hardware Restart process, files normally FTPed to the server are routed to a problem directory in the logging device.

When the server is running again, these files are FTPed to the server.

- **Shut Down the Server's Hardware** - The Shutdown Hardware option should only be selected if the server's hardware must be completely shut down—for example, if the server will be physically relocated. When this option is selected, the server shuts off, and files normally FTPed to the server will be routed to a problem directory in the logging device. When the server is rebooted, these files will be FTPed to the server.
- **Restart the Server'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 Server'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 window from the Server menu again to return to the Shut Down screen.



NOTE: *When the Restart Software option is selected, the server will take five to 10 minutes to reboot. After this time, you can go to another screen or log off.*

Web Client Server Management screen

The Web Client Server Management screen displays when the Web Client Server Management option is selected from the Server menu. This screen is used for enabling specified Web Client server features.

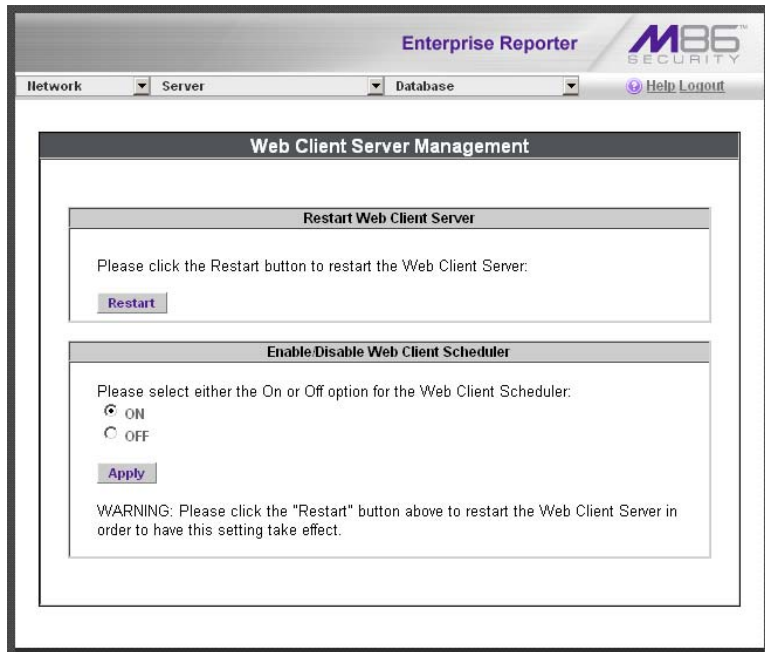


Fig. 1:2-26 Web Client Server Management screen

Restart the Web Client Server

In the Restart Web Client Server frame, click **Restart** to restart the Web Client server. As a result of this action, a screen displays with the following message: “The Web Client Server will restart in a few minutes.” Click **OK** to return to the Web Client Server Management screen.

Enable/Disable the Web Client Scheduler

1. In the Enable/Disable Web Client Schedule frame, click the appropriate radio button to specify whether or not to automatically run scheduled Web Client reports:

- “ON” - Choose this option to let the Web Client automatically run scheduled reports.



WARNING: *Do not select this option if using the Access Client to run scheduled reports; duplicate reports will be generated.*

- “OFF” - Choose this option to use the Access Client for running scheduled reports, or if you do not want the Web Client to run scheduled reports.

2. Click **Apply**.

3. Click **Restart** to restart the Web Client Server.

Hardware Failure Detection screen

The Hardware Failure Detection screen displays when the Hardware Failure Detection option is selected from the Server menu. This screen is used for showing the status of each drive on the RAID server.

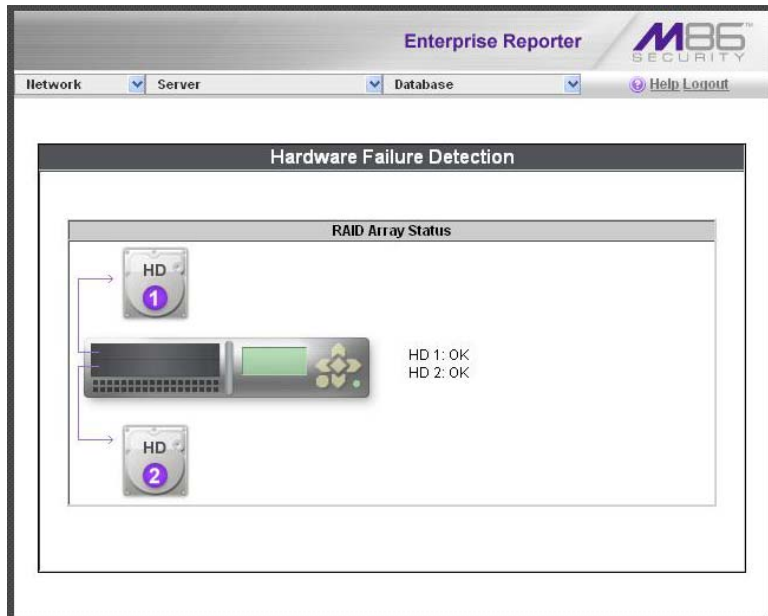


Fig. 1:2-27 Hardware Failure Detection screen, 300 series model

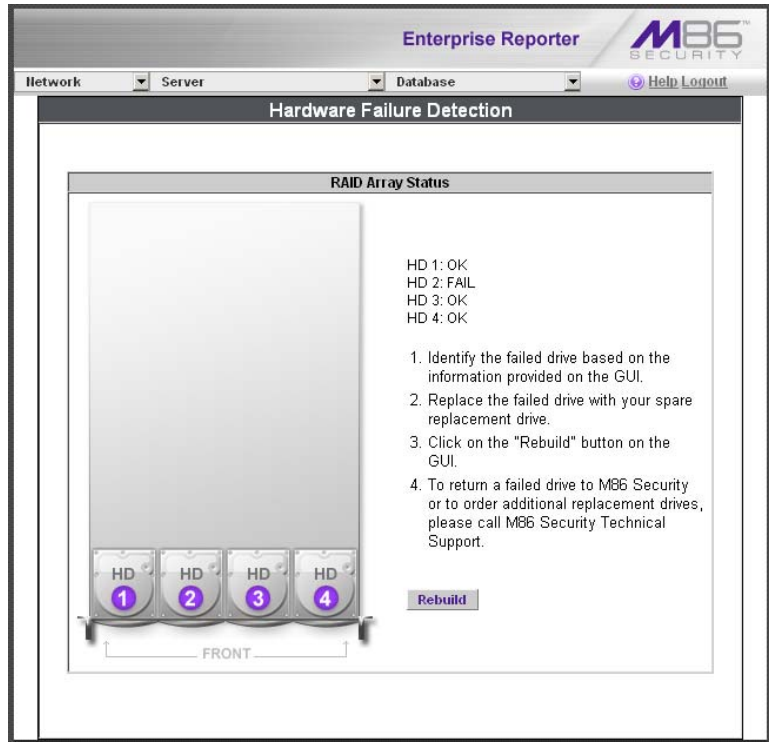


Fig. 1:2-28 Hardware Failure Detection screen, 500 or 700 series

View the Status of the Hard Drives

The current RAID Array Status displays for all hard drives (HD 1 and HD 2 for 300 series models, and HD 1 through HD 4 for 500 and 700 series models). If all hard drives are functioning without failure, the text "OK" displays for each corresponding drive number listed at the right of the screen, and no other text displays.

If any of the hard drives has failed, the message "FAIL" displays for the corresponding drive number listed at the right of the screen, 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 SR Appendix II: RAID and Hardware Maintenance.

Database Menu

The Database pull-down menu includes options for configuring the database. These options are: IP.ID, Username Display Setting, 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 server 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 Web Client when logging a user's Internet activity.

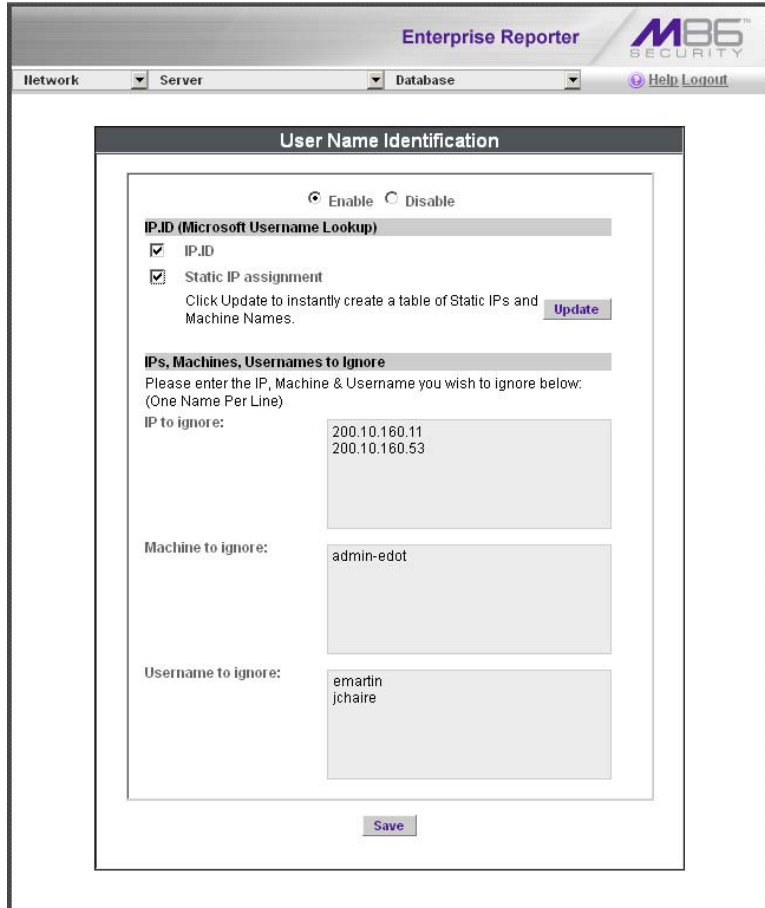




Fig. 1:2-29 User Name Identification screen with IP.ID activated


As the administrator of the server, 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 ER 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 ER is the same for each Web access logging device the ER 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.

4. In the IP/Machine/Username to ignore list boxes, enter all IP addresses, machine names, and/or usernames the server should disregard when identifying users. Each entry should be made in a separate row.
5. After making all necessary entries on this screen, click the **Save** button.

Deactivate User Name Identification

1. Click the radio button corresponding to **Disable**.
2. Click the **Save** button.

Username Display Setting screen

This Username Display Setting screen displays when the Username Display Setting option is selected from the Database menu. This screen is used for configuring the username format imported from raw logs and customizing the username format that displays in reports.

The screenshot shows the 'Enterprise Reporter' interface with the 'M86 SECURITY' logo. The navigation bar includes 'Network', 'Server', and 'Database' dropdown menus, and a 'Help Logout' link. The main content area is titled 'Username Display Setting' and is divided into two sections:

- Current Username Display Setting:** A section with the text 'The current display name format is:' followed by an empty text input field.
- Modify Username Display Setting:** A section with the instruction 'Please SELECT the username in the raw log from the following fields:'. It contains a list of 'Available Fields' with a scrollable dropdown menu showing 'Domain Name', 'Organization Name', 'Department Name', and 'User Name'. Below this is an 'Add' button. Further down, it says 'Please select how you want the username displayed on the ER report and click "Apply":'. This is followed by a 'Raw Log Fields:' dropdown menu and another 'Add' button. At the bottom of this section is a 'Display username:' text input field and 'Apply' and 'Reset' buttons.

A red warning message is displayed at the bottom of the screen: **WARNING: After applying or updating a username format, please re-run the User Group Import from the Admin console. This ensures the new user group patterns can be used in drill down reports for these user groups.**

Fig. 1:2-30 Username Display Setting screen

View the Current Username Display Setting

In the Current Username Display Setting frame, the current username format displays—if previously entered in the Display username field and saved on this screen.

Modify the Username Display Setting

In the Modify Username Display Setting frame, make selections from list boxes and apply results for the new username format to be displayed in the report.

1. By default, the following choices display in the Available Fields list box: Domain Name, Organization Name, Department Name, User Name. Make a selection from this list for the first field displayed in your server console and raw logs that you wish to include in the username format in the report.
2. Click **Add** to include this selection in the Raw Log Fields list box below.



NOTE: Follow steps 1 and 2 for each consecutive field to be added to the Raw Log Fields list box.



TIP: Click the Reset button on this screen at any time to revert to the default settings.



WARNING: It is important to select the correct fields from this list, in the order in which they appear in your server console. For example, if the username format on the console is Domain Name\Department Name\User Name, and only User Name and Department Name are selected from the Available Fields list box—in that order—the report will display information in the wrong order. In this example, if the Domain Name is LOGO, the Department Name is Admin, and the User Name is JSmith, the report will show JSmith\Admin, instead of LOGO\Admin\JSmith.

3. In the Raw Log Fields list box, select the first field to be displayed in the username format on the report.

4. Click **Add** to include your selection in the Display username field below.



NOTE: Follow steps 3 and 4 for each field to be added to the Display username field below. Each additional selection added to the display name is preceded by a backslash (\).

5. Click **Apply** to save your entries and to display the new username format in the Current Username Display Setting frame.



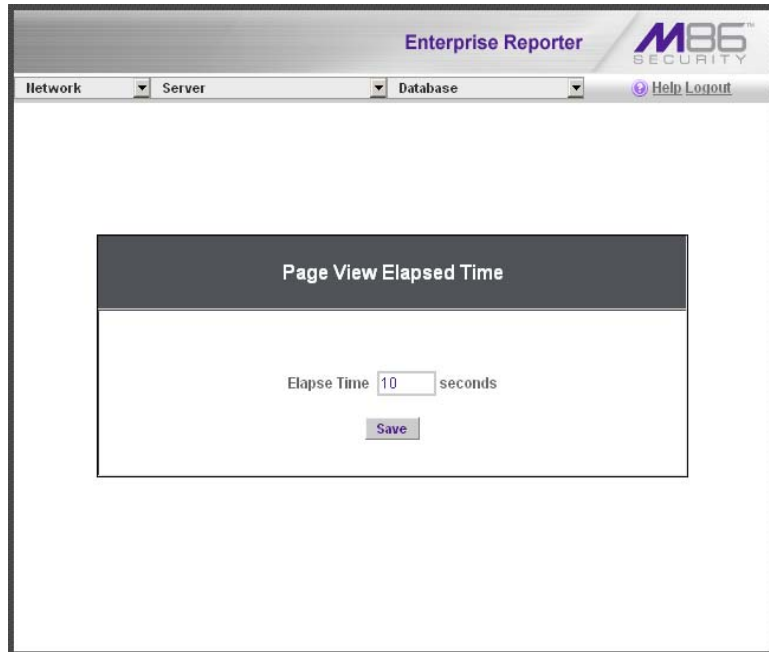
NOTE: Changes made to username display settings in this screen will not be effective until the next day's reports are generated.



WARNING: After modifying a username format, be sure to import users and groups using the User Group Import screen. See the User Group Import screen for information on importing user groups.

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.



The screenshot shows the 'Enterprise Reporter' interface. At the top, there are navigation tabs for 'Network', 'Server', and 'Database'. The 'Database' tab is selected. In the top right corner, there is a logo for 'M86 SECURITY' and a 'Help Logout' link. The main content area is titled 'Page View Elapsed Time'. Below the title, there is a text input field labeled 'Elapse Time' containing the number '10', followed by the text 'seconds'. Below the input field is a 'Save' button.

Fig. 1:2-31 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.

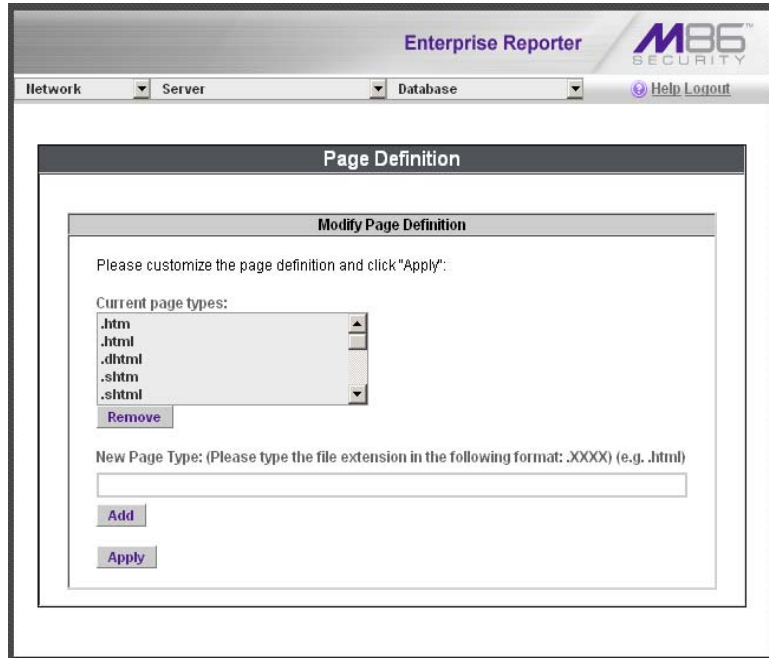


Fig. 1:2-32 Page Definition screen

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 WebClient application.

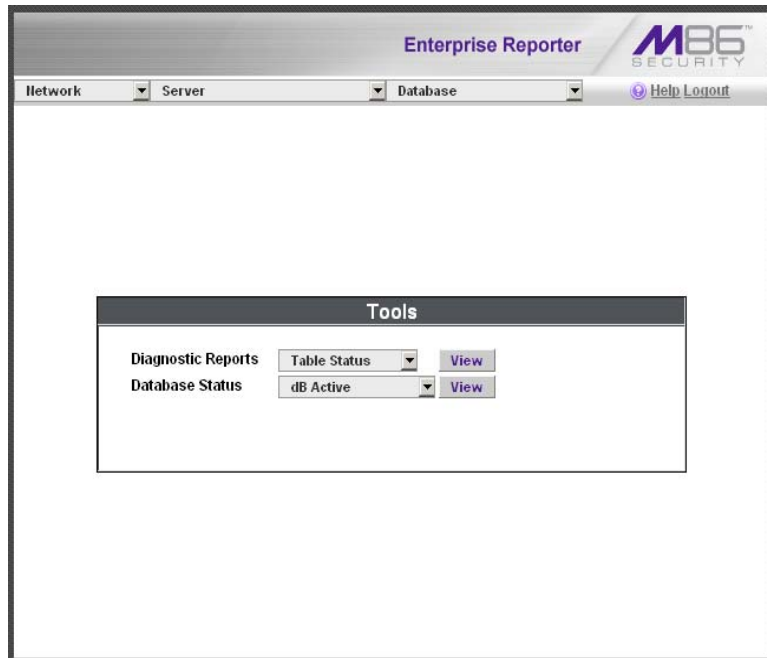


Fig. 1:2-33 Tools screen

The following options are available on this screen:

- View Diagnostic Reports
- View Database Status Logs

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 ER process when processing log files.

- **db Expiration** - This log includes information about expiring data on the server.
- **db Expire Summary** - This log provides a list of data expiration from summary tables.
- **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.
- **File Watch Log** - This log shows a list of records that were imported from one machine to another.

- **Software Update Log** - This log gives information about applied software updates.
 - **MYSQL Log** - This log provides information pertaining to the MySQL server.
 - **Error Entry - Web Filter** - This log displays a list of Web Filter query errors.
3. Click the “X” in the upper right corner of the pop-up window to close the window.

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 ER, and provides an estimated date when that data will expire. By reviewing the current database disk space utilization and the average number of daily hits on your ER, adjustments can be made to the number of weeks of live and archive data you wish to store in the future before that data expires.

The screenshot shows the 'Expiration' screen in the Enterprise Reporter interface. The page title is 'Expiration' and the status is 'Status as of 2009-12-23 01:27:34'. The interface includes a navigation bar with 'Network', 'Server', and 'Database' menus, and a 'Help Logout' link. The main content area displays a list of statistics and a 'Change Settings' section.

| Expiration | |
|---|---|
| Status as of 2009-12-23 01:27:34 | |
| Date scope for total data | 2009-12-11 00:09:26 - 2009-12-23 00:09:44 |
| Total number of week(s) stored | 2 week(s) |
| Current live data (yearweekno/date scope) | 200949 - 200951 2009-12-11 00:09:26 - 2009-12-23 00:09:44 |
| Total number of live week(s) | 2 week(s) |
| Current archive data (yearweekno/date scope) | 0 - 0 0 - 0 |
| Total number of archive week(s) | 0 week(s) |
| Database disk space utilization (used database space/total database space) | 3.44 % (1.73/50.33 Gbytes) |
| Target percentage of live data | 100 % |
| Last 8 weeks hits/day average | 112849 |
| Estimated total week(s) of live data | 226 week(s) |
| Estimated total week(s) of archive data | 0 week(s) |
| Estimated number of week(s) until next expiration | 49 week(s) |
| Change Settings | |
| Hits/day | 112849 |
| Percentage of live data | 100 % |
| <input type="button" value="Calculate"/> | |
| Estimated total week(s) of live data | <input type="text"/> week(s) |
| Estimated total week(s) of archive data | <input type="text"/> week(s) |
| <input type="button" value="Save"/> | |

Fig. 1:2-34 Expiration screen



NOTE: *Though the database is backed up automatically each day, 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 ER.)*

Expiration Screen Terminology

The following terminology is used on the Expiration screen:

- **Live** - pertains to indexed data on the hard drive of the server for the most recent weeks—the period designated as “live.” Indexed data includes pages and objects that were accessed by users on the Internet, as well as the indexes for these items.

When setting up the server to store data, M86 Security recommends that you allocate the highest percentage possible for live data storage, since reports run faster if indexes are available for pages and objects.

If your server is set up to store live data only (100 percent live data), you will be able to store less data than if you store both live and archive data, since indexes require additional storage space.

- **Archive** - pertains to non-indexed data on the hard drive of the server for the oldest weeks—the period designated as “archive.” Non-indexed data might include pages and/or objects that were accessed by users on the Internet.

Since archive data contain no indexes, they occupy less space on the server than live data—which include indexes and pages/objects. However, reports generated for periods of time with archive data take longer to process since indexes are not included for that data.

- **Expire** - pertains to the action of dropping data from the server when there is no room left on the hard drive for additional storage. When the hard drive reaches its maximum data storage capacity, indexes from the oldest week of data stored on the server are dropped, or “expired” from the server. Thereafter, when more space is needed on the server, the oldest week of non-indexed data “expires.”

Expiration Rules

The administrator of the server specifies the number of weeks of data that will be stored on the server, based on the storage capacity of the hard drive, and the number of hits on the server. After inputting the percentage of live data to be stored, the server translates that figure into the equivalent of weekly time periods for live and/or archive data storage.

When the server reaches the maximum number of weeks allocated for live data storage, the oldest week of live data stored on the server attains an archive data status. In attaining an archive data status, the index for that week of data is dropped from the database tables.

When the server reaches its maximum number of weeks allocated for archive data storage, the oldest week of non-indexed data stored on the server is automatically dropped (expired) from the database.

Once data expires, it cannot be recovered.

View Data Storage Statistics

In the Status section of this screen, the date and time of the last database expiration 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 run:

- **Data scope for total data** - the date and time range of all live and archive data currently stored on the server. 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.
- **Total number of week(s) stored** - the number of weeks represented in the total data date scope.
- **Current live data (yearweekno/date scope)** - the range of dates and times of live data currently stored on the server.

The first line displays the range of year(s) and weeks in the YYYYWW format, where “Y” represents the year, and “W” represents the week number in that year (01-52).

The second line displays the first date and time in the range of live data currently stored on the server. The date displays in the YYYY-MM-DD format, and the time displays in military time (1-24 hours) using the HH:MM:SS time format.

The third line displays the last date and time in the range of live data currently stored on the server, using the same format as in the second line of data.

- **Total number of live week(s)** - the number of weeks represented in the live data date scope.

- **Current archive data (yearweekno/date scope)** - the range of dates and times of archive data currently stored on the server.

The first line displays the range of year(s) and weeks in the YYYYWW format, where “Y” represents the year, and “W” represents the week number in that year (01-52).

The second line displays the first date and time in the range of archive data currently stored on the server. The date displays in the YYYY-MM-DD format, and the time displays in military time (1-24 hours) using the HH:MM:SS time format.

The third line displays the last date and time in the range of archive data currently stored on the server, using the same format as in the second line of data.

- **Total number of archive week(s)** - the number of weeks represented in the archive data date scope.
- **Database disk space utilization** - the percentage of space currently being used on the hard drive for both live and archive data. If a high percentage displays, you may want to expire data in the near term (see Change Data Storage Settings).
- **(used database space/total database space)** - the amount of space in Gigabytes currently being used on the hard drive for both live and archive data, and the total amount of space in Gigabytes (Gbytes) on the hard drive allocated to database storage.
- **Target percentage of live data** - the percentage of live data to be stored on the server. If this figure is 100, only live data will be stored. If this figure is less than 100, the remaining percentage to be stored will be archive data.

The percentage that displays can be changed by entering and saving a different figure in the Percentage of live data field in the Change Settings section of this screen.

- **Last 8 weeks hits/day average** - the average number of hits on the server per day, based on the last eight weeks of data stored on the server.

The following data that displays is current as of the last changes made in the Change Settings section of the screen:

- **Estimated total week(s) of live data** - the number of weeks of live data the server will store, based on your specifications. This number is affected by the hits/day on the server, and the maximum number of weeks of data the server is able to hold.

The number of weeks of live data to be stored can be changed by making a new entry in the Percentage of live data field in the Change Settings section of this screen, and saving the result of your calculations that displays below in the Estimated total week(s) of live data field.

- **Estimated total week(s) of archive data** - the number of weeks of archive data the server will store, based on your specifications. This number is affected by the hits/day on the server, and the maximum number of weeks of data the server is able to hold.

The number of weeks of archive data to be stored can be changed by making a new entry in the Percentage of live data field in the Change Settings section of this screen, and saving the result of your calculations that displays below in the Estimated total week(s) of archive data field.

- **Estimated number of week(s) until next expiration** - the number of weeks from this week that data on the server will expire.

Change Data Storage Settings

The Change Settings section of the screen is used for updating the amount of data that will be stored on the server in the future. By making an entry in this section of the screen, you dictate how data on the box will expire.

1. At the Hits/day field, the number of hits on the server per day displays. This is the same figure that displays in the Last 8 weeks hits/day average field in the Status section above.
2. In the **Percentage of live data** field, enter a figure for the percentage of data you wish to be stored as live data on the box. If you want all data to be live data only, enter 100.
3. Click the **Calculate** button to display the Estimated total week(s) of live data and Estimated total week(s) of archive data in the fields beneath the Calculate button.

After viewing your results, you can adjust the number of weeks that data will be saved on the server, if necessary. To do so, follow steps 1 - 3 again.

4. After reviewing and accepting the final calculation(s), click the **Save** button. As a result of your entries, the following occurs:
 - the figure saved in the Percentage of live data field displays in the Target percentage of live data field in the Status section
 - the figures displayed in the Estimated total week(s) of live/archive data fields display in the Estimated total week(s) of live/archive data fields in the Status section
 - the Estimated number of week(s) until next expiration field may display a new figure, based on the new settings you saved.

When the next database expiration runs, all other fields in the Status section will reflect the new calculations.



TIP: M86 Security recommends that you set up your server to store more live data than archive data for the benefit of administrators and sub-administrators who generate reports via the Web Client application. Report processing times are slower when generating reports that include non-indexed data.

If your server is set up to store only live data, you will be able to store less data than if you store both live and archive data, since indexes require additional storage space.



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 Web Client when generating specified types of reports: Search String Reporting, Block Request Count, Blocked Searched Keywords, Wall Clock Time, Object Count. This screen also is used for enabling and configuring the password security feature to be used for the Administrator console and/or Web Client (see Fig. 1-2:34).



NOTE: Optional features can be enabled or disabled at any time.

Enterprise Reporter **M86 SECURITY**

Network | Server | Database | Help Logout

Optional Features

Please select which Enterprise Reporter features you would like to enable or disable. M86 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 R3000 must have Search Engine Keywords enabled and, if applicable, the CER must have the reporting feature turned "Off".

WARNING: Applying the Blocked Searched Keywords settings will restart the web client server.

Wall Clock Time

The "Wall Clock Time 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 days prior to expiration

Lockout by Username

On
 Off

Lockout by IP Address

On
 Off

Allowable Number of Failed Password Attempts

Failed Password Attempts Timespan (in minutes)

Apply

Fig. 1:2-35 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 Request Executive Report can be generated by the administrator.

1. Click the radio button corresponding to “ON” to make the Top 20 Users by Blocked Request Executive Report selection available in an administrator’s Executive Reports menu.
2. Click **Apply** to apply your setting.



NOTE: *Since Executive Reports are processed each night, any changes made to settings today will not effective until the following day.*

Enable Blocked Searched Keywords

If Blocked Searched Keywords is enabled, the Top 20 Blocked Searched Keywords Executive Report can be generated by the administrator.

1. Click the radio button corresponding to “ON” to make the Top 20 Users by Blocked Request Executive Report selection available in an administrator’s Executive Reports menu.
2. Click **Apply** to apply your setting.



WARNING: Applying this setting restarts the Web Client server.



NOTE: Since Executive Reports are processed each night, any changes made to settings today will not be effective until the following day.

Enable Wall Clock Time

If Wall Clock Time is enabled, Wall Clock Time Reports can be generated by the administrator. These reports use the Wall Clock Time 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 Wall Clock Time Report selection available in an administrator’s Custom Reports menu.
2. Click **Apply** to apply your setting.



NOTE: Since Wall Clock Time reports are processed each night, any changes made to settings today will not be effective until the following day.

Enable Page and/or Object Count

In the Object Count frame, indicate whether drill down, Wall Clock Time, 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, Wall Clock Time, 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 Administrator console or Web Client can be set to expire after a specified number of days, and/or lock out the user from accessing the Administrator console and Web Client 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 User Name and Password in the login screen and clicks Login, he/she will be prompted to re-enter his/her User Name 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 ER application.



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 ER application.



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 Web Filter servers to send LDAP user group membership information to this ER, for performing a user group import on demand, and for viewing on demand user group import criteria.

The screenshot displays the 'User Group Import' interface within the Enterprise Reporter application. At the top, the navigation bar includes 'Enterprise Reporter' and the M86 SECURITY logo. Below the navigation bar, there are dropdown menus for 'Network', 'Server', and 'Database', along with a 'Help Logout' link. The main content area is titled 'User Group Import' and contains the following elements:

- Four input fields for 'Web Filter IP' addresses, labeled 'Web Filter IP 1' through 'Web Filter IP 4'. The first field contains the IP address '192.168.20.17'.
- Four checkboxes corresponding to each IP field, labeled 'Import from this Web Filter'. The checkbox for the first IP is checked.
- A button labeled 'More Web Filters'.
- A warning message: 'Importing user groups may take a long time depending on the number of Web Filters and the number of users for each Web Filter.'
- An 'Import Now' button.
- A section titled 'Current Status for User Group Import:' containing a text box with the following status updates:
 - Importing groups from Web Filter 192.168.20.17.....
 - Running dbipgroups
 - Importing user groups finished successfully.

Fig. 1:2-36 User Group Import screen



WARNING: Be sure to import users and user groups whenever modifications are made to usernames in the Username Display Setting screen. See the Username Display Setting screen for information on modifying usernames.

Import User Groups



NOTE: Web Filter IP fields are populated by default if one or more Web Filter servers are connected to this ER.

1. Specify the **Web Filter IP** address of each Web Filter to send LDAP user group membership data to this ER.
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.

ER SERVER APPENDIX SECTION

Appendix A

Evaluation Mode

By default, the ER Server module and Web Client are set to the evaluation mode. This appendix explains how to use the ER in the evaluation mode, and how to activate the ER Server to function in the activated mode.

Administrator Console

When accessing the **Server > Server Status** screen for the first time, the ER Status pop-up box opens to inform you that the ER unit is currently in the evaluation mode:

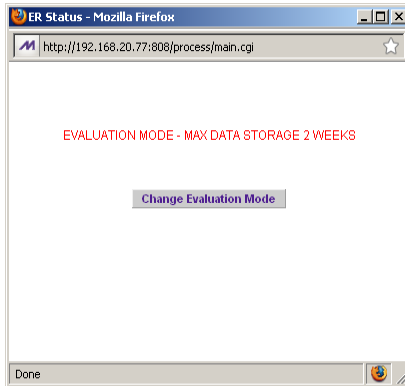


Fig. A-1 ER Status pop-up box

The ER 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 ER’s data storage scope.

You have the option to either use the ER in the evaluation mode, or change the evaluation mode in one of two ways—by extending the evaluation period, or by activating the ER so that it can be used in the activated mode.



NOTE: The message: “EVALUATION MODE - MAX DATA STORAGE ‘X’ WEEKS” also displays at the top of the Expiration screen in the Administrator console. Refer to the Expiration screen sub-section in Chapter 2 of the ER Administrator portion of this user guide 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 ER 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.

The screenshot shows the 'Expiration' screen in Enterprise Reporter M86 Security. The status is as of 2009-12-23 01:27:34. A red banner indicates 'EVALUATION MODE - MAX DATA STORAGE 2 WEEKS'. Below this, a link is provided to activate the box. The main content area lists various data storage statistics:

| | |
|--|--|
| Date scope for total data | 2009-12-11 00:09:26 - 2009-12-23 00:09:44 |
| Total number of week(s) stored | 2 week(s) |
| Current live data (yearweekno/date scope) | 200949 - 200951 2009-12-11 00:09:26 - 2009-12-23 00:09:44 |
| Total number of live week(s) | 2 week(s) |
| Current archive data (yearweekno/date scope) | 0 - 0 0 - 0 |
| Total number of archive week(s) | 0 week(s) |
| Database disk space utilization (used database space/total database space) | 3.44 % (1.73/50.33 Gbytes) |
| Target percentage of live data | 100 % |
| Last 8 weeks hits/day average | 112849 |
| Estimated total week(s) of live data | 226 week(s) |
| Estimated total week(s) of archive data | 0 week(s) |
| Estimated number of week(s) until next expiration | 49 week(s) |

Below the statistics is a 'Change Settings' section with input fields and a 'Calculate' button:

| | |
|---|------------------------------|
| Hits/day | 112849 |
| Percentage of live data | 100 % |
| Estimated total week(s) of live data | <input type="text"/> week(s) |
| Estimated total week(s) of archive data | <input type="text"/> week(s) |

Fig. A-2 Expiration screen

When the ER is in the evaluation mode, the following message displays at the top of the screen: “Evaluation Mode – Max Data Storage ‘X’ Weeks” (in which ‘X’ represents the maximum number of weeks in the ER’s data storage scope).

Since the evaluation period is set for a fixed time period, you cannot make adjustments to the amount of data that will be stored on the Server. Thus, the **Save** button is not included at the bottom of the screen.

Change the Evaluation Mode

After the designated evaluation period has expired, you may extend your evaluation period, or activate the unit and use it in the activated mode. There are two ways to change the evaluation mode from the Administrator console:

- in the ER 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:

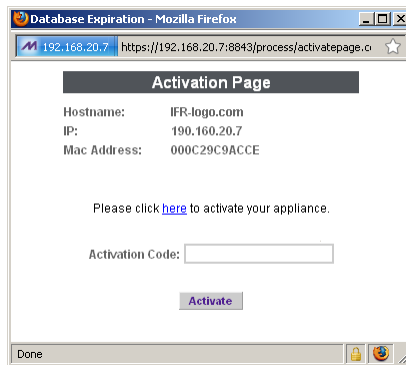


Fig. A-3 Activation Page pop-up box

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 Enterprise 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 activating 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.

WEB CLIENT INTRODUCTORY SECTION

Enterprise Reporter

Though many companies have Internet filtering solutions to prevent employees from accessing inappropriate, non-work related Web sites, simply blocking these sites is not enough. Administrators want the ability to know who is accessing which site, the duration of each site visit, and the frequency of these visits. This data can help administrators identify abusers, develop policies, and target sites to be filtered, in order to maximize bandwidth utilization and productivity.

The Enterprise Reporter (ER) from M86 Security is designed to readily obtain this information, giving the user 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.

Operations

In simplified terms, the ER operates as follows: the ER Server accepts log files (text files containing Web access data) from a source device such as the M86 Web Filter. M86 Security’s proprietary programs “normalize” the transferred data and insert them into a MySQL database. The ER Web Client reporting application accesses this database to generate a virtually unlimited number of queries and reports.

About this Portion of the User Guide

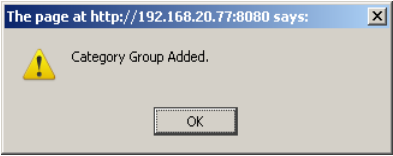



The Enterprise Reporter Web Client portion of the user guide addresses the administrators designated to configure the ER Server module and the ER Client, and the sub-administrator(s) given permission by the Client administrator to use the Client.

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

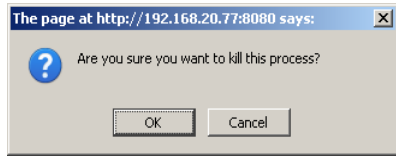
- **Web Client Introductory Section** - This section provides an overview and information on how to use this portion of the user guide to help you access the Client and become familiarized with the application.
- **Web Client Administrator Section** - This section includes information for administrators to configure the Client application.
- **Web Client User Section** - This section includes information on using the Client application to generate reports.
- **Web Client Appendices Section** - Appendix A provides information on how to use the ER Client in the evaluation mode, and how to switch to the activated mode. Appendix B includes information on configuring Lotus Notes to work with Client application reports, instead of Microsoft Outlook. Appendix C includes a glossary of terms 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.

- **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, window, or screen that can be clicked with your mouse to execute a command.

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


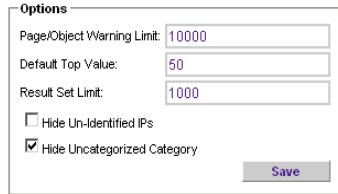
- **dialog box** - a box that opens in response to a command made in a window or screen, and requires your input. You must choose an option by clicking a button (such as “Yes” or “No”, or “Next” or “Cancel”) to execute your command. As dictated by this box, you also might need to make one or more entries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



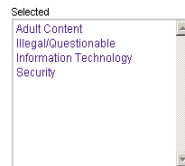
- **field** - an area in a dialog box, window, or screen that either accommodates your data entry, or displays pertinent information. A text box is a type of field.



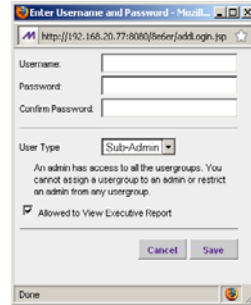
- **frame** - a boxed-in area in a dialog box, window, or screen that includes a group of objects such as fields, text boxes, list boxes, buttons, and/or radio buttons. Objects within a frame belong to a specific function or group. A frame often is labeled to indicate its function or purpose.



- **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 screen that accommodates and/or displays entries of items that can be added or removed.



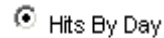
- **pop-up box or pop-up window** - a box or window that opens after you click a button in a dialog box, window, or screen. This box or window may display information, or may require you to make one or more entries. Unlike a dialog box, you do not need to choose between options.



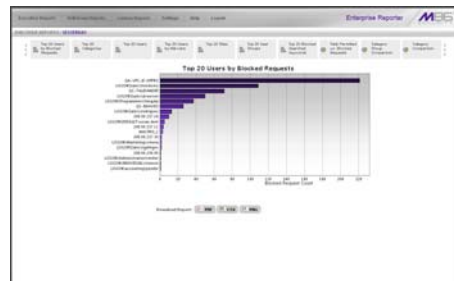
- **pull-down menu** - a field in a dialog box, window, or screen that contains a down arrow to the right. When you click the arrow, a menu of items displays from which you make a selection.



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



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



- **text box** - an area in a dialog box, window, or screen that accommodates your data entry. A text box is a type of 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** - displays on a screen, and can contain frames, fields, text boxes, list boxes, icons, buttons, and radio buttons. Types of windows include ones from the system such as the Save As window, pop-up windows, or login windows.



Getting Started

This sub-section helps the ER Client administrator and ER Client sub-administrator become familiarized with basic log in and log out procedures, and navigating the screen of the ER Web Client.

Before getting started, the administrator of the ER Administrator module needs to configure the software components described in the following Web Client Administrator Section. The ER Client administrator should then set up his/her unique password for accessing the Web Client. Finally, the ER Client administrator must set up each designated sub-administrator with permissions in order for an authorized user to use the ER Client.

Procedures for Logging On, Off

Access the ER Web Client Login window

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

- by clicking the Enterprise Reporter icon in the SR Welcome window (see Access ER Web Client from the SR Portal)
- by launching an Internet browser window supported by the ER Web Client and then entering the ER Web Client's URL in the Address field (see Enter ER Web Client's URL in Address field)

Access ER Web Client from the SR Portal

Click the Enterprise Reporter icon in the SR Welcome window:



Fig 1:1-1 Enterprise Reporter icon in SR 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 SR Appendix I: Disable Pop-up Blocking Software.*

Clicking the Enterprise Reporter icon opens a separate browser window/tab containing the ER Web Client Login window (see Fig. 1:1-2).

Enter ER Web Client's URL in Address field

1. Launch an Internet browser window supported by the ER Web Client.
2. In the address line of the browser window, type in "https://" and the ER Web Client's IP address or host name, and use port number ":8443" for a secure network connection, plus "/8e6er".

For example, if your IP address is 210.10.131.34, type in **https://210.10.131.34:8443/8e6er/**. Using a host name example, if the host name is logo.com, type in **https://logo.com:8443/8e6er/**.

With a secure connection, the first time you attempt to access the ER Web Client'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-sr.pdf>***

3. After accepting the security certificate, click **Go** to open the ER Web Client Login window (see Fig. 1:1-2).

Log In



NOTE: A maximum of eight users can use the Web Client simultaneously. However, for optimum results, M86 Security recommends no more than four users generate reports at the same time.

1. In the login window, type in the generic Username **manager**, and Password **8e6Report**, if you have not yet set up your own user name and password. Otherwise, enter your personal **Username** and **Password**:



Fig. 1:1-2 Login window

2. Click **Login** to open the application.



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

Administrators who access the Client application for the first time should change the administrator password. This ensures that only the administrator will be able to access information for all user groups. The administrator username and password is modified in the User Permissions window, accessible via User Permissions option from the Settings menu. (See the Web Client Administrator Section for information on the User Permissions window.)



NOTE: If your password has been set by the administrator to expire after a specified number of days, upon clicking the **Login** button, the login window re-displays with a message informing you that your password has expired.

The screenshot shows the 'Enterprise Reporter' login interface. At the top left, it says 'Enterprise Reporter' and at the top right is the 'M86 SECURITY' logo. A message reads: 'Your account has expired. Please change your password to login.' Below this, the 'Username' field contains 'manager'. The 'Password' and 'Confirm Password' fields are both filled with eight dots. A 'Change Password' button is located below the password fields. At the bottom of the window, it says 'Server: 192.168.20.77'.

Fig. 1:1-3 Client Login window, password expired

Beneath your displayed Username, enter eight to 20 characters for the new password in both the **Password** and **Confirm Password** fields, including at least one alpha character, one numeric character, and one special character. The password is case sensitive. Click **Change Password** to open an alert box confirming the changed password activity. Click **OK** to close the alert box and to open the application.

If logging in as an administrator—or as a sub-administrator with authorization to view Executive Reports—by default, yesterday’s pre-generated (canned) report displays in the screen, including thumbnail images in the “dashboard” above the report. A list of menu topics and sub-topics display in the navigation toolbar above the screen:

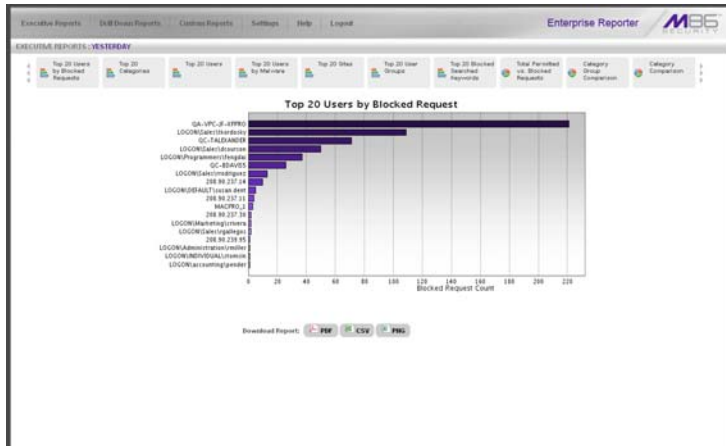


Fig. 1:1-4 Default Executive Report, administrator ID



NOTES: If the ER Server module does not contain any data—as on a newly installed unit—the default report page will not show any thumbnail images or bar chart report, and the following text displays: “This report cannot be displayed because there is no data to show for this report.”

On a new unit or a unit with a newly-applied software update, the following message may display on the screen instead of the default report: “The report cannot be displayed because there is no data to show for this report at this time. For a new server, it takes about 24 hours before data is available for processing. If a software update was recently applied on an existing server, it may take several hours before data is available.”

If logging in as a sub-administrator, by default the Custom Wizard Report displays if authorization was not granted for this account to access Executive Reports:

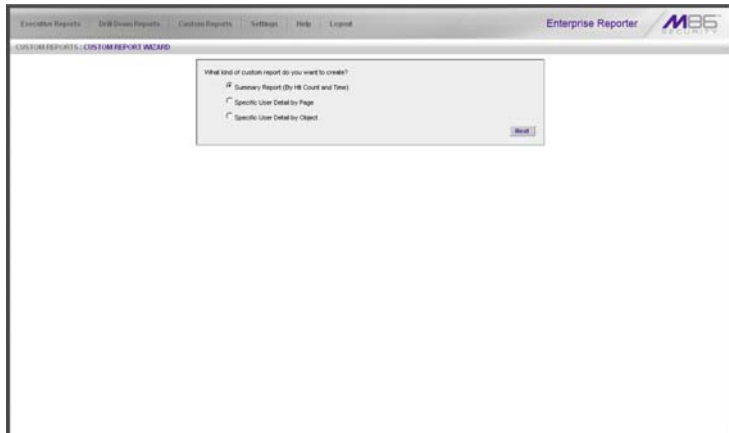



Fig. 1:1-5 Default screen, sub-administrator ID

 **TIP:** User permissions are set up by the administrator via the User Permissions option, available from the Settings menu.

Client Screen Navigation

Links in the Navigation Toolbar

The navigation toolbar at the top of the screen consists of the following links and menu topics for configuring and using the Client:

- **Executive Reports** - mouse over this link to open the Executive Reports menu. Administrators and authorized sub-administrators can click any Executive Report menu option to obtain an overview of end user Internet activity. This link does not display for sub-administrators who are not authorized to view Executive Reports.
- **Drill Down Reports** - mouse over this link to open the Drill Down Reports menu. These menu options let you drill down into reporting data to identify specific Internet usage criteria.
- **Custom Reports** - mouse over this link to open the Custom Reports menu. These menu options let you generate, edit, save, and/or run reports customized to your specifications.
- **Settings** - mouse over this link to open the Settings menu. These menu options let you customize the Client application.
- **Help** - mouse over 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** - mouse over this link to log out of the Client (see Log Out for details on log out procedures).



NOTE: *More about buttons, thumbnails, icons, and the navigation toolbar—and the functions of the corresponding windows and screens for these tools—can be found in the Web Client Administrator Section and Web Client User Section of this portion of the user guide.*

Using the Client

1. Before you can begin using the Client, the ER Server administrator must customize the ER Server module for using the Client.
2. Next, the Client administrator should customize the Client application's settings via the Settings option.
3. Once the ER Server module and the Client have been customized, the database can be queried and report views generated for the reporting type of your choice: Executive Report (administrators and authorized sub-administrators only), Drill Down Report, Custom Report.
4. A report view can be exported in a specified file format, printed, emailed, and/or saved.
5. A saved report can be scheduled to run at a given time.

Log Out

To log out of the Client application, click the **Logout** button in the navigation toolbar to re-display the login window.

Click the "X" in the upper right corner of the logout window or tab to close the window/tab.

Exiting the Client application will log you out of the ER Client, but will not log you out of the SR server, nor turn off the server.



WARNING: *If you need to turn off the SR server, follow the shut down procedures outlined in the Shut Down screen sub-section under the Server Menu section in Chapter 2 of the ER Administrator Section of the Enterprise Reporter portion of this user guide. Failure to properly shut down the server can result in data being lost or corrupted.*

Re-login

Each Client session is timed so that it remains active as long as there is activity in the Client within an eight hour period. You need to log into the Client again after an eight hour period of inactivity, or in the event that the ER Server module was restarted.

