EventTracker Enterprise
User Guide
Version 7.4
Copyright
All intellectual property rights in this work belong to Prism Microsystems, Inc. The information contained in this work must not be reproduced or distributed to others in any form or by any means, electronic or mechanical, for any purpose, without the prior permission of Prism Microsystems, Inc., or used except as expressly authorized in writing by Prism Microsystems, Inc.
Copyright © 1999 - 2013 Prism Microsystems, Inc. All Rights Reserved.

Trademarks
All company, brand and product names are referenced for identification purposes only and may be trademarks or registered trademarks that are the sole property of their respective owners.

Disclaimer
Prism Microsystems, Inc. reserves the right to make changes to this manual and the equipment described herein without notice. Prism Microsystems, Inc. has made all reasonable efforts to ensure that the information in this manual is accurate and complete. However, Prism Microsystems, Inc. shall not be liable for any technical or editorial errors or omissions made herein or for incidental, special, or consequential damage of whatsoever nature resulting from the furnishing of this manual, or operation and performance of equipment in connection with this manual.
# Table of Contents

- About this Guide ..................................................................................................................................... 20
- Who should read this guide ............................................................................................................. 20
- Typographical Conventions .............................................................................................................. 20
- Document Revision Control .................................................................................................................. 23
- How to Get In Touch .............................................................................................................................. 24
- Documentation Support ................................................................................................................... 24
- Customer Support ............................................................................................................................. 24
- Related Documents ............................................................................................................................... 24

## Chapter 1 Getting Started ........................................................... 25
- About EventTracker ............................................................................................................................... 26
- EventTracker Services and Ports ......................................................................................................... 27
- Start EventTracker ................................................................................................................................ 29
  - To start EventTracker ........................................................................................................................ 29
- EventTracker Control Panel .................................................................................................................. 38
  - Admin Menu .......................................................................................................................................... 40
  - Tools Menu ............................................................................................................................................. 41
  - Incorporate Your Company Logo .......................................................................................................... 42
    - To incorporate your Company Logo ..................................................................................................... 42
  - Application and Chart Theme ............................................................................................................... 42
- Update EventTracker Users List .......................................................................................................... 43
  - To update Users List ........................................................................................................................... 43
- Exit EventTracker ................................................................................................................................... 45

## Chapter 2 Analyze Incidents ..................................................................................................................... 47
- Incidents Dashboard ............................................................................................................................. 48
  - To analyze incidents dashboard ......................................................................................................... 48
- Graphical View ....................................................................................................................................... 49
- Tabular View .......................................................................................................................................... 50
- Tune Alerts Configuration .................................................................................................................... 54
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Tune Alerts</td>
<td>54</td>
</tr>
<tr>
<td>All Incidents</td>
<td>54</td>
</tr>
<tr>
<td>Log Search</td>
<td>55</td>
</tr>
<tr>
<td>Knowledge Base</td>
<td>56</td>
</tr>
<tr>
<td>Search Incidents</td>
<td>56</td>
</tr>
<tr>
<td>Web Slices</td>
<td>60</td>
</tr>
<tr>
<td>Add Web Slices to the Favorites Bar</td>
<td>60</td>
</tr>
<tr>
<td>Chapter 3 StatusTracker</td>
<td>62</td>
</tr>
<tr>
<td>About StatusTracker</td>
<td>63</td>
</tr>
<tr>
<td>Get Started with StatusTracker</td>
<td>63</td>
</tr>
<tr>
<td>Create User Defined Group</td>
<td>66</td>
</tr>
<tr>
<td>To add group</td>
<td>66</td>
</tr>
<tr>
<td>To add systems in a group</td>
<td>67</td>
</tr>
<tr>
<td>To add application(s) for monitoring</td>
<td>71</td>
</tr>
<tr>
<td>To add application(s) to a system</td>
<td>71</td>
</tr>
<tr>
<td>To add application(s) to more than one system</td>
<td>72</td>
</tr>
<tr>
<td>Select an application</td>
<td>73</td>
</tr>
<tr>
<td>New application option</td>
<td>75</td>
</tr>
<tr>
<td>Detect application option</td>
<td>76</td>
</tr>
<tr>
<td>Edit Application</td>
<td>77</td>
</tr>
<tr>
<td>To edit default applications</td>
<td>77</td>
</tr>
<tr>
<td>View Request Status</td>
<td>79</td>
</tr>
<tr>
<td>Delete Group</td>
<td>80</td>
</tr>
<tr>
<td>Rename Group</td>
<td>80</td>
</tr>
<tr>
<td>Remove Monitoring</td>
<td>81</td>
</tr>
<tr>
<td>To remove multiple systems/websites from monitoring</td>
<td>81</td>
</tr>
<tr>
<td>To remove a system/website from monitoring</td>
<td>82</td>
</tr>
<tr>
<td>Change Status</td>
<td>83</td>
</tr>
<tr>
<td>To change the System/Application status to Maintenance</td>
<td>83</td>
</tr>
<tr>
<td>To change maintenance status</td>
<td>84</td>
</tr>
<tr>
<td>Change multiple systems status to Maintenance</td>
<td>85</td>
</tr>
</tbody>
</table>
To generate Scheduled Reports ......................................................................................................... 153
To generate defined reports ............................................................................................................... 156
Enterprise Feeds ................................................................................................................................. 161
Reports Wizard .................................................................................................................................... 162
Reports Exceptions ............................................................................................................................. 162
Refine & Filter Options ....................................................................................................................... 163
Report Calendar ................................................................................................................................... 164
To access Report Calendar ............................................................................................................. 164
To view scheduled reports in time slot ......................................................................................... 165
To view scheduled reports on a particular day ............................................................................. 166
Report Status ....................................................................................................................................... 166
  On Demand/Queued Status ........................................................................................................... 168
Favorites .............................................................................................................................................. 168
Explorer ................................................................................................................................................ 171
  Perform search in EventVault Explorer ......................................................................................... 171
Flex History .......................................................................................................................................... 176
Analytics ............................................................................................................................................... 180
  Configure EventVault Explorer to use remote SQL Server .......................................................... 184
Chapter 9 My EventTracker Reports ...................................................................................................... 185
  My EventTracker Dashboard ............................................................................................................ 186
  My EventTracker Reports Dashboard/Configuration ...................................................................... 186
Chapter 10 Change Audit ........................................................................................................................ 187
  About Change Audit ........................................................................................................................ 188
  Change Audit Dashboard ............................................................................................................... 188
    To view Change Audit dashboard ................................................................................................ 188
Last Changes .......................................................................................................................................... 191
  View statistical data of Change Type/Object Type. ................................................................. 192
  View chart summary of Change Type/Object Type .................................................................. 193
Set Dashboard Preferences ................................................................................................................. 193
  Authorize the Unauthorized Changes ......................................................................................... 193
  View Access History ...................................................................................................................... 195
View Additional Information on Files ................................................................. 197
Enable OS Auditing on Folder(s) ........................................................................ 197
Policy Dashboard .................................................................................................. 203
  Customize the Policies Dashboard .................................................................... 204
EventTracker Inventory Manager .......................................................................... 208
Change Policies .................................................................................................... 208
  Analyze Policy Comparison Results ................................................................. 210
Schedule Change Assessment .............................................................................. 214
  To schedule Change Assessment ..................................................................... 214
  Edit Change Assessment Schedules ................................................................. 217
Run Schedules On Demand .................................................................................. 217
  To run the schedules on demand ...................................................................... 217
Delete Scheduled policies .................................................................................... 218
System Inventory .................................................................................................. 218
  To view application(s) and update(s) ................................................................. 218
Chapter 11 Config Assessment ............................................................................ 222
Schedule Config Assessment ............................................................................... 223
  To schedule Config Assessment .................................................................... 223
View Schedule Details and History ..................................................................... 228
  Edit Config Assessment Schedules ................................................................. 229
Run Schedules On Demand .................................................................................. 230
  To run the schedules On Demand .................................................................. 230
Search Published Reports ..................................................................................... 230
View Config Assessment Results ........................................................................ 231
  Export Assessment Details ............................................................................. 238
  Search Rules by CCE Id .................................................................................. 239
  To view CCE ID of a rule ............................................................................... 240
Delete Scheduled policies .................................................................................... 241
  To delete a scheduled policy ......................................................................... 241
Config Assessment Dashboard ............................................................................. 243
  Configure Config Assessment Dashboard ....................................................... 243
Chapter 12 Alerts ..................................................................................................................................... 247
Alerts .................................................................................................................................................... 248
Risk Metrics ......................................................................................................................................... 248
Add Custom Alerts .............................................................................................................................. 249
To Add Custom Alerts .................................................................................................................. 249
Add Pre-defined Categories as Alerts ............................................................................................... 258
To Add Pre-defined Categories as Alerts ........................................................................................ 258
Delete Alerts ........................................................................................................................................ 259
To delete Alerts ................................................................................................................................ 259
Configure Alert Actions – Manager Side ............................................................................................ 259
To configure alert actions ................................................................................................................ 259
Configure E-mail Alert Action .......................................................................................................... 260
Configure Audible Alert Action ......................................................................................................... 261
Configure Console Message Alert Action ...................................................................................... 261
Configure RSS Alert Notification .................................................................................................... 262
Forward Events as SNMP Traps ........................................................................................................ 263
Forward events as syslog messages ............................................................................................... 264
Execute Remedial Action at EventTracker Manager Console System ........................................ 265
Execute Remedial Action at EventTracker Windows Agent System ........................................... 266
Edit Alert Actions ............................................................................................................................. 267
Chapter 13 Behavior Rules .................................................................................................................... 269
Manage Behavior Rules ...................................................................................................................... 270
To set Behavior rules ....................................................................................................................... 270
Add Behavior Rules .......................................................................................................................... 271
To Add behavior Rule ...................................................................................................................... 271
To add custom behavior rule in Behavior Dashboard ..................................................................... 275
Chapter 14 Behavior Settings ............................................................................................................... 277
Enterprise Activity Behavior Settings ............................................................................................ 278
Chapter 15 Category ............................................................................................................................ 280
Manage Category Groups ................................................................................................................... 281
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Category Groups</td>
<td>281</td>
</tr>
<tr>
<td>Modify Category Groups</td>
<td>282</td>
</tr>
<tr>
<td>Delete Category Groups</td>
<td>283</td>
</tr>
<tr>
<td>Manage Categories</td>
<td>284</td>
</tr>
<tr>
<td>Create Categories</td>
<td>284</td>
</tr>
<tr>
<td>Modify Categories</td>
<td>287</td>
</tr>
<tr>
<td>Delete Categories</td>
<td>287</td>
</tr>
<tr>
<td>Delete Event Rules</td>
<td>288</td>
</tr>
<tr>
<td>Add Categories as Alerts</td>
<td>289</td>
</tr>
<tr>
<td>Move Category</td>
<td>289</td>
</tr>
<tr>
<td>Chapter 16 Collection Point and Collection Master</td>
<td>291</td>
</tr>
<tr>
<td>Collection Point model</td>
<td>292</td>
</tr>
<tr>
<td>Scalability</td>
<td>292</td>
</tr>
<tr>
<td>Real world scenarios</td>
<td>293</td>
</tr>
<tr>
<td>View Collection Point Configuration</td>
<td>295</td>
</tr>
<tr>
<td>Add Collection Masters</td>
<td>296</td>
</tr>
<tr>
<td>Edit Collection Master Settings</td>
<td>298</td>
</tr>
<tr>
<td>Delete Collection Master Settings</td>
<td>298</td>
</tr>
<tr>
<td>View and manage CAB Status</td>
<td>298</td>
</tr>
<tr>
<td>Resend CAB Files</td>
<td>299</td>
</tr>
<tr>
<td>Collection Master</td>
<td>300</td>
</tr>
<tr>
<td>View Collection Point Details</td>
<td>301</td>
</tr>
<tr>
<td>Configure Collection Master listening port</td>
<td>302</td>
</tr>
<tr>
<td>Delete CAB Files</td>
<td>302</td>
</tr>
<tr>
<td>Delete Collection Point Details</td>
<td>302</td>
</tr>
<tr>
<td>Chapter 17 Event Filters</td>
<td>303</td>
</tr>
<tr>
<td>Filter Events from View</td>
<td>304</td>
</tr>
<tr>
<td>Configure Event Filters</td>
<td>304</td>
</tr>
<tr>
<td>Configure Event Filters with Exception</td>
<td>306</td>
</tr>
<tr>
<td>Understand Filters and Filter Exceptions</td>
<td>307</td>
</tr>
<tr>
<td>View and Edit Alert Details</td>
<td>308</td>
</tr>
</tbody>
</table>
Chapter 18 EventVault ........................................................................................................................................... 309
  EventVault Manager ............................................................................................................................................ 310
    To start EventVault Manager .......................................................................................................................... 310
    Verify Archive File(s). ...................................................................................................................................... 312
    Export Archive File(s) ...................................................................................................................................... 313
    EventVault Manager Configuration.................................................................................................................. 313

Chapter 19 IP Lookup Configuration .................................................................................................................. 315
  IP lookup Configuration ..................................................................................................................................... 316
    To Add IP Lookup .......................................................................................................................................... 316

Chapter 20 Manager............................................................................................................................................... 317
  Configure - Alert Events ..................................................................................................................................... 318
    Enable Alert Notification................................................................................................................................ 318
    Purge Alert Events Cache ................................................................................................................................ 319
    Enable Remedial Actions .................................................................................................................................. 319
    Suppress Duplicate Alerts .................................................................................................................................. 319
    Enable alert e-mail footer option .................................................................................................................. 320
    Configure Correlation Receiver ...................................................................................................................... 320
    Configure Keyword Indexer .............................................................................................................................. 321
    Configure EventTracker Knowledge Base Web Site .................................................................................... 322
    Configure Logon Banner .................................................................................................................................. 323
    Configure Cost Savings .................................................................................................................................... 323
    Syslog / Virtual Collection Point .................................................................................................................... 323
    Monitor syslogs for UNIX................................................................................................................................. 324
    Virtual Collection Points .................................................................................................................................. 324
    Configure EventTracker Receiver to Listen on Multiple Ports .................................................................. 325
    Virtual Collection Points for syslogs .............................................................................................................. 326
    Configure EventTracker Receiver Ports ......................................................................................................... 326
    Forward Raw syslog Messages ......................................................................................................................... 327
    Virtual Collection Points for Windows Events .............................................................................................. 327
    Example Scenario ............................................................................................................................................. 327
    Computer: Sys1 – Configure Ports .................................................................................................................. 328
Upgrade Agent (Sys2) from Manager (Sys1) ................................................................................. 328
Upgrade Agent (Sys2) from Manager (Sys1) ................................................................................. 329
Direct Log Archiver / Netflow Receiver .......................................................................................... 329
  Configure Direct Log File Archiver .......................................................................................... 329
  Enable Netflow Receiver ......................................................................................................... 329
  Add Netflow Receiver Port ...................................................................................................... 330
Agent Settings .................................................................................................................................. 331
  Configure Agent File Transfer Settings .................................................................................. 331
Configure Config Assessment Settings .......................................................................................... 331
Configure E-mail Settings .......................................................................................................... 332
  Manage Email Accounts ......................................................................................................... 332
  To replace Email Id .................................................................................................................. 333
  To Remove Email ID ................................................................................................................ 335
Configure StatusTracker Settings .................................................................................................. 337
Chapter 21 Parsing Rules .............................................................................................................. 338
About Parsing Rule ...................................................................................................................... 339
  The Need for Adding Parsing Rule in Flex Report .................................................................. 339
  Usage of Tokens in EventTracker ......................................................................................... 339
Prior Knowledge .......................................................................................................................... 340
Components of Parsing Rules ..................................................................................................... 340
  Token ....................................................................................................................................... 340
  Parsing Rule Occurrences ....................................................................................................... 340
  Display Name .......................................................................................................................... 340
  Separator .................................................................................................................................. 341
  Terminator ............................................................................................................................... 341
View Parsing Rules ....................................................................................................................... 341
Add Token Value Groups ............................................................................................................. 342
  Add Rule ................................................................................................................................. 343
  Token Value Wizard ............................................................................................................... 344
Create a new template ................................................................................................................. 347
Generate a Flex Report ............................................................................................................... 351
Chapter 22 Reports Settings .................................................................................................................. 357
Configure Published Reports .................................................................................................................. 358
To configure published reports settings. .............................................................................................. 358
Configure Cost Saving Reports Settings .............................................................................................. 360
Chapter 23 RSS Feeds ............................................................................................................................. 361
RSS Feeds ............................................................................................................................................ 362
Add RSS Feeds ..................................................................................................................................... 362
Delete RSS Feeds .................................................................................................................................. 364
Chapter 24 Manage System Groups ...................................................................................................... 365
About Systems Manager ....................................................................................................................... 366
To start System Manager ...................................................................................................................... 366
Discover Modes ..................................................................................................................................... 367
Auto Discover Mode ............................................................................................................................. 367
Manual Mode ....................................................................................................................................... 368
Add Computers Manually ..................................................................................................................... 368
Add a Single Computer .......................................................................................................................... 368
Add a Group of Computers .................................................................................................................... 370
Adding a Group of Computers from an IP subnet ................................................................................ 371
Logical System Groups .......................................................................................................................... 372
Create a New Logical Group – System Type ....................................................................................... 372
Create a New Logical Group – IP Subnet ............................................................................................ 374
Create a New Logical Group – Manual Selection .............................................................................. 375
Modify a Group .................................................................................................................................... 376
Delete a Group ...................................................................................................................................... 378
View System Details ............................................................................................................................. 379
Restart Agent Service ........................................................................................................................... 379
Query Agent Service Status .................................................................................................................. 383
Query Agent Version ............................................................................................................................. 383
Manage Asset Value .............................................................................................................................. 384
To set asset value for multiple systems in a group .............................................................................. 384
Delete Systems ..................................................................................................................................... 386
View Logs ............................................................................................................................................. 419
Chapter 31 Sitemap ................................................................................................................................. 421
Sitemap ................................................................................................................................................ 422
To view Sitemap ................................................................................................................................ 422
Chapter 32 Windows ............................................................................................................................... 423
View Managed Windows System Status .......................................................................................... 424
To view Windows System Status ....................................................................................................... 425
Load Tabs Together ......................................................................................................................... 426
Chapter 33 Knowledge Base .................................................................................................................. 428
Knowledge Base .................................................................................................................................. 429
To access Knowledge Base ............................................................................................................. 429
Chapter 34 EventVault Warehouse Manager ....................................................................................... 430
EventVault Warehouse Manager ....................................................................................................... 431
Configuration ................................................................................................................................... 432
Save EventBox Metadata .................................................................................................................. 433
Back up EventVault Data ..................................................................................................................... 433
Extract EventBox Data ........................................................................................................................ 434
Move CAB files .................................................................................................................................... 435
Delete an EventBox ............................................................................................................................ 435
View CAB Files by Port Number ........................................................................................................ 436
Chapter 35 Diagnostics ........................................................................................................................... 438
EventTracker Diagnostic Tool ............................................................................................................. 439
To start EventTracker Diagnostic Tool ........................................................................................... 439
Set Debug Levels ............................................................................................................................. 440
Obfuscate Classified Information ...................................................................................................... 442
Diagnostic Alert ............................................................................................................................... 445
SQL Log ................................................................................................................................................. 446
Backup Configuration .......................................................................................................................... 446
Chapter 36 License Manager .................................................................................................................. 448
License Manager ................................................................................................................................. 449
Chapter 37 Export Import Utility ............................................................................................................ 455
Export and Import Utility .................................................................................................................... 456
Export Categories ............................................................................................................................ 456
Export Filters ................................................................................................................................. 457
Export Alerts ................................................................................................................................. 458
Export System Groups ..................................................................................................................... 459
Export RSS Feeds ............................................................................................................................ 460
Export Scheduled Reports .............................................................................................................. 461
Export Behavior Rules .................................................................................................................... 462
Export Token Value ......................................................................................................................... 463
Import Categories ............................................................................................................................ 464
Import Filters ................................................................................................................................... 465
Import Alerts ..................................................................................................................................... 465
Import System Groups ..................................................................................................................... 466
Import RSS Feeds ............................................................................................................................ 469
Import Scheduled Reports .............................................................................................................. 470
Import Behavior Rules .................................................................................................................... 471
Import SCAP Content ..................................................................................................................... 471
Import Token Value ......................................................................................................................... 472
Chapter 38 Append Archives .................................................................................................................. 474
Append CAB Files ........................................................................................................................... 475
Chapter 39 Agent Configuration ............................................................................................................ 479
Managers ............................................................................................................................................. 480
Event Filters ......................................................................................................................................... 481
To filter Events ................................................................................................................................. 481
Filter Events with Exception ........................................................................................................... 482
To filter events with exception ....................................................................................................... 482
Filter Events with Advanced Filters ............................................................................................... 485
Enable SID Translation .................................................................................................................... 486
System Monitor ................................................................................................................................... 487
To configure system performance threshold ................................................................................. 488
Add USB Device in the Exception List ............................................................................................. 490
To configure USB Exception List ..................................................................................................... 490
Monitor Applications ........................................................................................................................... 492
To monitor application install/uninstall .......................................................................................... 492
Filter Applications that need not be monitored ........................................................................... 493
Filter Applications that need to be monitored ............................................................................. 494
Monitor Services ............................................................................................................................. 495
Configure Service Restart List ........................................................................................................ 495
Filter Services .................................................................................................................................. 497
Logfile Monitor ................................................................................................................................ 498
View File Details .............................................................................................................................. 505
Delete Log File Monitoring Settings .............................................................................................. 505
Search Strings .................................................................................................................................. 505
Monitor Check Point Logs ............................................................................................................... 507
Monitor VMware Logs ..................................................................................................................... 510
Monitor Network Connections ....................................................................................................... 513
To monitor network connection .................................................................................................... 513
Exclude Network Connections ....................................................................................................... 515
Include Network Connections to monitor ..................................................................................... 518
Suspicious Connections .................................................................................................................. 520
Monitor Suspicious Connections ................................................................................................... 520
Add Programs to the Trusted List ................................................................................................. 522
Add Firewall Exceptions to the Trusted List ................................................................................. 523
Monitor Processes ............................................................................................................................ 525
To monitor configured processes ................................................................................................. 525
Remove Processes from ‘List of Filtered Processes’ .................................................................... 526
Maintain Log Backup ...................................................................................................................... 526
To backup event logs automatically ............................................................................................ 526
Transfer Log Files ............................................................................................................................ 529
To transfer Windows and Application Log Files .......................................................................... 529
Config Assessment ......................................................................................................................... 531
To enable Config Assessment ....................................................................................................... 531
Syslog FTP Sever ............................................................................................................................ 532
To transfer Windows events as Syslog messages.................................................................532
Back up Current Configuration...............................................................................................535
To backup current configuration settings...........................................................................535
Chapter 40 Traffic Analyzer ...............................................................................................537
Event Traffic Analysis ..........................................................................................................538
To start Traffic Analyzer ......................................................................................................538
View by Category ....................................................................................................................539
View by Event Id ......................................................................................................................540
View by Custom Selection ......................................................................................................542
Keyword Analysis ..................................................................................................................543
Add Keywords for Analysis ....................................................................................................544
Add Commonly Occurring Words to Exclude from Analysis ...........................................545
Chapter 41 Agent Management Tool ..................................................................................547
Windows Agent Management Tool .......................................................................................548
Access Agent Management Tool ........................................................................................548
Query Agent Service Status – System/Group/All/Custom..................................................549
Restart Agent Service – System / All / Group / Custom .......................................................550
Query Version of the Agent Service – System / Group / All / Custom ..................................552
Remove the Agent Component - System / Group / All / Custom .........................................554
Delete Systems from the agent service - System / Group / All / Custom...............................556
Chapter 42 SCAP Profile Editor .........................................................................................558
SCAP Benchmark Profile Editor ........................................................................................559
Chapter 43 TrapTracker ......................................................................................................562
About TrapTracker ...............................................................................................................563
TrapTracker Components ....................................................................................................563
Chapter 44 Change Audit .....................................................................................................564
EventTracker Inventory Manager .........................................................................................565
Change Audit Results Summary Console ...........................................................................565
Change Policy Dashboard ......................................................................................................566
Configuration Policy Dashboard ...........................................................................................566
Chapter 45 About EventTracker ........................................................................................567
About EventTracker ..............................................................................................................568
Chapter 46 Access Configuration via SCAP ................................................................. 569
SCAP ............................................................................................................................... 570
SCAP content ..................................................................................................................... 571
SCAP implementation in EventTracker ............................................................................ 571
Appendix – HIPAA .......................................................................................................... 573
HIPAA Compliance Reports ............................................................................................. 573
User Logon report .............................................................................................................. 573
User Logoff report ............................................................................................................. 573
Logon Failure report ......................................................................................................... 573
Audit Logs access report .................................................................................................. 573
Appendix – SOX ................................................................................................................. 574
Sarbanes – Oxley Compliance Reports ............................................................................. 574
User Logoff report ............................................................................................................. 574
User Logon report ............................................................................................................. 574
Logon Failure report ......................................................................................................... 574
Audit Logs access report .................................................................................................. 574
Security Log Archiving Utility .......................................................................................... 574
Track Account management changes .............................................................................. 575
Track Audit policy changes ............................................................................................... 575
Track individual user actions ............................................................................................ 575
Track application access ................................................................................................... 575
Track directory / file access .............................................................................................. 575
Appendix – GLBA ................................................................................................................. 576
GLBA Compliance Reports .............................................................................................. 576
User Logon report ............................................................................................................. 576
User Logoff report ............................................................................................................. 576
Logon Failure report ......................................................................................................... 576
Audit Logs access report .................................................................................................. 576
Appendix – Security Reports ............................................................................................ 577
Security Reports ............................................................................................................... 577
Successful and failed file access ......................................................................................... 577
Successful logons preceded by failed logons ................................................................. 577
Audit log cleared events by user....................................................................................................577
Invalid logons by date.....................................................................................................................577
Daily reboot statistics .....................................................................................................................577
CPU load peaks by computers.......................................................................................................577
Account usage outside of normal hours........................................................................................578
Audit policy history .......................................................................................................................578
Accounts that were never logged on ............................................................................................578
Administrative Access to Computers ............................................................................................578
File Access by User .......................................................................................................................579
Hot fixes by Computer ..................................................................................................................579
Last logon by Domain Controller ...............................................................................................579
User Account Locked Out ..........................................................................................................580
Appendix – BASEL II ....................................................................................................................581
BASEL II .......................................................................................................................................581
Appendix – FISMA ..........................................................................................................................582
FISMA ...........................................................................................................................................582
FISMA Sec. 3505 .............................................................................................................................582
FISMA Sec. 3544 .............................................................................................................................582
Appendix – PCI DSS .......................................................................................................................583
PCI DSS .........................................................................................................................................583
Glossary .........................................................................................................................................584
About this Guide

This guide will help you to use every option of EventTracker and provides detailed procedures for the same.

Who should read this guide

Intended audience:
- Administrators who are assigned the task to monitor and manage events using EventTracker
- Operations personnel who manage day-to-day operations using EventTracker

Typographical Conventions

Before you start, it is important to understand the typographical conventions followed in this guide:

<table>
<thead>
<tr>
<th>This</th>
<th>Represents</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold</strong></td>
<td>Input fields, radio button names, checkboxes, drop-down lists, menus, and menu options, buttons on the screen and keyboard keys.</td>
</tr>
<tr>
<td>(Text_to_customize)</td>
<td>A placeholder for something that you must customize. For example, (Server_Name) would be replaced with the name of your server / machine name or an IP address.</td>
</tr>
<tr>
<td>Constant width</td>
<td>Text that you enter, program code, files and directory names, function names.</td>
</tr>
<tr>
<td>✉️</td>
<td>A Note, providing additional information about a certain topic.</td>
</tr>
</tbody>
</table>

Some of the frequently used icons which you will come across in this document are mentioned in the table below.

<table>
<thead>
<tr>
<th>Click</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔄⚠️</td>
<td>Caution</td>
</tr>
<tr>
<td>📊</td>
<td>Line Graph</td>
</tr>
<tr>
<td>📊</td>
<td>View stacked bar graph.</td>
</tr>
<tr>
<td>📊</td>
<td>View bar graph.</td>
</tr>
<tr>
<td>📊</td>
<td>View pie graph.</td>
</tr>
<tr>
<td>🔄🔍</td>
<td>Use to expand / collapse the panes.</td>
</tr>
<tr>
<td>📊🔍</td>
<td>Magnify a graph.</td>
</tr>
<tr>
<td>✉️🔍</td>
<td>Edit title of the graph.</td>
</tr>
<tr>
<td>Click</td>
<td>To</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>Collapse a pane.</td>
<td>Click to collapse a pane.</td>
</tr>
<tr>
<td>Expand a pane.</td>
<td>Click to expand a pane.</td>
</tr>
<tr>
<td>Refresh the page with latest events</td>
<td>Click to refresh the page with latest events</td>
</tr>
<tr>
<td>Search the search phrase.</td>
<td>Click to search the search phrase.</td>
</tr>
<tr>
<td>Edit the Dashlet.</td>
<td>Click to edit the Dashlet.</td>
</tr>
<tr>
<td>Minimize the Dashlet.</td>
<td>Click to minimize the Dashlet.</td>
</tr>
<tr>
<td>Maximize the Dashlet.</td>
<td>Click to maximize the Dashlet.</td>
</tr>
<tr>
<td>Dismiss the Dashlet.</td>
<td>Click to dismiss the Dashlet.</td>
</tr>
<tr>
<td>Refine/Filter icon.</td>
<td>Click to refine/filter the Dashlet.</td>
</tr>
<tr>
<td>No data icon.</td>
<td>Click to view the No data icon.</td>
</tr>
<tr>
<td>Cancelled icon.</td>
<td>Click to cancel the Dashlet.</td>
</tr>
<tr>
<td>Processing icon</td>
<td>Click to view the Processing icon.</td>
</tr>
<tr>
<td>Success icon.</td>
<td>Click to view the Success icon.</td>
</tr>
<tr>
<td>Failed icon.</td>
<td>Click to view the Failed icon.</td>
</tr>
<tr>
<td>Go icon.</td>
<td>Click to go to the Go icon.</td>
</tr>
<tr>
<td>Geo Location icon.</td>
<td>Click to view the Geo Location icon.</td>
</tr>
<tr>
<td>Back icon.</td>
<td>Click to go back to the Back icon.</td>
</tr>
<tr>
<td>Help icon.</td>
<td>Click to view the Help icon.</td>
</tr>
<tr>
<td>Flex Reports icon.</td>
<td>Click to view the Flex Reports icon.</td>
</tr>
<tr>
<td>Unflagged.</td>
<td>Click to unflag the Dashlet.</td>
</tr>
<tr>
<td>Flagged and requires immediate action.</td>
<td>Click to flag the Dashlet and mark it as requiring immediate action.</td>
</tr>
<tr>
<td>Checked and solved.</td>
<td>Click to check and solve the Dashlet.</td>
</tr>
<tr>
<td>Notes icon.</td>
<td>Click to view the Notes icon.</td>
</tr>
<tr>
<td>File changes found.</td>
<td>Click to view file changes found.</td>
</tr>
<tr>
<td>Icon</td>
<td>To</td>
</tr>
<tr>
<td>------</td>
<td>----</td>
</tr>
<tr>
<td><img src="image" alt="Registry changes found." /></td>
<td>Registry changes found.</td>
</tr>
<tr>
<td><img src="image" alt="File and registry changes found." /></td>
<td>File and registry changes found.</td>
</tr>
<tr>
<td><img src="image" alt="Fresh items." /></td>
<td>Fresh items.</td>
</tr>
<tr>
<td><img src="image" alt="Items accepted." /></td>
<td>Items accepted.</td>
</tr>
<tr>
<td><img src="image" alt="Items ignored." /></td>
<td>Items ignored.</td>
</tr>
<tr>
<td><img src="image" alt="Items rejected." /></td>
<td>Items rejected.</td>
</tr>
<tr>
<td><img src="image" alt="A failed rule marked as Deviation." /></td>
<td>A failed rule marked as Deviation.</td>
</tr>
<tr>
<td><img src="image" alt="Rule that failed to comply." /></td>
<td>Rule that failed to comply.</td>
</tr>
<tr>
<td><img src="image" alt="Rule that complied." /></td>
<td>Rule that complied.</td>
</tr>
<tr>
<td><img src="image" alt="A rule with the result &quot;error&quot;, &quot;unknown&quot;, &quot;not applicable&quot;, &quot;not checked&quot;, &quot;not selected&quot;, &quot;informational&quot;, or &quot;fixed&quot; is considered an exception." /></td>
<td>A rule with the result &quot;error&quot;, &quot;unknown&quot;, &quot;not applicable&quot;, &quot;not checked&quot;, &quot;not selected&quot;, &quot;informational&quot;, or &quot;fixed&quot; is considered an exception.</td>
</tr>
<tr>
<td><img src="image" alt="Indicates no comment had been entered by the user." /></td>
<td>Indicates no comment had been entered by the user.</td>
</tr>
<tr>
<td><img src="image" alt="Indicates the user had entered comments." /></td>
<td>Indicates the user had entered comments.</td>
</tr>
<tr>
<td><img src="image" alt="CAB files are present." /></td>
<td>CAB files are present.</td>
</tr>
<tr>
<td><img src="image" alt="CAB files are not present." /></td>
<td>CAB files are not present.</td>
</tr>
<tr>
<td><img src="image" alt="Log Book icon." /></td>
<td>Log Book icon.</td>
</tr>
<tr>
<td><img src="image" alt="Export to excel icon." /></td>
<td>Export to excel icon.</td>
</tr>
<tr>
<td><img src="image" alt="Email icon." /></td>
<td>Email icon.</td>
</tr>
<tr>
<td><img src="image" alt="Explore icon" /></td>
<td>Explore icon</td>
</tr>
<tr>
<td><img src="image" alt="Analytics icon" /></td>
<td>Analytics icon</td>
</tr>
<tr>
<td><img src="image" alt="Delete icon" /></td>
<td>Delete icon</td>
</tr>
<tr>
<td><img src="image" alt="Report Calendar" /></td>
<td>Report Calendar</td>
</tr>
<tr>
<td><img src="image" alt="Report Status" /></td>
<td>Report Status</td>
</tr>
<tr>
<td><img src="image" alt="Information icon" /></td>
<td>Information icon</td>
</tr>
</tbody>
</table>
Document Revision Control

This section defines the conventions followed for the document revision control number. The revision control number is an alphanumeric identifier, unique to the document. The components of the acronym identify the following:

- First word – name of the product
- Second word – version of the product
- Third word – document description

![Diagram](image)

**Figure 1**

The document revision control number for this guide is as given below:

<table>
<thead>
<tr>
<th>File Name</th>
<th>EventTracker v7.3 Enterprise User Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Updated in accordance with release version 7.4.</td>
</tr>
<tr>
<td>Status</td>
<td>Draft</td>
</tr>
<tr>
<td>Release Date</td>
<td>April 30, 2013</td>
</tr>
</tbody>
</table>
How to Get In Touch

The following sections provide information on how to obtain support for the documentation and the software.

Documentation Support
Prism Microsystems, Inc. welcomes your comments and suggestions on the quality and usefulness of this document. For any questions, comments, or suggestions on the documentation, you can contact us by e-mail at support@eventtracker.com

Customer Support
If you have any problems, questions, comments, or suggestions regarding EventTracker, contact us by e-mail at support@eventtracker.com. While contacting customer support, have the following information ready:

- Your name, e-mail address, phone number, and fax number
- The type of hardware, including the server configuration and network hardware if available
- The version of EventTracker and the operating system
- The exact message that appeared when the problem occurred or any other error messages that appeared on your screen

Related Documents

- Install Guide
- Upgrade Guide
- Direct Log Archiver
- Agent DLA
- Virtual Collection Points
- Log Search
- Parsing Rule
- Change Audit
- Install and Customize Web Server (IIS)
- IIS Custom Error Setting
- Securing IIS Web Server with SSL
Chapter 1
Getting Started

In this chapter, you will learn about:

- EventTracker Services and Ports
- EventTracker Control Panel
- EventTracker Admin Menu
- EventTracker Tools Menu
About EventTracker

EventTracker framework is Prism Microsystems, Inc's flagship event log monitoring and management product. The EventTracker solution is a scalable, enterprise-class Security Information and Event Management (SIEM) solution for Windows systems, Syslog/Syslog NG (UNIX and many networking devices), SNMP V1/V2, legacy systems, applications and databases.

EventTracker is a reliable and practical software-only solution, to monitor, track, and manage critical events that occur in Windows 2000/2003/XP/Vista/2008/2008R2/7/8/2012, MSCS system(s) and UNIX-style Syslog in your enterprise.

Installation of EventTracker is quick, simple, and intuitive. EventTracker comes with a thorough resource kit with several nifty utilities, which alleviates the pain of day-to-day administration of your enterprise network. Log Volume Analysis is similar to Log Analysis but with more bells and whistles, which gives you an incisive insight into the event traffic flow in your enterprise.

- Agent Optional Architecture
- Cross-platform support
- Centralized Warehouse
- Auto back-up / clear native event logs
- Real-time Alerts
- Event Correlation
- User tracking
- Process, network and service monitoring
- Granular filtering
- Change auditing
- Configuration assessment
- NetFlow monitoring
- Virtual Collection Points
- Execute Remedial Actions
- Monitor file transactions that occur in the inserted media (USB or other devices)
- Generate audit reports based on Collection Point Sites
- Manage Active Directory (AD) Organizational Units (OU)
- SID translation
- Generate audit-ready compliance reports (HIPAA, SOX, FISMA, GLBA, PCI)
- Log book
- Parsing of token
- Persist data
- Instant search option

## EventTracker Services and Ports

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
<th>Startup Type</th>
<th>Log on as</th>
<th>Allow service to interact with desktop</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Event Correlator</strong></td>
<td>Correlates the received events from the agent and performs the action based on the rules.</td>
<td>Automatic</td>
<td>Local System account</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>EventTracker Agent</strong></td>
<td>Relays local log data and is usually managed by the central EventTracker Console. If uninstalled locally, corresponding changes will be necessary at the Console. May be restarted to pick up new configuration. Performs configuration assessment for received requests and sends back the assessment results.</td>
<td>Automatic</td>
<td>Local System account</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>EventTracker Alerter</strong></td>
<td>Used by EventTracker to manage RSS notifications generated via Alerts.</td>
<td>Automatic</td>
<td>Local System account</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>EventTracker EventVault</strong></td>
<td>An EventTracker component to compress and securely store the raw log data.</td>
<td>Automatic</td>
<td>Local System account</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>EventTracker Indexer</strong></td>
<td>Responsible for indexing the key words of event properties. Event properties include Computer, Source, EventID, Domain, User, LogType, EventType, and Description.</td>
<td>Automatic</td>
<td>Local System account</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>EventTracker Receiver</strong></td>
<td>Enables EventTracker to receive log data from the configured sources. If stopped, EventTracker cannot function. May be restarted to pick up new configuration.</td>
<td>Automatic</td>
<td>Local System account</td>
<td>Yes</td>
</tr>
<tr>
<td>Service</td>
<td>Description</td>
<td>Startup Type</td>
<td>Log on as</td>
<td>Allow service to interact with desktop</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------------------</td>
<td>--------------</td>
<td>-------------------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>EventTracker Remoting</td>
<td>This service is used to send any request (like install agent/upgrade agent/uninstall agent etc.) to communicate with the EventTracker agent service.</td>
<td>Automatic</td>
<td>User Account</td>
<td>Yes</td>
</tr>
<tr>
<td>EventTracker Reporter</td>
<td>Responsible for reports / Flex Report execution and log search.</td>
<td>Automatic</td>
<td>Local System account</td>
<td>Yes</td>
</tr>
<tr>
<td>EventTracker Scheduler</td>
<td>Used by EventTracker to initiate scheduled activities like CAB integrity verification, traffic analysis. Also initiates User Activity monitoring and 'Collection Point' related activities. Fetches configuration assessment requests from queue and dispatches the request to EventTracker agents running on target system.</td>
<td>Automatic</td>
<td>Local System account</td>
<td>Yes</td>
</tr>
<tr>
<td>WcwService</td>
<td>Used to take periodic snapshots and entertain change assessment requests.</td>
<td>Automatic</td>
<td>Local System account</td>
<td>Yes</td>
</tr>
<tr>
<td>Status Tracker</td>
<td>This service is used to keep track of system up and down.</td>
<td>Automatic</td>
<td>Local System account</td>
<td>Yes</td>
</tr>
<tr>
<td>Trap Tracker Receiver</td>
<td>Receives traps in the form of an alert or other asynchronous event about a managed subsystem.</td>
<td>Automatic</td>
<td>Local System account</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**NOTE**

In case any EventTracker services are not running a warning message is displayed when you log in.

Figure 2
### Start EventTracker

**To start EventTracker**

1. Select the **Start button**, select **All Programs**, and then select **Prism Microsystems**.
2. Select **EventTracker**, and then select **EventTracker Enterprise**.

   (OR)

   Double-click the **EventTracker Enterprise** shortcut on desktop.

   EventTracker displays the login page.
EventTracker displays the logs processed information only when a CAB file is created locally on the server.
3 Type valid user credentials, and then click **Login**.

EventTracker displays the **Incidents** dashboard.
EventTracker Main menu consists of following menu’s as mentioned in the table.

<table>
<thead>
<tr>
<th>Click</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incidents</td>
<td>Analyze alert events occurred in all managed systems.</td>
</tr>
<tr>
<td>Status</td>
<td>Monitors the status (Up/ Down times) of systems and applications present in an Enterprise</td>
</tr>
<tr>
<td>Behavior</td>
<td>Add/remove Security or Operations related enterprise activity dashlets</td>
</tr>
<tr>
<td>Click</td>
<td>To</td>
</tr>
<tr>
<td>-------</td>
<td>----</td>
</tr>
</tbody>
</table>
| Dashboard (A Keyword Indexing Dashboard) | Add/remove Security/Operations/Compliance related keyword indexing dashlets  
Configure, customize, and reset Security/Operations/Compliance dashlets. |
| NetFlow | Analyze NetFlow messages collected and archived by EventTracker Direct Log Archiver. |
| Search | Provides Log Search |
| Reports | Consists of Security, Operation, Compliance and Flex Reports |
| My EventTracker | Personalize EventTracker. Only the user who has generated/configured reports has the permission to view them. |
| Change Audit | Helps to analyze voluntary and involuntary changes occurred in managed systems. |
| Config Assessment | Run SCAP Benchmarks against the managed systems. |

**NOTE**

You may not be able to see some of the features in the EventTracker Main menu if required license is not purchased.

4. Click the **Admin** hyperlink at the upper-right corner.  
   DO NOT click on Admin drop down.  
   EventTracker displays the EventTracker Diagnostics tab.
Figure 7

<table>
<thead>
<tr>
<th>Icon</th>
<th>Represents</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>EventTracker service status</td>
</tr>
<tr>
<td></td>
<td>Service stopped.</td>
</tr>
<tr>
<td></td>
<td>Service is running.</td>
</tr>
<tr>
<td></td>
<td>Service not installed.</td>
</tr>
</tbody>
</table>

Move the mouse pointer over the service, EventTracker displays the status in a tooltip.
Click the name of the service, EventTracker displays the description of the service in a pop-up window.
(Example: Agent).

Figure 8

Figure 9

Figure 10
6 Click ➢ icon to restart the service or click ➤ icon to start the stopped service.

7 On the Virtual collection point statistics pane, click a hyperlink in the System count column to view the name of the systems forwarding events through a particular port. EventTracker displays the name of the systems in a pop-up window.

8 Click a hyperlink in the Event count column to view the Event-O-Meter.
9 On the **Disk space information** pane, move the mouse pointer over the graph. EventTracker displays the space used and free space information in a tooltip.

10 **System(s) with no events in the last 1 hour** pane will name the agent/managed systems that have not reported to manager system in the last one hour.

11 **Event cache file status** represents the number of event cache files created and the number of cab files present on the machine.

12 Click the **Control Panel** tab. EventTracker displays the ‘Control Panel’ tab. It consists of shortcuts that help you to quickly access EventTracker modules.

<table>
<thead>
<tr>
<th>Click</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Alerts" /></td>
<td>Manage alerts, alert actions, and alert threat level.</td>
</tr>
<tr>
<td><img src="image" alt="Behavior Rules" /></td>
<td>Define and manage behavior rules. These rules could be added as behavior dashlets in the Security, Operations and My EventTracker tabs.</td>
</tr>
<tr>
<td><img src="image" alt="Behavior Settings" /></td>
<td>Configuring settings for the ‘Enterprise Activity Behavior’ module.</td>
</tr>
</tbody>
</table>
Event Tracker Ver. 7.4 Enterprise User Guide

<table>
<thead>
<tr>
<th>Category</th>
<th>Event categories are knowledge packs. You can add / modify / delete your own categories. You can also edit / delete pre-defined categories.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection Master</td>
<td>EventTracker ‘Collection Master’ collects CAB files forwarded by Collection Point(s).</td>
</tr>
<tr>
<td>Collection Point</td>
<td>Forwards CAB files to ‘Collection Master(s)’</td>
</tr>
<tr>
<td>Event Filters</td>
<td>Configure manager side event filters.</td>
</tr>
<tr>
<td>Eventvault</td>
<td>Functions as warehouse for CAB files. Manage archives and configure retention and validation.</td>
</tr>
<tr>
<td>IP lookup config</td>
<td>Customizable IP Address verification/detailed information.</td>
</tr>
<tr>
<td>Parsing rules</td>
<td>Parsing Rules</td>
</tr>
<tr>
<td>Manager</td>
<td>Define Virtual Collection Points, enable Syslog, configure DLA, enable NetFlow receivers etc.</td>
</tr>
<tr>
<td>Report Settings</td>
<td>Manage settings that affect report generation and e-mail delivery.</td>
</tr>
<tr>
<td>RSS</td>
<td>Configure and manage RSS feeds.</td>
</tr>
<tr>
<td>Systems</td>
<td>Manage EventTracker Windows agent and Change Audit agent.</td>
</tr>
<tr>
<td>Users</td>
<td>Manage privileges and permissions of the users defined in the EventTracker user group.</td>
</tr>
<tr>
<td>Weights</td>
<td>Assign weight values to Event Source, Event ID, Categories, etc. These are used in the tag cloud display in the Search/Refine dialog (EventTracker Log Search).</td>
</tr>
<tr>
<td>Windows Agent Conf</td>
<td>Manage configuration of EventTracker Windows Agent.</td>
</tr>
</tbody>
</table>

EventTracker Control Panel

1. Select the **Start button**, select **All Programs**, and then select **Prism Microsystems**.
2. Select **EventTracker**, and then select **EventTracker Control Panel**.

   (OR)

   Double-click the **EventTracker Control Panel** shortcut on desktop.

   EventTracker displays the login page.
NOTE

You may not be able to see some of the features in the Control Panel if required license is not purchased.

To open a module, click the respective icons.

