Netsurion. | EventTracker®

EventTracker: User Guide

Version 9.3

Publication Date: May 9, 2022

Copyright

All intellectual property rights in this work belong to Netsurion. 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 Netsurion or used except as expressly authorized in writing by Netsurion.
Copyright © 2022 Netsurion. 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

Netsurion reserves the right to make changes to this manual and the equipment described herein without notice. Netsurion has made all reasonable efforts to ensure that the information in this manual is accurate and complete. However, Netsurion 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.

The information contained in this document represents the current view of Netsurion on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Netsurion MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Netsurion, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2022 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

About this Guide 20
Who should read this guide? 20
Typographical Conventions 20
Document Revision Control 24
How to get in touch 25
Documentation Support 25
Customer Support 25
Related Documents 25
What is new in EventTracker v9.3 26
What is new in EventTracker v9.3.1 26
What is new in EventTracker v9.3.2 27
What is new in EventTracker v9.3.3 27
What is new in EventTracker v9.3.4 27
What is new in EventTracker v9.2 27
1. Getting Started 29
1.1 About EventTracker 30
1.2 EventTracker Services and Ports 31
1.3 Starting EventTracker 33
1.4 Admin Menu 38
1.5 Tools Menu 41
1.6 EventTracker Control Panel 41
1.7 Profile Menu 44
1.7.1 Viewing Profile 44
1.7.2 Advanced Window 44
1.8 Help option 50
1.8.1 Licensing Details 50
1.8.2 User Guide Details 51
1.9 Keeping the Tear Away feature functioning forever without being logged out 51
1.10 Updating EventTracker Users List 54

1.10.1 Updating Users List 54

1.11 Exiting EventTracker 55

2. Dashboard 58

2.1 Overview of the Home Dashboard 59

2.2 Overview of My Dashboard 60

2.2.1 Creating a Dashboard 61

2.2.2 Configuring a Dashlet 61

2.2.3 Creating a Dashlet using CIM fields 64

2.2.4 Creating a Dashlet using SQL Database 65

2.2.5 Exporting Dashlets 68

2.2.6 Importing Dashlets 69

2.3 Attackers pane and Targets pane 69

2.3.1 Attackers pane 69

2.3.2 Targets pane 69

2.3.3 List of URLs for firewall proxy exclusion 72

2.4 Processes tab 82

2.4.1 List of URLs for firewall proxy exclusion in Processes 82

2.4.2 Unknown Process Filter 85

2.4.3 Digital Signature (Signed/Unsigned) 88

2.4.4 Log Search for a process 90

2.4.5 Searching using File Name/ MD5 Hash 91

2.4.6 Adding to Safe List/Unsafe List 93

2.4.7 Importing Process to Safe List/Unsafe List 94

2.5 Dormant tab 95

2.6 Unsafe processes 95

2.7 Incidents tab 96

2.7.1 Incidents Dashboard 96

2.7.2 Graphical View 101

2.7.3 Searching Incidents 103

2.7.4 Viewing incidents in Tabular View 107

2.7.5 Log Search feature 109
2.8 Knowledge Base option 110
2.9 Advanced Search 110
2.10 Tile Dashboard 113
2.10.1 Tiles Flip 118
2.11 Machine Learning 118
2.11.1 Monitor Machine Learning Dashlet 119
2.11.2 Adding Machine Learning Dashlets 120
2.11.3 Resetting Personalization 124
2.11.4 Volume Analysis option 125
2.11.5 Analyzing Windows Logon 127
2.11.6 Analyzing Windows Logon 127
2.11.7 Analyzing Windows Application 128
2.11.8 Analyzing EventID Activity 128
2.12 Analyze IP Address 129
2.12.1 Filter List 133
2.12.2 Analyzing Windows Network 135
2.12.3 Analyzing Windows Process 136
2.12.4 Analyzing Windows Runaway Process 138
2.12.5 Analyzing System 139
2.12.6 Analyzing Windows Interactive Logon Activity 140
2.12.7 Analyzing Windows User Location Affinity 141
2.13 Change Audit 142
2.13.1 About Change Audit 142
2.13.2 Change Audit Dashboard 142
2.13.3 Viewing Change Audit dashboard 142
2.14 Last Changes tab 147
2.14.1 Viewing statistical data of Change Type/Object Type 148
2.14.2 Viewing chart summary of Change Type/Object Type 148
2.15 Setting Dashboard Preferences 149

2.15.1 Authorizing the Unauthorized Changes 149

2.15.2 Viewing Access History 151

2.15.3 Viewing Additional Information on Files 152

2.16 Enabling OS Auditing on Folder(s) 152

2.17 Policy Dashboard tab 157

2.17.1 Customizing the Policies Dashboard 158

2.18 EventTracker Inventory Manager 160

2.19 Change Policies tab 161

2.19.1 Analyzing Policy Comparison Results 163

2.20 Scheduling Change Assessment 166

2.20.1 Editing Change Assessment Schedules 168

2.20.2 Running Schedules on Demand 168

2.20.3 Deleting Scheduled policies 169

2.21 Compliance Dashboard 169

2.21.1 Creating a Dashboard 171

3. Search 176

3.1 Searching Logs 177

3.1.1 Basic search 177

3.2 Searching from Elastic 179

3.2.1 Advanced Search 179

3.3 Three tabs - Elastic, Cache and Archives in Log search result window 181

3.3.1 Add Search to Dashboard/Casebook 184

3.4 Searching from Archives 186

3.4.1 Advanced Search 186

3.4.2 Adding Search Criteria 187

3.5 Smart Tokens 188

3.5.1 RegEx in Log Search 190

4. Reports 195

4.1 Reports Configuration 196

4.2 Security/Operations/Compliance/Flex Reports/Alphabetical Reports/Favorites 197

4.2.1 Security reports 197
4.2.2 Operations reports 197
4.2.3 Compliance reports 198
4.2.4 Flex reports 198
4.2.5 Favorites tab 198
4.3 Generating Alphabetical Reports 198
4.4 Reports Dashboard page 199
4.4.1 Top Level Summary tab 203
4.5 Generating on Demand Reports 207
4.6 Generating Queued Reports 214
4.7 Generating Scheduled Reports 215
4.7.1 Scheduled Reports - Run Now 221
4.8 Generating defined reports 223
4.9 Reports Wizard 227
4.10 Reporting Exceptions 227
4.11 Refine and Filter Options 228
4.12 Report Calendar 229
4.12.1 Viewing scheduled reports in time slot 230
4.12.2 Viewing scheduled reports on a day 231
4.13 Report Status 231
4.13.1 On Demand/Queued Status button 232
4.14 Favorites tab 233
4.14.1 Explorer 234
4.14.2 Perform search in EventVault Explorer 235
4.15 Flex report history 239
4.15.1 Configuring EventVault Explorer to use remote SQL Server 243
4.16 Collection Point 245
4.16.1 Configuring Reports to Collection Masters 245
4.17 Collection Master 249
4.17.1 Viewing the CP generated reports 249

5. Active Watch List ... 251
5.1 Active Watch List ... 252
5.1.1 Creating Active Watch List Groups ... 253
5.1.2 Editing Groups ... 256
5.2 Adding a new class ... 257
5.2.1 Editing an Existing Class ... 260
5.3 Adding a new pattern ... 261
5.4 Importing a list ... 263
5.4.1 Deleting a list/entity ... 265
5.4.2 Linking to group ... 266
5.4.3 Moving to Group ... 268
5.5 TAXII Server Configuration ... 269
6. Alerts ... 272
6.1 Alerts ... 273
6.2 Risk Metrics ... 273
6.2.1 Alert Email Template feature ... 274
6.2.2 Configuring Alerts with Active Watch List ... 274
6.3 Adding Custom Alerts ... 277
6.4 Copying of Alerts ... 286
6.5 Adding Pre-defined Categories as Alerts ... 288
6.6 Deleting Alerts ... 289
6.7 Configuring Alert Actions – Manager Side ... 289
6.7.1 Configuring E-mail Alert Action ... 289
6.7.2 Forwarding Events as SNMP Traps ... 290
6.7.3 Forwarding events as syslog messages ... 294
6.7.4 Executing Remedial Action at EventTracker Manager Console System ... 297
6.7.5 Executing Remedial Action at EventTracker Windows Agent System ... 297
6.7.6 Editing Alert Actions ... 299
7. Machine Learning Jobs ... 301
7.1 Manage Machine Learning Jobs ... 302
7.2 Adding Machine Learning Jobs ... 304