If your Client session is timed out, when you click a button, thumbnail, or menu item in the Client report screen, the following message displays: “Your session may have timed out, or the Web server has been restarted. Please close your browser window and open a new browser window to log back in to the ER Web Client.”

To log in again, perform one of two actions:

- Close your browser window, and then open a new browser window/tab to log back into the Client.
- In your current browser window/tab, click **Logout** to log out of the Client. This action opens the login window so you can log back into the Client again.

WEB CLIENT ADMINISTRATOR SECTION

Introduction

This section of this portion of the user guide provides instructions to administrators on how to set up the ER Web Client application for sub-administrators to use. Information on generating Executive Reports is also included.

Before the Client application can be used, the ER Server module must 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).

After verifying that the necessary components are installed, configured, and functioning, the Client administrator can begin setting up the Client application for sub-administrators.



NOTE: Information about the ER Server module can be found in the ER Administrator portion of this user guide.

Chapter 1: Installation and Maintenance

Environment Requirements

ER Server module

- ER Server module must 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)

Workstation

The following components must be installed in order to use the Client:

- Windows XP, Vista, or 7 Operating Systems running Internet Explorer (IE) 7 or 8, or Firefox 3.5 for Client usage
- Macintosh OS X Version 10.5 or 10.6 running Safari 4.0 or Firefox 3.5 for Client usage

The following minimum environment requirements must be fulfilled in order to use the Client:

- Pentium III class processor or greater
- 512 MB RAM minimum, 1 GB RAM recommended
- 2 GB hard drive space for saving files
- screen resolution settings of 1024 x 768 are recommended
- if pop-up blocking software is installed on the workstation, it must be disabled



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

Client Updates

Updates for the Client are available in ER software releases that are downloaded to the SR server. Once applied to the ER Server module, Client users will be able to obtain all the new features and enhancements currently available.



NOTES: *After installing a software update, the following message may display in the screen instead of the default report: “The report cannot be displayed because there is no data to show for this report at this time. For a new server, it takes about 24 hours before data is available for processing. If a software update was recently applied on an existing server, it may take several hours before data is available.”*

Refer to the Software Update screen sub-section in the ER Administrator portion of this user guide for information about installing software updates on the ER Server module.

Chapter 2: Configuring the Client

Settings

To begin configuring the Client, mouse over the **Settings** link in the navigation toolbar to open its menu of customization options:

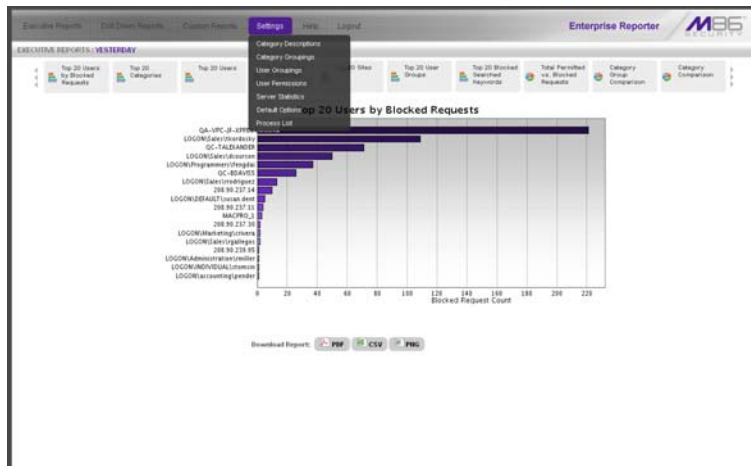


Fig. 2:2-1 Settings menu (administrator), default Executive Report

Click an option in the Settings menu to display the specified window in the panel. The following options are available to administrators: Category Descriptions, Category Groupings, User Groupings, User Permissions, Server Statistics, Default Options, and Process List.



NOTE: Information about Server Statistics and Default Options—available to both administrators and sub-administrators—can be found in Chapter 2 of the Web Client User Section.

Category Descriptions

The Category Descriptions option is used for viewing category names and descriptions of filtering categories used by the Web access logging device(s).



NOTE: When logs are imported each hour, new library categories are automatically entered and will display when the Client is accessed.

To view details on a filter category, click Category Descriptions in the Settings menu to display the Category Descriptions window in the panel:

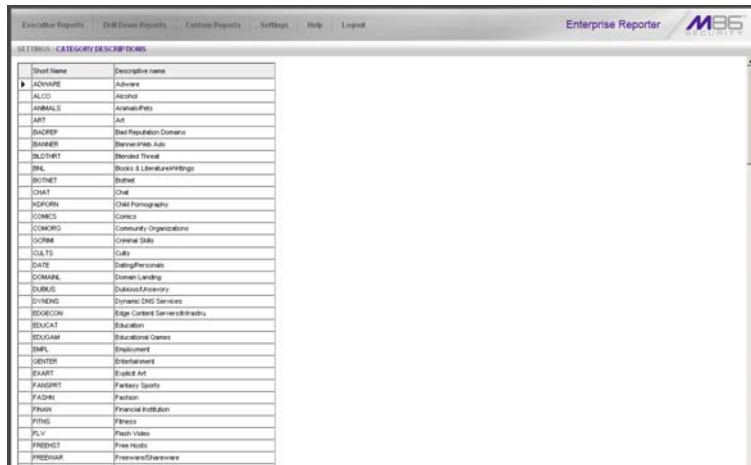


Fig. 2:2-2 Category Descriptions window

View Details for a Filter Category

In the Category Descriptions window, filter categories display as rows of records. The following information is included for each record: Short Name of the category and its corresponding Descriptive name.

In the Record field at the bottom of the window, the number of the selected record displays, along with the total number of records (categories).



TIP: *The selected record is designated by an arrow in the box to the left of a row. To select another record, click the box in that row to display the arrow. You also can navigate to another record by using the Record navigation field. Click in the box between the arrow buttons and enter a new record number to go to that record. Or click any of the four arrow buttons to advance forward or backward through the list of records. In the order in which they display in the Record field, clicking these buttons moves you to the first record, the record prior to the selected record, the record following the selected record, and the last record.*

Category Groupings

The Category Groupings option is used for defining a customized group of filter categories, if you wish to run reports using certain filter categories only.

To create, edit, or delete a category group, click Category Groupings in the Settings menu to display the Category Groupings window in the panel:



Fig. 2:2-3 Category Groupings window

The Category Groupings window is comprised of two frames used for setting up and maintaining category groupings: Group Information, and Group Definitions.

Group Information frame

The Group Information frame displays to the left in the Category Groupings window. In this frame you can add, rename, or delete a category group.

Any category groups that were created display in alphanumerical order in the list box in this frame.

Add a Category Group

1. In the field to the left of the Add button, type in the name for the category group.
2. Click the **Add** button to add this entry to the list box above.



NOTE: *The category group you added also displays in the Group Name pull-down menu in the Group Definitions frame to the right.*

Rename a Category Group

1. Select the category group from the list box by clicking on your choice to highlight it.
2. Click the **Rename** button to open the Group Rename dialog box:

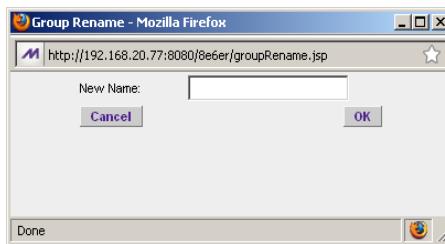


Fig. 2:2-4 Edit a Category Group Name

3. In the **New Name** field, enter the new category group name.



TIP: Click **Cancel** if you wish to return to the *Category Groupings* window without saving your modifications.

4. Click **OK** to close the Group Rename dialog box and to update the list box in the Group Information frame with your edits.



NOTE: The category group you renamed also displays in the *Group Name* pull-down menu in the *Group Definitions* frame to the right.

Delete a Category Group

1. Select the category group from the list box by clicking on your choice to highlight it.
2. Click the **Delete** button to remove the category group from the list box.



NOTE: The category group you deleted also is removed from the *Group Name* pull-down menu in the *Group Definitions* frame to the right.

Group Definitions frame

The Group Definitions frame displays to the right in the Category Groupings window. In this frame you define a category group by specifying which categories will belong to that group.

Add Categories to a Category Group

1. Select a category group from the **Group Name** pull-down menu. Any categories previously entered display in the list box in this frame.
2. Click the **Add To Group** button to open the Add To Group pop-up box:

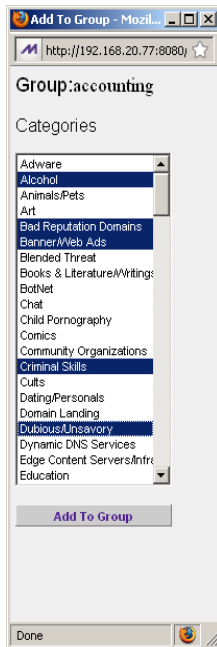


Fig. 2:2-5 Add To Group

3. Select a category from the pop-up box by clicking on your choice to highlight it.



TIP: To select multiple categories, press the *Ctrl* key on your keyboard and then click on categories to highlight them.

4. Click the **Add To Group** button in the pop-up box to specify the selected categories to be added to the Group Definitions frame list box.
5. Click the "X" in the upper right corner of the Add To Group pop-up box to close it, and to add all selected categories to the list box in the Group Definitions frame.

Delete a Category from a Category Group

1. Select a category group from the **Group Name** pull-down menu to display all categories for that category group in the list box.
2. Select the category to be removed by clicking on your choice to highlight it.
3. Click the **Delete Item(s)** button to remove the category from the list box for that category group.

User Groupings

The User Groupings option is used for defining a customized group of users, if you wish to run reports for certain users only.

To create, edit, or delete a user group, click User Groupings in the Settings menu to display the User Groupings window in the panel:

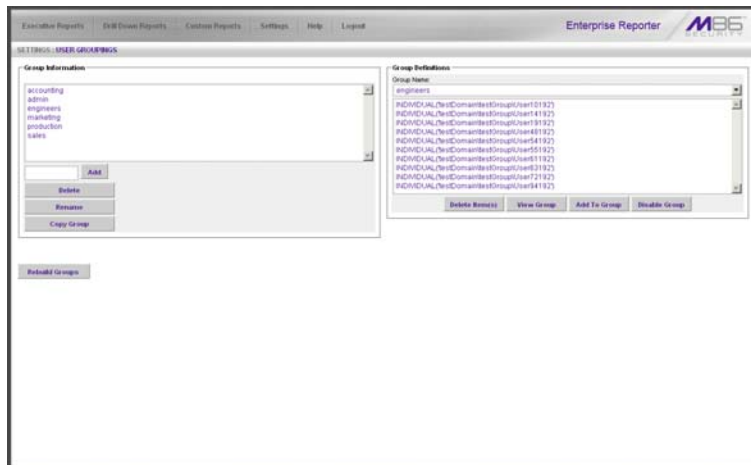


Fig. 2:2-6 User Groupings window

The User Groupings window is comprised of two frames used for setting up and maintaining user groupings: Group Definitions and Group Information.

After making all additions, modifications, or deletions in this window, click **Rebuild Groups**.



NOTES: *When clicking Rebuild Groups, the window becomes blank and displays the following message: “Please wait while the groups are being rebuilt...”. When the user groups have been rebuilt, the window refreshes itself and becomes available again.*

Reports for a newly-created user group will only be available after the user group is created, even though reporting data may be available for each individual user prior to the time the user group was created.

Group Definitions frame

The Group Definitions frame displays to the left in the User Group Setup window. In this frame you can view members of a user group, define any non-imported user group by specifying which users will belong to that group, and indicate whether or not to disable a user group.

View a List of Users in a User Group

1. Select a user group from the **Group Name** pull-down menu. Users set up for that group display in the list box in this frame.
2. To view the entire list of users in the format used on the server, click the the **View Group** button to open the Users in the ‘user group’ pop-up box:

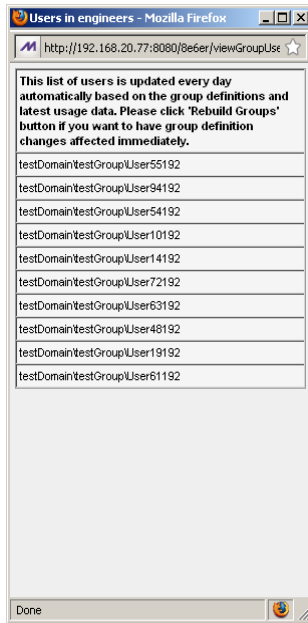


Fig. 2:2-7 Users in user group pop-up box

Each user included in the user group displays as a separate row in this pop-up box.



NOTE: If you have just copied or created a new user group, the pop-up box does not yet show any users and the following message displays: “Sorry there are no Users in the ‘X’ group at this moment.” (in which ‘X’ represents the group name). Any modifications just made to a user group will not immediately display, since the list of users is updated automatically each hour based on the group definitions and latest usage data. In order to have group definition changes effective immediately, click **Rebuild Groups**.

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

Define a User Group

When defining a user group, you can add and/or exclude users to/from that group—unless the group was imported to the ER Server module from a Web Filter's LDAP server, since imported user group data cannot be edited. Modifications to a non-imported user group can be made at any time, as necessary.

1. Select a non-imported user group from the **Group Name** pull-down menu. Users set up for that group display in the list box in this frame.
2. Click the **Add To Group** button to open the pop-up box where you define users to be added/excluded to/from the group:

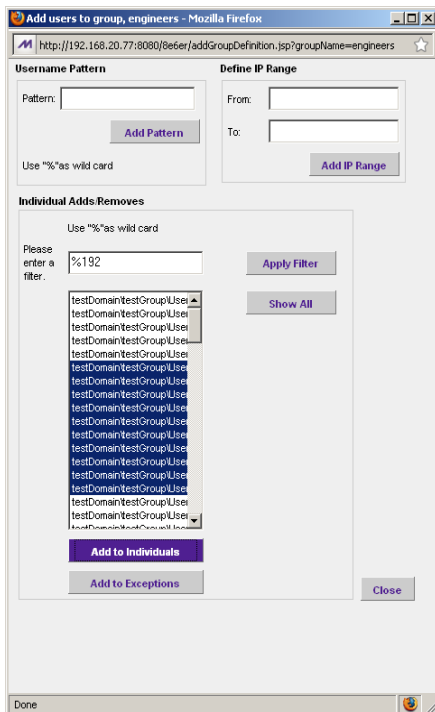


Fig. 2:2-8 Add Users to group



TIPS: To view a list of all users, go to the *Individual Adds/Removes* frame and click the *Show All* button to display the list of users in the list box.

To clear your entries in this pop-up box without accepting them, **do not** click any of the buttons in the frames described below. Instead, click the *Close* button in the pop-up box, and return to step 1.

3. Make entries in one of the three frames:

- **Username Pattern** - This frame is used for including users from a specific group (such as “sales”) on the network. In the **Pattern** field, enter the appropriate characters and wild card “%” to add specified users to the group. For example, type in **sales%** to add anyone to the group who has a “sales” designation on your network. Click the **Add Pattern** button to add the pattern.
- **Define IP Range** - This frame is used for including users based on a range of IP addresses. For example, you might have one range of IP addresses for sales, and another for admin. Enter the IP address range in the **From** and **To** fields. Click the **Add IP Range** button to add the IP address range.
- **Individual Adds/Removes** - This frame is used for including and/or excluding specified users. Click the **Show All** button to display a list of all users in the list box. To narrow down the list of users, make an entry in the **Please enter a filter** field using the “%” wild card, and click the **Apply Filter** button to only display the users you specified. To select from users in the list box, click on the user(s) to highlight your choice(s). After making all choices, click **Add to Individuals** to include the selected users to the group, or click **Add to Exceptions** to exclude the users from the group.



TIP: In the Individual Adds/Removes frame, if you know which users you would like to add/exclude to/from the group, you can bypass the step for showing all users and making your selections. To use this shortcut, enter the criteria in the Please enter a filter field along with the “%” wild card, and then click the Apply Filter button to display your results in the list box.

4. After you have made your entries, click **Close** to close the pop-up box.

The following information displays in the Group Definitions frame list box when a selection for the group is made from the Group Name pull-down menu:

- If an entry was made in the Username Pattern frame, “PATTERN” and the character(s) you entered display(s).
- If entries were made in the IP Range frame, “IP RANGE(‘X.X.X.X’ AND ‘X.X.X.X’)” displays, in which ‘X.X.X.X’ represents the IP address that was entered in the From or To field.
- If entries were made in the Individual Adds/Removes frame, “INDIVIDUAL(...)” and/or “EXCEPTION(...)” displays, in which ‘(...)’ represents specific details about the entry.



NOTE: A combination of any of items above may display in the Group Definitions frame list box, based on entries you made in any of the frames in the pop-up box.

Disable a User Group

1. Select a user group from the **Group Name** pull-down menu. Users set up for that group display in the list box in this frame.
2. Click the **Disable Group** button to exclude the user group from reports.



TIPS: This function for specifying which user groups will not be included in reports is useful in conjunction with the Copy Group function—disabling an imported user group but enabling its copied counterpart.

Any user group that is currently disabled can be enabled by selecting the Group Name and clicking Enable Group.

Delete User(s) from User Group

1. Select a user group from the **Group Name** pull-down menu. Users set up for that group display in the list box in this frame.
2. Click on the user to highlight your selection.



TIP: To select multiple users, press the *Ctrl* key on your keyboard and then click on the users to highlight them. To select a block of users, click the first user, press the *Shift* key on your keyboard, and then click the last user.

3. Click the **Delete Item(s)** button to remove the user(s) from the user group.

Group Information frame

The Group Information frame displays to the right in the User Group Setup window. In this frame you can add, rename, copy, or delete a user group.

Any user groups that were created display in the list box in this frame, along with any LDAP user groups imported from the Web Filter to the ER Server module.

Add a User Group

1. In the field to the left of the Add button, type in the name for the user group.
2. Click the **Add** button to add this entry to the list box above.



NOTE: The user group you added also displays in the Group Name pull-down menu in the Group Definitions frame to the left.

Rename a User Group

1. Select the user group from the list box by clicking on your choice to highlight it.
2. Click the **Rename** button to open the Group Rename dialog box:

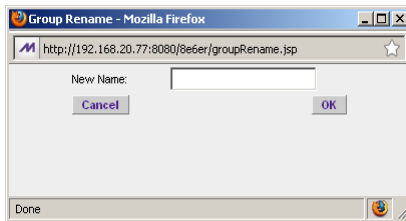


Fig. 2:2-9 Group Rename dialog box

3. In the **New Name** field, enter the new user group name.



TIP: Click **Cancel** if you wish to return to the User Groupings window without saving your modifications.

4. Click **OK** to close the Group Rename dialog box and to update the list box in the Group Information frame with your edits.



NOTE: *The user group you renamed also displays in the Group Name pull-down menu in the Group Definitions frame to the left.*

Copy a User Group

The Copy Group feature is useful when importing an LDAP user group from a Web Filter server, since imported LDAP user groups cannot be modified, but any copied user group can be modified.

1. Select the user group from the list box by clicking on your choice to highlight it.
2. Click the **Copy Group** button to add the copied user group name to the list box, with “-Copied” appended to the name.



NOTE: *The user group you copied also displays in the Group Name pull-down menu in the Group Definitions frame to the right.*

Delete a User Group

1. Select the user group from the list box by clicking on your choice to highlight it.
2. Click the **Delete** button to remove the user group from the list box.



NOTE: *The user group you deleted also is removed from the Group Name pull-down menu in the Group Definitions frame to the right.*

User and Group Permissions

The User and Group Permissions option is used for creating and maintaining user accounts so that administrators and authorized sub-administrators can view reports for their group(s) and change their own passwords. This option requires user groups to be set up via the User Groupings option from the Settings menu.

To assign permissions, or to edit permissions that have been assigned, click User Permissions in the Settings menu to display the User and Group Permissions window in the panel:



Fig. 2:2-10 User and Group Permissions window

Using the User and Group Permissions window, you can maintain the list of sub-administrators and user groups.

Add User

When adding a user who will be authorized to use the Client, you must first: Set up the user's username and password, specify if the user will have rights as an administrator or sub-administrator, and then indicate if the user will be able to access Executive Reports. Next, you must specify the user group(s) to which the user will belong.

1. Click the **Add User** button to open the Enter Username and Password dialog box:

Fig. 2:2-11 Add User

2. In the **Username** field, enter up to 20 characters without spaces—this may include upper- and/or lowercase alphanumeric characters, and special characters.
3. 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.
4. Type in the same characters in the **Confirm Password** field.
5. Indicate the **User Type** by selecting the level of user permissions (“Admin” or “Sub-Admin”). An administrator

will have access to all features in the Web Client, and will have access to all user groups. A sub-administrator will only be able to manage his/her account and user groups assigned to him/her.

6. An administrator has access to all Executive Reports. For a sub-administrator, specify if this user will be **Allowed to View Executive Report** by clicking the corresponding checkbox.



TIP: Click **Cancel** if you wish to return to the Sub-Admin and Group Information window without saving your entries.

7. Click **Save** to add the user to the list of available users.



NOTE: The list of administrators and sub-administrators can be viewed in the User Information dialog box, accessible by clicking **Edit All Users**. If a sub-administrator was added, the username additionally is included in the Sub-Admin pull-down menu in the Sub-Admin Information frame and also displays in the Add Sub-Admin pull-down menu in the Group Information frame.

If a sub-administrator was just added to the list, you must now add at least one user group to the sub-administrator's account by making entries in either the Sub-Admin Information frame or the Group Information frame. While both frames contain similar contents, each serves a different function. The Sub-Admin Information frame is used for maintaining a list of authorized sub-administrators, while the Group Information frame is used for maintaining user groups.

Sub-Admin Information frame

In the Sub-Admin Information frame, you can add a user group to the sub-administrator's account, or remove a user group from the sub-administrator's account.



NOTE: *User groups will not show up in the sub-administrator's generated reports until the following day.*

Add User Group to a Sub-Admin

1. Select the **Sub-Admin** from the pull-down menu. If any user groups have been added to the sub-administrator's account, these groups display in the list box below.
2. From the **Add To Group** pull-down menu, select the group to be added to the sub-administrator's account.
3. Click **Go** to add the user group to the sub-administrator's account, and to display the group name in the list box above.

Remove User Group from a Sub-Admin

1. Select the **Sub-Admin** from the pull-down menu. The sub-administrator's group(s) display(s) in the list box below.
2. Select the group to be removed from the sub-administrator by clicking on your choice to highlight it.
3. Click the **Delete Group From Sub-Admin** button to remove the group from sub-administrator's account and from the list box.

Group Information frame

In the Group Information frame, you update user groups by adding or removing sub-administrators.

Update User Group by Adding a Sub-Admin

1. Select the **Group** from the pull-down menu. Any sub-administrator added to this user group displays in the list box below.
2. From the **Add Sub-Admin** pull-down menu, select the sub-administrator to be added to the group.
3. Click **Go** to display the sub-administrator's username in the list box above.

Update User Group by Removing a Sub-Admin


1. Select the **Group** from the pull-down menu. Any sub-administrators added to this user group display in the list box below.
2. Select the sub-administrator to be removed from the group by clicking on your choice to highlight it.
3. Click the **Remove Sub-Admin From Group** button to remove the sub-administrator from the list box.

Edit Password, Change Permissions, Delete User

Click the **Edit All Users** button in the Sub-Admin and Group Information window to open the User Information dialog box:

Fig. 2:2-12 Edit user password, change permissions, delete user

In this dialog box you can modify an administrator or sub-administrator's password, change a sub-administrator's permissions for accessing Executive Reports, or delete an administrator or sub-administrator from the user list.

 **TIP:** Click *Cancel* if you wish to close the dialog box and return to the Sub-Admin and Group Information window without saving any edits.

Change a User's Password

1. In the User Information dialog box, select the username of the administrator or sub-administrator from the **Username** pull-down menu.
2. In the **Password** field, type in the new password using eight to 20 characters—including at least one alpha character, one numeric character, and one special character. The password is case sensitive.

- Press the Tab key on your keyboard to move to the **Confirm Password** field, and type in the same characters you entered in the Password field.

Database Process List

The Database Process List option is used for viewing or halting a process that is currently running.

To access information about current processes, click Process List in the Settings menu to display the Process List window in the panel:

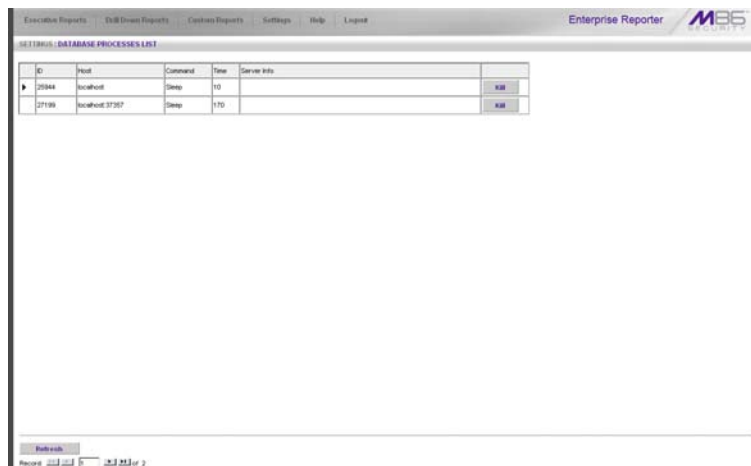


Fig. 2:2-13 Process List window

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 (“Killed”, “Query”, “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).

in the Record field at the bottom of the window, the number of the selected record displays, along with the total number of records.

Click the **Refresh** button to refresh the list of records.



TIP: *The selected record is designated by an arrow in the box to the left of a row. To select another record, click the box in that row to display the arrow. You also can navigate to another record by using the Record navigation field. Click in the box between the arrow buttons and enter a new record number to go to that record. Or click any of the four arrow buttons to advance forward or backward through the list of records. In the order in which they display in the Record field, clicking these buttons moves you to the first record, the record prior to the selected record, the record following the selected record, and the last record.*

Terminate a Process

1. Select the process to be terminated and click **Kill**. This action opens a dialog box with the message: “Are you sure you want to kill this process?”



WARNING: *Be sure that you do not kill the wrong process.*



TIP: *Click Cancel to resume the process and to close the dialog box.*

2. Click **OK** to terminate the process. After the process is killed, an alert box opens displaying the message: “Process Killed!”
3. Click **OK** to close the alert box.

WEB CLIENT USER SECTION

Introduction

This section of the user guide provides instructions to sub-administrators on how to utilize the Client application to generate report views and interpret results.

Chapter 1: Installation Requirements

The following components must be installed in order to use the Client:

- Windows XP, Vista, or 7 Operating Systems running Internet Explorer (IE) 7 or 8, or Firefox 3.5 for Client usage
- Macintosh OS X Version 10.5 or 10.6 running Safari 4.0 or Firefox 3.5 for Client usage

The following minimum environment requirements must be fulfilled in order to use the Client:

- Pentium III class processor or greater
- 512 MB RAM minimum, 1 GB RAM recommended
- 2 GB hard drive space for saving files
- screen resolution settings of 1024 x 768 are recommended
- if pop-up blocking software is installed on the workstation, it must be disabled



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

Chapter 2: Customizing the Client

This chapter provides information on customizing the Client to generate reports based on your specified settings.

Settings

To begin customizing the Client, log in to the Client, then mouse over the **Settings** link in the navigation toolbar to open a menu of customization options:

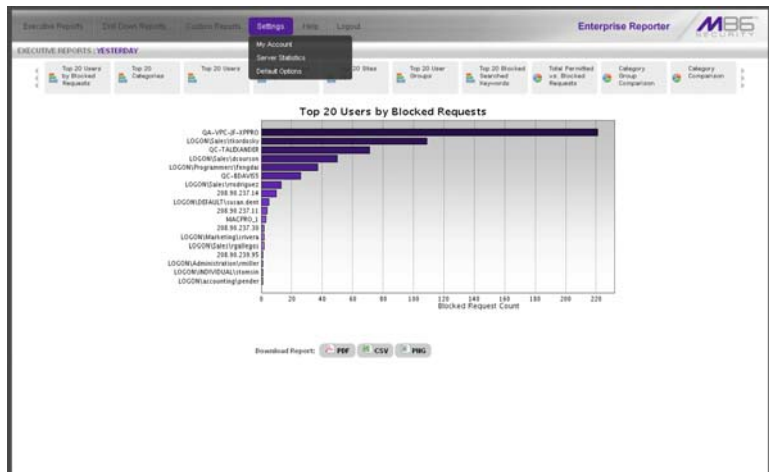


Fig. 3:2-1 Settings menu (sub-administrator), default Executive Report

Click an option in the Settings menu to display the specified window in the panel. The following options are available to sub-administrators: My Account, Server Statistics, and Default Options.

My Account

The My Account option displays only for sub-administrators who have been set up by the administrator to use the Client. My Account is used for viewing a list of users who are included in your user group(s), and for updating your password.

To access your account, click My Account in the Settings menu to display the My Account window in the panel:

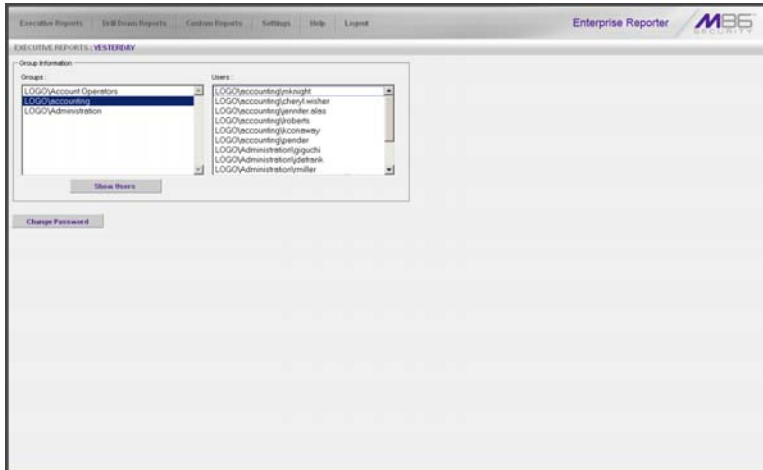


Fig. 3:2-2 My Account window


Upon accessing My Account, any user group to which your username has been assigned (via the User Permissions option from the Settings menu) displays in the Groups list box.

View Users in a User Group

To view a list of users in your user group:

1. In the Groups list box, select the user group by clicking on your choice to highlight it.

2. Click the **Show Users** button to display the users in the Users list box to the right (see Fig. 3:2-2).

 **TIP:** If there is another user group listed that you wish to view, follow the steps above to view the usernames in that user group.


Change Password

1. Click the **Change Password** button to open the Change User Password dialog box:



Fig. 3:2-3 Change User Password

2. Type in the **Old Password**.
3. Type in the **New Password**, entering eight to 20 characters—including at least one alpha character, one numeric character, and one special character. The password is case sensitive.
4. Type in the same characters for the new password in the **Confirm New** field.

 **TIP:** Click **Cancel** if you wish to return to the My Account box without saving your entries.

5. Click **OK** to save your settings.

ER Server Information

The ER Server Information window contains details about data storage on the ER Server module, the time the Web Client Server was last restarted, and the ER Server module's IP address and current software version number.

Click Server Statistics in the Settings menu to display the ER Server Information window in the panel:

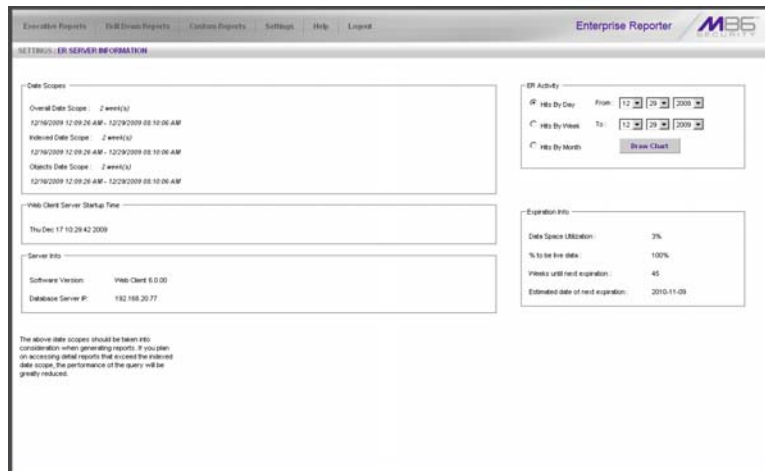


Fig. 3:2-4 ER Server Information window

This window is comprised of five frames: Date Scopes, ER Activity, Web Client Server Startup Time, Server Info, and Expiration Info.



NOTES: *The following message displays on a newly-installed ER: “Server statistics are not available at this time. If the ER server was newly installed, server statistics will be available after the first time statistics are correlated for the server. Server statistics are correlated immediately after midnight, Monday through Saturday. If this problem persists, please contact your system administrator.”*

Date Scopes

In the Date Scopes frame, the number of week(s) of data stored on the ER Server module, and the date and time range display for the following date scopes:

- **Overall Date Scope** - this date scope pertains to all data currently stored on the Server module, including both live (indexed) and archive (non-indexed) data.
- **Indexed Date Scope** - this date scope pertains only to live data currently stored on the Server module. Live data can include Web pages and objects, and will always include the indexes for these items. Objects include images from Web pages, and items such as JavaScript files and flash files.
- **Objects Date Scope** - this date scope pertains only to objects currently stored on the Server module. If this date scope overlaps the date ranges for indexed and non-indexed data currently stored on the Server module, both live and archive items will be included in this date scope.

Web Client Server Startup Time

The Web Client Server Startup Time frame contains the following information pertaining to the last time the Web Client Server 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 Web Client Server has restarted and terminated the report generation process.*

Server Info

The Server Info frame contains the following ER Server module information: **Software Version** number and **Data-base Server IP** address.

ER Activity

In the ER Activity frame, 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.

By default, the **Hits By Day** radio button is selected, and in the From and To fields, today’s date displays in the MM, DD, and YYYY format.

1. Specify the time period for the chart you wish to draw by doing the following:
 - Click the radio button corresponding to **Hits By Day**, **Hits By Week**, or **Hits By Month**.
 - At the **From** and **To** fields, make a selection from any of the pull-down menus for month (1-12), day (1-31), or year (2000-2011).
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).

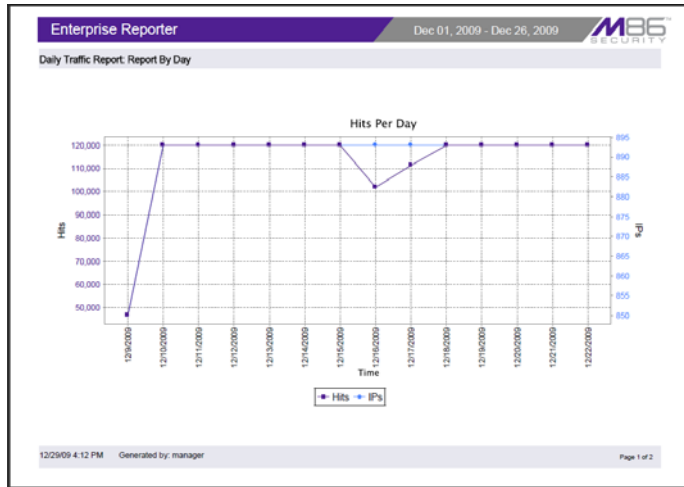


Fig. 3:2-5 Hits Per Day chart

- **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.

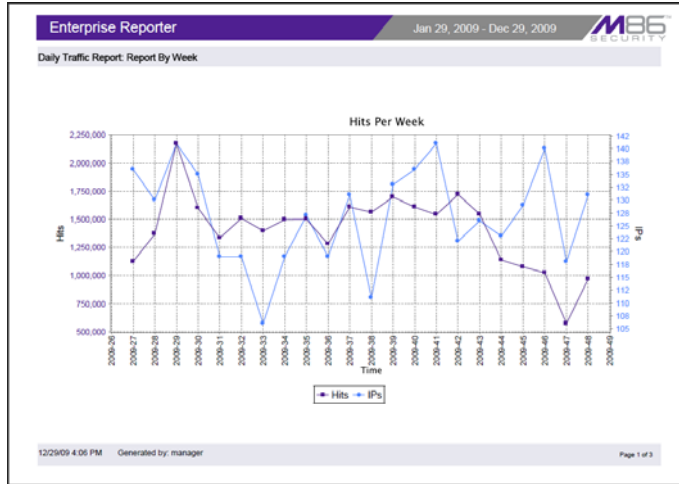


Fig. 3:2-6 Hits Per Week chart

- **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.

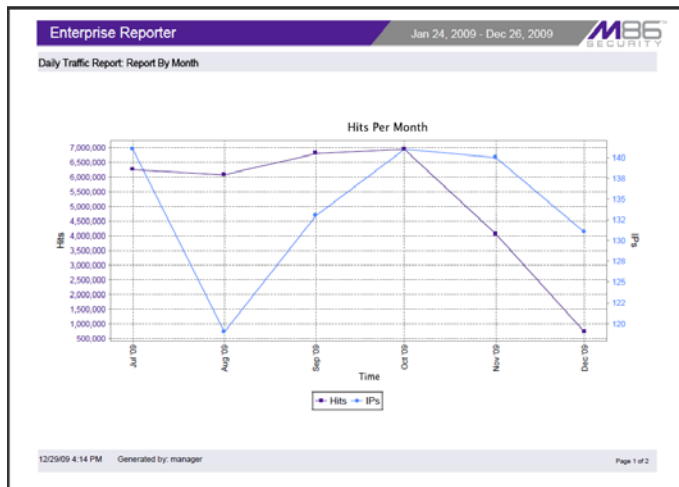




Fig. 3:2-7 Hits Per Month chart

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 ER Server Information window.

Expiration Info

In the Expiration Info frame, the following data displays:

- **Data Space Utilization** - the percentage of database storage space currently being used on the ER Server module
- **% to be live data** - the percentage of data that is set to be live data stored on the ER Server module
- **Weeks until next expiration** - the number of weeks from this week that data on the ER Server module will expire
- **Estimated date of next expiration** - the date scheduled for the next automatic database expiration

Default Options

Default Options is used for specifying various settings to be used in reports.

Click Default Options in the Settings menu to display the Default Options window in the panel:



Fig. 3:2-8 Default Options window

Set New Defaults

1. Enter the maximum number of records that can be returned by a detail report query before triggering the **Page/Object Warning Limit** message. This warning message indicates that the number of records exceeds the number specified in this field. The default is “1000” records.
2. Enter the **Default Top Value** of records that will be generated for summary reports. The default is “50” records.

3. Enter the maximum number of records that will be included in a report's **Result Set 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.

4. By default, the **Hide Un-Identified 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.

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 Options window.

Chapter 3: Executive Reports

This chapter provides information about “canned” reports that display on the screen as bar charts or pie charts. By clicking a button beneath the chart image (PDF, CSV, PNG) report information can be viewed in the specified file format (.pdf, .csv, .png). Executive Reports contain pre-generated data for a specified period of time (Yesterday, Last Week, Last Month, Week to Yesterday, or Month to Yesterday) for any of the following report topics or entities showing Internet activity:

- **Top 20 Users by Blocked Requests** - bar chart report based on each end user’s total number of Blocked and Warn Blocked requests. This report is only available if the Block Request Count feature is enabled in the Optional Features screen on the ER Server module.
- **Top 20 Categories by Page Count** - bar chart report based on the total page count for each filtering category set up in the Category Description list from the Settings menu.
- **Top 20 Users by Page Count** - bar chart report based on each end user’s total page count.
- **Top 20 Users by Malware Hit Count** - bar chart report based on each end user’s total 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.
- **Top 20 Sites by Page Count** - bar chart report based on the total page count for the most popular sites accessed by end users.
- **Top 20 User Groups by Page Count** - bar chart report based on the total page count for each user group set up in the User Groupings list from the Settings menu.

- **Top 20 Blocked Searched Keywords** - bar chart report based on the total number of blocked keyword requests. This report is only available if the Block Searched Keywords Report feature is enabled in the Optional Features screen on the ER Server module.
- **Total Permitted vs. Blocked Requests** - pie chart report based on the total page count for all filtering categories set up to pass and all filtering categories set up to be blocked.
- **Category Group Comparison** - pie chart report based on the total page count for each filtering category group set up in the Category Groupings window from the Settings menu.
- **Category Comparison** - pie chart report based on the total page count for each filtering category set up in the Category Description list from the Settings menu.
- **User Group Comparison** - pie chart report based on the total page count for each user group set up in the User Groupings list from the Settings menu.

Once you have obtained an overview of Internet activity using Executive Reports, you can generate customized or drill down report views, save these views, export them, and/or schedule these reports to run at a designated time.

Generate an Executive Report

By default, upon successfully logging into the Web Client user interface, yesterday’s report view showing either the Top 20 Users by Blocked Requests or Top 20 (Internet Filtering) Categories by Page Count displays in the panel:

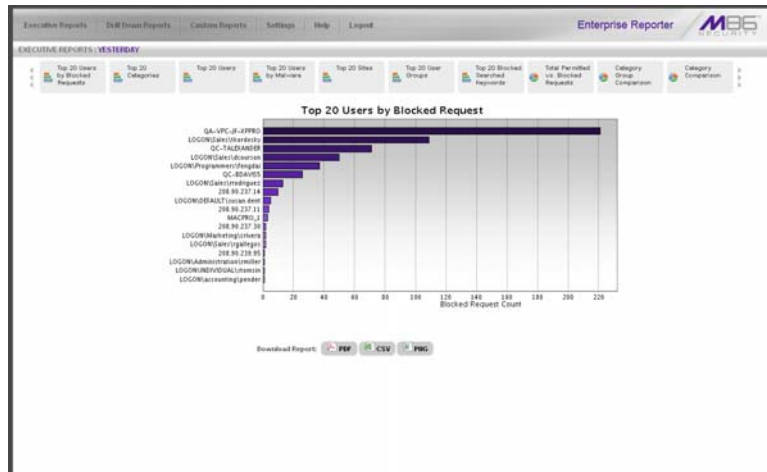




Fig. 3:3-1 Yesterday’s Top 20 Users by Blocked Requests Report

 **TIP:** Click the left arrow or right arrow at the edges of the dashboard to display thumbnail images that are currently hidden.

 **NOTE:** If the ER Server module does not contain any data—as on a newly installed unit—the default report page will not show any thumbnail images or bar chart report in the panel, and the following text displays: “This report cannot be displayed because there is no data to show for this report.”

To generate an Executive Report:

1. From the navigation toolbar, click an Executive Reports menu topic for the time period to be included in the report: Yesterday, Last Week, Last Month, Week to Yesterday, or Month to Yesterday.
2. Click a thumbnail in the dashboard for the selected report option to display as the report view.



NOTE: If necessary, click another time period or thumbnail to display that specified report view in the panel.

- To see details for the generated Executive Report view, click the button beneath the chart image to open a report view in the specified file format: PDF (portable document format), CSV (comma separated value), PNG (portable network graphics).

Executive Report in the PDF format

Clicking the **PDF** button opens a separate browser window containing the Executive Report in the .pdf format:

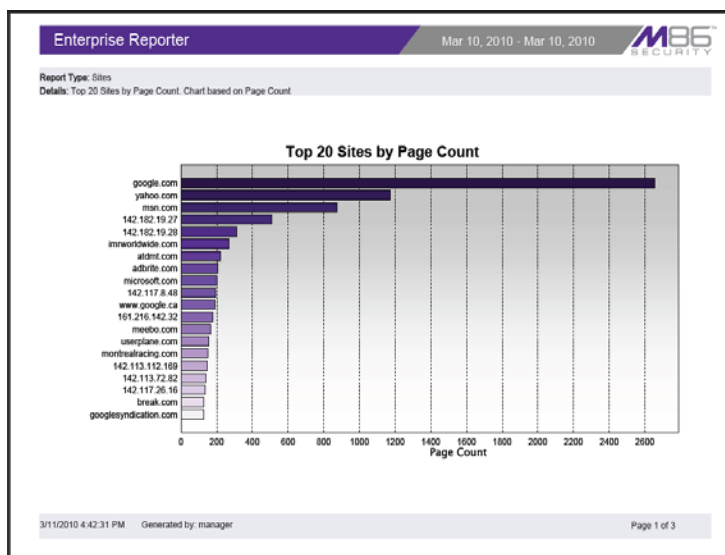


Fig. 3:3-2 Sample Bar Chart Executive Report in the PDF format

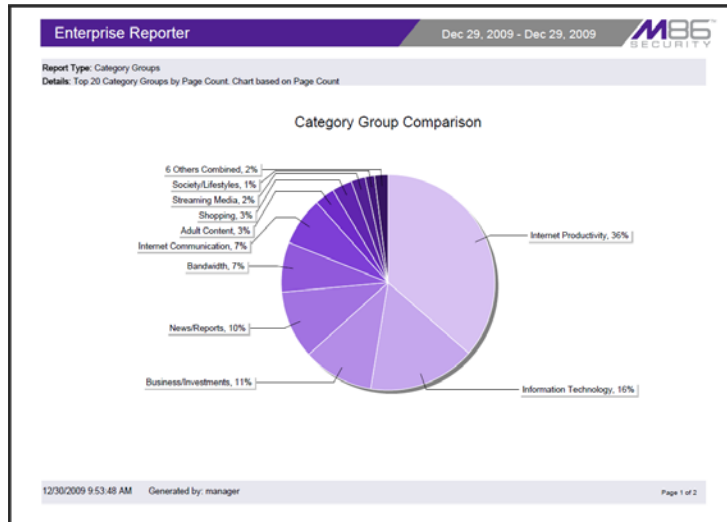


Fig. 3:3-3 Sample Pie Chart Executive Report in the PDF format

The header of the generated report includes the date range, Report Type, and criteria Details.

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 footer of the report includes the username of the person who generated the report (Generated by), the Date and Time the report was generated, and Page number and page range.

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 Requests 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.

Executive Report in the CSV format

Clicking the **CSV** button opens a separate browser window containing the Executive Report in the .csv format:

| Sites | Category Count | IP Count | User Count | Page Count | Object Count | Time (HH MM SS) | Hit Count | Blocked Hits |
|------------------------|----------------------------------|----------|------------|------------|--------------|-----------------|-----------|--------------|
| google.com | 5 | 45 | 42 | 2,855 | 110 | 1:48:50 | 2,765 | 0 |
| yahoo.com | 1 | 1 | 1 | 1 | 1 | 1:51:20 | 1,394 | 0 |
| msn.com | 7 | 115 | 131 | 874 | 2,088 | 1:59:30 | 2,972 | 0 |
| 142.102.19.27 | 6 | 17 | 147 | 507 | 0 | 0:38:0 | 507 | 0 |
| 142.102.19.28 | 7 | 14 | 124 | 310 | 0 | 0:33:20 | 310 | 0 |
| innworldwide.com | 1 | 8 | 57 | 269 | 28 | 0:19:40 | 297 | 0 |
| abdnk.com | 2 | 31 | 281 | 221 | 359 | 0:27:40 | 579 | 0 |
| adobe.com | 2 | 2 | 38 | 209 | 0 | 0:15:0 | 209 | 0 |
| microsoft.com | 1 | 10 | 78 | 203 | 78 | 0:8:0 | 281 | 0 |
| 142.117.0.48 | 1 | 1 | 1 | 1 | 1 | 0:9:30 | 192 | 0 |
| www.google.ca | 2 | 23 | 200 | 198 | 168 | 0:28:30 | 358 | 0 |
| 161.216.142.32 | 1 | 1 | 1 | 1 | 1 | 0:8:30 | 178 | 0 |
| meebo.com | 1 | 7 | 61 | 166 | 0 | 0:21:50 | 166 | 0 |
| useplane.com | 1 | 8 | 7 | 15 | 19 | 0:23:0 | 172 | 0 |
| mondrianaclacmg.com | 2 | 2 | 19 | 150 | 302 | 0:60:45 | 452 | 0 |
| 142.113.112.169 | 1 | 1 | 1 | 1 | 1 | 0:6:30 | 146 | 0 |
| 142.113.72.82 | 1 | 1 | 1 | 1 | 1 | 0:5:10 | 138 | 0 |
| 142.117.26.16 | 1 | 1 | 1 | 1 | 1 | 0:6:10 | 134 | 0 |
| break.com | 2 | 2 | 26 | 127 | 200 | 0:14:20 | 335 | 0 |
| google syndication.com | 1 | 1 | 7 | 126 | 126 | 0:18:10 | 237 | 0 |
| Grand Total | 50 | 347 | 3,210 | 6,116 | 3,691 | 10:29:50 | 11,807 | 0 |
| Site Count | 20 | | | | | | | |
| 3/11/2010 4:44:13 PM | M06 Security Enterprise Reporter | | | | | | | |
| Filter | None | | | | | | | |
| Generated by | manager | | | | | | | |

Fig. 3:3-4 Sample Executive Report in the CSV format

The header of the generated report includes the report title, Sort Order, and date 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, product name, Filter specifications, and the login ID of the user who generated the report.