<table>
<thead>
<tr>
<th>Click</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>EventVault</td>
<td>Functions as warehouse for CAB files. Manage archives and configure retention &amp; validation.</td>
</tr>
<tr>
<td>Diagnostics</td>
<td>Alerts if any problem occurs in the EventTracker.</td>
</tr>
<tr>
<td>License Manager</td>
<td>Provides license details, features opted for, license usage of EventTracker.</td>
</tr>
<tr>
<td><strong>Export Import Utility</strong></td>
<td>Enables you to export/import custom Categories, Filters, Alerts, Scheduled Reports, Domains, Systems, RSS Feeds, and Behavior Rules during migrate/upgrade process, and to transfer EventTracker data from one system to the other in your enterprise.</td>
</tr>
<tr>
<td><strong>Append Archives</strong></td>
<td>Use this utility to merge backup CAB files. Indexing is done automatically.</td>
</tr>
<tr>
<td><strong>EventTracker Agent Configuation</strong></td>
<td>To configure the system for reporting to multiple managers, to filter events, to monitor services, software installations, processes, system health, and to archive the events database.</td>
</tr>
<tr>
<td><strong>Traffic Analyzer</strong></td>
<td>To analyze event traffic patterns. The data can be used to filter out irrelevant events and perform other operation tasks.</td>
</tr>
<tr>
<td><strong>Agent Management</strong></td>
<td>A diagnostic tool to check the health status of remote agents, restart the failed agent services and to check the version of remote agents.</td>
</tr>
<tr>
<td><strong>SCAP Profile Editor</strong></td>
<td>To tailor/edit the predefined SCAP benchmark profile.</td>
</tr>
<tr>
<td><strong>TrapTracker</strong></td>
<td>To manage traps received from SNMP enabled devices.</td>
</tr>
<tr>
<td><strong>Change Audit</strong></td>
<td>An application that used to track the occurred changes on a computer's file system and registry and provides you with a lifeline to restore it back to a working configuration.</td>
</tr>
<tr>
<td><strong>About EventTracker</strong></td>
<td>View License Usage, updates applied and other details.</td>
</tr>
</tbody>
</table>

## Admin Menu

<table>
<thead>
<tr>
<th><strong>Click</strong></th>
<th><strong>To</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Alerts</td>
<td>Manage alerts, alert actions, and alert threat level.</td>
</tr>
<tr>
<td>Behavior Rules</td>
<td>Define and manage behavior rules. These rules could be added as behavior dashlets in the Security, Operations and My EventTracker tabs.</td>
</tr>
<tr>
<td>Behavior Settings</td>
<td>Configuring settings for the 'Enterprise Activity Behavior' module.</td>
</tr>
<tr>
<td>Category</td>
<td>Event categories are knowledge packs. You can add / modify / delete your own categories. You can also edit / delete pre-defined categories.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Event Filters</td>
<td>Configure manager side event filters.</td>
</tr>
<tr>
<td>EventVault</td>
<td>Functions as warehouse for CAB files. Manage archives and configure retention &amp; validation.</td>
</tr>
<tr>
<td>IP Lookup Configuration</td>
<td>Customizable IP Address verification/detailed information.</td>
</tr>
<tr>
<td>Manager</td>
<td>Define Virtual Collection Points, enable Syslog, configure DLA, enable NetFlow receivers etc.</td>
</tr>
<tr>
<td>Parsing Rules</td>
<td>User defined token bound with dynamic report template to generate flex report</td>
</tr>
<tr>
<td>Report Settings</td>
<td>Manage settings that affect report generation and e-mail delivery.</td>
</tr>
<tr>
<td>RSS</td>
<td>Configure and manage RSS feeds.</td>
</tr>
<tr>
<td>Systems</td>
<td>Manage EventTracker Windows agent and Change Audit agent.</td>
</tr>
<tr>
<td>Users</td>
<td>Manage privileges and permissions of the users defined in the EventTracker user group.</td>
</tr>
<tr>
<td>Weights</td>
<td>Assign weight values to Event Source, Event ID, Categories, etc. These are used in the tag cloud display in the Search/Refine dialog (EventTracker Log Search).</td>
</tr>
<tr>
<td>Windows Agent Config</td>
<td>Configure EventTracker Windows Agent.</td>
</tr>
<tr>
<td>Correlator</td>
<td>Correlates events and performs rule set based actions.</td>
</tr>
</tbody>
</table>

**NOTE**

You may not be able to see some of the features in the EventTracker Admin menu if required license is not purchased.

## Tools Menu

<table>
<thead>
<tr>
<th>TOOL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event-O-Meter</td>
<td>View per port trends of events against specified time range.</td>
</tr>
<tr>
<td>Log Book</td>
<td>An electronic book in which users can add entries from Incidents, Reports, Change Audit, Config Assessment</td>
</tr>
<tr>
<td>Log View</td>
<td>View per category per system logs. You have the liberty to choose category / system groups / systems.</td>
</tr>
<tr>
<td>Sitemap</td>
<td>View index of the web site.</td>
</tr>
<tr>
<td>Windows</td>
<td>View different activities that take place on a particular system. (Example: Software Installed, printer activity etc.)</td>
</tr>
</tbody>
</table>
Incorporate Your Company Logo

This option helps you incorporate your company logo into EventTracker.

To incorporate your Company Logo

1. Browse and locate ‘prism.jpg’ in the installation directory/images folder, typically ...\Program Files\Prism Microsystems\EventTrackerWeb\images.
2. Rename the "prism.jpg" image file.
3. Copy your company logo into that folder and then rename it as prism.jpg.
4. Log on to EventTracker Enterprise.
   Find that the Prism logo at the upper-left corner is replaced with your company logo.

**NOTE**

The dimension should be 80 x 30 pixels.

Application and Chart Theme

You can change the theme of EventTracker application and charts.

1. Select name at the top right hand side corner.
2. Select **Application Theme** drop-down and then select **Blue/Olive**.
   Olive is selected by default.
3. Select **Chart Theme** drop-down and then select the required option.
4. To preview the chart theme, select **Preview**.
   Chart Theme Preview window displays.
5. To view the changes done in application and chart theme, select **Change** hyperlink to update.

**Update EventTracker Users List**

This option helps you update EventTracker configuration, if:
- New users are added to the “EventTracker” user group
- You face Log on issues

**To update Users List**

1. Select the **Start button**, select **All Programs**, and then select **Prism Microsystems**.
2. Select **EventTracker**, and then select **Update Users List**.
   EventTracker displays Update EventTracker Users console.
If a non-admin user is promoted as an Administrator then checkbox against the user is selected. To promote a non-admin user, please refer to the Promote a Non-Admin User as an Administrator section.

3. **Click Ok.**

EventTracker updates 'EventTracker Configuration' and displays the success message:

```
53 users found in the 'EventTracker' group. EventTracker configuration updated successfully.
```

![Figure 16](image)
Exit EventTracker

This option enables you to log out of EventTracker.

A) To exit EventTracker, select name at the upper-right corner and then select icon.
EventTracker logs you out gracefully.

NOTE
When two users log in with the same user credentials, EventTracker logs out the first user and allows the second user to create the session.

NOTE
When there is no user interaction for a specified length of time, EventTracker logs out the user.
EventTracker denies access, when a user tries to log on without appropriate access permissions and privileges.

![Welcome to EventTracker](image)

**NOTE**

Welcome to EventTracker

Please enter your user name and password

User Name: Karen

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

Invalid username or password

Login

125,126,910 logs processed since install on Oct 18, 2012.
73,945 logs processed today.

- Designed for IE 8.0 and above, Firefox 3.6 and above
- This web application uses pop-up windows
- Best viewed in 1024x768 screen
Chapter 2
Analyze Incidents

In this chapter, you will learn how to:

- Incidents Dashboard
- Tune Alerts
- Search Incidents
- Web Slices
Incidents Dashboard

Incident dashboard helps you to interpret alert events received from managed systems. Internal scoring algorithm automatically computes and ranks alert severity levels. Only the most critical alerts that need to be attended first are displayed on the dashboard.

To analyze incidents dashboard

1. Log on to EventTracker Enterprise.
   EventTracker displays the Incidents dashboard by default, containing both acknowledged and unacknowledged incidents. You can click on the graph and manage the generated incidents. By default, EventTracker displays the incidents that are generated for past 24 hours in the Top 5 systems by Risk or by Systems pane.

   In Top 5 incidents by count pane, it provides details about the incidents and number of times that particular incident had occurred.

   In Top 5 incidents by Risk pane, it provides details about the incidents that have been identified based on the severity (i.e. Critical, Serious, High, Medium, Low).

   In Top 5 systems by Count pane, it shows details about the top 5 systems which have the highest number of incidents generated.

   In Incidents for last 7 days pane, a pictorial graph is displayed with information about the incidents that took place in last 1 week.

   If you click any graph, then Search Criteria window displays providing additional information which is explained in detail in the forthcoming section of this chapter.
2. To view systems by risk, click **View by** drop down, and then select **Risk**.
3. To view by systems, click **View by** drop down, and then select **Systems**.
4. To view the duration of incident details, click **Duration** drop down, and then select the required option.
5. To refresh the Dashboard, select **Refresh every** drop down, and then select the required option.
6. To rotate tabs, click **Rotate** option.

**Graphical View**

1. Select the **Incident** menu, select **Graph** tab.
The graphical view pane will list the Top 5 unacknowledged incidents by Risk or Count. The pictorial representation can be viewed in pie, bar or stacked bar graph.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group</td>
<td>Enterprise system groups are listed in this drop-down list. By default, EventTracker selects the ALL option.</td>
</tr>
<tr>
<td>View By</td>
<td>View data by risk or count.</td>
</tr>
<tr>
<td>Top</td>
<td>By default, top 5 systems with more incidents are displayed in the top pane. You can select up to top 20 systems for displaying in the top pane.</td>
</tr>
<tr>
<td>Acknowledged</td>
<td>Check this option to see the list of incidents that are acknowledged. By default, the dashboard displays only the unacknowledged incidents.</td>
</tr>
</tbody>
</table>

2. Click on the graph to view detailed information. Search window displays and details are explained in the forthcoming section.

### Tabular View

1. Select the **Incident** menu, and then select **Tabular** tab.

   By default, EventTracker displays the unacknowledged incidents that are generated for past 24 hours. To view only the acknowledged incidents, check the acknowledged option.
2. Click the '+' symbol to view detail information i.e., Event Id, Source, Event Type, Description.

3. Click Flag icon to change the status of the incident.

<table>
<thead>
<tr>
<th>Flag icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRAY</td>
<td>Un-flagged and no action has been taken</td>
</tr>
<tr>
<td>RED</td>
<td>Flagged and relevant action is required for that particular incident to solve an issue</td>
</tr>
<tr>
<td>GREEN</td>
<td>Checked the incident and necessary action has been taken care of</td>
</tr>
</tbody>
</table>

4. Click Search hyperlink.

Search Incidents window displays. The detailed information is given in detail in the next section.

5. Click Ack option to acknowledge the incident.

6. Click Notes icon to add comments about a particular incident.

7. Click Email icon to mail an incident.
8. Click **Log Book** icon to update data in Log Book.

A logbook message displays.

![Logbook](image)

Figure 24

9. To add a new logbook entry, click the **Add new** button.

10. To add to an existing logbook, click the **Add to existing** button.

    Log Book window displays.

![Log Book](image)

Figure 25

11. Enter/Modify the required data, and then click the **Save** button.

    For detailed information about Log Book, refer **Log Book**.
Tune Alerts Configuration

This option helps you to modify alerts configuration settings. You can even activate or deactivate the alerts.

To Tune Alerts

1. In Tabular tab, click the Event Id or System dropdown in the bottom pane, select Tune Alert.

2. Make required changes in Event Filter, Custom, Systems, and Actions pages, and then click the Finish button.

   The modified alert configuration is saved.

   **NOTE**

   For detail information on Alert configuration, refer Alerts.

All Incidents

a. Click System drop down. Select All Incidents.

   Search Incidents window displays.

b. In Search Incidents window, select the Event ID.

   You will be redirected to EventTracker Knowledge Base.
Log Search

‘Log Search’ feature is added to search for logs pertaining to the **System** or **Event Id**. The results obtained can further be refined.

1. In **Dashboard or Tabular** tab, click the **Event Id** or **System** dropdown in the bottom pane, select **Log Search**.

   Log Search - Timeline window displays.

   ![Log Search - Timeline](image)

   **Figure 28**

Log Search for a **System** will display all the events related to that particular system.

Log Search for an **Event ID** will display the results for the selected Event Id and the system name where the event was generated.

For more information on log search, refer [Log Search](#) document.
Knowledge Base

A) Click **Knowledge Base** option to view event details in the 'EventTracker Knowledge Base' Web site.

![EventTracker Knowledge Base Image]

**Figure 29**

Search Incidents

1. To view the total incidents occurred on a particular system; click a graph 'Incidents dashboard' or 'Graphical' tab.

   Search Incidents Window displays.
### EventTracker User Guide

**Figure 30**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date/Time</td>
<td>Date and time on which the incident occurred.</td>
</tr>
<tr>
<td>Incident #</td>
<td>A unique number assigned for each generated incident.</td>
</tr>
<tr>
<td></td>
<td>The Incident number will be in the form of YYYYMMXXXX, where YYYY represents the year, MM represents the month, and XXXX is the auto incremented number that will be reset to 1000 on the first day of every month.</td>
</tr>
<tr>
<td>Risk</td>
<td>Move the pointer over risk value to view vulnerability scan summary and to identify incident risk in terms of threat level, asset value, and vulnerability value.</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Asset Value = Undefined</td>
</tr>
<tr>
<td></td>
<td>Vulnerability = Undefined</td>
</tr>
<tr>
<td></td>
<td>When the vulnerability scanner(s) (e.g., Nessus, Qualys) scans manager systems for vulnerability, EventTracker vulnerability parser parses the scan result file and displays the scan summary in a tooltip. This helps to quickly find the criticality of the vulnerability on the managed system(s).</td>
</tr>
<tr>
<td>Event Id</td>
<td>Event identifier associated with the generated alert.</td>
</tr>
<tr>
<td>System</td>
<td>The system name where the incident occurred.</td>
</tr>
<tr>
<td>Log Type</td>
<td>The event/incident recorded in the following logs i.e. Application, Security, System logs.</td>
</tr>
<tr>
<td>Source</td>
<td>The source of the event. This can be the name of a program, a system component, or an individual component of a large program.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User</td>
<td>The user name of the user that was logged on when the incident occurred.</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description about the incident occurred.</td>
</tr>
<tr>
<td>Ack status</td>
<td>Check this option to acknowledge the incident. EventTracker opens Bulk Acknowledge window.</td>
</tr>
</tbody>
</table>

1) In the Notes pane, enter appropriate details about the action taken on the acknowledged incident.
2) Click appropriate Acknowledge option.
   The incident(s) will be acknowledged for the selected Interval.
3) Click the Save button to save the information.

**Notes**

1) Click the Notes icon.

   a) In Notes pane, write the comments about the particular alert or course of action taken on the alert, and then click the Ok button.
   Notes History pane will display the comments about the particular alert or action taken on the particular alert in the past.

   b) Email an incident including current Notes and Ack status.
   Click Email icon.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>To, Cc, Subject</td>
<td>Enter relevant data in To, Cc, Subject fields and then click Send. Configure the SMTP server settings to notify the incident via Email. To configure Email refer Manager -&gt; Email Configuration.</td>
</tr>
<tr>
<td>Copy to notepad</td>
<td>Click Copy to notepad icon. Event Information window displays with Event details.</td>
</tr>
<tr>
<td>Export</td>
<td>Click the icon to export the incident details in 'Excel' format.</td>
</tr>
<tr>
<td>EventTracker :: Alert Configuration</td>
<td>EventTracker :: Alert Configuration window displays. For detail information please refer Alerts.</td>
</tr>
<tr>
<td>Logbook</td>
<td>Click Logbook icon to view data in Log Book. For detail information please refer Log Book.</td>
</tr>
</tbody>
</table>
Web Slices

A Web Slice is a specific portion of a webpage that you can subscribe to, and which enables you to see when updated content - such as the current temperature, or a changing auction price is available from your favorite websites. Once you have subscribed to the Web Slice, it appears as a link on the Favorites bar. When the Web Slice is updated, the link on the Favorites bar will appear with bold formatting. You can then click the link to see the updated content.

Adding EventTracker latest incidents as Web Slice has number of advantages like,

- The latest incidents can be seen without actually logging into the EventTracker Enterprise.
- You will receive frequent notifications on the Favorites bar to view latest incidents.
- It will provide you the details of latest 20 incidents.


Add Web Slices to the Favorites Bar

Web Slice is a web feed technology introduced in Internet Explorer 8. You need to have IE 8 to add and view Web Slices

1) In the Incidents menu, select Tabular View, and then move the mouse pointer over the bottom pane. EventTracker displays the (Web Slices) icon at the left hand side.

2) Click Web Slice icon. EventTracker displays the confirmation window.

3) Click Add to Favorites Bar. EventTracker adds the Web Slice to the Favorites bar.

4) Click Latest 20 incidents drop-down list on the Favorites bar.
EventTracker displays the summary of top 20 Alerts.

![Latest 20 incidents](image)

**Figure 33**

http://localhost/EventTracker/WebSlice/AlertsSlice
Chapter 3
StatusTracker

In this chapter, you will learn how to:

- Create user defined group
- Add System for monitoring
- Add Application for monitoring
- Remove system/application from monitoring
- Delete Group
- View request status
- Editing Resources
- Polling Summary
- Generate Reports
About StatusTracker

StatusTracker is a robust, reliable, proactive and easy to handle tool developed by Prism Microsystems, Inc. It monitors and manages the TCP/IP networks, Web sites, applications, and ports in mission critical environment with ease and comfort.

Status Tracker helps users in:

- Audit requirements suggested by GLBA, HIPAA, Sarbanes/Oxley, California Senate Bill 1386, the USA Patriot Act and NISPOM

StatusTracker is added in EventTracker to monitor the status of all the systems running within an enterprise and is installed on the manager server.

Get Started with StatusTracker

1. Log on to EventTracker Enterprise.
2. Click the Status menu.

EventTracker displays StatusTracker panel.

![Figure 34](image-url)
NOTE

All Resource Groups displays the list of systems in the top pane and applications in the bottom pane, which are currently down.

Right Pane

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System name</td>
<td>Name of the system which is being monitored.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the system.</td>
</tr>
<tr>
<td>Display Name</td>
<td>Display name of the system.</td>
</tr>
<tr>
<td>Type</td>
<td>Name of the operating system</td>
</tr>
<tr>
<td>Status</td>
<td>Current status of the system.</td>
</tr>
<tr>
<td>Notes</td>
<td>Additional details regarding the system status.</td>
</tr>
<tr>
<td>Application name</td>
<td>Name of the application, which is being monitored.</td>
</tr>
</tbody>
</table>

Sliding Pane:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Tree</td>
<td>Contains all the default and custom groups found in the organization. The groups under resource tree can be used for add group/system/application, delete group, rename group, and remove monitoring purposes.</td>
</tr>
</tbody>
</table>

3 In the Resource Tree pane, click the required group name. EventTracker displays Group details in the right pane.
### Field | Description
---|---
System | Search for system
Application | Search for application
Device Icon | Description

- ![Icon](image1) System is up
- ![Icon](image2) System is up but some applications in the system are down
- ![Icon](image3) System is down
  You cannot add application to this system. If you try to add application then an error message will be displayed
- ![Icon](image4) System is kept aside for maintenance
- ![Icon](image5) System is initializing
- ![Icon](image6) Applications present in the system
- ![Icon](image7) Notes added for resources
- ![Icon](image8) Application is up

![Message from webpage](image9)

**Message from webpage**

Applications cannot be added as the system is down

[OK]
Important To Know

If the StatusTracker license is exhausted, then EventTracker displays an error message.

In addition, you cannot add more resources for monitoring if the license containing StatusTracker resources has been fully exhausted. In this case, if you try to add any system, then StatusTracker will display an error message.

Create User Defined Group

This option helps you to select systems from different domain/group, and create a new group. Creating a user-defined group is needed when you want to monitor systems that are present in different domain/groups within the organization.

To add group

1. Open StatusTracker panel.
2. In ‘Resource Tree’ pane, right click All Resource Groups.
3. Click Add Group.
   
   EventTracker displays Add Group window.
4 Enter appropriate group name in **Group name** box, and then click **Ok**.

For example: New Group

EventTracker displays the newly created group under resource tree pane.

As there are no systems/applications added in the newly created group, the right pane displays message saying 'No resources are being added or monitored'.

**NOTE**

The user defined group name can be changed.

a) To edit the group name, right click the user-defined group and select **Rename Group**.

b) Change the group name in 'Rename Group' pop-up window, and then click **Ok**.

To add systems in a group

Once you create a user defined group, the first step is to add systems in the group.

1 In **Resource Tree** pane, right click user-defined group.

   For example: SysTrack.
EventTracker displays shortcut menu.

![Figure 40](image)

2 Click **Add System**.

EventTracker displays Add Systems window.

![Figure 41](image)

3 Enter system name or IP address in the **System/IP Address** field.

Select **Auto discover applications** option, if required.

For example- NEMO

(OR)

Select **IP subnet range** option, and then enter the IP subnet range in the **Subnet range** field.

Select **Perform scheduled discovery** and **Auto discover applications** options, if required.

For example- 192.168.1.1 to 192.168.1.100
(OR)

Select **Website** option, and then enter the Website address in the **Website** field.

For example - [http://kb.prismmicrosys.com/evtPass/eventid.htm](http://kb.prismmicrosys.com/evtPass/eventid.htm)

**NOTE**

A **SNMP community string** is a text string that acts as a password. By default, SNMP Community String will be set as ’Public’.

If you rename the SNMP community string, then system to be added should match the community string.

4. If you wish to select the default applications present in the systems then check the **Auto discover applications** option.

5. In **Poll Settings** pane, set the poll frequency in **Poll each resource every – minutes** field.
   
   The default frequency is set to 2 minutes. This means, added computer will be polled/ monitored after every two minutes.

6. Click the **OK** button.

EventTracker displays the added systems/ IP subnet range/ Website in the right pane.
For example - Systems named ‘NEMO’ and [http://kb.prismmicrosys.com/evtPass/eventid.htm](http://kb.prismmicrosys.com/evtPass/eventid.htm) website added to the **New Group**.

While adding system to the group, **Auto discover applications** option was selected for ‘ELC’ system. Click the ‪️ sign in front of the system name to see the list of applications.

7 Click ‪️ sign to see the list of default applications present in the system.

<table>
<thead>
<tr>
<th>Application name</th>
<th>Port no.</th>
<th>Status</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>80</td>
<td>Up more than 20 mins</td>
<td></td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>Up more than 20 mins</td>
<td></td>
</tr>
<tr>
<td>File Sharing, Event</td>
<td>139</td>
<td>Up more than 20 mins</td>
<td></td>
</tr>
<tr>
<td>Terminal Server Clic</td>
<td>3306</td>
<td>Up more than 20 mins</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE**

For a system or website to be monitored in StatusTracker, **ICMP (Internet Control Message Protocol)** should be enabled. If ICMP is disabled, systems or websites status will always appear as down.
To add application(s) for monitoring

The applications present in system can be added for monitoring. Apart from the list of pre-defined applications, this option allows you to add new application(s) as well as to automatically detect all the applications present in the system.

To add application(s) to a system

Using this option, you can add application(s) to an individual system.

1. In the Resource Tree pane, select the group name where the system resides for which application(s) needs to be added for monitoring.
2. Click the system name dropdown, and then select Add application(s).

EventTracker displays Add application dialog box.
3. Select an appropriate option to search the application.
4. Change the polling frequency to poll the selected application, if required.
5. Click the Ok button.

To add application(s) to more than one system

In this option, you can select only one application at a time, but it can be added to any number of systems available under the group.

1. In the Resource Tree pane, right click the group name where application(s) needs to be added for monitoring to a number of systems, and then click Add application.
EventTracker displays **Add application for systems** dialog box.

![Add Application for Systems Dialog Box](image)

**Figure 49**

1. Select an appropriate option to search the application.
2. Check the system name(s) option to add the application.
3. Change the polling frequency to poll the selected application, if required.
4. Click the **Ok** button.

### Select an application

You can select the application to be added from the list of predefined applications. Only one application can be selected at a time, but it can be added to any number of systems available under the group.

1. Click the **Select application** option, if not selected.
NOTE

Click the Application name or System name to sort the respective column.

2 Select the application from the list of applications in the top pane.
   (OR)
   Enter the application name in the Application name field, and then click the Search button.
   Select the application name.

3 In the bottom pane, click the checkbox to select the required system for which you wish to add the selected application.
   (OR)
   Enter the system name in the System name field, and then click Search.
   Select the system name.
   (OR)
   If you wish to add the selected application to all the systems present in the group, then select the checkbox in front of System name.

4 In Poll Settings pane, change the poll frequency for the application, if required.
5 Click the **OK** button.

### New application option

1. Click **New application** option.

![Figure 51](image)

2. In the **Application name** field, enter the application name that you wish to add to the system(s).
3. For your record, provide a brief description about the application in the **Description** field.
4. Enter the valid port number in **Port** field on which the application is listening.
   (OR)
   - Click the **Search** button.

**NOTE**

*Search* button is provided to look out for the port numbers that are available from EventTracker Knowledge website.

EventTracker opens **EventTracker Knowledge website**.

5. Enter the system name in **System name** field, and then click the **Search** button.
   - Select the system name.
(OR)
Click the checkbox to select the required system for which you wish to add the selected application.
(OR)
If you wish to add the entered application to all the systems present in the group then select the checkbox in front of System name.

6 In Poll Settings pane, change the poll frequency for the application, if required.
7 Click the OK button.

Detect application option

This option will help you to detect all the applications present under the selected system(s).

1 Click Detect application option.

2 Enter the system name in System name field, and then click the Search button.
   Select the system name.
   (OR)
   Click the checkbox to select the required system for which you wish to detect the default application(s).
   (OR)
If you wish to detect the default application(s) for all the systems present in the group then select the checkbox in front of System name.

3. In Poll Settings pane, change the poll frequency for the application, if required.

4. Click the OK button.

**Edit Application**

**Edit Applications** option is provided to modify the details of default applications. Along with the details, status of the application can also be changed from active to inactive or vice-versa.

**To edit default applications**

1. In StatusTracker panel, click the Edit applications hyperlink at the top left corner.

   StatusTracker displays Edit application pop-up window.

   ![Figure 53](image)

   Figure 53

2. To search the application, enter the Application name/ Port number/Description/Application status in the respective fields.

3. Click Filter icon, and then click the required filter criteria.
StatusTracker displays the search result.

4. Click **Edit** icon in front of the application name to edit the application details. StatusTracker displays a dialog box.
2 Edit the Application Name, Port number, and Description in the respective fields.
3 Click the Active checkbox to change the status of application from active to inactive and vice-versa.
4 Click Update.
5 In Edit application dialog box, click the Save button.
   StatusTracker saves the changes made in the application.
6 Click the Close button.
   Updated changes can be seen under respective applications.

View Request Status

This option will take you through list of systems/applications added along with the details. It also gives you the status of the system/application added in the group. The status can be New (For fresh request), Success (For successful addition of system/application), Failed (For addition of system/application failed), and Process (For request under process).

1 Open StatusTracker.
2 Click the Progress hyperlink at the top left corner.
   StatusTracker displays View add Systems/applications request status window.
3 Click the refresh button to get the updated status.
4. Use the Status dropdown, to see the specific status progress.
5. Sort the activities by date/system/type/status in the Sort by dropdown.
6. Click Export to export the status details in the excel sheet.

Delete Group

1. Right click on user-defined group, which is to be deleted, and click Delete Group. StatusTracker displays confirmation message box.

![Confirmation Message](image)

**Figure 58**

**NOTE**
The groups which is discovered via auto discover will not be deleted.

2. Click OK.
All the systems and applications will be moved to the 'Default' group (EventTracker defined group).

**NOTE**
The systems and applications will be moved from user-defined group to the 'Default' group, but the resources will continue to be monitored as before. Only the mapping with the current group is removed.

Rename Group

1. Right click the group name which needs to be renamed and then click Rename Group.
Rename Group window displays.

2. Enter the required Group name and then click the Ok button.
   The group is now renamed.

Remove Monitoring

You can remove number of systems or Websites from monitoring present in a group and also can choose a single system to remove from monitoring.

To remove multiple systems/websites from monitoring

1. Right click the group name where system(s) or Website(s) to be removed from monitoring is present, and then click Remove monitoring.
StatusTracker displays **Remove monitoring** pop-up window. **Remove monitoring** dialog box displays all the systems and Websites belonging to the selected group.

2. To remove individual system/Website from monitoring, click the checkbox in front of the required system/Website name.
   
   (OR)
   
   To remove all the systems from monitoring, click the checkbox in front of **System Name**.

3. Click the **OK** button.

**To remove a system/website from monitoring**

1. Click the system/application name dropdown, and click **Remove monitoring**.

StatusTracker displays confirmation message.
For user defined group-systems and applications:

![Message from webpage](image)

Figure 64

For EventTracker defined group-systems and applications:

![Message from webpage](image)

Figure 65

2. Click **OK**.

**NOTE**

If a system in user-defined group is removed from monitoring, then it will also be deleted from the default group.

### Change Status

This option can be used to temporarily put the system or application out of monitoring. You can change the system/application status from up/down to maintenance and from maintenance to up. Status Tracker will not monitor those system(s)/application(s) which are under maintenance. This increases the efficiency of StatusTracker thereby preventing unnecessary polling of system(s)/application(s).

### To change the System/Application status to Maintenance

1. Click the system name/application name dropdown, and click **Change Status**.
StatusTracker displays corresponding **Change Status** window.

2. Click ‘**Maintenance**’ from the **Status** dropdown, and then click **Ok**.

   StatusTracker page displays the system or application status as maintenance.

   ![Figure 68](image)

   ![Figure 69](image)

**To change maintenance status**

1. Select the system/application, which is under ‘**Maintenance**’ status, and then click the dropdown menu.

2. Click **Change Status**.

   StatusTracker displays ‘Change Status’ window.

3. In **Status** dropdown, change the status to **Up**, and then click the **OK** button.
NOTE

The system or application status cannot be changed from maintenance to down. You can use ‘Change Status’ option to temporarily put the system / application out of monitoring. The Maintenance status needs to be Manually ‘Up’.

Change multiple systems status to Maintenance

1. To change multiple systems to maintenance, right click a group and then select Change Status.

2. Select System Name option to change status of all systems or individual systems accordingly.

3. Select Change status from drop down, and then select Up/Down to Maintenance or Maintenance to Initializing accordingly.
4. Select the **Change Status** button. The status of the system(s) is changed.

**Edit Resources**

The system or application resource details can be changed for identification purpose.

1. To edit resources, click the system/application name dropdown, and select **Edit Resource**. StatusTracker displays **Edit Resources** pop-up window.
2. Make the appropriate changes in the respective fields, and then click the **Ok** button.

**View Resource Details**

1. Click the system/application name dropdown, and select **Resource Details**. StatusTracker displays **Resources Details** pop-up window.
2 Click the Ok button.

Polling Summary

Polling summary gives you the system/application status in a specified time period.

1 Click the system/application name dropdown, and select Polling summary. StatusTracker displays Polling summary dialog box.

![Polling Summary Dialog Box](image)
2. Select the duration of polling in **From** and **To** fields, and then click the **Show** button.
3. Click **Export**, if you wish to export the polling summary details in Excel sheet.
4. Click the **Close** button.

**Add Notes**

This option is provided to add extra information about the system or application. For example, it can be used to specify the reason for a system being put under maintenance.

1. Click the system/application name dropdown, and select **Add notes**.
   StatusTracker displays **Add notes** pop-up window.

   ![Add notes pop-up window](image)
   **Figure 78**

2. Enter the system/application relevant details, and then click the **Ok** button.

**Synchronize discovery**

1. To synchronize discovery of the systems and applications with EventTracker tool, select **Admin** drop-down and then select **Manager**.
   Manager Configuration window displays by default.
2. Select **StatusTracker** tab and then select **Synchronize discovery with EventTracker** option.

**StatusTracker Reports**

A StatusTracker report gives you the summary details of monitored system(s) or application(s) activities over a period of time. The results obtained from this report can be used to examine on how many systems/applications are added/deleted/modified, and the status of particular resource in a specific duration.

**To generate Status Tracker Reports Summary**

1. Log on to EventTracker Enterprise, click the **Reports** menu, and then select **Dashboard** or **Configuration**.
2. Click the **New button** in **Dashboard / Configuration**.
3. Select **Operations** tab. In the **Report Tree** pane, expand **EventTracker** node.
4. Select any one of the reports related to Status Tracker.

![Figure 79](image)

Also in **Operations** tab, you can find **StatusTracker Reports Summary** and the screenshot is given below.
### EventTracker: StatusTracker

<table>
<thead>
<tr>
<th>Report</th>
<th>Contains</th>
</tr>
</thead>
<tbody>
<tr>
<td>EventTracker: StatusTracker resource added</td>
<td>The details of system(s)/application(s) added in the group(s)/system(s) within the specified time.</td>
</tr>
<tr>
<td>EventTracker: StatusTracker resources deleted</td>
<td>The details of system(s)/application(s) deleted from the group(s) within the specified time.</td>
</tr>
<tr>
<td>EventTracker: StatusTracker resources down</td>
<td>The details of system(s)/application(s) whose status is 'Down' for a given time period.</td>
</tr>
<tr>
<td>EventTracker: StatusTracker resource group added</td>
<td>The details of the group(s), which are added in the StatusTracker in a given time period.</td>
</tr>
<tr>
<td>EventTracker: StatusTracker resource group deleted</td>
<td>The details of the group(s), which are deleted from the StatusTracker over a given period.</td>
</tr>
<tr>
<td>EventTracker: StatusTracker resource group modified</td>
<td>The details of the group(s), which are modified over a given period.</td>
</tr>
<tr>
<td>EventTracker: StatusTracker resource modified</td>
<td>The details of the resource(s), which are modified over a given period.</td>
</tr>
<tr>
<td>EventTracker: StatusTracker resource up</td>
<td>The details of system(s)/application(s) whose status is ‘up’ for a given time period.</td>
</tr>
<tr>
<td>Application Resources</td>
<td>The details of application(s) for a certain period of time irrespective of their status.</td>
</tr>
<tr>
<td>Report</td>
<td>Contains</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>System Resources</td>
<td>The details of system(s) for a certain period of time irrespective of their status.</td>
</tr>
</tbody>
</table>

5. Select any one of the **Report Type** (i.e. On Demand/Queued/Scheduled/Defined).
   EventTracker displays Reports Wizard window.
6. Click **Next >>**.
7. In the **Interval** pane, select the report duration in **Select interval/Select date range** field.
8. Check the ‘**Limit to time range**’ option to limit the report time range to specified timings.
9. In **More options** pane, select the **Format option** and **Export type** from the respective dropdown.
10. Click **Next >>**.
11. If required, set the **Refine** and **Filter** criteria, and then click **Next >>**.
12. Enter appropriate **Title, Header, Footer**, and **Description** for the report, and then click **Next >>**.
13. Cross check the **Disk cost analysis for the report**, and then click **Next >>**.
14. Click **Generate report**.
   For detail information to generate Scheduled/Defined/Queued/On Demand Reports refer **Reports** chapter.

**Edit Scheduled Discovery**

This option gives more information about status of the system or application.

1. Click **Edit Scheduled Discovery** hyperlink.
   Scheduled discovery information of systems/applications window displays.
2. Select the respective **IP Range** drop-down to **Edit** data.

3. Select the checkbox and click the **view** hyperlink.

   Discovery status information window displays.

4. Select the duration in **From** and **To** fields and then select the **Show** button.

5. Click **Export** icon to export data to excel file.
Chapter 4
Behavior

In this chapter, you will learn how to:

- Monitor Behavior Dashlet
- Add Dashlet
- Analyze Admin/User Activity
- Analyze Application Activity
- Analyze EventID Activity
- Analyze IP Address Activity
- Analyze Logon Failure Activity
- Analyze Network Activity
- Analyze Process Activity
- Analyze Runaway Process Activity
- Analyze Software Activity
- Analyze System Activity
- Analyze USB Activity
- Monitor USB Activity
- Configure Enterprise Activity Behavior Settings
- Manage Behavior Rules
- Add Behavior Rules
Monitor Behavior Dashlet

Manually reviewing and analyzing enterprise wide event log data in order to identify patterns of suspicious behavior is a time consuming and tedious task, which leaves ample room for errors and missed conditions. In order to reliably get the right information, rules have to be defined for anomalous conditions - and these are only as good as the person writing the rules/performing the review. In addition, you have to know what you are looking for to write the rules.

EventTracker addresses this issue with its Enterprise Activity Monitor, a dashboard that automatically provides information about unusual behavior by:

- Continuously monitoring the event log stream
- Performing a combination of statistical and behavioral correlation
- Detecting both new activity and activities that significantly deviate from normal operations

Conditions detected include:

- Abnormally high or low admin and user activity
- Abnormally high or low system, process or IP activity
- First seen for IP addresses, admins, users, processes etc.
- Sudden changes in event volumes

Behavior Dashlets

EventTracker’s behavior dashboard is categorized into Security and Operations. The dashboard provides you dashlets with the predefined set of rules, and allows you to add custom dashlets created with your own rule set. It is left to your discretion to organize the dashlets as per your requirement. The security and operational activities of an enterprise are presented in graphical form in this dashboard. By Default, EventTracker displays the last 24-hour data.

| Security                        | Admin Activity                      |
|                                | Application activity                |
|                                | Event ID Activity                  |
| To monitor security related events | IP address Activity                |
|                                | Logon Failure Activity             |
|                                | Network Activity                   |
| Operations                     | Process Activity                   |
| To monitor anomalies in system performance (CPU, disk, memory), service failures, network connections, printer usage etc. | RunAway Process Activity |
|                                | Software Activity                 |
|                                | System Activity                   |
|                                | USB Activity                      |
|                                | User Activity                     |
|                                | User defined Activities           |
For **Security** and **Operations** behavior, procedure to configure and customize dashlets, volume analysis, and reports generation are same.

The Dashlets are not refreshed automatically. Click the **Refresh** button to refresh the dashlet.

## Add Behavior Dashlets

This option helps to add dashlets to view enterprise behavior. Behavior dashboard displays enterprise activities through default dashlets. Using **Customize** option the behavior dashlets can be added to the dashboard. Also new behavior dashlet can be added by creating custom **Behavior rule**.

### To add Dashlets

1. Log on to EventTracker Enterprise.
2. Click **Behavior** menu, and then click **Security/Operations** tab.
   
   EventTracker displays the Behavior dashboard with default dashlets.

   ![Behavior Dashboard](image)

   Figure 83

3. Click **Security/Operations** drop down and then select **Customize**.
EventTracker displays the Available Dashlets dialog box.

4. Check the required activity option, and then click Add. EventTracker adds the selected dashlet to the dashboard.

Important To Know
- Move the mouse pointer over a pie or the legend to view tooltip.
- Click a pie or legend.
- EventTracker moves you through Enterprise Activity Dashboard.

Reset Personalization

This option helps to reset the dashboard with default dashlets.

1. In Behavior menu, click Security/Operations Dashboard. Click the Reset personalization hyperlink. EventTracker displays the confirmation message box.
2. Click **OK** to reset the dashboard. EventTracker removes the custom dashboard that you have added.

**Volume Analysis**

This option provides a summary of total enterprise activities with respect to **Security** or **Operation**, which provides the distinct count of the activities and the total count of its occurrences. Volume analysis helps to analyze enterprise activity log volume.

1. In the **Behavior** menu, click **Security** or **Operations** dropdown, and then select **Volume Analysis**.

EventTracker displays the **Volume Analysis** dialog box.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Behavior</td>
<td>List of activities. Click Behavior to sort the list in ascending or descending order.</td>
</tr>
<tr>
<td>Unique</td>
<td>Count of unique activities.</td>
</tr>
</tbody>
</table>
Total Count | Total count of occurrences with respect to unique activities.

2 Click the required activity hyperlink to search the selected activity within a specified time range.

3 Select Event ID Activity option, set appropriate time range, and then click Generate.

![Figure 89](image1)

EventTracker displays the consolidated list of activities.

![Figure 90](image2)

4 Click the Print hyperlink to print the report.
Analyse User/Admin Activities

Non-admin User Activities

Following are the Event IDs considered for analyzing non-admin user activities.

<table>
<thead>
<tr>
<th>Windows XP/2003 Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>528, 529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 540, 551, 642, 644, 672, 675, 676, 682, and 683</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Windows Vista/7/8/2008/2012 Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>4624, 4625, 4634, 4647, 4738, 4740, 4768, 4771, 4772, 4778, and 4779</td>
</tr>
</tbody>
</table>

Admin User Activities

Following are the Event IDs considered for analyzing admin user activities.

<table>
<thead>
<tr>
<th>Windows XP/2003 Systems</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Windows Vista/7/8/2008/2012 Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>4670, 4706, 4707, 4714, 4715, 4716, 4720, 4722, 4724, 4725, 4726, 4727, 4728, 4729, 4730, 4731, 4732, 4733, 4734, 4735, 4737, 4738, 4739, 4741, 4742, 4743, 4744, 4745, 4746, 4747, 4748, 4749, 4750, 4751, 4752, 4753, 4754, 4755, 4756, 4757, 4758, 4759, 4760, 4761, 4762, 4764, 4765, 4766, 4767, 4781, 4782, 4783, 4784, 4785, 4786, 4787, 4788, 4789, 4790, 4794, 4865, 4866, 4867, 4907, and 4912</td>
</tr>
</tbody>
</table>

To analyze User/Admin Activity

1. Select the Behavior Menu and then select Security/Operations Dashboard.
2. In View Behavior Details for drop down, select User Activity/Admin Activity.

(OR)

Click the corresponding Pie/Bar/Stacked Bar graph.

EventTracker displays the “Enterprise Activity Detail” page.
• First pane **Activities from** displays activity details and weekly trend of activities
• Second pane **Activities for user** displays top five users by activities
  Options are provided to select number of users and chart type to view
• Third pane **Out of ordinary user occurrence** displays out of ordinary user activities, helps to monitor abnormal user activities
• Fourth pane **New users observed** displays new user activities
• **Left pane** displays the list of configured behavior rules
  A. Click a hyperlink in the alphabetical list.
  (OR)
  Type the search phrase in the search field, and then click **Search** icon
  EventTracker displays the list of searched criteria.
Log Search

To do a Log Search, move the mouse pointer over a field in User Name column/Event ID/top right hand side corner. From the drop down, click Log Search.

![Figure 93](image)

For more details regarding Log Search, refer Log Search.

Add to filter list

This option helps to filter or ignore activities for the specified entity.

A. In the left panel, click the corresponding User Name drop down, select Add to filter list.

![Figure 94](image)

Behavior filter list window displays.
B. Select the required option and then click the **Save** button.

### Analyze Application Activity

This option helps you analyze Application activity.

1. To analyze **Application Activity**, click pie chart to view application activity details per system.

```
Figure 96
```

OR

From **View behavior details for** dropdown, select **Application Activity** option, and then click 📊 icon. EventTracker displays the ‘**Enterprise Activity Detail**’ page.
Analyze EventID Activity

This option helps you analyze events by occurrence.

1. To analyze events by occurrences, click the **Event ID Activity** pie chart to view per event activity details.

![EventID Activity Pie Chart](image)

Figure 97

OR

From **View behavior details for** dropdown, select **Event ID Activity** option, and then click the ➡️ icon. EventTracker displays the ‘**Enterprise Activity Detail**’ page.

Analyze IP Address Activity

This option helps you analyze per IP trend of events.

IP address is extracted from the **Event Description**. If the extracted string matches the loopback address '127.0.0.1' or local system IP '0.0.0.0' then it is filtered out. Otherwise, it is considered as a valid IP address.

1. Click the **IP Address Activity** pie to view behavior details for IP address activities.
From View behavior details for dropdown, select IP Address Activity option and then click the icon.

EventTracker displays the "Enterprise Activity Detail" page.

By default, IP Class dropdown displays all IP addresses.
2. To view only Private or Public IP addresses, click the **IP Class** drop-down and then select **Private** or **Public** respectively.

3. To do a **Log Search**, move the mouse pointer over a row on the left pane or a row in the third and fourth panes. From the drop-down list, click **Log Search**.

   EventTracker opens the **Log Search** browser with query results.

3. Click **Classification** hyperlink.

   All private IP addresses are displayed.
4 Select any private IP address and then click **Update**.

5 Click **Resolve all IPs** hyperlink to get the DNS (Domain Name System) lookup for the respective IP addresses.

   EventTracker displays the confirmation message box.
6 Click OK to proceed further.

EventTracker starts resolving the IP addresses. Use the Stop hyperlink to abort the action. Once resolved, the DNS names will be reflected in the list.

7 Click the IP address dropdown in the left pane/ third pane/ fourth pane, and then select Whois. Whois option is provided to resolve WAN IP addresses and to know the owner details.
EventTracker moves you through the 'DomainTools' Web site.

**Figure 104**

Analyze Logon Failure Activity

This option helps you analyze log on failure events.

Event ID's considered under this activity are
Whenever these events are received, username is extracted and its count is maintained.

1. To analyze logon failure events, click the **Logon Failure Activity** pie chart to view per log on failure activity details.

   ![Logon Failure Activity Pie Chart](image)

   **Figure 105**

OR

From **View behavior details for** dropdown, select **Logon Failure Activity** option, and then click the icon.

EventTracker displays the ‘**Enterprise Activity Detail**’ page.

### Analyze Network Activity

This option helps you analyze network activities.

Event ID considered under this activity is **3223**. Whenever 3223 event is received, remote IP address and remote port information is extracted from the event, and its count is maintained.

1. Click the **Network Activity** pie chart to view the activity details of devices like printers, routers over the respective network.
From View behavior details for dropdown, select Network Activity option, and then click the icon. EventTracker displays the "Enterprise Activity Detail" page.

Analyze Process Activity

This option helps you analyze per user per system process utilization.

Event IDs 592 (non-Vista systems) and 4688 (Vista systems) are considered for process activity. Information like process name, process id, user name, domain name, and computer name are extracted from the 'Event Description'.

1. To analyze process by occurrence, click the Process Activity pie chart to view process utilization activities details.
OR

From View behavior details for dropdown, select Process Activity option, and then click the icon. EventTracker displays the Enterprise Activity Detail page.

Analyze Runaway Process Activity
This option helps you analyze runaway processes.

Event IDs considered under this activity are 3217 and 3218.

Whenever 3217 and 3218 events are received, process and system names are extracted and its count is maintained. Left pane would list the process names and right pane would list two counts for that process, one for high memory usage and one for high CPU usage.

1. To analyze Runaway process activity, click the RunAway Process Activity pie chart to view per runaway process activity details.

OR

From View behavior details for dropdown, select RunAway Process Activity option, and then click the icon.
EventTracker displays the Enterprise Activity Detail page.

Analyze Software Activity
This option helps you analyze software activity.

Event ID considered under this activity is 3208. Whenever 3208 event is received, software name and system name are extracted from the event, and its count is maintained. Left pane would list the software's and right pane would give breakup for software by system name and count.
1. To analyze software activity, click the **Software Activity** pie chart to view the software activity details per system.

![Software Activity Chart](image)

**Figure 109**

OR

From **View behavior details for** dropdown, select **Software Activity** option, and then click the icon.

EventTracker displays the **Enterprise Activity Detail** page.

### Analyze System Activity

This option helps you analyze activities occurred at systems. System name is extracted from ‘Event Properties’.

1. Click the **System Activity** pie chart to view the details of system activities in an enterprise.
OR

From View behavior details for dropdown, select Software Activity option, and then click the icon.

EventTracker displays the ‘Enterprise Activity Detail’ page.

Analyze USB Activity

This option helps you analyze USB activity.

Event ID considered under this activity is **3221**. Whenever 3221 event is received, application and system names are extracted from the event, and its count is maintained. Left pane would list the applications and right pane would give breakup for each application by system name and count.

1. Click the **USB Activity** pie chart to view USB activity details per system.
OR

From View behavior details for dropdown, select **USB Activity** option, and then click the 📦 icon. EventTracker displays the "**Enterprise Activity Detail**" page.

Monitor USB Activity

EventTracker provides advanced monitoring and analysis of the usage of these devices including:

- Tracking Insert/Removal
- Recording all activity (file writes to)
- Disabling according to predefined policy

With EventTracker, you can, for example:

- Set a policy that permits only certain devices to be used on servers
- Continuously monitor all USB usage on workstations
- Alert in real-time on the insertion of devices
- Block a specific device, if necessary
- Record all files that a user is writing to the USB

Included in the EventTracker Reports Engine are pre-packaged reports that can display all USB activity, including:

- Who the user was,
- What type of device was used
- What files were copied to the device

A complete inventory is captured that can be used for real-time analysis as well as a powerful forensic tool.

For more information, please refer the **System Monitor** section.
Chapter 5 Dashboard

In this chapter, you will learn how to:

- Keyword Indexed Dashboard
- Security Dashboard
- Operations Dashboard
- Compliance Dashboard
Keyword Indexed Dashboard

The Keyword Indexed Dashboard is designed to provide a big canvas for the user to add custom dashlets in the dashboard. The user is allowed to use standard columns (i.e. Event ID, Event User, Computer, Event Source, Domain, Event Type, and Event Log Type) / category / keywords to configure the dashlets to be added in the dashboard. The selected keywords/standard columns will be displayed as a trend graph in the dashboard.


The process to configure and customize the dashlets is identical for Security and Operations dashboard. For Compliance dashboard, the dashlets cannot be configured and customized. It displays %$%$%^%^ in the in-built dashlets.

Features of keyword indexed dashboard:

- User can edit or delete the configured keyword dashlets.
- A customized selection of standard column properties or keywords or categories can be used to create a dashlet.
- The configured dashlets can be viewed by different graph types. The zoom preview of graph is also possible.
- The graph will take you to log search page for the selected entity.
- Dashlets configured in Security/Operations are made available to all the users' enterprise wide and those configured in My EventTracker is made available to a user who has created them.

<table>
<thead>
<tr>
<th>Click</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Zoom Icon]</td>
<td>Zoom the graph.</td>
</tr>
<tr>
<td>![Edit Icon]</td>
<td>Edit the Dashlet.</td>
</tr>
<tr>
<td>![Minimize Icon]</td>
<td>Minimize the Dashlet.</td>
</tr>
<tr>
<td>![Maximize Icon]</td>
<td>Maximize the Dashlet.</td>
</tr>
<tr>
<td>![Dismiss Icon]</td>
<td>Dismiss the Dashlet.</td>
</tr>
</tbody>
</table>

Security Dashboard

This option helps to view quick statistics like trend of events occurred and summary on event categories.

1) To view Security Dashboard, click Configure.
Configure dashlets window displays.

2) Enter a Title.

There are 3 options provided i.e. Trending, User Defined, Category.

3) In Trending tab, expand the plus symbol and select any one of the options (i.e. Computer, Domain, Source, User, Event ID, Event Type, and Log Type). Select Configure.