7.2.1 Adding custom Machine Learning Jobs in Machine Learning Dashboard 308

8. Machine Learning Settings 310

8.1 Machine Learning Settings 311

9. Casebook Configuration 313

9.1 Using Casebook Configuration................................ 314

10. Category................................ 315

10.1 Managing Category Groups................................ 316

10.1.1 Creating Category Groups 316

10.1.2 Modifying Category Groups 317

10.1.3 Deleting Category Groups 317

10.1.4 Modifying Category................................ 318

10.2 Cloning category................................ 319

10.2.1 Removing Category Groups................................ 320

10.3 Managing Categories................................ 321

10.3.1 Creating Categories 321

10.3.2 Modifying Categories 324

10.3.3 Removing Categories................................ 325

10.3.4 Deleting Event Rules................................ 325

10.4 Adding Categories as Alerts 326

10.5 Moving Category................................ 327

11. Collection Point and Collection Master................................ 330

11.1 Collection Point model 331

11.1.1 Scalability................................ 331

11.2 Real world scenarios 331

11.3 Viewing Collection Point Configuration 333

11.4 Adding Collection Masters 335

11.5 Editing Collection Master Settings in Collection Point................................ 337

11.6 Deleting Collection Master Settings................................ 338

11.7 Managing Archives................................ 338

11.8 Resending CAB Files 339

11.9 Collection Master 339

11.10 Viewing and Editing Collection Point Details in Collection Master ... 341

11.11 Configuring Collection Master listening port ... 344

11.12 Deleting CAB Files ... 345

11.13 Deleting Collection Point Details ... 345

12. Admin Diagnostics ... 346

12.1 Diagnostics ... 347

13. Event Filters ... 350

13.1 Filtering Events from View ... 351

13.2 Event Filter (Global/Receiver/Archiver filter) ... 351

13.2.1 Understanding Filters and Filter Exceptions ... 356

13.3 Viewing and Editing Alert Details ... 357

14. EventVault ... 359

14.1 EventVault Manager ... 360

14.1.1 Starting EventVault Manager ... 360

14.2 Verifying Archive File(s) ... 361

14.3 Exporting Archive File(s) ... 362

14.4 Configuring EventVault Manager ... 363

15. FAQ Tile Configuration ... 365

15.1 Configuring FAQ Tiles ... 366

15.1.1 Permalink ... 369

16. Group Management ... 372

16.1 Group Management ... 373

17. IP Lookup Configuration ... 376

17.1 IP lookup Configuration ... 377

17.1.1 Adding IP Lookup ... 377

18. Knowledge objects ... 378

18.1 Knowledge Objects and Interesting tokens ... 379

18.2 Group Knowledge Objects ... 380

18.2.1 Adding Knowledge Objects to a Group ... 382

18.2.2 Searching Objects ... 384

18.3 Exporting Object ... 384

18.4 Importing Objects ... 386
18.5 Editing Knowledge Objects ... 387
18.6 Adding Rule to existing Knowledge Objects ... 388
18.7 Deleting Knowledge Objects ... 392
18.7.1 Example to create Knowledge Object ... 393
18.8 Conditional Tag Configuration for Knowledge Objects Search ... 396
19. Manager ... 400
19.1 Configuring - Alert Events ... 401
19.1.1 Enabling Alert Notification ... 401
19.1.2 Purging Alert Events Cache ... 402
19.1.3 Enabling Remedial Actions ... 402
19.1.4 Suppressing Duplicate Alerts ... 403
19.1.5 Enabling alert e-mail footer option ... 403
19.1.6 Configuring Correlation Receiver ... 404
19.1.7 Configuring Keyword Indexer ... 404
19.1.8 Configuration pane ... 406
19.1.9 Configuring Logon Banner ... 407
19.1.10 Configuring Cost Savings ... 407
19.1.11 Configuring Usage data ... 408
19.1.12 Group based Archiving ... 408
19.2 Syslog / Virtual Collection Point ... 408
19.2.1 Monitoring syslogs for UNIX ... 408
19.2.2 Virtual Collection Points ... 409
19.2.3 Configuring EventTracker Receiver to listen on Multiple Ports ... 409
19.2.4 Virtual Collection Points for syslogs ... 410
19.2.5 Forwarding Raw syslog Messages ... 411
19.2.6 Virtual Collection Points for Windows Events ... 412
19.2.7 Computer: Sys1 – Configure Ports ... 412
19.2.8 Upgrade Agent (Sys2) from Manager (Sys1) ... 413
19.2.9 Upgrade Agent (Sys2) from Manager (Sys1) ... 414

19.3 Direct Log Archiver 414
19.3.1 Configuring Direct Log File Archiver 414
19.4 Agent Settings 421
19.4.1 Configuring Agent File Transfer Settings 421
19.5 Configuring E-mail Settings 421
19.5.1 Managing Email Accounts 422
19.5.2 Replacing Email Id 424
19.5.3 Removing Email ID 424
19.6 Collection Master Ports 425
19.7 Elastic Search 427
19.7.1 Resolving Hostname through Elasticsearch 427
20. Parsing Rules 430
20.1 About Parsing Rules 431
20.1.1 The Need for adding Parsing Rules in Flex Report 431
20.1.2 Usage of Tokens in EventTracker 431
20.1.3 FAQ: If I bind new Token-value to the parsing rule, will those Token-values be saved permanently in the database? 432
20.2 Prior Knowledge 432
20.3 Components of Parsing Rules 432
20.3.1 Token 432
20.3.2 Parsing Rule Occurrences 432
20.3.3 Display Name 432
20.3.4 Separator 433
20.3.5 Terminator 433
20.4 Viewing Parsing Rules 433
20.5 Adding Token Value Groups 435
20.5.1 Adding Rule 436
20.5.2 Token Value Wizard 437
20.5.3 Using Default Template 439
20.5.4 Creating a new template 440

20.6 Generating a Flex Reports 444

21. Reports Settings 448

21.1 Configuring Published Reports 449

21.2 Configuring Cost Saving Report Settings 451

22. Manage System Groups 453

22.1 About Systems Manager 454

22.1.1 Starting System Manager 454

22.2 Discover Modes 456

22.2.1 Auto Discover Mode 456

22.2.2 Manual Mode 456

22.3 Adding Computers Manually 456

22.3.1 Adding a Single Computer 456

22.3.2 Adding a Group of Computers 458

22.3.3 Adding a Group of Computers from an IP subnet 459

22.4 Logical System Groups 460

22.4.1 Creating a New Logical Group – System Type 461

22.4.2 Creating a New Logical Group – IP Subnet 463

22.4.3 Creating a New Logical Group – Manual Selection 464

22.4.4 Modifying a Group 465

22.4.5 Deleting a Group 467

22.5 Viewing System Details 467

22.6 Restarting Agent Service 468

22.7 Query Agent Service Status 470

22.8 Query Agent Version option 471

22.9 Query for Agent Update Info 472

22.10 Managing Asset Value 475

22.10.1 Setting asset value for multiple systems in a group 476

22.11 Deleting Systems 478

22.12 Search Systems option 480

22.13 Set Sort by option 480

22.14 Systems Report 481

22.15 Configuring Agent-less collection via System Manager (limited features) 482

22.15.1 Adding Systems for Agent-less monitoring 482

22.15.2 Adding systems for Agent-less monitoring........ 482

22.16 Source type mapping to systems 488

22.16.1 Mapping the individual System to the “Source Type” 489

22.16.2 Mapping the Group to the “Source Type” 491

23. Manage Users........ 494

23.1 EventTracker Roles, Permissions & Privileges........ 495

23.1.1 Roles 495

23.1.2 Privileges........ 495

23.1.3 Permissions........ 495

23.2 Managed Service Provider feature 496

23.2.1 How it Works? 496

23.2.2 EventTracker with Local Account Authentication only/ Active Directory Authentication only .. 496

23.2.3 Assigning Permission to users 500

23.2.4 Assigning Privilege to users 501

23.2.5 Promoting a User as an Administrator or Read Only Administrator........ 502

23.3 EventTracker with Active Directory and Database Authentication 504

23.3.1 Adding an Admin User........ 506

23.3.2 Adding an MSP Admin(s) User........ 508

23.3.3 Adding a User(s) 509

23.4 Activating/Inactivating Users 511

23.5 Forgot Password option 513

23.6 Changing Password 515

23.7 Downloading Excel Template........ 516

23.8 Exporting to excel........ 517

23.9 FAQs 517

23.10 Logo Customization 519

23.10.1 Deleting logo........ 520

23.11 Export icon 521

24. Tag Weights 522

24.1 Assigning Weights to Tags 523

24.1.1 Assigning Weights to Multiple Tags 524

24.1.2 Adding Keywords as Tags 524

25. Casebook 526

25.1 About Casebook 527

25.2 Usage of Casebook 527

25.2.1 Creating a new Casebook 531

25.2.2 Adding data to an existing Casebook 535

26. Event Config 538

26.1 Event Config 539

27. Knowledge Base 541

27.1 Knowledge Base 542

27.1.1 Accessing Knowledge Base 542

28. Scheduled Scripts 543

28.1 Scheduled Scripts 544

28.1.1 Verifying Scheduled Script 546

28.1.2 Creating DLA to generate reports. 546

29. Sitemap 549

29.1 Sitemap 550

29.1.1 Viewing Sitemap 550

30. EventVault Warehouse Manager 551

30.1 EventVault Warehouse Manager 552

30.1.1 Configuration button 553

30.1.2 Configuring Archive Path for each VCP 554

30.1.3 Saving EventBox Metadata 559

30.1.4 Backing up EventVault Data 560

30.1.5 Extracting EventBox Data 560

30.1.6 Moving CAB files 561

30.1.7 Deleting an EventBox 562

30.1.8 Viewing CAB Files by Port Number 562
31. Diagnostics 564
31.1 EventTracker Diagnostic Tool 565
31.1.1 Starting EventTracker Diagnostic Tool 565
31.1.2 Setting Debug Levels 567
31.1.3 Obfuscating Classified Information 569
31.1.4 Diagnostic Alert 571
31.2 SQL Log 572
31.3 Backup Configuration option 573
31.4 Restore Configuration option 574
31.5 Advanced Settings 575
31.5.1 Do not collect agent less configuration files 577
31.6 Status Pane 578
32. License Manager 580
32.1 License Manager option 581
33. Export Import Utility 585
33.1 Exporting and Importing Utility 586
33.1.1 Exporting Categories 586
33.1.2 Exporting Filters 587
33.1.3 Exporting Alerts 588
33.1.4 Exporting System Groups 588
33.1.5 Exporting Reports 589
33.1.6 Exporting Machine Learning 592
33.1.7 Exporting Token Value 592
33.1.8 Importing Categories 593
33.1.9 Importing Filters 594
33.1.10 Importing Alerts 594
33.1.11 Importing System Groups 595
33.1.12 Importing Reports 597
33.1.13 Importing Machine Learning 602
33.1.14 Importing Token Value 602