Executive Report in the PNG format

Clicking the **PNG** button opens a separate browser window containing the Executive Report in the .png format:

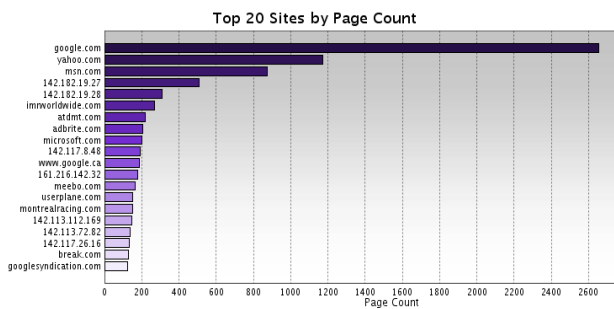


Fig. 3:3-5 Sample Executive Report in the PNG format

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 an Executive Report

From the open generated report file, the Executive Report can be exported in some of the following ways:

- print the report - select the print option from the toolbar—or click the print icon—to open the Print dialog box, and proceed with standard print procedures.
- save the report - select the save option from the toolbar—or click the save icon—to open the Save a Copy dialog box, and proceed with standard save procedures.

Chapter 4: Summary and Detail Reports

The two basic reports administrators and sub-administrators can generate with customizations are the summary report and the detail report. Report views for these reports are implemented via the Drill Down Reports and the Custom Reports sections of the Client application.

While summary and detail reports share some common components with Executive Reports and Wall Clock Time or Blocked Request reports, each kind of report also has its own unique components.

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 summary and detail 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.

Summary Drill Down Report View

The summary drill down report view provides a snapshot of end user activity for a specified report type and defined date of activity recorded by the ER Server module.

These reports are generated via menu options from Drill Down Reports and the Custom Report Wizard from Custom Reports.

| Category | IP | User | Date | Site | Page Count | Object Count | Time |
|------------------------------|----|------|------|------|------------|--------------|---------|
| Search Engines | | 95 | 71 | 54 | 2,263 | 6,245 | 8:46:20 |
| Information Technology | | 73 | 83 | 236 | 6,004 | 6,813 | 7:57:45 |
| Yahoo! Inc. | | 12 | 12 | 12 | 3,703 | 22 | 8:46:20 |
| Research In Motion | | 82 | 87 | 140 | 2,476 | 6,400 | 8:59:20 |
| Web Based Email | | 24 | 34 | 22 | 2,623 | 3,081 | 8:53:56 |
| General Business | | 84 | 87 | 100 | 2,000 | 4,123 | 8:18:10 |
| SES | | 30 | 36 | 21 | 1,866 | 715 | 8:8:20 |
| Edge Content Synchronization | | 66 | 66 | 25 | 1,460 | 3,056 | 1:21:30 |
| Windows Live Messenger | | 4 | 6 | 10 | 1,247 | 8 | 3:39:46 |
| Jobboards | | 2 | 2 | 2 | 1,130 | 6 | 0:2:40 |
| Shipping | | 66 | 67 | 66 | 876 | 2,834 | 1:52:10 |
| Financial Institution | | 27 | 30 | 80 | 891 | 463 | 1:10:30 |
| Search Engines (Edge Search) | | 83 | 84 | 24 | 800 | 1,036 | 1:29:20 |
| Flash Video | | 16 | 16 | 112 | 764 | 67 | 0:58:40 |
| Manufacturing Services | | 83 | 86 | 4 | 736 | 287 | 0:56:10 |
| Reference | | 29 | 29 | 27 | 693 | 1,051 | 0:48:30 |
| Parents | | 40 | 40 | 14 | 689 | 2,074 | 0:59:50 |
| Online Communities | | 12 | 26 | 6 | 623 | 1,403 | 0:18:40 |
| Weather/Travel | | 6 | 10 | 6 | 616 | 1,006 | 0:23:10 |
| Name | | 40 | 46 | 61 | 454 | 2,306 | 0:37:40 |
| Chat | | 17 | 17 | 4 | 381 | 19 | 0:30:20 |
| Image Chat | | 6 | 6 | 6 | 376 | 67 | 0:52:10 |
| Web Log/Personal Pages | | 24 | 27 | 37 | 306 | 771 | 0:33:40 |
| Search Streaming Media | | 36 | 36 | 29 | 295 | 1,173 | 0:27:10 |
| MSN & AOL | | 6 | 7 | 36 | 294 | 19 | 0:18:40 |
| Media & Television | | 6 | 16 | 17 | 233 | 622 | 0:18:40 |
| Internet Service Provider | | 12 | 12 | 6 | 216 | 140 | 0:16:50 |
| Parental Control Systems | | 2 | 6 | 140 | 116 | 17 | 0:13:10 |

Fig. 3:4-1 Summary Drill Down Report view (administrator)

The summary drill down report view is horizontally organized into three sections:

- Header section - includes buttons for customizing the current view: New Report, Modify Report, Export Report, Save Report, and Set Result Limit. The following information displays beneath the row of buttons: Report type, Display criteria, Date, Search criteria, Sort by criteria. Beneath this row of data, the navigation path for the first record in the current report view displays to the far left. The Record navigation field at far right lets you navigate to a specific record and includes the total number of records.

Similarly with summary reports, these reports are generated via menu options from Drill Down Reports and the Custom Report Wizard from Custom Reports.

As with the summary report view, the detail report view is also horizontally organized into three sections but includes different content in its header and body:

- Header section - includes the following data: report type, Date, Sort by criteria, and Display information for records. Checkboxes (used for specifying columns to be included in the body of the report) display to the right of this information: Category, User IP, User name, Site, Filter Action, Content Type, Content, and Search String. The following buttons display below: Modify Report, UnCheck All / Check All. The following Other Options buttons display to the right: Export Report, Save Report, and New Report. The navigation path for the first record in the current report view displays below to the far left. The Record navigation field at far right lets you navigate to a specific record and includes the total number of records.
- Body 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 by populating the corresponding checkbox in the header: Categories, User IP, User name, Site, Filter Action, Content Type, Content criteria, Search String, URL (hyperlink).
- Footer section - includes the username of the login ID used for this session (Logged in as).

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

Back button

If using Internet Explorer, click the Back button in the toolbar of the browser window to return to a previous page in the current report.

Record navigation field

The total number of records displays to the right of the Record navigation field, located above the rows of records:

Record:  1 of 500

This indicator helps you determine how long it will take to generate a report view or to print a report. If there are many records, you may wish to filter your results to reduce the time it will take to process the report.

The selected record is designated by the record number displayed in the Record navigation field, and by an arrow ► to the left of a record in the body of a report view.

To select another record, do any of the following:

- click the specified row to display the arrow preceding that record, and the record number in the Record navigation field.
- in the **Record** navigation field, enter a new record number in the white box between the arrow buttons to go to that record.
- in the Record navigation field, click any of the four arrow buttons to advance forward or backward through the list of records. In the order in which they display in the Record field, clicking these buttons moves you to the first record, the record prior to the selected record, the record following the selected record, and the last record.

Summary Report View Tools and Tips

Filter columns and buttons

In a summary drill down report view, filter columns display after the column containing the record name, and precede the Count columns (Category Count, IP Count, User Count, Site Count, Page Count, Object Count, Time HH:MM:SS). Filter columns include an oblong button for each record in the report view.

| | Categories | Category/ IPs | Category/ Users | Category/ Sites |
|-------------------------------------|-------------------|---------------|-----------------|-----------------|
| <input checked="" type="checkbox"/> | Instant_Messaging | | | |
| <input checked="" type="checkbox"/> | Search_Engines | | | |
| <input checked="" type="checkbox"/> | General_Business | | | |
| <input checked="" type="checkbox"/> | Banner/Web Ads | | | |
| <input checked="" type="checkbox"/> | Chat | | | |

Clicking a specific filter button for a record gives more in-depth analysis on a given record displayed in the current view.

Count columns and column arrows

In a summary drill down report view, columns for specified “item counts” display in the body of the report view. The column for the current report type does not display and therefore cannot be selected.

| Category Count | IP Count | User Count | Site Count | Page Count | Object Count | Time HH:MM:SS |
|----------------|----------|------------|------------|------------|--------------|---------------|
| | 63 | 37 | 132 | 35,963 | 434 | 95:40:20 |
| | 95 | 60 | 60 | 8,885 | 6,088 | 10:59:0 |
| | 97 | 57 | 116 | 4,542 | 6,919 | 8:19:10 |
| | 94 | 56 | 87 | 4,458 | 8,883 | 8:8:0 |
| | 30 | 20 | 12 | 3,223 | 207 | 7:33:30 |

- **Category Count** - displays the number of categories a user has visited, or the number of categories included within a given site. Categories are set up for the Web Filter via the Settings menu option. 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 on the user’s machine.
- **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 arrow to the right of any record 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 clicking the corresponding checkboxes.

- **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 arrow to the right of any record 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 clicking the corresponding checkboxes.



NOTE: If “Pages only” was specified in the Object Count frame of the Optional Features screen in the Administrator 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 ER Administrator portion of this user guide for information about Object Count frame options.

- **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, 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.

| <input checked="" type="checkbox"/> | Categories | Category/ IPs | Category/ Users | Category/ Sites | |
|-------------------------------------|-------------------|----------------------------------|----------------------------------|----------------------------------|--|
| <input checked="" type="checkbox"/> | Instant_Messaging | <input type="button" value="v"/> | <input type="button" value="v"/> | <input type="button" value="v"/> | |
| <input checked="" type="checkbox"/> | Search_Engines | <input type="button" value="v"/> | <input type="button" value="v"/> | <input type="button" value="v"/> | |
| <input checked="" type="checkbox"/> | General_Business | <input type="button" value="v"/> | <input type="button" value="v"/> | <input type="button" value="v"/> | |
| <input checked="" type="checkbox"/> | Banner/Web_Ads | <input type="button" value="v"/> | <input type="button" value="v"/> | <input type="button" value="v"/> | |
| <input checked="" type="checkbox"/> | Chat | <input type="button" value="v"/> | <input type="button" value="v"/> | <input type="button" value="v"/> | |

When exporting a report, only selected records are included. To de-select a record, click the checkbox to remove the check mark from the checkbox.

To de-select all records, click the checkbox in the column header. Clicking the checkbox in the column header again reselects all records.

Detail Report View Tools and Tips

Page link navigation

If more than one page of records was returned by a detail report query, one or more Page numbers display(s) above the rows of records: Page: 1 [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [Next](#)

Click the page number to navigate to that page of records.

Report Type columns

In the detail report view header, by default all checkbox(es) are populated to include all column(s) for records in the current report view. Any column can be hidden from view by clicking the corresponding checkbox to remove the check mark. Clicking **UnCheck All** excludes all columns from displaying in the current report view. This button toggles back to **Check All** when at least one of the checkboxes is empty.

DETAIL BY OBJECT REPORT

Categories
 Date: 12/20/2009
 Sort by Date, Ascending
 Display All records

Category
 User IP
 Site
 Filter Action
 Content Type
 Content
 Search String

OTHER OPTIONS:

Record 1 of 457

| Date | Category | User IP | User | Site | Filter Action | Content Type | Content | Search String | |
|------------------------|----------|------------|-------------------------------|----------------|---------------|--------------|----------------------------|---------------|-------------------------------|
| 12/20/2009 12:09:36 AM | Shopping | 10.1.1.47 | testDomain\test\sup\user76110 | ebayimg.com | Allowed | Wildcard | http://ebayimg.com/ | | http://200... |
| 12/20/2009 12:09:42 AM | Shopping | 10.1.1.103 | testDomain\test\sup\user27513 | shoprogies.com | Allowed | URL | http://www.shoprogies.com/ | | http://www... |
| 12/20/2009 12:09:42 AM | Shopping | 10.1.1.103 | testDomain\test\sup\user27513 | shoprogies.com | Allowed | URL | http://www.shoprogies.com/ | | http://www... |
| 12/20/2009 12:09:42 AM | Shopping | 10.1.1.103 | testDomain\test\sup\user27513 | shoprogies.com | Allowed | URL | http://www.shoprogies.com/ | | http://www... |
| 12/20/2009 12:09:42 AM | Shopping | 10.1.1.162 | testDomain\test\sup\user69408 | ebayimg.com | Allowed | Wildcard | http://ebayimg.com/ | | http://200... |
| 12/20/2009 12:09:43 AM | Shopping | 10.1.1.162 | testDomain\test\sup\user69408 | ebayimg.com | Allowed | Wildcard | http://ebayimg.com/ | | http://200... |

- **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: user-name, 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 Administrator user interface.



NOTE: Refer to the *Optional Features* screen sub-section of the *ER Administrator* portion of this user guide 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 ER'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:



Using escape characters in an NT domain query

When running a query on an NT domain and special characters are present in the search string, escape characters must be included in the username entry.

MySQL recognizes the following escape sequences:

- \ ' A single quote (') character.
- \" A double quote (") character.
- \\ A backslash (\) character.
- \% A percentage (%) character.
- _ An underscore (_) character.

Example:

- Single quote: \'
- Original string: John Smith's
- New string: John Smith\'s

Scenario 1: If usernames are entered as follows:

```
CO-Administration\Steve.Williams  
CO-Financial\Susan.Reynolds
```

In order to find these users via a New Custom Report query in the ER client, you need to add a secondary "\" to all "\" entries in the string, as follows:

```
CO-Administration\\Steve.Williams  
CO-Financial\\Susan.Reynolds
```

Scenario 2: If a domain name precedes the username, as in the following entries:

```
COOP\CO-Administration\Steve.Williams  
COOP\CO-Financial\Susan.Reynolds
```

Entries should be as follows:

```
COOP\\CO-Administration\\Steve.Williams  
COOP\\CO-Financial\\Susan.Reynolds
```


Header Buttons for Customization Options

Clicking a button in the header of a report view opens a pop-up box that lets you customize the current report view. The following header buttons are available in the summary and detail report views: New Report, Modify Report, Export Report, and Save Report.

The Set Result Limit button is additionally available in summary report views.



NOTE: Information on using the fields in these pop-up boxes can be found in the Report View Components sub-section.

New Report button

This option that is available in both summary and detail reports lets you generate a new drill down report view for a date range other than the current (default) date.

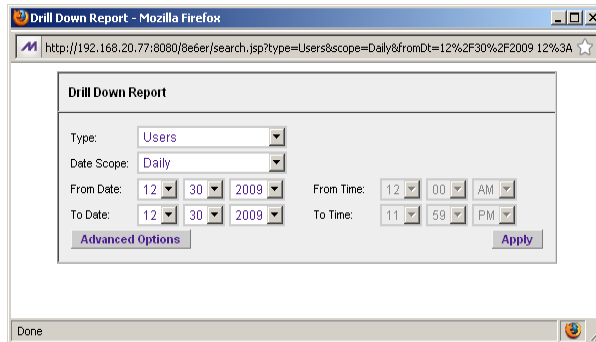


Fig. 3:4-3 New Drill Down Report pop-up box

Click the **Advance Options** button to display additional fields in this box that let you modify the way the view is sorted, or enter search criteria:

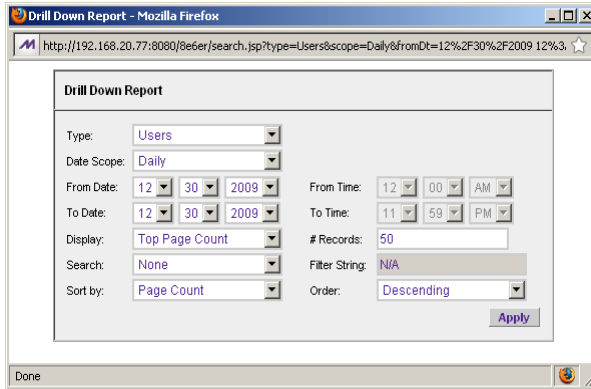




Fig. 3:4-4 New Drill Down Report with Advance Options

 **TIP:** To view only basic options, press the Back Space key on your keyboard to close the Advance Options display.

 **NOTE:** After all modifications are made, click **Apply** to save your settings and to close the pop-up box.

Set Result Limit button

This option lets you specify the maximum number of records to be included in the summary report view, instead of the default number (entered in Default Options).

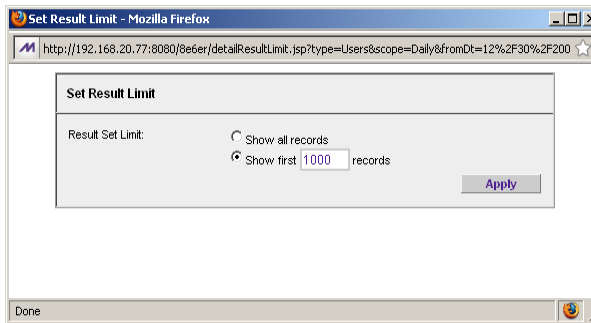



Fig. 3:4-5 Set Result Limit pop-up box

 **NOTE:** After all modifications are made, click **Apply** to save your settings and to close the pop-up box.

Modify Report button

Drill Down Report option

For summary reports, this option lets you modify the current report view by doing any of the following: specify the maximum number of records to be included other than the number entered in Default Options; perform a search for specified text, or sort the report in ascending or descending order by a specified column.

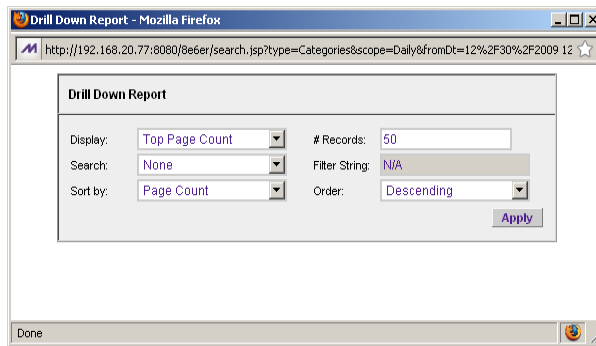


Fig. 3:4-6 Drill Down Report pop-up box

Detail Custom Report option

For detail reports, this option lets you modify the current report view by doing any of the following: change the date scope, sort the report in ascending or descending order by a specified column, and specify the maximum number of records to be included other than the number entered in Default Options.

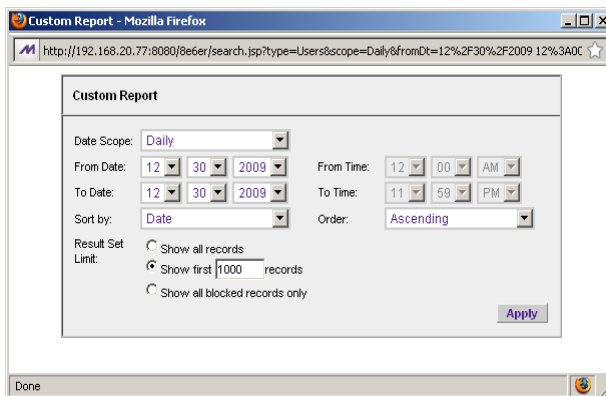



Fig. 3:4-7 Custom Report pop-up box

 **NOTE:** After all modifications are made, click **Apply** to save your settings and to close the pop-up box.

Export Report button

Export Drill Down Report option

This option lets you email or view the current summary report view in the specified output format.

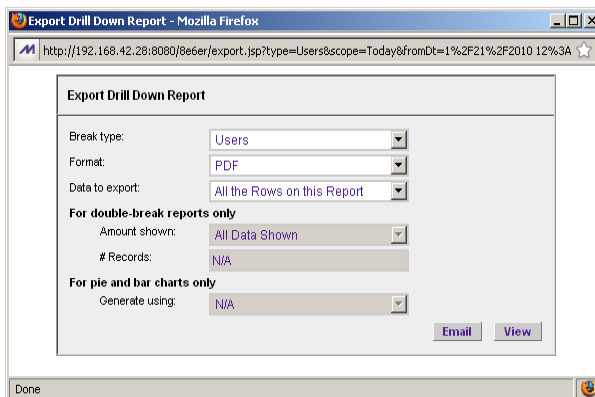


Fig. 3:4-8 Export Drill Down Report pop-up box

Export Custom Report option

This option lets you email or view the current detail report view in the specified output format, defining the break type, file format, and maximum number of records to be included in the report view instead of the default number (entered in the Default Options window).

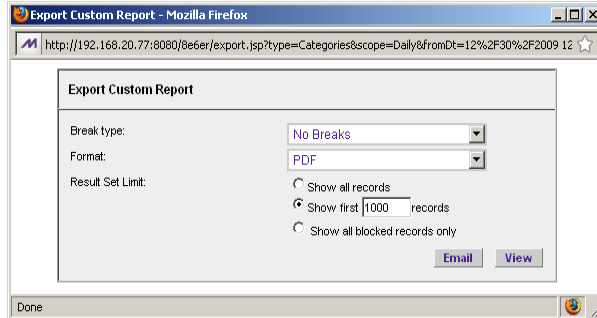


Fig. 3:4-9 Export Custom Report pop-up box



NOTES: After all modifications are made, click **Email** to open the Email Report pop-up box where email criteria is entered, or click **View** 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 Report button

This option lets you save the current report view so a report using these customizations can be run again later at a designated time.

Summary Drill Down Report option

Fig. 3:4-10 Save Custom Report pop-up box for summary reports

 **TIP:** The Copy (Ctrl+C) and Paste (Ctrl+V) functions can be used in the fields in the Save Custom Report pop-up box.

Detail Drill Down Report option

Fig. 3:4-11 Save Custom Report pop-up box for detail reports



NOTES: After all modifications are made, click **Save and Schedule** to open the Event Schedules window where a schedule can be set up for running the report, **Save and Run** to save the report in the specified format and then email it to the designated email address(es), or **Save Only** to save the report.

See Custom Report Wizard in Chapter 6 for information about using these report options.

Report View Components

Report Fields and Usage

The following fields are used in the Custom Report Wizard, Save Custom 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. Category groups are set up using the Category Groupings option from the Settings menu.
- **User Groups** - this option performs a query on Internet activity of user groups. User groups are set up using the User Groupings option from the Settings 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 ER Server module'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 Date 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 Date** and **To Date** pull-down menus where you specify the range of months (1-12) and/or years (2000-2011).
- **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 Date** and **To Date** pull-down menus where you specify the range of months (1-12), days (1-31), and/or years (2000-2011). The generated report view includes data for the specified days only, if the data for these days are stored on the Server.
- **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's time range specified in the **From Time** and **To Time** fields. Make a selection for the hour (1-12), minutes (00-59), and AM or PM.
- **Part of Yesterday** - this option generates the report view for yesterday's time range specified in the **From Time** and **To Time** fields. Make a selection for the hour (1-12), minutes (00-59), and AM or PM.
- **Part of Specific Day** - this option generates the report view for the specified time range on the specified date. In the **From Date** field, make a selection for the month (1-12), day (1-31), and year (2000-2011). In the **From Time** and **To Time** fields, make a selection for the hour (1-12), minutes (00-59), and AM or PM.
- **User Defined** - this option generates the report view for the specified time range within the specified date range. In the **From Date** and **To Date** fields, make a selection for the month (1-12), day (1-31), and year (2000-2011).

In the **From Time** and **To Time** fields, make a selection for the hour (1-12), minutes (00-59), and AM or PM.

Display and # Records fields

The Display and # Records fields are used for specifying the number of records from the query you wish to include in the summary report view, and how these records will be sorted.

At the **Display** field, make a selection from the pull-down menu for the records to be shown on the screen: “All Data Shown”, “Top Category Count”, “Top IP Count”, “Top User Count”, “Top Site Count”, “Top Page Count”, “Top Object Count”, “Top Time”, “Top Hit Count”.

In the **# Records** field, “N/A” displays greyed-out if “All Data Shown” was selected at the Display field. If any other selection was made at the previous field, the default number saved in the Default Options window displays in this field. Enter the maximum number of top records to be included in the query.



NOTE: *The Default Top Value entry in the Default Options window is accessible via Default Options in the Settings menu. See the Default Options sub-section in Chapter 2: Customizing the Client for information about the Default Top Value.*

Search and Filter String fields

The Search and Filter String fields are used for specifying search criteria in the current summary report view.

At the **Search** field, make a selection from the pull-down menu for the search term to be used: “None”, “Contains”, “Starts with”, “Ends with”.

In the **Filter String** field, “N/A” displays greyed-out if “None” was selected at the Search field. If any other selection was made at the previous field, enter text in this field corresponding to the type of search term selected.

Sort by and Order fields

The Sort by and Order fields are used for specifying the manner in which the generated report view will be sorted.

For summary 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".

For detail 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".

At the **Order** field, make a selection from the pull-down menu for the order in which to display the sort option count: "Ascending", "Descending".

Result Set Limit fields

The Result Set Limit fields are used for specifying the maximum number of records to be included in the report view.

Indicate the **Result Set Limit** by selecting the appropriate radio button:

- **Show all records** - Click this radio button to include all records returned by the report query.
- **Show first 'X' records** - Click this radio button to only include the first set of records returned by the report query.

Indicate the number of records to be included in a set by making an entry in the blank field, represented here by the 'X'.

- **Show all blocked records only** - 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 format when the report view is emailed or viewed.

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”, or double-break report types such as “Users/Sites”.

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 report is emailed or viewed.

At the **Data to export** field, select the amount of data to be exported from the pull-down menu: “All the Rows on this Report”, or “Only the Selected Rows on this Page”. The second selection is available only if some of the records in the report view were deselected.

For double-break reports only

The Amount shown and # Records fields are used in double-break reports and are deactivated by default.



NOTE: *These fields also display in Save Custom Report under the label: For single-break reports only.*

Amount shown field

The Amount shown field is used for specifying how the report view will be sorted. By default, “All Data Shown” displays greyed-out and this field becomes activated when a double-break report type is selected at the Break type field.

At the **Amount shown** field, make a selection from the pull-down menu for an available sort option: “All Data Shown”, “Top Category Count”, “Top IP Count”, “Top User Count”, “Top Site Count”, “Top Page Count”, “Top Object Count”, “Top Time”, “Top Hit Count”.

Records field

The # Records field is used for specifying the number of records that will display for the selected sort option. By default, “N/A” displays greyed-out and this field becomes activated when a Top item Count is selected at the Amount shown field.

In the activated **# Records** field, the number saved in the Default Options window displays by default. This number can be edited to indicate the number of records to be included in the exported report.



NOTE: *The Default Top Value entry in the Default Options window is accessible via Default Options in the Settings menu. See the Default Options sub-section in Chapter 2: Customizing the Client for information about the Default Top Value.*

For pie and bar charts only

Generate using field

The Generate using field is used for specifying how a Categories pie chart or bar chart will be sorted. By default, “N/A” displays greyed-out and this field becomes activated when a pie or bar chart report type 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: “IP Count”, “User Count”, “Site Count”, “Page Count”, “Object Count”, “Time”, “Hit Count”.

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 deselected in the Default Options window.



NOTE: *The Default Options window is accessible via Default Options in the Settings menu. See the Default Options subsection in Chapter 2: Customizing the Client for more information about the Hide Un-Identified 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 Options window.

For E-Mail output only / Email Report fields

The For E-Mail output only fields and Email Report fields are used for entering email criteria pertinent to the report to be sent to the designated addressee(s).

Specify the following in the **For E-Mail output only** field or the Email Report pop-up box 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 field

The Detailed Info field is used for specifying which columns of data will be excluded from detail reports.

In the **Detailed Info** field, by default all checkboxes corresponding to detail 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 Administrator user interface.



NOTE: Refer to the *Optional Features* screen sub-section of the *ER Administrator User Guide* for information about the *Search String* feature.

Exporting a Report

The email option for exporting reports lets you electronically send the report in the specified file format to designated personnel.



NOTES: If you are using *Lotus Notes* as your primary e-mail client instead of *Microsoft Outlook* or *Outlook Express*, refer to *Appendix B* in the *Web Client Appendices Section* for information on how to configure *Lotus Notes* to work with the *ER Client*.

For reports generated in the *HTML* format, the contents of the file will be embedded in the email message. For reports generated in any other format [*MS-DOS Text*, *PDF*, *Rich Text Format*, *Comma-Delimited Text*, *Excel (Chinese)*, *Excel (English)*], the file will be sent as an email attachment.



WARNING: If using a spam filter on your mail server, email messages or attachments sent by the Client 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 Drill Down Report* or *Export Custom Report* pop-up box, click the **Email** button to open the *Email Report* pop-up box:

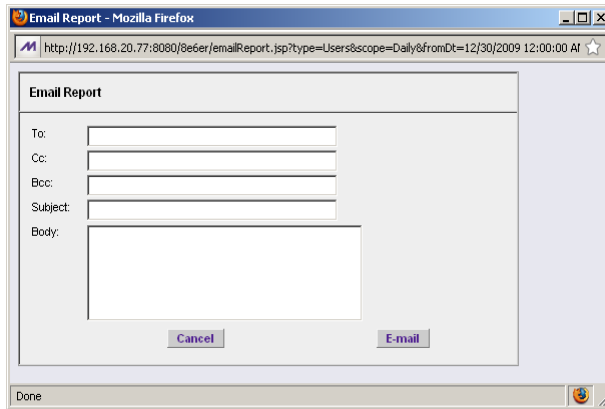



Fig. 3:4-12 Email Report pop-up box

2. In the **To** field, enter the email address of each intended report recipient, separating each address by a comma (,) and a space.
3. An entry in each of the following fields is optional:
 - **Subject** - Type in a brief description about the report.
 - **Cc** - 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** - 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.

 **TIP:** Click **Cancel** to close the Email Report pop-up box and to return to the report view.

4. Click **E-mail** to send the report to the designated recipient(s). As a result of this action, the Email Report pop-up box now displays information to indicate the report is being generated.



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.

After the report is generated in the specified file format, the Email Result pop-up box displays this message: “The report has been sent to the following address(es)”, and lists the email address(es) below:

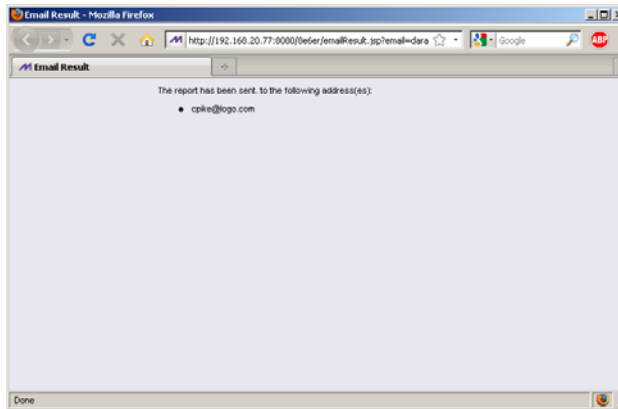


Fig. 3:4-13 Email Result pop-up box

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

View and Print Options

The view and print options for exporting 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 Drill Down Report or Export Custom Report pop-up box, click the **View** button to open the ER Report browser window/tab containing the status of the report being generated.

When completely generated, the ER Report browser window/tab displays “Report Finished” and can be closed. The generated report view opens in a separate window 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 within a fixed column width for each record.

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** - highlight 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)

To close the report file window/tab, click the "X" in the upper right corner of the window/tab.

Sample Report File Formats

The following report file formats are available for emailing and viewing: 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:

Category Groups
 Sort Order: Page Count, descending
 From: 12/30/2009 12:00:00 AM
 To: 12/30/2009 11:59:59 PM

| Category Groups | Category | IP Count | User Count | Site Count | Page Count | Object Count | Time (MM:MM:SS) | Hit Count | Blocked Hits | |
|-------------------------|----------|-----------|------------|--------------|------------|--------------|-----------------|-----------------|---------------|----------|
| Information Technology | 4 | 241 | 1,764 | 50 | 1,193 | 3,512 | 4:21:20 | 6,715 | 0 | |
| Internet Communication | 4 | 81 | 599 | 21 | 1,001 | 628 | 2:10:20 | 1,629 | 0 | |
| Internet Productivity | 4 | 84 | 810 | 45 | 617 | 1,441 | 1:51:50 | 2,278 | 0 | |
| Web Threats | 3 | 35 | 290 | 16 | 535 | 628 | 1:59:10 | 1,173 | 0 | |
| Entertainment | 7 | 37 | 254 | 32 | 324 | 1,926 | 0:33:10 | 2,250 | 0 | |
| Shopping | 2 | 17 | 116 | 21 | 312 | 456 | 0:24:10 | 960 | 0 | |
| Business/Investments | 4 | 73 | 354 | 34 | 265 | 4,497 | 0:16:10 | 4,752 | 0 | |
| Travel/Events | 3 | 14 | 114 | 16 | 106 | 1,532 | 0:13:50 | 1,718 | 0 | |
| Adult Content | 4 | 9 | 90 | 13 | 141 | 603 | 0:21:10 | 764 | 0 | |
| Recreation | 4 | 21 | 175 | 18 | 154 | 660 | 0:14:20 | 814 | 0 | |
| News/Reports | 3 | 38 | 237 | 28 | 129 | 1,431 | 0:15:20 | 1,940 | 0 | |
| Society/Lifestyles | 3 | 21 | 142 | 12 | 95 | 1,017 | 0:11:10 | 1,112 | 0 | |
| Games | 1 | 6 | 46 | 5 | 57 | 67 | 0:51:50 | 124 | 0 | |
| Government/Law/Politics | 1 | 4 | 27 | 4 | 21 | 308 | 0:21:20 | 329 | 0 | |
| Streaming Media | 1 | 6 | 58 | 6 | 14 | 184 | 0:21:20 | 398 | 0 | |
| Education | 2 | 6 | 48 | 6 | 7 | 85 | 0:11:10 | 92 | 0 | |
| Remote Access | 1 | 1 | 7 | 1 | 7 | 21 | 0:11:30 | 28 | 0 | |
| Community/Organizations | 1 | 1 | 4 | 1 | 4 | 0 | 0:01:40 | 4 | 0 | |
| Security | 1 | 1 | 4 | 1 | 4 | 0 | 0:01:40 | 4 | 0 | |
| Health/Fitness | 1 | 2 | 8 | 2 | 0 | 132 | 0:01:0 | 132 | 0 | |
| Grand Total | | 54 | 718 | 5,167 | 332 | 7,106 | 19,938 | 11:41:40 | 27,044 | 0 |

Category Group Count: 20
 12/31/2009 11:57:40 AM
 Filter: None
 Generated by: manager

Fig. 3:4-14 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:

| Category Group | Category | IP Count | User Count | Site Count | Page Count | Object Count | Time (HH:MM:SS) | Hit Count | Blocked |
|-------------------------|----------|----------|------------|------------|------------|--------------|-----------------|-----------|---------|
| Information Technology | 4 | 241 | 1,784 | 50 | 3,193 | 3,822 | 4:21:0 | 5,718 | 0 |
| Internet Communication | 4 | 81 | 595 | 21 | 1,051 | 826 | 2:10:20 | 1,029 | 0 |
| Internet Productivity | 4 | 84 | 820 | 48 | 617 | 1,861 | 1:55:0 | 2,278 | 0 |
| Web Threads | 3 | 85 | 390 | 18 | 886 | 618 | 1:01:0 | 1,173 | 0 |
| Entertainment | 7 | 37 | 254 | 32 | 324 | 1,926 | 0:33:10 | 2,200 | 0 |
| Shopping | 2 | 17 | 128 | 21 | 312 | 688 | 0:34:10 | 865 | 0 |
| Business/Investments | 4 | 73 | 854 | 34 | 288 | 4,487 | 0:26:10 | 4,782 | 0 |
| Travel/Events | 3 | 14 | 114 | 18 | 186 | 1,532 | 0:13:50 | 1,718 | 0 |
| Adult Content | 4 | 9 | 90 | 13 | 161 | 623 | 0:21:0 | 764 | 0 |
| Sports/ath | 4 | 21 | 178 | 18 | 184 | 860 | 0:14:20 | 814 | 0 |
| News/Reports | 3 | 39 | 237 | 29 | 129 | 1,431 | 0:15:20 | 1,880 | 0 |
| Software/Reviews | 3 | 21 | 142 | 12 | 86 | 1,017 | 0:11:0 | 1,112 | 0 |
| Games | 1 | 6 | 48 | 6 | 87 | 67 | 0:5:50 | 124 | 0 |
| Government/Law/Politics | 1 | 4 | 37 | 4 | 21 | 558 | 0:2:20 | 829 | 0 |
| Company/Press | 1 | 6 | 88 | 6 | 14 | 284 | 0:2:20 | 308 | 0 |
| Education | 2 | 6 | 48 | 6 | 7 | 85 | 0:11:0 | 92 | 0 |
| Remote Access | 1 | 1 | 7 | 1 | 7 | 21 | 0:1:50 | 28 | 0 |
| Community/Organizations | 1 | 1 | 4 | 1 | 4 | 0 | 0:0:40 | 4 | 0 |
| Security | 1 | 1 | 4 | 1 | 4 | 0 | 0:0:40 | 4 | 0 |
| Health/Fitness | 1 | 2 | 8 | 2 | 0 | 132 | 0:0:0 | 132 | 0 |
| Grand Total | 54 | 718 | 5,187 | 332 | 7,106 | 19,938 | 11:41:40 | 27,044 | 0 |
| Count 20 | | | | | | | | | |

12/31/2009 12:04:00 PM Generated by: manager Filter: None Page 1 of 1

Fig. 3-4-15 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:

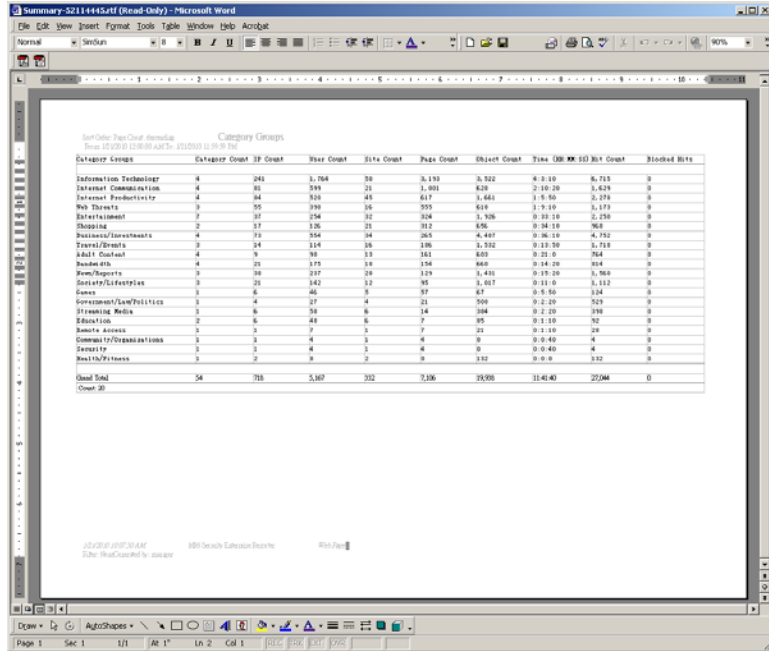


Fig. 3-4-16 Category Groups report, RTF format

HTML

This is a sample of the Category Groups report in the HTML format, saved with a .html file extension:

| Category Group | IP Count | User Count | Site Count | Page Count | Object Count | Time (HH:MM:SS) | Hit Count | Blocked Hits |
|-------------------------|----------|------------|------------|------------|--------------|-----------------|-----------|--------------|
| Information Technology | 4 | 341 | 1,764 | 50 | 3,393 | 3,522 | 4,310 | 6,715 |
| Internet Communication | 4 | 81 | 599 | 21 | 1,891 | 426 | 2,102 | 1,826 |
| Internet Productivity | 4 | 84 | 520 | 45 | 617 | 1,661 | 1,530 | 3,278 |
| Web Threads | 3 | 55 | 390 | 16 | 555 | 618 | 1,910 | 1,173 |
| Entertainment | 7 | 37 | 254 | 32 | 324 | 1,826 | 0:33:10 | 2,250 |
| Shopping | 2 | 17 | 126 | 21 | 312 | 656 | 0:34:10 | 968 |
| Business/Investments | 4 | 73 | 554 | 34 | 265 | 4,487 | 0:36:10 | 4,752 |
| Travel/Events | 3 | 14 | 114 | 18 | 186 | 1,332 | 0:13:50 | 1,718 |
| Adult Content | 4 | 8 | 303 | 13 | 161 | 633 | 0:21:0 | 764 |
| Banking/Fin | 4 | 21 | 175 | 18 | 154 | 660 | 0:14:20 | 914 |
| News/Reports | 3 | 39 | 237 | 28 | 129 | 1,431 | 0:15:20 | 1,560 |
| Society/Lifestyles | 3 | 21 | 142 | 12 | 95 | 1,017 | 0:11:0 | 1,112 |
| Games | 1 | 6 | 46 | 5 | 57 | 67 | 0:5:30 | 124 |
| Government/Law/Politics | 1 | 4 | 27 | 4 | 21 | 508 | 0:2:20 | 529 |
| Streaming Media | 1 | 6 | 58 | 6 | 14 | 384 | 0:2:20 | 398 |
| Education | 2 | 6 | 48 | 6 | 7 | 85 | 0:1:10 | 92 |
| Remote Access | 1 | 1 | 7 | 1 | 7 | 21 | 0:1:10 | 28 |
| Community/Organizations | 1 | 1 | 4 | 1 | 4 | 0 | 0:0:40 | 4 |
| Security | 1 | 1 | 4 | 1 | 4 | 0 | 0:0:40 | 4 |
| Health/Fitness | 1 | 2 | 8 | 2 | 0 | 132 | 0:0:0 | 132 |
| Category Groups | | | | | | | | |
| Grand Total | 54 | 718 | 5,167 | 332 | 7,336 | 19,308 | 11:41:40 | 27,044 |
| Count: 30 | | | | | | | | |

12/3/2009 12:42:38 PM M86 Security Enterprise Reporter
 Filter Name: Generated by: manager

Fig. 3:4-17 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:

| Category Groups | Category Count | IP Count | User Count | Site Count | Page Count | Object Count | Time (HH:MM:SS) | Hit Count | Blocked Hits |
|-------------------------|----------------|----------|------------|------------|------------|--------------|-----------------|-----------|--------------|
| Information Technology | 4 | 241 | 1,764 | 50 | 3,193 | 3,522 | 4:3:10 | 6,715 | 0 |
| Internet Communication | 4 | 81 | 599 | 21 | 1,001 | 628 | 2:10:20 | 1,629 | 0 |
| Internet Productivity | 4 | 84 | 520 | 45 | 617 | 1,661 | 1:5:50 | 2,278 | 0 |
| Web Threats | 3 | 59 | 390 | 16 | 555 | 618 | 1:9:10 | 1,173 | 0 |
| Entertainment | 7 | 37 | 254 | 32 | 324 | 1,926 | 0:33:10 | 2,250 | 0 |
| Shopping | 2 | 17 | 126 | 21 | 312 | 656 | 0:34:10 | 968 | 0 |
| BusinessInvestments | 4 | 73 | 554 | 34 | 265 | 4,487 | 0:36:10 | 4,752 | 0 |
| TravelEvents | 3 | 14 | 114 | 16 | 186 | 1,532 | 0:13:50 | 1,718 | 0 |
| Adult Content | 4 | 9 | 90 | 13 | 161 | 603 | 0:21:0 | 764 | 0 |
| Bandwidth | 4 | 21 | 175 | 18 | 154 | 660 | 0:14:20 | 814 | 0 |
| News/Reports | 3 | 38 | 237 | 28 | 129 | 1,431 | 0:15:20 | 1,560 | 0 |
| Society/Lifestyles | 3 | 21 | 142 | 12 | 95 | 1,017 | 0:11:0 | 1,112 | 0 |
| Games | 1 | 6 | 46 | 5 | 57 | 67 | 0:5:50 | 124 | 0 |
| Government/Law/Politics | 1 | 4 | 27 | 4 | 21 | 508 | 0:2:20 | 529 | 0 |
| Streaming Media | 1 | 6 | 58 | 6 | 14 | 384 | 0:2:20 | 389 | 0 |
| Education | 2 | 6 | 48 | 6 | 7 | 85 | 0:1:10 | 92 | 0 |
| Remote Access | 1 | 1 | 7 | 1 | 7 | 21 | 0:1:10 | 28 | 0 |
| Community/Organizations | 1 | 1 | 4 | 1 | 4 | 0 | 0:0:40 | 4 | 0 |
| Security | 1 | 1 | 4 | 1 | 4 | 0 | 0:0:40 | 4 | 0 |
| Health/Fitness | 1 | 2 | 8 | 2 | 0 | 132 | 0:0:0 | 132 | 0 |
| Grand Total | 54 | 718 | 5,167 | 332 | 7,106 | 19,938 | 11:41:40 | 27,044 | 0 |
| Category Group Count | 20 | | | | | | | | |

Fig. 3.4-18 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 | Category Count | IP Count | User Count | Site Count | Page Count | Object Count | Time (HH:MM:SS) | Hit Count | Blocked Hits | |
|--------------------------|----------------------------------|----------|------------|------------|------------|--------------|-----------------|-----------|--------------|---|
| Information Technology | 4 | 241 | 1,764 | 50 | 3,193 | 3,522 | | 4,6715 | 0 | |
| Internet Communication | 4 | 81 | 699 | 21 | 1,001 | 620 | | 2,1,629 | 0 | |
| Internet Productivity | 4 | 84 | 520 | 45 | 617 | 1,661 | | 1,2,278 | 0 | |
| Web Threats | 3 | 55 | 390 | 16 | 555 | 618 | | 1,1,173 | 0 | |
| Entertainment | 7 | 37 | 254 | 32 | 324 | 1,926 | | 0,2,290 | 0 | |
| Shopping | 2 | 17 | 126 | 21 | 312 | 656 | | 0,968 | 0 | |
| Business/Investments | 4 | 73 | 554 | 34 | 265 | 4,467 | | 0,4,752 | 0 | |
| Travel/Events | 3 | 14 | 114 | 16 | 196 | 1,532 | | 0,1,718 | 0 | |
| Adult Content | 4 | 9 | 90 | 13 | 161 | 603 | | 0,754 | 0 | |
| Bandwidth | 4 | 21 | 175 | 18 | 154 | 660 | | 0,814 | 0 | |
| News/Reports | 3 | 38 | 237 | 28 | 129 | 1,431 | | 0,1,560 | 0 | |
| Society/Lifestyles | 3 | 21 | 142 | 12 | 95 | 1,017 | | 0,1,112 | 0 | |
| Games | 1 | 6 | 45 | 5 | 27 | 67 | | 0,124 | 0 | |
| Governments/Law/Politics | 1 | 4 | 27 | 4 | 21 | 508 | | 0,529 | 0 | |
| Streaming Media | 1 | 6 | 58 | 6 | 14 | 384 | | 0,398 | 0 | |
| Education | 2 | 6 | 48 | 6 | 7 | 95 | | 0,92 | 0 | |
| Remote Access | 1 | 1 | 7 | 1 | 7 | 21 | | 0,25 | 0 | |
| Community/Organizations | 1 | 1 | 4 | 1 | 4 | 0 | | 0,4 | 0 | |
| Security | 1 | 1 | 4 | 1 | 4 | 0 | | 0,4 | 0 | |
| Health/Fitness | 1 | 2 | 8 | 2 | 0 | 132 | | 0,132 | 0 | |
| Grand Total | | 54 | 718 | 5,167 | 332 | 7,106 | | 19,938 | 11,27,044 | 0 |
| Category Group Count: 20 | | | | | | | | | | |
| 12/31/2009 1:00:55 PM | M86 Security Enterprise Reporter | | | | | | | | | |
| Filter: None | | | | | | | | | | |
| Generated by: manager | | | | | | | | | | |

Fig. 3-4-19 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 5: Drill Down Reports

This chapter provides information about generating drill down reports from the Drill Down Reports menu. As explained in the previous chapter, drill down reports let you query the database to access more detailed information about end user Internet activity. The following types of reports can be generated from this 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, if category groups previously have been set up via the Settings menu.
- **All User Groups** - includes activity by all user groups, if user groups previously have been set up via the Settings menu.
- **Single User Group** - after selecting the user group from a list of available choices, this report shows activity for that user group, if the user group previously has been set up via the Settings menu.

As previously discussed, 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.