4) In User Defined Tab, enter the required fields (i.e. Event ID, Event Source, Computer, Domain, Event Type, Log Type, and User) and select Configure.
5) In **Category** tab, select any one of the Category and then select **Configure**.
6) Select **Customize**.

7) Add the required option in **Available Dashlets**. Select **Add**.

![Available Dashlets](image)

**Figure 116**

After necessary configuration, security dashboard displays a graph of events.

![Security Dashboard](image)

**Figure 117**

**Reset Personalization**

1) Click **Security/Operations** drop down, select **Reset Personalization**.

All configuration selected will be removed.

**Operations Dashboard**

This works in a similar fashion like Security Dashboard and the options are the same. To configure, customize or reset personalization please refer the steps addresses for Security Dashboard.
Compliance Dashboard

The Compliance dashboard consists of Incidents, Compliance Reports, Flex Reports and Config Assessment.

Incidents
To view data for incidents in Compliance Dashboard, configure an alert as mentioned in Alerts chapter (Topic: To add custom alerts).

Compliance Reports
A summary of reports that are configured in Reports Menu -> Configuration -> Report Groups -> Compliance is displayed here. Please refer Reports Menu -> Compliance Reports.

Flex Reports
A summary of reports that are generated in Reports Menu -> Configuration -> Report Groups -> Flex is displayed here. Please refer Reports Menu -> Flex Reports.

Config Assessment
A summary of reports that are generated in Config Assessment -> Reports is displayed here.
Chapter 6
Netflow

In this chapter, you will learn about:

- Netflow Receiver
- Interpret Netflow
About Netflow

A Cisco-proprietary IP statistics collection feature that collects information on IP flows passing through a router.

Source:

For more information, click

Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Differentiated Services</td>
<td>Differentiated Services (DiffServ) is a new model in which traffic is treated by intermediate systems with relative priorities based on the type of services (ToS) field. The six most significant bits of the DiffServ field is called as the DSCP. Source: <a href="http://www.cisco.com/en/US/tech/tk543/tk757/technologies_tech_note09186a00800949f2.shtml#dscpandassuredforwardingclasses">http://www.cisco.com/en/US/tech/tk543/tk757/technologies_tech_note09186a00800949f2.shtml#dscpandassuredforwardingclasses</a></td>
</tr>
<tr>
<td>Code Point (DSCP)</td>
<td></td>
</tr>
<tr>
<td>Input logical interface</td>
<td>One of the first things to learn, when you are dealing with SNMP, is ifIndex. This is a primary key of all objects. Consider it a way that all of the interfaces (physical and logical) are broken down and assigned a value. This value is assigned during boot up of a device, and it may not be changed. If any information needs to be polled for that particular interface, it must use that assigned value. Source: <a href="http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080157626.shtml">http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080157626.shtml</a></td>
</tr>
</tbody>
</table>

EventTracker Netflow Analyzer

EventTracker Netflow Analyzer is a Netflow collector, analyzer, and reporting engine integrated together. ‘EventTracker Netflow Analyzer’ helps you gain in-depth visibility into your network traffic and its patterns, thus empowering you to investigate, troubleshoot, and quickly remediate network slowdowns.

- Monitor network traffic per interface
- Configure Netflow Collector with minimal effort, visualize near real-time network traffic
- Break-up summary with visual charts to quickly and easily identify top talkers, applications, and protocols hogging network bandwidth
- Network traffic reports with just a few clicks
- Long-term retention of Netflow data for trending and capacity planning
- Cost effective
Benefits

1. **Identify what applications comprises the network traffic**
   - a. Analyze statistics about every single application routed through the network interface
   - b. Compare application usage patterns
   - c. Determine potential root causes of network performance problems
   - d. Prioritize applications based on ToS (Type of service).

2. **Identify top conservationists**
   - a. Identify hosts (clients, servers, networked devices, and so on) conversed using applications
   - b. Isolate top talkers that impact business-critical applications

3. **Gain visibility across ports**

4. **Understand bandwidth utilization and growth.**
   - a. Understand how bandwidth and application utilization grows over time
   - b. Plan for future capacity requirements
   - c. Make informed decisions regarding bandwidth upgrades by trending application growth on particular interfaces

---

**Enable EventTracker Netflow Receiver**

This option helps to enable 'EventTracker Netflow Receiver' to collect Netflow logs.

1. To enable Netflow receiver, log on to **EventTracker Enterprise**. Click **Admin** dropdown, and then click **Manager**.
2. Click the **syslog / Virtual Collection Point** tab. In ‘Virtual Collection Points’ pane, click **Add**.

   EventTracker displays the **Receiver Port** pop-up window.

![Receiver Port](image)

---

*Figure 118*
3 Add appropriate port details, and then click **Save**.

---

**NOTE**

This port must be exclusive to the Direct Log Archiver to archive Netflow logs.

---

4 Click the **Direct Log Archiver / Netflow Receiver** tab.

5 Check the **Direct log file archiving from external sources** option.

6 From the **Associated virtual collection point** drop-down list, select the port that you have added earlier.

   Example: Port number 9995

7 In the **Netflow data storage folder** field, type the path of the folder where Netflow logs are dumped.

   (OR)

   Click the **Browse** button to select the folder.

   You can use the default ports or add ports to collect Netflow logs. Default netflow data storage folder can be used for the newly added ports.

8 Click **Save**.

   To collect Netflow data, EventTracker creates a netflow system instance once you enable netflow receiver.

9 To view detail information on all domain computers, click **Admin** dropdown, and then click **Manager**.

10 Select **Systems**.

   Systems manager displays all domain computers with Netflow data.
Interpret Netflow Data

This option helps to view and interpret Netflow logs collected by EventTracker Netflow Receiver.

1. Click **Netflow** menu.

   EventTracker displays the **Conversations** tab on the Netflow Dashboard, provides historical trends conversations happened between network interfaces.

   ![Figure 120](image-url)

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP</td>
<td>Interface IP from where the conversation originated.</td>
</tr>
<tr>
<td>Destination IP</td>
<td>Interface IP to where the conversation is destined for.</td>
</tr>
<tr>
<td>Application</td>
<td>Application that was used.</td>
</tr>
<tr>
<td>Port</td>
<td>Port through which the communication happened.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol that was used to carry on the conversation.</td>
</tr>
<tr>
<td>DSCP (Differentiated Services Code Points)</td>
<td>DSCP is a 6 bit value. The six-bits of the DS field are used as a code point to select the PHB (Per Hop Behavior) a packet experiences at each node.</td>
</tr>
<tr>
<td>Traffic</td>
<td>Aggregation of bytes between the source and destination during a specified period of time.</td>
</tr>
</tbody>
</table>
2. **Click Application tab.**

   Provides historical trends of applications used.

   ![Figure 121](image)

   **Table 1: Top 10 Applications**

<table>
<thead>
<tr>
<th>Application Name</th>
<th>Port</th>
<th>Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown</td>
<td>24</td>
<td>353.9 GB</td>
</tr>
<tr>
<td>Unknown</td>
<td>26</td>
<td>350.87 GB</td>
</tr>
<tr>
<td>Unknown</td>
<td>45</td>
<td>346.15 GB</td>
</tr>
<tr>
<td>Remote File (RIP) — used to transfer files between machines</td>
<td>34</td>
<td>345.37 GB</td>
</tr>
<tr>
<td>Telnet protocol — unencrypted fast communications</td>
<td>23</td>
<td>348.14 GB</td>
</tr>
<tr>
<td>Management Utility</td>
<td>2</td>
<td>348.12 GB</td>
</tr>
<tr>
<td>nameserver, ARPA Host Name Server Protocol</td>
<td>42</td>
<td>323.4 GB</td>
</tr>
<tr>
<td>DAYTIME — (RFC 867)</td>
<td>43</td>
<td>322.29 GB</td>
</tr>
<tr>
<td>Unknown</td>
<td>44</td>
<td>320.76 GB</td>
</tr>
</tbody>
</table>

3. **Click Protocol tab.**

   Provides historical trends of protocols used.
4. Click Traffic Destination tab.

Provides historical trends of destination to where the traffic destined for.

![Traffic Destination Tab](image1)

**Figure 122**

![Traffic Destination Data](image2)

**Figure 123**
5. Click **Traffic Source** tab.

   Provides historical trends of source from where the network traffic originated.
6. **Click Utilization** tab.

Provides historical trends of utilization of network interfaces.
7. Click **Volume** tab.

Provides historical trends of volume of traffic that happened through network interfaces.

![Figure 126](image-url)
Chapter 7
Search

In this chapter, you will learn about:

- Basic Search
- Advanced Search
Search Logs

EventTracker Log Search is Google like search facility available for quick search of events, it supports simple string search to parameterized search.

Searching can be done based on following Tags i.e. Log Type, Event Type, Category, Event ID, Source, Domain, System, User. Searching can be done in two methods

- Basic Search
- Advanced Search

Details regarding Basic Search and Advanced Search are mentioned below.

For detail information, refer Log Search.
Chapter 8
Reports

In this chapter, you will learn how to:

- Reports Dashboard
- Reports Configuration
- Generate different reports
  - On Demand
  - Queued
  - Scheduled
  - Defined
- Security/Operations/Compliance/Flex Reports/Alphabetical
- Reports Exception
- Reports Status
- Report Calendar
- Refine and Filter Option
- Enterprise Feeds
- Explorer
- Flex History
- Analytics
- Configure EventVault Explorer to use Remote SQL Server
Reports Dashboard

It displays all the reports generated in Alphabetical, Security, Compliance and Flex Reports.

1. Click the Reports menu, and then click Dashboard.

   EventTracker displays the ‘Reports Dashboard’ page. In the left pane, Status Graph displays a graph showing Status of the reports, Generated By the respective Reports (Alphabetical/Security/Operations/Compliance/Flex Report).

2. Click the New button to generate the respective reports.
The details to generate different Report Types in Security/Operations/Compliance/Flex Reports/Alphabetical is explained in the next section.

3 Click the respective PDF, Word icon to view detail report in Word or PDF format. The second column displays the status of report.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🚫</td>
<td>No record found</td>
</tr>
<tr>
<td>🔄</td>
<td>Processing report</td>
</tr>
<tr>
<td>✅</td>
<td>Report generated successfully</td>
</tr>
<tr>
<td>⚠️</td>
<td>Failed to generate report</td>
</tr>
<tr>
<td>✗</td>
<td>Cancelled report</td>
</tr>
</tbody>
</table>

4 Click the Flag 🚫 icon to change the status of the report.
### Flag icon and Description

<table>
<thead>
<tr>
<th>Flag icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRAY</td>
<td>Un-flagged and no action has been taken</td>
</tr>
<tr>
<td>RED</td>
<td>Flagged and relevant action is required for that particular incident to solve an issue</td>
</tr>
<tr>
<td>GREEN</td>
<td>Checked the report and necessary action has been taken care of</td>
</tr>
</tbody>
</table>

### Field and Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Name of the report</td>
</tr>
<tr>
<td>Type</td>
<td>Formatting option of the report</td>
</tr>
<tr>
<td>Generated By</td>
<td>Type of report On Demand/Scheduled/Queued/Defined</td>
</tr>
<tr>
<td>Generated on</td>
<td>Date and time when the report was generated</td>
</tr>
<tr>
<td>Size(kb)</td>
<td>Size in KB of the report</td>
</tr>
<tr>
<td>Report Status</td>
<td>Status of the report such as Success, Failed, No data and Cancelled</td>
</tr>
</tbody>
</table>

5. Click **Info** icon to view **Report Details** and **Exception Details**. Report details window displays by default.
a. Select **Use Configuration** drop-down, select **Create defined report** or **Create scheduled report**.
b. Click **Go** hyperlink.
c. Click **Exception Details** to view details about the exceptions generated.
d. Click **Flag for Follow up** icon to add more information. Notes window displays.
e. Enter relevant data in **Notes** and **Add flag/clear note:** and click the **OK** button.

6. Click on **Title** hyperlink to view details about the report in **PDF, Word, HTML** format etc. Summary Report Details window displays.

7. Click **Export** icon to export data to excel.

8. Click **Log Book** icon to update data in Log Book.

A logbook message displays.

a) To add a new logbook entry, click the **Add new** button.

b) To add to an existing logbook, click the **Add to existing** button.

Log Book window displays.
Enter relevant data and then click **Save**.

For detail information about Log Book refer hyperlink.

9. Click **Notes** icon to add comments about a particular report.
10. Select any option and then select the **Delete** button to delete a report from the **Dashboard** view.
11. To view data about **Reports** in Calendar, click **Report Calendar** icon.
13. To search any report, enter relevant data in Search textbox and then click the **Search** button.
14. To perform an advance search, click the **Advance Search** icon. Advance Search window displays.

---

Figure 132

---

15. Enter/select relevant data and then click the **Search** button. Relevant data is displayed based on the search criteria.

---

**Reports Configuration**

This gives a status view of all the reports that have been generated via Scheduled/Queued/Defined.

1. Select **Scheduled/Queued/Defined** option to generate the respective reports and then click the **New** button.
2. To view the respective **Security/Operation/Compliance/Flex Reports** that are configured, click the respective **Report groups**.
3. To rename or delete a group in **Reports Configuration** tree, right-click any group, select **Rename Group** or **Delete Group** accordingly.
4. To email a report, click Email icon.

5. Select any report option and then click Information icon to view the report details and exception details.

6. Enter/select the required options to generate Scheduled/Queued/Defined reports.

7. Select any report option and then click the Run Now icon to run the respective Scheduled/Queued/Defined reports.

8. Select the Scheduled drop-down to run the report All / Daily / Twice Daily / Hourly / Weekly / Once in a week.

9. To search for a report, enter the search criteria and click the Search button.

10. To delete a report, select any report and then select the Delete button.

11. To view data about Reports in Calendar, click Report Calendar icon.

12. To view status about Reports, click Report Status icon.

Security/Operations/Compliance/Flex Reports/Alphabetical Reports

1. Click the Reports menu, and then select Reports Configuration.

2. Select the New button.
   EventTracker displays the Reports page.

3. Select the required Security/Operations/Compliance/Flex reports /Alphabetical tab.

4. Select the required Report type i.e. On Demand, Queued, Scheduled, Defined.

5. Click Next>> and proceed further to generate a report.
   Details to generate On Demand, Queued, Scheduled, Defined reports is explained in below.

Security

Reports that show the occurrence of various security related events across systems, devices, and applications. These may be generated and reviewed on a regular schedule to pinpoint potential risks or breaches.

Security reports are useful to decisively counter the internal and external security threats.

Operations

System health monitoring is an important benefit of event log management. These reports are useful to observe anomalies in system performance (CPU, disk, memory), service failures, network connections, printer usage etc.
Compliance

Reports that show the compliance posture of enterprise assets, and are helpful to demonstrate alignment with standards.

Flex Reports

Flex Report is a client-side report generation component. It provides detail information about log, log volume, alerts, suspicious network traffic and cost saving reports.

To generate Alphabetical Reports

1. Log on to EventTracker Enterprise, click the Reports menu, and then select Dashboard or Configuration.
2. Click the New button in Dashboard / Configuration.
3. Select any one of the Compliance / Security / Operations / Flex reports / Alphabetical tab.
4. Click the alphabet hyperlink to view appropriate Category/Report/Flex Report list.

(OR)
Type the search phrase in the search field, click the **Search in current alphabet** checkbox, and then click **Search**.

Example: alert

NOTE

*Search in current alphabet* checkbox is not enabled when you click **All** hyperlink.

EventTracker displays the Category/Reports/Flex Report searched for.

(OR)

5 Select a **Category/Report/Flex Report** from Report name column.

6 Click **Next>>**.

EventTracker displays the Reports Wizard. To generate **On Demand, Queued, Scheduled and Defined** reports are explained in detail in the next section.

NOTE

You can also add Category/Reports/Flex Report to the favorites list. To do this select a Category/Reports/Flex Report and then click **Add to favorites**.

Similarly you can generate Security, Operations, Flex and Compliance Reports

To generate On Demand Reports

**On Demand** reports can be generated in the foreground and background as well. Reports that are generated in the foreground are called **On Demand** reports. Reports that are generated in the background are called **Queued** reports (explained in the next section).

1 Log on to EventTracker Enterprise, click the **Reports** menu, and then select **Dashboard** or **Configuration**.

2 Click the **New button** in **Dashboard / Configuration**.

3 Select any one of the **Compliance / Security / Operations / Flex reports / Alphabetical** tab.

4 Expand the **Report Tree** node and select any report.

5 Select **Report Type** as **On Demand**.

(OR)

Right click the respective report and then select **On Demand**.

6 Click **Next**.

For Example: In **Operations** menu, select **All Error Events**. **Report Type** selected is **On Demand**.
EventTracker displays the Reports Wizard.

**Figure 136**

**Figure 137**

This wizard is designed to simplify the report generation and scheduling process by guiding you through a set of steps. You select the report type, the systems, the time period, and options and the data filters (if any).

Reports can be generated in PDF, HTML, or WORD formats. After the criteria are selected, the wizard presents an estimate of disk cost and time required for report generation. The estimate is based on past data.

To continue, click Next.
7 Click **Next >>**.
8 Select the required options (like **Sites, Group, Systems, Show all sites, All Systems**).
9 Select **Realtime** or **File Transfer** and then click **Next>>**.


**Figure 138**

10 Select the required **Interval** and **Limit to time Range option**.
11 Select the required **Format option** (i.e. **Summary, Extended Summary, Detail, Trend Report**).
12 Select the required **Export Type** (i.e. **PDF file, Word Document, HTML file, Quick View (not saved on hard disk)**).
13 Select the required **Chart Type** (i.e. **Pie, Bar, Line graph**).
14 Select **Sort by Computer or User**.
15 Click the Next>> button.
16 Enter the appropriate Refine and Filter details.

17 Click the Next>> button.
18 Enter the relevant Title, Header, Footer, and Description data.

![Figure 141](image)

19 Click the Next>> button.

Review cost details and configure the publishing options window displays.

**NOTE**

Publishing options are disabled because On Demand (foreground processing) has been selected.
20 Click the **Next>>** button.

The last step of **Completing Report Configuration Wizard** displays.

21 Select **Override indexer** if required, and then select **Generate Report**.

On enabling override indexer, the indexer will not be used for filtering the cabs and all cabs will be searched for data.
OR
To make any other modifications click **Cancel** to exit the Wizard or **<<Back** to revert to previous wizard window.

**Generating reports** window displays initializing report queue and displays the summary of report generated.

![Figure 144]

22. To export data to PDF/Word/HTML, click **Export** drop-down.
23. Click **Export** icon to export data to view data in **Reports Dashboard**.

![Figure 145]

24. Select any one of the **System Group\Computer** hyperlink to view detail information.
To generate Queued Reports

Reports that are generated in the background are called Queued reports.

1. Log on to EventTracker Enterprise and then click the Reports menu.
2. Click the New button in Dashboard / Configuration.

**NOTE:**

If you select Queued in Reports Configuration, all queued reports are displayed with results and their status. To run any report, click Run Now icon.
3. Select any one of the Compliance / Security / Operations / Flex reports / Alphabetical tab.

4. Expand the Report Tree node and select any report. Select any Report Type as Queued. Click Next.

   For Example: In Compliance Report Tree, select Acceptable Use, Security: Logon failure events. 
   Report Type selected is Queued.

   EventTracker displays the Reports Wizard.

5. Select system(s) or group(s) for report and then click Next>>.

6. Select report duration on which period the report needs to be generated.

7. Select the appropriate Interval, Format option, Export type, Chart type and Sort by Computer or User.
8. Enter appropriate **Refine and Filter** options.

9. Click **Next>>**.

10. Enter the appropriate **Title, Header and Footer details**. Click **Next>>**.

11. To send results via E-mail, select **Enable publishing option**. Enter the correct E-mail address.

12. Select **Update status via RSS** feed drop down. Click **Next>>**.

   For more information regarding RSS Feed refer [RSS Feed](#).

The last step of Reports Wizard displays.

![Figure 149](image-url)

13. Select **Override indexer** if required, and then select **Add to Queue**.

   On enabling override indexer, the indexer will not be used for filtering the cabs and all cabs will be searched for data.

   The report is added to the queue and generated appropriately.

### To generate Scheduled Reports

**Scheduled reports** are used when you want to generate reports on specified date, time.

1. Log on to EventTracker Enterprise and then click the **Reports** menu.

2. Click the **New button** in **Dashboard / Configuration**.

3. Select any one of the **Compliance / Security / Operations / Flex reports / Alphabetical** tab.

4. Expand the **Report Tree** node and select any report.
5 Select any Report Type as Scheduled
(OR)
Right click the respective report and then select Scheduled.

6 Click Next.
For Example: In ‘Flex Reports’ Report Tree, select Logs, select Summary. Report Type selected is Scheduled.
EventTracker displays the Reports Wizard.

7 Select the required category / properties of events.

8 Select the appropriate options in Select system(s) or group(s) for report and then click Next>>.

9 Select duration for the report. Select the appropriate Schedule options, Format option (Standard Rule, Parsing Rule, Token Template), Export type, Sort by Computer or User.

![Log Summary - Report Wizard](image)

Figure 150

Parsing Rule and Token Template is explained in detail in Parsing Rules.

10 Click Next>>.

11 Select the required Refine and Filter Details.

12 Click Next>>.

13 Enter the appropriate Title, Header and Footer details. Click Next>>.

14 To send results via E-mail, select Enable publishing option. Enter the correct E-mail address.

15 Select Update status via RSS feed drop down. Select Show in Compliance Dashboard.
To know more about RSS feed please refer chapter RSS Feeds.

16 Click Next>>.

The last step of Report Configuration wizard displays.

17 Select Schedule.
The corresponding report displays in Reports Configuration.

To generate defined reports

Defined reports are used to generate the reports immediately.

1. Log on to EventTracker Enterprise and then click the Reports menu.
2. Click the New button in Dashboard / Configuration.
3. Select Defined, and then select the New button.
4. Select any one of the Compliance / Security / Operations / Flex reports / Alphabetical.
5. Expand the tree node, select any report, and then select Defined.
   (OR)
   Right click the respective report and then select Defined.
   For Example: In Flex Reports, select Logs Trend.
6. Select the Next button.
EventTracker displays the Reports Wizard.

![Figure 154](image)

7 **Select an event category or custom properties** option as per the requirement.

a) If **Select an event category** is checked, then click **Select Category** hyperlink.

![Figure 155](image)
Categories window displays.

Figure 156

b) Select **Name** option to select all categories or any one of the respective categories, and then select the **OK** button.

In this example, all categories are selected.
(OR)

i. **Select custom properties.**

ii. Enter the relevant **Event Type, Event id, Match in Source and Log Type.**

- **Click Next>>.**
- **Select system(s) or group(s) for report** and then click **Next>>.**
• Select the duration of the report.

• Select the required **Refine** and **Filter (Exclude)** details, and then click **Next>>**.
• Enter the appropriate **Title, Header and Footer details**. Click **Next>>**.

• In the last step of Report Configuration Wizard, select **Save**.
The corresponding report displays in **Security window**.

• To view report details, click the corresponding **Title** in **Security window**. Click **Next >>**.

• Verify the report details and then click **Save**.

### Enterprise Feeds

Enterprise Feeds can be configured and linked with Compliance, Security, and Operations Reports to send RSS notifications when the Scheduled Reports are generated. Any user can use these feeds and can also be linked with My EventTracker Reports.

1. Log on to **EventTracker Enterprise**.
2. To view Enterprise Feeds, click the **Admin** dropdown, and then click **RSS**.
   
   EventTracker displays the "RSS Feeds" page.
   
   For more information of configuring Enterprise Feeds, refer chapter **RSS Feeds**.
Reports Wizard

Reports Wizard has been designed to simplify the report generation and scheduling process by guiding you through a set of steps. You can select the report type, the systems, the time period and options and the data filters (if any).

Reports can be generated in PDF, HTML or WORD formats.

After the criteria are selected, the wizard presents an estimate of disk cost and time required for report generation. The estimate is based on past data.

Reports Exceptions

Exceptions that occurred during report generation are displayed in this page. You can also add and clear follow up notes for the exceptions.

Exceptions are raised under the following circumstances:

- Report generation fails.
- Report-processing time exceeds maximum allowed time (1 hour).
- E-mail fails.
Refine & Filter Options

Refine and Filter options in the Reports Wizard helps you to narrow down your filtering criteria while configuring reports.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Refine:</strong> Use this option if you are looking for specific information.</td>
<td>This field can take multiple strings separated by</td>
</tr>
<tr>
<td><strong>Match for User(s)</strong></td>
<td>This field can take multiple strings separated with &amp;&amp; or</td>
</tr>
<tr>
<td><strong>Filter (Exclude):</strong> Use this option if you want to ignore specific information.</td>
<td>Type the user names to exclude from report generation.</td>
</tr>
<tr>
<td><strong>Filter User(s)</strong></td>
<td>Type the information that you want to filter out in this field. Example- Suppose you want to generate software usage for a use and want to exclude all Microsoft applications from the report. Just enter Microsoft in this field.</td>
</tr>
<tr>
<td><strong>Filter specific information</strong></td>
<td>Use this option if you do not wish to see specific Event Id(s) or Event Source(s)</td>
</tr>
<tr>
<td><strong>Filter Event Id(s)</strong></td>
<td>Enter the Event Id(s), which you do not wish to see in the report. Use</td>
</tr>
<tr>
<td><strong>Filter Event Source(s)</strong></td>
<td>Enter the Event sources (s), which you do not wish to see in the report. Use</td>
</tr>
</tbody>
</table>
Report Calendar

Report Calendar helps you view the time slots occupied by the scheduled reports & scheduled analyses and to use the free slots efficiently for new schedules. Exploiting the free time slots enhances the performance of reports engine, which ultimately speeds up the report generation. Report Calendar displays the time slots of the current week starting from Monday through Sunday.

To access Report Calendar

1. Click Report Calendar icon.

EventTracker displays the Report Calendar in a pop-up window.

![Report Calendar](image)

**Figure 161**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>Select a frequency from this drop-down list to view respective reports.</td>
</tr>
<tr>
<td>Time range</td>
<td>Click to view reports scheduled in that time slot.</td>
</tr>
<tr>
<td>Day</td>
<td>Click to view reports scheduled on that day.</td>
</tr>
<tr>
<td>Show reports</td>
<td>EventTracker selects this checkbox and displays all reports schedules. Clear this checkbox and EventTracker displays only the reports schedules.</td>
</tr>
</tbody>
</table>
To view scheduled reports in time slot

1. Click the hyperlinks under **Time range**.

   EventTracker displays the reports / flex scheduled in that time slot.

![Scheduled Reports - Windows Internet Explorer](image)

**Figure 162**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Title of the scheduled reports</td>
</tr>
<tr>
<td>Type</td>
<td>Type of the scheduled reports</td>
</tr>
<tr>
<td>Frequency</td>
<td>Frequency of the report generation</td>
</tr>
<tr>
<td>Scheduled Time</td>
<td>Date and time set for report generation</td>
</tr>
<tr>
<td>Configured By</td>
<td>Name of the user who configured the report</td>
</tr>
<tr>
<td>Comments</td>
<td>View read-only comments entered by the user.</td>
</tr>
<tr>
<td></td>
<td>🟠 indicates no comment had been entered by the user.</td>
</tr>
<tr>
<td></td>
<td>🟢 indicates the user had entered comments.</td>
</tr>
</tbody>
</table>
2 Click in Comments column.
3 Enter the relevant comments and then click Close.
4 Click 📝 in the Comments column.
   EventTracker displays read-only Schedule Comments.

To view scheduled reports on a particular day

1 To view scheduled reports on a day, click the name of the day.
   EventTracker displays the reports scheduled on that day.
2 To view scheduled reports on a particular day and a time slot, click the links at the intersection of
   Time range and Day.
   EventTracker displays the reports scheduled on that day and time slot.

Report Status

Report snapshot displays the Overview and Queue status of the reports and flex irrespective of the
Collection Point Site. Report Status shows the status of all reports generated in
Security/Operations/Compliance/Flex Reports via On Demand, Queued, and Scheduled types.

1 Click the Report Status 📊 icon.
   EventTracker displays the Report Status Snapshot pop-up window.
### Active Users
No of user logged on to EventTracker.

### User
Select a user from this drop-down list to view the count of all reports configured by that user. EventTracker populates this drop-down list only when the logged in user has Admin privilege.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Name of the report / flex report</td>
</tr>
<tr>
<td>User name</td>
<td>Name of the user who configured the report / flex report</td>
</tr>
<tr>
<td>Queue type</td>
<td>Says whether report is Queued or On Demand.</td>
</tr>
<tr>
<td>Duration from</td>
<td>Report generation interval start time. EventTracker considers events occurred at this time onwards.</td>
</tr>
<tr>
<td>Duration to</td>
<td>Report generation interval end time. EventTracker considers events occurred till this time.</td>
</tr>
<tr>
<td>Status</td>
<td>Indicates the report generation stages.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>Last update</td>
<td>Date and time when the report generation was initiated.</td>
</tr>
<tr>
<td>Estimated time</td>
<td>Approximate time require to generate the report / flex report</td>
</tr>
<tr>
<td>Cancel processing</td>
<td>Click to abort report generation.</td>
</tr>
</tbody>
</table>

### On Demand/Queued Status

1. Click **On Demand/Queued Status** button. Reports Status displays.

2. Select a report and click the **Cancel Processing** button. The On Demand/Queued report is cancelled.

### Favorites

1. Log on to EventTracker Enterprise and then click the **Reports** menu.
2. Click the **New button** in **Dashboard / Configuration**.
3. Select **Alphabetical** tab.
4. Select any report and then select the **Add to Favorites** tab.
5. To view favorites click the **Favorites** tab.
6. To generate a report, select any report and the **Report Type**.

7. Click **Next** and proceed further as mentioned earlier in order to generate different reports.
Explorer

Existing Report/Log Search architecture goes through the typical CAB file processing for generating report or finding out specific data based on the given criteria. In real time environments (on heavy load scenarios, unknown conditions and multiple searches) this process takes lot of time and does not solve the immediate queries. Easy way to process quickly is to have the archived events in a cache, so that redundant processing of CAB files is eliminated.

Based on the given criteria EventVault generates search result from cache and saves the search results as Search history for future reference.

Run ad-hoc reports and save the data in a database. You can further drill-down the cached data by,

- Specifying Location, words, exact word/phrase or range of Event Id, in Advance search
- Selecting existing Category
- Constructing your own SQL Query

User can also configure EventVault Explorer to use remote SQL Server database. The reason is, SQL Server Express Edition has maximum database size limitation of 4 GB. Hence, to overcome this limitation an option is provided to use Remote SQL Server, which can be SQL Server Enterprise Full Edition. Unlike SQL Server Express Edition, SQL Server Enterprise Edition does not have any size limitation.

Perform search in EventVault Explorer

This option helps you to search CAB files.

1. Click the Reports menu, click Explorer, and then click the New Search tab.

   EventTracker displays the EventVault Explorer.
2 Enter the **Report title**.
   Ex: Change Audit

3 In **Duration** tab, select the **Interval**.

4 In **Systems** tab, select any one of the **Sites / Groups / Systems** option.
   You can also select **Show all sites / All Systems** or **Search System(s)**.

---

**Figure 167**
5. Set the **Refine / Filter** criteria.
6 Enter an appropriate **Description**.

7 Click **Search**.

EventTracker displays the Disk cost analysis pop-up window.

![Disk cost analysis](image)

**Figure 170**

8 Click **OK**.

EventTracker displays information message box.
9 Click **OK**.

EventTracker displays **Search History** tab with the result set. By default only 5 searches can be made but the user can increase it by changing the configuration settings (To change Configuration setting, click **Configuration** hyperlink and set the **Max history count**).

10 Click the **Status** hyperlink.

EventTracker displays EventVault Explorer processing status window.
### Status of unpacking Archives

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initializing</td>
<td>New request</td>
</tr>
<tr>
<td>Processing</td>
<td>Cab Extraction</td>
</tr>
<tr>
<td>Exception Occurred</td>
<td>Failed</td>
</tr>
<tr>
<td>Status of unpacking Archives</td>
<td>All the archives have been processed (unpacked) successfully.</td>
</tr>
</tbody>
</table>

## Flex History

Flex History provides detailed information about Flex Reports that have been configured since the reports are flexible. For a detailed flex report, when you select the option to persist data for a certain period, reports get appended for that period. Later the reports get purged.

The standard columns provided in EventTracker are Log Type, Source, Event ID, EventType, Category, Domain, System, User and Description.

You can create and extract your own custom columns from the standard columns provided. The results can be extracted in an Excel file since it supports all Excel features. It allows you to browse through underlined data.

For example:

If you need information about User, Log Type and Source only, then flex history can be configured to fetch the required data.

1. Click the **Reports** menu, and then select **Explorer**.
   
   EventTracker displays the EventVault Explorer.

2. Select the **Explore** option.
   
   Flex Data Refine window displays.
3 Select the required options and then click the **Search** button.

Ex: Select Account Domain option, and then click Search.

Show Refined Data window displays.
4 To view data volume, click **EventVault** icon.
5 To refine and narrow down the search criteria, click **Refine** icon.

6 Click **Tags** drop-down and select the required option.

Flex Refine Dialog displays.
7 Select the **Refine option** button.

Flex Refine Dialog displays.

![Flex Refine Dialog](http://www.example.com/178.png)

**Figure 178**

8 Enter the relevant search criteria and then click **Refine**.

9 To return to flex history tab, click the **Flex History** button.

10 To search data, click **Search again** icon.

11 To export data to excel, click **Export** icon.

**Analytics**

Analytics provides detail analysis of deviation values in flex reports. It provides a graphical representation of variation details based on threshold settings and analysis type.

For ex: Logon failure.

Let us consider an example where in many users are unable to login. If we run the analytics option been provided, it is easy to find out the deviation and the percentage of users who are unable to login. The graph provides a clear information and necessary steps can be taken care to avoid disasters.
1. Click **Tools** at the upper-right corner and then click **EventVault Explorer**. EventTracker displays the EventVault Explorer.

2. Select the **Analytics** option. Analysis window displays.

3. Select any two **Columns for analysis**. Note that you cannot select more than two columns.

4. Select the required **Threshold settings, Perform Analysis for, Analysis Type** options.

5. Select the **Analyze** button. The relevant analysis data displays.
6 Select the **Total Event Count** option.

Total event count window displays.

7 To return to **Flex History** tab, click **Flex History** hyperlink.
Configure EventVault Explorer to use remote SQL Server

Before you begin, read the below points carefully.

**NOTE**

- MS SQL Server Enterprise 2005 / 2008 / 2012 are supported.
- For best performance the instance of SQL Server Enterprise should be dedicated for this usage.
- The SQL Server instance should be accessible from the EventTracker server, preferably via fully qualified domain name (FQDN).
- Windows authentication is used for connecting to the SQL Server.

For successful configuration, follow the steps given below:

- Grant user (User used for EventTracker configuration) Sysadmin access on remote SQL Server.
- Create folder on remote SQL Server system to store EventVault Explorer database file and give user (User used for EventTracker configuration) full access on folder created on remote system.
- Click the 'Reports' menu, select 'Explorer'.
  The EventVault Explorer window will appear on the screen.
- Click Configuration hyperlink.
  EventVault Explorer Database Configuration window displays.

![EventVault Explorer Database Configuration](image)

**NOTE**

For more details, refer EventVault Explorer – Introduction and Usage document.
Chapter 9
My EventTracker Reports

In this chapter, you will learn about:

- Dashboard
- Reports
My EventTracker Dashboard

My EventTracker dashboard is similar to Security and Operations Dashboard. It provides the same features and functionality as mentioned in chapter 5 Dashboard. You can configure and customize the same.

My EventTracker Reports Dashboard/Configuration

My EventTracker Reports can be configured and viewed only by the owner who configured those reports. No other user can view or modify My EventTracker Reports. However, the administrator can view the configured reports and not the generated reports.

Procedure to configure On Demand, Queued, Scheduled, and Defined reports are identical for Security, Operations, Compliance, and Flex reports mentioned in chapter 8 Reports.
Chapter 10
Change Audit

In this chapter, you will learn about:

- Change Audit Dashboard
- Last Changes
- Policy Dashboard
- Change Policies
- System Inventory
About Change Audit

Change auditing is the way to monitor voluntary and involuntary changes on your system and to make sure that your system has not been compromised. Ultimately, it helps to detect and recover from the most insidious of system compromises.

Change Audit Dashboard

Change Audit dashboard works/possess similar features like Operations/Security Dashboard. It allows you to add Dashlets to view Unauthorized Changes, Unauthorized Changes History, Change By Object Type, and Change By Change Type.

To view Change Audit dashboard

I. Log on to EventTracker Enterprise.
II. Click Change Audit, and then click Dashboard.
   EventTracker displays the Change Audit Dashboard.
III. Click the Customize hyperlink.

EventTracker displays the Change Audit Dashlets pop-up window.
IV. Click **Edit** to edit the Title or Time Interval settings, and then click **Update**.

V. Select the required **Change Audit Dashlets** and then click **Add**.

EventTracker displays the Dashboard with newly added Dashlet(s).

VI. Click any graph or a legend to view respective Dashlet summary.
VII. Click any hyperlink to view respective change details.

VIII. Select **Access History**.
Access History flex report displays.

IX. Click Export icon to export data to excel.

Last Changes

Last changes display the summary of snapshot comparison results.

a. Log on to EventTracker Enterprise.

b. Click the Change Audit menu, click the Last changes tab.
   EventTracker displays the Last changes tab.
By default, EventTracker displays chart view summary of Authorized, Unauthorized, Configuration, and Business Knowledge Change Types for all managed systems irrespective of the system groups.

“No data available” implies that no change has been detected for the default Change Types when the last snapshot was taken.

c. Click any graph to view Change Details. Click Group by Path to sort the Item Name by path.

<table>
<thead>
<tr>
<th>Change Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorized</td>
<td>Detected changes that can be matched with an approved change request.</td>
</tr>
</tbody>
</table>
| Unauthorized       | Detected changes that cannot be matched to an approved change request.  

<table>
<thead>
<tr>
<th>Change Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td>Configuration audit helps to track all changes that have been made to a computer configuration, or to be able to restore the configuration of that computer back to a known valid restore point.</td>
</tr>
<tr>
<td>Business Knowledge</td>
<td>Is the concept in which an enterprise consciously and comprehensively gathers, organizes, shares, and analyzes its knowledge in terms of resources, documents, and people skills.</td>
</tr>
</tbody>
</table>

View statistical data of Change Type/Object Type.

A. In the View Type dropdown, click Data.

B. In the View By dropdown, click Change Type/Object Type.

EventTracker displays the statistical data of Change Type/Object Type.
View chart summary of Change Type/Object Type

a) In the View Type dropdown, click the Graph option.
b) In the View By dropdown, click Change Type/Object type.

EventTracker displays the default chart view summary of Change Type/Object Type.

Set Dashboard Preferences

To set Dashboard preferences, refer EventTracker Control Panel -> Change Audit.

Authorize the Unauthorized Changes

1. To authorize unauthorized changes, click the Last Changes tab.
2. Click the hyperlink under the respective columns under View Type - Data or click on the pie section under View Type - Graph.

EventTracker displays the Change Details pop-up window.
3. Select the change type as Unauthorized from the Change Type dropdown.
4. Select the required checkbox against the Item name to authorize.
5. Click the Authorize button.

![Figure 192](image-url)
EventTracker displays the Authorization comment window.

![Authorization comment window](image)

Figure 193

6. Type the reason why the selected item needs authorization in the **Authorization comment** field for future reference.
   
   This field is not mandatory.

7. Click **Save**.
   
   EventTracker displays the confirmation message pop-up window.

![Confirmation message](image)

Figure 194

8. Click **OK** to save changes.
   
   EventTracker authorizes the selected item and removes from the unauthorized list.
   
   You can also authorize items by grouping them based on a common location.

9. Click **Group by Path** to view items by location.
   
   EventTracker displays the Group by Path window.
10. If there are multiple paths displayed and you wish to select all paths, select the checkbox against Path, and then click the Authorize button to authorize all the items.

(OR)

To select individual path, select the checkbox for respective path, and then click the Authorize button.

**NOTE**

EventTracker enables Authorize button only for unauthorized items.

EventTracker displays the ‘Authorize” button when changes to ‘Unauthorized” items (*.exe, *.ocx, *.dll, *.sys, *.drv, *.msc, *.cpl, and *.vxd) are detected.

EventTracker displays the ‘More Info” button when new/modified/deleted DLLs and EXEs are detected.

**View Access History**

This option helps you view access history of files, folders, and registry keys in a chronological order.

**NOTE**

It is mandatory to enable Windows Object Access auditing on the target system prior to using this feature. For more details, refer [Enable OS Auditing on folder(s)](https://example.com).
1. Select an Item Name and then click **Access History**. EventTracker displays the progress bar.

2. Click **Export** to export the report into Excel format.
View Additional Information on Files

1. Select an Item Name and then click More Info. 

Enable OS Auditing on Folder(s)

1. Right-click the folder that you want to audit, select Properties.
   Example: \<system name>\Program Files\Prism Microsystems\EventTracker\Cache
2. Click the Security tab on the Properties window.

   ![Image of Security tab](image.png)  
   **Figure 198**

3. Click Advanced, and then click Auditing tab on the Advanced Security Settings window.
4. Click **Continue**.

Advance Security Settings for Cache window displays.

5. Click **Add**.

Select User, Computer, Service Account, or Group window is displayed.
6. To select the location from where you want to add users, click **Locations**.

7. Select the location from the **Locations** window and then click **OK**.

8. Enter the user name in the **Enter the object name to select** field.
   Example: Everyone
9. Click **Check Names**.
   If the user name is valid, the user name is displayed in the Enter the object name to select field. Otherwise, an error message is displayed.

10. Click **OK**.
    Auditing Entry for window is displayed.
11. Select **Full Control** under **Successful** and **Failed**.

![Auditing Entry for Cache](image)

**NOTE**

Select the **Access** options as per your requirement.

12. All other checkboxes are also selected automatically when you select **Full Control** checkbox.

13. Click **OK**.

Advanced Security Settings for Cache window displays with the newly added user.
14. Click **Apply**, and then click **OK**.

**NOTE**

Similarly, you can enable auditing on files.
Policy Dashboard

Policy Dashboards helps to add Dashlets to view the compliance status of systems against which the Policies were compared.

1) In Change Audit menu, click the Policy Dashboard drop down and then click the Configure.

![Figure 207](image)

2) EventTracker displays the Configure Benchmark Dashlets pop-up window.

3) Type a comprehensible name in the Display Name field.

4) Select a policy from the Policy Name field.

   EventTracker displays the Configure Benchmark Dashlet pop-up window with Schedule details of the selected Policy.
5) Click the checkbox to select the Schedule(s), and then click the **Configure** button.

**Customize the Policies Dashboard**

This option helps to customize the dashboard with configured Dashlets.

1) In **Change Audit** menu, click the **Policy Dashboard** drop down and then click **Customize**.

EventTracker displays the Available Dashlets pop-up window.
2) Click the checkbox to select the Dashlet(s), and then click **Add**. EventTracker adds the Dashlet(s) to the Dashboard.

OR

Click the checkbox to select the Dashlet(s), and then click **Delete**. EventTracker deletes the dashlet(s).

3) Click a pie chart or a legend to view respective system details.

EventTracker displays the System Details Pop-up window.
4) Click the View hyperlink to view Change Audit Assessment Details.
EventTracker Inventory Manager

EventTracker Inventory is an automated asset management tool, which scans all Change Audit, managed computers, and displays them in an easy accessible web and legacy interface.

Software inventory: To track and audit software installed on Change Audit managed computers.

For detail information please refer EventTracker Control Panel -> Change Audit.

Change Policies

Change Assessment Dashboard displays the most recent results of on demand / scheduled policy comparison.

1. Click the Change policies tab.

Policy details display in dashboard.

![Dashboard](Figure 214)

<table>
<thead>
<tr>
<th>Icon</th>
<th>Represents</th>
</tr>
</thead>
<tbody>
<tr>
<td>📜</td>
<td>File changes found.</td>
</tr>
<tr>
<td>📜</td>
<td>Registry changes found.</td>
</tr>
<tr>
<td>📜</td>
<td>File and registry changes found.</td>
</tr>
<tr>
<td>📜</td>
<td>Information icon</td>
</tr>
<tr>
<td>📜</td>
<td>Notes icon</td>
</tr>
</tbody>
</table>
### Icon Represents

<table>
<thead>
<tr>
<th>Icon</th>
<th>Represents</th>
</tr>
</thead>
<tbody>
<tr>
<td>📖</td>
<td>Logbook icon</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Select any title to view policy comparison results for that period and integrity violation details on the Dashboard.</td>
</tr>
<tr>
<td>Status</td>
<td>Select an option from this drop-down list to further filter the policy comparison result. Success – policy comparison executed successfully against the monitored systems. Integrity Violations – policy comparison executed successfully against the monitored systems but integrity violations have been found. Exceptions – policy comparison execution failed.</td>
</tr>
<tr>
<td>Delete</td>
<td>Select the checkbox against the policy comparison result and then click this button.</td>
</tr>
</tbody>
</table>

2. Click **Information** 🔄 icon to view Policy Details.
3. Click the **Flag** 📚 icon to change status of that particular policy.

<table>
<thead>
<tr>
<th>Flag icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>💡 😓</td>
<td>Un-flagged and no action has been taken</td>
</tr>
<tr>
<td>📝 🔴</td>
<td>Flagged and relevant action is required for that particular incident to solve an issue.</td>
</tr>
<tr>
<td>📝 🟢</td>
<td>Checked the incident and necessary action has been taken care of</td>
</tr>
</tbody>
</table>

4. Click **Notes** 📝 icon to enter relevant information about the respective policy.
5. Click any **Title** hyperlink to view Integrity violation details.
6. To add data to a log book, click **logbook** 📖 icon.
   Logbook window displays to add to a new or existing logbook.

7. To create a new logbook, click **Add new logbook**.
8. To add data to a new log book, click **Add to existing logbook**.
9. To delete a policy, select the **Delete** option and then click the **Delete** button.

---

**Figure 215**

---

209
Analyze Policy Comparison Results

a. To analyze policy comparison result, click the title of the policy comparison schedule on the Dashboard.

EventTracker displays the Policy Comparison Results page.
Figure 216

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>Name of the target system where the policy is compared</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Policy Name</td>
<td>Name of the policy compared on the target system.</td>
</tr>
<tr>
<td>Total Violations</td>
<td>Total number of violations detected.</td>
</tr>
<tr>
<td>Compared on</td>
<td>Date and time when the policy was compared.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the policy.</td>
</tr>
<tr>
<td>Item Name</td>
<td>Name of the policy item.</td>
</tr>
<tr>
<td>Policy Values</td>
<td>Values of the policy item selected in the left pane when the policy was configured.</td>
</tr>
<tr>
<td>Actual Values</td>
<td>Actual Values of the policy item selected in the left pane after the policy comparison is done. This reflects any change in the value of the policy item.</td>
</tr>
<tr>
<td>Item Description</td>
<td>Description of the item selected in the left pane is displayed at the bottom of the right pane.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept</td>
<td>If changes are found for the selected item, you can update the master policy with the new value.</td>
</tr>
<tr>
<td>Reject</td>
<td>If you find an item to be irrelevant to the present context, you can select and remove that item from the master policy.</td>
</tr>
<tr>
<td>Ignore</td>
<td>When you generate a report, ignored items will not be considered for report generation. Note that these items are not removed from the master policy.</td>
</tr>
<tr>
<td>Save</td>
<td>Save the policy with changes if any, with the same name.</td>
</tr>
<tr>
<td>Save As</td>
<td>Save the policy with changes if any, with a different name.</td>
</tr>
<tr>
<td>Close</td>
<td>To close the Dashboard.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Icon</th>
<th>Represents</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔄</td>
<td>Fresh items.</td>
</tr>
<tr>
<td>🔄✅</td>
<td>Items accepted.</td>
</tr>
<tr>
<td>🔄❌</td>
<td>Items ignored.</td>
</tr>
<tr>
<td>🔄❌❌</td>
<td>Items rejected.</td>
</tr>
</tbody>
</table>

b. Click the Item Name to Accept, Reject or Ignore the integrity violation.
If you reject the policy then a confirmation message displays.
c. Click **Save** or **Save As** after the changes has been done.

For more information on creating Configuring Policies, refer [Create Configuration Policy](#).

**Schedule Change Assessment**

This option helps you schedule change assessment.

**To schedule Change Assessment**

1. Click **Scheduled** in the **Actions** pane, and then click **New Schedule** in the bottom pane.

   OR

   Click **Policies** in the tree pane, right-click the required policy and then select **Add Scheduled**.

---

Figure 218

![Message from webpage]

Figure 218: Reject item dialog box.

Figure 219

![Schedule Change Assessment]

Figure 219: Scheduling Change Assessment.
EventTracker displays the Scheduled page.
2 Enter the title of the schedule in the **Title** field. Select a policy from the **Policy Name** drop-down list.

3 Type the name of the system(s) in the **Search system(s)** field and then click the search icon. EventTracker displays the system group of the systems searched.