34. Append Archives 603
34.1 Appending CAB Files..... 604
35. Agent Configuration 607
35.1 Agent Configuration 608
35.2 Security - Protect Agent Configuration Settings 608
35.3 Loading a Template 609
35.4 Systems option 611
35.4.1 To Report system name as FQDN 611
35.5 License Server Configuration 611
35.6 Managers tab 612
35.7 Event Filters option 614
35.7.1 Filtering Events with Exception 616
35.7.2 Filtering Events with Advanced Filters 621
35.7.3 Enabling SID Translation 622
35.8 Monitoring System 622
35.8.1 Configuring system performance threshold 623
35.8.2 USB and Other Device Changes 627
35.9 Adding USB device in the Exception List 627
35.10 Monitoring Processes 629
35.10.1 Monitoring application, install/uninstall 629
35.10.2 Filtering processes that need not be monitored 631
35.10.3 Filtering processes that need to be monitored 632
35.11 Monitoring Services 633
35.11.1 Configuring service restart list 633
35.11.2 Filtering Services 634
35.12 Logfile Monitor 635
35.12.1 Viewing File Details 642
35.12.2 Deleting Log File Monitoring Settings 642
35.12.3 Search Strings option 642
35.12.4 Monitoring Check Point Logs 644

35.12.5 Monitoring VMware Logs 647

35.12.6 Specifying the System Name and Event Source for LFM logs 650

35.12.7 Extracting Device ID from syslog devices 651

35.12.8 Monitoring Network Connections 652

35.12.9 Monitoring network connection 653

35.12.10 Excluding Network Connections 654

35.12.11 Including Network Connections to monitor 657

35.12.12 Suspicious Connections feature 659

35.12.13 Monitoring Suspicious Connections 659

35.12.14 Adding programs to the Trusted List 662

35.12.15 Adding Firewall Exceptions to the Trusted List 663

35.13 Monitoring Performance 664

35.13.1 Monitoring configured processes 664

35.13.2 Removing Processes from 'List of Filtered Processes' 667

35.14 Maintaining Log Backup 667

35.14.1 Backing up event logs automatically 667

35.15 Transferring Log Files 670

35.15.1 Transferring Windows and Application Log Files 670

35.16 Syslog FTP Server 674

35.16.1 Transferring Windows events as Syslog messages 674

35.16.2 Saving Current Configuration 677

36. Traffic Analyzer 679

36.1 Event Traffic Analysis 680

36.1.1 Starting Traffic Analyzer 680

36.2 Viewing by Category 681

36.3 Viewing by Event Id 681

36.4 Viewing by Custom Selection 683

36.5 Keyword Analysis option 684

36.5.1 Add Keywords for Analysis option 685

36.5.2 Add Commonly Occurring Words to Exclude from Analysis option 685

37. Agent Management Tool 687
37.1 Windows Agent Management Tool 688
37.1.1 Accessing Agent Management Tool 688
37.1.2 Querying Agent Service Status – System/Group/All/Custom 689
37.1.3 Restarting Agent Service – System / All / Group / Custom 690
37.1.4 Querying Version of the Agent Service – System / Group / All / Custom 692
37.1.5 Removing the Agent Component - System / Group / All / Custom 693
37.1.6 Deleting Systems from agent service - System / Group / All / Custom 694
37.1.7 Querying for Agent Update Info - System / Group / All / Custom 695
38. Port Configuration 697
38.1 About Port Configuration 698
39. Trap Tracker 699
39.1 About TrapTracker 700
39.2 TrapTracker Components 700
40. Change Audit 701
40.1 EventTracker Inventory Manager 702
40.2 Changing Audit Results Summary Console 702
40.3 Changing Policy Dashboard 703
40.4 Configuring Policy Dashboard 703
41. About EventTracker 704
41.1 About EventTracker 705
42. IT Glue Integration 706
43. ConnectWise integration 707
44. Anomalous Login Detection in EventTracker 708
Appendix – HIPAA 709
Appendix – SOX 710
Appendix – GLBA 712
Appendix – Security Reports 713
Appendix – BASEL II 717
Appendix – FISMA 718

Appendix – PCI DSS 719

Glossary 720

About this Guide

This guide will help you to use every option of EventTracker and provides the 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
- Operation 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:

This	Represents
Bold	Input fields, radio button names, checkboxes, drop-down lists, menus, and menu options, buttons on the screen and keyboard keys.
{Text_to_customize}	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.
Constant width	Text that you enter, program code, files and directory names, function names.
🗎	A Note, providing additional information about a certain topic.

Table 1

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

Click	To
🔔	Notification.
⊞	Dashboard Icon.

Click	To
⚙	FAQ Configuration
📄	Report icon.
☰	View stacked bar graph.
📊	View bar graph.
◔	View donut graph.
▌	Use to expand / collapse the panes.
< >	Expand / collapse icon.
✎	Edit icon
✎	Edit from Dashlet
↻	Refresh the page with latest events.
🔍	Search the search phrase.
−	Minimize the Dashlet.
+	Maximize the Dashlet.
✖	Close the Dashlet.
▽	Refine/Filter icon.
▨	No data icon.
☒	Cancelled icon.
»	Processing icon.
✓	Success icon.

Click	To
✖	Failed icon.
★	New icon
GO	Go icon.
📍	Geo Location icon.
< Back	Back icon.
Next >	Next Icon
⊘	Flex Reports icon.
!	Unflagged.
!	Flagged and requires immediate action.
!	Checked and solved.
💬	Add Notes icon.
🎚	Tune Alert Settings
📄	File changes found.
📋	Registry changes found.
📑	File and registry changes found.
✓	Items accepted.
⊖	Items ignored.
✖	Items rejected.

Click	To
🛡	A failed rule marked as Deviation.
☒	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.
🟢	CAB files are present.
🔴	CAB files are not present.
✚	Add to Casebook icon.
💬	Add Notes icon
⬆	Export data
⬇	Import data icon.
✉	Email icon.
🔭	Explore icon.
🔍	Analytics icon.
🗑	Delete icon.
📅	Report Calendar.
☑	Report Status.
ⓘ	Help\information icon.

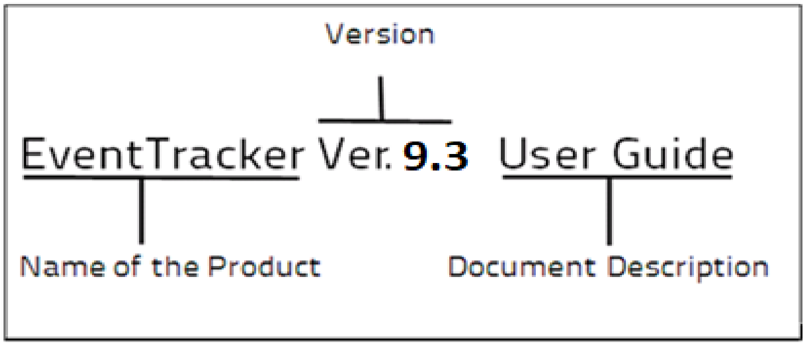
Click	To
⚙	Tools icon
🔍	Clear Search icon
🔎	Advanced Search icon
⧉	Sitemap
⇕	Move Up or Down
◤	Notes Exists
➢	Send to CM
▤	Unknown process filter

Table 2

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



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

File Name	EventTracker v9.3 User Guide
Description	Updated in accordance with release version 9.3
Status	Final
Release Date	18th FEB, 2020.

Table 3

How to get in touch

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

Documentation Support

EventTracker welcomes your comments and suggestions on the quality and usefulness of this document. For any queries, comments, or suggestions on the documentation, you can contact us by e-mail at eventtracker-support@netsurion.com

Customer Support

If you have any problems, questions, comments, or suggestions regarding EventTracker, contact us by e-mail at eventtracker-support@netsurion.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

Virtual Collection Points

Parsing Rule

Install and Customize Web Server (IIS)

IIS Custom Error Setting

Securing IIS Web Server with SSL

What is new in EventTracker v9.3

Now, EventTracker v9.3 comes with an additional layer of security assuredness by integrating/aligning with MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Framework (ATT&CK matrix). We believe this combination of cybersecurity intelligence can help your enterprise to stay on top of the ever-evolving threat landscape.