Generate a Drill Down Report

To generate a drill down report:

1. Click one of the following menu topics in the navigation toolbar for the type of report you wish to view: Categories, IPs, Users, Sites, Category Groups, All User Groups:

| Category Group | Group Category | Group IP | Group User | Group Site | Category Count | IP Count | User Count | Site Count | Page Count | Object Count | Time Interval |
|---------------------------|----------------|----------|------------|------------|----------------|----------|------------|------------|------------|--------------|---------------|
| Internet Communication | | | | | 4 | 241 | 1,704 | 95 | 3,363 | 3,832 | 4:30:00 |
| Internet Communication | | | | | 4 | 81 | 596 | 21 | 1,001 | 625 | 2:10:20 |
| Internet Periodicity | | | | | 4 | 84 | 530 | 40 | 817 | 1,881 | 1:50:00 |
| Web Threats | | | | | 3 | 65 | 300 | 10 | 555 | 810 | 1:8:10 |
| Endpoint | | | | | 3 | 20 | 294 | 34 | 344 | 1,508 | 9:40:10 |
| Shopping | | | | | 2 | 17 | 130 | 21 | 312 | 688 | 0:54:10 |
| Malware/Incidents | | | | | 4 | 73 | 504 | 34 | 305 | 4,487 | 0:30:10 |
| Transit | | | | | 3 | 14 | 114 | 10 | 186 | 1,832 | 0:13:00 |
| Anti-Spam | | | | | 4 | 16 | 190 | 19 | 181 | 855 | 0:21:00 |
| Bandwidth | | | | | 4 | 21 | 115 | 10 | 144 | 890 | 0:14:20 |
| Hosts/Ports | | | | | 3 | 36 | 337 | 30 | 138 | 1,451 | 0:16:00 |
| Security/Policies | | | | | 3 | 21 | 142 | 12 | 95 | 1,017 | 0:11:00 |
| Malware | | | | | 1 | 6 | 40 | 6 | 97 | 87 | 0:5:00 |
| Hosts/Ports/Logon/Off | | | | | 1 | 6 | 37 | 4 | 21 | 80 | 0:2:00 |
| Outgoing Mail | | | | | 1 | 6 | 56 | 8 | 14 | 384 | 0:2:00 |
| E-Mail | | | | | 2 | 6 | 40 | 6 | 7 | 85 | 0:1:10 |
| Malware/Ports | | | | | 1 | 1 | 7 | 1 | 7 | 21 | 0:1:10 |
| Communication/Connections | | | | | 1 | 1 | 4 | 1 | 4 | 25 | 0:1:40 |
| Security | | | | | 1 | 1 | 4 | 1 | 4 | 12 | 0:1:40 |
| Health/Status | | | | | 1 | 2 | 6 | 2 | 0 | 132 | 0:0:0 |

Fig. 3:5-1 Sample Drill Down Category Groups Report



NOTES: As the report is generating, a message describing the current status displays. If no records are available, an alert box opens displaying the message “No records returned!”

Information on generating a Single User Group report view is provided in the Generate a Single User Group Report sub-section.

2. Once the generated report has loaded in the window, use the tools in the panel to create the desired drill down view.
3. The drill down view can be exported, saved, and/or scheduled to run at a specified time.

Generate a Single User Group Report

To generate a Single User Group Report:

1. Click Single User Group from the Drill Down Reports menu to display the Single User Group window in the panel:



Fig. 3:5-2 Single User Group window

2. Specify the following report criteria: “Type”, “User Group”, “Date Scope”, and Advance Options such as “Display” / “# Records”, “Search” / “Filter String”, “Sort by” / “Order”.
3. Click **Apply** to generate the report. When the report has generated, the report view displays (see Fig. 3:5-1) and can be modified, exported, or saved.

Chapter 6: Custom Reports

This chapter provides information about custom reports that can be generated if more specific details are needed about end user Internet activity.

The following options are available from the Custom Reports menu:

- **Custom Report Wizard** - this option lets you use the wizard to generate a customized report, querying the database for hits, pages, or objects viewed by end users.
- **Sample Custom Reports** - this option includes “canned” selections of 10 of the most popular reports that you can readily generate in the PDF format.
- **Wall Clock Time Report** - this option is available to administrators only. Wall Clock Time reports use the Wall Clock Time algorithm to calculate the amount of time each end user spent accessing a given page or object.



NOTES: *Wall Clock Time Report is only available in the Custom Reports menu if the Wall Clock Time feature is enabled in the Administrator user interface. See the ER Administrator portion of this user guide for information about the Wall Clock Time feature.*

To include object hits in the Wall Clock Time Report, the “Pages and Objects” selection must be made in the Object Count frame of the Optional Features screen. See Optional Features in the ER Administrator portion of this user guide for more information about this selection.

- **Blocked Request Report** - this option is available to administrators only. Blocked Request reports show data for all specified users’ blocked requests within the designated time frame.



NOTE: *Blocked Request Report is only available in the Custom Reports menu if the Block Request Count feature is enabled in the ER Administrator user interface. See the ER Administrator portion of this user guide regarding the Block Request feature.*

- **Saved Custom Reports** - this option lets you view, edit, copy, delete, or run a customized report that was previously saved in the Client.
- **Event Schedule** - this option is used for creating and maintaining schedules for generating customized reports.
- **Executive Internet Usage Summary** - this option, available to administrators only, is used for specifying email addresses of personnel authorized to receive a report containing charts showing activity in selected library category groups. Reports can be sent to specified recipients on a daily, weekly, and/or monthly basis.

Custom Report Wizard

When clicking Custom Report Wizard in the Custom Reports menu, the main screen of the Custom Report Wizard displays in the panel:

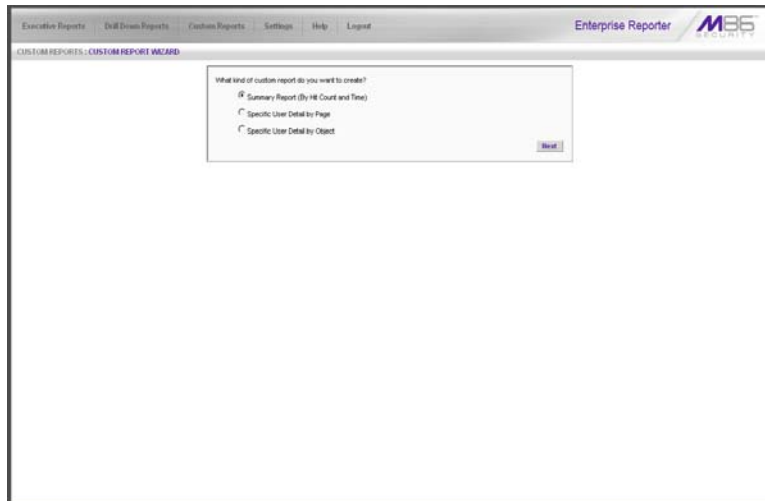


Fig. 3:6-1 Custom Report Wizard screen (administrator)

Step 1: Specify Report Option

- Select one of three available custom 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.
 - Specific User Detail by Page** - this report provides information about end user Web page access for a specified time period.
 - Specific User Detail by Object** - this report provides information about end user Web object access for a specified time period.
- Click **Next** to display the next screen of the wizard.

When selecting the summary report option, the following screen displays in the panel after clicking Next:

The screenshot shows the 'Summary Report (By Hit Count and Time)' wizard screen. The form is titled 'CUSTOM REPORTS - CUSTOM REPORT WIZARD - SUMMARY REPORT (BY HIT COUNT AND TIME)'. It contains the following fields and options:

- What type of summary results do you want?**
 - Type: Categories (dropdown)
- Do you want to narrow the summary results within specific criteria?**
 - Category: All (dropdown)
 - User IP: (text input)
 - Username: (text input)
 - Site: (text input)
 - Category Group: (dropdown)
 - User Group: (dropdown)
- Specify the date scope:**
 - Date Scope: Today (dropdown)
 - From Date: 11/21/2009 (calendar)
 - To Date: 11/21/2009 (calendar)
 - From Time: 11:00 AM (time)
 - To Time: 11:00 PM (time)
- Select the display and sort criteria:**
 - Display: All Data Shown (dropdown)
 - Sort by: Page Count (dropdown)
 - # Records: All (text input)
 - Order: Descending (dropdown)

Buttons at the bottom: Save Custom Report, View All Data Results.

Fig. 3:6-2 Summary Report wizard screen (administrator)

When selecting the detail report option, the following screen displays after clicking Next:

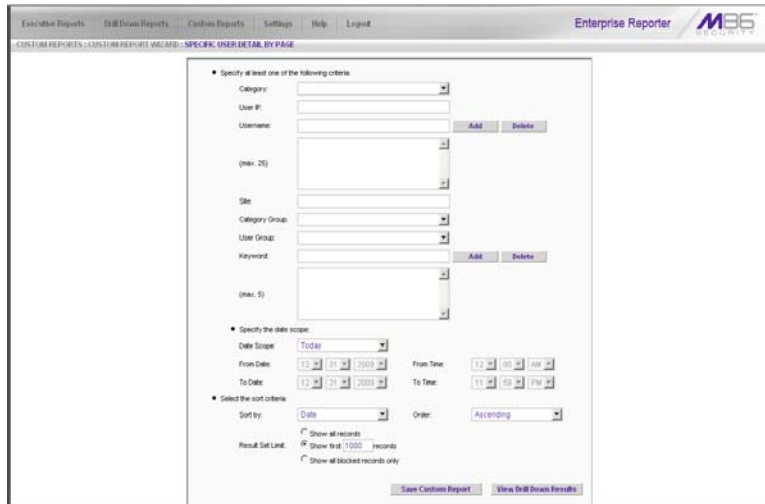


Fig. 3:6-3 Detail Report by Page wizard screen (administrator)



NOTES: The detail report by object screen is similar to the detail report by page screen, substituting the word “Object” for “Page” in the navigation path.

See Report View Components in Chapter 4: Summary and Detail Reports for various field entries in this wizard.

Step 2: Specify Report Selection

Summary report

Make a choice for the **Type** of report to be generated: “Categories”, “IPs”, “Users”, “Sites”, “Category Groups”, “User Groups”. This choice affects all other fields on the screen by enabling or disabling them as pertinent to your selection.

To **narrow** your results, choose from one of the following drill down report options: “Category”, “User IP”, “Username”, “Site”, “Category Group”, “User Group”.

Detail report

Select at least one of the following **criteria** to be included in your query: “Category”, “User IP”, “Username”, “Site”, “Category Group”, “User Group”, “Keyword”.



TIP: The Username and Keyword fields can be used in conjunction or individually to specify the username(s) and/or URL substring(s)/keyword(s) to include in a query, as described in the following sub-sections.

Batch user report

To generate a batch user report in which a single email is sent to the administrator with attached reports for up to 25 specified end users, make the following entries:

1. In the **Username** field, do one of the following to add a username in the list box below:
 - Type in the username
 - Enter valid alpha characters preceded and/or followed by a wildcard ('%'), or
 - Enter a wildcard ('%')
2. Click **Add**; if a wildcard was used and more than one match was found on the server, this action opens the

Specific Search pop-up box (see Fig. 3:6-8) that displays all available matches in the Username frame:

- a. Select up to 25 usernames from the pop-up box.
- b. Click **OK** to close the pop-up box and to populate the list box in the wizard screen.



TIP: To remove an entry from the list box, select it and then click **Delete**.



NOTE: If more than one Username is entered, the following message displays above the buttons at the bottom of this screen: 'NOTE: This report is very processor and time intensive and may take several minutes to complete.' and the **View Drill Down Results** button displays greyed-out. The report must now be saved and run at a later time.

URL sub-string, keyword report

To generate a URL sub-string and/or keyword report, make the following entries:

1. In the **Keyword** field, do one of the following to add keywords/URL sub-strings in the list box below:
 - Type in a keyword at least three characters in length
 - Enter up to 255 characters of a phrase
2. Click **Add**.



TIP: To remove an entry from the list box, select it and then click **Delete**.



NOTE: After adding an entry in the **Keyword** field, the following message displays above the buttons at the bottom of this screen: 'NOTE: This report is very processor and time intensive and may take several minutes to complete.' and the **View Drill Down Results** button displays greyed-out. The report must now be saved and run at a later time.

Step 3: Specify Date Scope

Select the **Date Scope** from the following choices available in the pull-down menu.



NOTE: *If more than one Username or if any Keyword was entered in this screen, 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”.*

Step 4: Specify Order Criteria

Summary report

Select the column for which top results should **Display** and indicate the **# Records**.

Specify the column the report should **Sort by** and in which **Order**.

Detail report

Select the column the report should **Sort by** and indicate in which **Order**.

Specify the **Result Set Limit** for the records to be included.

Step 5: 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:

- **Save Custom Report** - click this button to go to the Save Custom Report window 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 5: Drill Down Reports for information about drill down reports.*

- **View Drill Down Results** - click this button to view the generated Drill Down Report now in the specified report view format (see Figs. 3:6-4 and 3:6-5).



NOTE: The View Drill Down Results button greys-out if more than one Username or if any Keyword was entered for a detail report.

The screenshot shows the 'SUMMARY DRILL DOWN REPORT' interface. At the top, there are navigation tabs: 'Executive Reports', 'Drill Down Reports', 'Custom Reports', 'Settings', 'Help', and 'Logout'. The 'Enterprise Reporter M86 SECURITY' logo is in the top right. Below the navigation is a 'DRILL DOWN REPORTS: CATEGORIES' section with buttons for 'New Report', 'Modify Report', 'Export Report', 'Save Report', and 'Set Result Level'. The main area displays a table with columns: Categories, Category, Category, Category, Category, IP Count, User Count, Site Count, Page Count, Object Count, and HitCount. The table lists various categories such as Search Engines, Information Technology, Yahoo Mail, ResearchWeb Ads, Web Based Email, General Business, ERG, Edge Content News/Softw., Wireless Line Manager, JobsHome, Shipping, Financial Institution, Image Search & Image Search, Flash Ads, Informational News, Reference, Forums, Online Communities, Weather/Traffic, News, Chat, Google Chat, Web Legal/Financial Pages, Research Training Media, ICDL/IT, Music & Entertainment, Internet Service Provider, and Password/Profile Sharing.

Fig. 3:6-4 Summary Drill Down Report (administrator)

The screenshot shows the 'DETAIL BY OBJECT REPORT' interface. It includes the same navigation and logo as Fig. 3:6-4. Below the navigation is a 'DETAIL BY OBJECT REPORT' section with filters for 'Categories', 'Dates', 'Start By Date', and 'Display All records'. There are also checkboxes for 'Category', 'User IP', 'User', 'Filter Action', 'Content Type', 'Content', and 'Search String'. A 'Modify Report' button and a 'NoClick All' button are present. The main area displays a detailed table with columns: Date, Category, User IP, User, Site, Filter Action, Content Type, Content, and Search String. The table lists individual entries for the 'Shipping' category, showing dates from 12/05/2009 12:00:36 AM to 12/05/2009 3:00:48 AM, user IP addresses, usernames, and search strings.

Fig. 3:6-5 Detail by Page Drill Down Report (administrator)

Save Custom Report

1. Click the **Save Custom Report** button to display the Save Custom Report screen in the panel:

Fig. 3:6-6 Summary Save Custom Report (administrator)

Fig. 3:6-7 Detail Save Custom Report (administrator)

2. In the **Save Name** field, enter a name for the report. This name will display in the Report Name pull-down menu in the Saved Custom Reports option.



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. This description will display in the Report Description field in the Saved Custom Reports option.
4. Make a selection from pull-down menus for the following fields:
 - **Date Scope** - to change the date scope specified in the report view, make a selection from available choices in the pull-down menus.
 - **Break type** - available selections are based on the type of report specified.
 - **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.
 - **Hide Un-Identified IPs** - this checkbox is de-selected by default if the checkbox by this same name was de-selected in the Default Options window.



NOTE: The Default Options window is accessible via Default Options in the Settings menu. See the Default Options sub-section in Chapter 2: Customizing the Client for more information about the Hide Un-Identified IPs option.

5. 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.
 - **Result Set Limit** - indicate the maximum number of records to be included in the report.

6. **For double/single-break reports only**, if a selection was made in the Break type field, specify the top count option to be used in the **Amount shown** and **# Records** fields.
7. **For pie and bar charts only** in a summary report, if the report is being generated for Categories, Category Groups, or User Groups, and a selection was made in the Break type field, the **Generate using** field lets you select the count column sort option.
8. **For E-Mail output only**, type in the email address(es) of the recipient(s), and enter any pertinent information to be sent with the report.
9. 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 Event Schedules window where the Add Event to Schedule pop-up box opens so you can set up a schedule for running the report.
 - **Save and Run** - 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 Custom Reports window displays if you need to run this report again or another report.



NOTE: *If more than one Username or if any Keyword was entered in the report screen for a detail report, the Save and Run button is greyed-out and the following message displays above the buttons at the bottom of this screen: 'NOTE: This report is very processor and time intensive and may take several minutes to complete.'*

- **Save Only** - click this button to save your entries and to go to the Saved Custom Reports window where you can delete, edit, or run this report or another report.



NOTE: *See Event Schedules and Saved Custom Reports in this chapter for information on using these options.*



TIP: For an administrator, when specifying a save option, if the report Name you entered has already been used, a dialog box opens with the message: “Name already in use, would you like to overwrite? Event Schedules associated with this report will also be deleted.” You can choose to either overwrite the record with the current report criteria by clicking **OK**, or rename the report by clicking **Cancel** to close the dialog box without saving your edits.

Wizard Reporting Tips

Detail page Break report by Users, Category

To generate a detail report that includes page hits for the top users who accessed a specific category or category group:

1. Select “Specific User Detail by Page”, and then click **Next**.
3. Choose the **Category** or **Category Group**, and then click **Save Custom Report**.
3. Specify at least the following criteria: **Save Name**, **Break type** “Users”, **Amount shown** “Top Page Count”, and email **To** address.
4. Click **Save and Run** to generate and email the report to the designated email address.

Use wildcards in a Specific Search query

To generate a report for a specific username, user IP address, or site URL, enter the minimum criteria:

1. Select one of the three wizard options, and then click **Next**.
2. Specify the type of search to be performed by choosing the appropriate field (**User IP**, **Username**, or **Site**) and entering text in the following format: **%X%** (in which “X” represents the user’s IP address, the username, or the site URL).

Examples:

- User IP: **%200.10.100.51%**
 - Username: **%jsmith%**
 - Site: **%yahoo%**
3. Click **View Drill Down Results** to open the Specific Search pop-up box:

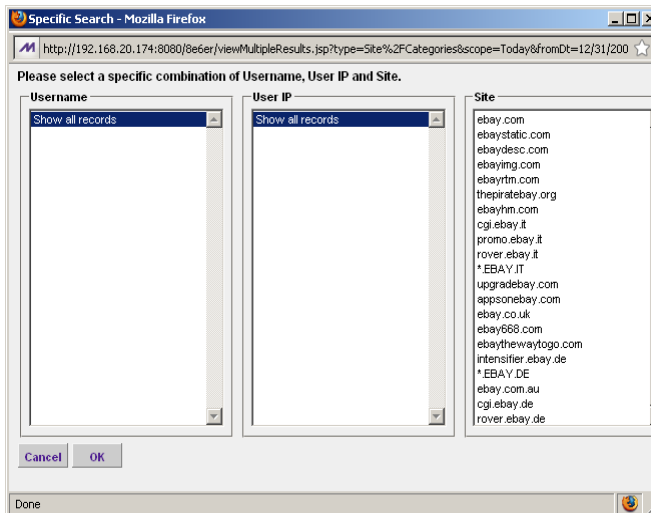


Fig. 3:6-8 Specific Search pop-up box showing site results

This pop-up box is comprised of three list boxes: Username, User IP, and Site. The list box pertinent to your query is populated with results—based on data stored in the system—returned by the search.

4. Make a selection from the list box, and then click **OK** to close the pop-up box and to begin generating the report.

Sample Custom Reports

To generate a sample custom report:

1. Choose Sample Custom Reports from the Custom Reports menu, and then click one of the following Custom Report options: “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”.

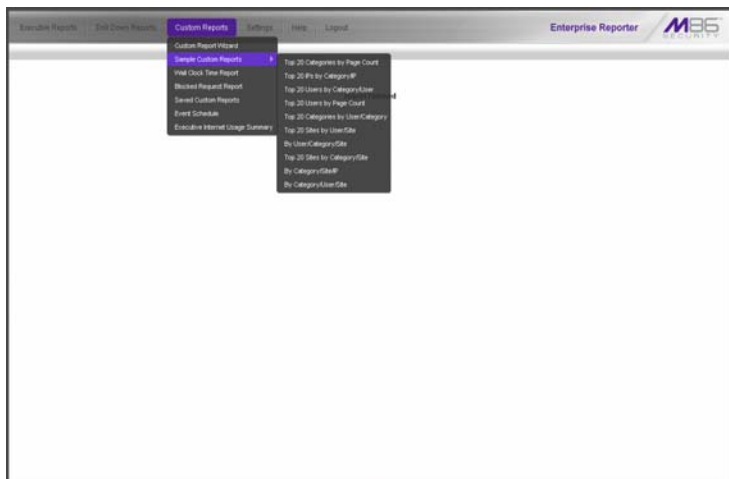




Fig. 3:6-9 Sample Custom Reports (administrator)

When the report has been generated, “Report Finished” displays in the window/tab and a separate browser window opens with the Sample Custom Report in the PDF format.

2. From the open PDF file, the Sample Custom 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 - click the save  icon to open the Save a Copy dialog box, and proceed with standard save procedures.
3. Click the “X” in the upper right corner of the report window to close it.

Report Format

For each report, the header of the reports contain the following information:

- **Sort Order: Page Count, descending**
- **From: / To:** today’s date displays
- the name of the report displays

The footer of the reports contain the following information:

- today’s date (MM/DD/YYYY) and time (HH:MM:SS AM/PM) the report was generated
- **Page** number
- **Filter: None**
- **Generated by:** manager’s login ID

Top 20 Categories by Page Count

The name of the report (Categories) displays in the header.

The body of the report contains the following columns: list of the top 20 Categories and corresponding IP Count, User Count, Site Count, Page Count, Object Count, Time (HH:MM:SS), Hit Count, and Blocked Hits.

The Grand Total and Count display at the end of the report.

| Enterprise Reporter | | Dec 30, 2009 - Dec 30, 2009 | | | | | M86 SECURITY | |
|--------------------------------------|----------|-----------------------------|------------|------------|--------------|-----------------|--------------|--------------|
| Sort Order: Page Count, descending | | Categories | | | | | | |
| Categories | IP Count | User Count | Site Count | Page Count | Object Count | Time (HH:MM:SS) | Hit Count | Blocked Hits |
| MSNMG | 62 | 475 | 248 | 3,594 | 670 | 6:30:20 | 4,270 | 0 |
| Search Engines | 101 | 1,417 | 10 | 2,508 | 1,778 | 3:5:50 | 4,244 | 0 |
| Banner/Pop Ads | 82 | 512 | 43 | 610 | 1,552 | 1:4:40 | 2,162 | 0 |
| Information Technology | 64 | 439 | 29 | 594 | 1,333 | 0:51:20 | 1,827 | 0 |
| Web Based Email | 45 | 376 | 12 | 525 | 479 | 1:51:10 | 999 | 0 |
| Chat | 30 | 235 | 7 | 408 | 16 | 0:58:40 | 454 | 0 |
| Shopping | 16 | 119 | 15 | 256 | 261 | 0:24:50 | 517 | 0 |
| General Business | 56 | 443 | 25 | 213 | 3,633 | 0:28:0 | 3,736 | 0 |
| Internet Radio | 11 | 86 | 5 | 124 | 192 | 0:10:30 | 316 | 0 |
| Entertainment | 17 | 123 | 14 | 121 | 465 | 0:12:0 | 566 | 0 |
| Travel | 11 | 59 | 11 | 110 | 1,310 | 0:8:40 | 1,420 | 0 |
| News | 32 | 194 | 28 | 92 | 1,224 | 0:10:20 | 1,318 | 0 |
| R Rated | 3 | 33 | 2 | 86 | 0 | 0:10:0 | 86 | 0 |
| Pornography/Adult Content | 7 | 69 | 10 | 71 | 411 | 0:10:20 | 482 | 0 |
| Vehicles | 3 | 25 | 3 | 64 | 222 | 0:3:10 | 296 | 0 |
| Online Greeting Cards | 2 | 17 | 2 | 64 | 1,213 | 0:4:50 | 1,277 | 0 |
| Gambling | 1 | 11 | 1 | 58 | 8 | 0:8:30 | 66 | 0 |
| Games | 6 | 48 | 5 | 57 | 67 | 0:5:50 | 124 | 0 |
| Online Auction | 7 | 44 | 6 | 56 | 355 | 0:9:20 | 481 | 0 |
| Dating/Personals | 13 | 84 | 5 | 45 | 542 | 0:4:50 | 587 | 0 |
| Financial Institution | 17 | 91 | 8 | 41 | 338 | 0:5:20 | 379 | 0 |
| Message Boards | 3 | 24 | 2 | 38 | 81 | 0:2:30 | 119 | 0 |
| Recreation | 5 | 28 | 5 | 36 | 254 | 0:4:18 | 290 | 0 |
| Web Logs/Personal Pages | 5 | 37 | 3 | 35 | 52 | 0+0 | 87 | 0 |
| Sports | 4 | 34 | 4 | 73 | 77 | 0:3:50 | 92 | 0 |
| Government | 4 | 27 | 4 | 21 | 509 | 0:2:20 | 529 | 0 |
| Movies & Television | 8 | 35 | 7 | 19 | 32 | 0:3:10 | 51 | 0 |
| Internet Service Provider | 3 | 15 | 1 | 18 | 0 | 0:0 | 18 | 0 |
| TESTING | 4 | 24 | 1 | 17 | 51 | 0:2:50 | 68 | 0 |
| Generic Streaming Media | 9 | 58 | 6 | 14 | 394 | 0:2:20 | 399 | 0 |
| Image Servers & Image Search Engines | 3 | 29 | 3 | 14 | 84 | 0:1:10 | 96 | 0 |
| Social Opinion | 4 | 20 | 2 | 14 | 221 | 0:2:0 | 235 | 0 |
| Weather/Traffic | 2 | 9 | 2 | 14 | 180 | 0:1:18 | 194 | 0 |
| Portals | 13 | 62 | 4 | 13 | 613 | 0:2:0 | 526 | 0 |

12/31/2009 10:33:21 AM Generated by: manager Filter: None Page 1 of 2

Fig. 3:6-10 Sample Categories report

Top 20 IPs by Category/IP

The name of the report (Category/IPs: Top 20 IPs by Page Count) displays in the header.

The body of the report contains the following information for each Category listed: columns showing the top 20 user IPs and corresponding User Count, Site Count, Page Count, Object Count, Time (HH:MM:SS), Hit Count, and Blocked Hits.

The category Total and IP Count display at the end of each Category section.

The Grand Total and Category Count display at the end of the report.

| Enterprise Reporter | | Dec 04, 2009 - Dec 04, 2009 | | | | M86 SECURITY | |
|---|------------|-----------------------------|------------|--------------|-----------------|--------------|--------------|
| Sort Order: Page Count, descending | | Category/IPs | | | | | |
| | | Top 20 IPs by Page Count | | | | | |
| Category:Uncategorized | | | | | | | |
| IPs | User Count | Site Count | Page Count | Object Count | Time (HH:MM:SS) | Hit Count | Blocked Hits |
| 192.168.80.80 | 1 | 16 | 961 | 278 | 0:30:54 | 1,237 | 0 |
| 192.168.30.82 | 1 | 26 | 855 | 227 | 0:19:0 | 1,002 | 0 |
| 208.90.237.42 | 2 | 7 | 791 | 211 | 0:22:24 | 1,002 | 0 |
| 208.90.239.80 | 1 | 1 | 742 | 0 | 0:2:24 | 742 | 0 |
| 208.90.239.118 | 1 | 1 | 738 | 0 | 0:0:18 | 738 | 0 |
| 208.90.237.244 | 1 | 3 | 725 | 0 | 0:0:32 | 725 | 0 |
| 208.90.239.3 | 1 | 1 | 704 | 0 | 0:5:24 | 704 | 0 |
| 192.168.30.06 | 1 | 11 | 675 | 24 | 0:34:22 | 699 | 0 |
| 192.168.30.87 | 1 | 30 | 238 | 87 | 0:10:24 | 293 | 0 |
| 208.90.237.60 | 1 | 4 | 143 | 1 | 0:2:28 | 144 | 0 |
| 192.168.102.118 | 1 | 23 | 139 | 112 | 0:8:4 | 251 | 0 |
| 208.90.237.101 | 1 | 17 | 125 | 483 | 0:0:24 | 608 | 0 |
| 192.168.30.84 | 1 | 10 | 97 | 2 | 0:8:4 | 99 | 0 |
| 208.90.237.15 | 1 | 25 | 95 | 107 | 0:15:36 | 232 | 0 |
| 208.90.239.84 | 2 | 0 | 93 | 322 | 0:3:4 | 468 | 0 |
| 208.90.239.37 | 1 | 20 | 88 | 75 | 0:2:20 | 183 | 0 |
| 208.90.237.47 | 1 | 13 | 75 | 459 | 0:1:44 | 533 | 0 |
| 208.90.239.17 | 2 | 10 | 69 | 95 | 0:1:24 | 134 | 0 |
| 208.90.237.50 | 1 | 20 | 56 | 116 | 0:3:30 | 172 | 0 |
| 208.90.237.8 | 1 | 16 | 56 | 90 | 0:2:48 | 148 | 0 |
| Total for Uncategorized | | | | | | | |
| IP Count: 20 sorted by Page Count, descending | | | | | | | |
| | 33 | 279 | 7,460 | 2,877 | 3:43:48 | 10,137 | 0 |
| Category:Peer-to-peer/File Sharing | | | | | | | |
| IPs | User Count | Site Count | Page Count | Object Count | Time (HH:MM:SS) | Hit Count | Blocked Hits |
| 208.90.239.80 | 1 | 1 | 362 | 6,267 | 0:22:32 | 6,333 | 0 |
| 208.90.239.37 | 1 | 1 | 4 | 0 | 0:0:15 | 4 | 0 |
| 12/31/2009 2:46:44 PM Generated by: manager Filter: None Page 1 of 40 | | | | | | | |

Fig. 3:6-11 Sample Category/IPs report

Top 20 Users by Category/User

The name of the report (Category/Users: Top 20 Users by Page Count) displays in the header.

The body of the report contains the following information for each Category listed: columns showing the top 20 Users (usernames/username paths) and corresponding IP Count, Site Count, Page Count, Object Count, Time (HH:MM:SS), Hit Count, and Blocked Hits.

The category Total and User Count display at the end of each Category section.

The Grand Total and Category Count display at the end of the report.

| Enterprise Reporter | | Dec 04, 2009 - Dec: 04, 2009 | | M86 SECURITY | | | | |
|---|----------|------------------------------|------------|--------------|-----------------|--------------|--------------|---|
| Sort Order: Page Count, descending | | Category/Users | | | | | | |
| | | Top 20 Users by Page Count | | | | | | |
| Category: Unategorized | | | | | | | | |
| Users | IP Count | Site Count | Page Count | Object Count | Time (HH:MM:SS) | Hit Count | Blocked Hits | |
| 192.168.30.80 | 1 | 15 | 961 | 278 | 0:36:24 | 1,237 | 0 | |
| 192.168.30.82 | 1 | 28 | 955 | 227 | 0:19:19 | 1,082 | 0 | |
| LOGO/Marketing/edavid | 1 | 7 | 780 | 200 | 0:52:16 | 908 | 0 | |
| 208.90.238.60 | 1 | 1 | 742 | 0 | 0:7:24 | 742 | 0 | |
| 208.90.238.115 | 1 | 1 | 736 | 0 | 0:8:19 | 736 | 0 | |
| 208.90.237.244 | 1 | 3 | 725 | 0 | 0:5:32 | 725 | 0 | |
| 208.90.239.3 | 1 | 1 | 704 | 0 | 0:5:24 | 704 | 0 | |
| 192.168.30.85 | 1 | 11 | 675 | 24 | 0:34:32 | 866 | 0 | |
| 192.168.30.87 | 1 | 39 | 230 | 57 | 0:10:24 | 293 | 0 | |
| LOGO/Sales/breaks | 1 | 4 | 143 | 1 | 0:2:28 | 144 | 0 | |
| News02021/INDIVIDUAL/USBR3_CA_USA_ch | 1 | 23 | 139 | 112 | 0:9:4 | 251 | 0 | |
| 208.90.237.101 | 1 | 17 | 125 | 483 | 0:8:24 | 809 | 0 | |
| 192.168.30.84 | 1 | 10 | 97 | 2 | 0:6:4 | 99 | 0 | |
| 208.90.237.15 | 1 | 25 | 85 | 187 | 0:5:24 | 262 | 0 | |
| LOGO/Programmer/fengtai | 1 | 20 | 88 | 75 | 0:2:20 | 163 | 0 | |
| LOGO/Administrator/miller | 1 | 13 | 75 | 450 | 0:1:44 | 533 | 0 | |
| LOGO/INDIVIDUAL/username | 1 | 10 | 67 | 60 | 0:1:20 | 133 | 0 | |
| 208.90.239.84 | 1 | 8 | 62 | 214 | 0:1:40 | 276 | 0 | |
| 208.90.237.8 | 1 | 15 | 56 | 90 | 0:2:48 | 146 | 0 | |
| LOGO/DEFAULT/username | 1 | 28 | 50 | 110 | 0:3:30 | 172 | 0 | |
| Total for Unategorized | | 20 | 278 | 7,420 | 2,517 | 3:42:12 | 9,943 | 0 |
| User Count: 20 sorted by Page Count, descending | | | | | | | | |
| Category: Peer-to-peer/File Sharing | | | | | | | | |
| Users | IP Count | Site Count | Page Count | Object Count | Time (HH:MM:SS) | Hit Count | Blocked Hits | |
| 208.90.238.60 | 1 | 352 | 6,297 | 16 | 5:22:32 | 6,313 | 0 | |
| 12/31/2009 2:49:55 PM | | Generated by: manager | | Filter: None | | Page 1 of 50 | | |

Fig. 3.6-12 Sample Category/Users report

Top 20 Users by Page Count

The name of the report (Users) displays in the header.

The body of the report contains columns with the following information for the top 20 Users: usernames/username paths and corresponding Category Count, IP Count, Site Count, Page Count, Object Count, Time (HH:MM:SS), Hit Count, and Blocked Hits.

The Grand Total and user Count display at the end of the report.

| Enterprise Reporter | | Dec 04, 2009 - Dec 04, 2009 | | M86 SECURITY | | | | | |
|------------------------------------|----------------|-----------------------------|------------|--------------|--------------|-----------------|-----------|--------------|--|
| Sort Order: Page Count, descending | | | | | | | | | |
| Users | | | | | | | | | |
| Users | Category Count | IP Count | Site Count | Page Count | Object Count | Time (HH:MM:SS) | Hit Count | Blocked Hits | |
| 208.90.238.60 | 23 | 1 | 421 | 6,788 | 794 | 0:37:44 | 7,542 | 0 | |
| LOOO\Sales\Deford | 34 | 1 | 139 | 2,362 | 4,472 | 1:31:09 | 6,804 | 0 | |
| LOOO\Sales\peters | 20 | 1 | 71 | 2,174 | 1,266 | 1:02:19 | 3,573 | 0 | |
| 192.168.30.80 | 28 | 1 | 143 | 1,917 | 3,360 | 1:23:10 | 4,277 | 1,125 | |
| 208.90.237.10 | 30 | 1 | 132 | 1,883 | 1,427 | 1:49:12 | 3,310 | 30 | |
| LOOO\DEFAULT\Taskbar.dlwt | 31 | 1 | 103 | 1,537 | 2,053 | 1:44:30 | 3,640 | 2 | |
| LOOO\Sales\Hunt | 19 | 2 | 83 | 1,561 | 595 | 0:55:16 | 2,177 | 0 | |
| LOOO\Marketing\edavid | 23 | 1 | 93 | 1,549 | 1,739 | 1:32:16 | 3,258 | 1 | |
| LOOO\Sales\jehua\mailface | 17 | 1 | 66 | 1,481 | 277 | 1:14:24 | 1,758 | 0 | |
| 208.90.237.17 | 33 | 1 | 114 | 1,374 | 1,447 | 0:55:12 | 2,821 | 43 | |
| 208.90.237.101 | 36 | 1 | 149 | 1,329 | 3,333 | 1:12:20 | 3,662 | 33 | |
| LOOO\Marketing\mbath | 25 | 1 | 119 | 1,296 | 1,723 | 0:25:40 | 3,021 | 0 | |
| 208.90.238.31 | 34 | 1 | 136 | 1,278 | 3,207 | 0:48:44 | 4,485 | 0 | |
| 208.90.238.19 | 25 | 1 | 80 | 1,240 | 882 | 1:8:48 | 2,122 | 0 | |
| LOOO\Sales\pouah | 29 | 1 | 70 | 1,240 | 840 | 1:8:4 | 2,080 | 0 | |
| LOOO\INDIVIDUAL\ho | 15 | 1 | 41 | 1,231 | 130 | 1:03 | 1,361 | 0 | |
| Novell\2007\INDIVIDUAL\USERS_CA_US | 27 | 1 | 140 | 1,218 | 2,550 | 0:51:04 | 3,768 | 0 | |
| A_rhoo | | | | | | | | | |
| LOOO\Sales\kondosky | 15 | 1 | 35 | 1,171 | 508 | 1:04:44 | 1,679 | 1 | |
| 192.168.30.80 | 17 | 1 | 84 | 1,115 | 1,429 | 0:30:40 | 2,544 | 0 | |
| 192.168.30.80 | 16 | 1 | 38 | 1,082 | 460 | 0:42:20 | 1,542 | 0 | |
| Grand Total | 406 | 21 | 2,316 | 34,028 | 30,836 | 27:16:82 | 65,464 | 1,238 | |
| Count: 20 | | | | | | | | | |

12/31/2009 2:56:55 PM Generated by: manager Filter: None Page 1 of 1

Fig. 3:6-13 Sample Users report

Top 20 Categories by User/Category

The name of the report (Users/Categories: Top 20 Categories by Page Count) displays in the header.

The body of the report contains columns with the following information for each User listed: top 20 Categories and corresponding IP Count, Site Count, Page Count, Object Count, Time (HH:MM:SS), Hit Count, and Blocked Hits.

The user Total and Category Count display at the end of each User section.

The Grand Total and User Count display at the end of the report.

| Enterprise Reporter | | Dec 04, 2009 - Dec 04, 2009 | | | | M86 SECURITY | |
|---|-----------|---------------------------------|--------------|--------------|-----------------|--------------|--------------|
| Sort Order: Page Count, descending | | User/Categories | | | | | |
| User: 208.90.238.60 | | Top 20 Categories by Page Count | | | | | |
| Categories | IP Count | Site Count | Page Count | Object Count | Time (HH:MM:SS) | Hit Count | Blocked Hits |
| Peer-to-peer/File Sharing | 1 | 352 | 6,287 | 10 | 5:22:32 | 6,313 | 0 |
| Flash Video | 1 | 15 | 170 | 0 | 0:20 | 170 | 0 |
| Financial Institution | 1 | 5 | 57 | 7 | 0:156 | 64 | 0 |
| Online Trading/Investment | 1 | 2 | 47 | 56 | 0:14 | 103 | 0 |
| Banner/Web Ads | 1 | 11 | 38 | 80 | 0:148 | 118 | 0 |
| General Business | 1 | 8 | 37 | 2 | 0:130 | 39 | 0 |
| Search Engines | 1 | 8 | 25 | 127 | 0:10 | 152 | 0 |
| Music | 1 | 2 | 24 | 68 | 0:14 | 82 | 0 |
| Entertainment | 1 | 2 | 18 | 208 | 0:82 | 220 | 0 |
| Image Servers & Image Search Engines | 1 | 2 | 18 | 1 | 0:40 | 18 | 0 |
| Web Based Email | 1 | 1 | 10 | 2 | 0:20 | 17 | 0 |
| Information Technology | 1 | 9 | 12 | 13 | 0:48 | 25 | 0 |
| Yahoo IM | 1 | 2 | 7 | 2 | 0:24 | 9 | 0 |
| Web Hosts | 1 | 2 | 7 | 0 | 0:12 | 7 | 0 |
| Intranet/Internal Servers | 1 | 1 | 6 | 0 | 0:24 | 6 | 0 |
| Uncategorized | 1 | 6 | 10 | 10 | 0:24 | 16 | 0 |
| Shopping | 1 | 1 | 5 | 0 | 0:20 | 5 | 0 |
| Edge Content Servers/Infrastructure | 1 | 4 | 2 | 37 | 0:8 | 39 | 0 |
| Free Hosts | 1 | 1 | 2 | 0 | 0:8 | 2 | 0 |
| Recreation | 1 | 1 | 1 | 0 | 0:4 | 1 | 0 |
| Total for 208.90.238.60 | 20 | 435 | 6,788 | 616 | 5:37:44 | 7,404 | 0 |
| Category Count: 20 sorted by Page Count, descending | | | | | | | |
| User: LOGON\Sales@deloid | | | | | | | |
| Categories | IP Count | Site Count | Page Count | Object Count | Time (HH:MM:SS) | Hit Count | Blocked Hits |
| Yahoo IM | 1 | 2 | 922 | 0 | 0:50:30 | 922 | 0 |
| Search Engines | 1 | 9 | 448 | 274 | 0:10:26 | 722 | 0 |
| 12/31/2009 3:10:20 PM Generated by: manager Filter: None Page 1 of 75 | | | | | | | |

Fig. 3:6-14 Sample User/Categories report

Top 20 Sites by User/Site

The name of the report (User/Sites: Top 20 Sites by Page Count) displays in the header.

The body of the report contains columns with the following information for each User listed: top 20 Sites and corresponding Category Count, IP Count, Page Count, Object Count, Time (HH:MM:SS), Hit Count, and Blocked Hits.

The user Total and Site Count display at the end of each User section.

The Grand Total and User Count display at the end of the report.

| Enterprise Reporter | | Dec 04, 2009 - Dec 04, 2009 | | M86 SECURITY | | | | |
|---|----------------|-----------------------------|------------|--------------|-----------------|--------------|--------------|---|
| Sort Order: Page Count, descending | | User/Sites | | | | | | |
| | | Top 20 Sites by Page Count | | | | | | |
| User: 208.90.238.60 | | | | | | | | |
| Sites | Category Count | IP Count | Page Count | Object Count | Time (HH:MM:SS) | Hit Count | Blocked Hits | |
| digitalhive.org | 2 | 1 | 422 | 91 | 0:59 | 479 | 0 | |
| 208.214.62.77 | 1 | 1 | 421 | 0 | 0:20:16 | 421 | 0 | |
| 75.47.114.65 | 1 | 1 | 223 | 0 | 0:2:52 | 223 | 0 | |
| 188.126.04.03 | 1 | 1 | 166 | 0 | 0:7:36 | 166 | 0 | |
| 78.82.203.131 | 1 | 1 | 138 | 0 | 0:6:40 | 138 | 0 | |
| 218.246.122.225 | 1 | 1 | 129 | 0 | 0:6:12 | 129 | 0 | |
| 82.80.80.27 | 1 | 1 | 125 | 0 | 0:8:20 | 125 | 0 | |
| 82.166.38.36 | 1 | 1 | 125 | 0 | 0:7:34 | 125 | 0 | |
| 69.155.113.134 | 1 | 1 | 99 | 0 | 0:3:20 | 99 | 0 | |
| 70.82.79.151 | 1 | 1 | 93 | 0 | 0:6:12 | 93 | 0 | |
| 122.162.90.18 | 1 | 1 | 89 | 0 | 0:4:20 | 89 | 0 | |
| 88.148.65.58 | 1 | 1 | 88 | 0 | 0:6:12 | 88 | 0 | |
| 77.109.72.221 | 1 | 1 | 87 | 0 | 0:5:44 | 87 | 0 | |
| 68.95.249.9 | 1 | 1 | 82 | 0 | 0:6:12 | 82 | 0 | |
| 94.23.42.170 | 1 | 1 | 81 | 0 | 0:2:8 | 81 | 0 | |
| 215.88.88.240 | 1 | 1 | 81 | 0 | 0:2:52 | 81 | 0 | |
| 91.121.151.193 | 1 | 1 | 80 | 0 | 0:2:59 | 80 | 0 | |
| 212.117.166.123 | 1 | 1 | 80 | 0 | 0:3:9 | 80 | 0 | |
| yahoo.com | 7 | 1 | 74 | 32 | 0:2:40 | 106 | 0 | |
| ameritrade.com | 2 | 1 | 48 | 0 | 0:1:44 | 68 | 0 | |
| Total for 208.90.238.60 | | 28 | 20 | 2,746 | 83 | 1:42:48 | 2,829 | 0 |
| Site Count: 20 sorted by Page Count, descending | | | | | | | | |
| User: LOGO\Sales\delrod | | | | | | | | |
| Sites | Category Count | IP Count | Page Count | Object Count | Time (HH:MM:SS) | Hit Count | Blocked Hits | |
| 88.180.217.13 | 1 | 1 | 914 | 0 | 0:58:12 | 914 | 0 | |
| google.com | 5 | 1 | 393 | 101 | 0:9:52 | 494 | 0 | |
| 12/31/2009 3:15:41 PM | | Generated by: manager | | Filter: None | | Page 1 of 83 | | |

Fig. 3.6-15 Sample User/Sites report

By User/Category/Site

The name of the report (User/Category/Sites) displays in the header.

The body of the report contains columns with the following information for each User and Category listed: Sites and corresponding IP Count, Page Count, Object Count, Time (HH:MM:SS), Hit Count, and Blocked Hits.

The category Total and Site Count display at the end of each User/Category section.

The Grand Total and User Count display at the end of the report.

| Enterprise Reporter | | | | | | |
|--|----------|------------|--------------|-----------------|-----------|--------------|
| User/Category/Sites | | | | | | MB6 SECURITY |
| Sort Order: Page Count, descending | | | | | | |
| User: 208.90.238.60 | | | | | | |
| Category: BannerWeb Ads | | | | | | |
| Sites | IP Count | Page Count | Object Count | Time (HH:MM:SS) | Hit Count | Blocked Hits |
| yieldmanager.com | 1 | 19 | 0 | 0:0:22 | 19 | 0 |
| atdmt.com | 1 | 8 | 13 | 0:0:20 | 21 | 0 |
| doubleclick.net | 1 | 5 | 24 | 0:0:16 | 29 | 0 |
| admix.com | 1 | 3 | 0 | 0:0:8 | 3 | 0 |
| trafficamp.com | 1 | 2 | 0 | 0:0:8 | 2 | 0 |
| advertising.com | 1 | 1 | 1 | 0:0:4 | 2 | 0 |
| 2mdn.net | 1 | 0 | 11 | 0:0:0 | 11 | 0 |
| msk.com | 1 | 0 | 0 | 0:0:0 | 0 | 0 |
| unicast.com | 1 | 0 | 5 | 0:0:0 | 5 | 0 |
| reput.com | 1 | 0 | 17 | 0:0:0 | 17 | 0 |
| adbrn.com | 1 | 0 | 1 | 0:0:0 | 1 | 0 |
| Total for BannerWeb Ads | | | | | | |
| Site Count: 11 sorted by Page Count, descending | | | | | | |
| User: 208.90.238.60 | | | | | | |
| Category: Dating/Personals | | | | | | |
| Sites | IP Count | Page Count | Object Count | Time (HH:MM:SS) | Hit Count | Blocked Hits |
| match.com | 1 | 0 | 133 | 0:0:0 | 133 | 0 |
| Total for Dating/Personals | | | | | | |
| Site Count: 1 sorted by Page Count, descending | | | | | | |
| User: 208.90.238.60 | | | | | | |
| Category: Edge Content Servers/Infrastructure | | | | | | |
| 12/31/2009 3:18:15 PM Generated by: manager Filter: None Page 1 of 537 | | | | | | |

Fig. 3:6-16 Sample User/Category/Sites report

Top 20 Sites by Category/Site

The name of the report (Category/Sites: Top 20 Sites by Page Count) displays in the header.

The body of the report contains columns with the following information for each Category listed: Sites and corresponding IP Count, Page Count, Object Count, Time (HH:MM:SS), Hit Count, and Blocked Hits.

The category Total and Site Count display at the end of each Category section.