4 Select the system(s). Click **Show All** to view all managed systems and system groups.

(OR)

5 Select system(s)/system group(s) from the **Systems** list.

6 Select the required time duration to run the schedule. Select an option from the **Frequency** drop-down list for how often the policy runs.

**NOTE**

EventTracker enables the **Week Day** drop-down list only when you select the Weekly option from the **Frequency** drop-down list.
7 Click **Save**.

**Edit Change Assessment Schedules**

This option helps you edit Change Assessment schedules.

1 To Edit Change Assessment Schedules, select a scheduled policy in the bottom pane. Click **Edit**.

![Figure 222](image)

2 Make appropriate changes in the relevant fields, and then click **Save**.

**Run Schedules On Demand**

This option helps you run schedules on demand.

To run the schedules on demand

a. Select a scheduled policy in the bottom pane. Click **Run Now**.

   EventTracker displays the message box with appropriate message.
Delete Scheduled policies

This option helps to delete schedules.

a) Select any scheduled policy in the bottom pane, and then click **Delete**.

EventTracker displays the confirmation message box.

b) Click **OK** to delete the schedule.

System Inventory

EventTracker System Inventory is an automated asset management tool, which scans all Change Audit, managed computers, and displays them in an easy accessible web and legacy interface.

Software inventory: To track and audit software installed on Change Audit managed computers.

To view application(s) and update(s)

1. In **Change Audit** menu, click **System Inventory**.
NOTE

You can also view the Inventory Manager in EventTracker Control Panel -> Change Audit.

2. In **System Information** pane, right-click any system and then select **Show Details**.
   By default, Inventory Manager displays system details of EventTracker Manager System.

![System Information](image)

**Figure 225**

3. Select the **Applications Installed** option.
   Inventory Manager displays the itemized list of applications installed on the selected system.
4. To view more information regarding any application, select any Application Name.

5. To view recent updates, click Updates tab.
Inventory Manager displays the itemized list of hot fixes, patches, and updates installed on the selected system.

**NOTE**

Currently there are no updates installed on the selected system, hence there is no information displayed.

6. Click the **Export** icon to export data to excel file.
Chapter 11
Config Assessment

In this chapter, you will learn about

- Dashboard
- Reports
Schedule Config Assessment

This option helps to schedule Config Assessment

To schedule Config Assessment

1) Logon to EventTracker Enterprise. Click Config Assessment menu, and then click Reports tab.
2) Click Scheduled on the ‘Actions’ pane, and then click New Schedule in the bottom pane.

OR

Click any Benchmarks in the tree pane, right-click the required benchmark and then select Add Scheduled.

EventTracker displays the Scheduled page.
3 Type the title of the schedule in the **Title** field. Select a policy from the **Policy Name** drop-down list.

![NOTE]

**Policy Name** is grayed out because it has already been selected via Add Scheduled option.

4 Type the name of the system(s) in the **Search system(s)** field and then click the search icon. EventTracker displays the system group of the systems searched.

5 Select the system(s). Click **Show All** to view all managed systems and system groups.

(OR)

Select system(s)/system group(s) from the **Systems** list.

6 Select the required time duration to run the schedule. Select an option from the **Frequency** drop-down list for how often the policy should run.

![NOTE]

EventTracker enables the Week Day drop-down list only when you select the Weekly option from the Frequency drop-down list.
7 Click **Save**.

8 To view **Benchmark details**, click **Information** 📘 icon.

---

**Benchmark details**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Top Pane</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Title</strong></td>
<td>Title of the Configuration Assessment schedule.</td>
</tr>
<tr>
<td><strong>System</strong></td>
<td>Name of the system against which the benchmarks were compared.</td>
</tr>
<tr>
<td><strong>Passed</strong></td>
<td>Benchmark rules that found to comply.</td>
</tr>
<tr>
<td><strong>Failed</strong></td>
<td>Benchmark rules that failed to comply.</td>
</tr>
<tr>
<td><strong>Exceptions</strong></td>
<td>A rule with the result &quot;error&quot;, &quot;unknown&quot;, &quot;not applicable&quot;, &quot;not checked&quot;, &quot;not selected&quot;, &quot;informational&quot;, or &quot;fixed&quot; is considered as an exception.</td>
</tr>
<tr>
<td><strong>Deviations</strong></td>
<td>Rules that are not implemented on the managed systems could be declared as deviations with reasons why and when it could be implemented.</td>
</tr>
<tr>
<td><strong>Result File</strong></td>
<td>Click the View hyperlink to view the result file.</td>
</tr>
<tr>
<td><strong>Duration</strong></td>
<td>Select an option to view benchmark comparison execution by period. Duration ranges from 1 day to 12 months.</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>Select an option to view configuration assessment result by status. Valid options are Success and Fail.</td>
</tr>
</tbody>
</table>

**Bottom Pane displays the Benchmark details.**
10. Click the Flag icon to change status of that particular policy.

<table>
<thead>
<tr>
<th>Flag icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRAY</td>
<td>Un-flagged and no action has been taken</td>
</tr>
<tr>
<td>RED</td>
<td>Flagged and relevant action is required for that particular incident to solve an issue.</td>
</tr>
<tr>
<td>GREEN</td>
<td>Checked the incident and necessary action has been taken care of</td>
</tr>
</tbody>
</table>

11. Click Notes icon to enter relevant information about the respective policy.
12. Click any Title hyperlink to view config assessment result details.
13. Click **View** hyperlink to view **OVAL Results** in HTML file.

14. To add data to a log book, click **logbook** icon.
   Logbook window displays to add to a new or existing logbook.
15. To create a new logbook, click Add new logbook. 
16. To add data to a new log book, click Add to existing logbook.  
17. To delete a policy, select the Delete option and then click the Delete button.

**View Schedule Details and History**

1. To View Schedule Details and History, on the bottom pane, click the hyperlink in the Title column. EventTracker displays the Config Assessment History window.

2. Click the History tab to view schedule execution history.
Edit Config Assessment Schedules
This option helps you edit Config Assessment schedules.

1. To Edit Config Assessment Schedules, select a scheduled policy in the bottom pane. Click **Edit**.

![Figure 235](image)

![Figure 236](image)
2 Make appropriate changes in the relevant fields, and then click **Save**.

**Run Schedules On Demand**

This option helps you run schedules on demand.

**To run the schedules On Demand**

1. Select a scheduled policy in the bottom pane. Click **Run Now**.

   EventTracker displays the message box with appropriate message.

   ![Message from webpage](image)

   *Figure 237*

**Search Published Reports**

This option helps to search generated scheduled reports.

1. To search a published report, select a schedule on the bottom pane. Click the search button.

   EventTracker displays the **Published report search** window.
2. Type the name of the report in the **Title** field. Select the time duration.
3. Click **Search**.
4. Click **Reset** to clear all fields and start search afresh.
5. Click the **Export** button to export data to excel.

**View Config Assessment Results**

1. To view Config Assessment results, in reports click a hyperlink.
2. Select **Success** or **Fail** from the **Status** drop-down list.
A failed rule marked as Deviation. You can declare failed rule as deviation with proper rationale and tentative time frame when it could be rectified.

Rule that failed to comply.

Rule that complied.

A rule with the result "error", "unknown", "not applicable", "not checked", "not selected", "informational", or "fixed" is considered an exception.

3. Click the ☑ button to view description of the Benchmark and click View Oval definitions XML hyperlink.

Publication date specifies date at which the Benchmark attained the displayed status. Status includes any one of the following “accepted”, “draft”, “interim”, “incomplete”, and “deprecated”. 
EventTracker displays the File Download pop-up window.

4. Click **Open** to view OVAL definitions.

5. Click a **Rule Title** hyperlink in the **Assessment Results** pane to view Rule details.

6. Click the **CPE Results** hyperlink.
   
   EventTracker displays CPEOVAL results.
7. Click the **Patch Results** hyperlink.

EventTracker displays Patch OVAL results.
8. Click Publish as XCCDF Report.

EventTracker displays the FDCC XCCDF Report Details window.

9. Enter relevant data and then click Publish.
10. Click **Yes** to view the report in XML.
   (OR)
   Click **No** to close the window.

11. Click **Add as Deviation** for any failed rule.

   EventTracker displays the Deviation Details window.
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deviation Rationale</td>
<td>Type a valid reason why this rule was breached.</td>
</tr>
<tr>
<td>Plan of Action and Milestones (POAM) Planned</td>
<td>Select this checkbox. EventTracker enables the POAM Description field.</td>
</tr>
<tr>
<td>POAM Description</td>
<td>Type the course action that would be taken to rectify the deviation.</td>
</tr>
<tr>
<td>Deviation for this evaluation only</td>
<td>Select this checkbox if you wish EventTracker to remember the deviation for this evaluation only. Otherwise, EventTracker will remember for all evaluations. EventTracker hides the “Mark the deviation for this system only” checkbox.</td>
</tr>
<tr>
<td>Mark the deviation for (System Name) system only</td>
<td>Select this checkbox if you wish EventTracker to remember the deviation for this system only. Otherwise, EventTracker will remember for all systems.</td>
</tr>
</tbody>
</table>

12. Enter/select appropriate data and then click **Ok**.

   EventTracker displays the message box after successfully updating the deviation rationale.
13. Click OK.

EventTracker displays the **Remove Deviation** and **View/Edit** buttons on the FDCC Compliance Results window.

**Export Assessment Details**

This option helps you export assessment details.

1. Click **Export** drop-down.
2 From the drop-down list, choose Export Results to export Configuration Assessment results into Excel format.

3 From the drop-down list, choose Export CCE Ids to export summary report on Passed, Failed, and Exception CCE Ids into Excel format.

Search Rules by CCE Id
This option helps you search benchmark rules by CCE Id.

1 To search rules by CCE Id, type the CCE Id in the CCE Id field and then click Search icon.

Ex: CCE-9725-3

EventTracker displays the message box with count of matches found and highlights search result in yellow color.
To view CCE ID of a rule

1. Select a report in Config Assessment whose status is **Success** from the **Status** drop-down list.
2. Click the link in the **Title** column on the top pane.

**NOTE**

EventTracker displays this link only for successful benchmark assessment.

EventTracker displays the **Config Assessment results** page.
3 Click a rule on the Assessment Results pane to view corresponding details on the Rule Details pane. Rule Details include CCE Id.

Delete Scheduled policies

This option helps to delete schedules.

To delete a scheduled policy

a. Select any scheduled policy in the bottom pane, and then click **Delete**.
   EventTracker displays the confirmation message box.

b. Click **OK** to delete the schedule.
Config Assessment Dashboard

Configuration Assessment Dashboard allows you to add Dashlets to view itemized Config Assessment Results. To view data in Config Assessment Dashboard, first configure/customize the scheduled reports available in Benchmark tree pane.

NOTE

Configuring and Customizing Config Assessment Dashboard is similar to Security/Operations/Compliance/My EventTracker Dashboard.

Configure Config Assessment Dashboard

1. Logon to EventTracker Enterprise. Click Config Assessment, and then click Dashboard drop-down.
2. Click Configure.

![Figure 253](image)

3. EventTracker displays the Configure Benchmark Dashlet window.

![Figure 254](image)
4 Type a comprehensible name in the **Display Name** field. Select a benchmark from the **Benchmarks** drop-down list.

**NOTE**

Select a **Policy Name** which is already scheduled in **Config Assessment Scheduled Reports** otherwise data will not be displayed.

EventTracker displays the Configure Benchmark Dashlet window with Schedule details of the selected Policy.

5 Select the required Schedule(s) options and then click **Configure**.

## Customize Config Assessment Dashboard

1 Logon to **EventTracker Enterprise**. Click **Config Assessment**, and then click **Dashboard** drop-down.

2 Click **Customize**.

EventTracker displays the **Available Dashlets** window.

3 Select the required **Dashlet(s)** and then click **Add**.
4 EventTracker displays the **Dashboard** with newly added **Dashlet(s)**.

![Figure 257](image)

5 Click a graph or a legend to view respective **System Details**.

![Figure 258](image)

6 Click the **View** hyperlink in to view **Configuration Assessment results**.

7 Click the hyperlink in the **Passed Rules** column to view Benchmark rules that found to comply/failed to comply.

8 Click the hyperlink in the **Failed Rules** column to view Benchmark rules that failed to comply/found to comply.

9 Click the hyperlink in the **CPE Result** column to view CPE OVAL result.

10 Click the hyperlink in the **Patch Result** column to view CPE Patch result.
Click the hyperlink in the **OVAL** column to view OVAL XML report.

Click **Export** icon to **Export Results/CCE Ids** data to excel.

**Reset Personalization**

This option helps to reset the dashboard with default Dashlet(s).

1. To Reset Personalization, click the **Config Assessment** menu, click **Dashboard** drop-down. Click **Reset personalization**.

   EventTracker displays the confirmation message box.

   ![Message from webpage](image)

   **Figure 259**

2. Click **OK** to reset the dashboard.

   EventTracker removes the custom dashboard that you have added.
Chapter 12
Alerts

In this chapter, you will learn about:

- Add Custom Alerts
- Add Predefined Categories as Alerts
- Delete Alerts
- Configure Alerts Actions – Manager Side
Alerts

EventTracker generates an alert when a critical event occurs, such as security breaches, performance problems, etc. Configure an unlimited number of rule-based alerts with customizable event criteria including support for event-fired automatic (custom) actions for any defined event.

- Out of the Box alerts for the most common predefined alert condition
- Ability to create your own alert conditions
- Reliable framework for alerts
- Ability to minimize false positive
- Firing automatic actions as a receipt of event can increase system's availability

Risk Metrics

EventTracker ‘Risk Metrics’ considers three factors to calculate Risk (R). This calculation will be performed just before an alert is raised. Alert notification is sent only when the risk is greater than or equal to the threshold.

<table>
<thead>
<tr>
<th>T</th>
<th>Threat level (how severe the Alert is) assigned while creating Alerts</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Asset value of the system (how important or critical the computer is) set through the System Manager</td>
</tr>
<tr>
<td>V</td>
<td>Vulnerability (how vulnerable the computer is) automatically updated using third party vulnerability assessment reports.</td>
</tr>
</tbody>
</table>

Example #1:

Day 1

- System Type: Server
- Threat level: Medium
- Asset value: Medium
- Vulnerability: High
- Alert notification is sent since it is found to be highly vulnerable by running the vulnerability scanner.

Example #2:

Day 2

- System Type: Server
- Threat level: Medium
- Asset value: Medium
- Vulnerability: Low (system is hardened by applying hotfixes, patches, & service packs)
- Alert notification is not sent since it is found to be not vulnerable by running the vulnerability scanner.

### Add Custom Alerts

This option enables you to configure alert, add events to alert, and configure alert actions.

#### To Add Custom Alerts

1. Click Admin dropdown, and then click Alerts.

EventTracker displays Alert Management page.

![Image of Alert Management page](Image)

**Figure 260**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search</td>
<td>Type the search string and then click GO. This helps to easily locate the alert you are looking for.</td>
</tr>
<tr>
<td>Page Size</td>
<td>Select an option from this drop-down list to display the maximum number of alerts in a page.</td>
</tr>
<tr>
<td>Alert Name</td>
<td>Name of the alert. Click the hyperlink to modify alert details.</td>
</tr>
<tr>
<td>Threat level</td>
<td>Severity of the alert.</td>
</tr>
<tr>
<td>Active</td>
<td>Select or clear the checkbox to activate or deactivate the alert.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Beep</td>
<td>Select this checkbox to configure audible alert notification.</td>
</tr>
<tr>
<td>E-mail</td>
<td>Select this checkbox to configure e-mail alert notification. The SMTP server should be configured to send Email.</td>
</tr>
<tr>
<td>Message</td>
<td>Select this checkbox to configure console message alert notification.</td>
</tr>
<tr>
<td>RSS</td>
<td>Select this checkbox to configure notification through RSS Feeds.</td>
</tr>
<tr>
<td>Forward as SNMP</td>
<td>Select this checkbox to forward alert notification as an SNMP trap.</td>
</tr>
<tr>
<td>Forward as SYSLOG</td>
<td>Select this checkbox to forward alert notification as a SYSLOG message.</td>
</tr>
<tr>
<td>Remedial Action at Console</td>
<td>Select this checkbox to configure custom action to be executed on receipt of an event at the manager side.</td>
</tr>
<tr>
<td>Remedial Action at Agent</td>
<td>Select this checkbox to configure custom action to be executed on receipt of an event at the agent side. You execute these actions only on Windows systems where agents are deployed. You cannot execute these actions on NIX systems where agent less monitoring is deployed.</td>
</tr>
<tr>
<td>Activate Now</td>
<td>Click to activate the selected alert.</td>
</tr>
<tr>
<td>Add alert</td>
<td>Click to add custom alert.</td>
</tr>
<tr>
<td>Delete</td>
<td>Select the checkbox against the alert that you want to delete, and then click Delete. Select the checkbox adjacent to the “Alert Name” column to select all Alerts.</td>
</tr>
</tbody>
</table>

2. On the Alert Management page, click the Add alert button to add new alert. EventTracker displays the Alert configuration page.
OR

Click the name of the alert that you wish to modify.

EventTracker displays the Alert configuration page.
### Fields Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat level</td>
<td>Select severity of the alert.</td>
</tr>
<tr>
<td>Threshold level</td>
<td>Alert notification is sent when the risk is greater or equal to the threshold.</td>
</tr>
<tr>
<td>Show in</td>
<td>Select 'Compliance Dashboard' from dropdown to view the selected alert details in the compliance dashboard.</td>
</tr>
</tbody>
</table>

3 Type the new alert name in the **Alert Name** field. Example: My Alert

4 Select the severity of threat from the **Threat level** drop-down list.

5 Select the threshold from the **Threshold level** drop-down list.

6 If you wish to see the alert in compliance dashboard then in **Show in** dropdown, select 'Compliance Dashboard'.

7 Click the **Add button** to add event details.

EventTracker displays the **Add Event** dialog box.

![Add Event dialog box](Image)

Figure 263

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Type</td>
<td>It describes the type of log to be monitored.</td>
</tr>
<tr>
<td>Event Type</td>
<td>Classification of event severity: Error, Information, Warning in the System and Application logs; Audit Success or Audit Failure in the Security log. Select an event type from the drop-down list.</td>
</tr>
<tr>
<td>Category</td>
<td>Classification of the event by the event source. This information is primarily used in the security log. For example, for security audits, this corresponds to one of the event types for which success or failure auditing can be enabled in Group Policy. Type the category number in this field. This field supports numeric data type only.</td>
</tr>
<tr>
<td>User</td>
<td>Type the name of the user.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Event Id</td>
<td>A number identifying a particular event. The first line of the description usually contains the name of the event type. For example, 6005 is the ID of the event that occurs when the Event log service is started. The first line of the description of such an event is “The Event log service was started.” The Event ID and the Source can be used by product support representatives to troubleshoot system problems. Type the event ID number in this field. This field supports numeric data type only.</td>
</tr>
<tr>
<td>Source</td>
<td>The software that logged the event, which can be either a program name such as “SQL Server,” or a component of the system or of a large program such as a driver name. For example, “Elkie” indicates an EtherLink II driver. Type the source in this field.</td>
</tr>
<tr>
<td>Match in Description</td>
<td>Type a sub-string of the description that needs to be matched. EventTracker supports multiple strings separated by the following operands. &amp;&amp; stands for AND condition. II stands for OR condition. If you type Successful Logon &amp;&amp; New Trusted Domain II Removing Trusted Domain, EventTracker will filter out the events that are matching Successful Logon, (AND) New Trusted Domain (OR) Removing Trusted Domain.</td>
</tr>
<tr>
<td>Description exception</td>
<td>Type a sub-string of the description that needs to be exempted.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error</td>
<td>A significant problem, such as loss of data or loss of functionality. For example, if a service fails to load during startup, an Error will be logged.</td>
</tr>
<tr>
<td>Warning</td>
<td>An event that is not necessarily significant, but may indicate a possible future problem. For example, when disk space is low, a Warning will be logged.</td>
</tr>
<tr>
<td>Information</td>
<td>In event that describes the successful operation of an application, driver, or service. For example, when a network driver loads successfully, an Information event will be logged.</td>
</tr>
<tr>
<td>Audit</td>
<td></td>
</tr>
<tr>
<td>Success</td>
<td>An audited security access attempt that succeeds. For example, a user's successful attempt to log on the system will be logged as a Success Audit event.</td>
</tr>
<tr>
<td>Failure</td>
<td>An audited security access attempt that fails. For example, if a user tries to access a network drive and fails, the attempt will be logged as a Failure Audit event.</td>
</tr>
<tr>
<td>Verbose</td>
<td>A Verbose event is a debugging trace. (Applies only to Vista)</td>
</tr>
<tr>
<td>Critical</td>
<td>A critical event is a fatal error or application crash. (Applies only to Vista)</td>
</tr>
</tbody>
</table>

8. Enter the required fields, and then click Add.
9. Click Event Filter hyperlink (OR) click Next ➩.
   EventTracker displays the Event Filter page.
10. Click **Add** to add event details for the event filter.
11. Enter the required fields, and then click **Add**.
12. Click **Custom** hyperlink (OR) click Next.
   
   EventTracker displays the **Custom** page.

![Figure 264](image)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply All Time</td>
<td>If selected, alerts actions are executed for events occurred all through the day (24 hours).</td>
</tr>
<tr>
<td>Apply between these time</td>
<td>If selected, alerts actions are executed for events occurred during the specified time frame.</td>
</tr>
<tr>
<td>Alert based on Count</td>
<td>This option lets you to receive alert notification only when the same event occurs for the specified number of times within the specified duration. Check the Enable option, to provide the event count and duration.</td>
</tr>
<tr>
<td>Archive Alert</td>
<td>Select the Store this alert in Alert Archives option to store the alert in the 'Alerts Archives'. Archived alerts will be used for the alert analysis.</td>
</tr>
</tbody>
</table>

13. Select **Apply All Time** option.

   (OR)

   Select the **Apply between this time** option, and then select **From** and **To** time from the calendar control.
In Alert based on count pane, check the Enable option, provide the number of event count in the Raise alert for event count field, and then provide the time in seconds in the Duration field.

**NOTE**

The default value for Raise alert for event count is 2 and Duration is 3600 in seconds.

Click Systems (OR) click Next. EventTracker displays the Systems page.

By default, EventTracker selects the All Systems checkbox to apply the Alert to all monitored groups/systems. Clear this checkbox to select groups/systems.

Select the Groups / Systems / All Systems for which the alert is to be monitored.

Click Actions hyperlink (OR) click Next. EventTracker displays the Actions page.
256

To configure an alert, action is not mandatory. Alert actions can be configured at any point of time.

18 Select and configure the type of action from the respective tabs (i.e. E-mail, RSS, Beep, Net message, SNMP, syslog, Agent Remedial Action, Console Remedial Action).

19 Click Finish.

EventTracker adds the newly created alert and displays it on the Alert Management page.
20 To activate the newly added alert, select the checkbox under **Active** column.

EventTracker displays the success message pop-up window. EventTracker saves the alert configuration.

![Figure 267]

```
NOTE
```

The configured alert details can be modified/edited at any point of time. On the **Alert Management** page, click the alert name to be modified/edited. Make the necessary changes in **Alert Configuration** page, and then click the **Finish** button to save the changes.

![Figure 268]
Add Pre-defined Categories as Alerts

This option helps to add pre-defined categories as alerts.

To Add Pre-defined Categories as Alerts

1) Click the Admin dropdown, and then click Category.

2) EventTracker displays the Category Management page.

3) Right-click the category that you wish to add as an alert. From the shortcut menu, select Add as Alert.

EventTracker displays the Alert Management -> Event Details page.
4) Complete the alert configuration process as described in Add Custom Alerts.

Delete Alerts

This option enables you to delete Alerts.

To delete Alerts
1) On the Alert Management page, select the alert to be deleted.
2) Click the Delete button.

Configure Alert Actions – Manager Side

This option enables you to configure alert actions that are to be executed at the EventTracker manager system.

To configure alert actions
1) Configure an alert as explained in Add Custom Alerts.
2) Click an appropriate tab to configure alert actions.
You have the liberty to set more than one alert action. You can also associate an alert action with pre-defined alerts by selecting appropriate checkboxes on the Alert Management page.

## Configure E-mail Alert Action

This option enables you to configure an E-mail(s) to send as an alert action.

1. On the Alert configuration page, click Actions hyperlink, and then click the E – mail tab.
   OR
2. On the Alert Management page, click the checkbox under E-mail column.

   EventTracker displays the Email dialog box.

   ![Email Configuration](image)

   Figure 271

3. Enter required details.

4. On the Alert Configuration page, click the Finish button to save the alert action.
   OR
   In the Email dialog box, click OK.

5. On the Alert Management page, click the checkbox under Active column, and then click the Activate Now button to activate the alert action.

**FAQ: I setup an email alert and it is not working. What should I do?**

Please crosscheck the following.

- The SMTP server mentioned must be accessible from the Console system. That is either the system must be able to access Internet or the SMTP server must be reachable over the LAN.
- Ensure valid email addresses are provided in both "To Address" and "From Address".
- In case you have not configured Email, then Manager -> Email Configuration.
Configure Audible Alert Action
This option enables you to configure audible alert action.

1 On the Alert configuration page, click Actions hyperlink, and then click the Beep tab.
   OR
   On the Alert Management page, click the checkbox under Beep column.

![Beep Configuration dialog box]

Figure 272

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Type a brief description about the beep action.</td>
</tr>
<tr>
<td>Beep Count</td>
<td>Type the number of beeps that should be generated at the PC speaker.</td>
</tr>
<tr>
<td>Duration</td>
<td>Type how long should the beep be sustained.</td>
</tr>
<tr>
<td>Delay</td>
<td>Type the time interval to pause between consecutive beeps.</td>
</tr>
<tr>
<td>Frequency</td>
<td>Type the frequency (Hertz) of the beep sound.</td>
</tr>
</tbody>
</table>

2 Enter appropriate values in the relevant fields.

3 On the Alert Configuration page, click the Finish button to save the alert action.
   OR
   In the Beep dialog box, click OK.

4 On the Alert Management page, click the checkbox under Active column, and then click the Activate Now button to activate the alert action.

Configure Console Message Alert Action
This option enables you to configure a console message alert. A notification message will be sent to the selected machine.

1 On the Alert configuration page, click Actions hyperlink, and then click the Net message tab.
OR

On the **Alert Management** page, click the checkbox under **Message** column.

EventTracker displays the **Message** dialog box.

![Figure 273](image)

2 Type the name of system in **Machine Name** field.

3 On the **Alert Configuration** page, click the **Finish** button to save the alert action.

OR

In the **Message** dialog box, click **OK**.

4 On the **Alert Management** page, click the checkbox under **Active** column, and then click the **Activate Now** button to activate the alert action.

### Configure RSS Alert Notification

This option helps you to get notified via RSS, alerts raised by EventTracker for configured events.

1 On the **Alert configuration** page, click **Actions** hyperlink, and then click the **RSS** tab.

OR

On the **Alert Management** page, click the checkbox under **RSS** column.

EventTracker displays the RSS dialog box.

![Figure 274](image)

2 Select RSS Feed from the **RSS Feed Name** drop-down list.
3 On the **Alert Configuration** page, click the **Finish** button to save the alert action.

   OR

   In the **RSS** dialog box, click **OK**.

4 On the **Alert Management** page, click the checkbox under **Active** column, and then click the **Activate Now** button to activate the alert action.

   **NOTE**

   You must create RSS Feeds prior to using this feature. To configure RSS Feed, refer [RSS Feed](#).

---

**Forward Events as SNMP Traps**

All incoming events are compared with the configured alert. Whenever there is a match between an event and the alert criteria, a copy of the event is forwarded as an SNMP trap to the specified destination.

1 On the **Alert configuration** page, click **Actions** hyperlink, and then click the **SNMP** tab.

   OR

   On the **Alert Management** page, click the checkbox under **Forward as SNMP** column. EventTracker displays the **SNMP** dialog box.

   ![SNMP Dialog Box](image)

   **Figure 275**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trap Destination</td>
<td>Type the IP address or host name.</td>
</tr>
<tr>
<td>Port No</td>
<td>Type the UDP port number in this field.</td>
</tr>
<tr>
<td></td>
<td>This field supports numeric data type only.</td>
</tr>
</tbody>
</table>

2 Type appropriately in the relevant fields.

3 On the **Alert Configuration** page, click the **Finish** button to save the alert action.

   OR

   In the **SNMP** dialog box, click **OK**.
4 On the Alert Management page, click the checkbox under Active column, and then click the Activate Now button to activate the alert action.

Forward events as syslog messages
All incoming events are compared with the configured alert. Whenever there is a match between an event and the alert criteria, a copy of the event is forwarded as a syslog message to the specified destination.

1 On the Alert configuration page, click Actions hyperlink, and then click the syslog tab.
(OR)
On the Alert Management page, select the checkbox under Forward as syslog.
EventTracker displays the syslog dialog box.

![Syslog Dialog Box](image)

Figure 276

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Select either TCP or UDP as the transport protocol mode.</td>
</tr>
<tr>
<td>Load last selection</td>
<td>Click to load the last saved configuration of a syslog message.</td>
</tr>
<tr>
<td>Destination</td>
<td></td>
</tr>
<tr>
<td>syslog Destination</td>
<td>Type the IP address or host name.</td>
</tr>
<tr>
<td>Port No</td>
<td>Type the port number corresponding to the transport mode selected.</td>
</tr>
<tr>
<td>syslog Details</td>
<td></td>
</tr>
<tr>
<td>RFC 3164 syslog facility type</td>
<td>Return facility value from a received and processed syslog message.</td>
</tr>
</tbody>
</table>
### Field Description

This is the text representation of the facility.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 3164 syslog severity type</td>
<td>Return severity value from a received and processed syslog message. This is the text representation of the severity.</td>
</tr>
<tr>
<td>Event Properties</td>
<td>Select the event properties to be included in the description of the syslog message. EventTracker by default selects Event ID, Source, and Description options. You can select properties as per your choice.</td>
</tr>
<tr>
<td>syslog Format</td>
<td></td>
</tr>
<tr>
<td>Replace new lines (CRLF) with</td>
<td>Replaces the newline characters in the syslog message with tab or space.</td>
</tr>
<tr>
<td>Insert prefix</td>
<td>Check Insert Prefix option and then provide the prefix. The system messages sent to the syslog device inserts this prefix to all the messages it intercepts on their way to the message file.</td>
</tr>
<tr>
<td>Include priority code</td>
<td>Each syslog message is one line. A message can contain a priority code, marked by a digit enclosed in &lt; &gt; (angle braces) at the beginning of the line. The priority code represents both the Facility and Severity of the message.</td>
</tr>
</tbody>
</table>

2. Select/enter appropriately in the relevant fields.
3. Click OK.

**Execute Remedial Action at EventTracker Manager Console System**

This option enables you to configure custom action to be executed on receipt of an event at the manager system.

1. On the **Alert configuration** page, click **Actions** hyperlink, and then click the **Console Remedial Action** tab.

OR

On the **Alert Management** page, click the checkbox under **Remedial Action at Console** column.

EventTracker displays the **Console** dialog box.

![Console dialog box](Figure 277)
2 Type the path of the custom action file in the **File** field.

3 Click **OK**.

**NOTE**

a) To enable remedial action at manager console, click **Admin** drop-down, select **Manager**.

b) Select **Enable Remedial Action** option and then click the **Save** button.

---

**Execute Remedial Action at EventTracker Windows Agent System**

Though EventTracker is shipped with predefined alerts that are applicable to all monitored systems irrespective of O/S and mode of monitoring (Agent based or Agent less), to get alert notification messages you need to explicitly configure alert actions. While configuring alert actions it is left to your discretion to include and exclude systems. Same rule holds good for user-defined alerts.

**NOTE**

Remedial actions can be executed only on systems where EventTracker agent has been deployed.

Excluding systems for alert actions doesn't mean that you are excluding them from monitoring. EventTracker logs all events that occur in monitored systems into the database, you can plow through the data by performing Log Search.

So, utilize this feature judiciously to draw maximum benefits.

**To execute remedial action at the agent system,**

1 On the **Alert configuration** page, click **Actions** hyperlink, and then click the **Agent Remedial Action** tab.

OR

On the **Alert Management** page, click the checkbox under **Remedial Action at Agent** column.

EventTracker displays the **Agent** dialog box.
Select an appropriate remedial action option.

3 Type appropriate description in the **Notes** field for future reference.

4 Click **Ok**.

**NOTE**

To enable remedial action at agent side refer EventTracker Control Panel -> **Agent Configuration**.

### Edit Alert Actions

This option enables you to edit the alert actions.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Script</td>
<td>Type the name of the script in Script Name field. Script files are stored in the default EventTracker Agent installation path typically <code>...\Program Files\Prism Microsystems\EventTracker\Agent</code></td>
</tr>
<tr>
<td>Restart Service</td>
<td>Type the name of the service that you want to restart in Service Name field.</td>
</tr>
<tr>
<td>Restart System</td>
<td>This option will restart the agent system on the occurrence of the configured event ID.</td>
</tr>
<tr>
<td>Shut Down System</td>
<td>This option will shut down the agent system on the occurrence of configured event ID.</td>
</tr>
<tr>
<td>Stop Service</td>
<td>Type the name of the service that you want to stop in Service Name field.</td>
</tr>
<tr>
<td>Terminate Process</td>
<td>You can configure this action only for events 3217, 3218, 3221, 3223, and 3226.</td>
</tr>
</tbody>
</table>
1 On the Alert Management page, click the Alert Name for which you wish to edit the alert actions.
2 On the Alert configuration page, click Actions hyperlink.
3 Click appropriate tab(s) to edit the alert action(s).
4 Click the Finish button to save the changes.
5 On the Alert Management page, click the checkbox under Active column, and then click the Activate Now button to activate the alert action.

A message from webpage displays.

![Message from webpage](image)

Figure 279
Chapter 13
Behavior Rules

In this chapter, you will learn how to:

- Manage Behavior Rules
- Add Behavior Rules
- Add custom rule in Behavior Dashboard
Manage Behavior Rules

This option helps to set behavioral rules for enterprise activity. You can add these rules as dashlets under **Behavior → Security / Operations**.

To set Behavior rules

1. Click the **Admin** dropdown, and then click **Behavior Rules**.

   EventTracker displays the **Behavior Rules** page with pre-defined rules.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>Name of the Rule.</td>
</tr>
<tr>
<td>Break-Up-Column</td>
<td>Based on this configuration, EventTracker displays the break up details on the Enterprise Activity monitoring page.</td>
</tr>
<tr>
<td>Display Name</td>
<td>Name of the custom column.</td>
</tr>
<tr>
<td>Active</td>
<td>Clear this checkbox to inactivate the Behavior Rule (Dashlet).</td>
</tr>
<tr>
<td>Delete</td>
<td>To delete a Rule Name</td>
</tr>
<tr>
<td>Activation/Deactivation Time</td>
<td>Displays the time of activation or deactivation</td>
</tr>
</tbody>
</table>
Add Behavior Rules

This option helps to add behavior rules.

To Add behavior Rule

i. In Behavior Rules page, click Add Rule.
   EventTracker displays the Rule Configuration page.

<table>
<thead>
<tr>
<th>'Threshold settings' fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn</td>
<td>Behavior learning period (in minutes). The behavior of custom rule will be monitored for the set learning period and a threshold value will be benchmarked.</td>
</tr>
<tr>
<td>Custom</td>
<td>Specify a threshold count for occurrence of the custom rule.</td>
</tr>
<tr>
<td>Period</td>
<td>Threshold period in minutes. The custom rule will be monitored for the duration specified in this field. The number of occurrences of custom rule in this duration will be compared with the benchmarked threshold value/ count.</td>
</tr>
<tr>
<td>Evaluate Every</td>
<td>The custom rule will be evaluated every 'N' minute to analyze the activities.</td>
</tr>
<tr>
<td>Variation</td>
<td>The variation percentage can be added manually to decide the out of ordinary activities. Positive- If the threshold count observed for the given threshold period is greater than the custom count or learned threshold value then it is considered as positive occurrence of the event rule.</td>
</tr>
</tbody>
</table>
If selected, only positive variation activities will be accounted for the analysis.

Negative- If the threshold count observed for the given threshold period is lesser than the custom count or learned threshold value then it is considered as negative occurrence of the event rule.

If selected, only negative variation activities will be accounted for the analysis.

Both- Both the positive and negative variation percentage of the event rule will be analyzed for the selected threshold Period.

2 In the Rule Name field, provide a name for the new rule.
   Ex: Audit Success.

2 In the Event Rule tab, click the Add button to add event details.

   EventTracker displays the Event Configuration dialog box.

![Event Configuration dialog box](image)

   Figure 282

3 Enter appropriate details in the respective fields, and then click Add.

   The newly created event rule gets listed on Event Rule tab.

4 Click the Processing Rule tab.
NOTE

You can select processing rule from a custom list or you can configure it on your own.

7. Select the processing rule from **Available list** or using **Add new** button.

**Available list** – It is a pre-defined rule set.
a. Select the checkbox to add a **Token-value** as processing rule, and then click the **OK** button. These Token-values are extracted from ‘**Event Description**’.

(OR)

Select an appropriate option from the **Standard column** drop-down list. These column names are extracted from ‘**Event Properties**’. EventTracker adds the processing rule.

8 Click the **Add new** button.

EventTracker displays the required fields for you to enter.

![Figure 285](image)

Enter appropriate data in the relevant fields, and then click the **Add** button.

9 **Add Break-up** column details.

![Figure 286](image)
These fields are mandatory. EventTracker considers these details for grouping of events and displays the break up details on the right panes in the Enterprise Activity Details page.

5. Click **Save**.

EventTracker displays the **Behavior Rules** page with newly added rule(s).

To add custom behavior rule in Behavior Dashboard

1. Click **Behavior** menu, and then click **Security/Operations** drop-down.
2. Select the **Customize** option from the drop-down list.

   **Available Dashlets** dialog box displays the newly added behavior rule as a dashlet.
3. Check the newly created behavior rule option, and then click Add.
   EventTracker displays the dashlet on the Behavior dashboard.

4. Click a pie on the chart or a legend to view non-admin user activity details.
   EventTracker displays the ‘Enterprise Activity Detail’ page.
Chapter 14
Behavior Settings

In this chapter, you will learn about:

- Configuring Behavior Settings
Enterprise Activity Behavior Settings

This option helps you configure Enterprise Activity monitoring parameters.

1. Click the Admin dropdown, and then select Behavior Settings.
   EventTracker displays the Behavior Settings page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Activity</td>
<td>This parameter is used for backward compatibility. Any time any user crosses 2500 (default) activities - EventTracker will generate an event.</td>
</tr>
<tr>
<td>Monitor enterprise activity</td>
<td>This is only for user and admin activity (IP, process, alerts and event-ids are excluded)</td>
</tr>
<tr>
<td>Event threshold</td>
<td>Event 3269 is generated when the total count of Admin, non-admin user activities exceed the threshold. Set the maximum event threshold per user that is pertinent to your environment.</td>
</tr>
<tr>
<td>Purge Frequency</td>
<td>EventTracker purges the enterprise activity data older than the configured number of days.</td>
</tr>
<tr>
<td>Purge user data older than</td>
<td></td>
</tr>
</tbody>
</table>
## Threshold settings

<table>
<thead>
<tr>
<th>Minimum Count</th>
<th>This is a preliminary check for out-of-ordinary activity. The behavior correlation is performed for a particular activity only if it exceeds the threshold.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Variation</td>
<td>This is a preliminary check for out-of-ordinary activity. Behavior correlation is performed for a particular activity, only if this threshold is crossed.</td>
</tr>
<tr>
<td>Behavior learning period</td>
<td>This parameter is used for behavior correlation as well as for identifying new object. Based on the statistics prepared on the data collected during this period, an activity is declared whether it is new or out-of-ordinary activity.</td>
</tr>
</tbody>
</table>

## Top activities

| Top activities displayed | Only the selected number of activities will be displayed on the left hand side pane of the ‘Enterprise Activity Details’ page. |

## Generation Interval

| Select the enterprise activity interval | Enterprise activities are displayed for the selected number of days. |
| Enable DNS lookup for IP addresses | Select this checkbox to resolve IP addresses. |
| Enable Process lookup for applications | Select this checkbox to know more about the processes. |

## Geolocation Setting

| Geolocation Setting | Enterprise Activity Details page displays IP addresses in geo location map. Provide geo location API key to activate geo location. Click 🌍 icon to know how to get API key for geo location. |
Chapter 15
Category

In this chapter, you will learn about

- Category Management
- Add Categories as alerts
- Move Categories
Manage Category Groups

A set of relevant Categories can be organized under a Group.

Create Category Groups

This option enables you to organize Category groups whereby you can add, delete, and modify categories in that group.

1. Click the Admin hyperlink, and then click Category.
2. Right-click All Categories or any other Category group.
   EventTracker displays the shortcut menu.

   1. From the shortcut menu, click New Group.

   ![Figure 290](image)

3. From the shortcut menu, click New Group.

   **NOTE**

   If you select any other group than All categories, then the new group you create will be created as a sub-group under the group which is indicated in the Parent Node field.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent Node</td>
<td>Name of the parent group under which EventTracker adds the newly created group as a sub-group.</td>
</tr>
<tr>
<td>Enter Group name</td>
<td>Type the name of the group.</td>
</tr>
</tbody>
</table>

4. Type the name of the group in the Enter Group Name field.
5 Click **OK**.
EventTracker creates the group under the selected parent group.
Follow the same procedure to create sub-group(s).

6 Click **Reports** drop down, and select **Operations**.
EventTracker displays the newly added Category group under the selected parent group.

**Modify Category Groups**
This option enables you to modify a Category group.

1 Right-click the group that you want to modify.
EventTracker displays the shortcut menu.

2 From the shortcut menu, choose **Edit Group**.
EventTracker displays the Edit Group page on the right pane.
3 Type appropriate group name in the **Enter Group Name** field.
4 Click **OK**.

**NOTE**
You cannot edit the name of the Parent Node.

**Delete Category Groups**

This option enables you to remove a Category Group.

1 Right-click the group that you want to delete.

   EventTracker displays the shortcut menu.

   ![Category Management](image)

   **Figure 292**

2 From the shortcut menu, click **Remove Group**.
EventTracker displays the Confirmation message box.
3. Click **OK** to remove or **Cancel** to abort.

**Manage Categories**

A set of relevant events can be grouped under a Category. For example, you can create a set of MS-Exchange events under one Category and use this Category to show all events that occurred in MS-Exchange. This is far easier and flexible than generic reports.

**Create Categories**

This option enables you to organize categories in an ordered manner. You can create, modify, and delete the categories.

1. Right-click the groups where you want to add Categories.
   EventTracker displays the shortcut menu.

   ![Category Management](image)

2. From the shortcut menu, click **New Category**.
   EventTracker displays the **Category Details** page on the right pane.
Field | Description
--- | ---
Parent Group | The parent node under which the new category is created.
Event Category Name | Type the name of the Event Category.
Description | Type a brief description of the Event Category.
Show In | This field allows you to add the new category to be shown under the Operations, Security, and/or Compliance Tree. Any new category by default will be added under Operations.

3. Enter appropriate data in relevant fields.
4. Click **Add** to add Event Rule.

EventTracker displays the Event Configuration pop-up window.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Rule</td>
<td></td>
</tr>
<tr>
<td>Event Type</td>
<td>Select an event type from the drop-down list. The option describes the types of events Error, Warning, Information, Audit Success, Audit Failure, Success, Critical, and Verbose.</td>
</tr>
<tr>
<td>Category</td>
<td>Type the category number in this field. This field supports numeric data type only.</td>
</tr>
<tr>
<td>Log Type</td>
<td>This field describes the options are System, Security, Application, DNS Server, File Replication, and Directory Service.</td>
</tr>
<tr>
<td>Event ID</td>
<td>Type the event ID number in this field. This field supports numeric data type only.</td>
</tr>
<tr>
<td>Source</td>
<td>Type the source in this field.</td>
</tr>
<tr>
<td>User</td>
<td>Type the user name in this field.</td>
</tr>
<tr>
<td>Match in Event Description</td>
<td>Type a sub-string of the description that needs to be matched.</td>
</tr>
<tr>
<td>More information</td>
<td>Type the additional information about the event category in this field.</td>
</tr>
</tbody>
</table>

**NOTE**

If a field is left blank, a wildcard match for that field is assumed. For example, leaving the user field blank implies that any value in that field is acceptable.
5. Enter appropriate data in the relevant fields.
6. Click **Add** and then click **Save**.

### Modify Categories
This option helps you modify Categories.

1. To modify categories, right-click the Category that you want to modify.
   
   EventTracker displays the shortcut menu.

   ![Category Management](image)

   **Figure 296**

   2. From the shortcut menu, click **Edit Category**.
   
   EventTracker displays the **Category Details** page on the right pane.

   3. To edit event details, select an event and then click **Edit**.
   
   EventTracker displays the **Event Configuration** pop-up window.

   4. Enter appropriate data and then click **Save**.

### Delete Categories
This option enables you to delete a Category.

1. Right-click the Category that you want to delete.
   
   EventTracker displays the shortcut menu.
2. From the shortcut menu, click **Remove Category**.  
   EventTracker displays the Confirmation message box.
3. Click **OK**.  
   EventTracker deletes the selected Category.

### Delete Event Rules

This option helps you delete Event Rules.

1. Right-click the Category that you want to edit.  
   EventTracker displays the shortcut menu.
2. From the shortcut menu, click **Edit Category**.  
   EventTracker displays the **Category Details** page.
3. Select the **Event Rule** that you want to delete.
4. Click **Delete**.
   EventTracker displays the Confirmation message box.

5. Click **OK**.
   EventTracker deletes the selected event rule.

6. Click **Save** on the **Category Details** page.

### Add Categories as Alerts

This option enables you to add Categories as Alerts.

1. Right-click the Category that you want to add as Alert.
   EventTracker displays the shortcut menu.

2. From the shortcut menu, click **Add as Alert**.
   EventTracker displays the Alert Management -> Event Details page.
   Enter appropriate details as explained in the **Add Custom Alerts**.

### Move Category

This option helps you to move categories.

1. To move a category, right-click the Category that you want to edit.
   EventTracker displays the shortcut menu.
2. From the shortcut menu, click **Move Category**. EventTracker displays the **Category Details** page.

3. Enter appropriate data and then click **Save**.
Chapter 16
Collection Point and Collection Master

In this chapter, you will learn how to:

- View Collection Point Configuration
- Add Collection Masters
- Edit Collection Master Settings
- Delete Collection Master Settings
- View CAB Status
- Resend CAB Files
- Start Collection Master
- View Collection Point Details
- Configure Collection Master listening port
- Delete CAB Files
- Delete Collection Point Details
Collection Point model

As the volume of event logs and the complexity of corporate network infrastructure grow day-by-day at an unfathomable rate, mining the esoteric event log data becomes a taxing task for the network administrator. Prism recognized the gravity of the issue and came up with a holistic and single view management model called Collection Point model.

Collection Point model facilitates you to collect cab files from geographically or logically dispersed branch offices and generate consolidated audit reports from a centralized location. Collection Point works on a client-server model, whereby the Collection Points (clients) installed at the branch office locations periodically send the cab files to the Collection Master (server) installed at the corporate headquarters.

Since Collection Point model utilizes TCP as a transport layer, Collection Master (server) acknowledges every packet sent by Collection Points (clients). This assures recovery from data that is damaged, lost, duplicated, or delivered out of order by the Internet communication system. Moreover, the encryption mechanism assures the confidentiality and integrity of data is not compromised while it traverses through the public network. Every Collection Point (client) can be configured to report up to five Collection Masters (servers) simultaneously.

**Standard Console**

Best suited for (single-level) flat topologies where all monitored nodes report directly to one or more EventTracker Managers.

**Collection Master Console**

It is best suited for hierarchical topologies. Being designated as a Collection Master, receives archives (CAB files) replicated by Collection Points.

**Collection Point Console**

Best suited for hierarchical topologies where all monitored nodes report directly to a local EventTracker Manager, which is designated as a Collection Point, replicates archives (CAB files) to one or more Collection Masters.

**Scalability**

Collection Point model is best suited for organizations having multiple sites. The sites may geographically spread across the globe or do exist in the same precinct but with a robust setup.
Real world scenarios

Scenario 1:

In the below-depicted scenario, all the Collection Points (clients) send their respective cab files periodically to the Collection Master (server) at the corporate headquarters.

Figure 301
Scenario 2:

In this scenario, SITE 1 does exist physically in the same premises, which runs n number of EventTracker Managers. Each EventTracker Manager running Collection Point (client) will send the respective cab files to the Collection Master (server). The crux of the matter is that the Collection Master treats every individual EventTracker Manager running Collection Point (client) and the constellation of EventTracker Agents as different entities, no matter whether they exist in the same campus or on the same floor.

![Diagram](image-url)
Scenario 3:

The scenario above corroborates the statement that one Collection Point (client) could be configured to report up to five Collection Masters (servers).