For more information please refer to EventTracker MITRE ATT&CK™ User Guide

What is new in EventTracker v9.3.1

New features and enhancements available as part of update ET93U20-021 (Feature update 9.3.1)

- Two-factor Authentication (2FA) support using Google Authenticator App.

  The Authenticator configured on your phone provides an additional level of security to the EventTracker Login. It is an effective yet a simple way to authenticate and protect the users from the hackers. With 2FA enabled, hackers would not be able to log in even if the password is known.

  For more information please refer to Two-factor Authentication (2FA) Guide

- EventTracker Threat Center (ETC) integration as an IP reputation provider.

  EventTracker Threat Center is Netsurion' s Threat Center Platform. It is a repository of threats indicators. It accumulates series of different threat feeds, gathers information about IP addresses, scans an IP address with multiple IP blacklist and finds security threats. EventTracker Threat Center is used as an alternate IP reputation provider and is maintained by Netsurion.

  For more information please refer to EventTracker Threat Center (ETC) Guide

- Filter Support for Anomalous Login Detection and support for both Private IPs and Public IPs

  Anomalous Login Detection feature detects intrusion, fraud and fault by the network intruders. The unauthorized entries can be identified based on username and IP address. Anomalous Login Detection now supports both Private IPs and Public IPs. In addition, filter option is provided to exclude any Username or IP address or both Username and IP address.

  For more information please refer to Anomalous Login Detection Guide

What is new in EventTracker v9.3.2

New features and enhancements available as part of update ET93U20-026 (Feature update 9.3.2)

- Database shrinking support and diagnostic warning for database exceeding threshold limit.
  - Shrinking (Includes all databases).
    - Scheduled
    - On Demand (Shrink now option)
  - Diagnostic alert for SQL transaction log threshold (Default 1 GB).
  - Diagnostic event (3272) for database size threshold.
    - Warning alert once db size crosses 5GB (Default)
    - Critical alert once db size crosses 8GB (Default)

- Octet count framing in syslog over TCP/TLS (RFC 5425 compliant).

- Incidents email to contain notes/comments.
  - When Email is sent from Incident page, it will contain Notes/Comments that were added to the incidents.

What is new in EventTracker v9.3.3

New features and enhancements available as part of update ET93U20-031 (Feature update 9.3.3)

- New and improved system selection interface in Log Search and Report configuration.

  For more information please refer to New SystemSelection Interface User Guide.

What is new in EventTracker v9.3.4

New features and enhancements available as part of update ET93U20-035 and ET93U20-036.

- Enhancements in Syslog Receiver to extract Device ID/Name and assign Device type.

  For more information please refer to Device Name and Device Type Extraction Guide

- Enhancements in EDR to allow/deny a parent process name along with parent process hash and enhancements in EDR GUI

  For more information please refer to Endpoint Detection and Response (EDR) v9x User Guide

What is new in EventTracker v9.2

- **Group based archiving**

  Data for the respective group will be stored in dedicated files (in the form of cabs) with group name suffix added.

- **Source type mapping to systems**

Systems can be mapped to a particular “Source Type” which will improve the Elasticsearch indexer performance.

- **Conditional Tag configurations**

  Conditional tagging helps users to perform efficient log search across all log sources.

- **IT Glue integration**

  EventTracker can be integrated to IT Glue which helps to view EventTracker generated Security and Compliance Summary reports in IT Glue portal.

- **Pre-Installer changes**

  The pre-installer setup has undergone several changes to speed up and automate the installation process. For detailed information regarding this, kindly refer to the EventTracker v9.3 Install Guide.

- **ConnectWise integration**

  EventTracker can be integrated into ConnectWise Manage which helps in integrating EventTracker Casebook with the ConnectWise ticketing system.

- **Anomalous Login Detection in EventTracker**

  EventTracker is introducing a new kind of capability to identify Anomalous Login activity.

1. Getting Started

In this chapter, you will learn about:

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

1.1 About EventTracker

EventTracker framework is EventTracker Security LLC 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 2012 R2/10/2016/2019, 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
- 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)
- Casebook
- Parsing of token
- Persist data
- Instant search option

1.2 EventTracker Services and Ports

Service	Description	Startup Type	Logon as	Allow service to interact with desktop
Event Correlator	Correlates the received events from the agent and performs the action based on the rules.	Automatic	Local System account	Yes
EventTracker Agent	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.	Automatic	Local System account	Yes
EventTracker Alerter	Used by EventTracker to download feeds from TAXII server and run the Diagnostic in scheduled time.	Automatic	Local System account	Yes
EventTracker Elasticsearch Indexer	Service used to parse and normalize events/logs, and then indexed into Elasticsearch.	Automatic	Local System account	Yes
Elasticsearch 7.2.1 (elasticsearch-service-x64)	Elasticsearch is a search engine used to index and fetch the normalized events/logs.	Automatic	Local System account	Yes
EventTracker EventVault	An EventTracker component to compress and securely store the raw log data.	Automatic	Local System account	Yes
EventTracker Indexer	Responsible for indexing the key words of event properties. Event properties include Computer, Source, EventID, Domain, User, LogType, EventType, and Description.	Automatic	Local System account	Yes
EventTracker Receiver	Enables EventTracker to receive log data from the configured sources. If stopped, EventTracker cannot function. May be restarted to pick up new configuration.	Automatic	Local System account	Yes

Service	Description	Startup Type	Logon as	Allow service to interact with desktop
EventTracker Remoting	This service is used to send any request (like install agent/upgrade agent/uninstall agent etc.) to communicate with the EventTracker agent service and log search.	Automatic	User Account	Yes
EventTracker Reporter	Responsible for reports / Flex Report execution.	Automatic	Local System account	Yes
EventTracker Scheduler	Used by EventTracker to initiate scheduled activities like CAB integrity verification, traffic analysis. Also initiates User Activity monitoring and 'Collection Point' related activities.	Automatic	Local System account	Yes
WcwService	Used to take periodic snapshots and entertain change assessment requests.	Automatic	Local System account	Yes
Trap Tracker Receiver	Receives traps in the form of an alert or other asynchronous event about a managed subsystem.	Automatic	Local System account	Yes
EventTracker Monitoring Daemon	Monitors the agent/sensor service status. Whenever the agent service is down, it restarts the service.If the service is not restarted, it makes three attempts, each between an interval of 15 minutes, to restart the agent service.	Automatic	Local System account	Yes

Table 4

NOTE

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

EventTracker Module	Port(s)
EventTracker Agent	14506/TCP
Windows Receiver	14505(TCP/UDP) - optional and multiple VCP's can be configured
Syslog Receiver	514(UDP/TCP) can be configured to any number of ports
Collection Master	14507/TCP - optional and can be configured to any TCP port
Correlation Receiver	14509/TCP
EventTracker – Change Audit Agent	14502 (TCP) - to transfer snapshot between client and Server. 14508 (TCP) - used for real-time comparison of any system with the golden snapshot located at the server.
License Server	14503/TCP
EventTracker Active WatchList	14504
Elasticsearch	9200

Table 5

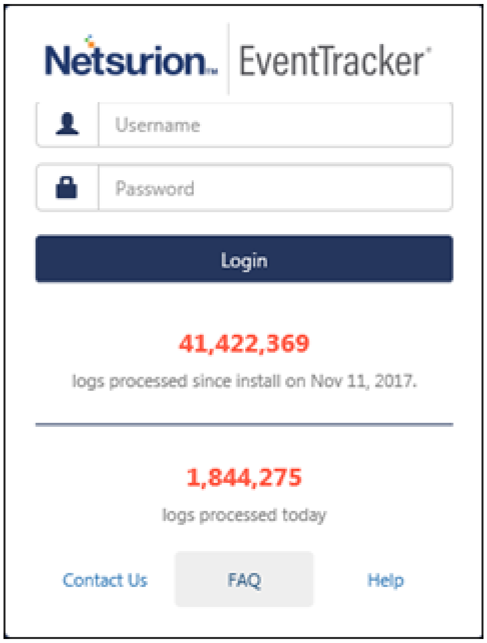
In case the user creates multiple Virtual Collection Points, ensure the port used does not contradict with the Default ports used.

1.3 Starting EventTracker

1 Click **Start,** select **All Programs,** and then select **Prism Microsystems.**
2 Click **EventTracker,** and then select **EventTracker**.

(OR)
Double-click the **EventTracker** shortcut on desktop.

EventTracker opens the login page.



Netsurion | EventTracker

Username

Password

Login

41,422,369

logs processed since install on Nov 11, 2017.