The Grand Total and Category Count display at the end of the report.

| Enterprise Reporter | | Dec 04, 2009 - Dec 04, 2009 | | | | M86 SECURITY | | |
|---|----------|-----------------------------|------------|--------------|-----------------|--------------|--------------|---|
| Sort Order: Page Count, descending | | Category/Sites | | | | | | |
| | | Top 20 Sites by Page Count | | | | | | |
| Category:Uncategorized | | | | | | | | |
| Sites | IP Count | User Count | Page Count | Object Count | Time (HH:MM:SS) | Hit Count | Blocked Hits | |
| 8e6.net | 15 | 15 | 3,041 | 0 | 0:37:44 | 3,041 | 0 | |
| 208.00.238.136 | 5 | 5 | 803 | 0 | 0:52:56 | 803 | 0 | |
| sementon.org | 1 | 1 | 580 | 0 | 0:38:20 | 580 | 0 | |
| 192.168.201.121 | 1 | 1 | 481 | 87 | 0:59:56 | 568 | 0 | |
| 192.168.20.90 | 2 | 2 | 433 | 256 | 0:6:18 | 689 | 0 | |
| 192.168.20.220 | 2 | 2 | 310 | 22 | 0:4:52 | 332 | 0 | |
| 8e6.com | 5 | 5 | 254 | 0 | 0:19:24 | 254 | 0 | |
| 60.248.169.141 | 1 | 1 | 241 | 23 | 0:6:24 | 264 | 0 | |
| x-space.info | 1 | 2 | 208 | 0 | 0:13:52 | 208 | 0 | |
| 216.246.122.102 | 2 | 2 | 126 | 0 | 0:1:56 | 126 | 0 | |
| 192.168.20.217 | 1 | 1 | 79 | 7 | 0:4:9 | 86 | 0 | |
| frjan.com | 2 | 2 | 76 | 0 | 0:4:4 | 76 | 0 | |
| 216.246.122.63 | 3 | 3 | 73 | 0 | 0:0:48 | 73 | 0 | |
| 199.203.243.203 | 3 | 3 | 64 | 323 | 0:3:12 | 387 | 0 | |
| 205.188.66.157 | 1 | 2 | 58 | 384 | 0:2:12 | 432 | 0 | |
| 216.246.122.101 | 1 | 1 | 57 | 0 | 0:0:40 | 57 | 0 | |
| 216.52.233.225 | 1 | 1 | 54 | 0 | 0:3:36 | 54 | 0 | |
| 216.246.122.108 | 2 | 2 | 42 | 0 | 0:0:24 | 42 | 0 | |
| hr-coachonline.com | 1 | 1 | 41 | 0 | 0:0:8 | 41 | 0 | |
| 68.142.207.36 | 1 | 1 | 40 | 0 | 0:0:40 | 40 | 0 | |
| Total for Uncategorized | | 51 | 53 | 7,061 | 1,082 | 3:39:24 | 8,143 | 0 |
| Site Count: 20 sorted by Page Count, descending | | | | | | | | |
| Category:Peer-to-peer/File Sharing | | | | | | | | |
| Sites | IP Count | User Count | Page Count | Object Count | Time (HH:MM:SS) | Hit Count | Blocked Hits | |
| 203.214.62.77 | 1 | 1 | 421 | 0 | 0:20:16 | 421 | 0 | |
| digitalhive.org | 1 | 1 | 416 | 16 | 0:4:44 | 432 | 0 | |
| 12/31/2009 3:19:18 PM | | Generated by: manager | | Filter: None | | Page 1 of 48 | | |

Fig. 3.6-17 Sample Category/Sites report

By Category/Site/IP

The name of the report (Category/Site/IPs) displays in the header.

The body of the report contains columns with the following information for each Category and Site listed: IPs and corresponding User Count, Page Count, Object Count, Time (HH:MM:SS), Hit Count, and Blocked Hits.

The category Total for each site and IP Count display at the end of each Category/Site section.

The Grand Total and Category Count display at the end of the report.

The screenshot shows the 'Enterprise Reporter' interface with the report title 'Category/Site/IPs' and the date range 'Dec 04, 2009 - Dec 04, 2009'. The M86 SECURITY logo is visible in the top right. The report is sorted by Page Count, descending.

| IPs | User Count | Page Count | Object Count | Time (HH:MM:SS) | Hit Count | Blocked Hits |
|--|------------|------------|--------------|-----------------|-----------|--------------|
| 208.60.237.15 | 1 | 0 | 19 | 0:03 | 19 | 0 |
| Total for 1105.govinfoevents.com | | | | | | |
| IP Count: 1 sorted by Page Count, descending | | | | | | |
| Category:Uncategorized | | | | | | |
| Site: 110.178.12.4 | | | | | | |
| IPs | User Count | Page Count | Object Count | Time (HH:MM:SS) | Hit Count | Blocked Hits |
| 208.60.239.37 | 1 | 11 | 0 | 0:15 | 11 | 0 |
| Total for 110.178.12.4 | | | | | | |
| IP Count: 1 sorted by Page Count, descending | | | | | | |
| Category:Uncategorized | | | | | | |
| Site: 123.129.242.168 | | | | | | |
| IPs | User Count | Page Count | Object Count | Time (HH:MM:SS) | Hit Count | Blocked Hits |
| 208.60.239.37 | 1 | 3 | 0 | 0:4 | 3 | 0 |
| Total for 123.129.242.168 | | | | | | |
| IP Count: 1 sorted by Page Count, descending | | | | | | |
| Category:Uncategorized | | | | | | |

At the bottom of the report, it shows the date and time '12/31/2009 3:20:07 PM', the user 'Generated by: manager', the filter 'Filter: None', and the page number 'Page 1 of 13'.

Fig. 3.6-18 Sample Category/Site/IPs report

By Category/User/Site

The name of the report (Category/User/Sites) displays in the header.

The body of the report contains columns with the following information for each Category and User listed: Sites and corresponding IP Count, Page Count, Object Count, Time (HH:MM:SS), Hit Count, and Blocked Hits.

The category Total for each user and Site Count display at the end of each Category/User section.

The Grand Total and Category Count display at the end of the report.

| Enterprise Reporter | | Dec 04, 2009 - Dec 04, 2009 | | M86 SM SECURITY | | |
|--|----------|-----------------------------|--------------|-------------------------------|-----------|--------------|
| Sort Order: Page Count, descending | | Category/User/Sites | | | | |
| Category:Uncategorized | | | | | | |
| User:192.168.30.74 | | | | | | |
| Sites | IP Count | Page Count | Object Count | Time (HH:MM:SS) | Hit Count | Blocked Hits |
| 66.66.27.220 | 1 | 1 | 0 | 0:0:4 | 1 | 0 |
| 65.55.25.90 | 1 | 1 | 0 | 0:0:4 | 1 | 0 |
| Total for 192.168.30.74 | | 2 | 2 | 0:0:8 | 2 | 0 |
| Site Count: 2 sorted by Page Count, descending | | | | | | |
| Category:Uncategorized | | | | | | |
| User:192.168.30.60 | | | | | | |
| Sites | IP Count | Page Count | Object Count | Time (HH:MM:SS) | Hit Count | Blocked Hits |
| 192.168.20.90 | 1 | 406 | 143 | 0:0:32 | 551 | 0 |
| 208.90.234.134 | 1 | 386 | 0 | 0:24:09 | 366 | 0 |
| 192.168.20.220 | 1 | 90 | 5 | 0:1:24 | 95 | 0 |
| 860.com | 1 | 58 | 0 | 0:3:48 | 58 | 0 |
| 208.90.239.69 | 1 | 15 | 17 | 0:0:29 | 32 | 0 |
| 65.245.209.92 | 1 | 9 | 0 | 0:0:4 | 9 | 0 |
| bonobonahotel.com | 1 | 6 | 73 | 0:0:6 | 79 | 0 |
| 65.55.73.248 | 1 | 2 | 0 | 0:0:6 | 2 | 0 |
| psnetmedical.com | 1 | 2 | 38 | 0:0:6 | 42 | 0 |
| 63.245.209.81 | 1 | 1 | 0 | 0:0:4 | 1 | 0 |
| qvz26.com | 1 | 1 | 0 | 0:0:4 | 1 | 0 |
| 65.55.194.29 | 1 | 1 | 0 | 0:0:4 | 1 | 0 |
| 207.46.14.233 | 1 | 1 | 0 | 0:0:4 | 1 | 0 |
| 65.55.21.250 | 1 | 1 | 0 | 0:0:4 | 1 | 0 |
| 65.245.209.105 | 1 | 1 | 0 | 0:0:4 | 1 | 0 |
| Total for 192.168.30.60 | | 15 | 961 | 0:38:24 | 1,237 | 0 |
| Site Count: 15 sorted by Page Count, descending | | | | | | |
| Category:Uncategorized | | | | | | |
| 12/31/2009 3:23:49 PM Generated by: manager Filter: None Page 1 of 634 | | | | | | |

Fig. 3.6-19 Sample Category/User/Sites report

Wall Clock Time Report

The Wall Clock Time Report option is accessible by administrators only and provides textual results of end user Internet usage activity for a specified time period, based on the Wall Clock Time algorithm (see Wall Clock Time algorithm in this sub-section). This algorithm calculates 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.



NOTE: *The Wall Clock Time Report option does not display if the Wall Clock Time feature is disabled in the ER Administrator user interface. Refer to the Optional Features screen sub-section of the ER Administrator portion of this user guide for information about enabling or disabling the Wall Clock Time feature.*

Generate a Wall Clock Time Report

For administrators, the Wall Clock Time Report window displays in the panel when Wall Clock Time Report is clicked in the Custom Reports menu:

Fig. 3.6-20 Wall Clock Time Report window (administrator)

To generate a Wall Clock Time 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 pull-down menu to the right. 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 text box to the right, 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 text box to the right, 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 Wall Clock Time** - 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 open a separate ER Report browser window containing the status of the report being generated. When completely generated, “Report Finished” displays, and the report view in PDF format opens in a separate window.

As with other Web Client 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.

3. From the open PDF file, the Wall Clock Time 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 - click the save  icon to open the Save a Copy dialog box, and proceed with standard save procedures.
4. Click the “X” in the upper right corner of both the ER Report window and the PDF report window to close these windows.

View the Wall Clock Time Report

The header of the generated Wall Clock Time report includes the date range, Report Type, and Details criteria.

The body of the report includes the end user NAME, WALL CLOCK 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.

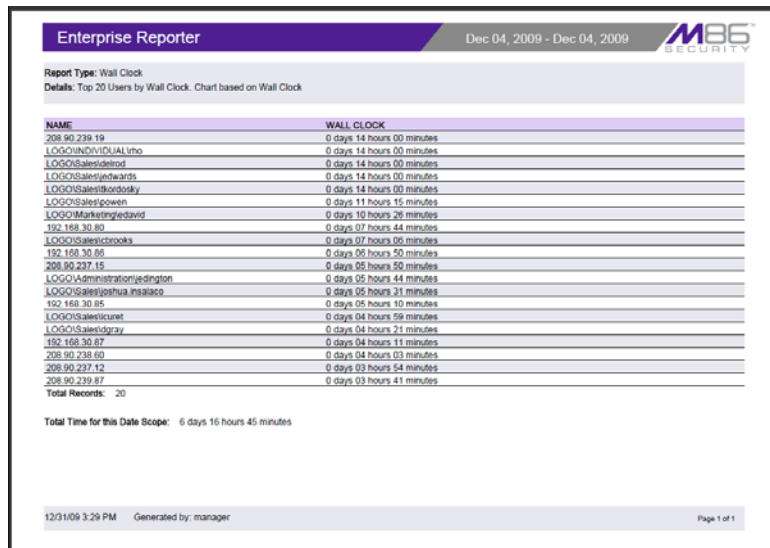


Fig. 3:6-21 Sample Wall Clock Time Report for Top 20 Users

Wall Clock Time 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 Wall Clock Time:

| | |
|----------|--------------------------------------|
| 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.

Use wildcards in a Specific Search query

To generate a report for a specific username or user IP, enter the minimum criteria:

1. Select “Show Specific User” or “Show Specific IP”.
2. Enter text in the following format: %X% (in which “X” represents the username or the user’s IP address).

Examples:

- Show Specific User: %jsmith%
 - Show Specific IP: %200.10.100.51%
3. Click **Create Report** to open the specific search page:

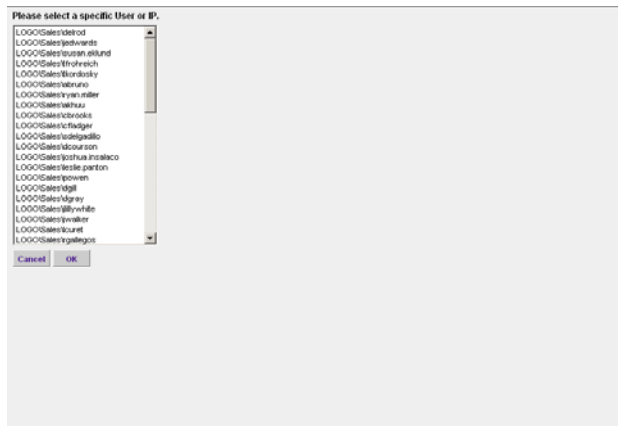


Fig. 3:6-22 Specific search page box showing username results

This page is comprised of a list box containing usernames or user IPs stored in the system—pertinent to your query—returned by the search.

4. Make a selection from the list box, and then click **OK** to close the page and to begin generating the report.

Blocked Request Report

The Blocked Request Report option is accessible by administrators only and provides textual results of end user Internet usage activity of blocked URLs for a specified time period.



NOTE: The Blocked Request Report option does not display if the Block Request Count feature is disabled in the ER Administrator user interface. Refer to the Optional Features screen sub-section of the ER Administrator portion of this user guide for information about enabling or disabling the Block Request Count feature.

Generate a Blocked Request Report

For administrators, the Blocked Request Report window displays in the panel when Blocked Request Report is clicked in the Custom Reports menu:

The screenshot shows the 'Blocked Request Report' window in the Enterprise Reporter interface. The window title is 'CUSTOM REPORTS - BLOCKED REQUEST REPORT'. It contains a 'Criteria' section with the following options:

- Show all records
- Show User Group
- Show Specific User
- Show Specific IP
- Top 20 Users by Blocked Requests

Below the criteria is a 'Date Scope' dropdown menu set to 'Yesterday'. Underneath are 'From Date' and 'To Date' fields, both set to '12/06/2009'. A 'Create Report' button is located at the bottom right of the window.

Fig. 3:6-23 Blocked Request Report window (administrator)

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 pull-down menu to the right. 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 text box to the right, 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 text box to the right, 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 open a separate ER Report browser window containing the status of the report being generated. When completely generated, “Report Finished” displays, and the report view in PDF format opens in a separate window.

As with other Web Client 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.

3. From the open PDF file, the Blocked Request 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 - click the save  icon to open the Save a Copy dialog box, and proceed with standard save procedures.
4. Click the “X” in the upper right corner of both the ER Report window and the PDF report window to close these windows.

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.

Enterprise Reporter Dec 04, 2009 - Dec 04, 2009 **M86** SECURITY

Report Type: Blocked Request Report
Details: Top Users

| NAME | Blocked Count |
|--------------------------|---------------|
| 192.168.30.85 | 1128 |
| 208.90.238.33 | 121 |
| 208.90.237.8 | 109 |
| 208.90.237.17 | 43 |
| 208.90.237.101 | 33 |
| 208.90.237.15 | 30 |
| 208.90.237.244 | 28 |
| 208.90.738.30 | 20 |
| 208.90.239.50 | 19 |
| 208.90.239.3 | 18 |
| 208.90.239.115 | 16 |
| 208.90.739.24 | 16 |
| 208.90.237.245 | 8 |
| 208.90.237.245 | 8 |
| 208.90.239.120 | 8 |
| 208.90.739.34 | 8 |
| 208.90.239.62 | 8 |
| 208.90.239.63 | 8 |
| 208.90.239.68 | 8 |
| 208.90.237.195 | 3 |
| Total Records: 20 | |
| Total Count: 1637 | |

12/31/09 3:30 PM Generated by: manager Page 1 of 1

Fig. 3:6-24 Blocked Request Report for Top 20 Users



NOTE: To use wildcards in a Blocked Request Report query, see *Use Wildcards in a Specific Search query from the Wall Clock Time Report sub-section.*

Saved Custom Reports

The Saved Custom Reports option lets you view, copy, or edit data in a report you created, run a report, or delete a report.

This window displays in the panel when Saved Custom Reports is selected from the Custom Reports menu:

Enterprise Reporter M86

CUSTOM REPORTS - SAVED CUSTOM REPORTS

Report Name: manager

Show All Reports Show My Reports

Report Description: test

General Info:

Report: Users

Date Scope: Current Week

From Date: 12/27/2009 From Time: N/A

To Date: 1/2/2010 To Time: N/A

Specific Info:

| | | | | | |
|-----------------|------|----------------|------|---------------------|-----|
| Category: | None | Show Category: | N/A | Show Filter Action: | N/A |
| User IP: | None | Show IP: | N/A | Show Content Type: | N/A |
| Username: | None | Show Username: | N/A | Show Content: | N/A |
| Site: | None | Show Site: | N/A | Show Search String: | N/A |
| Category Group: | None | Break: | N/A | | |
| User Group: | None | Keywords: | None | | |

Output Info:

Output: E-Mail As Attachment

File Type: PDF

File Name:

Fig. 3:6-25 Saved Custom Reports window (administrator)



NOTE: The radio button options in the top frame do not display for sub-administrators.

View Information in a Saved Custom Report

In the top frame, all report selections display in the Report Name pull-down menu.

If you are logged in as an administrator:

1. Click the radio button corresponding to either option:
 - **Show All Reports** - This selection displays in the Report Name pull-down menu a list of all recorded reports
 - **Show My Reports** - This selection displays in the Report Name pull-down menu only the reports you recorded



NOTE: *The radio button options do not display for sub-administrators.*

2. Make a selection from the **Report Name** pull-down menu to display the Report Description below this frame, and to populate the General Info, Specific Info, and Output Info frames:
 - **General Info:** Report type; Date Scope; From/To Date; From/To Time (if available)
 - **Specific Info:** Category, User IP, Username, Site, Category Group, User Group, Show Category, Show IP, Show Username, Show Site, Show Filter Action, Show Content Type, Show Content, Show Search String, Break type, Keyword(s)
 - **Output Info:** Output format, File Type, File Name

Edit a Custom Report

The Save Report pop-up window is used when editing a summary or detail report.

1. Click **Edit Report** to open the Save Report pop-up window where you can edit report settings for a saved report.

When editing a summary report, the Save Report pop-up window appears as follows:

Save Report

Save Name:

Description:

Date Scope:

From Date: From Time:

To Date: To Time:

Break type:

Output type:

Format:

For single-break reports only

Amount shown: # Records:

For pie and bar charts only

Generate using:

For E-Mail output only

To:

Cc:

Bcc:

Subject:

Body:

Fig. 3:6-26 Save Report, edit summary report

When editing a detail report, the Save Report pop-up window appears as follows:

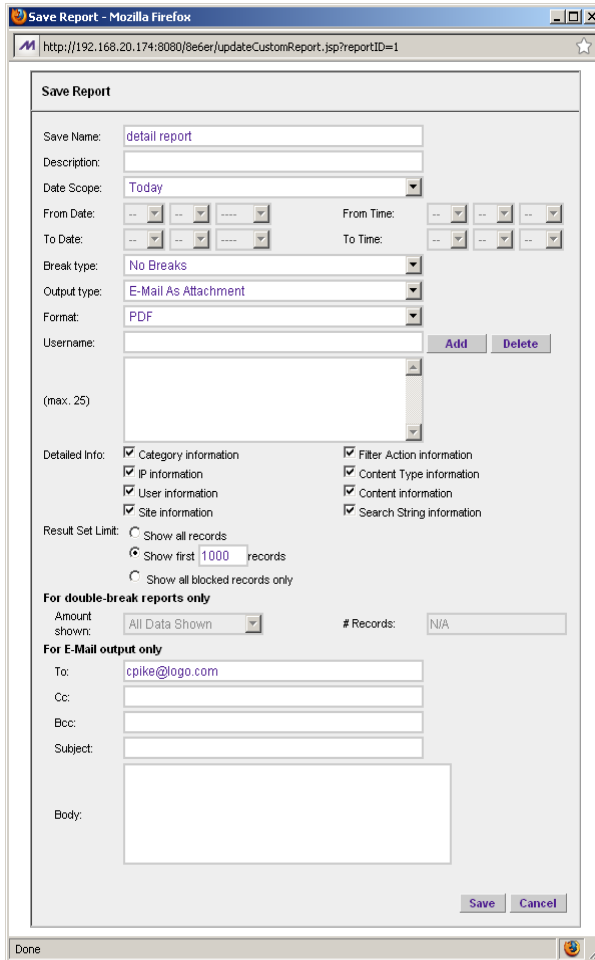




Fig. 3:6-27 Save Report, edit detail report

 **NOTE:** When editing a report, the Hide Un-Identified IPs field does not display if this option is deselected in Default Options.

 **TIPS:** The Copy (Ctrl+C) and Paste (Ctrl+V) functions can be used in the fields in the Save Report pop-up window.

*When editing a summary or detail report, click **Cancel** to exit the **Save Report pop-up window** without saving your edits.*

2. After making your selections and entries, click **Save**.

Add a Username

1. In the **Username** field of a summary or detail report, do one of the following to add a username in the list box below:
 - Type in the username
 - Enter valid alpha characters preceded and/or followed by a wildcard ('%'), or
 - Enter a wildcard ('%')
2. Click **Add**; if a wildcard was used and more than one match was found on the server, this action opens the **Specific Search pop-up box** (see Fig. 3:6-8) that displays all available matches in the **Username** frame:
 - a. For a summary report, select the username from the pop-up box. For a detail report, select up to 25 usernames from the pop-up box.
 - b. Click **OK** to close the pop-up box and to populate the list box in the wizard screen.



TIP: To remove an entry from the list box, select it and then click **Delete**.

Copy a Custom Report

The copy feature is a great time saver, letting you use settings from a saved summary or detail report.

1. From the **Report Name** pull-down menu, select the report to be copied.
2. Click **Copy Report** to open the Copy Custom Report pop-up window where you make modifications for the new report.

See Edit a Custom Report for information on fields that display in the Copy Custom Report pop-up window.



NOTE: *When copying a report:*

- *The Description field displays the text “Copy of ‘X’”, in which ‘X’ represents the report name*
- *The Cancel button does not display*
- *The Hide Un-Identified IPs field does not display if this option is deselected in Default Options*
- *The Username field and accompanying list box do not display*

Run a Custom Report

Click **Run Report** to open a separate browser window that displays information to indicate the report is being generated.

After being completely generated, the report is emailed to the specified recipient(s).

Delete a Custom Report

To remove the custom report from choices available in the Report Name pull-down menu, and the Event Schedule option:

1. Select the report from the **Report Name** pull-down menu.
2. Click **Delete Report**.



NOTE: *If a custom report is scheduled to run via the Event Schedule option, deleting the report removes it from the Scheduled Events box.*

Event Schedules

The Event Schedules option is used for maintaining a schedule for generating a customized report.

To view details on a scheduled event, or to edit, add, or delete a scheduled event, click Event Schedule in the Custom Report menu to display the Event Schedules window in the panel:



Fig. 3:6-28 Event Schedules window (administrator)

If logged in as the administrator, all scheduled events display. If logged in as a sub-administrator, only the events scheduled by that sub-administrator login ID display. If the Web Client Scheduler is turned off, the message “To view event schedules, please enable Web Client scheduler using ER Admin GUI.” displays in place of scheduled events.



NOTE: Refer to these user guide sections for information about the following topics:

- To save reports using the Save Custom Report option, see this chapter and Chapter 5: Drill Down Reports, under the Save Custom Report option sub-sections.
- To enable or disable the Web Client to run scheduled events, see the Web Client Server Management screen sub-section of the ER Administrator portion of this user guide.

View Details or Edit a Scheduled Event

In the Event Schedules window, events display as rows of records. The following information is included for each record: Name assigned to the scheduled event, Interval when the report is scheduled to run, date Last Run, Report Name, Start Time for the report to run, and Creator of the schedule (login username). Delete and Edit buttons display to the left of each row.

In the Record field at the bottom of the window, the number of the selected record displays, along with the total number of records (scheduled events).

Click the **Refresh** button to refresh the list of records and to scroll to the top of the list.



TIP: The selected record is designated by an arrow in the white box to the left of a row. To select another record, click the white box in that row to display the arrow. You also can navigate to another record by using the Record navigation field. Click in the box between the arrow buttons and enter a new record number to go to that record. Or click any of the four arrow buttons to advance forward or backward through the list of records. In the order in which they display in the Record field, clicking these buttons moves you to the first record, the record prior to the selected record, the record following the selected record, and the last record.

View Details for a Scheduled Event

To view additional information on an event, click the **Edit** button for that event. This action opens the Update Scheduled Event dialog box:

The screenshot shows a web browser window titled "Update Scheduled Event - Mozilla Firefox". The address bar shows a URL starting with "http://192.168.20.218:8080/8ef6er/updateSchedules.jsp?schiD=". The main content area is a form with the following fields:

- Name:
- Report to Run:
- When to Run:
- Day of the Week:
- Start Time:
- Server Time: 01/04/2010 01:57:26 PM PST

At the bottom right of the form are two buttons: "Cancel" and "Save". The status bar at the bottom of the browser window shows "Done".


Fig. 3:6-29 View event details

The following information displays in this dialog box: 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, Start Time to run, and Server Time details.

Edit a Scheduled Event

1. In the Event Schedules window, click the **Edit** button for the event you wish to modify. This action opens the Update Scheduled Event dialog box (see Fig. 3:6-29). In this dialog box you can:

- 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 Event Schedules window without saving your edits.

2. Click the **Save** button to display the updated criteria in the Event Schedules window.

Add an Event to the Schedule

1. In the Event Schedules window, click the **Add Event** button to open the Add Event to Schedule dialog box:

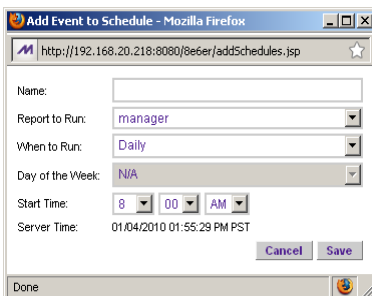


Fig. 3:6-30 Add an event

This dialog box also opens when saving a custom report using the Custom Report Wizard, and selecting the Save and Schedule option.

2. Enter a **Name** for the event.
3. Select the **Report to Run** from the pull-down menu.
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 (1st - 31st).

5. Select the **Start Time** for the report: 1 - 12 for the hour, 00 - 59 for the minute, 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 Event Schedules window without saving your edits.*

6. Click **Save** to add the scheduled event.

Delete a Scheduled Event

1. In the Event Schedules window, click the **Delete** button for the event you wish to delete. This action opens a dialog box with the message: “Are you sure you want to delete this event?”
2. Click **OK** to execute your action and to close the dialog box. This action also opens an alert box with the message: “Event deleted!”
3. Click **OK** to close the alert box.

Scheduling a Report to Run

Once a report view has been saved, it can be scheduled to run at a designated time.

To schedule a report to run:

1. Go to the Custom Reports menu in the navigation toolbar and select Event Schedule.
2. In the Event Schedules window, click **Add Event**.
3. In the Add Event to Schedule pop-up box, select the Report to Run from the saved custom reports listed in the pull-down menu.
4. Specify criteria for scheduling the event, and then click **Save**.

Executive Internet Usage Summary

The Executive Internet Usage Summary option is used for specifying email addresses of users authorized to receive bar and line chart reports showing activity in library category groups of your choice.

To set up and maintain a list of library category groups to be included in the report, and the email addresses of intended recipients of this report, click Executive Internet Usage Summary in the Custom Report menu to display the Executive Internet Usage Summary window in the panel:

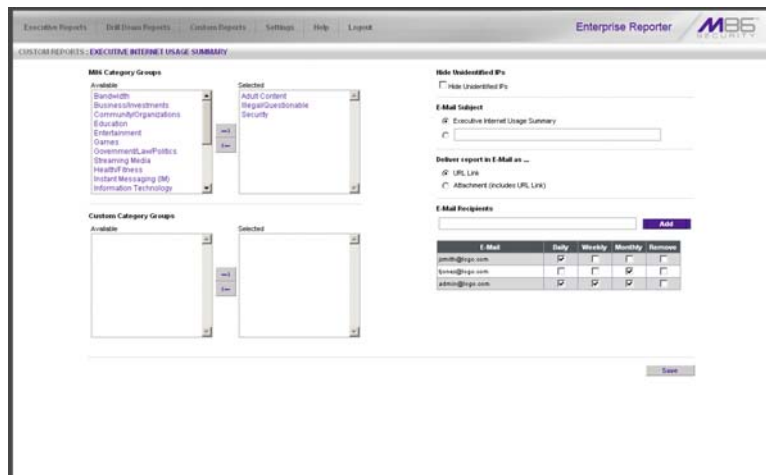


Fig. 3:6-31 Executive Internet Usage Summary window (administrator)

The panel contains the following frames used for configuring and using this feature: M86 Category Groups, Custom Category Groups, Hide Unidentified IPs, E-Mail Subject, Deliver report in E-Mail as..., and E-Mail Recipients.

After making all settings in this window, click the Save button.

Specify category groups for the report

The M86 Category Groups frame and the Custom Category Groups frame contain the Available and Selected list boxes.

in the M86 Category Groups frame, by default the following library category groups are included in the Selected list box: Adult Content, Illegal/Questionable, and Security.

In the Custom Category Groups frame, by default any library category groups included in the Category Groupings window from the Settings menu display in the Available list box.

Add category groups to the Selected list box

1. To add category groups to the Selected list box, select the category groups in the Available list box.



TIP: 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.

2. Click the “—>” arrow to move the category groups to the Selected list box.

Remove category groups from the Selected list box

1. To remove category groups from the Selected list box, select the category groups in the Selected list box.



TIP: 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.

2. Click the “<—” arrow to move the category groups to the Available list box.

Hide Unidentified IP addresses

In the Hide Unidentified IPs frame, 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.*

Specify E-Mail Subject

In the E-Mail Subject frame, 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.

Specify how the report will be accessed

In the Deliver report in E-Mail as... frame, 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.

Maintain a list of users to receive reports

In the E-Mail Recipients frame, specify the user(s) to receive the report and the frequency of delivery.

1. Click in the empty field and type in the email address.
2. Click **Add** to clear the field and to add the email address in the list box below.
3. By default, checkmarks populate the frequency checkboxes: **Daily**, **Week**, **Month**. 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.

To remove a recipient from the list of users authorized to receive reports, click the **Remove** checkbox to enter a check mark. After **Save** is clicked, the user will be removed from the E-Mail Recipients frame.

Save your settings

Click **Save** to save all settings made in this window.

Sample Executive Internet Usage report

The recipient of the Executive internet Usage Summary report receives an email containing a .pdf attachment of the report (if the size of the .pdf file is within the limits) as well as a link to the report.

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.

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.

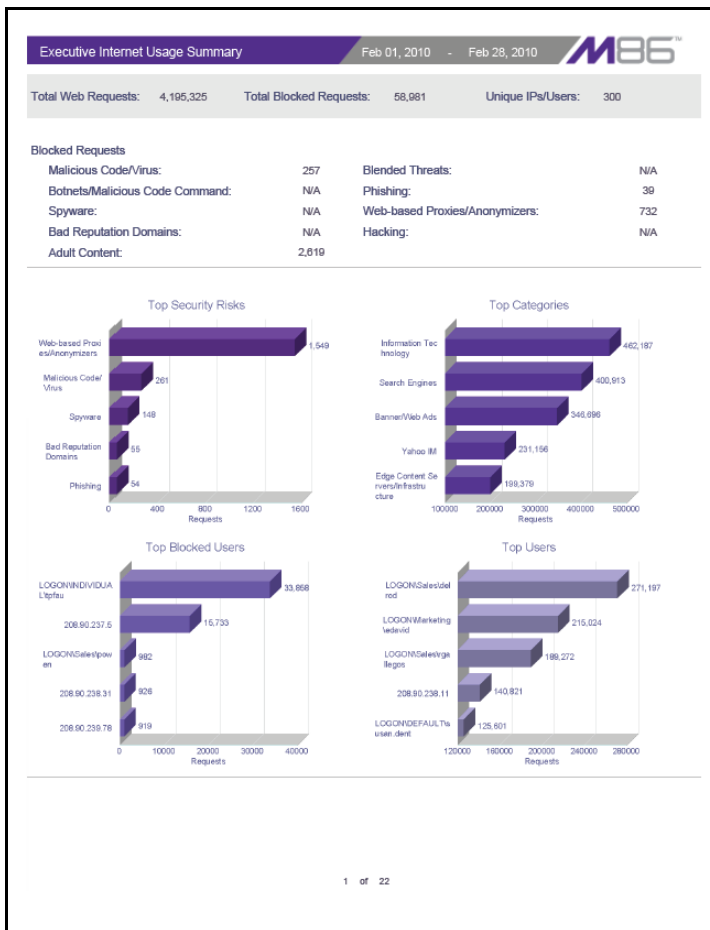


Fig. 3:6-32 Executive Internet Usage Summary monthly report, page 1

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.

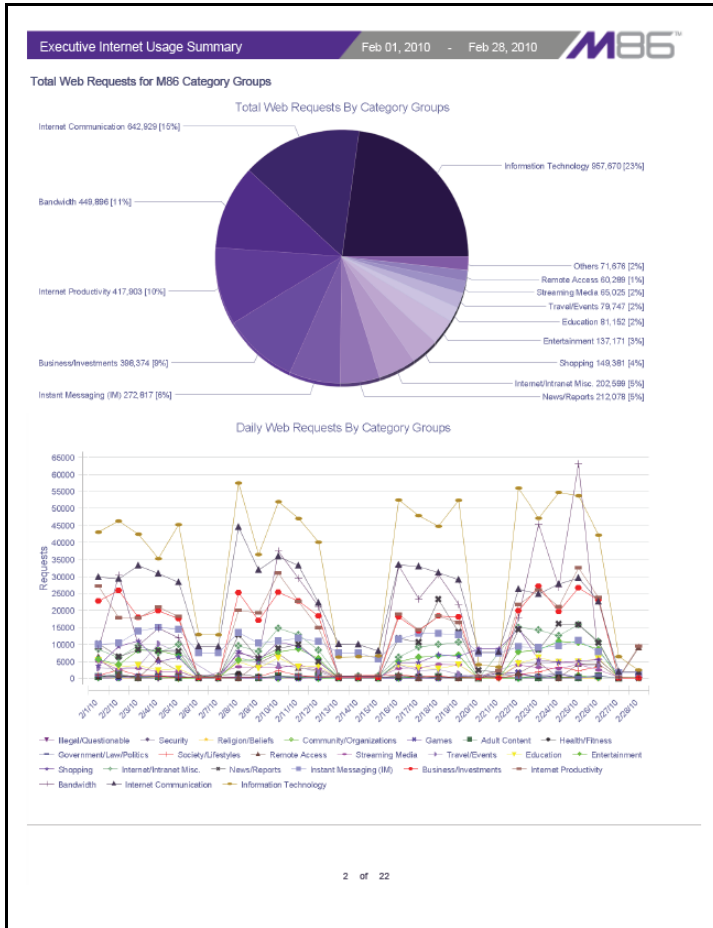


Fig. 3:6-33 Executive Internet Usage Summary monthly report, page 2

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.

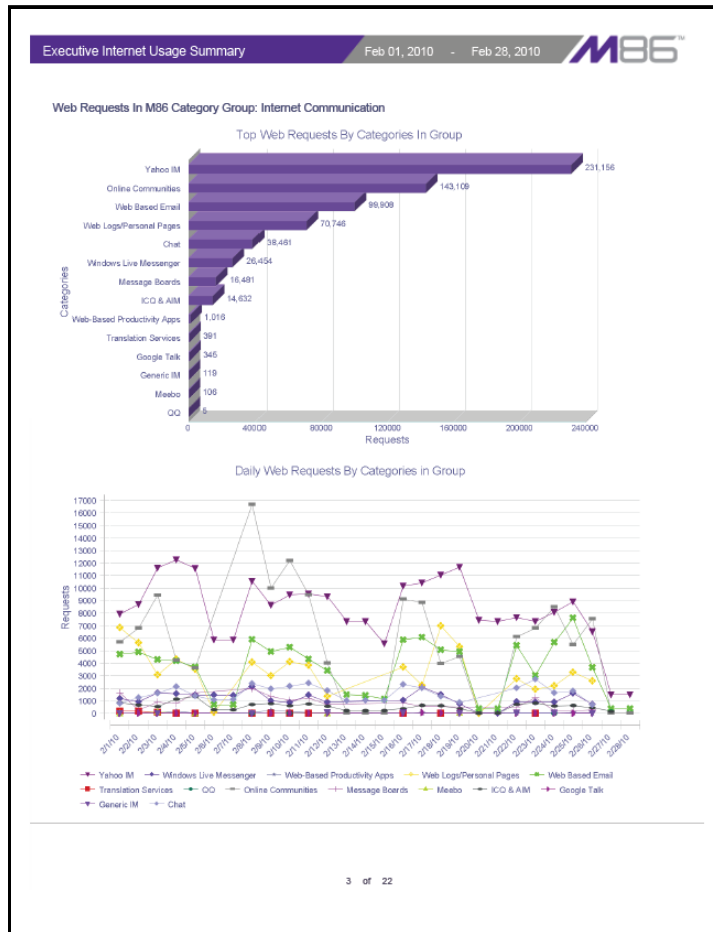


Fig. 3:6-34 Executive Internet Usage Summary monthly report, page 3

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 | | | | | | | |
|--|------------|----------|------------|--------------|----------------|---------------|------------|
| | | | | Feb 01, 2010 | - | Feb 28, 2010 | M86 |
| Top 10 Users In M86 Category Group: Internet Communication | | | | | | | |
| Users | Page Count | IP Count | Site Count | Object Count | Category Count | Time HH:MM:SS | Hit Count |
| LOGON\Sales\deirod | 54,355 | 1 | 54 | 1729 | 7 | 18:30:30 | 56,084 |
| LOGON\Sales\jedwards | 30,768 | 1 | 42 | 1481 | 8 | 09:50:50 | 32,249 |
| 208.90.239.11 | 30,006 | 1 | 81 | 366 | 6 | 00:57:20 | 30,372 |
| LOGON\Sales\idgray | 16,935 | 4 | 48 | 12259 | 8 | 16:17:40 | 29,194 |
| 208.90.238.11 | 10,936 | 1 | 94 | 13664 | 8 | 00:55:40 | 24,600 |
| LOGON\Sales\ryan.miller | 22,111 | 1 | 30 | 221 | 6 | 12:05:10 | 22,332 |
| LOGON\DEFAULT\susan.dent | 17,753 | 1 | 59 | 2636 | 6 | 08:14:20 | 20,389 |
| LOGON\Sales\jgreen | 11,135 | 2 | 45 | 8946 | 6 | 21:41:20 | 20,081 |
| LOGON\Administration\miller | 4,773 | 1 | 80 | 14611 | 8 | 06:38:30 | 19,384 |
| LOGON\INDIVIDUAL\matheron | 17,719 | 1 | 21 | 715 | 8 | 23:14:50 | 18,434 |

4 of 22

Fig. 3:6-35 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.

WEB CLIENT APPENDICES SECTION

Appendix A

Evaluation Mode

By default, the ER Server module and Client are set to the evaluation mode. This appendix explains how to use the ER Client in the evaluation mode.



NOTE: *Contact the administrator of the ER Server module to activate the ER Client to function in the activated mode.*

Client

On a box in the evaluation mode, when navigating to the ER Server Information window, the Evaluation Mode alert box opens.

Evaluation Mode alert box

The Evaluation Mode alert box provides information about the maximum number of weeks of data storage:

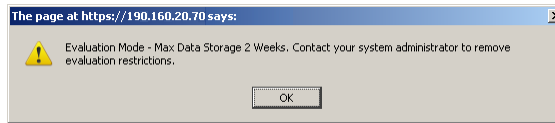


Fig. A-1 Evaluation Mode alert box

Click **OK** to close the Evaluation Mode alert box.

ER Server Information window

In the evaluation mode, the ER Server Information window displays the note “*Evaluation Mode Enabled” above the ER Activity frame:

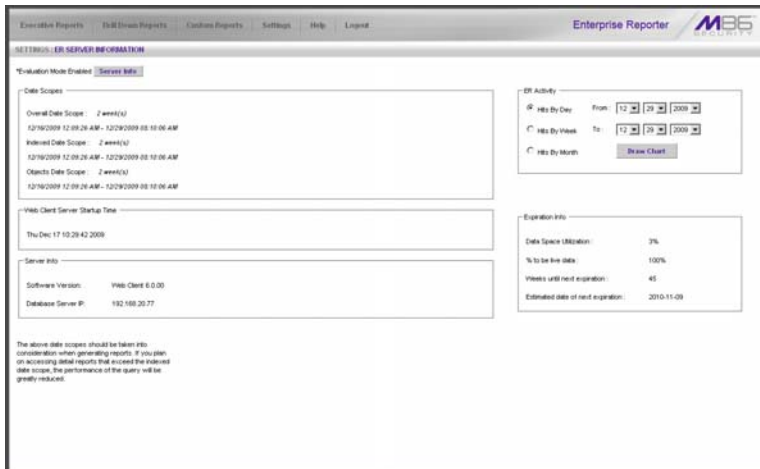


Fig. A-2 ER Server Information window

Click the **Server Info** button to the right of the “*Evaluation Mode Enabled” note to open the Evaluation Mode alert box (see Fig. A-1).



NOTE: The ER Server administrator can change the ER’s mode from evaluation to activated by submitting the Enterprise Reporter Product Activation request form to M86 Security.

Appendix B

Lotus Notes Configuration

This appendix provides information on configuring the ER Client to use Lotus Notes (4.5 and above) in a Microsoft Windows environment in which Lotus Domino is the primary e-mail server.

Making these configurations ensures that e-mail reports sent from the ER Client are transported via the MAPI client in Outlook Express directly to the IP Address of the Lotus Domino e-mail server. This setup avoids any delays or “hung” reports that may occur if settings point to the Lotus Notes client, since Lotus Notes utilizes the MAPI .DLL differently than mail clients native to the Windows OS.



NOTE: *Versions of Lotus Notes prior to 4.5 do not contain the necessary MAPI transport .DLL.*

Steps for Former MS Outlook / Express Users

Follow these steps if Microsoft Outlook or Outlook Express was the primary e-mail client used on your system.

1. Delete any current e-mail accounts residing in Outlook or Outlook Express.
2. If Outlook is currently installed with your Microsoft Office system, uninstall Outlook—but **not** Outlook Express.

Steps for Installing, Configuring Lotus Notes

Step 1: Install Lotus Notes

Install and configure Lotus Notes to connect to your network's Lotus Domino server.



NOTE: Check with your System Administrator if you are unsure about your settings.

Step 2: Configure Microsoft Mail Client

Make the following configurations for the Microsoft Mail Client from the control panel:

1. When running the Internet Connection and Internet Explorer e-mail client wizard, be sure the e-mail address is set to the "Internet address" of your Lotus Notes account.



NOTE: If this account has not yet been set up in Lotus Domino, create it now, and then run the e-mail client wizard.

2. When the e-mail account wizard requests the server address, use the IP Address only—**not** the Lotus Name—of your Lotus Domino server.



TIP: These settings also can be generated directly by using the "mail" settings in the Windows control panel. Again, any previous non-Lotus Notes accounts must be deleted.

Step 3: Verify Internet Explorer Settings

1. Open Internet Explorer.
2. Go to **Tools > Internet Options > Programs** tab.
3. Check your "E-mail" and "Newsgroups" settings to make sure they are set to "Outlook Express"—**not** Lotus Notes.

Appendix C

Glossary

This glossary includes definitions for terminology used in this user guide.

double-break report - a report that uses two sets of criteria, such as User/Sites or Category/IPs.

hit count - the number of pages and/or objects end users access as the result of entering URLs in a browser window.

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.

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.

Wall Clock Time count - the amount of time end users spend on the Internet, based on the Wall Clock Time 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.

TAR INTRODUCTORY SECTION

Threat Analysis Reporter

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

M86's Threat Analysis Reporter (TAR) is designed to offer administrators or management dynamic, real time graphical snapshots of their network's Internet traffic, supported by remediation tools to manage and control user-generated Web threats. Working in conjunction with M86's Web Filter, TAR interprets end user Internet activity from the Web Filter's logs and provides data that can be viewed via an easy-to-read dashboard of gauges the administrator can drill down into, thereby identifying the source of the threat.

About this Portion of the User Guide

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

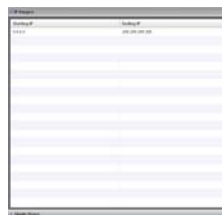
The TAR portion of the user guide is organized into the following sections:

- **TAR Introductory Section** - This section provides general information on how to use this portion of the user guide to help you configure the TAR application.
- **TAR Preliminary Setup Section** - This section includes information on creating and maintaining user accounts.
- **TAR Configuration Section** - This section includes information on configuring TAR to alert you to any end user Internet activity not within your organization’s Internet usage policies.
- **TAR Administration Section** - This section includes functions for maintaining the TAR application or its database.
- **TAR Appendices** - Appendix A provides details on setting up and using the System Tray feature for TAR alerts. Appendix B features a glossary of technical terminology used in this portion of the user guide.

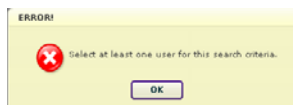
Terminology

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.



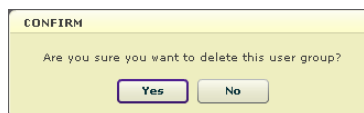
- **button** - an object in a dialog box, alert box, window, or panel that can be clicked with your mouse to execute a command.



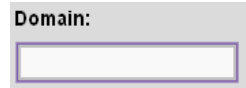
- **checkbox** - a small square in a dialog box, window, or panel used for indicating whether or not you wish to select an option. This object allows you to toggle between two choices. By clicking in this box, a check mark or an “X” is placed, indicating that you selected the option. When this box is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



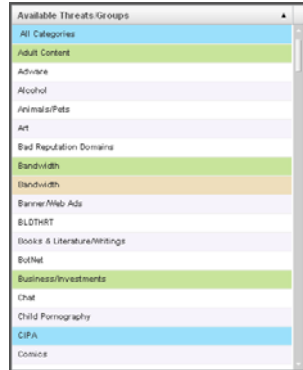
- **dialog box** - a box that opens in response to a command made in a window or panel, and requires your input. You must choose an option by clicking a button (such as “Yes” or “No”, or “Next” or “Cancel”) to execute your command. As dictated by this box, you also might need to make one or more entries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



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



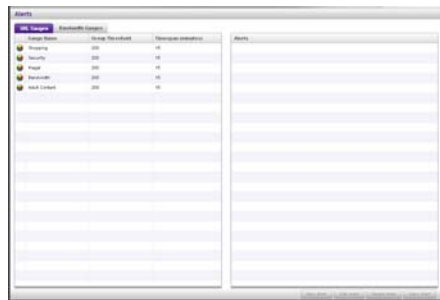
- frame** - a boxed-in area in a dialog box, window, or panel that includes a group of objects such as fields, text boxes, list boxes, buttons, radio buttons, checkboxes, accordions, tables, tabs, and/or tables. Objects within a frame belong to a specific function or group. A frame often is labeled to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



- 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.



- **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.




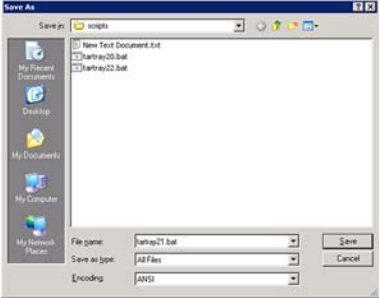
- **screen** - a main object of an application that displays across your monitor. A screen can contain panels, windows, frames, fields, tables, text boxes, list boxes, icons, buttons, and radio buttons.



- **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.


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


- **text box** - an area in a dialog box, window, or screen that accommodates your data entry. A text box is a type of field. (See “field”.)
- **window** - can contain frames, fields, text boxes, list boxes, icons, buttons, and radio buttons. Types of windows include ones from the system such as the Save As window, pop-up windows, or login windows.



Getting Started

Procedures for Logging On, Off

Access the TAR Administrator Login window

The TAR Administrator user interface is accessible in one of two ways:

- by clicking the Threat Analysis Reporter icon in the SR Welcome window (see Access TAR Administrator Console from SR Portal)
- by launching an Internet browser window supported by the Threat Analysis Reporter and then entering TAR's URL in the Address field (see Enter TAR Administrator Console's URL in Address field)

Access TAR Administrator Console from SR Portal

Click the TAR icon in the SR Welcome window:



Fig. 1:1-1 TAR icon in SR 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 SR Appendix I: Disable Pop-up Blocking Software.

Clicking the TAR icon launches a separate browser window/tab containing the TAR Login window (see Fig. 1:1-2).

Enter TAR's URL in the Address field

1. Launch an Internet browser window supported by TAR.
2. In the address line of the browser window, type in "https://" and TAR's IP address or host name, and use port number ":8443" for a secure network connection, plus "/8e6tar".