View Collection Point Configuration

1. To view Collection Point configuration, log on to EventTracker Enterprise.
2. Click Admin dropdown, and then click the Collection Point.
   
   EventTracker displays the Collection Point page.
Add Collection Masters

Every Collection Point can be configured to send CAB files simultaneously up to 5 Collection Masters. The Collection Master may exist in the same domain or in the trusted domain.

1. To configure Collection Master, click the Configure tab if not selected.
2. Click the Add button.
### Collection Point Configuration

#### Configure

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configure</strong></td>
<td>Configured Collection Master(s) details are displayed on this page.</td>
</tr>
<tr>
<td><strong>Destination</strong></td>
<td>Type the name / IP address of the Collection Master.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Default port is 14507. You can modify the port number. Port numbers should be same on both the Collection Master and Collection Point.</td>
</tr>
<tr>
<td><strong>Encrypt Data</strong></td>
<td>Select an appropriate option to encrypt data. Go through the links provided in the section to know more about FIPS compliance.</td>
</tr>
<tr>
<td><strong>Active</strong></td>
<td>Select this checkbox to activate the Collection Master. Collection Point will not send CAB files to the Collection Master(s) that is Inactive.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Type short description about the Collection Master.</td>
</tr>
<tr>
<td><strong>Queue exist CABs</strong></td>
<td>By default, EventTracker selects the Queue exist CABs checkbox and queues all existing CAB files. Clear this checkbox to queue only new CAB files.</td>
</tr>
</tbody>
</table>

---

**NOTE**

By default, EventTracker selects the **Active** checkbox. When you clear this checkbox, Collection Point will not send CAB files to the Collection Master that you have deactivated.

Collection Point can be configured to report up to 5 Collection Masters simultaneously. You can configure as many Collection Masters as possible and activate / deactivate them as the situations demand.
3 Enter/select appropriate data in the relevant fields and then click **Add**.

### Edit Collection Master Settings

1. To edit Collection master settings, click **Configure** tab if not selected.
2. Select the Collection Master, and then click **Edit**.
3. Enter/select appropriate changes in the relevant fields, and then click **Save**.

### Delete Collection Master Settings

1. Click the **Configure** tab if not selected.
2. Select the Collection Master and then click **Delete**.

   EventTracker displays the confirmation pop-up window.

   ![Message from webpage](image)

   **Figure 306**

3. Click **Ok**.

   EventTracker deletes the selected Collection Master Configuration settings

### View and manage CAB Status

This option helps you view status of the CAB files that are transferred and being transferred by the Collection Point to the Collection Master(s).

1. To manage the CAB files, click the **Manage CAB** tab.
Field | Description
--- | ---
Select Destination | Select Destination from the drop-down list. All configured Collection Masters are listed in this drop-down list.
Select CAB Status | Select the status of the CAB files from this drop-down list and then click Show. Available options are Success, Failed, Not Sent, In Progress and Queued.
Sort By | Sort the CAB files based on From date / To date / CAB name.

Resend CAB Files

1. Select the Collection Master from the **Select Destination** drop-down list.
2. Select the status from the **Select CAB Status** drop-down list.
3. Select the required CAB files, and then select **Resend CAB**.
   Collection Point resends the CAB file(s) to the destination(s).
Collection Master

This option helps you open Collection Master Console.

1. To access Collection Master, log on to EventTracker Enterprise.
2. Click the Admin hyperlink, and then click Collection Master.

EventTracker displays the Collection Point Master page.

Field Description
Select Collection Point Select the Collection Point from this drop-down list. All clients reporting to the Collection Master are listed in this drop-down list.
Select CAB status Select the status of the cab files from this drop-down list and then click Show. Available options are Success, Failed, and In Progress.
Collection Master Port No By default, Collection Master and Collection Point communicate through port 14507. You can also change this port no. Type the port number and then click Save.

Field Description
Name Name of the CAB file.
### Field Description

- **Period**: Start and end time of events accommodated in the CAB file.
- **Collection Point Name**: Name of the Collection Point that forwarded the CAB file.
- **Size (KB)**: Size of the CAB file in kilobytes.
- **Transmission start time**: Date and time when the Collection Point started to send the CAB file.
- **Transmission Time**: Time taken to reach the destination.
- **Status**: Transmission status of CAB files.

### View Collection Point Details

This option helps you view details of the Collection Points that are forwarding CAB files to the Collection Master.

1. To view Collection Point data, click the **Collection Point Details** tab.

EventTracker displays the Collection Point Details page.

#### Figure 309

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection Point Name</td>
<td>Displays the name of the Collection Points that are reporting to the Collection Master.</td>
</tr>
<tr>
<td>Version Info</td>
<td>Displays the version of the Collection Points.</td>
</tr>
</tbody>
</table>
| Archive Path           | Displays the path of the folder where cab files of the respective Collection Points are stored at the Collection Master computer. Example: ...
  \Program Files\Prism Microsystems\EventTracker\Archives\NEW YORK[192.168.1.38] |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Received CAB Time</td>
<td>Date and Time when the Collection Master received the last CAB file.</td>
</tr>
<tr>
<td>Last Received CAB Name</td>
<td>Name of the last CAB file that is received from Collection Points.</td>
</tr>
</tbody>
</table>

Configure Collection Master listening port

This option helps you configure listening port of the Collection Master. By default, EventTracker Collection Master and Collection Points communicate through port 14507. You can configure this port number from the Collection Master Console. If you configure a new port other than the default one, you have to configure at the Collection Points with the same port number for successful communication between the Collection Points and Collection Master.

1. To configure Collection Master listening port, click the **CAB Status** tab.
2. Type the port number in the **Collection Master Port No** field.
3. Click **Save**.

Delete CAB Files

1. To delete CAB files, click the **CAB Status** tab.
2. Select the checkbox on the title bar to select all CAB files.
   (OR)
   Select the checkbox against the CAB files.
3. Click **Delete**.

Delete Collection Point Details

1. To delete Collection Point data, click the **Collection Point Details** tab.
2. Select the Collection Point and then select **Delete**.

**NOTE**

When you delete details of a particular Collection Point, EventTracker will also delete their respective CAB files.
Chapter 17
Event Filters

In this chapter, you will learn how to:

- Configure Event Filters
- Configure Event Filters with exception
Filter Events from View

Fine grain filtering for meaningful monitoring support for both view and source filters based on wildcard matches of id, type, source, user, event description.

- Filter non-essential events – collect and manage only important events – minimum traffic.
- Filter any event(s) for display only (these are still logged into the event database).
- Monitor only specific events.
  
  Example,
  
  - Log all events into the database but display only Audit Failure.
  - Create a separate monitoring window for Exchange Server events.
- Filter any specific category of events
  
  Example, Monitor all events except information events.
- Exclusive filters according to your own criteria –
  
  Example, Filter all Information events except defined list.
  
  A few specific events are frequently generated but you wish to exclude these and monitor all other events.
- BOOLEAN operators in filter policy definitions – provides the ability to match multiple strings in fields to create sophisticated filter policy definition.

Configure Event Filters

This option enables you to filter events of minor significance from the view.

1. To configure Event Filters, log on to EventTracker Enterprise. Click the Admin dropdown, and then click Event Filters.
   
   EventTracker displays the Event Filters page.
2. Click Add Filter.
   
   EventTracker displays the Event Filter Configuration page.
3. Enter the name of the filter in the **Filter Name** field and a brief description in the **Description** field.
4. By default, EventTracker selects the **Active** checkbox. Uncheck the checkbox to deactivate the filter. EventTracker retains the configuration settings. You can again activate the event filter by checking the "active" checkbox.
5. In **Event Filter Configuration** page, click **Add**.
6. In **Add Event** dialog box, enter appropriate data in the relevant fields.

**NOTE**

If you leave a field blank, EventTracker assumes a wildcard match for that field. For example, leaving the user field blank implies that any value in that field is acceptable.

7. Click **Add**.
   EventTracker displays the 'Event Filter Configuration' page with newly added filter details.
8. Click the **Systems** tab.
   **All Systems** option is selected by default, which means the filter is applied to all the monitored systems.
9. Select required system groups / systems to apply the filter.
10. Click **Finish**.
    EventTracker displays the Event Filters page with newly added event filter.
11. Click **Activate Now** to activate the event filter.

**Configure Event Filters with Exception**

This option enables you to filter events with an exception.

1. On the **Event Filters** page, click the respective Filter Name to modify.

EventTracker displays the **Event Filter Configuration** page.

2. Click the **Filter Exception** tab.
3 Click **Add** to add filter exception criteria.

4 Enter/select appropriately in the relevant fields, and then click **Add**.
   
   EventTracker displays the **Filter Exception** tab with newly added filter exception.

5 Click the **Finish** button to save the changes.

**NOTE**

For example, if you wish to filter out all events of **Event Type** - **Information** but interested in monitoring a particular event for example – Event ID 3223. Then in this case, all events of 'Information' event type will be filtered out but with one exception of event 3223.

6 Click **Activate Now** to activate the event filter.

**Understand Filters and Filter Exceptions**

This section helps you understand how filters and filter exceptions work.

1 Click the name of the event filter.

2 In the **Filter Detail** tab, select the filter rule to be deleted, and then click the **Delete** button.
   
   EventTracker displays the confirmation message box.

3 Click **OK** to remove the filter details.
EventTracker removes the filter details.

4 Click the Filter Exception tab.
The filter exception you have set earlier remains unaltered.

5 Select the exception rule to be deleted, and then click the Delete button.
EventTracker displays the confirmation message box.

6 Click OK to remove filter exceptions.
EventTracker removes the selected filter exception.

---

**NOTE**

It is obvious from the above scenario; it is your responsibility to manage Filters and Filter Exceptions. The table given below will provide you a clear idea how the combination of Filters and Filter Exceptions work.

<table>
<thead>
<tr>
<th>Filter</th>
<th>Filter Exception</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>N</td>
<td>EventTracker filters all events from the view.</td>
</tr>
<tr>
<td>N</td>
<td>Y</td>
<td>EventTracker allows all events.</td>
</tr>
<tr>
<td>Y</td>
<td>Y</td>
<td>EventTracker allows events with exception.</td>
</tr>
<tr>
<td>N</td>
<td>N</td>
<td>EventTracker allows all events.</td>
</tr>
</tbody>
</table>

---

**View and Edit Alert Details**

This option facilitates to locate alert from the alert event displayed in the Management Console.

- Right-click an event and select the Show Alert Rule option from the shortcut menu to view the exact alert, which caused this event.
Chapter 18
EventVault

In this chapter, you will learn how to use:

- EventVault Manager
- Verify Archive Files
- Export Archive Files
EventVault Manager

EventVault Manager provides the capability to archive the events from the EventTracker database. The EventVault provides a simple, but important mechanism to securely archive event logs for future use and more specifically for auditing purposes.

In most enterprise networks with multiple critical servers and workstations, the event log data can become huge and unmanageable. Those event data may not be immediately required once the initial analysis is completed. At the same time they cannot be completely discarded, as they will be required for future audits. EventVault solves this problem and provides mechanisms to identify if any of the EventVault data has been tampered with.

Archives are .mdb files that are compressed into .cab files called as ‘EventBox” and are stored in the Archives folder. If EventTracker is installed in the default path then these files could be located in the archives directory. The range of events that each EventBox contains is stored into an index file in the Archives folder. These EventBoxes are sorted by period and can be viewed from EventVault Manager.

To start EventVault Manager

1. Click the Admin dropdown, and then select EventVault.

EventTracker displays EventVault Manager screen.
<table>
<thead>
<tr>
<th>Click</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td>Configure EventVault Manager to archive the events from EventTracker database.</td>
</tr>
<tr>
<td>Verify</td>
<td>Verify the integrity of selected EventBoxes.</td>
</tr>
<tr>
<td>Show</td>
<td>View the CAB files for a specific period.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From</td>
<td>Date &amp; Time of the first event stored in the CAB file.</td>
</tr>
<tr>
<td>To</td>
<td>Date &amp; Time of the last event stored in the CAB file.</td>
</tr>
<tr>
<td>Archive Name</td>
<td>Name of the CAB file. etar1269949644-14505.cab</td>
</tr>
<tr>
<td></td>
<td>etar – EventTracker Archive</td>
</tr>
<tr>
<td></td>
<td>1269949644 – Time ticks</td>
</tr>
<tr>
<td></td>
<td>14505 – Port number (through which the EventTracker Receiver service received the events)</td>
</tr>
<tr>
<td></td>
<td>cab – File extension of cabinet files</td>
</tr>
<tr>
<td>Path</td>
<td>Path of the folder where the archives are stored typically, EventTracker install path\ port number \ year \ month</td>
</tr>
<tr>
<td>Size (KB)</td>
<td>Size of the CAB file in KB.</td>
</tr>
<tr>
<td>Total Events</td>
<td>Total number of events accommodated in the CAB file.</td>
</tr>
<tr>
<td>Port Number</td>
<td>Port number through which the EventTracker Receiver service received the events.</td>
</tr>
<tr>
<td>Raw data</td>
<td>Display size of that particular raw data available</td>
</tr>
<tr>
<td>Archives</td>
<td>Display size of that particular archive</td>
</tr>
</tbody>
</table>
Verify Archive File(s)

1. To verify the archive files, select any Archive file option and then select **Verify**.

![Verify Archive File](image)

Figure 315

The data is downloaded in a text file.

2. Click **Open** to view the result.

   (OR)

3. Save the file in local drive and then click **Open** to view result.
Export Archive File(s)

1. To export the archive files, select any Archive file, and then select the **Export** button.

![Figure 316](image)

The data will be exported in an excel file.

2. Click **Open** to view the result.

   (OR)

3. Save the file in local drive and then click **Open** to view result.

EventVault Manager Configuration

1. Click the **Configuration** hyperlink to configure **EventVault Manager**. **Configuration** window displays.
2. Enter relevant data and click **Ok**.

   For detail information refer chapter Control Panel -> EventVault.
Chapter 19
IP Lookup Configuration

In this chapter, you will learn about:

- Add IP Lookup
IP lookup Configuration

Every machine that is on a TCP/IP network (a local network, or the Internet) has a unique Internet Protocol (IP) address. IP-Lookup helps you to find information about your current IP address or any other IP address. Internet Protocol (IP) address can be resolved to the corresponding domain name by using IP lookup configuration feature. User can use any IP lookup website/URL which accepts IP address as input and resolves it to domain name. It supports both IPv4 and IPv6 addresses.

To Add IP Lookup

1) Click the Add New button.

![Add IP Lookup](image)

**EventTracker :: Add IP Lookup** window displays.

2) Enter the Display Name: in the box.
   Users can give any relevant name in display name field.

3) Enter the URL.
   User can provide any IP lookup website in this field. Configure IP lookup configuration as per usage and add IP lookup address.

4) Click the Save button.

5) In Behavior menu, select Security dropdown.

6) Select any IP address Activity, and then select the Go button.
   The respective IP address is displayed as configured in Add IP Lookup configuration.
Chapter 20
Manager

In this chapter, you will learn how to use:

- Configure Alert Events
- Syslog/Virtual Collection Point
- Direct Log Archiver/Netflow Receiver
- Agent Settings
- E-mail Configuration
- Status Tracker
Configure - Alert Events

Enable Alert Notification

This option helps you track success/failure alert notification status.

1) To enable alert notification, click the Admin dropdown, and then click Manager.
2) Click the Configuration tab, if not selected.

3) Select the Enable alert notification status checkbox, if not selected by default.

**NOTE**

You might receive notifications for the configured alerts, but you may not be able to track the success/failure status of those notifications if you disable this option.

4) To turn off alerts, click Turn off alerts option.
5) To turn off filters, click Turn off filters option.
6) Click Save.
Purge Alert Events Cache

This option helps you purge alert events cache. By default, EventTracker retains event data for seven days. You can configure to hold minimum 24-hour and maximum 90 days event data. You cannot completely purge the cache.

1) To purge alert events cache, in **Manager Configuration** page, click the **Configuration** tab.
2) Select the **Enable Alert Events Cache for Analyzing Alerts** checkbox, if not selected by default.
3) EventTracker enable **Purge events from cache older than – days** field, if not selected by default.
4) Type the duration in **Purge events from cache older than – days** field.
5) Click **Save**.

Enable Remedial Actions

It is mandatory to enable remedial action at the manager console. Otherwise, you cannot execute remedial action at the agent systems.

1) To configure Remedial Actions, in **Manager Configuration** page, click the **Configuration** tab.
2) Select the **Enable Remedial Action** checkbox, if not selected by default.
   
   EventTracker displays the Caution dialog box.

   ![Caution Dialog Box](image)

   *Figure 320*

3) Click **OK**, and then click **Save**.

Suppress Duplicate Alerts

EventTracker provides the facility of generating user configurable alerts for events received by the EventTracker. This feature is very useful in case the user is not always available at the manager console.

In case the multiple instances of an event with a configured alert are received in a short period of time then a large number of alerts will be generated, this could confuse the user.

‘Duplicate Alert Suppression’ feature will handle such a deluge of alerts by suppressing any alert in case it is a duplicate of an alert received earlier, within a particular time frame.
The above settings inform the EventTracker to allow a MAXIMUM of 5 DUPLICATE alerts to be triggered within a timeframe of 300 seconds. An alert is considered a duplicate only if it is triggered by the same event.

This option helps you suppress duplicate alerts.

1) To suppress duplicate Alerts, in Manager Configuration page, click the Configuration tab.
2) Select the Suppress Duplicate Alerts checkbox.

![Figure 321](image)

EventTracker enables the Alert suppression interval and Maximum number of alerts allowed fields.

3) Enter appropriate data and then click Save.

Enable alert e-mail footer option

This option enables the footer option in e-mail. If the email footer is enabled then all the default alerts which are enabled will contain the manager email footer content. But when the user configures a new alert with email action then the user can provide a custom email footer also for the particular alert.

1) To enable footer option in email, in Manager Configuration page, click the Configuration tab.
2) Select the Enables alert e-mail footer option.

![Figure 322](image)

3) Provide an appropriate description in Alert e-mail footer and then click Save.

Configure Correlation Receiver

This option helps you configure correlation receiver port to receive results of correlation rules.
1) To configure correlation receiver port, in Manager Configuration page, click the Configuration tab.

2) Type the port number in the Send results of all correlation rules to port field. Click Save.

**NOTE**

If ‘Event Correlator’ is not installed, then ‘Correlation Receiver’ pane is grayed out/ disabled. By default, correlation receiver receives rules through port 14509. For detail information about Correlator, refer EventTracker - Event Correlator.

Configure Keyword Indexer

This option helps you enable the ‘Keyword Indexer’ service to index keywords.

1) To Enable Keyword Indexing option in Manager Configuration page, click the Configuration tab.

2) Select the Enable Keyword Indexing checkbox.

EventTracker displays caution dialog box.

**NOTE**

- EventTracker by default selects Show statistics and Show graph options in the Log search pane.
- Show statistics and Show graph option is not enabled after up-gradation.
3) **Clear the Enable Keyword Indexing checkbox** if the 'Keyword Indexer' hogs the system resources.

3) **Click OK** to continue.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Indexing service</td>
<td>Keyword indexing process is carried out on the local machine. You are not allowed to change this option.</td>
</tr>
<tr>
<td>Remote Indexing service</td>
<td>Keyword indexing process is carried out on a remote machine to reduce the resource utilizations of the manager. You are not allowed to change this option. Click <a href="#">here</a> for more information on Remote Indexing.</td>
</tr>
<tr>
<td>Show statistic</td>
<td>Show/hide the statistics in the log search page. Clear the Show statistic checkbox to view only graphs in the log search page.</td>
</tr>
<tr>
<td>Show graph</td>
<td>Show/hide the graphs in the log search page. Clear the Show graph checkbox to view only statistics in the log search page.</td>
</tr>
</tbody>
</table>

4) **Click Save**.

**NOTE**

'Keyword Indexing' option is enabled by default on fresh install and will be grayed out in case the 'Keyword Indexing' feature is not present in the certificate file.

**Configure EventTracker Knowledge Base Web Site**

This option enables you to configure 'EventTracker Knowledge Base' Web site.

1) **To configure Knowledge Base website**, in **Manager Configuration** page, click the **Configuration** tab.

```
<table>
<thead>
<tr>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>KB website    : <a href="http://kb.prismmicrosys.com">http://kb.prismmicrosys.com</a></td>
</tr>
<tr>
<td>☑ Check for knowledge base updates</td>
</tr>
</tbody>
</table>
```

**Figure 325**
2) Type the URL of the Knowledge Base Web site in the KB Website field.

3) Check the Check for knowledge base updates option, if unchecked.

4) Click Save.

Configure Logon Banner

This option helps you configure the custom log on message. This banner is displayed to anyone who tries to gain access to EventTracker, prior to typing the user credentials. This could be a warning message or a custom message such as ‘Welcome! User” or ‘This system is for the use of authorized users only.’

Configure Cost Savings

Enable 'Collecting Cost Savings Information' option to run reports (available in Reports Menu -> Flex Reports -> Cost Savings). Enabling this option might hit the performance of ‘EventTracker Archiver’ process if the load of events to be processed is heavy.

1) In Manager Configuration page, click the Configuration tab, if not selected.

2) Check the Collect Cost Savings Information option, and then click Save.

Syslog / Virtual Collection Point

EventTracker by default selects the ‘Enable syslog receiver’ option to enable the EventTracker receiver to receive syslogs sent by non-Windows systems.
To enable syslog receiver, in Manager Configuration page, click the syslog / Virtual Collection Point tab.

Select the Enable syslog receiver checkbox, if not selected by default, and then click Save.

Monitor syslogs for UNIX
For monitoring syslog events, you must configure the UNIX computer to forward syslog events to the computer where the EventTracker Manager is installed. The default syslog port is UDP Port=514. Also, see the FAQ on syslog.

1. To configure UNIX systems to forward syslog messages to EventTracker, identify the IP Address of the computer that is hosting the EventTracker Manager.
2. Log on with the root account in the UNIX computer.
3. Open the syslog.conf file in a text editor. The default path of the syslog.conf file is /etc/syslog.conf.
4. Append the configuration details in the syslog.conf file to forward syslog messages to the EventTracker Manager computer.
5. Save and close the syslog.conf file.
6. Stop and restart the syslog daemon (syslog).
7. Example: To forward syslog error messages to the IP address 192.192.150.150, add the following detail to the syslog.conf file. *.err @192.192.150.150

**NOTE**
For more information, refer the syslog.conf or syslog MAN pages.
Syslog configuration may be platform-dependent and it is recommended that you check the platform documentation.

Virtual Collection Points
Virtual Collection Points (VCP) enable the existing receiver to behave like a collection master without having the physical Collection Points installed. The Existing Collection Point (CP-CM model) requires physically organized Collection Points reporting to a Collection Master. CP-CM model requires a number of hardware facilities and a large degree of deployment difficulty.

VCP provides the solution to break down the huge volume of input events using the existing set up with minimal configuration changes, thus helps to process the received data in a short time at the reporting end.
Configure EventTracker Receiver to Listen on Multiple Ports

EventTracker Receiver can be configured to listen to any number of ports for Traps and Unix/Linux/Solaris syslogs.

The engine limit for number of VCP's has been removed where as from the UI (Admin -> Manager) still there is a limit of 20 VCPs (10 Windows & 10 SYSLOG). Depending upon the system capacity (Disk, RAM, CPU, etc..) any number of VCPs can be created. Please contact support@eventtracker.com to increase the limit.

<table>
<thead>
<tr>
<th>ET Modules</th>
<th>Suggested Trap Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>EventTracker Receiver (Incoming)</td>
<td>14505 default port.</td>
</tr>
<tr>
<td></td>
<td>14515, 14525, 14535, 14545, 14555, 14565,</td>
</tr>
<tr>
<td></td>
<td>14575, 14585, 14595</td>
</tr>
<tr>
<td></td>
<td>514 (UDP/TCP) for syslogs.</td>
</tr>
</tbody>
</table>

For more information, refer Virtual Collection Point (VCP).
Virtual Collection Points for syslogs

Configure EventTracker Receiver Ports

This option helps you configure EventTracker receiver to listen on different ports.

1. Click the **syslog / Virtual Collection Point** tab.
2. Check **Enable syslog receiver** option if not checked by default, and then click **Add**.

   EventTracker displays the **Syslog Receiver Port** dialog box.

3. Type appropriate **Port Number** and **Description** in the respective fields.

   **NOTE**

   The suggested ports start from 1 to 65535 and any of the available ports can be configured.

4. In the **Cache path** field, type or browse the path to save the cache files.

   This is not mandatory, but changing the location would result in enhancing application's performance.

5. Click **Save**.
Forward Raw syslog Messages

This option helps you forward received syslog messages in raw format i.e. forwarded with the same format as it is received to a specified destination.

1. To forward syslog messages in raw format, select the **Raw syslog Forward** checkbox.

![Figure 329](image)

2. Type the host name or IP address of the destination in the **Trap Destination** field.

3. Select an appropriate **Mode** of transport.

4. Type an appropriate port with respect to the mode chosen.
   
   The suggested ports start from 1 to 65535 and any of the available ports can be configured.

5. Click **Save**.

Virtual Collection Points for Windows Events

EventTracker Receiver can be configured to listen on 10 ports for Windows Events.

Example Scenario

Consider EventTracker Agents in computers Sys2 and Sys3 are forwarding events to Sys1 (EventTracker Manager). By default, the communication happens through port 14505. Suppose you want to configure different ports say for example 14515 and 14525 for Sys2 and Sys3 respectively, do the following:
Computer: Sys1 – Configure Ports

1. In syslog / Virtual Collection Point tab, click Add button under Virtual Collection Points pane. EventTracker displays the Receiver Port dialog box.

   ![Receiver Port Dialog Box](image)

   **Figure 330**

2. Type appropriate Port Number and Description in the respective fields.
3. In the Cache path field, type/ browse the path to save the cache files.
4. Click Save.
   
   EventTracker adds the newly configured ports.
   
   EventTracker updates these changes in evtrxer.ini file (...\Program Files\Prism Microsystems\EventTracker) EventTracker creates EtaConfig_14515.ini & EtaConfig_14525.ini files in RemoteInstaller folder (...\Program Files\Prism Microsystems\EventTracker\RemoteInstaller).

### EventTracker Modules & Trap Ports utilized

<table>
<thead>
<tr>
<th>EventTracker Modules</th>
<th>Trap Ports utilized</th>
</tr>
</thead>
<tbody>
<tr>
<td>EventTracker Receiver</td>
<td>14505, 14515, 14525</td>
</tr>
</tbody>
</table>

Upgrade Agent (Sys2) from Manager (Sys1)

1. Click the Admin dropdown, and then click Systems.
2. Move the pointer over the system (sys2) that you wish to upgrade, and then click the dropdown.
3. From the shortcut menu, select **Upgrade agent**.
4. Select an appropriate agent to upgrade, and then click **Next**.
5. Select **Advanced**, and then select **Custom config** option.
6. Select the path of the custom `.ini` file (**EtaConfig_14515.ini**) from the **File** dropdown.
7. Click **Upgrade**.
   EventTracker overwrites **etaconfig.ini** file with new settings.

**Upgrade Agent (Sys2) from Manager (Sys1)**

1. Click the **Admin** dropdown, and then click **Systems**.
2. Move the pointer over the system (sys2) that you wish to upgrade, and then click the dropdown.
3. Click the system (sys3) that you wish to upgrade.
4. From the shortcut menu, select **Upgrade agent**.
5. Select an appropriate agent to upgrade, and then click **Next**.
6. Select **Advanced**, and then select **Custom config** option.
7. Select the path of the custom `.ini` file (**EtaConfig_14515.ini**) from the **File** dropdown.
8. Click **Upgrade**.
   EventTracker overwrites **etaconfig.ini** file with new settings.

**Direct Log Archiver / Netflow Receiver**

**Configure Direct Log File Archiver**

This option helps you archive log files collected from external sources.

1. To archive log files collected from external resources, click the **Admin** dropdown, and then click **Manager**.
2. Click the **Direct Log Archiver / NetFlow Receiver** tab.
3. Select the **Direct log file archiving from external sources** checkbox, if not selected.
4. To purge the log files, enter the number of days in **Purge files after – days** field.
5. Select a port from the **Associated virtual collection point** drop-down list.
6. Assign an exclusive port that is not associated with any collection groups.
7. Click **Save**.
   For more information about Direct Log Archiver (DLA), refer [DLA](#).

**Enable Netflow Receiver**

This option enables you to enable netflow receiver and read netflow logs.
1) To enable Netflow receiver, click the Admin dropdown, click Manager, and then click the Direct Log Archiver/Netflow Receiver tab.

2) Check the Enable netflow receiver option.
   EventTracker enables the Netflow data storage folder field.

3) Type the path of the folder or click the Browse button to select the folder.
   By default, netflow receiver receives netflow logs through 9991, 9992, and 9993 ports.

Add Netflow Receiver Port
This option helps to add netflow receiver port.

1. Click Add.
   EventTracker displays the NetFlow Receiver pop-up window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Type the netflow receiver port number.</td>
</tr>
<tr>
<td>Drop Rate</td>
<td>Drop Rate configures a sampling rate. This is a ‘REG_MULTI_SZ’ key with an integer value per port. The meaning of the value is that one packet in ‘Drop Rate’ packets will be discarded. Hence ‘Drop Rate’ of 2 would cause every other packet to be discarded. In this version sampling is deterministic (not probabilistic). In the absence of this registry entry, the default will be taken to be 0.</td>
</tr>
<tr>
<td>Decode Packet</td>
<td>Instruct the service how to record the sampled data. The key ‘Decode Packet’ is also of type ‘REG_MULTI_SZ’ and is a list of Boolean values (‘true’/’false’) that indicate whether the packets received on the corresponding port should be decoded and written to the ‘netflowcollectorXXX.txt’ file.</td>
</tr>
<tr>
<td>Record Binary</td>
<td>Instruct the service how to record the sampled data. Setting these values to ‘true’ will cause the received packets to be written to files simply as</td>
</tr>
</tbody>
</table>
Field | Description
--- | ---
| | binary data. Only one of 'Decode Packet' or 'Record Binary' may be both true for any particular port. If both are set to 'true' the Port will act as if 'Decode Packet' was set to true and 'Record Binary' was set to false. In the absence of these registry values the default will be to assume the 'Decode Packet' value is true and the 'Record Binary' value is false.

2 Select/enter appropriate data in the relevant fields, and then click OK.
3 Click Save.
For detail information about Netflow, refer Netflow.

Agent Settings

Configure Agent File Transfer Settings
This option enables you to configure agent file transfer settings.

1 Select Admin drop down, and then select Manager.
2 In the Manager Configuration page, click the Agent Settings tab.
3 Select the Allow direct agent file transfers checkbox, if not selected.

Associated virtual collection point is the port that you have configured for Direct Log Archiver.

By default, EventTracker stores the files transferred by the agents in the ...\Program Files\Prism Microsystems\EventTracker\DLA folder.

4 In the Data Store Folder field, type the path for new folder if you wish to change the file transfer location.

(OR)

Click the Browse button to navigate and select a folder.
5 Click Save.

Configure Config Assessment Settings
This option enables you to configure Config assessment settings.

1 Select Admin drop down, and then select Manager.
2 In the Manager Configuration page, click the Agent Settings tab.
3 Select the Encrypt Data Transfer checkbox, if not selected.

By default, EventTracker stores the SCAP files in the ...\Program Files\Prism Microsystems\EventTracker\SCAP\ folder.

4 In the Data Store Folder field, type the path for new folder if you wish to change the file transfer location.
(OR)

Click the **Browse** button to navigate and select a folder.

5  Click **Save**.

## Configure E-mail Settings

This option will help you to configure email settings. These are mandatory configuration settings to "Deliver report via E-mail" or "Notify report generation via E-mail" upon generation of scheduled reports. Additionally, to "Send via E-mail" the published reports.

1  Select **Admin** drop down, and then select **Manager**.

2  In the **Manager Configuration** page, click the **E-Mail configuration** tab.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Server</td>
<td>Type the name or IP address of your enterprise mail server.</td>
</tr>
<tr>
<td>Port</td>
<td>Type a valid SMTP server port number.</td>
</tr>
<tr>
<td>From E-mail id</td>
<td>Type a valid sender e-mail address.</td>
</tr>
<tr>
<td>To E-mail id</td>
<td>Type a valid recipient e-mail address.</td>
</tr>
<tr>
<td>Email attachment maximum size</td>
<td>Type the maximum size of attachment file in terms of MB. The default size will be 5 MB.</td>
</tr>
<tr>
<td>Enable authentication</td>
<td>Provides an access control mechanism. It can be used to allow legitimate users to relay mail while denying relay service to unauthorized users, such as spammers. Select this checkbox and type valid administrator user name and password.</td>
</tr>
<tr>
<td>Test E-mail</td>
<td>Click to check whether you have provided valid data. EventTracker displays the confirmation message box. Click OK to continue. EventTracker displays &quot;success&quot; message if the configuration is correct and &quot;failed&quot; message if the configuration is not correct.</td>
</tr>
</tbody>
</table>

3  Provide the details in required fields, and then click the **Save** button.

## Manage Email Accounts

All the Email Ids configured in alerts, reports, and flex reports can be managed from this Email search utility. The Email Ids can be replaced with a new Email Id or removed if it is no more in use or invalid address.

1  In the **Manager Configuration** page, click the **E-Mail configuration** tab.

2  Fill the required information to configure the SMTP server for sending email, and then click the **Save** button.

3  Click the **Manage email** hyperlink.
EventTracker displays **Email search utility** window.

![Email search utility window](image)

**Figure 332**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configured Email</td>
<td>The list of all configured email Ids.</td>
</tr>
<tr>
<td>Alerts</td>
<td>The list of alerts configured with the selected email Id.</td>
</tr>
<tr>
<td>Reports</td>
<td>The list of reports configured with the selected email Id.</td>
</tr>
<tr>
<td>Export alerts to excel / Export reports to excel</td>
<td>Click to export the alerts or reports along with the configured email Id.</td>
</tr>
<tr>
<td>Change Option</td>
<td>Remove or replace the configured email Id.</td>
</tr>
</tbody>
</table>

4. From **Configured Email** dropdown, select the required email Id, and then click the **Find** button.

The alert(s) and report(s) configured with the email Id will be displayed under **Alerts** and **Reports** tab, respectively.
To replace Email Id

1. Click the **Manage email** hyperlink.
   
   EventTracker displays 'E-mail search utility' window.

2. In the **Change Options** pane, select **Replace** from the dropdown, if not selected.
   
   ![Figure 333](image)

3. From the **Email ID** dropdown, select the Email Id to be replaced.

4. In **With** field, type the Email Id to be replaced.

5. In the ‘in’ field select where the Email Id is to be replaced. The options are in **Alerts** or in **Reports**.

6. Click the **Go** button.
   
   EventTracker displays confirmation message box.

7. Click the **OK** button.
   
   EventTracker displays success message box.

   ![Figure 334](image)

If any special character or wrong Email Id is provided, then EventTracker will display the error message.

   ![Figure 335](image)
8 Click the OK button in the success message box.

9 To verify the replacement, click the Configured Email dropdown, select the replaced Email address, and then click the Find button.

   EventTracker will display the alerts or reports configured with the selected Email Id.

To Remove Email ID

1 Click the Manage email hyperlink.

   EventTracker displays ‘E-mail search utility’ window.

2 In the Change Options pane, select Remove from the dropdown.

   ![Figure 336](image)

3 From the Email ID dropdown, select the Email Id to be removed.

4 In the ‘in’ field select where the Email Id is to be removed. The options are in Alerts or in Reports.

5 Click the Go button.

   EventTracker displays confirmation message box.

6 Click the OK button.

   EventTracker displays success message box.

   If only one report or alert is configured with the selected Email address then EventTracker will not allow remove the Email address.

   ![Figure 337](image)

7 Click the OK button in the success message box.
Configure StatusTracker Settings

1. Click the **Admin** dropdown, click **Manager**, and then click the **StatusTracker** tab.

2. In the **Purge frequency for StatusTracker** field, enter the number of days. The StatusTracker polling summary data will be purged after the specified number of day(s).

3. Check the **Synchronize discovery with EventTracker** option.
   
   Select this option if you wish to populate the groups along with their respective systems when "Auto discover" is carried out in System Manager.

4. Enter the string name in the **Community string for SNMP devices** field to configure the community string for SNMP devices.

5. Click **Save**.
Chapter 21
Parsing Rules

In this chapter, you will learn how to:

- Parsing Rule
- Components of Parsing Rules
- Add Token Value Groups
- Template
About Parsing Rule

Parsing rules are user-defined tokens. Apart from the standard report definition format, EventTracker reports module provides a simple, yet powerful log Flex Reports, reporting facility.

It helps to parse and include parts of clogged syslog like messages and Windows event descriptions as columns in reports.

Parsing rule helps you define new tokens, bind it with the dynamic report templates and generate flex reports. EventTracker displays the parsed data under those tokens defined by you.

While configuring Flex reports, you can also select the report columns you are interested in, apply filters, sort report columns, and rearrange the order of the columns that should appear in reports.

To put it in a nutshell Parsing rule helps to manipulate data and generate comprehensible reports.

The Need for Adding Parsing Rule in Flex Report

Scouring the components of log data is massively time. Data contains pieces of information.

Since valuable information is dumped in the log description, there should be a way to break down and analyze the data, and turn it into valuable business information.

Furthermore, there is no standardized message format as various vendors of NIX systems follow different conventions.

For example, comma-separates values, fixed-width text, and free-form text. An Administrator to decipher syslog messages.

Usage of Tokens in EventTracker

A common question that arises would be,

- ‘Is it not sufficient to generate Flex reports with templates provided with EventTracker?’
- Is EventTracker flexible enough to add tokens?
- If so, does not EventTracker provide any predefined tokens to simplify my work?
- Is it possible to define my own tokens?

If you’re preoccupied with these questions, relax!

EventTracker is shipped along with a precisely defined set of tokens for your convenience. Should you wish to add tokens if these predefined tokens do not align with your requirement, EventTracker provides adequate facilities to add/modify/delete tokens. Otherwise, default tokens are sufficient.
**FAQ:** If I bind new Token-value to the parsing rule, will those Token-values be saved permanently in the database?

It’s left to your discretion. While defining new Token-Value, you have the luxury of saving the Token-Values permanently in the database or binding the Token-Value just for one instance of report generation.

**Prior Knowledge**

It is appreciable to have comfortable knowledge and understanding of syslog message formats of different flavors of NIX systems. Though the fundamental tenets insist on simplicity, the creators of syslog write the messages according to their whim and caprice. So suit yourself to the environment you work in to understand the syntax and semantics of syslog messages.

**Components of Parsing Rules**

Components of Parsing rules are the basic elements that are essential in framing your queries to extract required data from the log messages.

**Token**

Token is the ‘key’ that reporter engine regards as a reference point and considers the string that succeeds for parsing. It is optional to provide token and can contain:

- Characters (a, b, c...)
- Numbers (1, 2, 3...)
- Special characters (#, $, %, space character...)
- or combination of all three (a1#)

**Parsing Rule Occurrences**

If there are multiple occurrences of token in the description, reporter engine considers only the first occurrence as reference point. So, be specific while you frame your query.

**Display Name**

Display Name is a temporarily assumed name (alias) for the queried string. This name will appear as token in the report. It is mandatory to provide display name and should be unique throughout the report. You can select any name and can contain:

- characters
• numbers
• or combination of these two
• special characters are not accepted

Separator
Separator is a character or word which separates key and value in the description. It is optional to provide separator and can contain:
• characters
• numbers
• special characters
• or combination of all three

Terminator
Terminator is character or word to determine end of key value pair in description. The queried string is extracted till the first occurrence of the terminator. It is optional to provide terminator and can contain:
• Characters
• Numbers
• Special characters
• or combination of all three
Thus, parsing rule offers flexibility to customize:
• Data selection
• Sort sequences

View Parsing Rules
1 To view Parsing Rules, click the Admin drop down, select Parsing Rules.
The default Token-Value groups display. EventTracker provides predefined parsing rules.
Add Token Value Groups

The default Token-Value Groups are available in the Token Value pane.

1. To add a new group, right click **Token-Value Groups**, select **New Group**.
2. Enter the relevant group name, description and then click **Add**.
   A new token value group is created.
Add Rule

1. To add a new rule, click the **Add Rule** button.

2. Enter relevant data, and then click **Add**.
   
   **Ex:** The following Key value pairs can be added in the following way.
   
   Display name: Logs Summary
   Token: Log Time
   Separator is `:`
   Terminator: \n
   The new rule displays in Token-Value pane.
To edit the token value, click **Edit**. Make the required changes and then click **Save**.

To delete the token value, click the **Delete** button.

To the token value to another group, click **Move to group**.

**NOTE**

You can move to another group if there are other Token-Value groups existing apart from the Default one.

**Token Value Wizard**

1. To view **Token Value Wizard**, click the **Admin** drop down, select **Parsing Rules**. The default **Token-Value** groups display.

2. Select the **Token Value Wizard** button. The Token-Value Wizard displays Sample Logs window.
3 Click any one of the Extract Token Value Pairs icon. Create Token-Value tab displays with additional data.
4 Select a **Token Value List** and then click the **Add >>** button. Ex: Select **Name** in Token Value List and then click **Add**.

![Figure 345](image)

**Token-Value Details display.**
You can make the changes in the default values displayed.

5 Click **Validate**, and then click **Save**.

![Figure 346](image)
Create a new template

1. In Create Token Value tab, click Create New Template.

2. Enter the required changes in Token Value option and Token.
3. Enter a Template name.

---

Figure 347

Figure 348
4. To filter the values further click the icon.
   EventTracker :: Defined Template window displays.

![Figure 349](image)

5. Enter the relevant data and then click **Add**.
   Ex:
   Enter a token name (i.e. New Token), Output value (i.e. Test New Token).
   You can select Regular Expression or Separator. A regular expression is used to find a particular pattern.
   Select a separator as ‘-’. It can be space, equal ‘=’ symbol etc.
   Select the ordinal values (i.e. Numeric) to further separate the rules.
6. Click **Add to template column**.
Define Parsing Rules(s) window displays.

The created new template displays in **Template** tab.
Generate a Flex Report

1. Log on to EventTracker Enterprise, click the **Reports** menu, and then select **Dashboard** or **Configuration**.
2. Click the **New button** in **Dashboard**.
   (OR)
   Click the **New Report** button in **Configuration**.
3. Select any one of the **Compliance / Security / Operations / Flex reports/Alphabetical** tab.
4. Expand the **Report Tree** node and select any report. Select **Report Type** as **On Demand**. Click **Next**.
   For Example: In **Flex Reports** tab, select **Logs**, and then select **Summary**.
   **Report Type** selected is **On Demand**.
   EventTracker displays the Reports Wizard.
5. Click **Next >>**.
6. Select the required options (like **Sites**, **Group**, **Systems**, **Show all sites**, **All Systems**).
7. Select **Realtime** or **File Transfer** and then click **Next>>**.
8. Select the required **Interval** and **Limit to time Range** option.
9. Select the required **Export Type** (i.e. PDF file, Word Document, HTML file, Quick View (not saved on hard disk)).
10. Select the required **Format** option.

Ex:
   a. If you select **Parsing Rule** option. Click **Next>>**.
Logs Summary displays to select the parsing rule.

Figure 353

Figure 354
b. Click **Select Parsing Rule** hyperlink.

Search Parsing Rule window displays.

![Search Parsing Rule](image)

Figure 355


c. Select the required options and then click OK.

Logs Summary (i.e. Step 5) displays.
d. Select any **Summary** option, select an appropriate option in **Sort by** drop-down.

e. Select **Map Tokens with same 'Tag' to a single column**, if required.

(OR)

a. If you select **Token Template**, click **Next>>**.
b. Select a template. (i.e. enter the template name which you had earlier configured in Parsing Rules – Token Value Wizard)

c. Select/Enter the required options and then click **Next>>**.

---

**Figure 357**

<table>
<thead>
<tr>
<th>Template Name</th>
<th>Template Description</th>
<th>Sample Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template 1</td>
<td>Description</td>
<td>Sample</td>
</tr>
<tr>
<td>Template 2</td>
<td>Description</td>
<td>Sample</td>
</tr>
<tr>
<td>Template 3</td>
<td>Description</td>
<td>Sample</td>
</tr>
</tbody>
</table>

**Note:** The report criteria should result in having some event description signature for which the template is defined.
11 Click the Next>> button.
12 Enter the appropriate Refine and Filter details.
13 Click the Next>> button.
14 Enter the relevant Title, Header, Footer, and Description data.
15 Click the Next>> button.

Review cost details and configure the publishing options window displays.

**NOTE**

Publishing options are disabled because On Demand (foreground processing) has been selected.

16 Click the Next>> button.

The last step of Completing Report Configuration Wizard displays.

17 Select Generate Report.
Chapter 22
Reports Settings

In this chapter, you will learn how to:

- Configure Published Reports
- Configure Cost Saving Report
Configure Published Reports

This option helps to configure published reports settings.

To configure published reports settings.

1. Click the Admin dropdown, and then click Report Settings.

   EventTracker displays the Published Reports tab.

   ![Published Reports Tab](image)

   **Figure 359**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reports backup directory</td>
<td>Folder to keep copies of generated reports. By default, EventTracker saves the reports in <code>\Program Files\Prism Microsystems\EventTracker\Reports</code> folder. You can select a different folder as you wish. On changing the folder, manually copy the reports from old to new folder.</td>
</tr>
<tr>
<td>Generate Default Report in case of no matching record found</td>
<td>If checked, EventTracker will generate a PDF with the message &quot;No Matching Record Found,&quot; if there are no matching records found for the Queued or Scheduled reports. The PDF will be generated irrespective of the report format type.</td>
</tr>
<tr>
<td>Reports purge frequency</td>
<td>Time schedule for the reporter to remove saved ‘On Demand/Queued’ and ‘Scheduled’ reports from the hard disk. EventTracker raises an event (2029) two days prior to deletion. EventTracker displays those events under the All Categories -&gt; EventTracker -&gt; EventTracker: Published reports cleanup Category.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear the checkboxes to retain all the reports forever. By default, Reporter will retain 'On Demand/Queued' and 'Scheduled' reports for 7 and 90 days respectively.</td>
<td></td>
</tr>
<tr>
<td>Prompt to publish on demand Quick View reports</td>
<td>On demand “Quick view” reports are by default not published/saved on hard disk. Selecting this option will prompt you with an option to save/publish the report before closing.</td>
</tr>
</tbody>
</table>
| Replace Domain/User fields from the Event Description if found | By default, EventTracker looks for the following keywords  
Keywords for Domain: Client Domain/ Domain/ User ID/ Account Domain (2nd Instance)  
Keywords for User: Client User Name/ Target Account ID/ User Name/ Account Name (2nd Instance)  
Advanced Reports looks for these keywords in event description. If corresponding key-value is not blank then it will overwrite the original domain/user field with key-value in the display.  
E.g. Event Domain is NT AUTHORITY. In Event Description Client Domain is TOONS. It will display TOONS instead of NT AUTHORITY  
If this checkbox is cleared, then EventTracker displays the original domain/user. |
| DNS Custom Column Resolution Url | URL to resolve IP address.                                                                                                                                 |
| Report Header | Specify a header for the published reports.                                                                                                     |
| Report Footer | Specify a header for the published reports.                                                                                                     |

### Event Id Description

<table>
<thead>
<tr>
<th>Event Id</th>
<th>Description</th>
</tr>
</thead>
</table>
| 2029     | Source: EventTracker  
Description Notification: Report file deletion  
Following file Logs - created on will be deleted on so, please take back up of the file if required.  
Event Information Cause :  
This event is logged when EventTracker On Demand and Schedule reports start purging the published files. |
Configure Cost Saving Reports Settings

1. Click the **Cost Saving Analysis** tab.

   ![Cost Saving Analysis Tab](image)

   Figure 360

2. Click **Edit** to modify the **Time (Seconds) taken for manual analysis** and **Analyst** field.

   - **Labor rates [Cost/Hour]** - Shows the fully loaded labor cost per hour of a system administrator's time. These values are used to compute total cost savings.
   - **Currency Type** – Labor cost will be displayed in the selected currency.

   ![Cost of Manual Analysis Table](image)

   ![Labor Rate Table](image)

   ![NOTE]

   Before generating any cost saving analysis, please make sure that **Collect cost savings information** checkbox is enabled in **Admin menu -> Manager -> Configuration (Cost Saving Report)**.
Chapter 23
RSS Feeds

In this chapter, you will learn how to:

- Configure & manage RSS Feeds
RSS Feeds

RSS/XML feeds can send notification to your computer upon generation of advanced reports or alerts raised by EventTracker. Contents will fly to your desktop faster than an e-mail notification.

EventTracker does not delete a RSS Feed permanently, when you delete it, rather it does make it inactive.

Add RSS Feeds
This option helps you add RSS feeds.