1,844,275

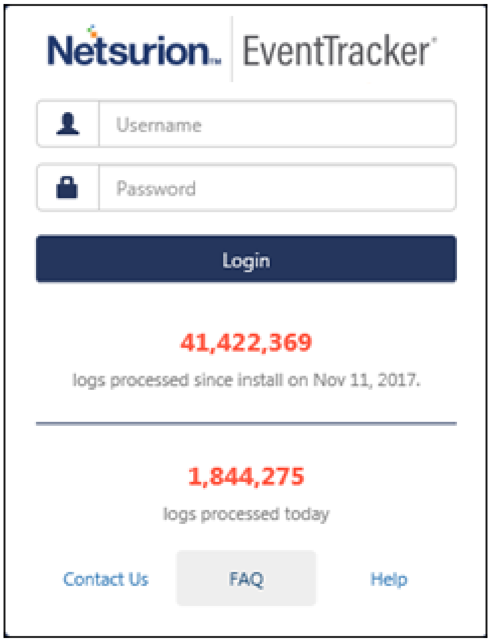
logs processed today

Figure 1

Click	To
Contact Us	Go to 'Contact page' on EventTracker Web site.
FAQ's	Go to FAQ page.
Help	View online help.

Table 6

EventTracker opens the logs processed information only when a CAB file is created locally on the server.



41,422,369

logs processed since install on Nov 11, 2017.

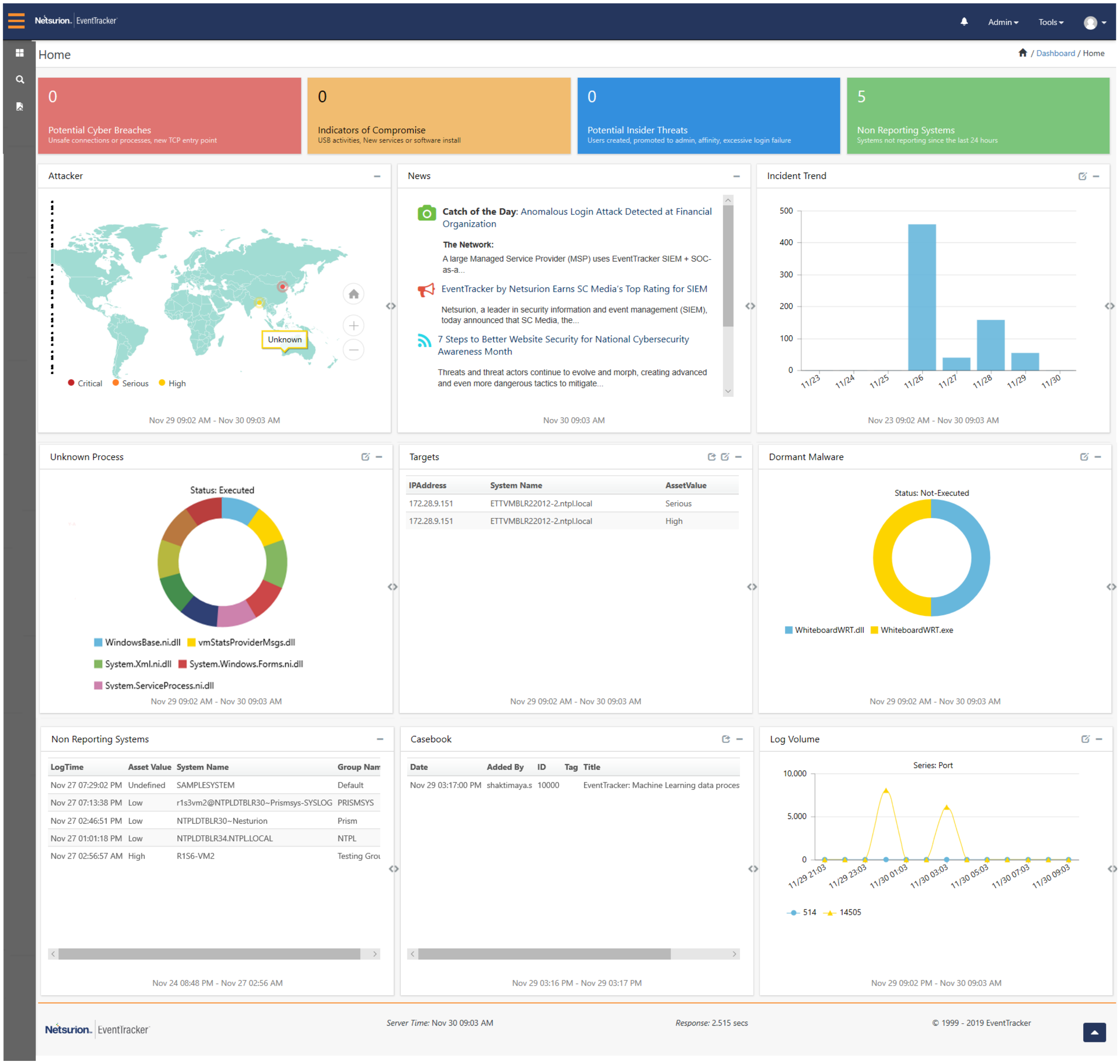
1,844,275

logs processed today

Figure 2

3 Type valid user credentials, and then click **Login**.

EventTracker opens the **Home** page.



Home

/ Dashboard / Home

0
Potential Cyber Breaches
Unsafe connections or processes, new TCP entry point

0
Indicators of Compromise
USB activities, New services or software install

0
Potential Insider Threats
Users created, promoted to admin, affinity, excessive login failure

5
Non Reporting Systems
Systems not reporting since the last 24 hours

Attacker

Nov 29 09:02 AM - Nov 30 09:03 AM

News

Catch of the Day: Anomalous Login Attack Detected at Financial Organization

The Network:

A large Managed Service Provider (MSP) uses EventTracker SIEM + SOC-as-a...

EventTracker by Netsurion Earns SC Media's Top Rating for SIEM

Netsurion, a leader in security information and event management (SIEM), today announced that SC Media, the...

7 Steps to Better Website Security for National Cybersecurity Awareness Month

Threats and threat actors continue to evolve and morph, creating advanced and even more dangerous tactics to mitigate...

Nov 30 09:03 AM

Incident Trend

Nov 23 09:02 AM - Nov 30 09:03 AM

Unknown Process

Status: Executed
🟦 WindowsBase.ni.dll 🟨 vmStatsProviderMsgs.dll
🟩 System.Xml.ni.dll 🟥 System.Windows.Forms.ni.dll
🟪 System.ServiceProcess.ni.dll

Nov 29 09:02 AM - Nov 30 09:03 AM

Targets

IPAddress	System Name	AssetValue
172.28.9.151	ETTVMBLR22012-2.ntpl.local	Serious
172.28.9.151	ETTVMBLR22012-2.ntpl.local	High

Nov 29 09:02 AM - Nov 30 09:03 AM

Dormant Malware

Nov 29 09:02 AM - Nov 30 09:03 AM

Non Reporting Systems

LogTime	Asset Value	System Name	Group Nam
Nov 27 07:29:02 PM	Undefined	SAMPLESYSTEM	Default
Nov 27 07:13:38 PM	Low	r1s3vm2@NTPLDTBLR30~Prismsys-SYSLOG	PRISMSYS
Nov 27 02:46:51 PM	Low	NTPLDTBLR30~Nesturion	Prism
Nov 27 01:01:18 PM	Low	NTPLDTBLR34.NTPL.LOCAL	NTPL
Nov 27 02:56:57 AM	High	R1S6-VM2	Testing Grou

Nov 24 08:48 PM - Nov 27 02:56 AM

Casebook

Date	Added By	ID	Tag	Title
Nov 29 03:17:00 PM	shaktimaya.s	10000		EventTracker: Machine Learning data proces

Nov 29 03:16 PM - Nov 29 03:17 PM

Log Volume

Nov 29 09:02 PM - Nov 30 09:03 AM

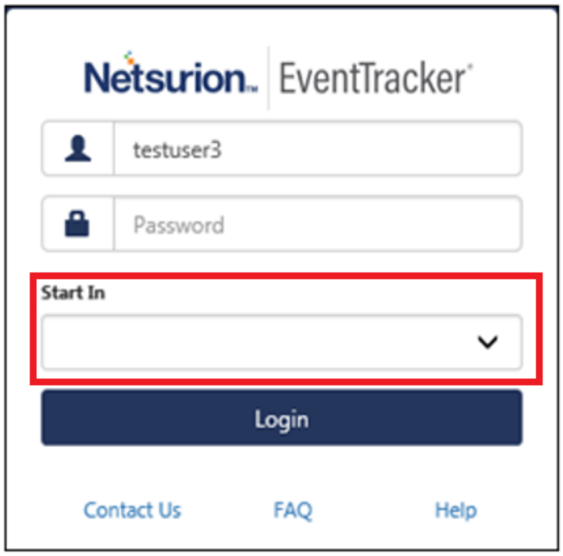
Server Time: Nov 30 09:03 AM

Response: 2.515 secs

© 1999 - 2019 EventTracker

Figure 3

For "**Admin given privileges to a user**", the EventTracker login page appears, as shown below with the **Start In**: field.



testuser3

Password

Start In

Figure 4

The user can select any other option from the dropdown list to be displayed, as the home page.

Now, login to the EventTracker web portal. The Home page is viewable.

EventTracker Dashboard menu consists of the following menu’s as mentioned in the table.