For example, if your IP address is 210.10.131.34, type in **https://210.10.131.34:8443/8e6tar/**. Using a host name example, if the host name is logo.com, type in **https://logo.com:8443/8e6tar/**.

With a secure connection, the first time you attempt to access the TAR 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-sr.pdf>**

3. After accepting the security certificate, click **Go** to open the TAR Login window (see Fig. 1:1-2).

Log in



NOTE: In this window, TAR'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:

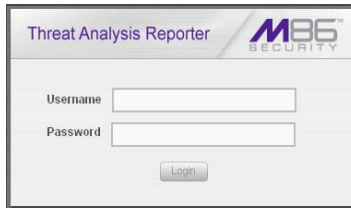



Fig. 1:1-2 TAR Login window

 **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.
3. Click the **Login** button to open the application, displaying the URL gauges dashboard in the panel by default. At the top of the screen, the following navigation toolbar menu links display: Gauges, Policy, Report/Analysis, Administration, Help, and Logout. URL and Bandwidth tabs display to the left above the panel:

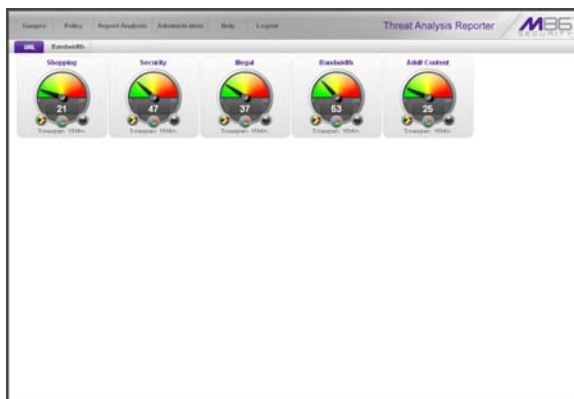


Fig. 1:1-3 Default TAR panel

Navigation toolbar menu links and topics

The navigation toolbar at the top of the screen consists of menu links to access topics for configuring and using the application:

- **Gauges** - mouse over this link to display menu selections for accessing panels that let you set up and manage URL and bandwidth gauges.
- **Policy** - mouse over this link to display menu selections for accessing panels that let you set up and maintain policies used for triggering warnings when gauges approach their upper threshold limits.
- **Report/Analysis** - mouse over this link to display menu selections for accessing applications and panels used for analyzing Internet usage data on your network.
- **Administration** - mouse over this link to display menu selections for accessing panels that let you set up and maintain administrator profiles and manage the TAR unit.
- **Help** - click this link to open a separate browser window or tab displaying the Threat Analysis Reporter Documentation page containing links to the latest user guides (in the .pdf format) for this product.
- **Logout** - click this link to log out of this application. When your session has been terminated, the login window re-displays.

Exit the user interface

To exit the user interface, click the “X” in the upper right corner of the browser window or tab.

Exiting the Administrator console will log you out of TAR, but will not log you out of the SR server, nor turn off the server.

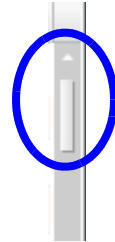


WARNING: *If you need to turn off the SR server, follow the shut down procedures outlined in the Shut Down screen sub-section under the Server Menu section in Chapter 2 of the ER Administrator Section of the Enterprise Reporter portion of this user guide. Failure to properly shut down the server can result in data being lost or corrupted.*

Navigation Tips and Conventions

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

- **Move a pop-up window** - Click the toolbar of a pop-up window and simultaneously move your mouse to relocate the pop-up window to another area in the current browser window.
- **Scroll up and down, and across a list** - If available, use the scrollbar to the right or along the bottom of a frame or list box to view an entire list.




An extensive list can be viewed in its entirety by clicking the Previous and Next buttons.

- **Tab to the next field** - Press the Tab key on your keyboard to advance to the next field in a panel.
- **Expand, contract a column** - Columns can be expanded or contracted by first mousing over the divider in the column header to display the arrow and double line characters (<||>). A column is then expanded or contracted by left-clicking the mouse and dragging the column bar to the right or left.
- **Browser Back button, Refresh button** - Clicking either the Back button in the browser window or the Refresh button in your browser will refresh the TAR 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. 

TAR PRELIMINARY SETUP SECTION

Introduction

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

- Chapter 1: User Groups Setup - This chapter explains how to set up user groups—whose Internet activity will be monitored by group administrators.
- Chapter 2: Admin Groups Setup - This chapter explains how to set up permissions so that an administrator in your group will only be able to access areas of the TAR console that you specify.
- Chapter 3: Admins Setup - This chapter explains how to set up a group administrator account.

Chapter 1: User Groups Setup

On a new TAR application, 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:

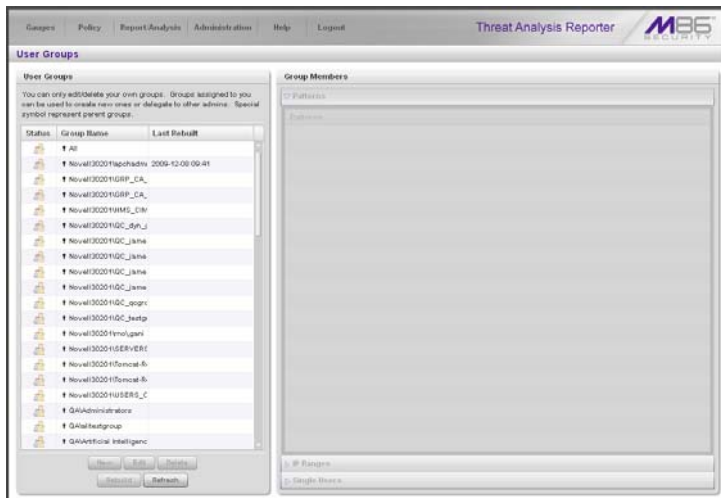


Fig. 2:1-1 User Groups panel

Names of user groups previously added by the administrator display in black text in the User Groups frame. Imported user groups display 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.



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



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

- Active Directory Mixed Mode
- Active Directory Native Mode
- Novell eDirectory
- Sun One

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

View User Group Information

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



NOTE: *User groups are automatically rebuilt daily.*

User group status key



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



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



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

View a list of members in a user group

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

1. Select the user group from the User Groups frame by clicking its Group Name to highlight that record. Based on this selection, the Group Members frame to the right becomes activated along with the following buttons in the section below, based on the status of the user group:
 - If the selected user group is ready to be rebuilt, this action activates all buttons (New, Edit, Delete, Rebuild, Refresh).
 - If the selected user group was not imported and cannot be rebuilt on demand, this action activates the New, Edit, Delete and Refresh buttons.

Add a User Group

To add a new user group:

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

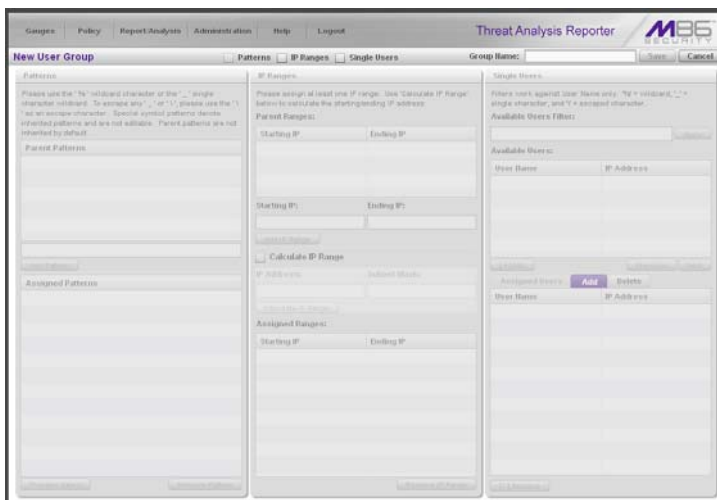



Fig. 2:1-3 New User Group panel

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

3. Enter at least three characters for the **Group Name** to be used for the new user group; this action activates the Save button.
4. Click the checkbox(es) to activate the pertinent corresponding frame(s) below: **Patterns**, **IP Ranges**, **Single Users**.

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

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


Patterns frame

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

Add a new pattern

To add a pattern to the new user group:

1. Do one of the following:
 - To add an inherited pattern, select the pattern from the Parent Patterns box to display that pattern in the field below.
 - To add a new pattern, enter the pattern in the field beneath the Parent Patterns box. For example: Enter `200.10.100.3%` to include all IP addresses with "200.10.100.3" as part of the IP address.
2. Click **Add Pattern** to include the pattern in the Assigned Patterns list box below.

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

View users resolved by the pattern

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

1. Select the pattern from the Assigned Patterns list box.
2. Click **Preview Users** to open the Preview Pattern Users pop-up window that shows the Patterns frame to the left and the Resolved Users frame to the right:

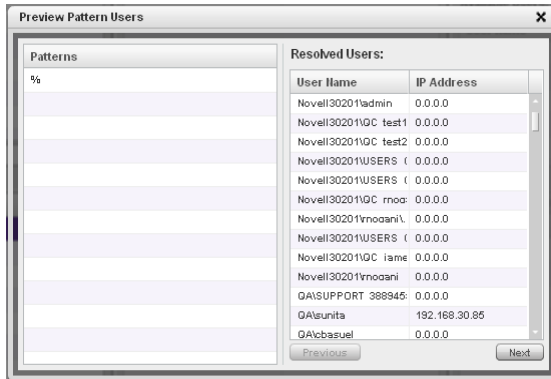


Fig. 2:1-4 Add user group Patterns, Preview Pattern Users

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

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

Remove a pattern

To remove a pattern in the Assigned Patterns list box:

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

- 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.*

The screenshot shows the 'New User Group' configuration page in the M86 Security Threat Analysis Reporter. The 'IP Ranges' frame is active, displaying the following sections:

- Parent Ranges:** A table with columns 'Starting IP' and 'Ending IP'. One entry is visible: Starting IP: 192.168.20.04, Ending IP: 192.168.20.07.
- Starting IP:** A text input field.
- Ending IP:** A text input field.
- Calculate IP Range:** A checkbox (unchecked) with a label 'Calculate IP Range'.
- IP Address:** A text input field.
- Subnet Mask:** A text input field.
- Assigned Ranges:** A table with columns 'Starting IP' and 'Ending IP'.

Other visible elements include the 'Parent Patterns' section on the left and the 'Single Users' section on the right. The interface includes navigation tabs at the top: Stages, Policy, Report Analysis, Administration, Help, Logout, and Threat Analysis Reporter.

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

Specify an IP range

To add an IP address range:

1. Do one of the following:
 - To make a selection from Parent Ranges, click the row in the Parent Ranges box to highlight and select that row, and also to add that Starting IP and Ending IP range in the Starting IP and Ending IP fields below. If necessary, edits can be made to these fields.
 - To add an IP address range without selecting from the Parent Ranges frame:
 - a. Enter the **Starting IP** address.
 - b. Enter the **Ending IP** address.
 - To calculate an IP address range:
 - a. Click the **Calculate IP Range** checkbox to activate the IP Address and Subnet Mask fields below.
 - b. Enter the **IP Address**.
 - c. Enter the **Netmask** which activates the Calculate Range button.
 - d. Click **Calculate IP Range** to display the Starting IP and Ending IP in the fields above.
2. Click **Add IP Range** to include that IP range in the Assigned Ranges list box below:

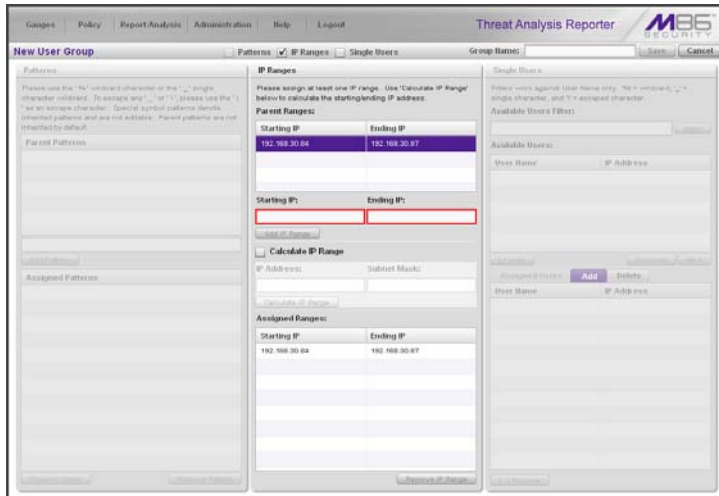


Fig. 2:1-6 Add user group, IP range added


Remove an IP address range

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

1. Click the row to highlight and select it; this action activates the Remove IP Range button below.
2. Click **Remove IP Range** to remove the IP address range from the list box.

Single Users frame

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

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

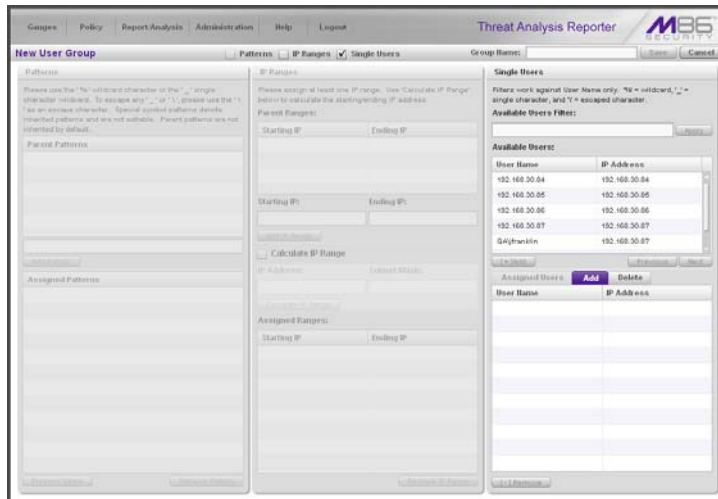


Fig. 2:1-7 Add user group, Single Users frame

Add one or more individual users

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

Use the filter to narrow Available Users results

To use the **Available Users Filter**:

1. Enter filter terms to narrow the selection of Available Users. For example: Type in *150%* to only display results matching an IP address that begins with “150”.
2. Click **Apply** to display filtered results in the Available Users box.

Select users to add to the Assigned Users list

To make selections from the Available Users box:

1. Select one or more IPs from the list to highlight the record(s).
2. Click **[+] Add** to include the selected user(s) in the Add Users tab.



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

Remove users from the Add tab

To remove users from this user group:

1. Select the user(s) from the Add tab; this action activates the [-] Remove button:

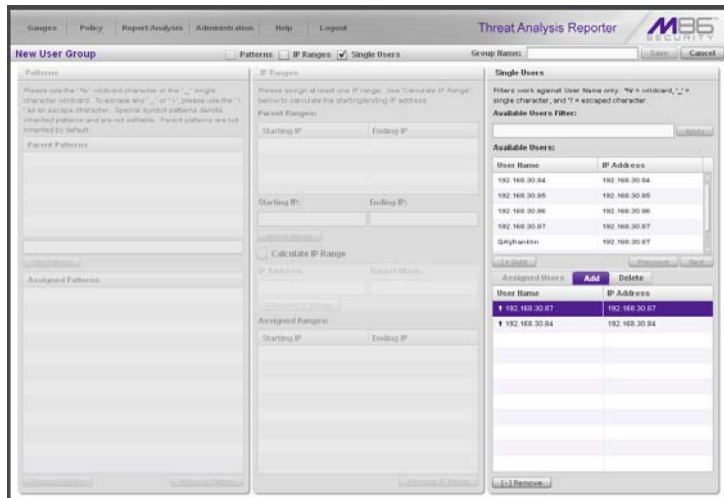


Fig. 2:1-8 Add user group, remove user from Single Users tab

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

Edit a User Group



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

To edit a user group:

1. From the main User Groups panel, select the user group from the list in the User Groups frame.
2. Click **Edit** to display the User Group panel showing activated frames—i.e. if the Patterns frame had settings made in it, that frame is activated; if the Single Users frame was the only frame with settings made in it, that frame is activated. Any frame without settings made in it displays greyed-out.
3. Make any of these edits:
 - To make entries in a frame that is not yet activated, click the available checkbox to activate that frame: **Patterns, IP Ranges, Single Users**.
 - Make any of these edits in a frame:
 - Patterns frame - add or remove a pattern.
 - IP Ranges frame - add or remove an IP address range.
 - Single Users frame - add or remove one or more users.



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

- If necessary, edit the name of the user group in the **Group Name** field.
4. Click **Save** to save your edits and to return to the User Groups panel.

Rebuild the User Group

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

1. In the User Groups panel, select the user group to be rebuilt.
2. Click **Rebuild** to initiate the rebuild process for that user group.
3. After a few minutes, click the **Refresh** button to refresh the display in the panel. Note that the Last Rebuilt column for user group you rebuilt now displays the date and time of the rebuild.

Delete a User Group



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

To delete a user group:

1. In the User Groups panel, select the user group from the User Groups list.
2. Click **Delete** to open the Confirm dialog box with the message: "Are you sure you want to delete this user group?"



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



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

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

Chapter 2: Admin Groups Setup

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

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

In the navigation toolbar, 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:

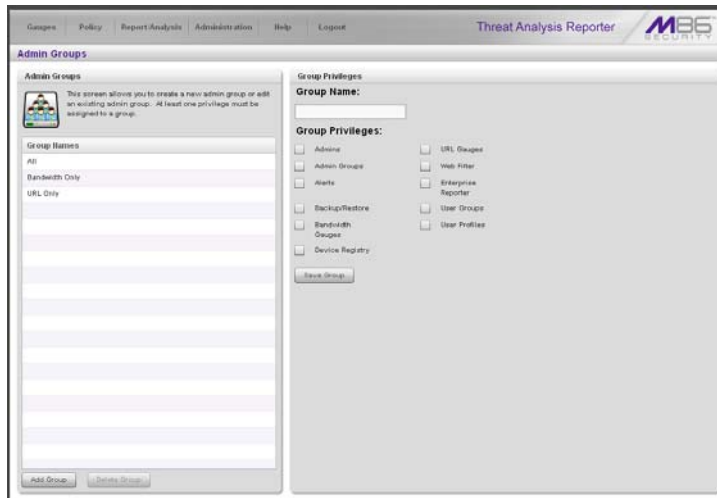



Fig. 2:2-1 Admin Groups panel

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

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

Add a Group

1. At the bottom of the Admin Groups frame, Click **Add Group**.
2. At the top of the Group Privileges frame, type in up to 32 characters for the **Group Name**.

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

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

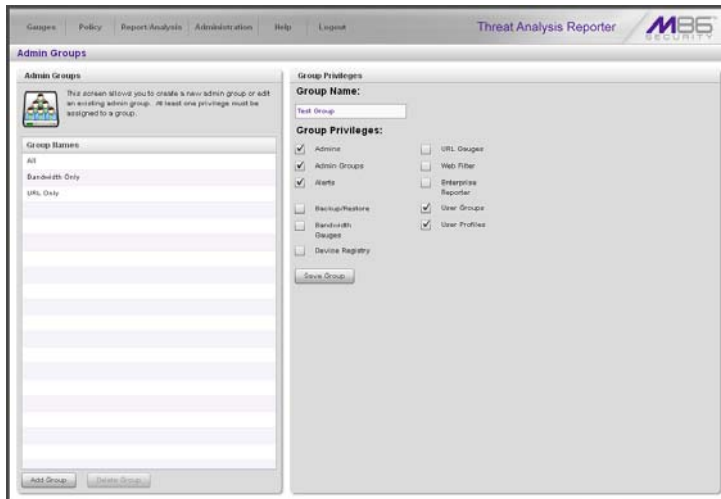


Fig. 2:2-2 Add a new Group

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

- **Backup/Restore** - Perform a backup and/or restoration on the TAR application.
- **Bandwidth Gauges** - Monitor and manage bandwidth gauges for inbound and outbound traffic.
- **Device Registry** - Edit settings for a Web Filter or TAR (a bandwidth IP address range for TAR can also be added or removed); add another Web Filter; view information about devices connected to the TAR application; or synchronize—with TAR—the source Web Filter's supplied library category updates, custom categories, and/or user group information.
- **URL Gauges** - Monitor and manage URL gauges.
- **Web Filter** - Access the Web Filter application to configure user filtering profiles.
- **Enterprise Reporter** - Access the ER applications to configure the database and generate reports on end user Internet activity.
- **User Groups** - Manage user groups.
- **User Profiles** - Manage a list of end users' logged events.



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

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

View, Edit an Admin Group's Permissions

View Admin Group settings

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

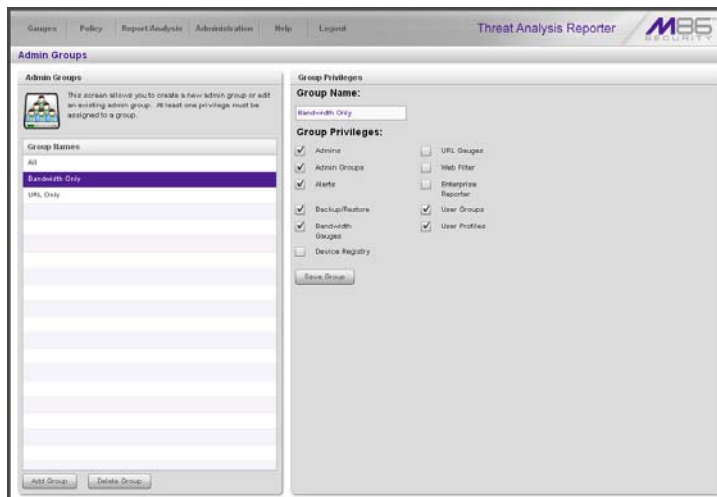


Fig. 2:2-3 Admin Groups group selections

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

Edit Admin Group settings

1. In the Group Privileges frame, perform any of the following actions:
 - Modify the **Group Name**
 - Add functions to be monitored by the administrator group
 - Remove functions to be monitored by the administrator group
2. Click **Update Group** to save your settings and to clear all selections in the Group Privileges frame.

Delete an Administrator Group

1. In the Group Names list box, click the name of the administrator group to highlight the group name, activate all buttons, and to populate the Group Privileges frame with previously-saved settings.
2. Click **Delete Group** to open the Confirm dialog box with the message: “Are you sure you want to delete this admin group?”
3. Click **Yes** to close the dialog box and to remove the administrator group from the Group Names list box.



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

Chapter 3: Admins Setup

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

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

In the navigation toolbar, mouse over the Administration menu link and select **Add/Edit Admins** to display the Add/Edit Admins panel:

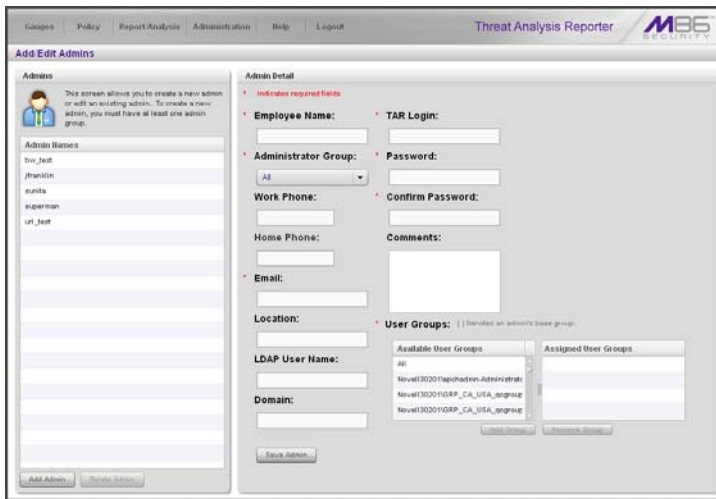


Fig. 2:3-1 Add/Edit Admins panel

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



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

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

Add an Administrator Profile

1. At the bottom of the Admins frame, click **Add Admin** to clear and reset the Admin Detail frame.
2. In the Admin Detail frame, make the following entries or selections as appropriate:

Fig. 2:3-2 New administrator information entered but not yet saved

- Type in the group administrator's **Employee Name**.
- Select the **Administrator Group** (previously set up in the Admins Group panel) from the available choices in the pull-down menu.
- Optional: Type in the group administrator's **Work Phone** number, without entering special characters such as parentheses (), a hyphen (-), a period (.), or a left slash (/).

- Optional: Type in the group administrator's **Home Phone** number without entering any special characters.
- Type in the group administrator's **Email** address.
- Optional: Type in identifying information about the group administrator's physical office **Location**.
- Optional: If the administrator has an Active Directory LDAP account, user name, and domain, type in the alphanumeric group administrator's **LDAP User Name** exactly as set up on the Active Directory domain in which he/she is registered.
- Optional: If an entry was made in the LDAP User Name field, type in the exact characters for the LDAP Active Directory **Domain** name in which the group administrator is registered.



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

- Type in the **TAR Login ID** the group administrator will use to access the TAR 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 TAR Login ID, and enter that same password again in the **Confirm Password** field. These entries display as asterisks for security purposes.
- Optional: Type in any **Comments** to be associated with the group administrator's account.

3. In the User Groups section, select the user group(s) to be monitored by the group administrator:
 - In the Available User Groups list box, click the user group(s) to highlight your selection(s), and to activate the Add Group button.
 - Click **Add Group** to include the user group(s) in the Assigned User Groups list box.



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

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

View, Edit Admin Detail

View Admin Details

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

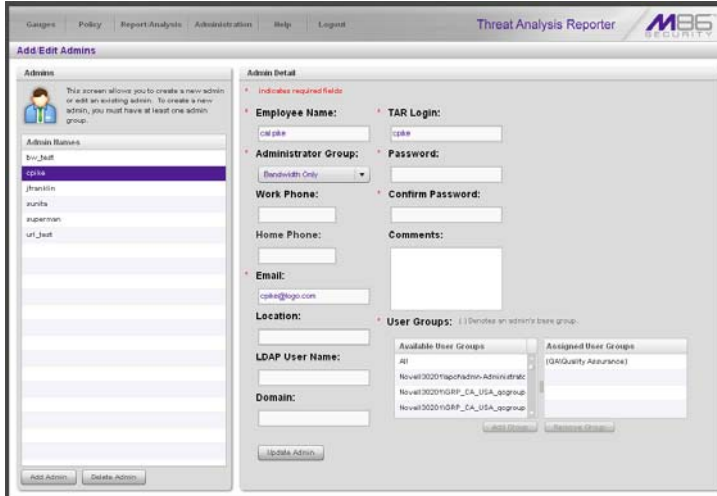



Fig. 2:3-3 Add/Edit Admins, Admin Names selection

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

Additionally, the checkbox for “Update this account on all local appliances” displays beneath the User Groups section.

Edit Account Info

1. In the populated Admin Detail frame:
 - The following information can be updated: Employee Name, Administrator Group selection, Email address, TAR Login ID, Password and Confirm Password entries, and User Groups selections.
 - The following information can be added, modified, or deleted: Work Phone number, Home Phone number, Location information, LDAP User Name or Domain name—the latter two fields are available if using LDAP—and Comments.
 - For the global administrator account, by checking the checkbox labeled “Update this account on all local appliances”, the account information updated for this account will be updated for all applications on the SR appliance—i.e. ER Administrator Module and ER Web Client, in addition to TAR.
2. After making any modifications, click **Update Admin** to save your edits.



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

Delete Admin



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

1. In the Admin Names list box, select the group administrator's TAR Login ID.
2. Click **Delete Admin** to open the Confirm dialog box with the message: "Are you sure you want to delete this admin?"



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

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

TAR CONFIGURATION SECTION

Introduction

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

- Chapter 1: Gauge Components - This chapter describes the types of gauges, the components of a gauge, how to read a gauge, and how to perform shortcuts using gauges.
- Chapter 2: Custom Gauge Setup, Usage - This chapter explains how gauges are configured and monitored.
- Chapter 3: Alerts, Lockout Management - This chapter explains how alerts are set up and used, and how to manage end user lockouts.
- Chapter 4: Analyze Usage Trends - This chapter explains how trend charts are used for assessing end user Internet/network activity. For additional or historical information about end user Internet usage trends, the Web Filter's user interface and the ER's Web Client reporting application and Administrator console can be accessed from the TAR user interface.
- Chapter 5: Identify Users, Threats - This chapter explains how to perform a custom search on Internet/network usage by a specified user, or for a specified threat or threat group.

Chapter 1: Gauge Components

Types of Gauges

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

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

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

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

Anatomy of a Gauge

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

The illustration below depicts a URL gauge and a bandwidth gauge and some of their components:

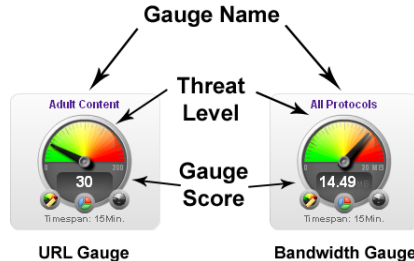


Fig. 3:1-1 URL and bandwidth gauge anatomy

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

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

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

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

- URL gauge - score includes the total number of end user hits (page count plus blocked object count) for all library categories the gauge monitors.
- Bandwidth gauge - score includes the total number of bytes (kB, MB, GB) of inbound/outbound end user traffic for all protocols/ports the gauge monitors.

How to Read a Gauge

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

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

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

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



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

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



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

Bandwidth Gauge Components

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

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

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

- **80** - HTTP TCP port used for transferring and listening
- **443** - HTTPS TCP/UDP port used for encrypted transmission over TLS/SSL
- **8080** - HTTP Alternate (http-alt) TCP port used under the following conditions: when running a second Web server on the same machine (the other is using port 80), as a Web proxy and caching server, or when running a Web server as a non-root user. This port is used for Tomcat.
- **FTP** - File Transfer Protocol gauge monitors the protocol used for transferring files from one computer to another on the Internet or an intranet.

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

- **20** - FTP TCP/UDP data port for file transfer
- **21** - FTP TCP/UDP control (command) port for file transfer
- **SMTP** - Simple Mail Transfer Protocol gauge monitors the protocol used for transferring email messages from one server to another.

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

- **25** - SMTP TCP/UDP port used for email routing between mail server email messages
- **110** - POP3 (Post Office Protocol version 3) TCP port used for sending/retrieving email messages
- **P2P** - Peer-to-Peer gauge monitors the protocol used for communication between computing devices—desktops, servers, and other smart devices—that are linked directly to each other.

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

- **1214** - TCP/UDP port for Kazaa, Morpheous, Grokster, etc.
- **4662** - TCP/UDP port for eMule, eDonkey, etc.
- **4665** - TCP/UDP port for eDonkey 2000
- **6346** - TCP/UDP port for Gnutella file sharing (Frost-Wire, LimeWire, BearShare, etc.)
- **6347** - TCP/UDP port for Gnutella
- **6699** - UDP port for Napster
- **6881** - TCP/UDP port for BitTorrent
- **IM** - Instant Messaging gauge monitors the protocol used for direct connections between workstations either locally or across the Internet.


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


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


Gauge Usage Shortcuts

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

- View Gauge Ranking** - Clicking a gauge or right-clicking a gauge and selecting this topic from the menu displays the Gauge Ranking panel. The table in this panel contains a list of library categories/protocols/ports that comprise the gauge, along with the list of current users driving the gauge's score. (See View End User Gauge Activity in Chapter 2 of the TAR Configuration Section.)
- Edit Gauge** - Clicking the left icon at the bottom of a gauge—or right-clicking a gauge and then selecting this menu topic—displays the panel that lets you edit the gauge's components. This is a shortcut to use instead of going to the Add/Edit Gauges panel, selecting the gauge, and then clicking Edit Gauge. (See Modify a Gauge in Chapter 2 of the TAR Configuration Section.)


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


- Trend Charts** - Clicking the middle icon at the bottom of a gauge—or right-clicking a gauge and then selecting this menu topic—displays a Trend Chart for this particular gauge that lets you



analyze the gauge's activity. (See View Trend Charts in Chapter 4 of the TAR Configuration Section.)

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

Chapter 2: Custom Gauge Setup, Usage

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

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

1. In the navigation toolbar, mouse over the the Gauges menu link and select **Add/Edit Gauges** to open the Add/Edit Gauges panel:

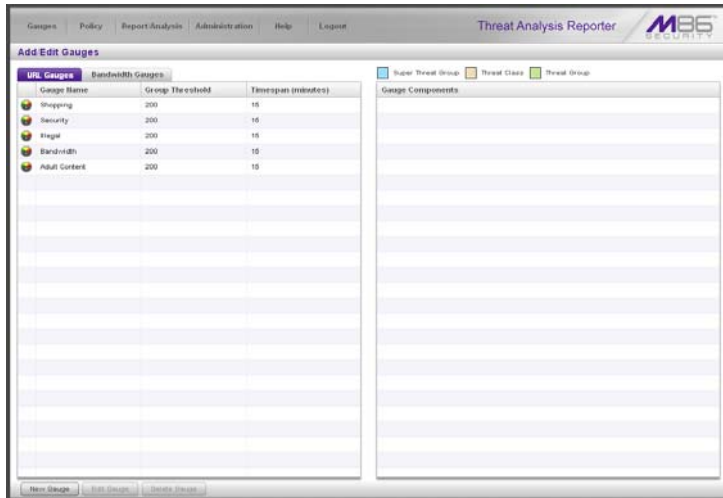


Fig. 3:2-1 Add/Edit Gauges panel

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

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

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

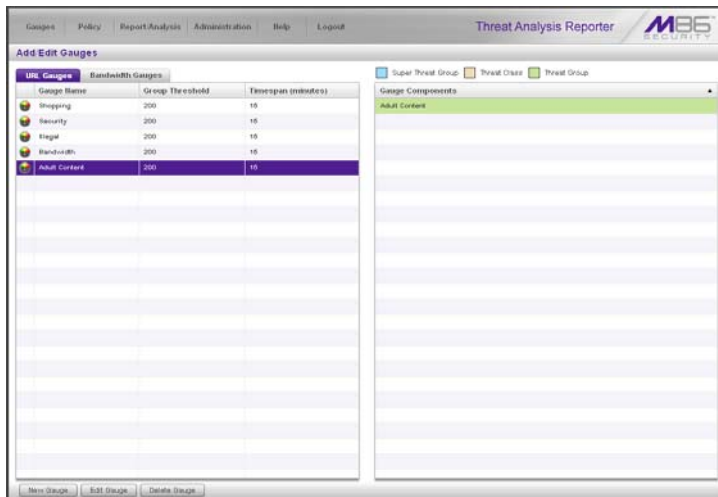


Fig. 3:2-2 Gauge Components frame populated

Add a Gauge

In the Add/Edit Gauge panel, click **New Gauge** to display Gauge panel:

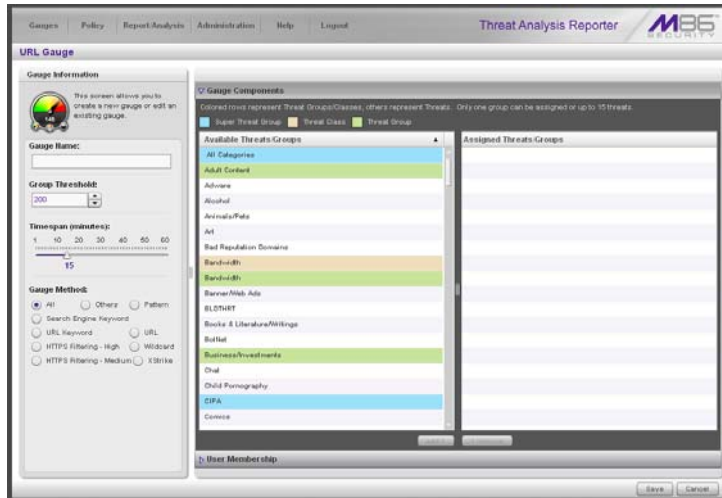


Fig. 3:2-3 Add a new gauge

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

When adding a new gauge, do the following:

- Name the gauge, and specify group threshold limits, timespan values, and the method(s) to be used by the gauge (see Specify Gauge Information).
- Select the library categories/protocols/ports for the gauge to monitor (see Define Gauge Components).
- Assign user groups whose end users' Internet/network activity will be monitored by the gauge (see Assign User Groups).

Specify Gauge Information

In the Gauge Information frame:

1. Type in at least two characters for the **Gauge Name** using upper and/or lowercase alphanumeric characters, and spaces, if desired.
2. Specify the **Group Threshold** ceiling of gauge activity. The default and recommended value is **200** for a URL gauge and **20 MB** for a bandwidth gauge. This ceiling can be adjusted after using TAR for awhile and evaluating activity levels at your organization.

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

3. Use the slider tool to specify the **Timespan (minutes)** for tracking gauge activity (1 - 60 minutes). The default and recommended value is **15** minutes. The timespan will always keep pace with the current time period, so that if a timespan of 15 minutes is specified, the gauge will always reflect the most recent end user activity from the past 15 minutes.
4. If necessary, specify a different **Gauge Method** to be used for tracking gauge activity:
 - For a URL gauge - **All** (default), **Others** (all gauge methods, not including Keywords or URLs), **Pattern**, **Search Engine Keyword**, **URL Keyword**, **URL**, **HTTPS 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 TAR must have “Search Engine Keyword Filter Control” or “URL Keyword Filter Control” enabled.

Define Gauge Components

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



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

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


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



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

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

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

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

Assign user groups

To assign user groups to be monitored by the gauge:

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

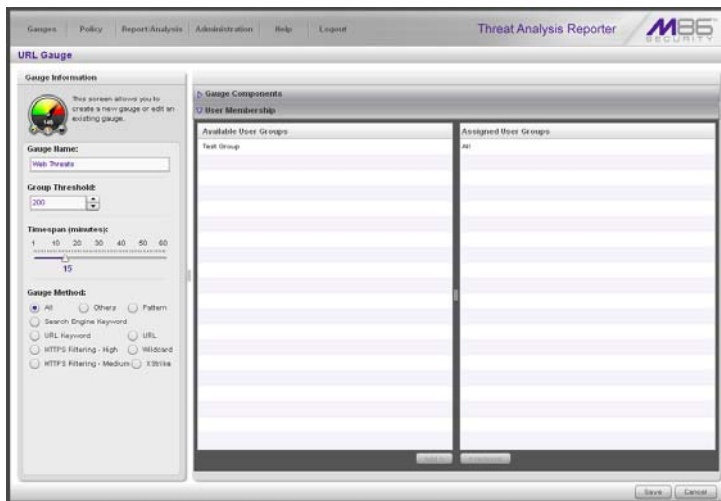




Fig. 3:2-4 User Membership accordion opened

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

2. From the Available User Groups list, select the user group to highlight it.
3. Click **add >** to move the user group to the Assigned User Groups list box.

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

Save gauge settings

After adding users, click **Save** to return to the Add/Edit Gauges panel that now includes the name of the gauge you just added:

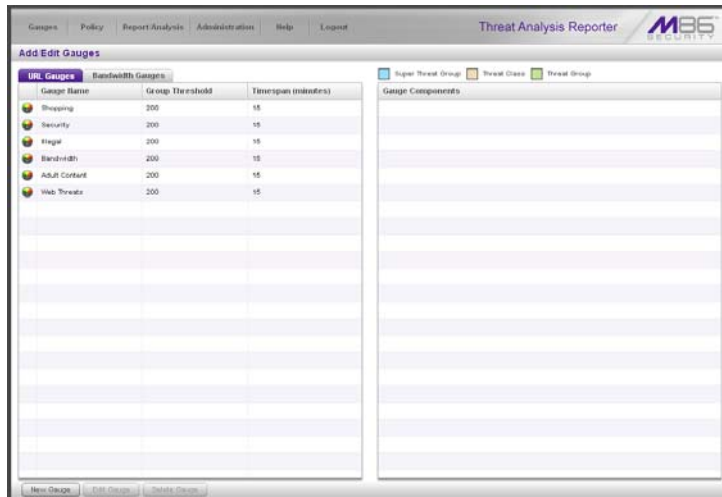


Fig. 3:2-5 New gauge added

Modify a Gauge

Edit gauge settings

1. In the Add/Edit Gauge panel, click the URL Gauges or Bandwidth Gauges tab.
2. Select the gauge from the list to activate all buttons below and populate the Gauge Components frame to the right:

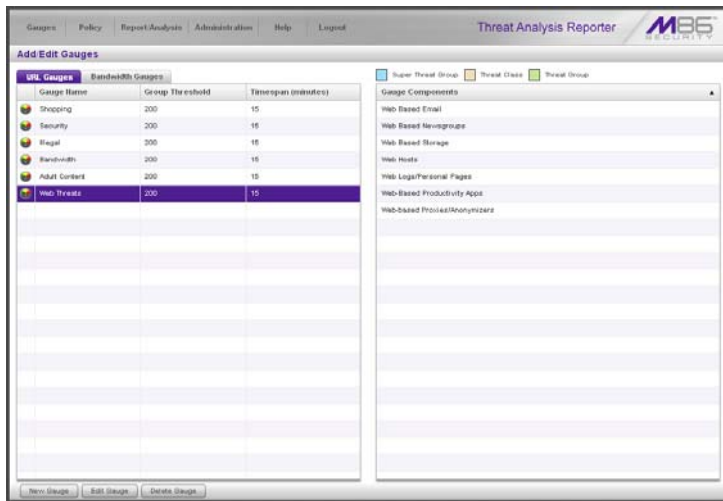


Fig. 3:2-6 Select the gauge to be edited

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

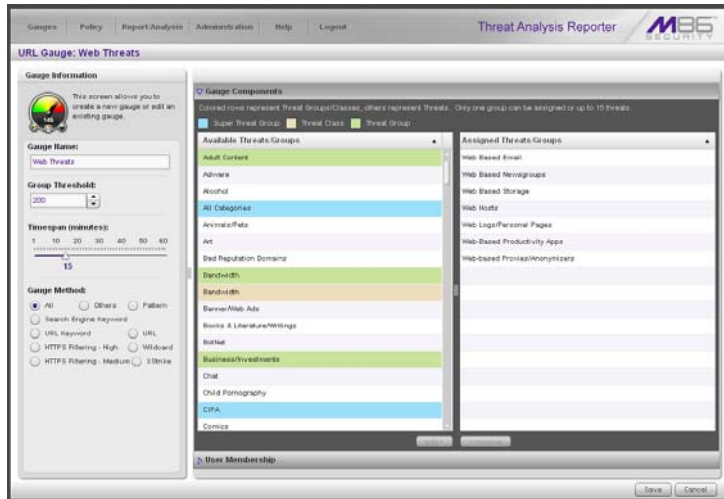



Fig. 3:2-7 Edit gauge settings

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

4. Edit any of the following criteria, as necessary:
 - Gauge Information - Gauge Name, Group Threshold, Timespan in minutes, Gauge Method (see Specify Gauge Information).
 - Gauge Components (see Define Gauge Components).
 - User Membership (see Assign user groups).
5. Click **Save** to save your edits and return to the Add/Edit Gauges panel.

Hide, Disable, Delete, Rearrange Gauges

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

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

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

1. In the navigation toolbar, mouse over the Gauges menu link and select **Dashboard Settings** to display the Dashboard Settings panel:

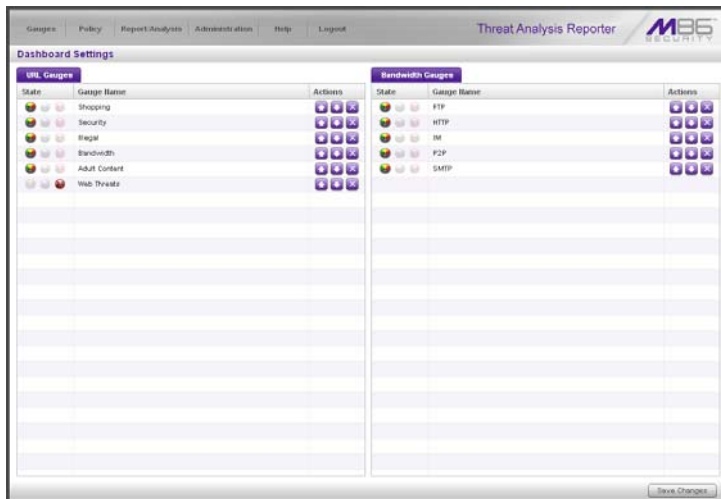





Fig. 3:2-8 Dashboard Settings panel

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:

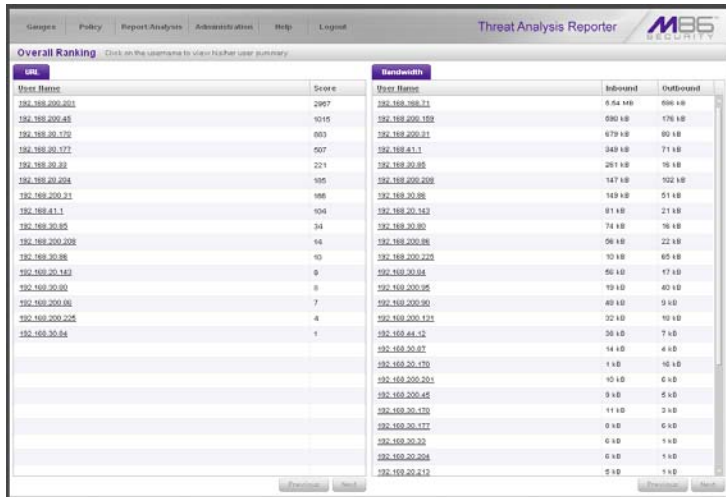


Fig. 3:2-9 Overall Ranking panel

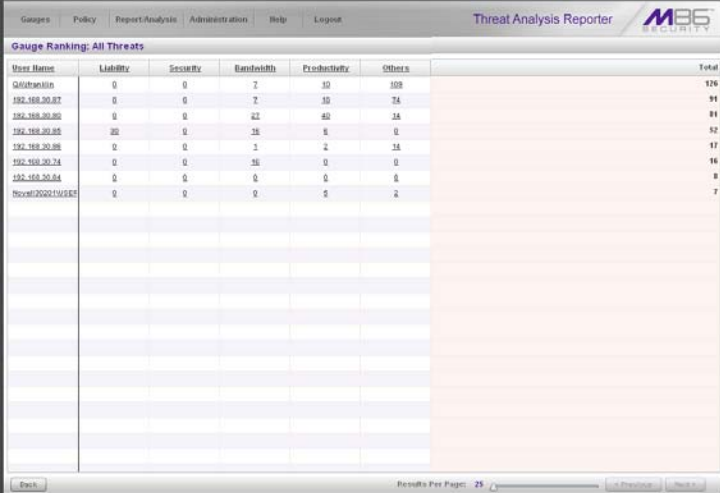
The URL frame displays to the left and the Bandwidth frame displays to the right, containing the User Name (or IP address) and Score for each user currently affecting one or more gauges.

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

2. To drill down and view additional information about an end user's activity, click the **User Name** in the appropriate tab to access the User Summary panel (see Monitor, Restrict End User Activity).
3. In the User Summary panel, you can view URLs visited by the end user and lock out that user from accessing designated areas of the Internet/network.

View a Gauge Ranking table

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



| Users Name | Liability | Security | Bandwidth | Productivity | Others | Total |
|-----------------|-----------|----------|-----------|--------------|--------|-------|
| GoldmanSachs | 0 | 0 | 2 | 10 | 108 | 120 |
| 192.168.20.217 | 0 | 0 | 2 | 10 | 24 | 36 |
| 192.168.20.202 | 0 | 0 | 22 | 40 | 24 | 86 |
| 192.168.20.205 | 20 | 0 | 26 | 8 | 0 | 54 |
| 192.168.20.206 | 0 | 0 | 1 | 2 | 24 | 27 |
| 192.168.20.214 | 0 | 0 | 16 | 0 | 0 | 16 |
| 192.168.20.244 | 0 | 0 | 0 | 0 | 8 | 8 |
| Novel2002111287 | 0 | 0 | 0 | 2 | 2 | 4 |

Fig. 3:2-10 Gauge Ranking table



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

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

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

- Access the User Summary panel by clicking the **User Name** (see Monitor, Restrict End User Activity: View User Summary data). In the User Summary panel, you can view URLs visited by the end user and lock out that user from accessing designated areas of the Internet/network.
- Access the Threat View User panel by clicking a user's score for a gauge (see Monitor, Restrict End User Activity: Access the Threat View User panel). In the Threat View User panel, you view current details for the gauge.

Monitor, Restrict End User Activity

View User Summary data

The User Summary panel contains the following frames:

- User Detail Information frame to the left that includes the Group Membership and Lockout accordions. The Group Membership accordion is expanded by default and displays a list of groups in which the end user belongs.
- Gauge Readings frame to the right that includes the URL Gauges and Bandwidth Gauges tabs, each showing the Gauge Name and end user's Total score for each gauge in the dashboard.