1. Log on to EventTracker Enterprise, click the Admin dropdown, and then click RSS.

EventTracker displays the RSS Feeds page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feed Name</td>
<td>Name of the feed.</td>
</tr>
<tr>
<td>Description</td>
<td>Short description of the feed.</td>
</tr>
<tr>
<td>Added By</td>
<td>Name of the user who configured the feed.</td>
</tr>
<tr>
<td>Added Date</td>
<td>Date and time when the feed was added.</td>
</tr>
<tr>
<td>Show</td>
<td>Select an option to view by status of the feeds.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Click</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add New</td>
<td>Add new feeds.</td>
</tr>
<tr>
<td>Edit</td>
<td>Edit feeds</td>
</tr>
</tbody>
</table>
Delete feeds. Once the feeds are deleted, they are not deleted from the db permanently; rather EventTracker changes the status of the feeds as Inactive. Inactive feeds cannot be reactivated.

2. Click **Add New**.

EventTracker displays the RSS Feeds dialog box.

![RSS Feeds dialog box](image)

Figure 362

3. Provide a **Feed Name**, and relevant description in **Feed Description** for future reference.

4. Click **Save**.

EventTracker displays the **RSS Feeds** page with newly added RSS feed.
Delete RSS Feeds

This option helps you delete RSS feeds.

1. Select the feed that you wish to delete, and then click **Delete**.

   EventTracker displays the confirmation message box.

   ![Confirmation Message]

   Figure 364

2. Click **OK**.

   EventTracker deletes the selected RSS feed from the list.
Chapter 24
Manage System Groups

In this chapter, you will learn how to:

- Auto Discover System Groups
- Add Logical System Group
- Manage Asset Value
About Systems Manager

This is a centralized location to discover and manage the systems that are present in an enterprise domain and to deploy the remote agents.

Systems manager helps you to:

- Automatically discover enterprise domains and systems
- Manually add systems if you opt to
- Manage EventTracker Windows agent and Change Audit agent
- Manage logical system groups

To start System Manager

13. Click the Admin dropdown, and then select Systems.

EventTracker displays Systems manager screen.

Field | Description
--- | ---
Computer | Name of the computer or name of the DLA / NetFlow instance.
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Operating system installed on the computer.</td>
</tr>
<tr>
<td>EventTracker Port</td>
<td>Port through which the EventTracker Windows agent and the EventTracker manager communicates.</td>
</tr>
<tr>
<td>EventTracker Version</td>
<td>Displays EventTracker version and build number.</td>
</tr>
<tr>
<td>Change Audit Version</td>
<td>Displays Change Audit version and build number.</td>
</tr>
<tr>
<td>Asset Value</td>
<td>Asset value indicates how important or critical the computer is.</td>
</tr>
</tbody>
</table>

### Click To

<table>
<thead>
<tr>
<th>Click</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Group</td>
<td>Create logical system groups.</td>
</tr>
<tr>
<td>Delete Group</td>
<td>Delete logical system groups.</td>
</tr>
<tr>
<td>Interface Manager</td>
<td>Modify Netflow interface details.</td>
</tr>
<tr>
<td>Installation Status</td>
<td>Checks install / upgrade / uninstall status of EventTracker Windows agent / Change Audit agent. Also, to check status of computer search.</td>
</tr>
<tr>
<td>Non Reporting Systems</td>
<td>Search a list of systems which have not reported any events to the EventTracker manager in a specific duration of time.</td>
</tr>
<tr>
<td>Search Computers</td>
<td>Manually add enterprise domains and computers.</td>
</tr>
<tr>
<td>System Report</td>
<td>Generate status report of managed and unmanaged computers.</td>
</tr>
<tr>
<td>Auto Discover</td>
<td>Automatically discover enterprise domains and computers.</td>
</tr>
</tbody>
</table>

### Discover Modes

System Manager adds domains and computers in two modes, namely Auto and Manual. In auto-discover modes 'System' manager creates system groups based on enterprise domains.

### Auto Discover Mode

The Auto Discovery mode detects and adds all systems found on all trusted domains. The auto discovery process includes an initial quick detection for systems and a background search for more systems.

1. To automatically discover systems, click the Admin dropdown, and then click Systems.
2. Click Auto Discover at the upper-right corner.

System manager displays confirmation message.
Click the **Ok** button.
System manager automatically starts adding domains and computers.
OR
Click **Cancel** to cancel auto-discovery.

**NOTE**
Only the user who initiated auto-discovery can cancel it. **Auto Discover** mode is easy to use and is recommended for networks having less than 100 systems.

**Manual Mode**
Unlike in ‘Auto discover’ mode, system manager will not discover any domains or computers in this mode. You have to add them manually.

**Add Computers Manually**
In ‘Auto discover’ mode, the ‘System’ manager automatically discovers domains and computers when you keep adding them in your enterprise. All you need to do is to refresh the System manager. However, in ‘Manual’ mode, you have to add them explicitly.

**Add a Single Computer**
This option enables you to add a computer.
1. Click the **Admin** dropdown, and then click **Systems**.
   EventTracker displays **Systems** manager page.
2. Click **Search Computers** button.
   System Manager displays the **Add Computer(s)** pop-up window.
3 Select the **Add a single computer (by name or by IP address)** option, if not selected.

4 Type the name of the computer in the **Enter computer name or IP Address** field.

5 Provide valid **User Credentials**, and then click **Ok**.

   System manager displays the message box.

6 Click **OK**, and then click the ![Refresh](icon) icon to refresh the **Systems** manager.

7 Click the **Installation Status** button to view the status.
Add a Group of Computers
This option enables you to add a group of Computers.

**NOTE**

It is possible to add Computers only with available Domains.

1. To add a group of computers, select the **Add a group of Computers from available Domains** option.

   ![Figure 369](image)

   **Figure 369**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add computers from domain</td>
<td>This drop-down list lists the available domains. Select a domain from where you want to add computers.</td>
</tr>
<tr>
<td>Add computers of type</td>
<td>Select a system type from the drop-down list.</td>
</tr>
</tbody>
</table>

2. Select appropriate options, and then click **OK**.

   A **Message from webpage** window displays.

   ![Figure 370](image)

   **Figure 370**
Click the icon to refresh the Systems manager in order to view installation status.

Adding a Group of Computers from an IP subnet

This option enables you to create a new logical Group of systems based on IP subnet, especially to add legacy Workgroup computers.

1. To add computers from an IP subnet, select the Add computers belonging to an IP range option.

![Figure 371](image)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP range</td>
<td>Type the IP address range to be added.</td>
</tr>
<tr>
<td>DNS discovery alone</td>
<td>The specified IP range will be discovered using DNS method.</td>
</tr>
<tr>
<td>SNMP discovery alone</td>
<td>The specified IP range will be discovered using SNMP method.</td>
</tr>
<tr>
<td>Ping discover alone</td>
<td>The specified IP range will be discovered using Ping method.</td>
</tr>
<tr>
<td>All</td>
<td>The specified IP range will be discovered using DNS/SNMP/Ping method.</td>
</tr>
<tr>
<td>SNMP community string</td>
<td>A password which is necessary to read/write SNMP data.</td>
</tr>
</tbody>
</table>

2. Enter appropriate data in the relevant fields, and then click OK.

3. Click the icon to refresh the Systems manager.

The computers are added to the selected domain.
Logical System Groups

Logical system groups help you group computers that you wish to monitor exclusively. You can select computers by O/S type, from IP subnet or pick them manually.

Create a New Logical Group – System Type

This option enables you to create a new logical Group of systems based on system type.

1. To create a new logical group and systems based on System Type, click Admin drop down, select Systems.

2. Click the Create Group button.

System manager displays the Create Group dialog box window.

![Create Group Dialog Box](image)

**Figure 372**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>Type the group name in this field. The group name should be unique.</td>
</tr>
<tr>
<td>Group Description</td>
<td>Type the group description in this field.</td>
</tr>
</tbody>
</table>
| Group Type       | Select the group type option. The options are System Type, IP Subnet and Select Manually.  

- System Type – Enables you to add the selected system type to the group.  
- IP Subnet – Enables you to add the IP subnet to the group.  
- Select Manually – Enables you to add the systems manually from the available list to the group. |
Enter appropriate data in relevant fields, and then click Next.

If you select the System Type option, System Manager displays the Create Group dialog box with the option to select O/S type.

Select the system type from the Select System Type drop-down list and then click Finish.
System Manager creates and populates the newly created system group with the systems that have O/S type selected.

Create a New Logical Group – IP Subnet

This option enables you to create a new logical Group of systems based on IP subnet

1. To create a new logical group and add systems based on IP subnet, select the IP Subnet option in the Create Group pop-up window.

2. Click Next.

   System Manager displays the Enter Subnet pane.

3. Type the Subnet Address, and then click Finish.
System Manager creates and populates the newly created system group with the systems from the IP subnet selected.

Create a New Logical Group – Manual Selection

This option enables you to create a new logical Group of systems and manually add Computers to that Group.

1. To create a new logical group and add systems manually to that group, select the Select Manually option in the Create Group window.

![Create Group Window](image)

2. Click Next.

System Manager displays the Create Group pop-up window with the option to select managed and unmanaged systems.
3. Select the **Show managed systems only** checkbox to view only managed systems in the list.
4. Select the systems you want to add to the group from the list and select the **Add>>** button.
5. Click **Finish**.

   System Manager creates and populates the newly created system group with the systems selected.

### Modify a Group

Though the System Manager groups the auto discovered computers under their respective groups, you can move systems back and forth between groups as you deem fit.

1. To modify a group, open the System Manager. Right-click the group that you want to edit.

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Type the system-related information in this field.</td>
</tr>
<tr>
<td>Group Members</td>
<td>Select the computer that you want to remove from the group. Click &lt;&lt; Remove.</td>
</tr>
<tr>
<td>Available Systems</td>
<td>Select the computer that you want to add to the group. Click Add &gt;&gt;. The selected computer is added to the list of Group Members.</td>
</tr>
<tr>
<td>Port</td>
<td>Select the port number from the dropdown list.</td>
</tr>
</tbody>
</table>

---

**Figure 378**

![Create group dialog box](image-url)
System Manager displays the shortcut menu.

Figure 379

2. From the shortcut menu, choose **Edit**.

System Manager displays the details of the group with the available systems list.

Figure 380
3 Select the available systems, select **Add>>** or **Remove**, and then click **Save**.

Delete a Group

This option enables you to delete an existing Group.

1 To delete a group, in System Manager. Select the group and then click **Delete Group**.

   (OR)

   Click the **Delete Group** button.

   System Manager displays the confirmation message box.

   ![Figure 381](image)

2 Click **OK**.

   System Manager displays the list of system groups.

   ![Figure 382](image)

3 Select a group and then click **Delete**.
View System Details

This option helps you view system group details and system details like IP address, O/S Type, port, and Agents running on the system.

1. Click Admin drop-down menu, select Systems.
2. To view system group details, in Groups pane, right-click a system group.
   System Manager displays the shortcut menu.
   From the shortcut menu, choose Details.
   System Manager displays the system group Details window.
3. To view managed system details, in Systems pane, move the mouse pointer over a managed system, and then click the dropdown.
   System Manager displays the shortcut menu.
   From the shortcut menu, choose Details.
   System Manager displays the system Details window.

![Details](image)

Figure 383

Restart Agent Service

This option helps to restart EventTracker Windows Agent service in managed systems.

1. Click Admin drop-down menu, select Systems.
2. To restart Agent services in a group, right-click a system group.
   System Manager displays the shortcut menu.
3. From the shortcut menu, choose Restart agent service.
   (OR)
To restart Agent services in a managed system, move the mouse pointer over a managed system, then click the dropdown.

System Manager displays the shortcut menu.

4. From the shortcut menu, choose **Restart agent service**.

![Figure 384](image)

System Manager displays the Restart agent service window.

![Figure 385](image)
5 Enter valid user credentials and then click **Restart agent service**.

System Manager displays the status of the action.

![Message from webpage](image)

**Figure 386**

6 To view the status, click the **Installation Status** button.

System Manager displays the Installation Status window.

![Installation Status](image)

**Figure 387**

7 Click the **View** link in the Description column.

System Manager displays the status of the remote agent.
<table>
<thead>
<tr>
<th>EventTracker Agent Restart Report</th>
<th>Created : 18/03/2018 10:42</th>
</tr>
</thead>
<tbody>
<tr>
<td>System : ESXWIN2K3VM11</td>
<td></td>
</tr>
<tr>
<td>System Name : ESXWIN2K3VM11</td>
<td></td>
</tr>
<tr>
<td>Restart Status</td>
<td></td>
</tr>
<tr>
<td>Success</td>
<td></td>
</tr>
</tbody>
</table>

Figure 388
Query Agent Service Status

This option helps you query EventTracker Windows Agent service status.

1. To query agent service status, click Admin drop-down menu, select Systems.
2. To restart Agent services in a group, right-click a system group. From the shortcut menu, choose Agent service status.
3. To query Agent service status in a managed system, move the mouse pointer over a managed system, and then click the dropdown. From the shortcut menu, choose Agent service status.
   System Manager displays the Agent service status window.
4. Enter valid user credentials and then click Agent service status.
   System Manager displays the status of the action.
5. To view the status, click the Installation Status button.
   System Manager displays the System Status window.
6. Click the View link in the Description column.
   System Manager displays the status of the remote agent.

![Agent service is already running.](Figure 389)

Query Agent Version

This option helps you query EventTracker Windows Agent version.

1. To query agent version, click Admin drop-down menu, select Systems.
2. To query Agent version in a group, right-click a system group. From the shortcut menu, choose Query for agent version.
3. To query Agent version in a managed system, move the mouse pointer over a managed system. From the shortcut menu, choose Query for agent version.
System Manager displays the Query for Agent version window.

4 Type valid user credentials and then click **Query for Agent version**.

   System Manager displays the status of the action.

5 As advised on the pop-up window, click the **Installation Status** button.

   System Manager displays the System Status window.

6 Click the **View** link in the Description column.

   System Manager displays the version of the remote agent.

![Figure 390](image)

**Manage Asset Value**

This option helps you set the asset value of managed systems. Asset Value is the importance or criticality of the computer.

1 Move the mouse pointer over the system that you want to set asset value.

   System Manager displays the shortcut menu.

2 From the shortcut menu, choose **Manage Asset value**.

   System Manager displays the Manage Asset Value pop-up window.

3 Select the value from the **Asset value** drop-down list, and then click **Save**.

**To set asset value for multiple systems in a group**

1 To set asset value for multiple systems in a group, right-click a system group.
System Manager displays the shortcut menu.

2. From the shortcut menu, choose **Manage Asset Value**.

   System Manager displays the Manage Asset Value pop-up window.

   ![Figure 391](image1.png)

3. Select **Edit** to change the current asset value of the particular system.

   ![Figure 392](image2.png)

4. Select the asset value from the dropdown, and then click **Update**.
5 To assign same asset value for multiple systems, select the checkbox for the particular systems, and then click **Assign multiple** button.

EventTracker displays Assign Asset Value pop-up window.

![Assign Asset Value pop-up window](image)

**Figure 393**

6 Select the value from the **Asset value** drop-down list, and then click the **Assign** button.

### Delete Systems

This option helps to remove unmanaged systems.

1 Right-click the system group from where you want to remove the systems.

   System Manager displays the shortcut menu.
2. From the shortcut menu, click **Delete systems**.

System Manager displays the Delete systems window.

3. Select the required option and then click **Next>>**.
4 Select the system, and then click **Delete**.

![Delete systems](image)

**Figure 396**

You can select multiple systems by holding CTRL key on your keyboard.

OR

Click the **Check/Uncheck all** checkbox to select all the systems, and then click **Delete** button.

System Manager displays the confirmation message box.

![Message from webpage](image)

**Figure 397**

5 Click **OK** to confirm
System Manager removes the system.

Search Systems

From the list of all domain computers, this option helps to search system(s) by name.

1. Type the name of the system in the **Search in list** field. Click the **Go** button.
   EventTracker displays the search result.
2. Click **Show All** button to view all systems.

Set Sort by Option

This option helps to set the sort option. Sorting can be done in four ways i.e. **Name, Asset Value, Port** and then **Status**.

1. Select an option from the **Sort by** drop-down list.

   ![Sort by drop-down list](Figure 398)

   • If you select Name, EventTracker displays the system names in alphabetical order.
   • If you select Asset value, EventTracker displays the system names by priority starting from High.
   • If you select Port, EventTracker displays the system names with the port number (in descending order) on the top of the list.
   • If you select Status, EventTracker displays the system names by priority starting from Low.
Chapter 25
Manage Users

In this chapter, you will learn how to:

- Elevate normal user as an EventTracker Administrator
EventTracker Roles, Permissions & Privileges

Roles
Role can be defined in terms of the authorization and obligation policies for a particular job function, which specify what actions the user is permitted or is obliged to do.

Fine-grained role based security model secures the content of the application and the enterprise network at large.

Privileges
Privileges are the rights granted to roles to access EventTracker modules.

Permissions
Permissions are the rights granted to users to access computer groups.

By default, this user is assigned administrator role. You cannot view / modify privileges and permissions of administrators.

An administrator can:
- Access all modules and system groups
- Promote a non-admin user as an administrator
- Demote an administrator
- Grant / revoke permissions and privileges to non-admin users

A non-Admin user
- Cannot access the EventTracker Web Control Panel
- Is restricted to the permissions and privileges granted

Even if the user is a member of EventTracker User Group, EventTracker denies access if the user is not explicitly granted permissions and privileges.
Promote a Non-Admin User as an Administrator

This option helps to promote a non-admin user as an administrator.

To promote a Non-Admin user as Administrator

1. Log on to EventTracker Enterprise.
2. Click Admin dropdown, and then click Users.

EventTracker displays the User Management page.
If you have license for XML API feature, EventTracker displays an additional column 'Interactive User'. By default, all members of EventTracker Group are interactive users. Interactive users can access the EventTracker application and non-interactive users can access EventTracker API.

Clear the Interactive User checkbox against the user you wish to make non-interactive.

EventTracker displays the confirmation message box.

3 Under **Administrator**, select the checkbox against the user you wish to promote as an administrator. EventTracker displays the confirmation message box.

4 Click **OK**.

EventTracker elevates the user as an administrator.
Demote an Administrator

This option helps to demote an administrator.

1. To demote an administrator, clear the checkbox against the admin user that you wish to demote. EventTracker displays the confirmation message box.

2. Click OK.

EventTracker demotes the administrator.

**NOTE**

When an admin user is demoted, EventTracker revokes privileges on all EventTracker modules and permission on all system groups.
Assign Permissions to Non-Admin Users

This option helps to assign permissions to non-admin users on enterprise system groups.

1. Move the mouse pointer over the user name that you want to assign permissions.
   EventTracker displays the drop-down list.

   ![Assign Permission Drop-down List](Figure 405)

2. Select **Assign Permission** from the drop-down list.
   EventTracker displays the Add Permission window.

   ![Add Permission Window](Figure 406)

3. Select the required options and then click **OK**.

View Permissions

This option helps to view permissions assigned to non-admin users on enterprise system groups.
1. To view permissions, move the mouse pointer over the user name that you want to assign permissions. EventTracker displays the drop-down list.

   ![Figure 407](image)

   **Figure 407**

2. Select **View Permissions** from the drop-down list. EventTracker displays the View Permission window.

   ![Figure 408](image)

   **Figure 408**

### Assign Privileges to Non-Admin Users

This option helps to assign access privileges to non-admin users on EventTracker modules.

1. Move the mouse pointer over the user name that you want to assign permissions. EventTracker displays the drop-down list.

   ![Figure 409](image)

   **Figure 409**
2. Select **Assign Privileges** from the drop-down list.

EventTracker displays the Add Privileges window.

![Add Privileges Window](image)

**Figure 410**

3. Click on the check box against the module that you wish to grant access to the user and then click the **OK button**.

**View Privileges**

This option helps to view access privileges assigned to users on EventTracker modules.

1. To view privileges, move the mouse pointer over the user name that you want to assign permissions.

EventTracker displays the drop-down list.
2. Select **View Privileges** from the drop-down list. EventTracker displays the **View Privileges** window.

---

**Export**

1. To export data to excel, click the **Export** icon. You can view the data in an excel file.
Chapter 26
Tag Cloud Weights

In this chapter, you will learn how to:

- Assign Weights to Tags
- Add Keywords as Tags
Weights

A tag cloud is a set of related tags with corresponding weights. The weights are represented using font sizes or other visual clues. Tag clouds are interactive: tags are hyperlinks typically allowing the user to drill down on the data. Tag clouds display order is generally alphabetical.

When the search is over, EventTracker Log Search browser displays the Tag menu in the Menu bar, which in turn has options to refine the query result.

![Figure 413](image)

Assign Weights to Tags

This option helps to assign weights to tags.

1. Log on to EventTracker Enterprise. Click the Admin dropdown, and then click Weights.

   EventTracker displays the Weight configuration page.
2 Select an option from the **View configuration for** drop-down list.

EventTracker displays the Weight configuration page with corresponding details.

3 Click **Edit** against the tag you wish to reassign the Weight.
4 Select an appropriate option from the drop-down list in the **Weight** column and then click **Update**. EventTracker updates the Tag with newly assigned weight.

### Assign Weights to Multiple Tags

This option helps you assign weights to multiple tags.

1. Select the checkbox against the tags you wish to assign weights and then click **Assign Multiple**. EventTracker displays the Assign Weight pop-up window.

2. Select the required option from the **Weightage** drop-down list and then click **Assign**.

EventTracker assigns weights to the selected tags.

### Add Keywords as Tags

This option helps to add keywords as tags.

1. Select **Keyword** from the **View configuration** for drop-down list. Click **Add new**. EventTracker displays the Add Keyword Weight pop-up window.
2 Type keyword in the **Keyword** field.
   Example: Hardware Events

3 Select an option from the **Weight** drop-down list, and then click **OK**.
Chapter 27
Windows Agent Config

In this chapter, you will learn how about:

- Windows Agent Config
- Security
Windows Agent can be configured in UI interface or in the Control Panel.

1. Log on to EventTracker Enterprise. Click the Admin dropdown, and then click Windows Agent Config.

![Figure 420](image-url)

Only Security is explained in this section. For detail information regarding rest of the tabs present in the above figure, refer ET Control Panel -> EventTracker Agent Configuration.

Apply Configuration Settings to Specified Agents

This option enables you to apply the current configuration settings of the selected system to other specified Agents from one centralized location.

1. Log on to EventTracker Enterprise. Click the Admin dropdown, and then click Windows Agent Config.
2. Select the system from the Select system hyperlink.
3. Click Apply this configuration to agents button.

EventTracker displays the ‘Apply client configuration across enterprise’ dialog box.
Available options | Description
---|---
Apply All Settings | Select this option to apply all settings including the default and modified settings.
Apply Only Modified Settings | EventTracker selects this option by default. Leave as it is to apply only the modified settings.
Apply Only Selected Settings | Select this option to apply only the selected settings made under respective configuration options. EventTracker enables the checkboxes. Select appropriate configuration options and then click Apply.

4 Select a system group.

EventTracker displays the managed systems associated with the selected group.
5 Select the systems.
6 Click Apply. EventTracker displays confirmation message.

![Message from webpage]

Figure 422

7 Click OK. EventTracker displays the message ‘Settings applied successfully’.
8 Click OK and then click Save.

Security - Protect Agent Configuration Settings

This option enables you to protect the EventTracker agent configuration settings. You can allow local system or specified remote system(s) to modify the agent configurations. Once the agent configuration is protected, then the agent settings will be modified only by local system and/or specified IP addresses.

To protect Agent configuration settings for local and Agent systems

1 Log on to EventTracker Enterprise. Click the Admin dropdown, and then click Windows Agent Config.
2 Select the system from the Select System hyperlink.
3 Click the Security tab. EventTracker displays Agent Configuration Protection pane.
Field | Description
--- | ---
Enable protection for agent configuration | Select this checkbox to enable other options in this dialog box.

Settings can be modified on the following system(s) | Local System:
Select this checkbox to protect the current configuration settings only for the local system. Other users cannot modify your settings from their machines.

Enter IP Address:
Select this checkbox to protect the current configuration settings for other machines.

IP Address:
Type the IP addresses in this dialog box.
You can configure the current configuration settings up to five IP addresses.
The IP addresses specified in this field can modify the agent configuration settings.

Remedial Action | Select the checkbox to enable the remedial action.

3. Select the **Enable protection for Agent configuration** checkbox.
4. Select/enter appropriate data in relevant fields, and then select the **Save** button.
In this chapter, you will learn about:

- Event-O-Meter
Event-O-Meter

Event-O-Meter is an analytical graphical chart that helps quickly visualize per port trends of events against specified time range. In addition, numerical data has also been provided in a tabular format. It displays the volume of data in terms of number of logs. The data displayed is by hour and day.

To view Event-O-Meter

1. Click the Tools menu, and then click Event-O-Meter.
   
   Event-O-Meter Line Graph displays by default.

   ![Event-O-Meter Line Graph](image)

   **Figure 424**

   The graph shows details about real time data and transfer of files being processed. It also includes number of logs and the size of these log files occurring at a specific port in the specified time duration.

2. Select the required Time duration to view respective Event Count.

3. Select Real Time / File Transfer/ Both options as per the requirement.

4. Click Bar/Pie chart icon to view data respectively.

5. Click View Tabular Data icon at the upper-right corner to view tabular data.
Figure 425
Chapter 29
Log Book

In this chapter, you will learn about:

- Usage of Log Book
About Log Book

Log Book is an electronic book in which users can add entries from Incidents, Reports, Change Audit, Config Assessment and prepare notes directly. A user can also auto date/sign entries.

When doing quarterly review, we can take report to remind ourselves of the 'victories'. When we do log review of alerts and reports, we sometimes come across a low disk condition, an application crash, a SQL injection attempt etc. In order to prevent such hazardous attacks, a log book is provided so that service can be restored or necessary precaution can be taken care of.

Usage of logbook

1. Log on to EventTracker Enterprise.
2. Select the Tools drop-down, and then select Log Book.

   The log book displays only added entries.

3. To add a new logbook, click New Logbook Entry.

   Log Book window displays.
4. Enter **Title** of the alert/report.

5. Select **Tag** from the drop-down.

6. Select priority level from **Severity** drop-down.

7. Enter the valid Email address in **Mailto** field.

8. Enter relevant information in **Reason** field.

9. Enter **System Information**, i.e. **Computer Name, Owner, IP address, Criticality, Location, Component Installed, Operating System** etc.

10. In **Investigation** pane, **Impact Determined, Investigation Procedure** undertaken to resolve the issue, **Investigation Action Taken, Application Name** that caused the problem, **Host Information** and **Recommendation**.

11. To add references, click the **References** tab and then click **Attach file**.

12. Enter the required and mandatory information and then click the **Save** button.

13. To search logbook information, click the **Advance Search** hyperlink.
14. Enter the relevant search information, and then click the **Search** button.

**NOTE**

- A user has to add investigation information since it is mandatory.
- System Information provides information about a particular system.
- For a Log Book entry, there can be N number of activities.
- A user who adds the log book, only can edit log book and others can only add activity.
- A user who has created the activity can only edit his/her activity.
- Others can add comments which will be shown in history.
- The logbook shows only added logbook entries details and how to search the available logbook entries.
- After adding the log book, the user can edit logbook completely but whereas other users can add only investigation details. Other users don't have permission to delete an uploaded file and references.
Example

1. Select the **Incidents** menu, and then select the **Tabular** tab.

![Figure 429](image)

2. Select any incident and click the **logbook** icon. Logbook window displays.

![Figure 430](image)
3. Enter the relevant information i.e. **Reason**, **Investigation** information, **Mail To** details etc. If required, update the **Severity** of the incident.

4. Click the **Save** button.

5. To view details of this Incident, click the **History** tab.

6. To add data to the existing logbook, click the **Edit Logbook** button.

7. To add more investigation details, click the **Add investigation details** button.

8. To view details, select the **Tools** menu and then select **Logbook**.
Chapter 30
Log View

In this chapter, you will learn how to:

- View Logs
View Logs

This option enables you to view category wise events occurred at managed systems.

1. Log on to EventTracker Enterprise. Click the **Tools** dropdown, and then click **Log View**.

   ![Log View](image)

2. Check the **All Systems** option to view logs of all managed systems
   (OR)
   Click the **Select system(s)** hyperlink to make customize selection.
   EventTracker displays **Systems** pop-up window.

3. Enter the system name in **Search system(s)** field or select a group/system(s), and then click **Ok**.

4. Check the **All Categories** option to view all category events (or) check the **All Alerts** option to view all alert events.
   (OR)
   Click the **Select a category** hyperlink.
   EventTracker displays **Categories** pop-up window.
   Enter category name in the **Search category** field (or) click category name in the category tree, and then click **Close**.

5. Select the period from **Time Duration** drop-down list. Click the **Go** button.
   EventTracker displays the search result.
Figure 433

6 Click **Show more result** button, to see more results on the given search criteria.

7 Click **New Search** button to clear the search criteria and start a fresh search.

**NOTE**

From **Log View**, an event can be added as an alert.

In the **Event ID** column, click the event Id dropdown, and then click **Add as Alert**. EventTracker displays ‘Alert Configuration’ window. Make the required changes, and then click the **Finish** button.
Chapter 31
Sitemap

In this chapter, you will learn how to:

- View Sitemap
Sitemap

Sitemap provides a view of index of the web site.

To view Sitemap

1. Log on to EventTracker Enterprise, click **Tools** and then click the **Sitemap**.

EventTracker displays the sitemap.

![Sitemap](image_url)
Chapter 32
Windows

In this chapter, you will learn how to:

- View Windows System Status
- Tabs Configuration
View Managed Windows System Status

In the EventTracker, you can get a peek view of the Windows system status.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Click to</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TABS</strong></td>
<td></td>
</tr>
<tr>
<td>System Details</td>
<td>View system details like O/S type, Asset value and top 10 Alert events occurred in the last one-hour. At the maximum you can opt to view alert events occurred in the last 24 hours. Click the refresh button to refresh the pane with recent alert details.</td>
</tr>
<tr>
<td>Event Category</td>
<td>This report provides per Category count of *All error events, *All information events, *All warning events, *All audit success events, *All audit failure events occurred in the last one-hour. At the maximum you can opt to view events occurred in the last 24 hours. Click the refresh button to refresh the pane with recent events.</td>
</tr>
<tr>
<td>Event Source</td>
<td>This report provides per source event count. Helps to identify top 10 event sources for the last one-hour. At the maximum you can opt to view sources for the last 24 hours. Click the refresh button to refresh the pane with recent source of events.</td>
</tr>
<tr>
<td>File/Resource Access Failures</td>
<td>Failed attempts to access shared resources such as files and folders are captured by these reports. Windows file/folder auditing must be enabled appropriately for these reports to generate meaningful data. Usage: These reports are usually run and reviewed regularly to detect access to mission critical resources.</td>
</tr>
<tr>
<td>Login Failures</td>
<td>The security logon features include logging all unsuccessful login attempts. The user name, date and time are included in this report.</td>
</tr>
<tr>
<td>Log Volume</td>
<td>Provides information on count of events received from the selected system. Usage: This report can be used to analyze maximum occurring events.</td>
</tr>
<tr>
<td>Patches / Hot Fixes</td>
<td>View details on patches / hot fixes applied on the server.</td>
</tr>
<tr>
<td>Printer Activity</td>
<td>View information on printer utilization providing details on jobs, users and pages sorted by print servers or users. Usage: This report can be used for chargeback of printer usage or from a security perspective to note unusual printer activity.</td>
</tr>
<tr>
<td>Software Installed</td>
<td>The EventTracker Agent for Windows can be configured to detect the installation of software applications. If this feature is enabled, this report provides information on software application install on the EventTracker Server for the chosen time period. Usage: This report is useful to track updates or changes to critical systems.</td>
</tr>
<tr>
<td>Software Usage</td>
<td>The EventTracker Agent for Windows, can be configured to detect the start and stop of software applications. If this feature is enabled, this report provides information on software application utilization across selected computers for the chosen time period. Usage: This report is typically used to manage licensing or to determine usage of specific applications. It is more useful on Workstations than on Servers</td>
</tr>
<tr>
<td>Storage</td>
<td>Disk utilization is a critical resource for servers and must be monitored. This report helps identify disk space availability and the presence of bad blocks. Usage: This report is used to decide on preventive remedial measures so as to minimize downtime or declining service levels.</td>
</tr>
<tr>
<td>Suspicious</td>
<td>The classic virus infection causes unrecognized EXEs to begin accessing the network.</td>
</tr>
<tr>
<td>Tab</td>
<td>Click to</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Network Activity</td>
<td>When enabled, the EventTracker Agent for Windows can be configured with a white-list of known ports or application and report exceptions. This helps identify potentially suspicious traffic. The report uses a database of known infections per port to identify potential threats. Usage: After suitably configuring the EventTracker Agent for Windows, this report is used to report on unusual traffic from unrecognized EXEs.</td>
</tr>
<tr>
<td>USB File Activity</td>
<td>This report provides per user details on USB activities that include file addition, deletion, changes, and respective total no. of times those activities were done.</td>
</tr>
<tr>
<td>Last hours</td>
<td>Select the time interval you wish to generate report.</td>
</tr>
<tr>
<td></td>
<td>Refresh the Dashboard.</td>
</tr>
</tbody>
</table>

**To view Windows System Status**

This option helps to quick view status of the managed Windows systems.

1. Log on to **EventTracker Enterprise**.
2. Click the **Tools** dropdown, and then click **Windows**.
   
   EventTracker displays the 'Windows Systems Dashboard'.

![Windows Systems Dashboard](image)

*Figure 435*

**NOTE**

EventTracker displays only the managed system groups systems and DLA system instances on the left pane.
3 Right-click a system on the left pane and then click Show Details. 
EventTracker displays the System Details tab and the relevant details.

4 Click a tab to view summary report. 
You can also select multiple tabs for parallel processing.

5 If displayed, click the Detail button to view detailed report. 
EventTracker displays the File Download pop-up window.

6 Click Save to save the *.pdf file in a safer location for future reference.

Load Tabs Together
This option helps you select tabs that you wish to load together, that is to process concurrently instead of selecting individual tabs.

1 Click the Tab configuration hyperlink. 
EventTracker displays Tab configuration window.

![Figure 436](image)
2. Select the **Tab name** option(s) that you wish to load together, and then click **Save**.

3. In All Windows Systems pane, right-click system name, and then click **Show Details**.
   
   EventTracker turns focus on the **System Details** tab and displays the relevant details. Also starts processing concurrently in the background the other tabs you have configured.
   
   You can also select tabs other than tabs you have configured to load together.
   
   EventTracker starts processing only when a tab is selected. When you click a new tab and come back to the previous tab, EventTracker starts processing afresh.

### NOTE

You have to select at least two tabs on the **Tab configuration** window. EventTracker displays the message box with appropriate message if you select just one tab.
Chapter 33
Knowledge Base

In this chapter, you will learn how to:

- Access Knowledge Base
Knowledge Base

A Web site containing information about Windows events and custom EventTracker events. Users can search for log-related information under one roof. KB contains carefully written articles that are kept up-to-date, an excellent information retrieval system (such as a search engine), and a carefully designed content format and classification structure.

To access Knowledge Base

1. Log on to EventTracker Enterprise, click Tools and then click Knowledge Base.

   EventTracker redirects to EventTracker Knowledge Base Web site http://kb.prismmicrosys.com/

---

Log Talk - A Blog Discussing Event Logs and How to Get Value From Them

Happy St. Patrick’s Day
March 15, 2013
...more

The EventTracker Knowledgebase is a free service provided by EventTracker, an industry leading SIEM and Log Management solution. EventTracker delivers business-critical solutions to consolidate, correlate and detect changes that impact the performance, availability and security of your IT infrastructure. With a proven history of innovation and leadership, EventTracker’s unique combination of enterprise-class log management and integrated change and configuration auditing are recognized as critical strategies for improving overall security, meeting and demonstrating compliance with regulatory mandates, and increasing operational efficiency.
Chapter 34
EventVault Warehouse Manager

In this chapter, you will learn how to:

- Use EventVault Warehouse Manager
- Save EventBox Metadata
- Backup Archives
- Extract EventBox data
- Move CAB files
1. To access **EventVault Warehouse Manager**, click the **Start** button, select **All Programs**, and then select **Prism Microsystems**.

2. Select **EventTracker**, select **EventTracker Control Panel** and then select **EventVault**. EventTracker opens EventTracker Control Panel window.

---

**Figure 438**

**Available EventBoxes**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Period</td>
<td>Time range of events stored in the CAB file.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the CAB file. etar1269949644-14505.cab etar – EventTracker Archive 1269949644 – Time ticks 14505 – Port number (through which the EventTracker Receiver service received the events) cab – File extension of cabinet files</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checksum</td>
<td>SHA 1 checksum number for tamper proof.</td>
</tr>
<tr>
<td>Path</td>
<td>Path of the folder where the archives are stored typically, EventTracker install path \ port number \ year \ month</td>
</tr>
<tr>
<td>Size (KB)</td>
<td>Size of the CAB file in KB.</td>
</tr>
<tr>
<td>Total Events</td>
<td>Total number of events accommodated in the CAB file.</td>
</tr>
<tr>
<td>Port Number</td>
<td>Port number through which the EventTracker Receiver service received the events.</td>
</tr>
</tbody>
</table>

3. Select **Collection Point(s):** drop-down, select the Collection Point cab file available.
   The details of CAB file displays.

## Configuration

1. Click the **Configuration** button.
   
   Configuration window displays.

![Configuration Window](image)

Vault Storage Folder displays the location of the folder where archives are stored.

2. To create CAB files, specify the time duration in **Force CAB file creation every:** drop-down. Archives will be created for the number of hours specified or when cache size exceeds 50 Mb.

3. To purge archive folders, select **Purge Archives older than** option and specify number of **days**. The user can purge the collection point cab file from the collection master.
Save EventBox Metadata
This option enables you to save the archive summary in a text file. It helps you to locate particular .cab files to view, retrieve or extract events.

1. To save EventBox Information, double-click EventVault on the EventTracker Control Panel.
2. Select the archive file(s) from the Available EventBoxes list.
   (OR)
   Select the Select All checkbox to select all the archive files.
3. Click Save EventBox Metadata on the toolbar.
   EventVault Manager displays the Save As window.
4. EventVault Manager saves the EventBox Info in archive-info.txt file.
   You can also type the file name in the File name field.
5. Select the path where you want to store the archive summary and then click Save.

Back up EventVault Data
This option enables you to backup EventVault data locally or remotely in a desired location for a long-term storage. It helps you to retrieve the backup data if the production archives are tampered.

1. Open the EventVault Warehouse Manager.
2. Select the CAB file(s) from the Available EventBoxes list.
   (OR)
   Select the Select All checkbox to select all the archive files.
3. Click Backup Archives on the toolbar.
   EventVault Warehouse Manager displays the confirmation message box.

   Figure 440

4. Click Yes.
   EventVault Warehouse Manager displays the Choose Directory window.
5. Select the folder where you want to store the event data and then click OK.
   EventVault Warehouse Manager displays the ArchIntegrity report in the Notepad after successful completion of backup.
If there is no archive file to back up, EventVault Warehouse Manager displays the message box with appropriate message.

Extract EventBox Data
This option enables you to extract EventBox data into an MS Access database.

1. Open EventVault Warehouse Manager.
2. Select the CAB file(s) from the Available EventBoxes list.
3. Click Extract.

EventVault Manager displays the Choose Directory window.

4. Select the path where you want to store the event data.
5. Click Save.

After extracting the event data, EventTracker displays the ArchIntegrity report in the Notepad.

**NOTE**
EventVault Warehouse Manager saves the extracted .cab file in the selected location with .mdb file extension. You can view the database file using MS Access.
Move CAB files
This option helps you move all or selected CAB files to a new location. After physically moving the CAB files, EventTracker updates the archive index. Moving the CAB files to a new location does not harm your scheduled reports. You can run on demand reports, define reports, and even configure new scheduled reports as you normally do.

1. To move CAB files, open the EventVault Warehouse Manager.
2. Select the CAB files from the Available EventBoxes list.
   (OR)
   Select the Select All checkbox to select all the EventBoxes.
3. Click Move.
   EventVault Warehouse Manager displays the confirmation message box.

   ![Confirm Archive Move](Figure 442)

4. Click Yes to proceed.
   EventVault Warehouse Manager displays the Choose Directory dialog box.
5. Select the location (local or network) and then click OK.
   EventVault Warehouse Manager moves all the selected files to the new location and displays the ArchIntegrity report in the Notepad.

Delete an EventBox
This option enables you to delete an EventBox.

1. Open the EventVault Warehouse Manager.
2. Select the CAB file(s) from the Available EventBoxes list.
3. Click Delete.
4. EventVault Warehouse Manager displays the Confirmation message box.
5 Click **OK**.

EventVault Warehouse Manager deletes the selected EventBox and displays the ArchIntegrity report in the Notepad.

**View CAB Files by Port Number**

This option helps you view CAB files by port number.

1 Open the EventVault Warehouse Manager.
2 Select **Show older than** or **Show From** option.
3 Set the time range.
4 Select a port number from the **Port Number** drop-down list.
5 Click **Show**.

EventVault Warehouse Manager displays the CAB files of the selected port for the selected time range.
Port Number drop-down list lists all ports configured, default and VCP. Had you appended legacy CAB files (v 6.0 and earlier), select the 0-Legacy option. Port numbers were not appended to the names of Legacy CAB files.
Chapter 35
Diagnostics

In this chapter, you will learn how to:

- EventTracker Diagnostic Tool
- Set Debug levels
- Obfuscate Classified Information
- Diagnostic Alert
- SQL Log
- Backup Configuration
EventTracker Diagnostic Tool

Windows (optionally) adds the Diagnostics Tool as a Startup program after successful installation of EventTracker. Diagnostics Tool alerts you if any problem occurs in the EventTracker.

Diagnostics data includes Product Information, System Information, License Information, Update Information, Service Status, Database, and Archive Status, configuration files and log dumps. It is further extended to set debug levels and mask sensitive information.

To start EventTracker Diagnostic Tool

1. Click the Start button, select All Programs, and then select Prism Microsystems.
2. Select EventTracker, select EventTracker Control Panel, and then select Diagnostics icon.

EventTracker displays EventTracker Diagnostics window.
3. Right-click the **Diagnostics Tool** icon on the taskbar.
   EventTracker displays the shortcut menu.

4. To set the frequency, move the mouse pointer over the **Run Frequency** option. EventTracker displays the options to set the frequency.
   If there is any error, then Diagnostics Tool displays the diagnostics message balloon to grab your attention.

**Set Debug Levels**
This option helps to set log severity levels for EventTracker modules.

1. Open **EventTracker Control Panel**, click **Diagnostics**, and then click **Debug Settings** button.
   Diagnostics Tool displays the Debug Levels window.
EventTracker writes the log messages in the respective log files with the severity levels set.

### EventTracker Module Log File Folder Path

<table>
<thead>
<tr>
<th>EventTracker Module</th>
<th>Log File</th>
<th>Folder Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>EventTracker Web</td>
<td><em>.</em></td>
<td>...\Program Files\Prism Microsystems\EventTrackerWeb\Logs</td>
</tr>
<tr>
<td>EventTracker Web</td>
<td>EventTracker.log</td>
<td>...\Program Files\Prism Microsystems\EventTracker\AdvancedReports\Logs</td>
</tr>
<tr>
<td>Receiver</td>
<td>evtxer*.txt, evtxlog-514.txt, evtxlog-14505.txt, evtxlog-14509.txt</td>
<td>...\Program Files\Prism Microsystems\EventTracker</td>
</tr>
<tr>
<td>EventVault</td>
<td>evtarlog.txt</td>
<td>...\Program Files\Prism Microsystems\EventTracker</td>
</tr>
</tbody>
</table>
**EventTracker Ver.7.4 Enterprise User Guide**

<table>
<thead>
<tr>
<th>EventTracker Module</th>
<th>Log File</th>
<th>Folder Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduler</td>
<td>etslog.txt</td>
<td>\Program Files\Prism Microsystems\EventTracker</td>
</tr>
<tr>
<td>Indexing Services</td>
<td>Prism.Keyword.Indexer.*.log</td>
<td>\Program Files\Prism Microsystems\EventTracker\AdvancedReports\Logs</td>
</tr>
<tr>
<td>Direct Log Archiver</td>
<td>LogFileParser.txt</td>
<td>\Program Files\Prism Microsystems\EventTracker</td>
</tr>
<tr>
<td>Alerter</td>
<td>ETRSSLog.txt</td>
<td>\Program Files\Prism Microsystems\EventTracker</td>
</tr>
<tr>
<td>Reporter</td>
<td>Prism.EventTracker.Report*.log</td>
<td>\Program Files\Prism Microsystems\EventTracker\AdvancedReports\Logs</td>
</tr>
<tr>
<td>Enterprise Activity</td>
<td>etuserlog.txt</td>
<td>\Program Files\Prism Microsystems\EventTracker</td>
</tr>
<tr>
<td>Collection Point/Master</td>
<td>evtCPlog.txt</td>
<td>\Program Files\Prism Microsystems\EventTracker</td>
</tr>
<tr>
<td>Change Audit</td>
<td><em>..</em></td>
<td>\Program Files\Prism Microsystems\WCWindows\Logs</td>
</tr>
<tr>
<td>Correlator</td>
<td>etcorlog.txt</td>
<td>\Program Files\Prism Microsystems\EventTracker\ETCorrel</td>
</tr>
<tr>
<td>TrapTracker</td>
<td>evtrxlog.txt</td>
<td>\Program Files\Prism Microsystems\TrapTracker</td>
</tr>
<tr>
<td>StatusTracker</td>
<td>monlog.txt</td>
<td>\Program Files\Prism Microsystems\StatusTracker</td>
</tr>
</tbody>
</table>

3. Select appropriately in the relevant fields.

4. Click **Save**.

**Obfuscate Classified Information**

This option helps to mask classified information in log files when you send the log files outside your enterprise for debugging.

1. To obfuscate classified information, Open **EventTracker Control Panel**. Click **Diagnostics**, and then click the **Obfuscate Output** checkbox.

   Diagnostics Tool displays Masking Configuration window.
Move the mouse pointer over the Help hyperlink to view help tips. Select the appropriate checkbox.

3. Click Save and then click the OK button.
   
   Diagnostics Tool enables the Edit Configuration button.

4. Click E-mail to send log files and configuration files for debugging.
   
   Diagnostics Tool displays the message box indicating to Limit CAB file details and/or Include XML files.

5. Click Next>.
Diagnostics Tool displays the EventTracker Diagnostics window with more mailing options.

6. Enter/select appropriate data in the relevant fields.
7. Click **Send**.
   EventTracker Diagnostic window displays message.
You can also save the log files and configuration files as a compressed file for future reference.

8 Click Save on the EventTracker Diagnostics window.

9 Type the problem description in the provided field.

10 Click Save.

Diagnostic Alert

When you access EventTracker from a remote location using a browser client, Diagnostics tool displays a warning message alert indicator and prompts you to respond if any problem occurs with EventTracker.

Diagnostics tool displays and hides the indicator based on the diagnostic frequency you set. By default, diagnostic frequency is set to 24 hours.

An admin user can view incident and problem descriptions. A normal user is only indicated that a problem has occurred.

1 Log on to EventTracker with admin user credentials.

   Diagnostics tool displays the diagnostic alert indicator.

2 Click the indicator icon.

   EventTracker displays the File Download pop-up window to open or save the diagnostic report.

3 Click Open to view the report.

   EventTracker opens the report in the Notepad.
SQL Log

1. Open **EventTracker Control Panel**, click **Diagnostics**, and then click the **SQL Log** button. **SQL Log Status** window displays.

2. Select the required options to **Purge** data and then click **Save**.

Backup Configuration

1. Open **EventTracker Control Panel**, click **Diagnostics**, and then click the **Backup Configuration** button. **Backup & Restore** window displays.
2. Select the required options and then select the Save/Restore button accordingly.
Chapter 36
License Manager

In this chapter, you will learn about:

- View, update, upgrade License Manager
License Manager

This option helps to upgrade license, view license usage, and update Certificate Revocation List (CRL).

1. Double-click License Manager on the EventTracker Control Panel.

![License Manager Interface](image)

2. Click View Certificate.

   EventTracker displays the Windows Certificate Viewer.
3  Click **Install Certificate** button to import certificate to a certificate store.  
   A certificate store is the system area where the certificates are kept.

4  Click **View Options/Features** on the License Manager window.
5 Click **View License Usage**.

![Available Features - Custom](image)

**Figure 457**

![EventTracker - License Usage](image)

**Figure 458**

- **Total Available**: 40241 (20201 + 10020 + 10020)
- **Total used**: 5 (3 + 1 + 0)
- **Available Indexed Log Volume is Unlimited**
6 Click **Upgrade License**.

![License Upgrade](image)

Figure 459

7 Click **Request License Upgrade** to request a new license to upgrade.
8. Enter appropriate data in the relevant fields.
9. Click **Save Request** to save the request in Notepad and send it later.
10. Click **Send Request** to send E-mail.

   (OR)

   If you already have a license to upgrade, click the browse button.
   EventTracker displays the Open dialog box.
   Go to appropriate folder and select the certificate file.
   Click **Open** and then click **Upgrade**.
11. Click **Update CRL** on the **License Manager** window.