Click	To
DASHBOARD	
Home	Customize and view Dashboards for Attackers, Log Volume, Incident Trend, Unknown Process, Targets, Dormant Malware, Non Reporting System and Casebook.
My Dashboard	Helps to view quick statistics and graphs like trend of events based on any flex persisted data.
Threats	View Attackers and Targets Dashboard and Analyze Unknown Processes.
Incidents	Analyze alert events occurred in all managed systems.
MITRE ATT&CK™	The MITRE ATT&CK™ provides a well-defined standard for attack identification and protection.
Machine Learning	Add/remove enterprise activity dashlets. Configure, customize, and reset dashlets. Generate volume analysis reports.
Change Audit	Helps to analyze voluntary and involuntary changes occurred in managed systems.
Compliance	View the data for compliance in this Dashboard.
Search	Perform a Log Search/Elastic Search
Reports	Consists of Security, Operation, Compliance and Flex Reports

Table 7

NOTE

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

4 Click the **Admin** option at the upper-right corner.

1.4 Admin Menu

1 Click on the **Admin** dropdown.
It consists of options that help you to quickly access EventTracker modules.

Click	To
Active Watch Lists	Import lists of ip address, process, users, etc for managing threat information.
Alerts	Manage Alert Configuration including notification and threat level.
Machine Learning Jobs	Define and manage Machince Learning Jobs. These are used to display behavior dashlets in the Security, Operations tabs.
Machine Learning Settings	Configuring settings for the “machine leaning” module.
Casebook Configuration	Customize Casebook entry columns as per your enterprise requirements.
Category	Event categories are used in reports, search and views. Pre-defined categories of knowledge are available. Users may create/edit categories.
Collection Master	EventTracker ‘Collection Master’ collects CAB files forwarded by Collection Point(s).
Diagnostics	Diagnostics displays Disk Usage status, VCP statistics, etc.
Event Filters	Configure manager side event filters to avoid archiving specific events.
Eventvault	Functions as warehouse for CAB files. Manage archives and configure retention and validation.
FAQ Tile Configuration	Configure FAQ tiles to display in Home/ Alerts/Systems and Report.
Group Management	Configure Alert action email based on system group
IP Lookup Configuration	Customizable IP Address verification/detailed information.

Click	To
Knowledge Objects	Knowledge objects are used for identification and extraction of meaningful information from the logs received.
Manager	Define Virtual Collection Points, enable Syslog, configure DLA, enable NetFlow receivers etc.
Parsing Rules	Parsing Rules
Report Settings	Manage settings that affect report generation and e-mail delivery.
Systems	Manage EventTracker Windows agent and Change Audit agent.
Users	Manage privileges and permissions of the users defined in the EventTracker user group.
Weights	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).
Windows Agent Config	Manage configuration of EventTracker Windows Agent.

Table 8

NOTE

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

1.5 Tools Menu

TOOLS	
Casebook	An electronic book in which users can add entries from Incidents, Reports, Change Audit.
Event Config	Enable/disable events generated in Change Audit and Direct Log Archiver.
Summary report Config	Instead of reviewing dozens of generated persists reports, this report will give complete user specified fields in a single report.
Knowledge Base	Go to EventTracker Knowledge Base Web site http://kb.eventtracker.com/
Scheduled Scripts	Scripts can be run through windows task scheduler
Sitemap	View index of the web site.

Table 9

🗎 NOTE

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

1.6 EventTracker Control Panel

1 Click **Start,** select **All Programs,** and then select **Prism Microsystems.**

2 Click **EventTracker,** and then select **EventTracker Control Panel**.

(OR)

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

EventTracker login page appears.

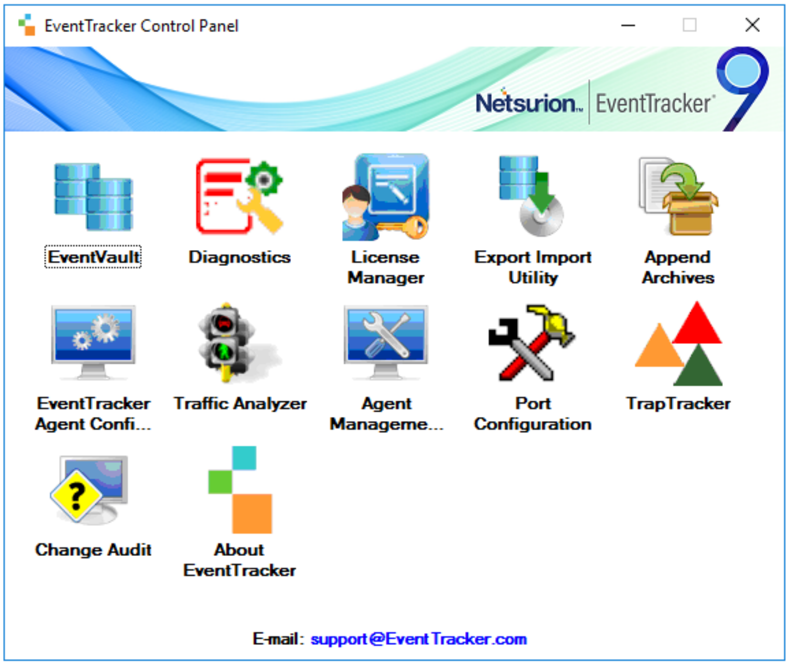


Figure 5

🗎 NOTE

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

3 To open a module, click the respective icons.

Click	To
EventVault	Functions as warehouse for CAB files. Manage archives and configure retention and validation.
Diagnostics	Alerts if any problem occurs in the EventTracker.
License Manager	Provides license details, features opted for, license usage of EventTracker.
Export Import Utility	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.
Append Archives	Use this utility to merge backup CAB files. Indexing is done automatically.
EventTracker Agent Confi...	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.
Traffic Analyzer	To analyze event traffic patterns. The data can be used to filter out irrelevant events and perform other operation tasks.
Agent Manageme...	A diagnostic tool to check the health status of remote agents, restart the failed agent services and to check the version of remote agents.
Port Configuration	To change the port and monitor the websites and its corresponding applications.
TrapTracker	To manage traps received from SNMP enabled devices.

Change Audit	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.
About EventTracker	View License Usage, updates applied and other details.

Table 10

1.7 Profile Menu

1.7.1 Viewing Profile

The user can view here the profile details.

1.7.2 Advanced Window

1. Click **Advanced**.

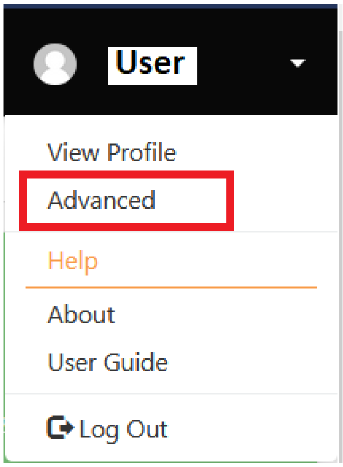
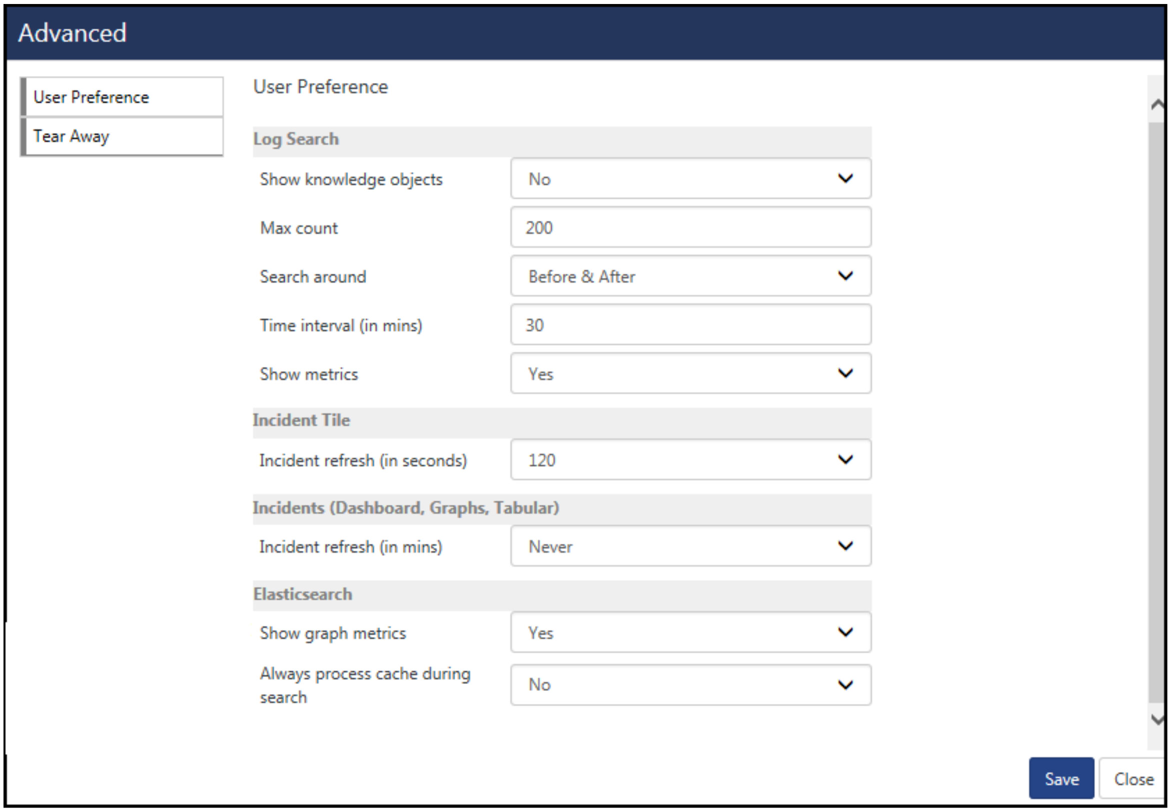