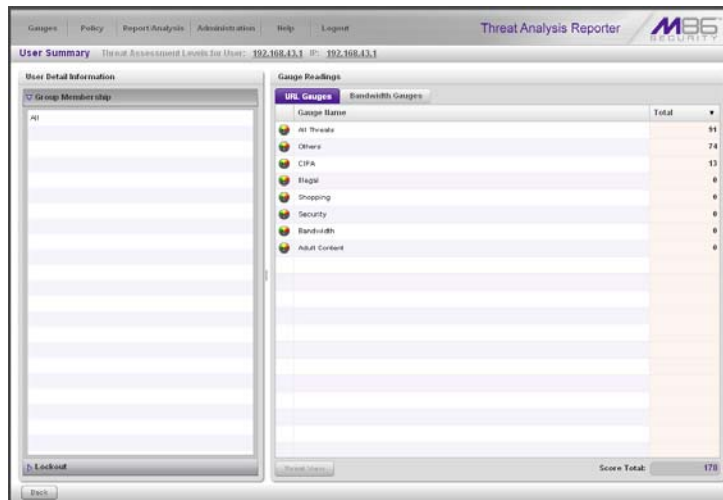


Fig. 3:2-11 User Summary panel

In this panel you can perform the following actions:

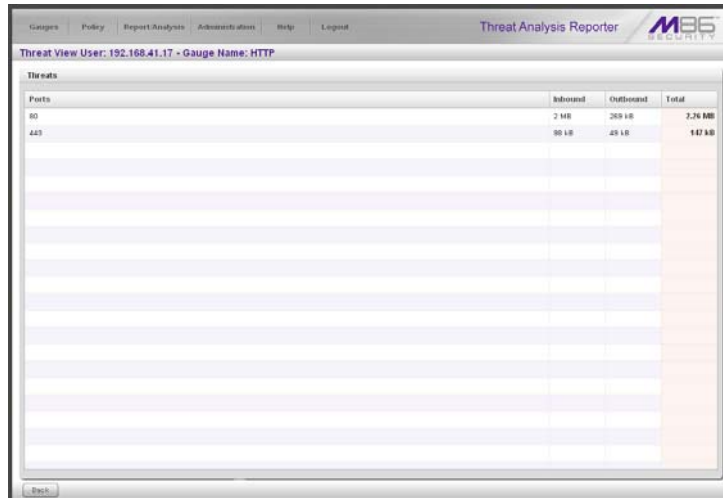
- Access the Threat View User panel to see which of the gauge's library categories/ports the end user accessed and the score (see Access the Threat View User panel).
- Access the Lockout option to lock out the end user from specified Internet/network privileges (see Manually lock out an end user).

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

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

Bandwidth Gauges tab selection

For Bandwidth gauges, the Threat View User panel contains the Threats frame showing the Ports column and corresponding Inbound/Outbound bandwidth usage by the end user for that port, and the combined Total inbound and outbound bandwidth usage by the end user for that port:



The screenshot shows the Threat Analysis Reporter interface. The top navigation bar includes links for Gauges, Policy, Report Analysis, Administrators, Help, and Logout. The main content area is titled "Threat View User: 192.168.41.17 - Gauge Name: HTTP". Below this, there is a "Threats" section with a table showing bandwidth usage for different ports.

| Ports | Inbound | Outbound | Total |
|-------|---------|----------|---------|
| 80 | 2 MB | 269 KB | 2.26 MB |
| 443 | 90 KB | 48 KB | 147 KB |

Fig. 3:2-13 Threat View User panel for Bandwidth Gauges tab selection

Manually lock out an end user

1. In the User Summary panel, in the User Detail Summary frame, click the Lockout accordion to open it:

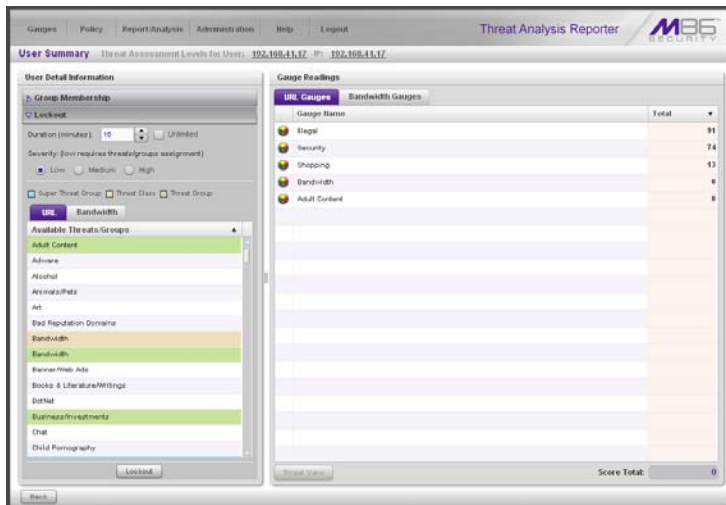


Fig. 3:2-14 User Summary panel, Lockout accordion expanded

2. Specify the **Duration** (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 Internet access (see Medium and High severity lockout).

- **High** - This selection locks out the end user from all network access (see Medium and High severity lockout).
4. After performing the additional steps based on the chosen lockout Severity level, click **Lockout** at the bottom of the frame to open the Info alert box with the message: "This user has been locked out."
 5. Click **OK** to close the alert box and to lock out the user from the designated library categories/ports for the specified duration of time.

Low severity lockout

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

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

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



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

Medium and High severity lockout

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

End user workstation lockout

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

Low severity URL lockout

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

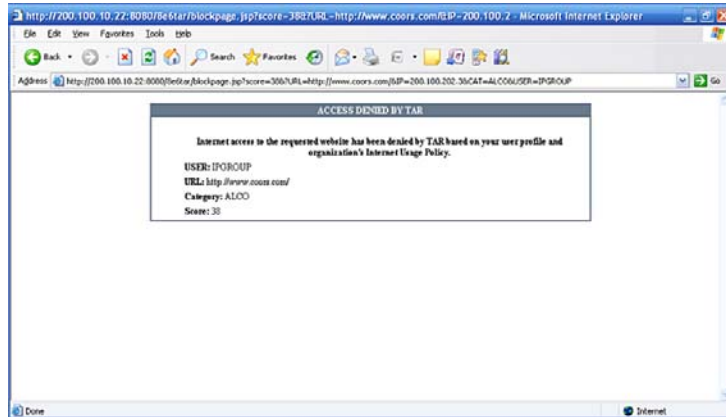


Fig. 3:2-15 Low severity URL lockout page

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

Medium severity URL and bandwidth lockout

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

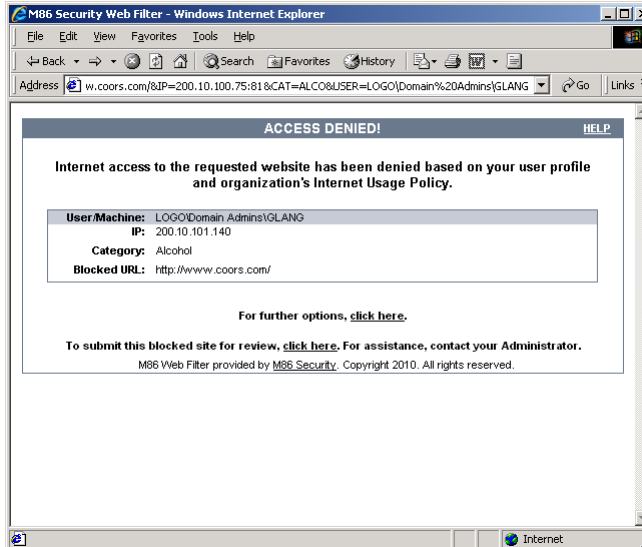


Fig. 3:2-16 Medium severity lockout page

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

By default, the following standard links are included in the block page: [HELP](#); [M86 Security](#); For further options, [click here](#); To submit this blocked site for review, [click here](#).



NOTE: Please refer to the Global Administrator Section of the Web Filter User Guide for information about fields in the block page and how to use them.

Low/high bandwidth, high severity URL lockout

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

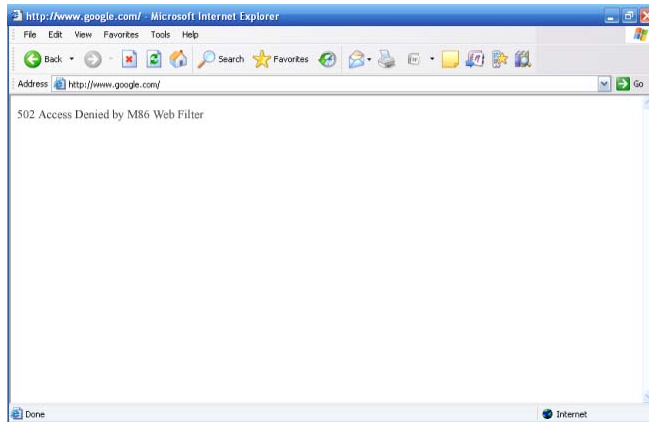


Fig. 3:2-17 Low severity bandwidth, high severity lockout page

This page contains the following information: “502 Access Denied by 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, as detailed in Chapters 2 and 3 of the TAR Preliminary Setup Section.

1. In the navigation toolbar, mouse over the Policy menu link and select **Alerts** to open the Alerts panel:

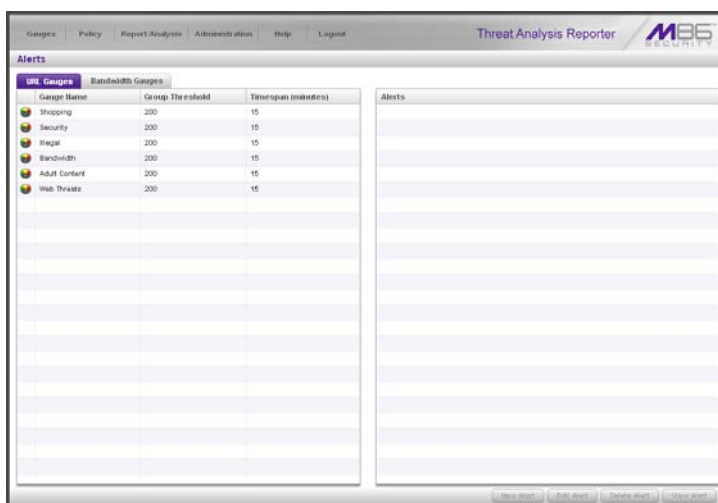


Fig. 3:3-1 Alerts panel

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

2. Do the following to view the contents in the tab to be used:
 - Click **URL Gauges** if this tab currently does not display. By default, this tab includes the following list of Gauge Names: Adult Content, Bandwidth, Illegal, Security, Shopping.

For each Gauge Name in this list, the following information displays: Group Threshold (*200*), Timespan (minutes)—*15* by default.
 - Click **Bandwidth Gauges** to view the contents of this tab. By default, this tab includes the following list of Gauge Names: FTP, HTTP, IM, P2P, SMTP.

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

Add an Alert

1. From the left frame, select the gauge for which an alert will be created; this action activates the New Alert button.
2. Click **New Alert** to open the panel for that gauge:

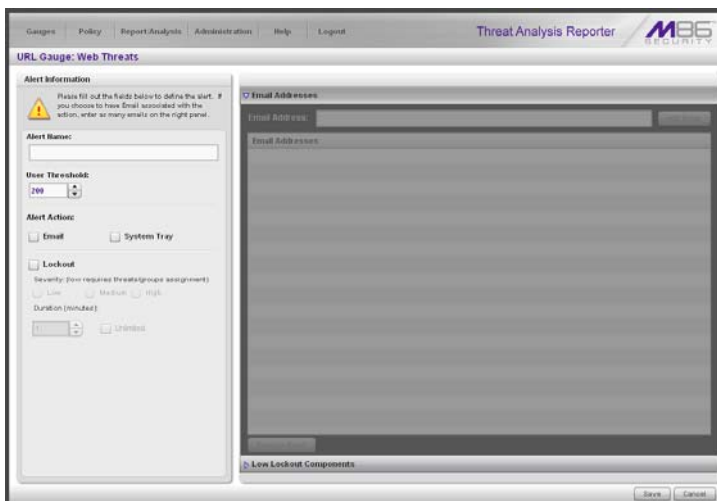


Fig. 3:3-2 Add a new Alert

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

3. In the Alert Information frame, type in the **Alert Name** to be used for the alert that will be delivered to the group administrator.
4. Specify the **User Threshold** ceiling of gauge activity that will trigger the alert.



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

5. In the Alert Action section, specify the mode(s) to use when an alert is triggered:
 - **Email** - An email alert notifies a group administrator via email if an end user has reached the threshold limit set up in a gauge alert.
 - **System Tray** - A TAR Alert message notifies a group administrator via his/her workstation's System Tray if an end user has reached the threshold limit set up in a gauge alert.
 - **Lockout** - The Lockout function locks out an end user from Internet/network access if he/she reaches the threshold limit set up in a gauge alert.



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

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


Email alert function

Configure email alerts

To set up the email alert function:

1. In the Alert Action section of the Alert Information frame, click the checkbox corresponding to **Email** to open the Email Addresses accordion in the target frame to the right.
2. Type in the **Email Address**.
3. Click **Add Email** to include the address in the Email Addresses list box.

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

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

Receive email alerts


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

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

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

System Tray alert function

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

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

Lockout function

To set up the lockout function:

1. Click the checkbox corresponding to **Lockout** to activate the Severity and Duration (minutes) fields.
2. Specify the **Severity** of the end users' lockout:

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

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

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

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




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

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

3. Specify the **Duration** (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):

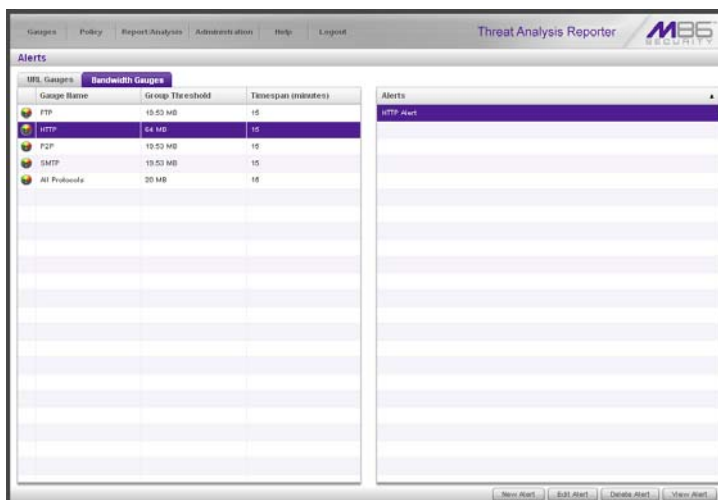


Fig. 3:3-3 Alert added

View alert settings

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

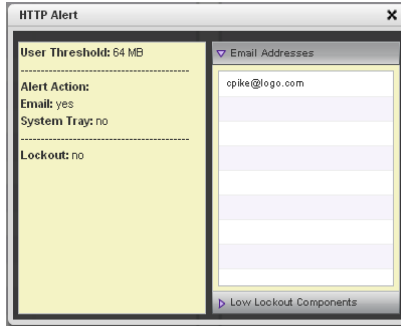


Fig. 3:3-4 View an alert

The following information displays to the left of this window:

- User Threshold amount
- Alert Action criteria (yes/no): Email, System Tray
- Lockout (yes/no)

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:

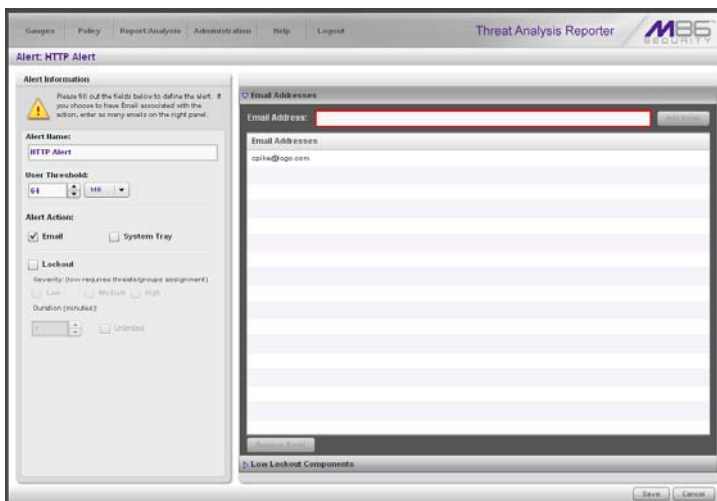


Fig. 3:3-5 Edit an alert

4. The following items can be edited:
 - Alert Name
 - User Threshold
 - Alert Action selections: Email, System Tray—the latter is only functional for Active Directory LDAP—and Lockout
 - Lockout Severity selection (Low, Medium, High)
 - Duration (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?”



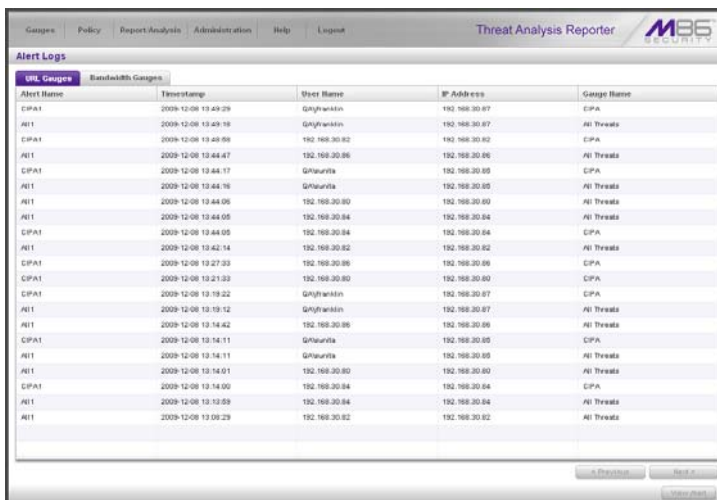
NOTE: Clicking *No* closes the dialog box without removing the alert, and returns you to the main Alerts panel.

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 |
|------------|---------------------|---------------|---------------|------------|
| CPA1 | 2009-12-08 13:49:29 | GlyFranklin | 192.168.30.87 | CPA |
| AI1 | 2009-12-08 13:49:18 | GlyFranklin | 192.168.30.87 | AI Threats |
| CPA1 | 2009-12-08 13:49:06 | 192.168.30.82 | 192.168.30.82 | CPA |
| AI1 | 2009-12-08 13:48:47 | 192.168.30.86 | 192.168.30.86 | AI Threats |
| CPA1 | 2009-12-08 13:48:17 | GWaurita | 192.168.30.85 | CPA |
| AI1 | 2009-12-08 13:48:16 | GWaurita | 192.168.30.85 | AI Threats |
| AI1 | 2009-12-08 13:48:05 | 192.168.30.80 | 192.168.30.80 | AI Threats |
| AI1 | 2009-12-08 13:48:05 | 192.168.30.84 | 192.168.30.84 | AI Threats |
| CPA1 | 2009-12-08 13:48:05 | 192.168.30.84 | 192.168.30.84 | CPA |
| AI1 | 2009-12-08 13:42:14 | 192.168.30.82 | 192.168.30.82 | AI Threats |
| CPA1 | 2009-12-08 13:27:33 | 192.168.30.86 | 192.168.30.86 | CPA |
| CPA1 | 2009-12-08 13:21:33 | 192.168.30.80 | 192.168.30.80 | CPA |
| CPA1 | 2009-12-08 13:19:32 | GlyFranklin | 192.168.30.87 | CPA |
| AI1 | 2009-12-08 13:19:12 | GlyFranklin | 192.168.30.87 | AI Threats |
| AI1 | 2009-12-08 13:18:42 | 192.168.30.86 | 192.168.30.86 | AI Threats |
| CPA1 | 2009-12-08 13:16:11 | GWaurita | 192.168.30.85 | CPA |
| AI1 | 2009-12-08 13:16:11 | GWaurita | 192.168.30.85 | AI Threats |
| AI1 | 2009-12-08 13:16:01 | 192.168.30.80 | 192.168.30.80 | AI Threats |
| CPA1 | 2009-12-08 13:16:00 | 192.168.30.84 | 192.168.30.84 | CPA |
| AI1 | 2009-12-08 13:10:59 | 192.168.30.84 | 192.168.30.84 | AI Threats |
| AI1 | 2009-12-08 13:08:29 | 192.168.30.82 | 192.168.30.82 | AI Threats |

Fig. 3:3-6 Alert Logs panel

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



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

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

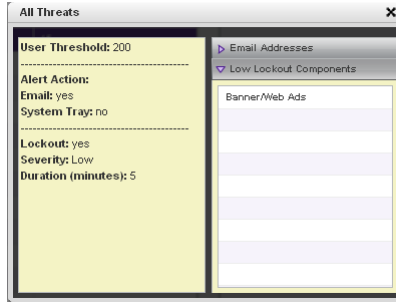
4. Click **View Alert** to open the alert viewer pop-up window:

Fig. 3:3-7 View an alert

The following information displays to the left of this window:

- User Threshold amount
- Alert Action criteria (yes/no): Email, System Tray
- Lockout (yes/no)

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.

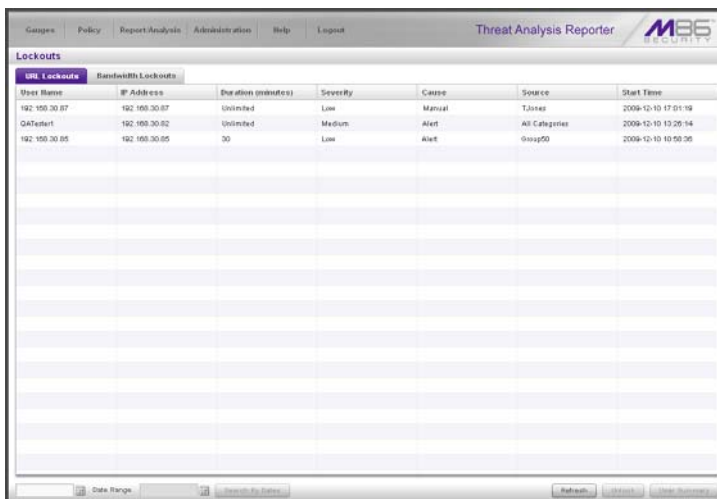
5. Click the “X” in the upper right corner of alert viewer pop-up window to close it.

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 |
|---------------|---------------|--------------------|----------|--------|----------------|---------------------|
| 192.155.30.87 | 192.155.30.87 | Unlimited | Low | Manual | T.Jones | 2009-12-10 17:01:59 |
| QA Tester | 192.155.30.82 | Unlimited | Medium | Alert | All Categories | 2009-12-10 13:26:14 |
| 192.155.30.85 | 192.155.30.85 | 30 | Low | Alert | Group00 | 2009-12-10 10:50:35 |


Fig. 3:3-8 View Lockouts

The lockout list contains records for all end users currently locked out of the Internet/network. Each end user’s record displays in a separate row. For each row in the list, the following information displays: User Name (or IP address); IP address; Duration (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:



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

2. Click the starting date to select it and to close the calendar pop-up window. This action populates the field with the selected date.
3. At the **Date Range** field, click the  calendar icon located to the right of the second date field; this action opens the larger calendar for the current month, with today's date highlighted.
4. Click the ending date to select it and to close the calendar pop-up window. This action populates the field with the selected date.

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



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

Unlock workstations

1. In the populated Lockouts panel, click each record to highlight it.
2. Click **Unlock** to unlock the end user(s) and to remove the record(s) from the list.



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

Access User Summary details

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

Chapter 4: Analyze Usage Trends

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

If more information is required in your analysis, the Web Filter application or the Enterprise Reporter's Web Client and Administrator console can be accessed via the TAR user interface so you can generate customized reports to run for a time period of your specifications.

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

View Trend Charts

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

- Pie trend chart for an individual URL or bandwidth gauge
- Pie trend chart for all collective URL or bandwidth gauges
- Line chart showing details for a pie chart

View activity for an individual gauge

To view activity for any individual URL or bandwidth gauge:

1. If the gauges dashboard does not currently display, 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:

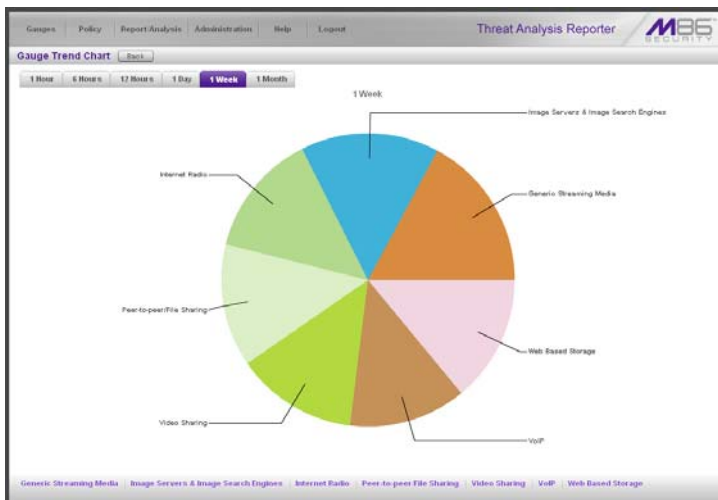


Fig. 3:4-1 Pie trend chart for an individual URL gauge

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

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

The top and bottom sections of this panel contain tabs.

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

View overall gauge activity

1. In the navigation toolbar, mouse over the Report/Analysis menu link and select the Trend Charts option.
2. Choose either **URL** or **Bandwidth** to display the Overall Trend Chart panel for the specified gauge type (URL or Bandwidth):

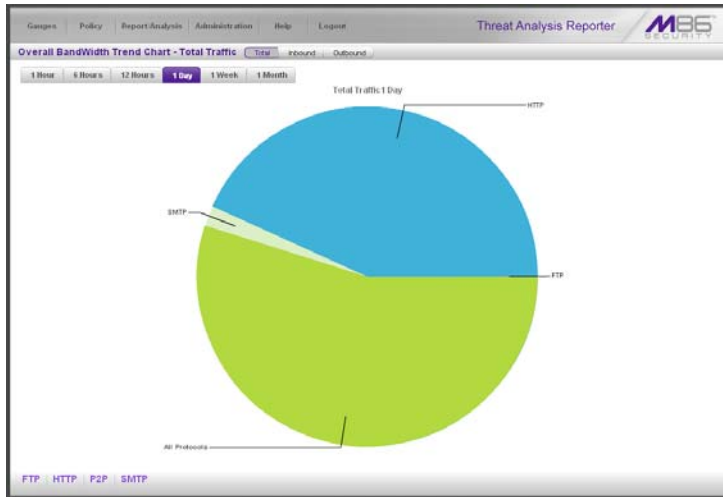


Fig. 3:4-2 Overall Bandwidth Trend Chart, Total Traffic

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

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

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

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

Navigate a trend chart

The following actions can be performed in this panel:

- View gauge activity for a different time period (1 Hour, 6 Hours, 12 Hours, 1 Day, 1 Week, 1 Month)
- Analyze gauge activity in a pie chart
- Analyze gauge activity in a line chart
- View Inbound, Outbound bandwidth gauge activity
- Print a trend chart from an IE browser window

View gauge activity for a different time period

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

- **1 Hour** - This selection displays the gauge URL/byte average score in 10 minute increments for the past 60-minute time period
- **6 Hours** - This selection displays the gauge URL/byte average score in 30 minute increments for the past six-hour time period
- **12 Hours** - This selection displays the gauge URL/byte average score in one hour increments for the past 12-hour time period
- **1 Day** - This selection displays the gauge URL/byte average score in one hour increments for the past 24-hour time period
- **1 Week** - This selection displays the gauge URL/byte average score in 12 hour increments for the past seven-day time period
- **1 Month** - This selection displays the gauge URL/byte average score in one-day increments for the past month's time period

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

Analyze gauge activity in a pie chart

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

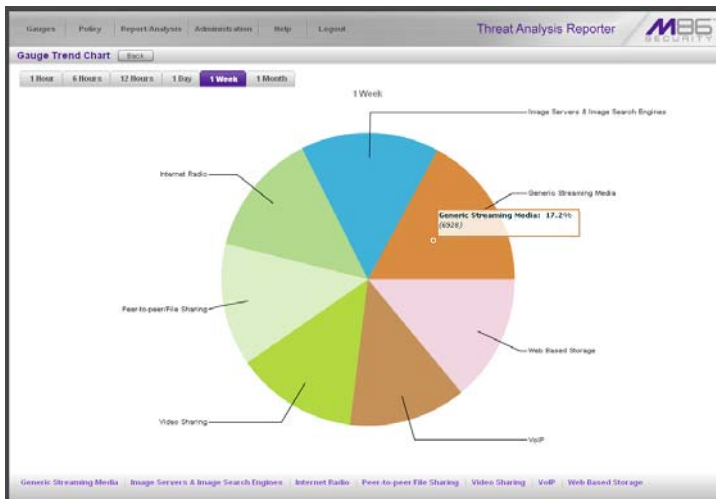


Fig. 3:4-3 Pie Gauge Trend Chart slice

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

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

Analyze gauge activity in a line chart

- To view a line chart showing activity for a slice of the pie chart, do either of the following:
 - Click that slice of the pie chart
 - Click the specified tab beneath the pie chart
 Either action displays the line Trend Chart:

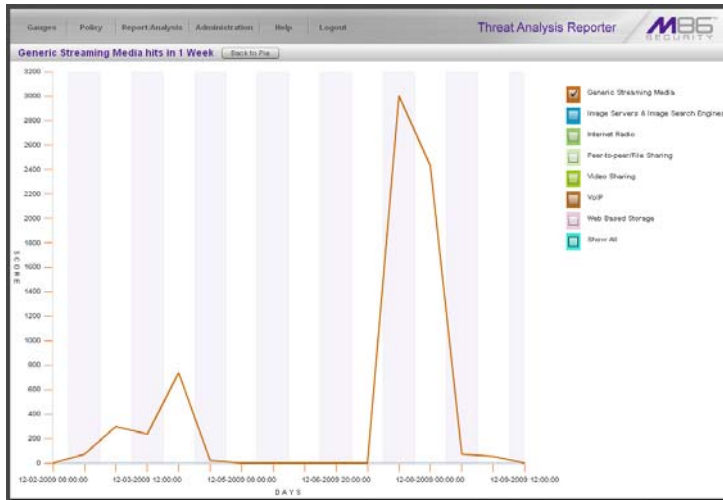


Fig. 3:4-4 Drill into a pie slice to display a line Trend Chart

By default, this chart contains the following information: linear depiction of the total end user SCORE in fixed time increments (using the MM-DD-YYYY HH:MM:SS format) for MINUTES 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.

- Perform any of the following actions in this chart:

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



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

- To view information about a specific point in the line chart, mouse over that point in the chart:

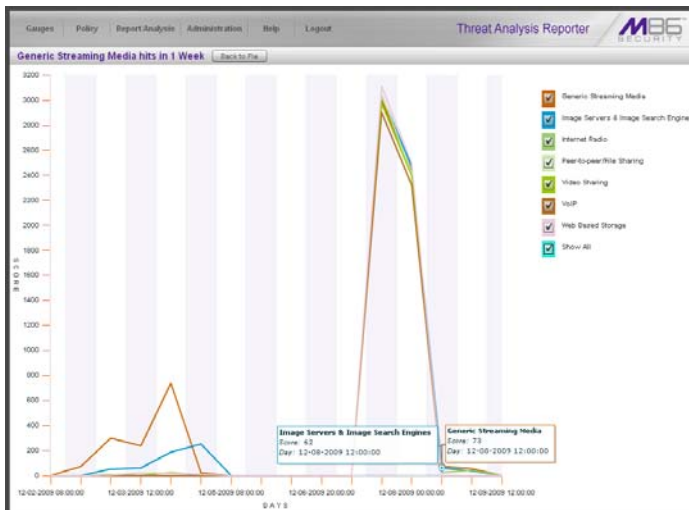


Fig. 3:4-5 Line Trend Chart data

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

Each box includes the following information: gauge component name, Score for that point, and Minutes 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.

Access Web Filter, ER Applications

The Web Filter can be accessed to configure this application and end user filtering profiles. ER Web Client reports can be generated for viewing historical Internet usage trend data, and the ER Administrator console can be accessed for troubleshooting or for further analysis.

Access the Web Filter

In the navigation toolbar, mouse over the Report/Analysis menu link and choose the IP address of the **Web Filter** to launch the login window for the Web Filter user interface at that IP address—or the Web Filter Welcome window, if using the global administrator single sign-on account.



NOTE: See the *Web Filter User Guide* for information on configuring and using the Web Filter.

Access the ER Web Client application

In the navigation toolbar, mouse over the Report/Analysis menu link and select **ER Reporter > Web Client** to launch the login window of the ER Web Client application—or the default Top 20 Users by Blocked Requests Executive Report, if using the global administrator single sign-on account.

Access the ER Administrator console

In the navigation toolbar, mouse over the Report/Analysis menu link and select **ER Reporter > Admin GUI** to launch the login window of the ER Administrator console—or the Server Status screen, if using the global administrator single sign-on account.

Chapter 5: Identify Users, Threats

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

Perform a Custom Search

In the navigation toolbar, mouse over the Report/Analysis menu link and select **Custom Search** to display the Custom Search panel:

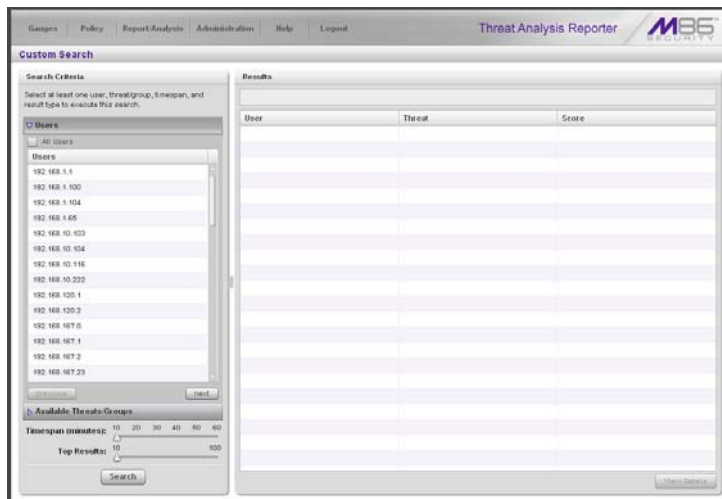


Fig. 3:5-1 Custom Search, Users accordion opened

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

Specify Search Criteria

1. In the **Users** accordion, do one of the following:
 - To identify users with the highest scores - Click the **All Users** checkbox to select all users in the list and to grey-out the list.
 - To identify the activities of a specific user - Select the user name/IP address from the list to highlight it.
2. Click the Available Threats/Groups accordion to open it.
3. Select either the **URL Threats** or **Bandwidth Threats** tab to display its list of library categories/protocols, and do either of the following:
 - To identify library categories or protocols with the highest scores - Select a category group or protocol that includes as many of categories/ports as possible.
 - To identify activities for a specific threat class/group - Select that threat class or group.

For bandwidth gauges, to query activities for a specific port number, click the **Port Number** checkbox to activate the port field and to deactivate the listed bandwidth protocol selections. Type a specific value in the pre-populated field, and/or use the up/down arrow buttons to increment/decrement the current value by one.
4. Use the **Timespan (Minutes)** slider to specify the time period in which the threat(s)/group(s) were accessed: last 10, 20, 30, 40, 50, 60 minutes.
5. If a user selection other than “All Users” was specified in the Users accordion, the **Top Results** slide becomes activated and you can make a selection for the maximum number of records to return in the results for that user: top 10, 20, 30, 40, 50, 60, 70, 80, 90, 100 records.
6. Click **Search** to display records returned by the query in the Results frame at the right side of the panel:

The screenshot shows the Threat Analysis Reporter interface. On the left, the 'Search Criteria' panel is set to 'Bandwidth Threats'. The 'Results' table on the right displays the following data:

| User | Ports | Inbound | Outbound | Total |
|-----------------|-------------|---------|----------|-------|
| 192.168.200.124 | 80 | 1002 | 614 | 2296 |
| 192.168.168.71 | 80 | 1375 | 120 | 1495 |
| 192.168.200.182 | 80 | 962 | 164 | 776 |
| 192.168.40.141 | 443 | 170 | 86 | 266 |
| 192.168.20.70 | Other Ports | 95 | 96 | 191 |
| 192.168.168.200 | Other Ports | 114 | 59 | 173 |
| 192.168.200.90 | Other Ports | 123 | 46 | 169 |
| 192.168.20.143 | 80 | 114 | 23 | 137 |
| 192.168.20.70 | 80 | 111 | 17 | 128 |
| Qikouita | 80 | 106 | 0 | 116 |
| 192.168.200.201 | 80 | 72 | 3 | 75 |
| 192.168.200.192 | Other Ports | 25 | 30 | 63 |
| 192.168.200.168 | 80 | 46 | 7 | 53 |
| 192.168.200.182 | 443 | 16 | 29 | 44 |
| 192.168.10.116 | 80 | 34 | 18 | 42 |
| 192.168.200.174 | 80 | 32 | 6 | 38 |
| 192.168.20.121 | Other Ports | 21 | 16 | 37 |
| 192.168.20.172 | Other Ports | 21 | 15 | 36 |
| 192.168.20.170 | Other Ports | 20 | 16 | 36 |
| 192.168.41.6 | 443 | 21 | 6 | 29 |
| 192.168.200.149 | 80 | 23 | 2 | 25 |
| 192.168.200.201 | Other Ports | 10 | 9 | 19 |
| 192.168.44.12 | 80 | 15 | 2 | 18 |

Fig. 3:5-2 Custom Search results for Bandwidth Threats

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

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

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

TAR ADMINISTRATION SECTION

Introduction

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



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

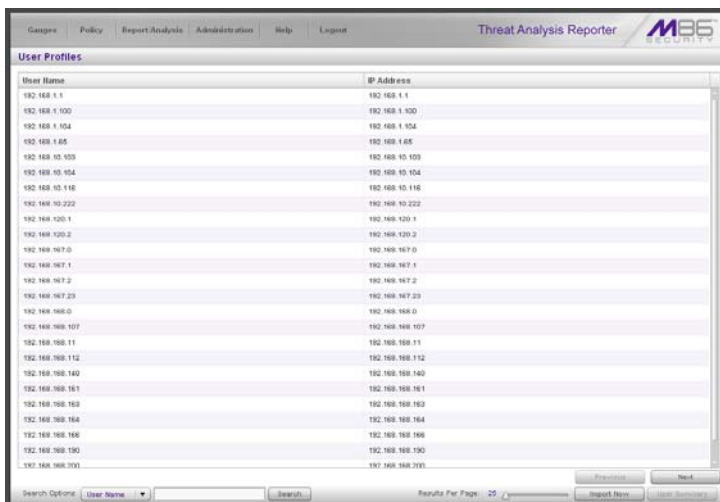
- Chapter 1: View the User Profiles List - This chapter explains the options for viewing end user information comprising the User Profiles list.
- Chapter 2: View Administrator Activity - This chapter explains how to view activity performed on TAR by the global or group administrators.
- Chapter 3: Maintain the Device Registry - This chapter provides information on viewing TAR's registry of associated devices; synchronizing TAR with the source Web Filter's library categories and user groups, and adding, editing or deleting a Web Filter to/from the registry. An SSL certificate for the SR can also be generated.
- Chapter 4: Perform Backup, Restoration - This chapter explains how to perform a backup on the TAR application, and how to restore user configuration settings saved in a previous backup to the application.

Chapter 1: View the User Profiles List

The User Profiles panel contains the list of users that is created when TAR first communicates with the source 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 TAR application. If there are any discrepancies, synchronization can be forced between the two servers (see Chapter 4: Maintain the Device Registry).

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

In the navigation toolbar, with the Administration tab selected, click **User Profiles** to display the User Profiles panel:



| 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 |
| 192.168.10.535 | 192.168.10.535 |
| 192.168.10.504 | 192.168.10.504 |
| 192.168.10.118 | 192.168.10.118 |
| 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 |
| 192.168.168.201 | 192.168.168.201 |

Fig. 4:1-1 View User Profiles list

By default, this panel is comprised of rows of end user records, sorted in ascending order by User Name (IP address). For each user name in the list, the corresponding end user IP Address displays.

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

Search the User Database

1. Specify search criteria by making a selection from the **Search Options** pull-down menu:
 - **User Name** - This selection performs a search by an end user's user name.
 - **IP Address** - This selection performs a search by an end user's IP address.
2. Make an entry in the blank field to the right:
 - If User Name was selected, enter a user name
 - If IP Address was selected, enter an IP address.
3. Click **Search** to display a record that matches your criteria.



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

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

View End User Activity

1. To drill down and view additional information about an end user's activity, select the user's record to highlight it.
2. Click **User Summary** to open the User Summary panel, and perform any of the actions described for this panel (see Monitor, Restrict End User Activity in the TAR Configuration Section, Chapter 2: Custom Gauge Setup, Usage).

Chapter 2: View Administrator Activity

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

In the navigation toolbar, with the Administration tab selected, click **Admin Trails** to display the Admin Trails panel:

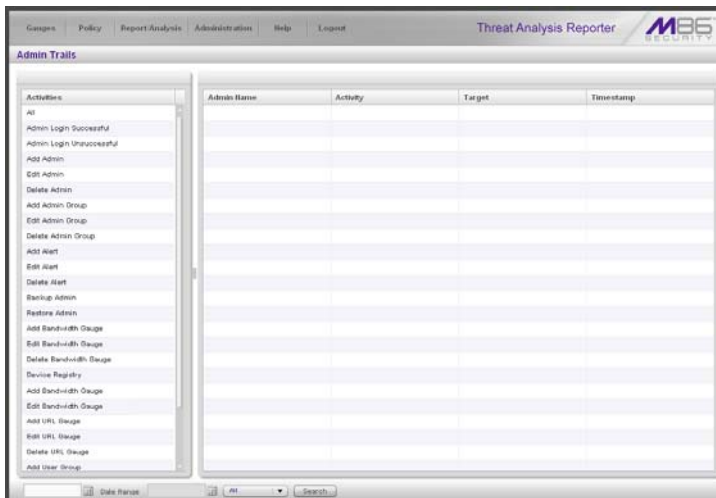


Fig. 4:2-1 Admin Trails panel

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


Perform a Search on a Specified Activity

To perform a search on a specified activity:

1. Select the type of Activity from available choices in the list: All, Admin Login Successful, Admin Login Unsuccessful, Add Admin, Edit Admin, Delete Admin, Add Admin Group, Edit Admin Group, Delete Admin Group, Add Alert, Edit Alert, Delete Alert, Backup Admin, Restore Admin, 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 Activity list will only display activity types performed on TAR within the past 30 days.

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



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

3. Click the starting date to select it and to close the calendar pop-up window. This action populates the field to the left of the calendar icon with the selected date.
4. Click the  calendar icon on the right to open the larger calendar for the current month, with today's date highlighted.
5. Click the ending date to select it and to close the calendar pop-up window. This action populates the field to the left of the calendar icon with the selected date.
6. To view the activity of a specified administrator, select the user name from the pull-down menu.

- Click **Search** to display the specified records for the selected dates in the Results list:

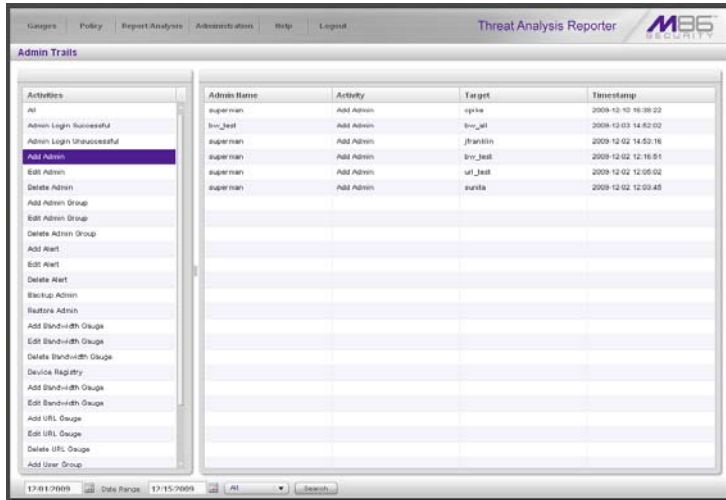


Fig. 4:2-2 Admin Trails results

Search results

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

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

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

- administrator name for Add/Edit/Delete Admin
- group name for Add/Edit/Delete Admin Group
- alert name for Add/Edit/Delete Alert
- gauge name for Add/Edit/Delete URL/Bandwidth Gauge.

Chapter 3: Maintain the Device Registry

TAR's device registry is used by the global administrator to view information about devices connected to the TAR unit, synchronize TAR with user groups and libraries from the source Web Filter, edit M86 appliance criteria, and add or delete a Web Filter from the registry. The Generate SSL Certificate function is also available so that the SR device will be recognized by your workstation as being valid.

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

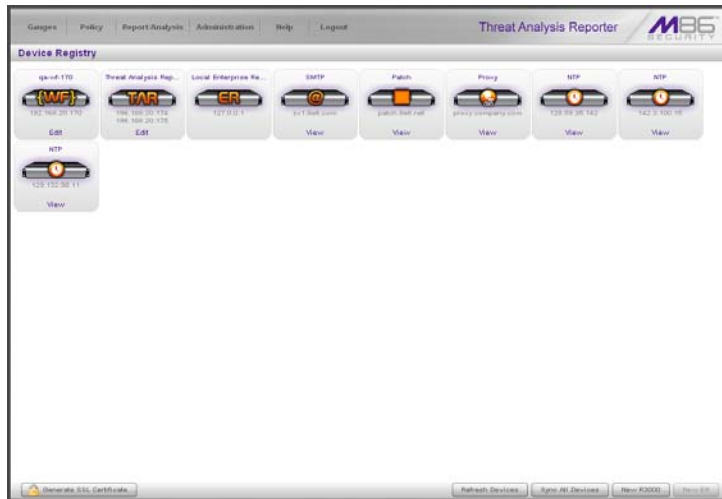


Fig. 4:3-1 Device Registry

This panel is comprised of icons representing devices set up to communicate with TAR. Except for the ER device set up during the wizard hardware installation process, 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:

- **Generate SSL Certificate** - Click this button to generate an SSL certificate for the SR unit.
- **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 another Web Filter to the device registry.



NOTE: *The New ER button is disabled since the ER is included in the SR unit by default and another ER unit cannot be added to the Device Registry.*

Generate SSL Certificate

Generate an SSL Certificate for the SR

Click **Generate SSL Certificate** to generate a Secure Socket Layer certificate that ensures secure exchanges between the SR server and your browser.

Web Filter Device Maintenance

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:

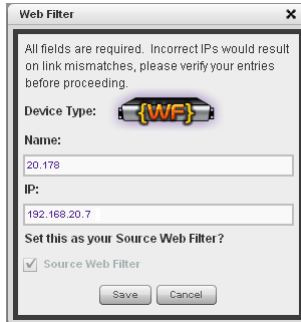


Fig. 4:3-2 Web Filter pop-up window

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:



Fig. 4:3-3 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.



TIP: A source Web Filter cannot be deleted. 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.

Threat Analysis Reporter Maintenance

View TAR device criteria

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

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

The following displays at the left side of this window: Device Type (TAR), Name of the application (Threat Analysis Reporter), and LAN1 and LAN2 IP 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 TAR 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:

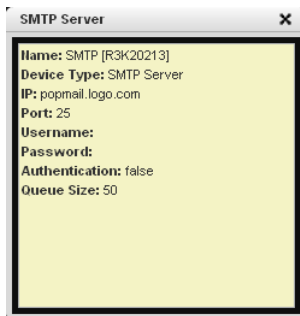


Fig. 4:3-5 SMTP window

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 NTP Server device criteria

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

View Proxy Server device criteria

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

Sync All Devices

A forced synchronization should be performed on the TAR unit if any of the source 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:

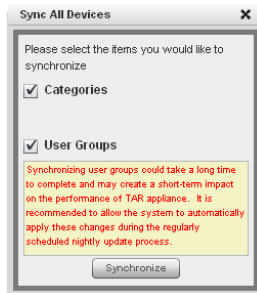


Fig. 4:3-6 Sync All Devices

2. Check the checkbox(es) pertaining to information to be synchronized between the Web Filter and TAR 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 TAR.
 - **User Groups** - Make this selection to synchronize LDAP user group information on the source Web Filter to TAR.