    A Certificate Revocation List (CRL) is a list of certificate serial numbers which have been revoked, are no longer valid, and should not be relied upon.

    A CRL, like a certificate, also has a validity date span. The date span ensures that the CRL is not used after a certain time, but also allows the application checking the CRL to cache the CRL so that it doesn't have to keep downloading it over and over again.
While installing EventTracker, CRL (PrismCA.crl) is downloaded to the default install path typically...
\Program Files\Prism Microsystems
EventTracker displays the Open dialog box.

12 Select the CRL file and then click **Open**.
13 Select the **Internet Connection** button. Enter relevant data and then click **Save**.

![Internet Connection Details](image)

**Figure 461**

14 To close License Manager, select the **Close** button.
Chapter 37
Export Import Utility

In this chapter, you will learn how to:

- **Export and Import**
  - Categories
  - Filters
  - Alerts
  - Systems and Groups
  - RSS Feeds
  - Scheduled Reports
  - Behavior Rules
  - Token Value

- **Import SCAP**
Export and Import Utility

Export and Import Utility enables you to export/import custom Categories, Filters, Alerts, Scheduled Reports, Domains, Systems, RSS Feeds, Token Value and Behavior Rules during migrate/upgrade process, and to transfer EventTracker data from one system to the other in your enterprise. Suppose, you have configured Scheduled Reports in System A and want to configure Scheduled Reports in System B with same configuration settings. You need not configure again in System B, just export the Scheduled Reports configured in System A and then import those .issch files into System B.

Export Categories

1. To export categories, select the Start button, select All Programs, and then select Prism Microsystems.
2. Select EventTracker, select EventTracker Control Panel, and then select Export Import Utility.

EventTracker displays the Export Import Utility window.

![Export Import Utility Window](image-url)

Figure 462
### EventTracker Ver.7.4 Enterprise User Guide

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Select a Category group(s) to add all Categories that belong to that group to the Selected list or expand the Category group(s) to add individual Category. Selected Category group(s) / Category(s) are added to the Selected list.</td>
</tr>
<tr>
<td>Selected</td>
<td>To remove Category group(s) / Category(s), clear the respective checkbox(s) in the Category list.</td>
</tr>
</tbody>
</table>

3. In **Export** tab, select the required **Category**, select the >> button and then select the **Export button**. EventTracker displays the **Save As** pop-up window.

4. Type the file name in the **File Name** field.

![NOTE](#)  

The valid file extension is .iscat.

5. Click **Save**. EventTracker displays the **Export Import Utility** message box.

![Figure 463](#)

6. Click **OK**.

### Export Filters

1. To export filters, select the **Start** button, select **All Programs**, and then select **Prism Microsystems**.

2. Select **EventTracker**, select **EventTracker Control Panel**, and then select **Export Import Utility**.

3. In **Export** tab, select the **Filters** option.
Select the required **Filters** and then click **Export**.

Type the file name in the **File Name** field.

**NOTE**

The valid file extension is `.isfil`.

Click **Save**.

EventTracker displays the Export Import Utility message box.

**Figure 464**

Click **OK**.

**Export Alerts**

1. To export alerts, select the **Start** button, select **All Programs**, and then select **Prism Microsystems**.
2. Select **EventTracker**, select **EventTracker Control Panel** and then select **Export Import Utility**.
3. In **Export** tab, select the **Alerts** option.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export E-mail Settings</td>
<td>Select this checkbox to export Alerts along with the corresponding e-mail settings, if any.</td>
</tr>
<tr>
<td>Alerts</td>
<td>Select an Alert / Alerts from this list.</td>
</tr>
<tr>
<td></td>
<td>Click Add-&gt; to add to the Selected list.</td>
</tr>
<tr>
<td></td>
<td>Click Add All&gt;&gt; to add all Alerts to the Selected list.</td>
</tr>
<tr>
<td></td>
<td>To select multiple Alerts, hold down the CTRL key on your keyboard and click the Alerts.</td>
</tr>
<tr>
<td>Selected</td>
<td>Select an Alert / Alerts from this list.</td>
</tr>
<tr>
<td></td>
<td>Click &lt;-Remove to remove the selected Alert / Alerts from this list.</td>
</tr>
<tr>
<td></td>
<td>Click &lt;&lt;Remove All to remove all Alerts from this list.</td>
</tr>
</tbody>
</table>

4. Select the required alerts and then click **Export**.

5. Type the file name in the **File Name** field.

### NOTE

The valid file extension is **.isalt**.

6. Click **Save**.

   EventTracker displays the Export Import Utility message box.

   ![Export Import Utility Message Box](image)

   **Figure 465**

7. Click **OK**.

**Export System Groups**

1. To export system groups, select the **Start** button, select **All Programs**, and then select **Prism Microsystems**.

2. Select **EventTracker**, select **EventTracker Control Panel** and then select **Export Import Utility**.

3. Select the **Systems and Groups** option.
   
   EventTracker displays the systems groups.
### EventTracker Ver.7.4 Enterprise User Guide

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems and Groups</td>
<td>Select a system group(s) to add all systems that belong to that group to the Selected list or expand the system group(s) to add individual system. Selected system group(s) / system(s) are added to the Selected list.</td>
</tr>
<tr>
<td>Selected</td>
<td>To remove system group(s) / system(s), clear the respective checkbox(s) in the Systems and Groups list.</td>
</tr>
</tbody>
</table>

4. Select the required system/groups and then click **Export**.
5. Type the file name in the **File Name** field.

**NOTE**

The valid file extension is **.issys**.

5. Click **Save**.

EventTracker displays the Export Import Utility message box.

![Export Import Utility](image)

6. Click **OK**.

### Export RSS Feeds

1. To export RSS feeds, select the **Start** button, select **All Programs**, and then select **Prism Microsystems**.
2. Select **EventTracker**, select **EventTracker Control Panel** and then select **Export Import Utility**.
3. Select **RSS Feeds** option, select the required **RSS** and then click **Add->/Add All>>**.
4. Click **Export**.
5. Type the file name in the **File name** field.
NOTE

The valid file extension is .issrss.

6 Click **Save**.

   EventTracker displays the Export Import Utility message box.

   ![Export Import Utility](image)

   Figure 467

7 Click **OK**.

Export Scheduled Reports

1 To export scheduled reports, select the **Start** button, select **All Programs**, and then select **Prism Microsystems**.

2 Select **EventTracker**, select **EventTracker Control Panel** and then select **Export Import Utility**.

3 Select the **Scheduled Reports** option.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduled Reports</td>
<td>Select a Scheduled report / reports from this list.</td>
</tr>
<tr>
<td></td>
<td>Click Add-&gt; to add to the Selected list.</td>
</tr>
<tr>
<td></td>
<td>Click Add All&gt;&gt; to add all Scheduled reports to the Selected list.</td>
</tr>
<tr>
<td></td>
<td>To select multiple Scheduled reports, hold down the CTRL key on your keyboard</td>
</tr>
<tr>
<td></td>
<td>and click the Scheduled reports.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selected</td>
<td>Select a Scheduled report / reports from this list.</td>
</tr>
<tr>
<td></td>
<td>Click &lt;-Remove to remove the selected Scheduled report / reports from this list.</td>
</tr>
<tr>
<td></td>
<td>Click &lt;&lt;Remove All to remove all Scheduled reports from this list.</td>
</tr>
</tbody>
</table>

4 Select the required **Scheduled Reports**, and then click **Export**.

5 Type the file name in the **File name** field.
NOTE

The valid file extension is .issch.

6 Click Save.

EventTracker displays the Export Import Utility message box.

7 Click OK.

Export Behavior Rules

1 To export behavior rules, select the Start button, select All Programs, and then select Prism Microsystems.

2 Select EventTracker, select EventTracker Control Panel and then select Export Import Utility.

3 Select the Behavior Rules option.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Behavior Rules</td>
<td>Select a Behavior Rule / Behavior Rules from this list. Click Add-&gt; to add to the Selected list. Click Add All&gt;&gt; to add all Behavior Rules to the Selected list. To select multiple Behavior Rules, hold down the CTRL key on your keyboard and click the Behavior Rules.</td>
</tr>
<tr>
<td>Selected</td>
<td>Select a Behavior Rule / Behavior Rules from this list. Click &lt;-Remove to remove the selected Behavior Rule / Behavior Rules from this list. Click &lt;&lt;Remove All to remove all Behavior Rules from this list.</td>
</tr>
</tbody>
</table>

4 Click Export.

5 Type the file name in the File name field.
6. Click **Save**.
   
   EventTracker displays the Export Import Utility message box.

   ![Figure 469](image)

7. Click **OK**.

**Export Token Value**

1. To export behavior rules, select the **Start** button, select **All Programs**, and then select **Prism Microsystems**.
2. Select **EventTracker**, select **EventTracker Control Panel** and then select **Export Import Utility**.
3. Select the **Token Value** option.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Token Value</strong></td>
<td>Select a Token Value from this list. Click Add-&gt; to add to the Selected list. Click Add All&gt;&gt; to add all Behavior Rules to the Selected list. To select multiple Token Values, hold down the CTRL key on your keyboard and click the Token Value.</td>
</tr>
<tr>
<td><strong>Selected</strong></td>
<td>Select a Token Value from this list. Click &lt;-Remove to remove the selected Token Value from this list. Click &lt;&lt;Remove All to remove all Token Value from this list.</td>
</tr>
</tbody>
</table>

4. Click **Export**.
5. Type the file name in the **File name** field.
NOTE

The valid file extension is .istoken.

6 Click Save.

EventTracker displays the Export Import Utility message box.

![Export Import Utility](image)

Figure 470

7 Click OK.

Import Categories

1 Select the Start button, select All Programs, and then select Prism Microsystems.
2 Select EventTracker, select EventTracker Control Panel, and then select Export Import Utility.
3 Click the Import tab.

EventTracker selects the Category option by default.

4 Click the browse button.

EventTracker displays the Open pop-up window.
5 Navigate and locate the category file you want to import.
6 Click Open.

EventTracker updates the Source field with the path of the Category file.

(OR)
Type the path of the Category file in the Source field.
7 Click Import.

EventTracker displays the Export Import Utility message box.
Click OK.

**Import Filters**

1. Select the Start button, select All Programs, and then select Prism Microsystems.
2. Select EventTracker, select EventTracker Control Panel, and then select Export Import Utility.
3. Click the Import tab.
4. Select the Filters option. Click the browse button .
   EventTracker displays the Open pop-up window.
5. Navigate and locate the filters file you want to import. Click Open.
   EventTracker updates the Source field with the path of the filters file.
   (OR)
   Type the path of the filters file in the Source field.
6. Click Import.
   EventTracker displays the Export Import Utility message box.
7. Click OK.

**Import Alerts**

1. Select the Start button, select All Programs, and then select Prism Microsystems.
2. Select EventTracker, select EventTracker Control Panel, and then select Export Import Utility.
3. Click the Import tab. Select the Alerts option.
4. Click the browse button .
   EventTracker displays the Open pop-up windows.
5. Navigate and locate the Alerts file you want to import. Click Open.
   EventTracker updates the Source field with the path of the Alerts file.
   (OR)
Type the path of the Alerts file in the **Source** field.

By default, EventTracker selects the **Import E-mail Settings** checkbox to import Alerts along with their e-mail configuration settings.

Clear this checkbox to import Alerts without the associated e-mail settings.

6 Select an appropriate **Set Active** option.

**NOTE**

**Active Alerts:** Active Alerts are Alert events that have at least one action set.

Select the **Only if notifications set** option to make an Alert active, had you set any sort of action to the Alert.

Select the **By default** option if you wish to make an Alert active irrespective of whether the Alert has an associated action or not.

7 Click **Import**.

EventTracker displays the Export Import Utility message box.

8 Click **OK**.

**Import System Groups**

1 Select the **Start** button, select **All Programs**, and then select **Prism Microsystems**.

2 Select **EventTracker**, select **EventTracker Control Panel**, and then select **Export Import Utility**.

3 Click the **Import** tab. Select the **Systems and Groups** option.

4 Select the **EventTracker (.issys)** option to import the .issys type file.

   (OR)

Select the **Custom format** option to import other type of files such as .txt files. The files should be written in the prescribed format.

   - Click **Add systems** option:
Text file contains one system name per line.

- Click **Remove systems** option:
No system name included in the text file.

- Select **Add systems & Groups** option.
Text file contains system and group name.

5. Click the browse button. EventTracker displays the Open pop-up windows.

6. Navigate and locate the systems and groups file you want to import. Click Open. EventTracker updates the Source field with the path of the systems and groups file. (OR)
   Type the path of the systems and groups file in the Source field.

7. Click Import. EventTracker displays the Export Import Utility message box.

8. Click OK.

**Import RSS Feeds**

1. Select the Start button, select All Programs, and then select Prism Microsystems.

2. Select EventTracker, select EventTracker Control Panel, and then select Export Import Utility.

3. Select the Import tab. Select the RSS option.

5. Click the browse button. EventTracker displays the Open pop-up window.
6 Navigate and locate the scheduled reports file you want to import. Click **Open**. EventTracker updates the Source field with the path of the RSS Feeds file.

(OR)
Type the path of the RSS Feeds file in the **Source** field.

7 Click **Import**.
EventTracker displays the Export Import Utility message box.

8 Click **OK**.

**Import Scheduled Reports**

1 Select the **Start** button, select **All Programs**, and then select **Prism Microsystems**.

2 Select **EventTracker**, select **EventTracker Control Panel**, and then select **Export Import Utility**.

3 Select the **Import** tab, and then select the **Scheduled Reports** option.

4 Click the browse button.
EventTracker displays the Open pop-up window.

5 Navigate and locate the Scheduled reports file you want to import. Click Open.

EventTracker updates the Source field with the path of the Scheduled reports file.

   (OR)
   Type the path of the Scheduled reports file in the Source field.

6 To schedule the time of report generation, select Scheduled Settings options.

7 Enter the Schedule Time.

8 Click Import.

   EventTracker displays the Export Import Utility message box.

9 Click OK.

Import Behavior Rules

1 Select the Start button, select All Programs, and then select Prism Microsystems.

2 Select EventTracker, select EventTracker Control Panel, and then select Export Import Utility.

3 Select the Import tab, Select the Behavior Rules option.

4 Click the browse button.
   EventTracker displays the Open pop-up window.

5 Navigate and locate the Behavior Rules file you want to import. Click Open.
   EventTracker updates the Source field with the path of the Behavior Rules file.

   (OR)
   Type the path of the Behavior Rules file in the Source field.

6 Click Import.
   EventTracker displays the Export Import Utility message box.

7 Click OK.

Import SCAP Content

1 Select the Start button, select All Programs, and then select Prism Microsystems.

2 Select EventTracker, select EventTracker Control Panel, and then select Export Import Utility.

3 Select the Import tab, and then select the SCAP option.
   EventTracker displays the EventTracker - SCAP Content Import Utility pop-up window.
All the 'Check validity...' checkboxes are selected by default.

4. Click the browse button.
   EventTracker displays the Browse for folder pop-up window.

5. Navigate and locate the input directory that contains SCAP content XML files. Click Ok.

6. Select appropriate benchmark from the Select benchmark dropdown.
   EventTracker displays the Export Import Utility message box.

7. Click OK.

Import Token Value

4. Select the Start button, select All Programs, and then select Prism Microsystems.

5. Select EventTracker, select EventTracker Control Panel, and then select Export Import Utility.

6. Select the Import tab, Select the Token Value option.

8. Click the browse button.
   EventTracker displays the Open pop-up window.

9. Navigate and locate the Behavior Rules file you want to import. Click Open.
EventTracker updates the Source field with the path of the Token Value file.

(OR)

Type the path of the Behavior Rules file in the Source field.

10 Click Import.

EventTracker displays the Export Import Utility message box.

11 Click OK.
Chapter 38
Append Archives

In this chapter, you will learn how to:

- Append CAB files
Append CAB Files

Append Archiver appends CAB files to the Archives folder and updates the archive index with minimal time consumption.

1. Double-click **Append Archives** on the EventTracker Control Panel.
   
   EventTracker displays the Append Archives window.

   ![Append Archives Window](Image)

   - Indicates the CAB files present in the Archives folder. EventVault Warehouse Manager will ignore redundant CAB files.
   - Indicates that the CAB files are not present in the destination folder i.e. EventTracker Archives folder.
After creating the index file, EventVault Warehouse Manager displays the Append Archives window with actual physical files present in the Archives folder.

**Search in Sub Folders** checkbox is selected by default. Clear this checkbox to search the archives in the root folder alone and not in the sub folders.

2. Click and select the path of the folder where you have stored the CAB files. Click **OK**.

EventVault Warehouse Manager displays the Append Archives window with CAB files to append.

You can select individual files by selecting the checkboxes against the respective CAB files or collectively by selecting the **Select all missing files** checkbox.

3. Click **OK**.

EventVault Warehouse Manager displays the progress of appending process. After the successful completion, EventVault Warehouse Manager displays the Append Archives message box.

4. Click **OK**.
EventVault Warehouse Manager displays the Append Archives window with list of CAB files appended. EventVault Warehouse Manager appends the cab files to the appropriate folders.
Figure 480
Chapter 39
Agent Configuration

In this chapter, you will learn how to:

- Manage Windows and syslog Managers
- Filter the events
- Monitor System
- Monitor Applications
- Monitor Services
- Monitor Log Files
- Monitor Network Connection
- Monitor Processes
- Maintain Log Backup
- Transfer Log Files
- Configuration Assessment
- Syslog FTP server
- Backup Current Configuration
Managers

All configurations for agent(s) are set by default during installation. If you are interested in changing the default configuration settings, then


![EventTracker Agent Configuration](image-url)  
*Figure 481*
2. Click appropriate tabs and configure the agent as you wish.

Event Filters

This option enables you to filter events being sent to the Manager. Select appropriate checkboxes under Basic Logs, Special Logs, and Event Types.

To filter Events

1. Double click EventTracker Control Panel, select EventTracker Agent Configuration.
2. Select the system from the Select System hyperlink. Click Event Filters tab.

EventTracker displays the Event Filters tab.

![Event Filters Configuration](image)

Figure 482
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Logs</td>
<td>Select appropriate checkboxes to filter the events being sent to the Manager.</td>
</tr>
<tr>
<td>Special Logs</td>
<td>Select appropriate checkboxes to filter the events being sent to the Manager.</td>
</tr>
<tr>
<td>Event Types</td>
<td>Select appropriate checkboxes to filter the events being sent to the Manager.</td>
</tr>
<tr>
<td>Example: Event Types -&gt; Warning</td>
<td>The filter is now set and all events with Event Type Warning will be filtered out and will not be sent to EventTracker Manager.</td>
</tr>
<tr>
<td>Enable SID Translation</td>
<td>Select this checkbox to enable SID translation. For more information on SID translation, refer SID-translate.pdf in the EventTracker installation folder.</td>
</tr>
<tr>
<td>Enable High Performance mode</td>
<td>Select this checkbox to switch the Agent performance modes.</td>
</tr>
<tr>
<td>Filter Exception</td>
<td>Click this button to set the filter exceptions for the specific events that you want to monitor.</td>
</tr>
<tr>
<td>Advanced Filters</td>
<td>Click this button to set the filters for the specific events that you do not want to monitor.</td>
</tr>
</tbody>
</table>

By default, EventTracker filters Information and Audit Success events.

3. Set the available filter options appropriately, and then click the **Save** button.

**Filter Events with Exception**

This option helps you to filter events with exception. For example, had you configured agent to filter **Information** events, all events of 'Information' event type will not be forwarded to the Manager. However, if you wish to send specific events of **Information** event type, you can exempt those events from filtering.

**To filter events with exception**

1. Double click **EventTracker Control Panel**, select **EventTracker Agent Configuration**.
2. Select the system from the **Select System** hyperlink.
3. Click the **Event Filters** tab.
   - EventTracker displays the Event Filters tab.
4. Click **Filter Exception**.
   - EventTracker displays the Filter Exception pop-up window with a list of events exempted from filtering.
5 To modify event details, select a row and then click **Edit**.
6 To remove event details, select a row and then click **Delete**.
7 To add filter exceptions, click **Add**.

EventTracker displays the Filter Exception pop-up window to select/enter event details.
8  Enter appropriate data in the relevant fields.
   For ex:
   Log Type: Application, Event Type: Information, Match in Source: Web Service

   ![Event Details](image)

   **Figure 485**

   "Match in Event Descr" field can take multiple strings separated with "&" or "||".
   - "&" stands for AND condition. - "||" stands for OR condition.
   For negating the result of match operation, prefix the string with "[$NOT$]". If there are
   multiple strings, then the result of the whole expression is negated. Only one "[$NOT$]"
   should be used in the string.
   Example:
   The string "[$NOT$]Logon Type: 4||Logon Type: 5" will match all events that DO NOT
   contain "Logon Type: 4" or "Logon Type: 5" in the description.
   For more information click here.

9  Click **OK**.

   EventTracker displays the Filter Exception pop-up window with the newly added filter exception.
Click Close, and then click Save.

Filter Events with Advanced Filters

Filters and Filter Exception go hand in hand, which means you can filter all the events but with exceptions. Whereas Advanced Filters help, you filter out a specific event allowing other events of that type.

1. To filter events with Advanced Filters, double click EventTracker Control Panel, select EventTracker Agent Configuration.
2. Select the system from the Select System hyperlink.
3. Click the Event Filters tab.
   EventTracker displays the Event Filters tab.
4. Click Advanced Filters.
   EventTracker displays the Advanced Filters pop-up window with a list of advanced filters.
Click **New**.

EventTracker displays the Advanced Filters pop-up window to select/enter event details.

6. Enter appropriate data in the relevant fields and then click **OK**.

   EventTracker displays the Advanced Filters pop-up window with the newly added filter.

7. Click **Close**.

   **NOTE**

   The filter is set and specific events matching the filter criteria will not be forwarded to EventTracker Manager. All Error Events will be forwarded to the Manager except the events matching the filtered criteria set.

8. Click **Save**.

**Enable SID Translation**

This option helps you enable SID translation.

1. Double click EventTracker Control Panel, select EventTracker Agent Configuration.

2. Select the system from the Select System hyperlink.

3. Click the Event Filters tab.

   EventTracker displays the Event Filters tab.

4. Select the system from the **Select System** hyperlink.

5. Click the **Event Filters** tab.
6 Select the **Enable SID Translation** checkbox.

EventTracker displays the Caution message box.

![Caution message box](image)

**Figure 488**

7 Click **Yes** and then click **Save**.

**NOTE**

This feature works in all versions of EventTracker from 5.2 upwards. More information please go through `SID-translate.pdf` found in the EventTracker installation folder typically, `...\Program Files\Prism Microsystems\EventTracker`.

---

**System Monitor**

Monitoring CPU, memory performance and disk usage of a system enables the administrator to monitor the general health of a system. You can configure general health thresholds for CPU and Memory Usage. All thresholds are measured in percent terms.

When the configured threshold is crossed, an event will be generated and reported to the manager. An event will also be generated when the thresholds are back to below configured levels.

Care is taken not to report spikes in CPU or memory usage by a process. Therefore, when an event is seen that a system is crossing thresholds, you can be sure that this is for a long enough period and need to investigate.

The default threshold limits are 80% for all variables. A configuration of 0% would disable the monitoring for that specific variable.
USB and other Device Changes option helps to monitor insertion or removal of USB and other media. Also helps to track file transactions that occur in the inserted media.

To configure system performance threshold

1. Double click **EventTracker Control Panel**, select **EventTracker Agent Configuration**.
2. Select the system from the **Select System** hyperlink.
3. Click the **System Monitor** tab.

   EventTracker displays the System Monitor tab.

![EventTracker Agent Configuration](image)

*Figure 489*
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance</td>
<td></td>
</tr>
<tr>
<td>CPU Performance (%)</td>
<td>Select a threshold limit to monitor CPU performance from the drop-down list.</td>
</tr>
<tr>
<td>Memory Usage (%)</td>
<td>Select a threshold limit to monitor memory usage from the drop-down list.</td>
</tr>
<tr>
<td>Disk Space Usage (%)</td>
<td>Select a threshold limit to monitor disk space usage from the drop-down list.</td>
</tr>
<tr>
<td>USB and other Device Changes</td>
<td></td>
</tr>
<tr>
<td>Report insert/remove</td>
<td>Select this checkbox to track insertion or removal of USB or other devices.</td>
</tr>
<tr>
<td>Record activity</td>
<td>Select this checkbox to monitor file transactions occur in the inserted devices.</td>
</tr>
<tr>
<td>Disable USB Devices</td>
<td>Select this checkbox to disable USB devices. The selection will enable the 'USB Exception List' button.</td>
</tr>
<tr>
<td>USB Exception List</td>
<td>Click this button to add the USB device ID or serial number in the exception list. The listed USB devices will not be disabled when inserted.</td>
</tr>
</tbody>
</table>

4. To change the disk space configuration values, click the Advanced button. Advance Disk Space Configuration window displays.

![Advanced Disk Space Configuration](image)

5. Enter the Drive: name. Ex: D drive.

6. Select/Enter the required value in Used more than % drop-down or Free less than (MB).

7. Click the Add button.
8 To edit or delete the disk space configuration, click the Edit or Delete button accordingly.

9 Click Save & Close once necessary changes have been done.

10 Select the required Performance, USB and other Device Changes options.

11 Click Save.

Add USB Device in the Exception List

While disabling USB Devices on a particular computer, you can also exempt and enable USB devices from monitoring.

To configure USB Exception List

1 Select the Disable USB Devices checkbox.

2 Click USB Exception List button.

   EventTracker displays the 'USB Exception List' pop-up window.
3 Type the USB serial number in decimal format or hexadecimal format in the Enter USB Serial Number field, and then select the Format option accordingly.

OR

Type USB device ID in the Enter USB Device ID field.

4 Click the Add button.

EventTracker adds the newly entered serial number or device ID in the exception list.

5 Click Save & Close button.

6 In 'Windows Agent Configuration' page, click the Save button to save the configuration changes.

**NOTE**

Please refer How to – Monitor Removable Media Device document for more details on creating exception list and its functionality.
Monitor Applications

This option enables you to monitor installation and un-installation of applications, and monitor application usage. EventTracker logs a custom information event whenever a monitored application is opened or closed. These events are received at the Console and helps in tracking the application usage.

EventTracker monitors all applications specified in ‘Monitor Specific Apps’ and ignores applications specified in ‘App Exception’.

To monitor application install/uninstall

1. Double click **EventTracker Control Panel**, select **EventTracker Agent Configuration**.
2. Select the system from the **Select System** drop-down, and then select the **Monitor Apps** tab.

EventTracker displays the ‘Monitor Apps’ tab.

![EventTracker Agent Configuration](image)

**Figure 493**
## Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor App Install/ Uninstall</td>
<td>Select this checkbox to monitor installation and un-installation of applications.</td>
</tr>
<tr>
<td>Monitor App Usage</td>
<td>Select this checkbox to monitor application usage. This selection enables the App Exceptions and Monitor Specific Apps buttons.</td>
</tr>
<tr>
<td>App Exceptions</td>
<td>Enables you to set the applications that you do not wish to monitor.</td>
</tr>
<tr>
<td>Monitor Specific Apps.</td>
<td>Enables you to set the applications that you wish to monitor.</td>
</tr>
</tbody>
</table>

4 Select appropriately the **Monitor App Install / Uninstall** and **Monitor App Usage** options.
5 Click the **Save** button.

### Filter Applications that need not be monitored

1 To filter applications that need not be monitored, double click **EventTracker Control Panel**, select **EventTracker Agent Configuration**.
2 Select the system from the **Select System** hyperlink.
3 Click the **Monitor Apps** tab.
   EventTracker displays the **Monitor Apps** tab.
4 Select the **Monitor App Usage** checkbox, if not selected.
5 Click **App Exceptions**.
   EventTracker displays 'List of applications that will not be monitored' pane.

6 Click the **Add** button.
   EventTracker opens a textbox to type the file name of the applications.

![App Exceptions](image)
7 Type the application name with .exe extension that you do not want to monitor.
   For Example: AppFile.exe
   NOTE: The Application name should be in .exe format.
8 Click OK and then click Save.

Filter Applications that need to be monitored
1 To filter applications that need to be monitored, double click EventTracker Control Panel, select EventTracker Agent Configuration.
2 Select the system from the Select System hyperlink.
3 Click the Monitor Apps tab.
   EventTracker displays the 'Monitor Apps' tab.
4 Select the Monitor App Usage checkbox, if not selected
5 Click Monitor Specific Apps.
   EventTracker displays 'List of app executables' pane.
6 Click Add.
   EventTracker opens a textbox to type the file name of the application.
Type the application name with .exe extension that you want to monitor.

Click OK and then click Save.

Monitor Services

By default, EventTracker monitors all Windows Services for stop/start. If a service stops, an event will be sent immediately to the Manager. An event will also be sent if a stopped service restarts.

You can also choose to automatically restart services that have been stopped.

There may be certain services that you may not want to monitor. You can filter out such services from the monitoring list.

The service name that needs to be configured can be either the name as displayed in Control Panel -> Services or the display name. While configuring the service name, please ensure that it is spelt correctly.

Configure Service Restart List

This option helps to add services to the restart list.

1. Double click EventTracker Control Panel, select EventTracker Agent Configuration.
2. Select the system from the Select System hyperlink.
3. Click the Services tab.

EventTracker displays the Services tab.
Field | Description
--- | ---
Services Monitoring | This checkbox is selected by default to monitor all Windows services. 'Service Restart List' and 'Service Monitor Exceptions' will be enabled only if 'Service Monitoring' checkbox is selected.
Service Restart List | By default following services are monitored:
  - EventTracker Alerter
  - StatusTracker
  - EventTracker EventVault
  - TrapTracker
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>EventTracker Indexer</strong></td>
<td>EventTracker Reporter</td>
</tr>
<tr>
<td><strong>EventTracker Receiver</strong></td>
<td>WcwService</td>
</tr>
<tr>
<td><strong>EventTracker Remoting</strong></td>
<td>EventTracker Scheduler</td>
</tr>
</tbody>
</table>

Click Add to add selected services to restart when they stop.
Click the Remove button to remove the services from the 'Services restart list'.

| Service Monitor Exceptions  | Click Add to add services that you do not want to monitor. Click Remove to remove the services from the list. |

4. Click **Add** under **Service Restart List**.
   EventTracker displays the **Enter Service Name** field to type the name of the service.

5. Type the name of the service, and then click **OK**.

6. Click **Save**.

**Filter Services**

1. Double click **EventTracker Control Panel**, select **EventTracker Agent Configuration**.
2. Select the system from the **Select System** hyperlink, and then select the **Services** tab.
3. Click the **Add** button under **Service Monitor Exceptions**.
4. Type the name of the service that you do not wish to monitor in the **Enter Service Name** field.
5. Click **OK** and then click **Save**.
Logfile Monitor

This option enables you to monitor multi-vendor log files with matching keyword entries. EventTracker generates an event if any matching record is found. The Log file monitoring configurations can be done through EventTracker Agent Configuration provided on the EventTracker Control Panel. In the EventTracker Enterprise (Web GUI), you can only view the Logfile monitoring settings.

2. Select the system from the Select System drop-down, and then select Logfile Monitor tab.

EventTracker opens the ‘Logfile Monitor’ tab.
<table>
<thead>
<tr>
<th>Click</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add File Name</td>
<td>Add a log file that you wish to monitor.</td>
</tr>
<tr>
<td>View File Details</td>
<td>View log file details.</td>
</tr>
<tr>
<td>Delete File Name</td>
<td>Delete the log file name from the list.</td>
</tr>
<tr>
<td>Search Strings</td>
<td>Configure the strings to search.</td>
</tr>
</tbody>
</table>

3 Click the **Add File Name** button.

EventTracker displays the 'Enter File Name' window.

4 Click the **Get All Existing Log Files** checkbox, if you want all the existing files prior to this configuration and the files that are logged after this configuration.

5 Select the logfile type from the **Select Logfile Type** drop-down list.

6 Type the path in the **Enter File Name** field.

   (OR)

   Click the browse button to locate the log file.

   EventTracker displays the 'Select Folder/File Name' dialog box.
7 Select the **Show all the files** checkbox to view all files with different file extensions.

8 Go to the appropriate folder, and then select an appropriate file which is associated with the selected 'Log File Type'.

9 Click **OK**. EventTracker displays the 'Enter File Name' window with the file location.

10 Click **OK**. EventTracker displays the 'EventTracker Agent Configuration' message box.
11 Click **Yes**.

EventTracker displays the Search String dialog box.

12 Click the **Add String** button.

EventTracker displays the ‘Enter Search String’ dialog box.
13 Select the file name from the **Select Field Name** drop-down list.

14 Type the string that you want to search in the **Enter Search String** field. EventTracker displays the Enter Search String dialog box.

15 Click **OK**. EventTracker displays the Search String dialog box.

16 Click **OK**. EventTracker displays the ‘Agent Configuration’ window with the newly added Logfile entry.
17 Click the **Save** button.
GOOD TO KNOW:
To select multiple files with the same or different file extension:
You can select multiple files with the same or different file extension by using wildcard character *.
Click the Add File Name button. In the Enter File name window, click the browse button to locate the log file.

In the Select Folder/File Name dialog box, click the OK button. (Do not select the file name from the folder.)

EventTracker displays the Select File Extension window.

Type the file name in the given field or leave as it is to consider all files in the selected folder with file extension 'w3c' for monitoring.

If you are specifically interested in monitoring ISA Firewall log files, type the file name as 'ISALOG*'

To select multiple files irrespective of file extensions, type '\*.*'.
View File Details
This option helps you to view files details.

1 To view file details in EventTracker Control Panel, open the EventTracker Agent Configuration window.
2 Select the system from the Select Systems drop-down list.
   EventTracker displays the 'Logfile Monitor' tab.
3 Click the Logfile Monitor tab.
4 Select the log file from the list under Logfile Name.
5 Click View File Details.
   EventTracker displays the 'Enter File Name' window.

![Enter File name](image)

   Figure 509

6 Click Close.

Delete Log File Monitoring Settings
This option helps you delete log file monitoring settings.

1 To delete log file monitor settings in EventTracker Control panel, open the EventTracker Agent Configuration window.
2 Select the system from the Select Systems drop-down list, and then select the Logfile Monitor tab.
3 Select the log file from the Logfile Name list, and then select Delete File Name.
4 Click Save on the Agent Configuration window.

Search Strings
This option helps you search strings.

1 In EventTracker Control panel, open the EventTracker Agent Configuration window.
2 Select the system from the Select Systems drop-down list. Select Logfile Monitor tab.

3 Select the log file from the Logfile Name list. Select Search Strings.

![Figure 510](image)

4 Click Add String.
   EventTracker displays the Enter Search String dialog box.

5 Select the file name from the Select Field Name drop-down list.

6 Type the string that you want to search in the Enter Search String field.
   EventTracker displays the Enter Search String dialog box with newly added search string entry.

![Figure 511](image)
7  Click OK. 
EventTracker displays the Search String dialog box with newly added search string.

To modify, click Edit String. Enter appropriately in the relevant fields in the displayed Enter Search String dialog box, and then click OK.

OR
To delete, select the string you want to delete and then click Delete String in the Search String dialog box.

8  Click OK on the 'Search String' dialog box.
EventTracker displays the 'Agent Configuration' window with the modified settings.

9  Click Save.

Monitor Check Point Logs 
This option helps you monitor logs generated by Check Point.

1  To monitor checkpoint logs in EventTracker Control panel, open the EventTracker Agent Configuration window.

2  Select the system from the Select System drop-down list, and then select the Logfile Monitor tab.

3  Click the Add File Name button.
EventTracker displays the Enter File Name dialog box.

4  Select the logfile type as 'CHECKPOINT' from the Select Logfile Type drop-down list.
EventTracker unfolds a pane with configuration options.
5 Select an option from the **Communication Method** drop-down list.

<table>
<thead>
<tr>
<th>Communication method options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPSEC_SSLCA</td>
<td>Encryption Method: 3DES</td>
</tr>
<tr>
<td></td>
<td>Compressed: No</td>
</tr>
<tr>
<td>OPSEC_SSLCA_COMP</td>
<td>Encryption Method: 3DES</td>
</tr>
<tr>
<td></td>
<td>Compressed: Yes</td>
</tr>
</tbody>
</table>

6 Type **LEA Server Name**.

7 Type the **Client DN**.
   Check Point generated this string while configuring the OPSEC Application.

8 Type the **Server DN**.
   This is the Check Point Gateway DN.

9 Click the browse button ![...](image) to locate SSLCA file.
10 Select the SSLCA file and then click **Open**.
EventTracker populates the SSLCA file field.

11 Type the **Server IP**.
This is the IP of the host where Check Point is installed.

12 Type the **Server Port**.
This can be any port but should be consistent with what you have entered earlier in the fwopsec.conf file.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>This option is selected by default. Select this option to receive live Check Point logs from the point in time the configuration takes effect.</td>
</tr>
<tr>
<td>Historical</td>
<td>Select this option to read from previous logs and the current logs as well. This option has two modes namely Current Logs and All Logs. Select the Current Logs option to read from the first record of the current log. This mode is selected by default. Select the All Logs option to read from all the backed up logs and the current logs.</td>
</tr>
</tbody>
</table>

13 Click **OK**.
EventTracker displays the `Agent Configuration` window.
Monitor VMware Logs

This option helps you monitor logs generated by VMware.

1. To monitor VMware logs in EventTracker Control Panel, open the EventTracker Agent Configuration window.
2. Select the system from the Select System drop-down list.

14. Click Save.
3 Click the **Logfile Monitor** tab.

4 Click the **Add File Name** button.
   EventTracker displays the 'Enter File Name' dialog box.

5 Select the logfile type as VMWARE from the **Select Logfile Type** drop-down list.
   EventTracker unfolds a pane with configuration options.

![Figure 514](image)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware URL</td>
<td>Type a valid URL, e.g. <a href="https://esxvcserver/sdk/vimService">https://esxvcserver/sdk/vimService</a> You can also replace the server name with the IP address.</td>
</tr>
<tr>
<td>User Name</td>
<td>Type valid user name.</td>
</tr>
<tr>
<td>Password</td>
<td>Type valid password.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Time connection timeout.</td>
</tr>
</tbody>
</table>

6 Type appropriately in the relevant fields.

7 Click **Test Connection** to check if the configuration parameters you have entered are correct.

8 Click **OK**.
   EventTracker displays the Agent Configuration window.
9. Click **Save**.
Monitor Network Connections

NCM (Network connection monitoring) provides you with the capability to effectively monitor for network connections on any system in your enterprise. It is a feature that provides you security beyond the firewall by detecting threats from inside the firewall as well as keeping the external attackers at bay.

It helps you keep track of various happenings like connections established by remote applications, unauthorized connections to server and connections made to standard ports.

NCM provides second level security beyond firewall. NCM can drastically reduce internal security threats and can be configured to raise an alert whenever any intruder outside a list of trusted IP addresses attempts to make network connection. The NCM functionality can also be set at high security mode wherein an event is generated for all incoming and outgoing connections.

The NCM functionality facilitates to achieve the following key objectives:

- Host based intrusion detection
- To provide second level security and complement to firewall and anti-virus
- In strengthening security policies
- To improve security policies against inside security breaches
- To monitor all network connections (TCP and UDP)
- For constant unattended, reliable monitoring of intrusion detection
- Flexible configuration as per the business requirement

To monitor network connection

1. Double click EventTracker Control Panel, select ’EventTracker Agent Configuration’.
2. Select the system from the Select System hyperlink.
3. Click the Network Connection Monitor tab.
   EventTracker displays the ’Network Connection Monitor’ tab.
Field | Description
--- | ---
TCP | This checkbox is selected by default to monitor TCP network connections.
UDP | This checkbox is selected by default to monitor UDP network connections.
Connection States
Open | This checkbox is selected by default to monitor opened TCP/UDP connections.
Changed | Select this checkbox to monitor TCP/UDP connections whose connection state has been changed recently.
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Close</td>
<td>This checkbox is selected by default to monitor closed TCP/UDP connections.</td>
</tr>
<tr>
<td>All Network Traffic (NCM): By default, EventTracker selects this option.</td>
<td></td>
</tr>
<tr>
<td>Exclude List</td>
<td>Click this button to configure the network connections that need not be monitored. A notification will be sent for the entries in this list, if the port is open.</td>
</tr>
<tr>
<td>Include List</td>
<td>Click this button to configure the network connections to monitor. Entries in this list will always be monitored. 'Include Network Connections List' always override the 'Exclude Network Connections List'.</td>
</tr>
<tr>
<td>Suspicious Traffic Only (SNAM)</td>
<td></td>
</tr>
<tr>
<td>Trusted List</td>
<td>Click this button to view and configure trusted network connections.</td>
</tr>
</tbody>
</table>

4. Select or clear the **TCP** or **UDP** checkbox.
5. Click the **Save** button.

### Exclude Network Connections

1. Double click **EventTracker Control Panel**; select ‘**EventTracker Agent Configuration**’.
2. Select the system from the **Select System** hyperlink.
3. Click the **Network Connection Monitor** tab.
   - EventTracker displays the ‘Network Connection Monitor’ tab.
4. Click **Exclude List**.
   - EventTracker displays the Exclude List pop-up window.

![Exclude List](image-url)

**Figure 517**
5 Click **New**.

EventTracker displays the Exclude List window to type Network Connection Details.

![Network Connection Details window](image)

**Figure 518**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Local Address Details</strong></td>
<td></td>
</tr>
<tr>
<td>Host Name or IP Address</td>
<td>Type the host name or the IP address in this field.</td>
</tr>
<tr>
<td>Local Port</td>
<td>Select a local port from the drop-down list.</td>
</tr>
<tr>
<td><strong>Remote Address Details</strong></td>
<td></td>
</tr>
<tr>
<td>Host name, IP Address or URL</td>
<td>Type the host name, IP address or URL in this field.</td>
</tr>
<tr>
<td>Remote Port</td>
<td>Select a remote port from the drop-down list.</td>
</tr>
<tr>
<td><strong>Select IP Address Range</strong></td>
<td>Click this button to add IP address range. EventTracker displays the IP Address Range Setting dialog box.</td>
</tr>
</tbody>
</table>
### Field Description

**Select IP Address Range**
- *Type the range until which you want to monitor the IP network connections.*
- *This option is available only when you Type the IP address in the Host name, IP address or URL field.*

**Subnet Range**
- *Enter the Remote IP Address Range (e.g. 192.168.1.1 to 51)*

**Remote IP Address**
- *192.168.1.1* to 

**Process Name**
- *Type the process name in this field.*

**Connection State**
- *Select a connection state from the drop-down list.*

<table>
<thead>
<tr>
<th>NOTE</th>
</tr>
</thead>
<tbody>
<tr>
<td>If a field is left blank, a wildcard match for that field is assumed. For example, leaving the Local Port field blank implies that any value in that field is acceptable.</td>
</tr>
</tbody>
</table>

6. Enter appropriate data in relevant fields.
7. Click **OK**.

EventTracker displays the Exclude List with the newly added entry.

![Exclude List](image)

**Figure 519**
8 To modify the network connection details, click **Edit**.
9 To delete the network connection details, select the network connection details you want to delete from the list, and then click **Delete**.
10 Click **Close** on the Exclude List pop-up window.
11 Click **Save**.

**Include Network Connections to monitor**

1 Double click **EventTracker Control Panel**; select ‘**EventTracker Agent Configuration**’.
2 Select the system from the **Select System** hyperlink.
3 Click the **Network Connection Monitor** tab.
   EventTracker displays the ‘Network Connection Monitor’ tab.
4 Select the appropriate checkboxes.
5 Click **Include List**.
   EventTracker displays the Include List pop-up window.
6 Select the **Monitor only the ports that are in this list** checkbox to monitor only the ports present in the list, and then click **Close**.

![Include List](image)

**Figure 520**

7 To add more network connection details, click **New**.
   EventTracker displays the Include List window to type network connection details.
8 Enter appropriate data in the relevant fields.
9 Click **OK**.

EventTracker displays the Include List with the newly added entry.
10 To modify the network connection details, click **Edit**.

11 To delete the network connection details, select the network connection details you want to delete from the list, and then click **Delete**.

12 Click **Close**, and then click **Save**.

### Suspicious Connections

This feature is an enhancement of the existing 'Network Connection Monitoring'. This option enables you to monitor the suspicious usage of TCP or UDP ports and their connection states. By default, all the connections are suspicious and you can exempt applications and ports from monitoring. EventTracker is shipped along with a list of applications and ports, which are not harmful to any enterprise environment. As discussed, EventTracker Agent will not monitor these White-listed applications and ports.

#### NOTE

Prior to enabling EventTracker Agent to monitor Suspicious Traffic, apply all the latest Microsoft patches / hotfixes if the operating system is Windows 2000.

### Monitor Suspicious Connections

This option helps you to monitor suspicious connections and to view predefined trusted connections list. EventTracker does not monitor the connections listed in Trusted List. You can also edit predefined trusted connection list and define your own set of trusted connection list.

1 To view Trusted List in EventTracker Control panel, open the **EventTracker Agent Configuration** window.

2 Select the system from the **Select Systems** drop-down list.

3 Click the **Network Connection Monitor** tab.

   EventTracker displays the Network Connection Monitor tab.

4 Select **Suspicious Traffic Only (SNAM)** option.

5 Click the **Trusted List** button.

   EventTracker displays the 'Trusted Connections List' dialog box
Figure 523

Click To

Add new trusted connections. EventTracker displays’ Trusted Port Details’ dialog box.

Type appropriate details in the relevant fields and then click **OK**. You can use wild cards to search processes. For example, had you configured Virtual Collection Points and wish to add all EventTracker Receiver processes, it is enough to provide the Process name as **EtReceiver*.exe**.

You can also use **...** browse button to locate the process.

Select a process from the list and then click **Edit**. EventTracker displays ‘Trusted Port Details’ dialog box.

Edit required details in the relevant fields and then click **OK**.
**GOOD TO KNOW:**

**Suspicious Traffic Only (SNAM)** option helps you to view, enable, and disable predefined trusted connections list. The connections listed in the **Trusted List** are exempted from monitoring. The trusted list contains a list of known good applications and ports through which the usual network connections between the processes happen.

You can edit the predefined trusted connection list and can define your own set of trusted connection list. By default, the **predefined trusted connections are enabled**, which means EventTracker exempts those processes and ports from monitoring.

Clear the checkbox next to the process that you wish to monitor by EventTracker. In some rows in the list, you might notice ‘Process Name’ field is empty, this signifies that any processes that communicate through the defined ports are deemed to be legitimate.

Similarly, in some rows you might notice that the ‘Local port’ and/or ‘Remote Port’ are 0 (zero). This signifies that the processes listed could use any available ports to communicate. EventTracker considers that traffic to be legitimate and exempts from monitoring.

---

**Add Programs to the Trusted List**

This option helps you add programs installed in your computer to the trusted list. You can enable or disable the entries in the trusted programs list. Enable means the processes and the ports used by the processes are legitimate and disable means illegitimate and EventTracker monitors them.

1. To add programs to trusted list, click Add Program.

   EventTracker displays the ‘Add Program to Trusted List’ window.
2. Select the checkbox against the programs or select the **Select All** checkbox to select all the programs.

3. Click **Add**.  
   EventTracker adds the selected program to the Trusted Connections List.

4. Click **Close** and then click **Save**.

### Add Firewall Exceptions to the Trusted List

This option helps you add the processes and ports in the Firewall programs and ports Exceptions to the trusted list.

1. To add firewall exception to the trusted list in **Trusted Connections List**, click **Add Firewall List**.  
   EventTracker displays the 'Add Program/Port to Trusted List' window.
By default, EventTracker selects the **Add Program** option and displays the programs in the exceptions list.

Or

Select the **Add Port** option, EventTracker displays available ports in the exception list.

2. Select the programs or select the **Select All** checkbox and then click **Add** to add programs to the trusted list.

EventTracker adds the selected items to the ‘Trusted Connections’ List.
Monitor Processes

Process monitoring enables the administrator to monitor the general health of processes on a system. You can configure general process health thresholds for CPU and Memory Usage per process. CPU usage is measured in terms of percentage while memory usage is measured in absolute terms.

When the configured threshold is crossed, an event will be generated and reported to the Manager. An event will also be generated when the thresholds are back to below configured levels.

Care is taken not to report spikes in CPU or memory usage by a process. Therefore, when an event is seen that a process is crossing thresholds, you can be sure that this is for a long enough period and need to investigate.

By default, all processes will be monitored and the default threshold limits are 1024MB of Memory Usage and 85% of CPU.

You can also choose to filter out processes that you do not want to monitor. By default, all processes will be monitored.