Figure 6

2. User Preference window opens.



Advanced

User Preference

Log Search

Show knowledge objects	No
Max count	200
Search around	Before & After
Time interval (in mins)	30
Show metrics	Yes

Incident Tile

Incident refresh (in seconds)	120

Incidents (Dashboard, Graphs, Tabular)

Incident refresh (in mins)	Never

Elasticsearch

Show graph metrics	Yes
Always process cache during search	No

Figure 7

3. Select **Show knowledge objects:** option.
4. Enter **Max count:** to be displayed.
5. In the **Search around** option, the user can specify the time range to search an event property. Select the option from the dropdown list.
6. Enter the appropriate **Time Interval**.

   The user can also configure the Incidents refresh time and can enable or disable the "**Show graph metrics**" option for the Elasticsearch and then click **Save**.
7. Select **Tear Away** option.

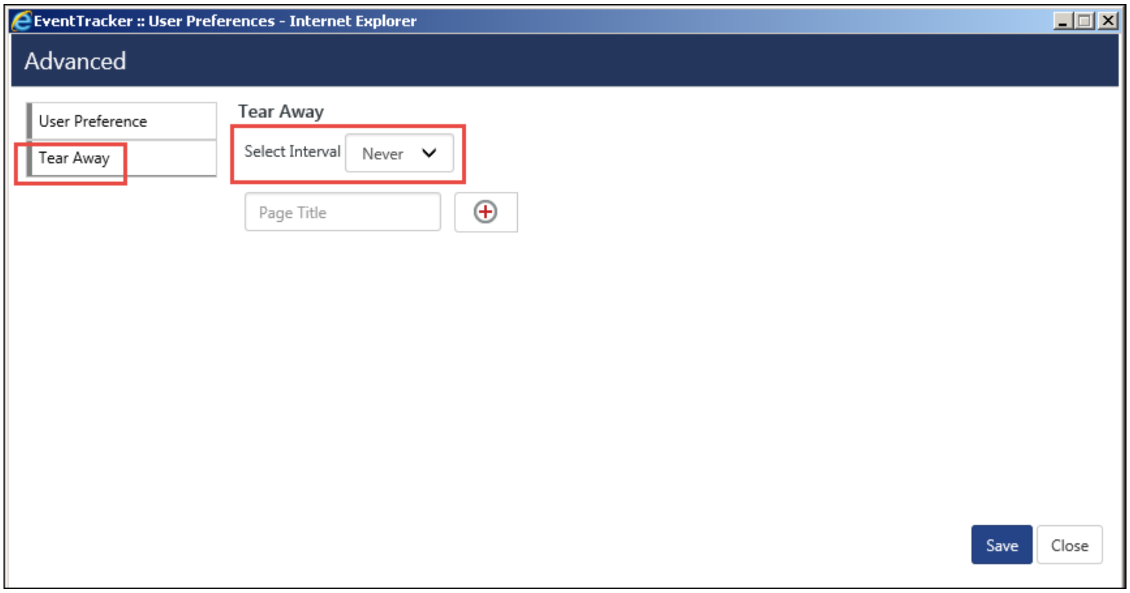


Figure 8

8. Select the desired Select Interval: option.

9. The user can create a customized page and add dashlets to the created page.

10. Enter the Page Title and to add it click ⊕ .

    In this example, we are adding “My Page”.