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



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

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

Chapter 4: Perform Backup, Restoration

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



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

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

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

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

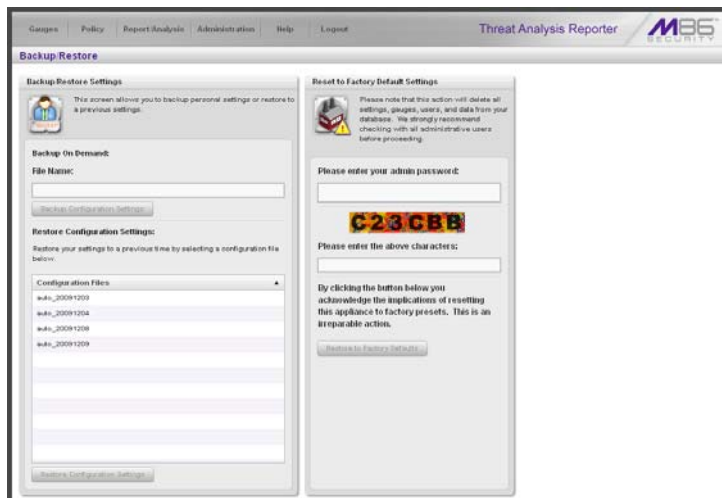


Fig. 4:4-1 Backup/Restore panel

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

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

By default, TAR performs an automatic backup each morning at 2:00 a.m. Automatic backup files display with the characters “auto_” and use the YYYYMMDD format. For example: **auto_20100116** displays for an automatic backup executed on January 16, 2010.



NOTE: *In the event that TAR should fail, please contact M86 Technical Support to restore TAR with the most recent backup.*

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

Execute a Backup on Demand

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

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

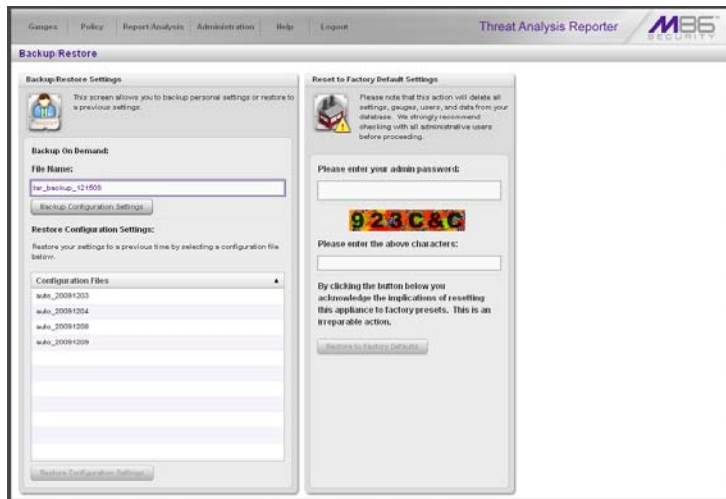



Fig. 4:4-2 Backup on demand

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

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

Restore User Settings

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

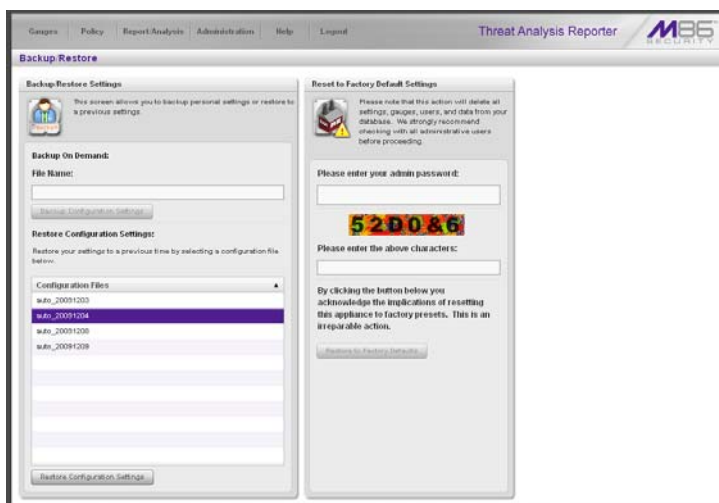


Fig. 4:4-3 Restore Personal Settings

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

Restore to Factory Default Settings

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



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

Reset to Factory Default Settings frame

1. In the Reset to Factory Default Settings panel, **Please enter your admin password** that was created during the TAR wizard hardware installation process.
2. Beneath the security characters, **Please enter the above characters:**

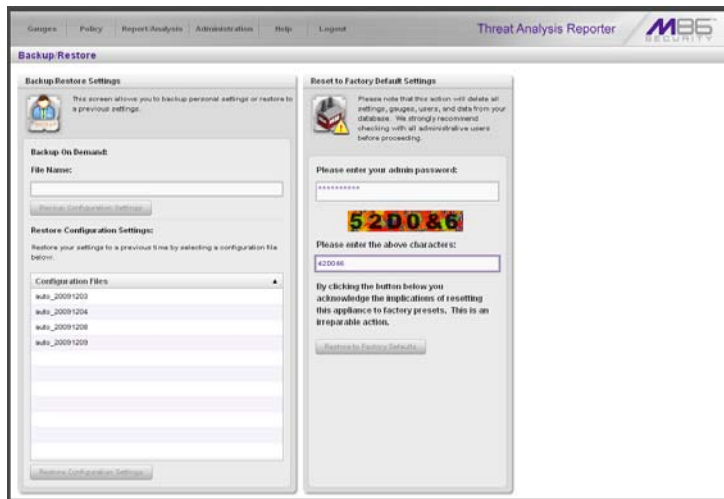


Fig. 4:4-4 Reset to Factory Default Settings frame

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



Fig. 4:4-5 End User License Agreement

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



Fig. 4:4-6 Wizard Login window

Wizard Login window

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

Threat Analysis Reporter M86 SECURITY

All fields are required except for ER. A "Source" Web Filter and at least one bandwidth range is required.

Main Administrator
Register the first administrator for the TAR box. Please make sure you use only alpha-numeric characters.

Username: _____ Email: _____
Password: _____ Confirm Password: _____

Bandwidth Range
The following IP ranges will be used to monitor the network traffic in your organization.

IP Address: _____ Subnet Mask: _____
Add

| IP Address | Subnet Mask |
|------------|-------------|
| | |
| | |
| | |
| | |

Remove

Web Filter Setup
These settings are used for communication with TAR agent to retrieve the data logs from Web Filter.

Server Name: _____ Server IP: _____
Set as Source Add

| Source | Server Name | Server IP |
|--------|-------------|-----------|
| | | |
| | | |
| | | |

Set as Source Remove

Do you have an Enterprise Reporter?
Yes No

Server Name: _____ Server IP: _____
Local Enterprise Reporter: _____ 127.0.0.1

Click "Save" to finish setting up your TAR >>> Save


Fig. 4:4-7 Wizard screen

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




WARNING: When resetting TAR to factory default settings, a new username and password must be created due to the single sign-on feature that lets the global administrator access all applications on the SR device from the TAR application. **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. In the Web Filter Setup section, type in the **Server Name** and **Server IP** address, indicate if this Web Filter will be **Set as Source**, and then click **Add** to include the server criteria in the list box below.

 **TIPS:** To add another Web Filter, follow the instructions in step 6 above. To remove a Web Filter from the list box, select it and then click **Remove**. To make a Web Filter the Source server—if no Web Filter in the list has yet been specified as the Source server, or if the IP address of the Source server has changed—select the Web Filter from the list box and then click **Set as Source**.

7. By default, the Enterprise Reporter section should be populated and greyed-out.

Click **Save** to save your entries and to go to the TAR login window:



The screenshot shows a login window for 'Threat Analysis Reporter' by M86 SECURITY. The window has a light gray background and a dark border. At the top left, the text 'Threat Analysis Reporter' is displayed in a purple font. To the right of this text is the M86 SECURITY logo, which consists of the letters 'M86' in a large, bold, purple font with 'SECURITY' in a smaller, black font underneath. Below the header, there are two input fields: 'Username' and 'Password'. Each field has a small arrow icon on the right side, indicating a dropdown menu. Below the input fields is a 'Login' button with a light gray background and a dark border.

Fig. 4:4-8 TAR Login window

TAR APPENDICES SECTION

Appendix A

System Tray Alerts: Setup, Usage

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

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



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

LDAP server configuration

Create the System Tray logon script

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

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

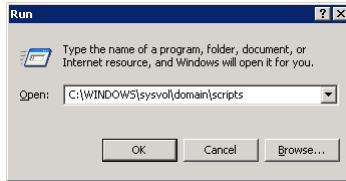


Fig. A-1 Run dialog box

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:

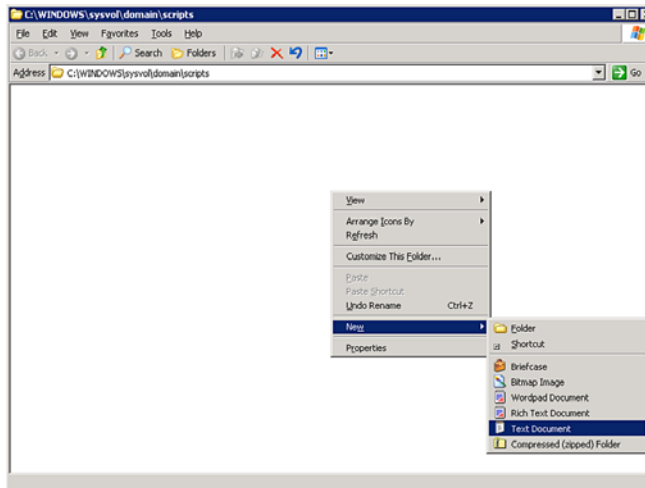


Fig. A-2 C:\WINDOWS\sysvol\domain\scripts window

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

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

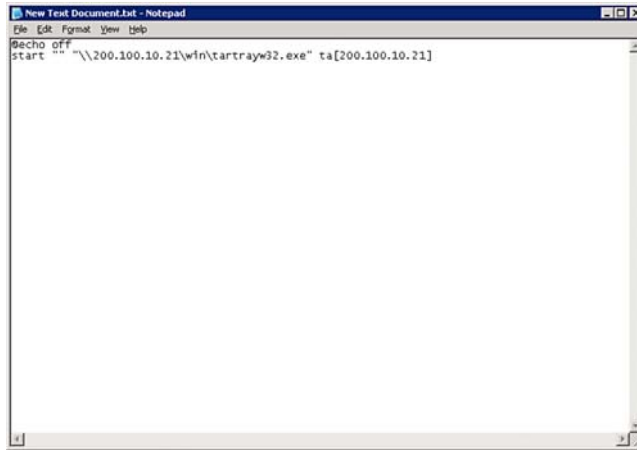


Fig. A-3 New Text Document

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

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

in which "X.X.X.X" represents the IP address of the TAR server, and "\\win\tartrayw32.exe" refers to the location of the TAR Alert executable file on the TAR server.

7. Go to: **File > Save As** to open the Save As window:

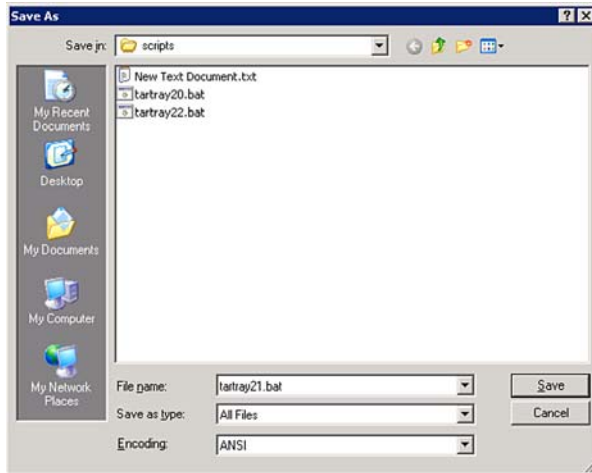


Fig. A-4 Save As dialog box

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:

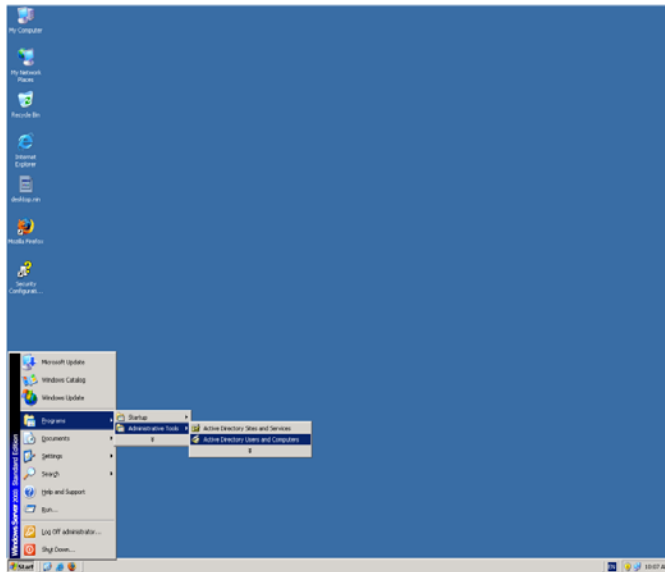


Fig. A-5 Programs > Administrative Tools > Active Directory Users

2. In the Active Directory Users and Computers folder, double-click the administrator's Name in the Users list to open the Properties dialog box for his/her profile:

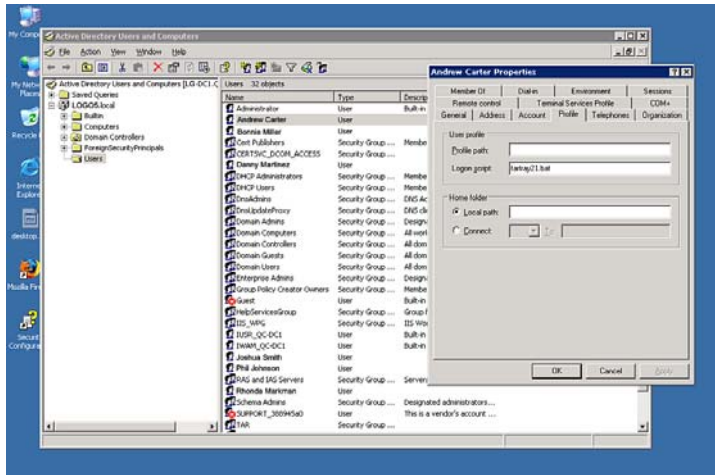



Fig. A-5 Properties dialog box, Active Directory Users folder

3. In the Properties dialog box, click the Profile tab to display its contents.
4. In the **Login script** field, type in the “.bat” filename. For example: **tartray21.bat**.
5. Click **Apply** to save your entry.
6. Click **OK** to close the dialog box.
7. Click the “X” in the upper right corner of the folder to close the window.

Administrator usage of System Tray

Once the System Tray logon script has been added to the administrator's profile, when the administrator logs on his/her workstation, the TAR Alert icon (pictured to the far left in the image below) automatically loads in his/her System Tray:



 **NOTE:** *The TAR Alert icon will not load in the System Tray if the TAR server is not actively running.*

Use the TAR Alert icon's menu

When right-clicking the TAR Alert icon, the following pop-up menu items display:

- Tar Admin Interface - clicking this menu selection launches a browser window containing the TAR Administrator Interface's login window.
- Reconnect - clicking this menu selection re-establishes the TAR Alert icon's connection to the TAR server, resetting the status of the TAR Alert icon to the standard setting.
- Exit - clicking this menu selection removes the TAR Alert icon from the System Tray.

Status of the TAR Alert icon

If there are no alerts for any gauges set up by the administrator, the following message displays when mousing over the standard TAR Alert icon: “Connected. No Alerts.”

However, if an alert is triggered, the TAR Alert icon changes in appearance from the standard gauge to a yellow gauge (pictured to the far left in the image below):



The following message appears briefly above the yellow gauge: “New M86 TAR Alert!” The following message displays whenever mousing over this icon: “New M86 TAR Alert”.

If more than one alert is triggered for the administrator, the message reads: “New M86 TAR Alert! (X Total)”, in which “X” represents the total number of new alerts. The following message displays whenever mousing over this icon: “X New M86 TAR Alerts”, in which “X” represents the total number of new alerts.

View System Tray alert messages

1. Double-click the TAR Alert notification icon to open the TAR Alert box:

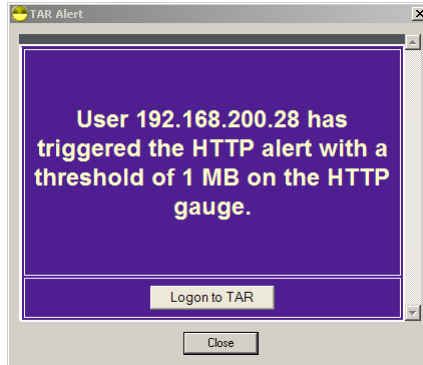


Fig. A-6 TAR Alert

This box contains the following message: “User (user-name/IP address) has triggered the (Alert Name) alert with a threshold of X (in which “X” represents the alert threshold) on the (URL dashboard gauge name) gauge.”

The Logon to TAR button displays beneath this message, followed by the Close button.

If more than one alert was triggered, the alert box includes the following message and button to the right of the Close button: “X more alerts” (in which “X” represents the number of additional alerts), and the Next >> button.

2. Click **Logon to TAR** to launch the TAR login window (see Fig. 1:1-1).

If there are additional alerts, click **Next >>** to view the next TAR Alert. Each time the Next >> button is clicked, the number of remaining alerts to be viewed decreases by one. The Next >> button no longer displays after the last alert is viewed.

3. Click **Close** to close the TAR Alert box.

Appendix B

Glossary

This glossary includes definitions for terminology used in this user guide.

base group - A user group consisting of end users whose network activities are monitored by the designated group administrator(s). Only the creator of the base group can modify the base group, delegate the base group to another group administrator, or delete the base group.

custom category - A unique library category on the Web Filter that includes URLs, URL keywords, and/or search engine keywords to be blocked. In TAR, global administrators can create and manage custom library categories and sync them to the source Web Filter.

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

global administrator - An authorized administrator of the network who maintains all aspects of TAR. The global administrator configures TAR, sets up user groups, administrator groups and group administrators, and performs routine maintenance on the server.

group administrator - An authorized administrator of TAR who maintains user group, administrator groups, group administrator profiles, and gauges.

HTTP - Hyper Text Transfer Protocol is used for transferring files via the World Wide Web or an intranet.

instant messaging - IM involves direct connections between workstations either locally or across the Internet.

library category - A list of URLs, URL keywords, and search engine keywords set up to be blocked.

LDAP - One of two authentication method protocols that can be used with TAR. Lightweight Directory Access Protocol (LDAP) is a directory service protocol based on entries (Distinguished Names). The other authentication method that can be used with TAR is IP groups.

peer-to-peer - P2P involves communication between computing devices—desktops, servers, and other smart devices—that are linked directly to each other.

protocol - A type of format for transmitting data between two devices. LDAP 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.

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 TAR.

TCP - An abbreviation for Transmission Control Protocol, one of the core protocols of the Internet protocol suite. Using TCP, applications on networked hosts can create connections to one another, over which streams of data can be exchanged.

Traveler - M86 Security's executable program that downloads updates to the SR 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").

SR TECHNICAL SUPPORT / PRODUCT WARRANTIES

Technical Support

For technical support, visit M86 Security's Technical Support Web page at <http://www.m86security.com/support/>, or contact us by phone, by email, or in writing.

Hours

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

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

Contact Information

Domestic (United States)

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

International

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

E-Mail

For non-emergency assistance, email us at [**support@m86security.com**](mailto:support@m86security.com)

Office Locations and Phone Numbers

M86 Corporate Headquarters (USA)

828 West Taft Avenue
Orange, CA 92865-4232
USA

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

M86 Taiwan

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

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

Support Procedures

When you contact our technical support department:

- You will be greeted by a technical professional who will request the details of the problem and attempt to resolve the issue directly.
- If your issue needs to be escalated, you will be given a ticket number for reference, and a senior-level technician will contact you to resolve the issue.
- If your issue requires immediate attention, such as your network traffic being affected or all blocked sites being passed, you will be contacted by a senior-level technician within one hour.
- Your trouble ticket will not be closed until your permission is confirmed.

Product Warranties

Standard Warranty

M86 Security warrants the medium on which the M86 product is provided to be free from defects in material and workmanship under normal use for period of one year (the “Warranty Period”) from the date of delivery. This standard Warranty Period applies to both new and refurbished equipment for a period of one year from the delivery date. M86 Security’s entire liability and customer’s exclusive remedy if the medium is defective shall be the replacement of the hardware equipment or software provided by M86 Security.

M86 Security warrants that the M86 product(s) do(es) not infringe on any third party copyrights or patents. This warranty shall not apply to the extent that infringement is based on any misuse or modification of the hardware equipment or software provided. This warranty does not apply if the infringement is based in whole or in part on the customer’s modification of the hardware equipment or software.

M86 Security specifically disclaims all express warranties except those made herein and all implied warranties; including without limitation, the implied warranties of merchantability and fitness for a particular purpose. Without limitation, M86 Security specifically disclaims any warranty related to the performance(s) of the M86 product(s). Warranty service will be performed during M86 Security’s regular business hours at M86 Security’s facility.

Technical Support and Service

M86 Security will provide initial installation support and technical support for up to 90 days following installation. M86 Security provides after-hour emergency support to M86 server customers. An after hours technician can be reached by voice line.

Technical support information:

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

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

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

E-mail: support@m86security.com

Have the following information ready before calling technical support:

Product Description: _____

Purchase Date: _____

Extended warranty purchased: _____

Plan # _____

Reseller or Distributor contact: _____

Customer contact: _____

Extended Warranty (optional)

The extended warranty applies to hardware and software of the product(s) except any misuse or modification of the product(s), or product(s) located outside of the United States. The extended warranty does not include new product upgrades. Hardware parts will be furnished as necessary to maintain the proper operational condition of the product(s). If parts are discontinued from production during the Warranty Period, immediate replacement product(s) or hardware parts will be available for exchange with defective parts from M86 Security's local reseller or distributor.

Extended Technical Support and Service

Extended technical support is available to customers under a Technical Support Agreement. Contact M86 Security during normal business hours, 8 a.m. to 5 p.m. PST, at (888) 786-7999, or if outside the United States, call 1+(714) 282-6111.

SR 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:

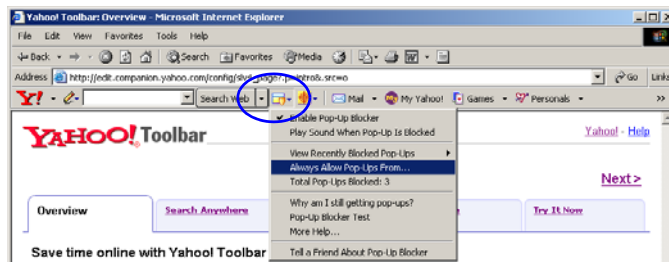


Fig. I-1 Select menu option Always Allow Pop-Ups From

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

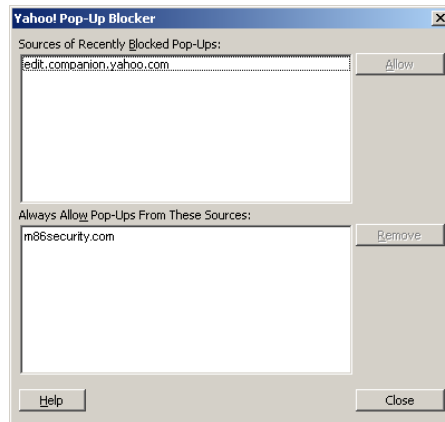


Fig. I-2 Allow pop-ups from source

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:

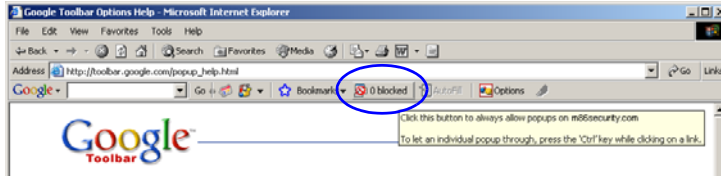


Fig. I-3 Pop-up blocker button enabled

Clicking this icon toggles to the Pop-ups okay button, adding the Client to your white list:

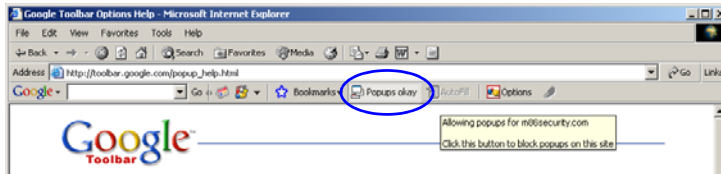


Fig. I-4 Pop-ups okay button enabled

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:

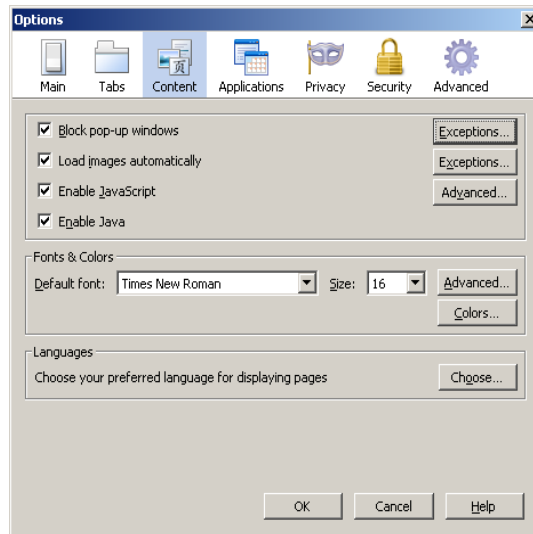


Fig. I-5 Mozilla Firefox Pop-up Windows Options

3. With the “Block pop-up windows” checkbox checked, click the **Exceptions...** button at right to open the Allowed Sites - Pop-ups box:

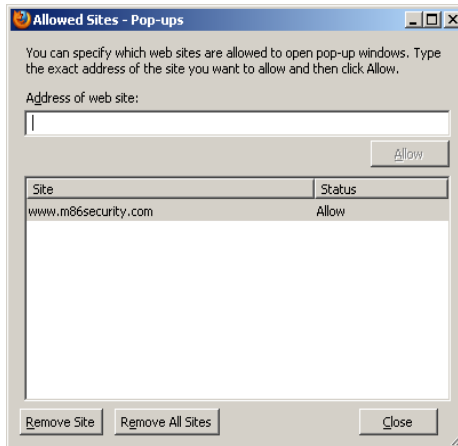


Fig. I-6 Mozilla Firefox Pop-up Window Exceptions

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:

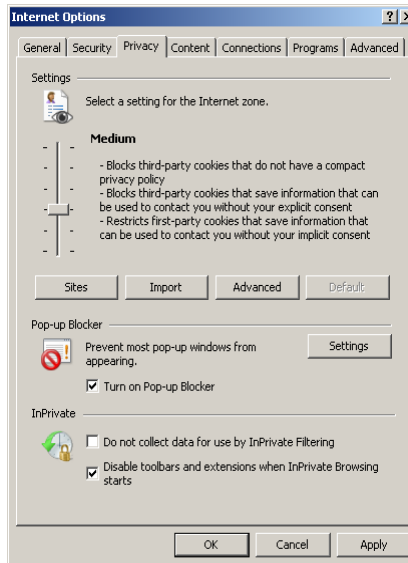


Fig. I-7 Enable pop-up blocking

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**:

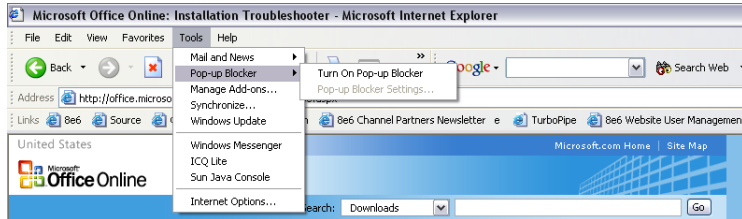


Fig. I-8 Toolbar setup

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:

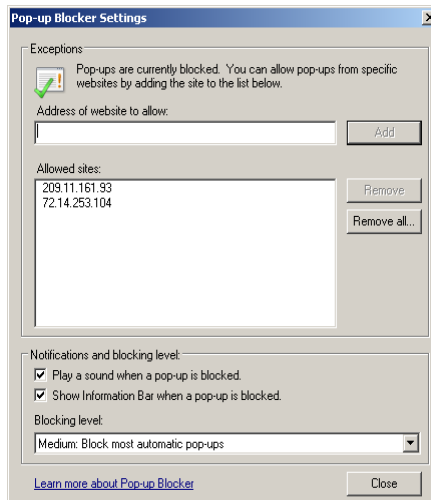


Fig. I-9 Pop-up Blocker Settings

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:

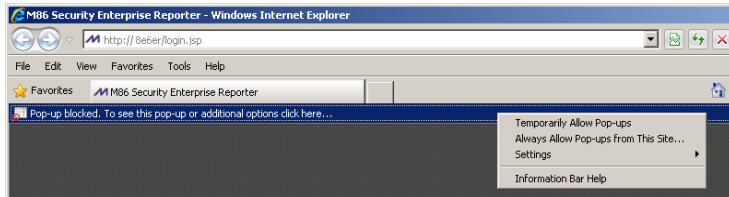


Fig. I-10 Information Bar menu options

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

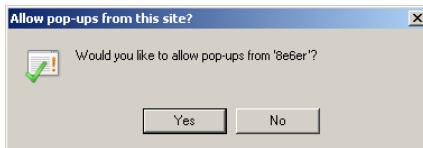



Fig. I-11 Allow pop-ups dialog box

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

The chassis of each model consists of the following components:

| 300 Series Model | 500 Series Models | 700 Series Models |
|-------------------------|--------------------------|--------------------------|
| 2 hard drives | 4 hard drives | 4 hard drives |
| 1 power supply | 1 power supply | 2 power supplies |
| 1 cooling fan | 3 cooling fans | 4 cooling fans |

Part 2: Server Interface

Front Control Panel on a 300 Series Unit

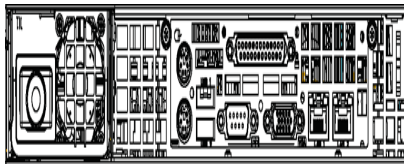
The keypad on the front of the server is used for performing basic server functions.



- **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 panels on 500 and 700 series units

Control panel buttons, icons, and LED indicators display on the right side of the 500 and 700 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 chassis front panel



700 series chassis front panel

The buttons and LED indicators for the depicted icons function as follows:



UID (button) and **U** icon – On a 700 series unit, when the UID button is pressed, a steady blue LED displays on both the front and rear of the chassis. These indicators are used for easy location of the chassis in a large stack configuration. The LED remains on until the button is pressed a second time.



Overheat/Fan Fail (icon) – This LED is unlit unless the chassis is overheated. A flashing red LED indicates a fan failure. A steady red LED (on and not flashing) indicates an overheating condition, which may be caused by cables obstructing the airflow in the system or the ambient room temperature being too warm.



NIC2 (icon) – A flashing green LED indicates network activity on LAN2. On a 500 series unit, 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 on LAN1. On a 500 series unit, 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.

Rear panel on the 700 series unit

Power Supplies (LED indicators) – The power supplies are located at the right on the rear of the chassis. An LED indicator is located above each of the power plugs. (See Power supply failure in the Troubleshooting sub-section for information on detecting a power supply failure and resolving this problem.)

UID (LED indicator) – On the rear of the 700 series chassis, to the right of the LAN ports, a steady blue UID LED indicator displays when the UID button on the control panel is pressed. This LED remains lit until the UID button is pressed again.



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, HD 2, HD 3, or HD 4). Upon receiving this alert, the administrator should verify the status of the drives by first going to the Hardware Failure Detection window in the Administrator console.



WARNING: Do not attempt to remove any of the drives from the unit at this time. Verification of the failed drive should first be made in the Administrator console before proceeding, as data on the server will be lost in the event that the wrong drive is removed from the unit.

Step 2: Verify the failed drive in the Admin console

The Hardware Failure Detection window in the ER Administrator console is accessible via the **Server > Hardware Failure Detection** menu selection:

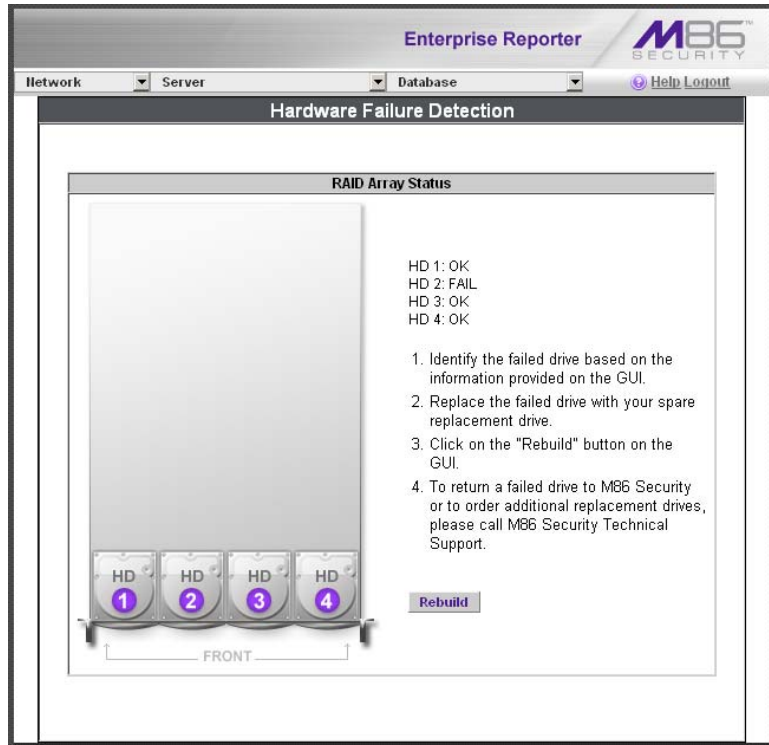


Fig. II-1 Hardware Failure Detection window

The Hardware Failure Detection window displays the current RAID Array Status for all the hard drives (HD) at the right side of the window.

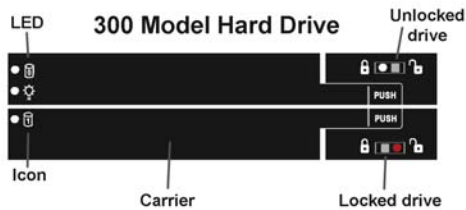
Normally, when both hard drives are functioning without failure, the text "OK" displays to the right of the hard drive number, and no other text displays in the window.

However, if a hard drive has failed, the message "FAIL" displays to the right of the hard drive number.

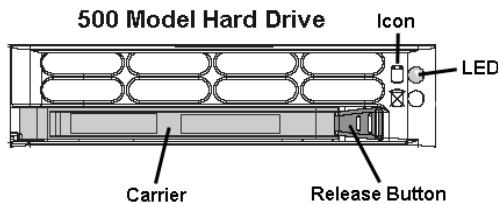
Before taking any action in this window, proceed to Step 3.

Step 3: Replace the failed hard drive

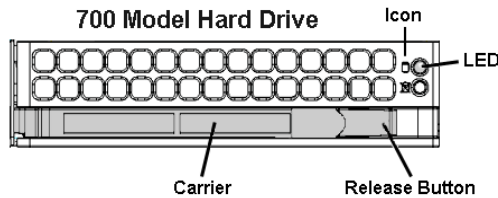
After verifying the failed hard drive in the Administrator console, go to the server to replace the drive.



300 series model hard drive carrier



500 series model hard drive carrier



700 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 or 700 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 and 700 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 or 700 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.

If you have a 700 series model and wish to replace this hot swappable power supply unit yourself, proceed to Step 3.

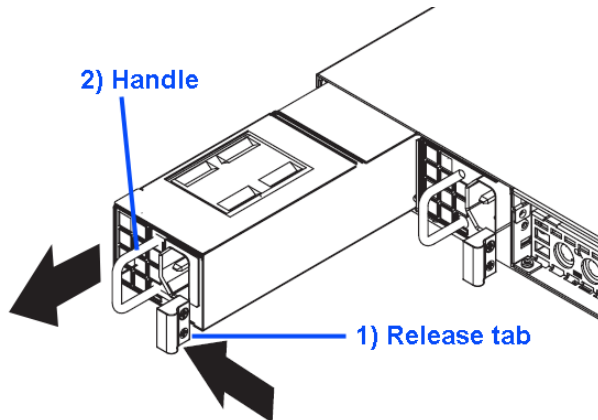
 **WARNING:** Be sure the correct failed power supply has been identified. Removing the wrong power supply will cause the system to crash.

Step 3: Unplug the power cord

To prevent electrical shock to yourself and damage to the unit, unplug the power cord from the failed 700 series power supply module. Proceed to Step 4.

Step 4: Replace a failed hot swap power supply

Remove the failed 700 series power supply by locating the red release tab and pushing it to the left (1), then pulling the curved metal handle on the power supply module towards you (2).



700 series model power supply module

Note that an audible alarm sounds and the LED is unlit when the power supply module is disengaged. Replace the failed power supply with your spare replacement power supply module. The alarm will turn off and the LED will be a steady green when the replacement power supply module is securely locked in place.

Fan failure

Identify a fan failure

A flashing red LED on a 500 or 700 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 or 700 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

Symbols

Records *91, 94*

A

Access Client *69*
accordion, terminology *181*
add/edit/delete administrators in ER Administrator console *21*
Add/Edit/Delete Administrators screen *27*
administrator
 log in to ER Server application *21*
Administrator console in ER *23*
alert box, terminology *13, 3, 181*
alert log in TAR *263*
alert messages in TAR *253*
Amount shown *94*
archive
 data setup on Server *89*
 terminology *90*
arrow, terminology *3*

B

Back button *71*
back up data
 to remote server *49*
back up ER data
 internal on demand backup *48*
backup *301*
 procedures *46*
Backup screen *45*
bandwidth
 gauge *220*
base group
 definition *318*
base group in TAR *196, 232*
Block Request Count *98*
Blocked Request Report *145*

- Blocked Searched Keywords 98
- Box Mode screen 24
- Break type 93
- button, terminology 13, 3, 181
- byte score in TAR 222

C

- category group
 - add additional groups in ER Web Client 26
 - how to add in ER Web Client 24
- charts
 - hits per day, week, month 52
- checkbox, terminology 13, 3, 181
- Client
 - ER Server Statistics 50
- components 4
- Conventions 3
- Copy a Custom Report 154
- count columns 73
- Ctrl key 190
- custom category
 - definition in TAR 318
- custom search in TAR 279

D

- data storage setup 89
- Data to export field 93
- Database Menu 73
- database status logs 85
- Date Scope 89
 - ER Server Statistics 51
 - Expiration screen 89
 - Username or Keyword entries 119
- Default Options 56
- Default Top Value in Web Client 56
- delete a gauge 236
- detail report
 - generate report view 69
- Detailed Info 96

- device registry in TAR 291
- diagnostic reports 85
- Diagnostics 39
- dialog box, terminology 13, 4, 181
- disable a gauge 236
- disable pop-up blockers 327
- Display and # Records fields 91
- double-break report 93, 94
- double-break report, definition 178
- Draw Chart button 52

E

- Edit User button
 - change passwords in Web Client 42
- Email Report 96
- End User License Agreement 305
- ER
 - restore data from backup 50
 - restore data from previous backup 50
- ER Activity, hits on Server 52
- ER Server
 - restart 66
 - shut down 66
- ER Web Client
 - change settings 20, 47
 - how to use 15
 - log in 10
 - log out 15
 - re-login 16
- escape characters, use of 80
- evaluation mode 173
- Event Schedules 156
- Executive Internet Usage Summary 162
- expand or contract a column in TAR 189
- expiration 91
- Expiration Info 55
- Expiration screen 89
- expire
 - data from Server 89
 - passwords 100

- terminology *91*
- Export Custom Report *85*
- Export Drill Down Report *84*
- export reports *76*
- Exporting a Report *98*

F

- field, terminology *14, 4, 182*
- File Transfer Protocol (FTP) *48, 66*
- filter columns and buttons *72*
- Filter String field *91*
- Firefox *5, 18, 46*
- For double-break reports only *94*
- For E-Mail output only *96*
- For pie and bar charts only *95*
- Format *93*
- frame, terminology *14, 4, 182*
- FTP
 - definition *318*
- FTP (File Transfer Protocol) *48, 49, 50, 66*
- FTP bandwidth gauge *223*

G

- gauge
 - restore configuration settings *301*
- generate
 - Blocked Request Report *146*
 - drill down report *110*
 - ER activity charts *52*
 - Single User Group Report *111*
 - static table of IP addresses, machine names *76*
 - Wall Clock Time report *139*
- Generate using *95*
- global administrator *180*
 - definition in TAR *318*
- group administrator *180*
 - definition in TAR *318*

H

- hardware 4
- Hardware Failure Detection screen 70
- hide a gauge 236
- Hide Un-Identified IPs 57, 95, 164
- hit count, definition 178
- hit, definition 52
- How to
 - access Saved Custom Reports 149
 - access the Add/Edit Gauges panel 227
 - add a category group in the Web Client 23
 - add a new alert 255
 - add a new gauge 229
 - add a user group in the Web Client 28
 - create a detail Object Count report from a summary report 74
 - create a detail Page Count report from a summary report 74
 - create a New Report from the current report view 81
 - display only a specified number of records 91
 - drill down into a gauge 242
 - edit a saved report 151
 - email a report 98
 - export a detail Custom Report 85
 - export a summary Drill Down Report 84
 - generate a custom Web Client report 114
 - generate a Drill Down Report 110
 - generate a Single User Group Report 111
 - generate an Executive Report 60
 - modify a Drill Down Report 83
 - navigate the TAR user interface 188
 - save a custom report 86
 - schedule a report to run 159
 - set up email alert notifications in TAR 256
 - use filter columns and buttons 72
 - view an email alert in TAR 257
 - view and print a Web Client report 101
 - view end user gauge activity 240
 - view URLs a user visited in TAR 240
- HTTP
 - definition 318
- HTTP bandwidth gauge 223
- HTTPS 5, 17

login 8, 19, 9, 186

I

- icon, terminology 4
- IM bandwidth gauge 224
- install
 - software update 60
- Installation Guide 7
- instant messaging
 - definition 318
- Internet Explorer 5, 18, 46, 177
- IP group
 - authentication method 309
- IP.ID 73
- IPGROUP
 - member type in TAR 195

J

- JavaScript 5

L

- LDAP 103, 31, 35, 36, 309
 - definition in TAR 319
 - server types supported in TAR 193
 - user authentication in TAR 195
- library categories
 - definition 318
- Linux OS 4
- list box, terminology 14, 4, 182
- live
 - data setup on Server 89
 - terminology 90
- Locked-out Accounts and IPs screen 30
- lockout 101
 - automatic lockout in TAR 258
 - end user workstation in TAR 250
 - function in TAR 256
 - list management in TAR 265
 - manual lockout in TAR 249

- unlock workstations in TAR 267
- lockout in TAR 214, 253
- log
 - database status 86
 - into TAR 186
 - off the ER Server application 22
 - on the ER Server 19
 - out of ER Web Client 15
 - out of TAR 188
- Lotus Notes
 - configuration 176

M

- M86 Security Reporter 7
- Macintosh 5, 18, 46
- mail server 98
- Manual Backup button 48
- Modify Report 83
- mouse
 - use to view truncated report data 79
- My Account
 - change password 48
- My Account option 48
- MySQL 4, 11, 67, 1

N

- NAS 4
- navigation toolbar in TAR 188
- Network Diagnostics screen 39
- Network Menu 23
- network requirements 5
- Network Settings screen 32
- Network Time Protocol (NTP) 37
- New Drill Down Report 81
- NT domain query 80
- NTP (Network Time Protocol) 37

O

- Object Count 99

- object count, definition 178
- Optional Features screen 96
- Order field 92
- Outlook Express 176
- Output type 95

P

- P2P
 - definition 319
- P2P bandwidth gauge 224
- Page Count 99
- page count, definition 178
- Page Definition screen 83
- Page links 77
- Page View Elapsed Time screen 81
- Page/Object Warning Limit in Web Client 56
- panel, terminology 182
- password
 - create for ER Administrator console 21
 - create for remote server's FTP account 48
 - create for Web Client user 38
 - expiration in ER Web Client 11
 - security option 100
- peer-to-peer
 - definition 319
- Ping 40
- pop-up blocking, disable 327
- pop-up box/window, terminology 14, 5, 183
- Print report 101
- Product Warranties section 324
- protocol
 - bandwidth gauge 220
 - definition 319
- Proxy Setting 65
- pull-down menu, terminology 14, 5, 183

R

- radio button, terminology 15, 5, 183
- RAID 70

- rearrange the gauge display 236
- Record navigation field in ER Web Client 22, 44, 71, 157
- records
 - exportation 76
 - sort by another column 75, 79
- recovery procedures in TAR 302
- Regional Setting screen 36
- re-login to ER Web Client 16
- remote server backup 49
- report
 - count columns 73
 - Date Scope field 89
 - delete a custom report 155
 - detail 69
 - double-break 93
 - edit a custom report 151
 - edit a custom report, add a Username 153
 - enter search terms 91
 - ER Activity 52
 - export 76
 - filters 72
 - page numbers 77
 - records 71
 - run a custom report 154
 - sample file formats 102
 - sample, Comma-Delimited Text 107
 - sample, Excel (English) 108
 - sample, HTML 106
 - sample, MS-DOS Text 103
 - sample, PDF 104
 - sample, Rich Text Format 105
 - scheduling a report to run 161
 - select record and columns to display 91
 - summary 68
 - view info on a saved custom report 150
- reports
 - diagnostic 86
- resize button, terminology 183
- restart the Server 66
- Result Set Limit 92
- Routing Table screen 34

- rules
 - elapsed time 82
 - expiration 91

S

- Safari 5, 18, 46
- Save Report 86
- screen, terminology 15, 5, 183
- search
 - NT domain with special characters 80
- search engine
 - definition 319
- Search field 91
- Search String Reporting 98
- Secure Access screen 57
- Self Monitoring screen 51
- Server
 - add, maintain routers 34
 - download software update 59
 - perform manual backup 48
 - set time 36
 - set up IP addresses 32
 - view statistics using Client 50
- Server Info for ER Server module 51
- Server Menu 45
- Server Status screen 55
- Set Result Limit 82
- Shift key 190
- Shut Down screen 66
- shutdown
 - SR server 22, 15, 189
- Single Sign-On 10, 307
- slider, terminology 184
- SMTP
 - definition 319
- SMTP bandwidth gauge 223
- SMTP Server Setting screen 53
- SNMP screen 43
- software 4
 - unapply 60

- Software Update screen 59
- Software Update Setting screen 64
- Sort by field 92
- sort records 75, 79
- sort records in TAR 190
- spam filter 98
- Specific Search 125, 144
- SSL Certificate 292
- summary report
 - generate report view 68
- synchronization
 - definition in TAR 319
 - Master User List update in TAR 284
 - update device registry in TAR 291
- system requirements 5
- System Tray 309

T

- tab, terminology 184
- table, terminology 15
- TAR Wizard 10
- TCP
 - definition 319
- TCP port in TAR 223
- technical support 57, 321
- terminate a process in ER Web Client 44
- Terminology 13, 3
- text box, terminology 15, 5, 184
- thumbnail, terminology 6
- time count, definition 178
- timed out session 16
- timespan 230
- timespan for gauges in TAR 235
- Tools screen 85
- tooltip information 190
- Trace Route 41
- Traveler
 - definition in TAR 319
- Type field
 - New Summary Report 88

U

- UDP
 - definition 319
- UDP port in TAR 223
- UID 339
- update
 - category group in ER Web Client 24
 - NTP server settings 37
 - routing table 35
 - scheduled event 158
 - server software 59
 - user group in ER Web Client 35
- update Web Client
 - user group, add/remove sub-admin 41
- UPS 5
- URL, definition 320
- user group
 - how to add 35
- User Group Import screen 103
- User Name Identification screen 73
- User Permissions
 - how to add a group to a sub-admin in the Web Client 40
- User Permissions button
 - change passwords in Web Client 42
- User Permissions menu option in ER Web Client 10
- Username Display Setting screen 78
- usernames and passwords 10

V

- view
 - diagnostic reports 86
 - ER Activity charts 52
 - record data truncated in a column 79
- View report 101

W

- Wall Clock Time 99
- Wall Clock Time count, definition 178
- Wall Clock Time Report 139

- Web access logging device 17, 21
- Web Client Server Management screen 68
- Web Client Server Startup Time 51
- Web Filter 1, 103, 1, 31, 35, 36
 - end user lockout in TAR 258
- window, terminology 16, 6, 184
- Windows 7 5
- Windows Vista 5
- Windows XP 5
- wizard 8
 - installation procedures 186, 212, 216, 283, 296
 - installation process 291
- workstation requirements 5