To monitor configured processes

1. Double click EventTracker Control Panel, select EventTracker Agent Configuration.
2. Select the system from the Select System drop-down, and then select the Processes tab.
   EventTracker displays the Processes tab.
3. Select the system from the Select System hyperlink.
4. Click the Processes tab.
   EventTracker displays the 'Processes Monitoring' window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Performance (%)</td>
<td>Select CPU Performance threshold limit from the drop-down list.</td>
</tr>
<tr>
<td>Memory Usage (MB)</td>
<td>Type the memory usage threshold limit in MB in this field.</td>
</tr>
</tbody>
</table>

5. Click the Add button.
   EventTracker unfolds an option to type the process name.
6. Type the process name in the Enter Process Name field.
7. Click OK.
   EventTracker adds the process to the List of Filtered Processes pane
8. Click the Save button.
NOTE

EventTracker generates the process event when the set threshold value crosses the limit for more than 3 minutes.

Remove Processes from ‘List of Filtered Processes’

1. Double click EventTracker Control Panel, select EventTracker Agent Configuration.
2. Select the system from the Select System drop-down, and then select the Processes tab.
   EventTracker displays the Processes tab.
3. Select the process form List of Filtered processes pane, select Remove and then select the Save button.

Maintain Log Backup

This option enables you to backup event logs automatically in the EventTracker Agent directory whenever the event logs are full. EventTracker automatically performs event log backup or archival in the standard Windows event log format (.evt/.evtx format).

To backup event logs automatically

1. Double click EventTracker Control Panel, select EventTracker Agent Configuration.
2. Select the system from the Select System drop-down, and then select the Log Backup tab.
   EventTracker displays the Log Backup tab.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear logs as needed</td>
<td>If selected, EventTracker Agent clears log file if and only if offset error is encountered. After clearing, Agent inserts &quot;3241&quot; event to notify the user. In this case, no backup is taken. This is true for any setting of the Windows Event Log’s &quot;When maximum log size is reached&quot; option (i.e. Overwrite events as needed, Overwrite events older than N days, Do not overwrite events (clear log manually)) EventTracker log backup and clear operation: Computer: EXCHTEST</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>Log file name: Application</td>
<td></td>
</tr>
<tr>
<td>Log file backup: Not applicable</td>
<td></td>
</tr>
<tr>
<td>Log file clear: Success</td>
<td>Reason: Received invalid offset error while reading the event log. For more information see Microsoft KB Article #177199.</td>
</tr>
<tr>
<td>Backup event logs</td>
<td>If the &quot;Backup event logs&quot; option is selected, and if the offset is lost at any point, no matter whether &quot;Clear log after backup&quot; checkbox is selected or not the respective log file will be backed up and cleared and the following 3241 event will be logged. EventTracker log backup and clear operation: Computer: EXCHTEST</td>
</tr>
<tr>
<td>Backup Path</td>
<td>By default backed up log files are stored in the EventTracker installation folder typically, ...\Program Files\Prism Microsystems\EventTracker\Agent</td>
</tr>
<tr>
<td>Keep backup files for</td>
<td>If selected, backup files older than selected number of days will be automatically deleted by the agent.</td>
</tr>
</tbody>
</table>

3 Select the required options and then click **Save**.
Transfer Log Files

This option enables you to transfer Windows and other application log files at scheduled times to the manager. Windows logs that are filtered out by the real time settings are cached for transfer (further filtering is available). This minimizes the EventTracker Receiver service workload and conserves the network bandwidth.

To transfer Windows and Application Log Files

1. Double click EventTracker Control Panel, select EventTracker Agent Configuration.
2. Select the system from the Select System drop-down, and then select the File Transfer tab.

EventTracker displays the File Transfer tab.

![EventTracker Agent Configuration](image)

Figure 527
Click button | To
--- | ---
Add | Enter EventTracker Manager name or IP address as destination.

Type the IP address or name of the Manager in the Manager field.
Click the Resolve button to identify newly added manager name or IP address and to check its availability in the network.
Select an option from the Encrypt drop-down list to encrypt and securely transfer the cached events to the destination.
Click OK.

Edit | You can edit the manager name or IP address and even can change the encryption option.

Remove | Delete the destination, i.e. manager name or IP address.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>Set the frequency of file transfer. You can set file transfer to occur every configure hours or daily at a particular time.</td>
</tr>
<tr>
<td>Purge Transferred Files</td>
<td>Set this option to purge files that are transferred to the Manager.</td>
</tr>
</tbody>
</table>
| Retry | Set the number of attempts made in a given time interval by the source Agent machine to transfer the files to the manager system.
You can also generate an event for each transfer attempt, successful transfer or failed transfer as per your choice. |
| Send Windows Events via File Transfer | Select this option to transfer Windows events to the configured managers at scheduled interval. Click the Filters button to further filter the events.
In DLA Filters dialog box, click Add to add the event details. |
| Send other log files via DLA | Select this option to transfer other application log files.
Type the path the folder where log files are dumped or click the browse button to select the folder. |
| Send Now | Click this option to override the Frequency option and transfer the files immediately.
This option is available only under EventTracker Control panel >> File Transfer. |

3. Select the required options and then select **Save**.
Config Assessment

This feature helps to validate actual system security and configuration against NIST recommendations. If enabled, EventTracker Agent listens for requests for assessment, conducts the assessment, and returns the results via the Security Content Automation Protocol (SCAP).

To enable Config Assessment

1. Double click EventTracker Control Panel, select EventTracker Agent Configuration.
2. Select the system from the Select System drop-down, and then select the Config Assessment tab. EventTracker displays the Config Assessment tab.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SCAP</td>
<td>If enabled, EventTracker Agent evaluates the configuration policy against the system and sends back the result to the Manager.</td>
</tr>
<tr>
<td>Working folder</td>
<td>EventTracker Agent stores the temporary files in this folder before it sends the result to the Manager.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purge files after</td>
<td>EventTracker Agent purges the contents of the temporary folder after this configured number of days.</td>
</tr>
</tbody>
</table>

3. Enter appropriate data and then click **Save**.

### Syslog FTP Server

This new feature is introduced to transmit windows events from local systems, as text files containing syslog messages.

### To transfer Windows events as Syslog messages

1. Open **EventTracker Control Panel**, double click **EventTracker Agent configuration** and then select **Syslog FTP server** tab.

A Syslog FTP server window displays.

![Figure 529](image-url)
2 Click the **Add** button.

EventTracker opens Syslog FTP destination window.

![sylog FTP Destination](image)

*Figure 530*

3 Select the **Protocol** name, from the protocol dropdown list.

If you select protocol as FTP then port number 21 will be selected by default in the **Port** field.

If you select protocol as SFTP/SCP, then the **port number 22** will be selected by default in the **Port** field.

4 Enter the server name or IP address in **Server (Name/IP)** field, where the syslog messages need to be transferred.

5 Enter the location in **Directory** field, where the files need to be transferred.

6 Enter the appropriate **Username** and **Password**.

7 Enter the host key in the **Host Key** field, which is provided by the System Administrator.

Host Key option is available only for SFTP/SCP.

8 Click **OK**.

The server details can be seen in the **FTP server(s)** field.

9 Click **Send as syslog Events via File Transfer** option to allow the file transfer to happen.

10 To send other log files, select **Send other log files** option, and then click the  browse button.

EventTracker displays **Browse for folder** pop-up window.

11 Select the log file folder, and then click **Ok**.

(OR)

Click the location where you want to create a folder, and then click **Make a New Folder** button.
EventTracker creates new folder under the selected location. Right click and rename the **New folder**, and then click **Ok**.

14 Select **Also purge files on server** if required.

15 Select **Message Options** to send/receive messages.

16 A syslog Message Options window displays.

![syslog Message Options window](image)

**Figure 531**

17 Select the required **Event Properties**, **syslog Format**.
18 To add new syslog facility or severity settings in RFC 3164 syslog Facility Settings, select the New button. To edit/delete the settings, select the corresponding Edit/Delete button.

19 To add new syslog facility or severity settings in RFC 3164 syslog facility Severity Settings, select the New button. To edit/delete the settings, select the corresponding Edit/Delete button.

20 Select OK, select Save and then select the Close button.

All the files placed in this folder will be transferred to the configured manager.

Back up Current Configuration

This option enables you to back up the current configuration settings.

To backup current configuration settings

1 Open EventTracker Control panel, and then click EventTracker Agent Configuration.
2 Select the system from the Select Systems drop down, select the File menu, and then select the Backup.

Figure 532
EventTracker, by default displays the 'Backup Current Configuration' dialog box.

3  Select the path where you want to backup the current configuration settings.

4  Enter the file name in the **File name** field.

5  The valid file extension is '*.ini'.

6  Click **Open**.

   EventTracker displays the 'EventTracker Agent Configuration' message box.

7  Click **OK**.
Chapter 40
Traffic Analyzer

In this chapter, you will learn how to:

Analyze Traffic by

- Category
- Event ID
- Custom Selection
- Keywords Analysis
Event Traffic Analysis

After EventTracker is deployed on numerous systems in a large Network it is very likely that you notice EventTracker receiving millions of events. Actually a majority of these events would be of little use to you. Using appropriate priority you can filter out unnecessary events to improve utility. ‘Filtering unnecessary events’ is a powerful feature based on priority configured by you.

Traffic Analyzer is a tool that is part of the EventTracker. It helps to find the details of the most common events and to set your order of priority. Accordingly create filters for non-essential events that are just increasing traffic but have little value.

Filtering is a continuous process. Priority may vary from one system to another. Over a period of time, with your experience, priority events can be separated from non-priority events in a specific system. Repeating this process every week enables you to receive only events of value in optimizing your operations. When non-priority events are filtered out EventTracker functions optimally.

This report provides total counts per system for each event id. Filter and display event count details based on user-defined criteria.

Usage: Analyze Windows specific security events, correlate events, broad searches per criteria with subsequent sorting and ordering of the result set.

To start Traffic Analyzer


   EventTracker displays the Traffic Analyzer.
View by Category

This option helps you analyze events based on Category.

1. Select the **View by Category** option, if not selected.
2. Select a Category from the **Category** drop-down list.
   
   Example: All Error Events.
3. Set the **Select Time Range** in From, To drop-down list.
4. Select the **All Systems** option to select all monitored systems.
   
   (OR)
   
   Select the **Specific Systems** option.
   
   Type the name of the systems separated by comma in the text box provided.
5. Click **Analyze**.
   
   Traffic Analyzer displays the report in the Notepad.
View by Event Id

This option helps you analyze hard coded Windows specific security events.

1. To analyze event traffic by event ID, Select the **View by Event Id** option.
Field | Description
--- | ---
Display all records: By default, this option is selected. All records will be displayed in the report in descending order.
Display only top: You can select this option if you want only a specified number of records to be displayed in the report.
Select Event Id: You can select 5 hard coded Windows security events for event traffic analysis.

<table>
<thead>
<tr>
<th>Event Id</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>540 Successful Network Logon</td>
<td>Selecting this id will generate 2 reports sorted by Username and IP address.</td>
</tr>
<tr>
<td>672 Authentication Ticket Granted</td>
<td>Selecting this id will generate 2 reports sorted by Username and IP address.</td>
</tr>
<tr>
<td>673 Service Ticket Granted</td>
<td>Selecting this id will generate 1 report sorted by IP Address.</td>
</tr>
<tr>
<td>675 Pre-authentication failed</td>
<td>Selecting this id will generate 2 reports sorted by Username and IP address.</td>
</tr>
<tr>
<td>680 Logon attempt</td>
<td>Selecting this id will generate 2 reports sorted by Username and Computer.</td>
</tr>
</tbody>
</table>

2. Type / select appropriate data in the relevant fields.
3. Select the **All Systems** option to select all monitored systems.

   (OR)

   Select the **Specific Systems** option.

   Type the name of the systems separated by comma in the text box provided.

4. Click **Analyze**.

   Traffic Analyzer displays the report in the Notepad.

   If you wish to display only a specified number of records in the report, type the number of records in the **Display only top** field or click the spin box.

### View by Custom Selection

This option helps you customize the selection criteria.

1. Select the **View by Custom Selection** option.

![Traffic Analyzer](image)

   **Figure 536**

2. Type appropriately in the relevant fields.
3. Select the **All Systems** option to select all monitored systems.
   
   (OR)

   Select the **Specific Systems** option.

   Type the name of the systems separated by comma in the text box provided.

4. Click **Analyze**.

   Traffic Analyzer displays the report in the Notepad.

---

**Keyword Analysis**

This option helps to analyze traffic by keywords.

1. Select the **Keywords Analysis** option.

---

Field | Description
--- | ---
Keywords Analysis: Helps to analyze events by keywords.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keywords Analysis: Helps to analyze events by keywords.</td>
<td></td>
</tr>
<tr>
<td>Contains All</td>
<td>Analyze logs that contain all keywords.</td>
</tr>
<tr>
<td>Contains Specific words</td>
<td>Analyze logs that contain specific keywords.</td>
</tr>
<tr>
<td>Excluding following words</td>
<td>Select this checkbox to exclude commonly occurring words.</td>
</tr>
</tbody>
</table>

2 Type appropriately in the relevant fields.

3 Select the **All Systems** option to select all monitored systems.
   (OR)
   Select the **Specific Systems** option.
   Type the name of the systems separated by comma in the text box provided.

4 Click **Analyze**.
EventTracker displays the report in the Notepad.

**Add Keywords for Analysis**
This option helps to add keywords.

1 Select the **Specific words** option.
   Traffic Analyzer enables the **Add**, **Edit**, and **Remove** buttons.

2 Click **Add**.
   Traffic Analyzer displays the Traffic Analyzer dialog box.

   ![Traffic Analyzer](image)

3 Type the keyword in the text box provided.
   Example: ETAdmin

4 Click **OK**.
   Traffic Analyzer adds the keyword to the list of keywords.

5 To analyze logs that contain a specific keyword, select a keyword from the list and then click **Analyze**.
Add Commonly Occurring Words to Exclude from Analysis

This option helps to add most commonly occurring words to exclude from analysis.

1. Select the **Exclude following words** option.
   Traffic Analyzer displays the list of commonly occurring words, enables Add, Edit, and Remote buttons.

2. Click Add.
   Traffic Analyzer displays the Traffic Analyzer dialog box.
3 Type the keyword in the text box provided.

4 Click OK.

Traffic Analyzer adds the new keyword to the list for exclusion.
Chapter 41
Agent Management Tool

In this chapter, you will learn how to:

- Access Agent Management Tool
- Query Agent Service
- Restart Agent Service
- Query Agent Version
- Remove Agent Component
- Delete Systems from Agent Service
Windows Agent Management Tool

Agent Management Tool is a diagnostic tool to check the health status of remote agents, restart the failed agent services and to check the version of remote agents. You ought to have Domain Admin privilege to use this utility.

Access Agent Management Tool


   EventTracker displays the Agent Management Tool.

![Agent Management Tool](image)

Figure 541

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>Works on a selected system which is managed with EventTracker Agent</td>
</tr>
<tr>
<td>Group</td>
<td>Works on all EventTracker managed systems belonging to selected Group/Domain</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>All</td>
<td>Works on all EventTracker managed systems</td>
</tr>
<tr>
<td>Custom</td>
<td>Works on systems which are listed in a plain text file</td>
</tr>
</tbody>
</table>

**Query Agent Service Status – System/Group/All/Custom**

This option enables you to query agent service status in the selected system/group/all/specified systems.

1. Select the relevant **Mode** option.
2. Select the system from the **System Name** drop-down list.
3. Select the **Query for Agent service status** option, if not selected.
4. Select the **Output Format** option i.e. **Text or CSV**.
5. Select or deselect **Run in background** option as per the requirement.
6. Click **Next >**.
   
   EventTracker displays the Enter Privileged account information dialog box.

   ![Enter privileged account information](image)

   **Figure 542**

7. Enter valid credentials, and then click **Execute**.
   
   EventTracker displays the EventTracker Management Tool message box.

   ![EventTracker Management Tool](image)

   **Figure 543**
8 Click OK.

EventTracker displays the result in the Notepad.

![Figure 544](image)

**NOTE**

Similarly you can select and manage EventTracker Agent in a Group, All, Custom.

**Restart Agent Service – System / All / Group / Custom**

This option enables you to restart the agent service in the selected system/all/group/specified systems.

1. To restart the agent service, select the relevant **Mode** option.
2. Select the system from the **System Name** drop-down list.
3. Select the **Restart Agent service** option.
4. Click **Next**.

EventTracker displays the Enter privileged account information dialog box.

5. Type valid username and password. Click **Execute**.

EventTracker displays the EventTracker Agent Management Tool message box.
6 Click **OK**.  
EventTracker displays the result in the Notepad.

![Figure 546](image)

---

Query Version of the Agent Service – System / Group / All / Custom

This option enables you to query the version of the agent service in the selected system / group / all / specified systems.

1 To query the version of the agent service in the selected system, select the relevant **Mode** option.
2 Select the system from the **System Name** drop-down list.
3 Select the **Query for Agent version** option.
4 Click **Next >**. 
EventTracker displays the **Enter privileged account information** dialog box.

5 Enter valid username and password. Click **Execute**. 
EventTracker displays the EventTracker Agent Management Tool message box.
6  Click **OK**.

EventTracker displays the result in the Notepad.

![Version Report in Notepad](image)

**Figure 550**

**Remove the Agent Component - System / Group / All / Custom**

This option enables you to remove the agent components for system/group/all/custom.

1. To remove agent components, select the relevant **Mode** option.
2. Select the **Remove Agent Component** option.
EventTracker displays **EventTracker Agent Management Tool** window.

**Figure 551**

**Figure 552**
3. Click **OK**.
   The selected system(s) from the drop down will be removed.

**Delete Systems from the agent service - System / Group / All / Custom**

This option enables you delete the version of the agent service for the selected system(s).

1. To delete systems, select the relevant **Mode** option.

   ![EventTracker Agent Management Tool](image)

   **Figure 553**

2. Select **Delete systems** and click **Next >**.
   EventTracker displays **EventTracker Management Tool** window.
3 Click **OK**
   The selected system(s) will be deleted.
Chapter 42
SCAP Profile Editor

In this chapter, you will learn how to:

- SCAP Profile Benchmark Editor
SCAP Benchmark Profile Editor

This option helps you to tailor/edit the predefined SCAP benchmark profile. You can save the updated benchmark profile as a new profile with different name.

1. Double-click **SCAP Profile Editor** on the **EventTracker Control Panel**. EventTracker displays SCAP Benchmark profile editor pop-up window.

![SCAP Benchmark Profile Editor](image)

2. In the **Select benchmark** dropdown, select an installed benchmark you wish to edit.

3. Select the type of profile element from **Select profile element type** dropdown.

<table>
<thead>
<tr>
<th>Profile element type</th>
<th>Used to</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Select/unselect a rule from a profile.</td>
</tr>
<tr>
<td></td>
<td>To edit the elements in Idref column, double click on element or right click on</td>
</tr>
</tbody>
</table>

Figure 555
### Select

Select an element, and then select **Edit**.

EventTracker displays a message.

<table>
<thead>
<tr>
<th>EventTracker - SCAP Benchmark Profile Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Please use the checkbox to enable/disable selectors.</td>
</tr>
<tr>
<td><img src="image" alt="EventTracker - SCAP Benchmark Profile Editor" /></td>
</tr>
</tbody>
</table>

### Set-value

Override the default value for a rule in the profile, without changing any of its other properties.

### Refine-value

Select from a list of value, value for a rule in the profile. To edit the refine value:

- Double click on element in Idref column or right click on element, and then select **Edit**.

EventTracker displays “Refine value element properties” pop up.

<table>
<thead>
<tr>
<th>'refine-value' element properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idref: Scripted_Window_Security_Restrictions1392check15_val</td>
</tr>
<tr>
<td>Title: Scripted_Window_Security_Restrictions</td>
</tr>
<tr>
<td>Description:</td>
</tr>
<tr>
<td>No Comment:</td>
</tr>
<tr>
<td>Operator:</td>
</tr>
<tr>
<td>Selector: Office2010 EC-Computer</td>
</tr>
</tbody>
</table>

Select the appropriate option in **Selector** dropdown.

### Refine-rule

Override the default properties (severity, weight, role etc) of a rule in the profile. This profile element

4. Select or clear the appropriate element checkbox, and then click **Save** to save the changes in existing benchmark list.

EventTracker displays the confirmation message.
(OR)

Click **Save As** to create a custom benchmark, which will be saved as XML file.

![Figure 557](image)

Click **Ok**.

EventTracker displays the confirmation message.

![Figure 558](image)

Click **Ok**.

The newly created benchmark can be seen in the **Select benchmark** dropdown.

**NOTE**

For more information on SCAP, refer [Access Configuration via SCAP](#).
Chapter 43
TrapTracker

In this chapter, you will learn how to:

- About Trap Tracker
- Trap Tracker Components
About TrapTracker

TrapTracker for Windows [TTW] is a scalable, standard-compliant framework that receives traps propagated by SNMP compliant devices in your enterprise. TTW provides options to categorize traps, generate custom reports and configure notifications on occurrence of a specific trap.

TrapTracker for Windows helps the user to:

- Monitor, consolidate, and analyze the traps sent by SNMP compliant devices
- Parse the MIB (based on ASN-1 format) files.
- Retrieve object and trap definitions from MIB file. This implies that MIB modules describing the traps are compiled to facilitate the translation of SNMP PDUs into user understandable format. Traps that cannot be translated should not be discarded, but should be displayed and stored in raw format.
- View the contents of MIB files in a format easily understood by the user.
- Compile and store multiple MIBs in a single file.
- Collect and consolidate Trap details, Category details and Alert details in the database.
- Configure real-time notification by E-mail, pager, beep, and custom action.
- Audit requirements suggested by GLBA, HIPAA, Sarbanes-Oxley Changing Client Service Account, California Senate Bill 1386, the USA Patriot Act and NISPOM.

TrapTracker Components

TTW version 4.x has the following components:

- A background process that receives and processes generic SNMP v1 and v2 traps; propagated by SNMP compliant devices.
- Feature-rich GUI application to categorize traps, filter traps for customized views, configure Alerts, upgrade license etc.
- A MibCompiler.

For detail information refer Trap Tracker Online Web Help
Chapter 44
Change Audit

In this chapter, you will learn how to:

- Results Summary Console
- Change Policy Dashboard
- Configuration Policy Dashboard
EventTracker Inventory Manager

EventTracker Inventory is an automated asset management tool, which scans all Change Audit, managed computers, and displays them in an easy accessible web and legacy interface.

Software inventory: To track and audit software installed on Change Audit managed computers.

For detail information regarding this chapter, please refer Change Audit.

Change Audit Results Summary Console

The Change Audit Results Summary Console consists of Change Policy Dashboard and Configuration Policy Dashboard.

1. Click the Change Browser button.
   
   EventTracker – Change Browser window displays.
For detail information regarding this chapter, please refer Change Audit.

Change Policy Dashboard

This dashboard gives the same view as in Change Audit menu -> Last Changes in EventTracker.

Please refer Change Audit for detail information.

Configuration Policy Dashboard

This policy dashboard provides information about the policy name, description and if there is any integrity violation.

If you have configured any Scheduled Policies in Change Audit menu -> Change Policies, the detail information is provided here.

1. Click the Analyze button.

   For detail information regarding this, please refer Change Audit.
Chapter 45
About EventTracker

In this chapter, you will learn about:

- EventTracker and License Information
About EventTracker

It provides you up-to-date information regarding the EventTracker application including version number, build. License information includes date of installation, date of expiry, support expiry information etc.

Figure 561

1. Click **Update Info** to view any updates/patches has been installed.

Figure 562

2. Click **System Info** to view system information.
In this chapter, you will learn about SCAP in detail.
SCAP

The Security Content Automation Protocol (SCAP) is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation (e.g., FDCC and FISMA compliance). The National Vulnerability Database (NVD) is the U.S. government content repository for SCAP. The Security Content Automation Protocol (SCAP), pronounced “S-Cap”, combines a number of open standards that are used to enumerate software flaws and configuration issues related to security. They measure systems to find vulnerabilities and offer methods to score those findings in order to evaluate the possible impact. It is a method for using those open standards for automated vulnerability management, measurement, and policy compliance evaluation. SCAP has two major elements. First, it is a protocol—a suite of six open specifications that standardize the format and nomenclature by which security software communicates information about software flaws and security configurations. Each specification is also known as a SCAP component. Second, SCAP includes software flaw and security configuration standardized reference data, also known as SCAP content. SCAP has several uses, including automating checks for known vulnerabilities, automating the verification of security configuration settings, and generating reports that link low-level settings to high-level requirements. SCAP defines how the following standards (referred to as SCAP ‘Components’) are combined:

**SCAP Components**

- Common Configuration Enumeration (CCE) - [http://cce.mitre.org/](http://cce.mitre.org/)
- Common Platform Enumeration (CPE) - [http://cpe.mitre.org/](http://cpe.mitre.org/)
- Extensible Configuration Checklist Description Format (XCCDF)
- Open Vulnerability and Assessment Language (OVAL)

The SCAP version allows the versions of the SCAP components to be referred to collectively.

**SCAP 1.0 includes:**

- XCCDF 1.1.4
- OVAL 5.3 and OVAL 5.4
- CCE 5.0
- CPE 2.2
- CVE
- CVSS 2.0

These open standards were created and are maintained by a number of different institutions including the MITRE Corporation, the NSA, and a special interest group within the Forum of Incident Response and Security Teams (FIRST). NIST recommends the use of SCAP for security automation and policy compliance activities. One of the primary goals of the SCAP is to encourage the development of checklists in XML formats, particularly checklists that are compliant with XCCDF and/or OVAL.

SCAP content

SCAP content or SCAP data stream consists of security checklist data represented in automated XML formats, vulnerability and product name related enumerations, and mappings between the enumerations. The SCAP security checklist data is configuration checklists written in machine-readable languages (XCCDF). SCAP checklists have been submitted to, and accepted by, the NIST National Checklist Program. They also conform to a SCAP template and style guide to ensure compatibility with SCAP products and services. The SCAP template and style guide talks about requirements for including SCAP enumerations and mappings within the checklist. SCAP checklists refer to SCAP test procedures (low level checks of machine state written in OVAL). SCAP test procedures are used in conjunction with SCAP checklists (http://nvd.nist.gov/ncp.cfm?scap).

SCAP content is a collection of four or more related XML files containing SCAP data using the SCAP components that provide the data necessary to evaluate systems for compliance with a configuration-based security policy. Patch checking content may also be included in this bundle. Files included for SCAP 1.0 are listed below, with the ‘XXXX” in each name representing a unique prefix for the bundle (e.g., fdcc-xp, fdcc-vista):

- XXXX-xccdf.xml - XCCDF 1.1.4 content
- XXXX-cpe-oval.xml - CPE OVAL 5.3 definitions
- XXXX-cpe-dictionary.xml - Minimal CPE 2.2 dictionary
- XXXX-oval.xml - OVAL 5.3 compliance definitions

SCAP implementation in EventTracker

EventTracker supports the following SCAP capabilities:

- Federal Desktop Core Configuration (FDCC) Scanner
- Authenticated Configuration Scanner
- Authenticated Vulnerability and Patch Scanner

EventTracker implements the SCAP 1.0 standard by implementing

- Common Vulnerability Enumeration (CVE)
- Common Configuration Enumeration (CCE)
- Common Platform Enumeration (CPE)
- Extensible Configuration Checklist Documentation Format (XCCDF)
- Open Vulnerability Assessment Language (OVAL) [EventTracker uses MITRE's reference implementation of OVAL]

EventTracker contains in-built SCAP content for FDCC and other benchmarks. EventTracker also allows the user to validate and import the latest SCAP content for the in-build benchmarks. EventTracker provides a Web interface that can be used to schedule the assessment or perform on demand assessment against the systems that have EventTracker agent installed on them. EventTracker user interface contains references to CCE entries for each of the rule results. Where applicable, the results also contain OVAL reference, CVE references, and CPE references. Each target system is assessed using CPE dictionary and has its operating system identified with a CPE reference. All CVE references have an external link to NVD.
Appendix – HIPAA

HIPAA Compliance Reports

The Health Insurance Portability And Accountability (HIPAA) regulation impacts those in healthcare that exchange patient information electronically. HIPAA regulations were established to protect the integrity and security of health information, including protecting against unauthorized use of disclosure of the information.

As part of the requirements, HIPAA states that a security management process must exist in order to protect against “attempted or successful unauthorized access, use, disclosure, modification or modification with system operations.” The organization must be able to monitor, report and alert on attempted or successful access to systems and application that contain sensitive patient information.

EventTracker provides the following reports to help comply with the HIPAA regulations:

User Logon report

HIPAA requirements (164.308 (a)(5) – log-in/log-out monitoring) states that user accesses to the system be recorded and monitored for possible abuse.

User Logoff report

HIPAA requirements clearly states that user accesses to the system be recorded and monitored for possible abuse. Remember, this intent is not just to catch hackers but also to document the accesses to medical details by legitimate users. In most cases, the very fact that the access is recorded is deterrent enough for malicious activity, much like the presence of a surveillance camera in a parking lot.

Logon Failure report

The security logon feature includes logging all unsuccessful login attempts. The user name, date and time are included in this report.

Audit Logs access report

HIPAA requirements (164.308 (a)(3) – review and audit access logs) calls for procedures to regularly review records of information system activity such as audit logs.
Appendix – SOX

Sarbanes – Oxley Compliance Reports

Section 404 of the Sarbanes – Oxley (SOX) act describes specific regulations requires for publicly traded companies to document the management’s “Assessment of Internal Controls” over security processes.

The standard requires that a security management process must exist in order to protect against attempted or successful unauthorized access, use, disclosure, modification or interference with system operations. In other words, being able to monitor, report and alert on attempted or successful access to systems and applications that contain sensitive financial information.

EventTracker provides the following reports to help comply with the SOX regulations:

User Logoff report
SOX requirements (Sec 302 (a)(4)(C) and (D) states that user accesses to the system be recorded and monitored for possible abuse.

User Logon report
SOX requirements (Sec 302 (a)(4)(C) and (D) states that user accesses to the system be recorded and monitored for possible abuse.

Logon Failure report
The security logon failure includes logging all unsuccessful login attempts. The user name, date and time are included in this report.

Audit Logs access report
SOX requirements (Sec (a)(4)(C) and (D) – review and audit access logs) calls for procedures to regularly review records of information system activity such as audit logs.

Security Log Archiving Utility
Periodically, the system administrator will be able to back up encrypted copies of the log data and restart the logs.
Track Account management changes
Significant changes in the internal controls sec 302 (a)(6). Changes in the security configuration settings such as adding or removing a user account to an administrative group. These changes can be tracked by analyzing event logs.

Track Audit policy changes
Comply with internal controls sec 302 (a)(5) by tracking the event logs for any changes in the security audit policy.

Track individual user actions
Comply with internal controls sec 302 (a)(5) by auditing user activity.

Track application access
Comply with internal controls sec 302 (a)(5) by tracking applications process.

Track directory / file access
Comply with internal controls sec 302 (a)(5) for any access violation.
Appendix – GLBA

GLBA Compliance Reports

Section 501 of the GLBA documents specific regulations require for financial institutions to protect ‘non-public personal information.’

As part of the GLBA requirements, it is necessary that a security management process exist in order to protect against attempted or successful unauthorized address, use, disclosure, modification or interference of customer records. The organization must be able to monitor, report and alert on attempted or successful access to systems and applications that contain sensitive customer information.

User Logon report

GLBA Compliance requirements state that user accesses to the system be recorded and monitored for possible abuse.

User Logoff report

GLBA requirements state that user accesses to the system be recorded and monitored for possible abuse.

Logon Failure report

The security logon feature includes logging all unsuccessful login attempts. The user name, date and time are included in this report.

Audit Logs access report

GLBA requirements (review and audit access logs) call for procedures to regularly review records of information system activity such as audit logs.
Appendix – Security Reports

Security Reports

Successful and failed file access
Auditors are generally concerned with knowing who did what, and when. Monitoring file access can provide that information. This will be especially useful as companies attempt to comply with internal policies and industry regulations.

Successful logons preceded by failed logons
Multiple failed logins, followed by a successful login could indicate a successful breach by a hacker.

Audit log cleared events by user
A successful hacker will attempt to remove any trace of their attack. Their attempts to clear the audit logs are captured and can be displayed with this report.

Invalid logons by date
Allows you to identify days of heavy invalid logins. Many invalid logins over a weekend could indicate an attempt to penetrate the network.

Daily reboot statistics
Daily reboot statistics can help system administrators identify systems that might be having problems.

CPU load peaks by computers
CPU load peaks can indicate a system that is either configured incorrectly or one that is simply overworked. This can allow the system administrator to identify the system having problems and either fix the issues or transfer some of the workload (or justify new hardware).
Account usage outside of normal hours

This report can identify those accounts that are being used outside of normal (definable) hours of operations. Users occasionally work late, but frequent account usage after hours can indicate a security breach.

Audit policy history

Tracking audit policy on enterprise systems is a key function for security auditors. The ‘Audit Policy History’ report will show each systems audit policy for each date it was collected. This way compliance to the audit policy is documented and can be tracked.

Accounts that were never logged on

Part of an administrator’s job is to deal with the clutter that collects in the NT4 SAM or Active Directory – or perhaps better stated, preventing it entirely. One of the more common sources of this clutter is redundant user accounts. In an effort to provide efficient service, those tasked with account creation often create new user accounts ahead of time for new employees or contractors. That way, when the new employee or contractor arrives, they can login and start to work immediately. In some organizations, this may mean dozens of accounts. Inevitable, job offers are declined or contractors’ start dates postponed. The result is accounts that exist but have never been used. These accounts potentially represent a security risk because

1. They usually have a well-known default password set and
2. They may already have been placed in security groups pertaining to their job function.

An unscrupulous individual could login as the new account, set password to one of their own choosing and gain access to sensitive data by way of the accounts’ group memberships. The ‘Accounts that were never logged on” report can highlight these risky redundant accounts. Armed with this information follow-up e-mails can then sent to the appropriate managers to determine what has transpired with the individuals for whom these accounts were created – i.e. did they really start work yet or not. Once the status of the employees is known, these accounts may then be disabled or deleted as required.

Administrative Access to Computers

Administrative access is required to perform many common tasks on workstations and servers. Such tasks include stopping and starting services, installing software and creating local groups for data permission. Care needs to be taken in the assignment of local administrative rights as clearly, an account with this right has a quite ranging ability to modify applications on SQL or IIS for example inappropriately assigned administrative access could lead to outages of business line applications.

On the other side of this equation are enterprising power users who will sometimes go out of their way to block administrators’ legitimate access to their machines. These situations cause innumerable problems when it comes time to do remote managements, hardware and software inventory, software rollouts and even access control list updating. In either case, administrators need to get a sense of who has local administrative authority on workstations and servers in their environment. The ‘Administrator Access by Computer” report can quickly provide this invaluable information.
File Access by User

Ensuring that appropriate permission is set on sensitive data is one side of the data security coin. The other is the process of auditing who is using the permissioned resources and when. There are times when it is important to know who the last person was to use their authorized access a resource. It is just as important to know if someone is trying to access a resource that he or she does not have access to.

Take the example of a spreadsheet containing salary information. “Mary Hart” works in human resources and is authorized to access this information. Each time she accesses the file, if auditing is enabled, this access will be recorded to Windows’ Event Logs as successful access. On the other hand, “George hogan” is an employee in the mailroom, with some time on his hands. He spends this time browsing the network. Since he is part of the company’s Administration Department, he has visibility of the department’s shared files. He may be able to see a folder called “Payroll Info” – when he tries to access this folder, however, he will receive the message “Access Denied.” The fact that he unsuccessfully tried to access this folder will also be recorded to the Event Logs as a ‘failed file access.’

The event log information described about is another distributed data source. Each files server maintains its own store of information on who accessed what file on that server and when. The challenge is to consolidate this information into one location and extract the most relevant transactions.

Hot fixes by Computer

Microsoft releases hot fixes on an almost weekly basis to remedy critical technical and security problems with the operating system. Clearly, these problems are considered serious enough that they might significantly disrupt a customer’s business if not repaired. This puts pressure on administrators to keep close track of which hot fixes are installed on servers and workstations – an essential but potentially time-consuming task. Being able to poll computers on a scheduled (e.g. weekly) basis to verify which hot fixes they have installed means having on fewer balls to juggle.

Reporter’s Hot Fixes by Computer report obviates the need to use a second tool to the collected hot fix information. The report interrogates the Registry of each workstation and server on the network to determine which hot fixes are installed. Like all of Reporter’s reports, this process can be scheduled at whatever interval the administrator deems appropriate. This way, the hot fixes check becomes part of the administrator’s standard list of scheduled audit reports. Frequent collection ensures that the most current information is always at hand.

Last logon by Domain Controller

As previously noted, identifying redundant user accounts is an important step towards achieving a secure network. We previously discussed the use of the “user never logged on report” to highlight accounts that were created but have never been used. Another more frequent and common scenario is an employee or contractor leaves the organizations but IT is not notified. Though policies may be in place that stipulate that the accounts of departed staff are to be disabled and eventually deleted – if IT doesn’t know that someone had left they really have no way of knowing which accounts need to disabled on a given day.

One indication of whether an account is being used or not is the ‘last logon time.” Each time a user enters their username and password (either at logon time or as part of unlocking their workstation), a logon transaction is recorded and the time of that transaction is stamped on to that user’s account. For the most part, if an account’s last logon time is more than 2 to 3 weeks in the past (this takes into
account possible employee vacations, training courses or travel), this is a good indication that the employee is not working with the company.

Reporter’s ‘Last Logon by Domain Controller” report is an authoritative source of users’ last logon times. The report polls all domain controllers (DCs) for the last logon seen by that DC for each user and then calculates the most recent time for insertion into the report. As part of a regular security audit process, this report could be scheduled to run on at least a weekly basis. Armed with this report, follow-up e-mails can then be sent to the appropriate managers to determine what has transpired with the employees whose accounts appear in the report – i.e. have these staff left the company or are they on some extended leave. Once the status of the employee is known, these accounts may then be disabled or deleted as required.

User Account Locked Out

User account lockouts occur when a user incorrectly enters password several times in succession. In most organizations, a user who enters their password incorrectly three times will have their account locked out (i.e. be barred from accessing the network) for some defined time period (e.g. 15minutes) or possibly, indefinitely.

Frequent user account lockouts can result from clumsy or forgetful users but they may also be an indication of some trying to gain unauthorized access to the network using their own or someone else’s account. Like file and resource access, account lockouts are recorded in Windows’ Event logs of each server that authenticates user access. Once again, the challenge is to pull this information together.

Reporter’s User Account Locked Out report extracts lock out events from all the data collected from servers across the company effectively mining out the transactions that might indicate suspicious activity. As part of the regular audit process, it would be advisable to schedule the execution of this report in the early morning hours just prior to start of business (e.g. at 6 a.m.).

This would highlight to the administrator or security officer all accounts that were locked during the overnight period. Careful review of the report could help to determine if sleepy users caused the lockouts or someone trying hack into the network at night. Another business use of this information can be to provide some insight into Help Desk call volumes. If, on a given day, there was a large increase in calls to the Help Desk, a quick perusal of the account lockout report might provide at least part of the explanation for the increase.
In the financial services industry, nothing is more than the trust of customers, shareholders, partners and regulators. The risk management officer’s primary task is to ensure trust is sustained through a systematic risk management program.

BASEL II defines operational risk, one of the pillars of the Accord, as “the risk of direct or indirect loss resulting from the inadequate or failed internal process or systems or from external events.”

If your company eventually intends to adopt the Advanced Measurement Approach (AMA), then you are required to measure aspects of operational risk, such as IT security.

It involves two steps. First, ensure that appropriate permission is set on sensitive data. Secondly, during the auditing process the user needs to have permission on the resources accessed at a particular point in time. There are times when it is important to know who was the last authorized person who had access to the resource. It is just as important to know if someone is trying to access a resource that he or she does....
Appendix – FISMA

FISMA

FISMA requires detailed annual E-Government security reports of all federal agencies. As to fulfill FISMA requirements, the agencies should implement the FISMA requirements and transmit the corresponding reports to Office of Management and Budget (OMB) by October of each year. According to the sections FISMA Sec. 3505 and FISMA Sec. 3544, the transmitted reports should summarize the following requirements to comply with FISMA.

FISMA Sec. 3505

Sec.3505.(c)(1) - Maintenance and results of major federal information systems or applications inventory security of the agency.

Sec.3505.(c)(2) - Inventory of networks interfaces not only within the agency, but also the network of other agencies or contractors working under the agency.

FISMA Sec. 3544

Sec.3544.(a)(1)(A)(i) - Information security protection against unauthorized access, use, disclosure, disruption, modification or destruction of information and information systems of the agency.

Sec.3544.(a)(1)(A)(ii) - Information security against unauthorized usage risks of the contractor or other organizations working on behalf of the agency.

Sec.3544.(a)(1)(A)(ii) - The responsibility of the head while the major federal systems operated either by the agency or by the contractor and other agencies under the agency.

Sec.3544. (b) - Integrity, authenticity, availability of the systems supporting the agency operations and assets.

Sec.3544. (b)(2)(C) - Detailed reporting on the existing risks and remedial actions. Effectiveness of Information Assurance program and progress in remedial plans and actions.

Sec.3544. (b)(2)(D) – Periodical risk management reporting. Accurate report on the current FISMA compliance status. Annual information on security training and Internet security training for the agency personnel and also the contractor.
PCI DSS stands for Payment Card Industry Data Security Standard. It was developed by the major credit card companies as a guideline to help organizations that process card payments prevent credit card fraud, hacking and various other security issues. A company processing card payments must be PCI compliant or they risk losing the ability to process credit card payments.

**Requirement 1:** Install and maintain a firewall configuration to protect cardholder data

**Requirement 2:** Do not use vendor-supplied defaults for system passwords and other security parameters

**Requirement 3:** Protect stored cardholder data

**Requirement 4:** Encrypt transmission of cardholder data across open, public networks

**Requirement 5:** Use and regularly update anti-virus software

**Requirement 6:** Develop and maintain secure systems and applications

**Requirement 7:** Restrict access to cardholder data by business need-to-know

**Requirement 8:** Assign a unique ID to each person with computer access

**Requirement 9:** Restrict physical access to cardholder data

**Requirement 10:** Track and monitor all access to network resources and cardholder data

**Requirement 11:** Regularly test security systems and processes

**Requirement 12:** Maintain a policy that addresses information security
## Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Configuration</td>
<td>Process of configuring the system for reporting to multiple managers, to filter events, to monitor services, software installations, processes, system health, and to archive the events database.</td>
</tr>
<tr>
<td>Alert Configuration</td>
<td>Process of configuring alert notifications in the form of Sound, E-mail, Console message or any Custom action.</td>
</tr>
<tr>
<td>Alerts</td>
<td>A feature that instructs programs that notify timely information about the events.</td>
</tr>
<tr>
<td>Analyzing Event Traffic</td>
<td>The process to analyze the event traffic patterns. The data can be used to filter out irrelevant events and perform other operation tasks.</td>
</tr>
<tr>
<td>Audible Alert</td>
<td>A feature that instructs programs that usually notifies information by sound.</td>
</tr>
<tr>
<td>Auto Discover Mode</td>
<td>Process of adding computers from your network automatically.</td>
</tr>
<tr>
<td>Change Audit</td>
<td>An application that used to track the occurred changes on a computer’s file system and registry and provides you with a lifeline to restore it back to a working configuration.</td>
</tr>
<tr>
<td>Change Management</td>
<td>The process that enables the user to monitor, analyze, understand, and recover from change.</td>
</tr>
<tr>
<td>Console Message Alert</td>
<td>A feature that instructs programs that usually notifies information to the selected machine.</td>
</tr>
<tr>
<td>CPU Performance</td>
<td>A term used to monitor the CPU performance.</td>
</tr>
<tr>
<td>CRL</td>
<td>A CRL is a list identifying revoked certificates, which is signed by a CA and made freely available at a public distribution point.</td>
</tr>
<tr>
<td>Custom Alert</td>
<td>A feature that instructs programs to execute custom action on receipt of an event.</td>
</tr>
<tr>
<td>Disk Space Usage</td>
<td>A term used to monitor the disk space usage.</td>
</tr>
<tr>
<td>E-mail Alert</td>
<td>A feature that instructs programs that usually notifies information by E-mail.</td>
</tr>
<tr>
<td>Event Filtering</td>
<td>Process of filtering the events that are not important. Monitoring unimportant events cause the database to occupy more disk space.</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Event Information</td>
<td>A window pane that displays the summary of event details in the EventTracker Management console.</td>
</tr>
<tr>
<td>Event Logs</td>
<td>A type of event message. The event logs are recorded whenever certain events occur, such as services starting and stopping, or users logging on and off and accessing resources.</td>
</tr>
<tr>
<td>Event Monitoring</td>
<td>A window pane that displays the real-time event information in the EventTracker Management console.</td>
</tr>
<tr>
<td>EventBox</td>
<td>An archived event data file. You can create an EventBox by using EventVault Warehouse Manager console.</td>
</tr>
<tr>
<td>EventTracker</td>
<td>An application that can be used to centrally monitor, analyze, and manage events being emitted by Windows 2000/2003/2008/2008 R2 /XP /Win 7 / Vista UNIX systems, and SNMP enabled devices.</td>
</tr>
<tr>
<td>EventVault</td>
<td>The console used to archive the events from EventTracker database. EventVault can operate in Automatic Archival and EventBox on demand methods.</td>
</tr>
<tr>
<td>Exclude List</td>
<td>The process to configure the network connections that need not to be monitored.</td>
</tr>
<tr>
<td>Filters</td>
<td>The process to filter out events that you do not want to monitor.</td>
</tr>
<tr>
<td>Include List</td>
<td>The process to configure the network connections to monitor. Include list Network connections always override the Exclude list Network connections.</td>
</tr>
<tr>
<td>IP Subnet</td>
<td>A 32-bit address used to identify a node on an IP internet. The address is typically represented with a decimal value of each octet separated by a period. For example: 192.168.7.27.</td>
</tr>
<tr>
<td>Knowledge Base</td>
<td>A Web site containing information about Windows events and custom EventTracker events.</td>
</tr>
<tr>
<td>Flex Report</td>
<td>Process of analyzing the event details by setting criteria such as date range, time range, rule, and computer.</td>
</tr>
<tr>
<td>Log Backup</td>
<td>A backup that copies event logs automatically in the EventTracker Agent directory whenever the event logs are full.</td>
</tr>
<tr>
<td>Logfiles</td>
<td>The process to monitor textual log files such as SQL or ISA logs, created by any vendor. You can also configure the strings to search. If any record matching the search string is found, an event will be generated.</td>
</tr>
<tr>
<td>Manager Configuration</td>
<td>It comprises of various options to configure Alert events, Keyword indexing, Syslog/virtual collection point, Direct Log Archiver / NetFlow Receiver, Agent File transfer settings, configuration assessment settings, SMTP server settings and StatusTracker settings.</td>
</tr>
<tr>
<td>Memory Usage</td>
<td>A term used to monitor the memory usage.</td>
</tr>
<tr>
<td>Monitor Syslog</td>
<td>The process to monitor Syslog being sent by an UNIX system.</td>
</tr>
<tr>
<td>NetFlow</td>
<td>A Cisco-proprietary IP statistics collection feature that collects information on IP flows passing through a router.</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Quick Statistics</td>
<td>The process to view the summary of event statistics such as Total events received, Total alerts received, Total systems monitored, and so on.</td>
</tr>
<tr>
<td>SNMP Event Manager</td>
<td>An application called TrapTracker used to monitor and manage critical traps emitted by network devices in your enterprise.</td>
</tr>
<tr>
<td>SNMP Traps</td>
<td>The process to receive trap messages generated by local or remote SNMP agents and forwards the messages to third party vendor software such as an NOC.</td>
</tr>
<tr>
<td>StatusTracker</td>
<td>An application used to monitor the status of your IT resources and provides you various reports.</td>
</tr>
<tr>
<td>Syslog Receiver</td>
<td>The process to set the SYSLOG receiver. After setting this option, the Manager will receive any SYSLOG being sent by an UNIX system.</td>
</tr>
<tr>
<td>System Information</td>
<td>The process to collect and view the system configuration information. You can view the information of System Summary, Hardware Resources, Components, Software Environment, Internet Settings, and Applications.</td>
</tr>
<tr>
<td>System Manager</td>
<td>A console helps you to manage groups, systems, and Agents.</td>
</tr>
<tr>
<td>System Performance</td>
<td>The process to monitor the system performance in graph, histogram, or report form.</td>
</tr>
<tr>
<td>System Statistics</td>
<td>A window that displays the system statistics in EventTracker Management console.</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol. TCP is responsible for verifying the correct delivery of data from Agent to server. TCP adds support to detect errors or lost data and to trigger transmission until the data is correctly and complete received.</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol. A connectionless protocol that, like TCP, runs on top IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network.</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>Vulnerabilities are weaknesses in process, administration, or technology that can be exploited to compromise your IT security.</td>
</tr>
<tr>
<td>Vulnerability Parsers</td>
<td>The parser reads the XML report generated by Vulnerability scanners and extracts vulnerability information from it.</td>
</tr>
<tr>
<td>Vulnerability Scanners</td>
<td>A vulnerability scanner is a computer program designed to assess computers, computer systems, networks, or applications for weaknesses.</td>
</tr>
</tbody>
</table>