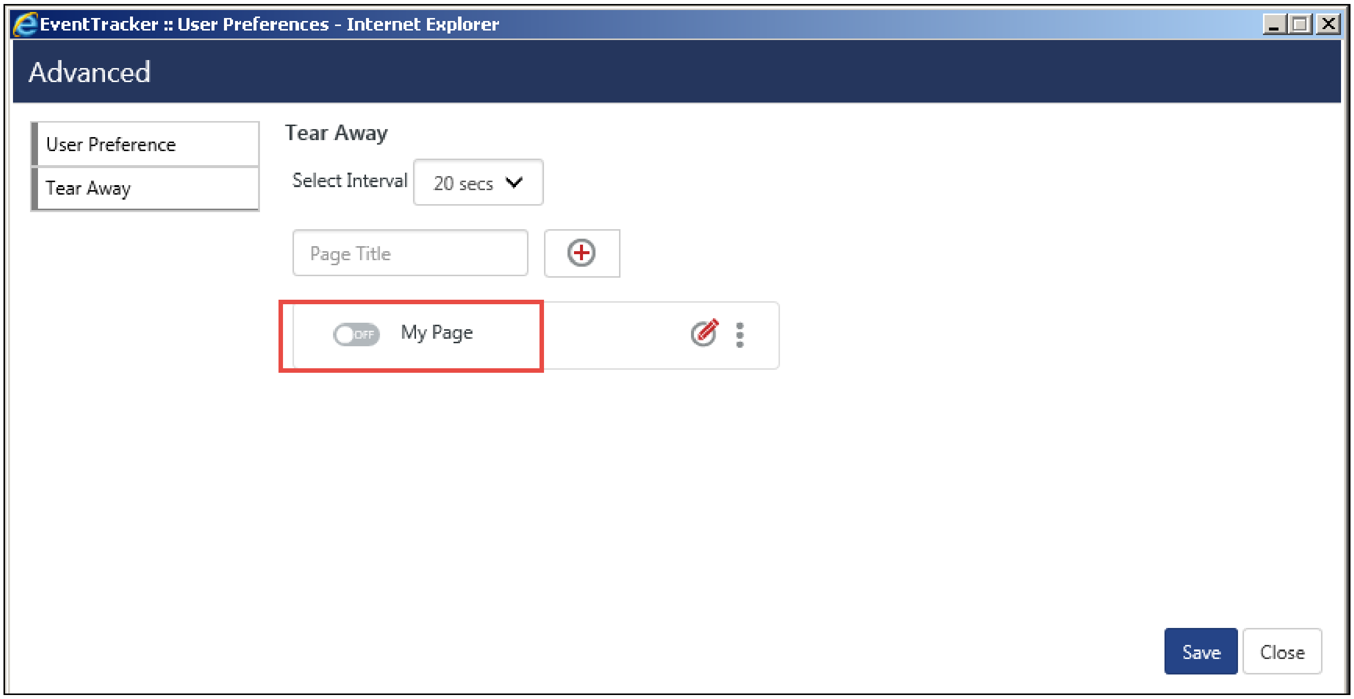


Figure 9

11. Now to add dashlet(s) to the created page, click ⋮ .

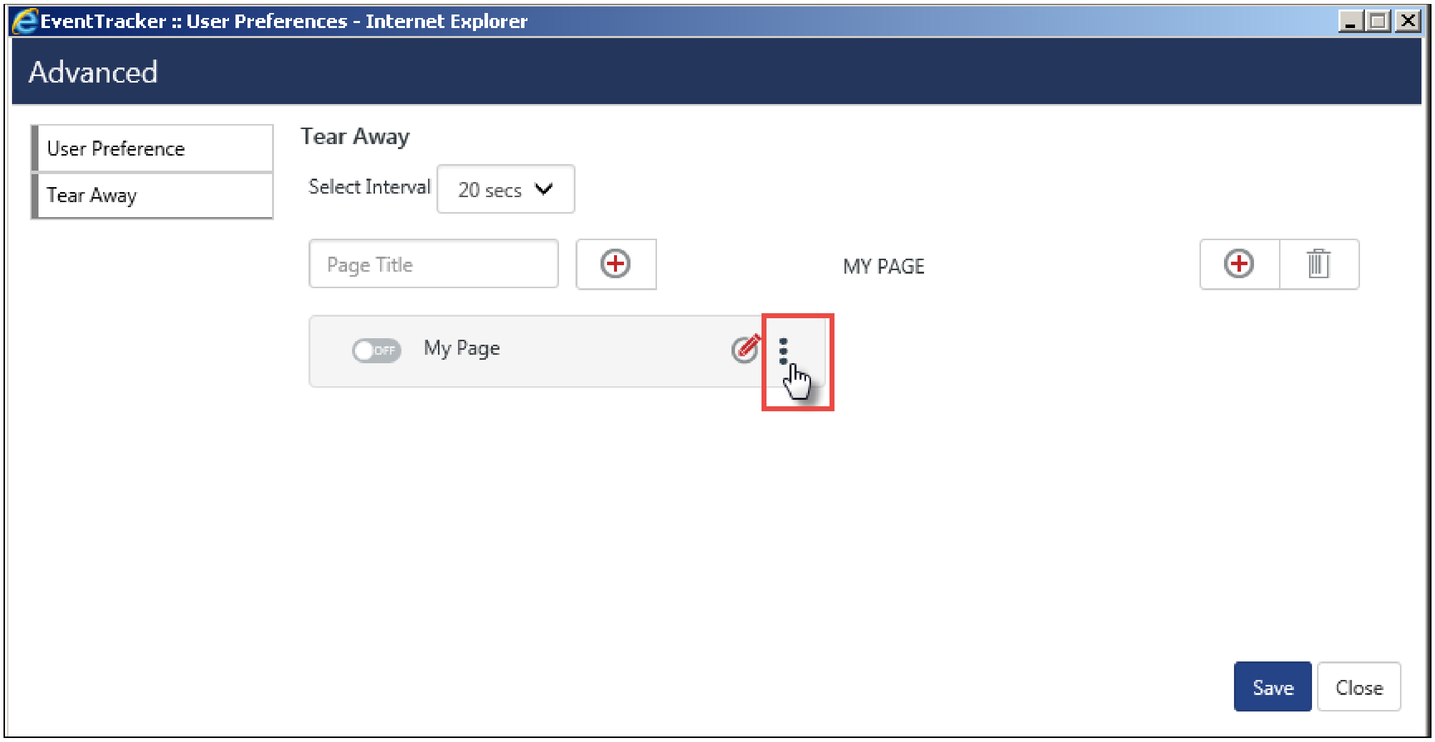


Figure 10

12. Select **Add** ⊕.

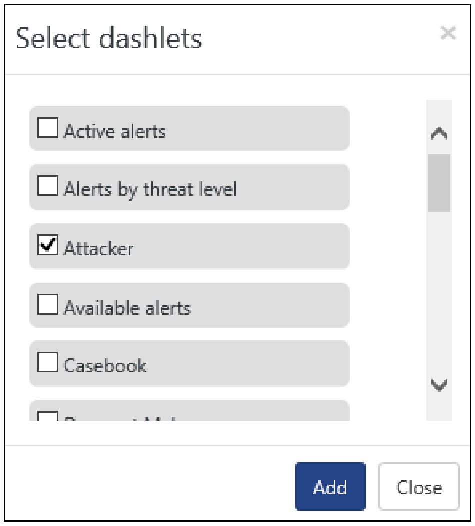


Figure 11

13. Select from the available list of dashlet(s) and click **Add**.

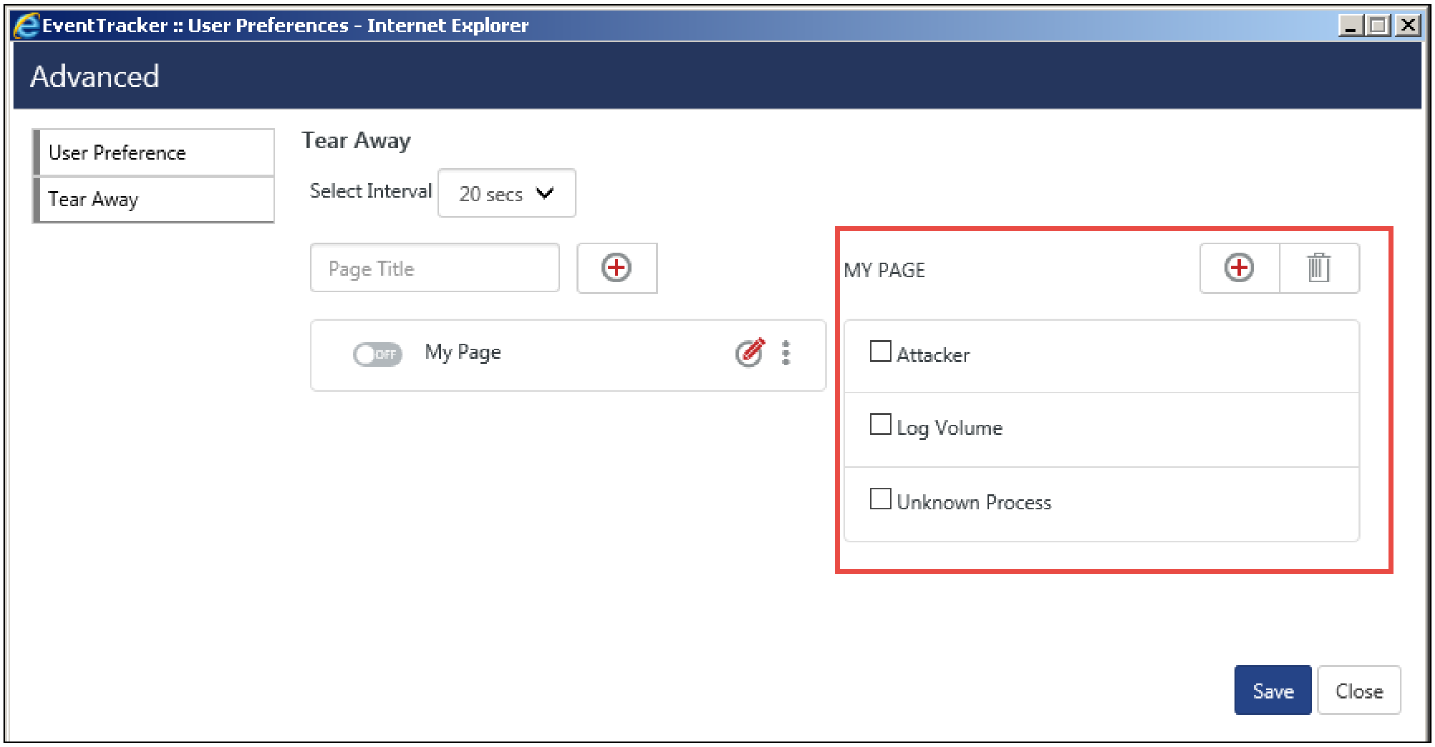
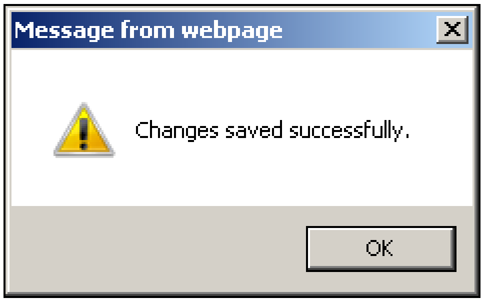


Figure 12

The Dashlet(s) gets added for "**My Page**". Select them and **Save**.

The below message opens

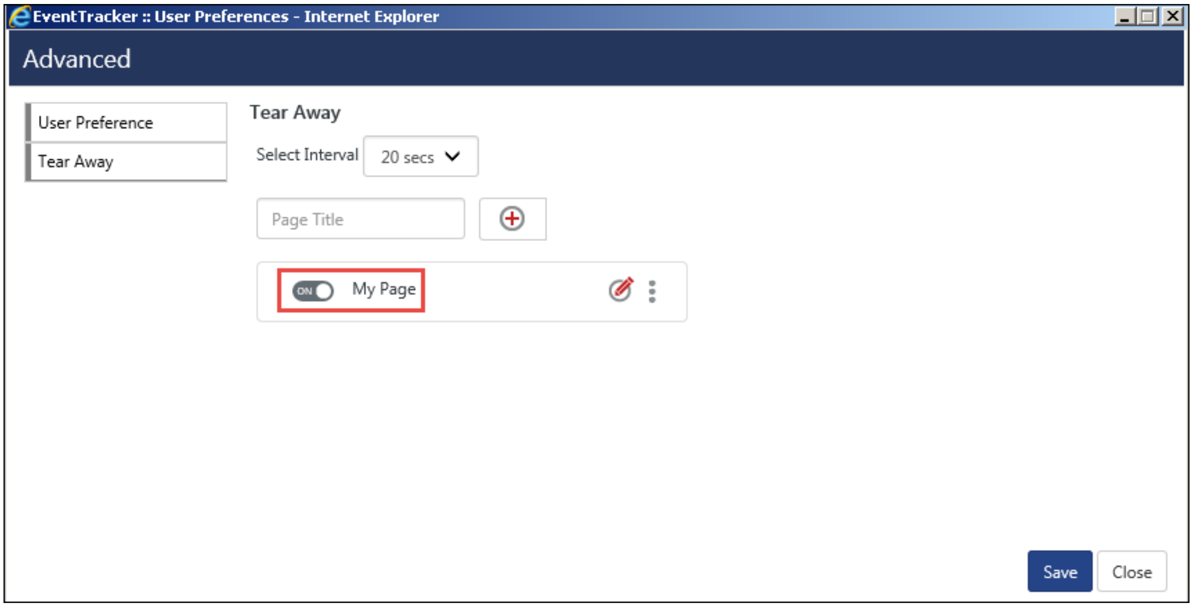


Message from webpage

Changes saved successfully.

Figure 13

To make it active, turn it to the "**ON**" mode.



Select Interval 20 secs

ON My Page

Figure 14

The created page will keep on displaying the selected dashlets in a new window and will refresh every selected (20 secs/1min/2 min...) interval.

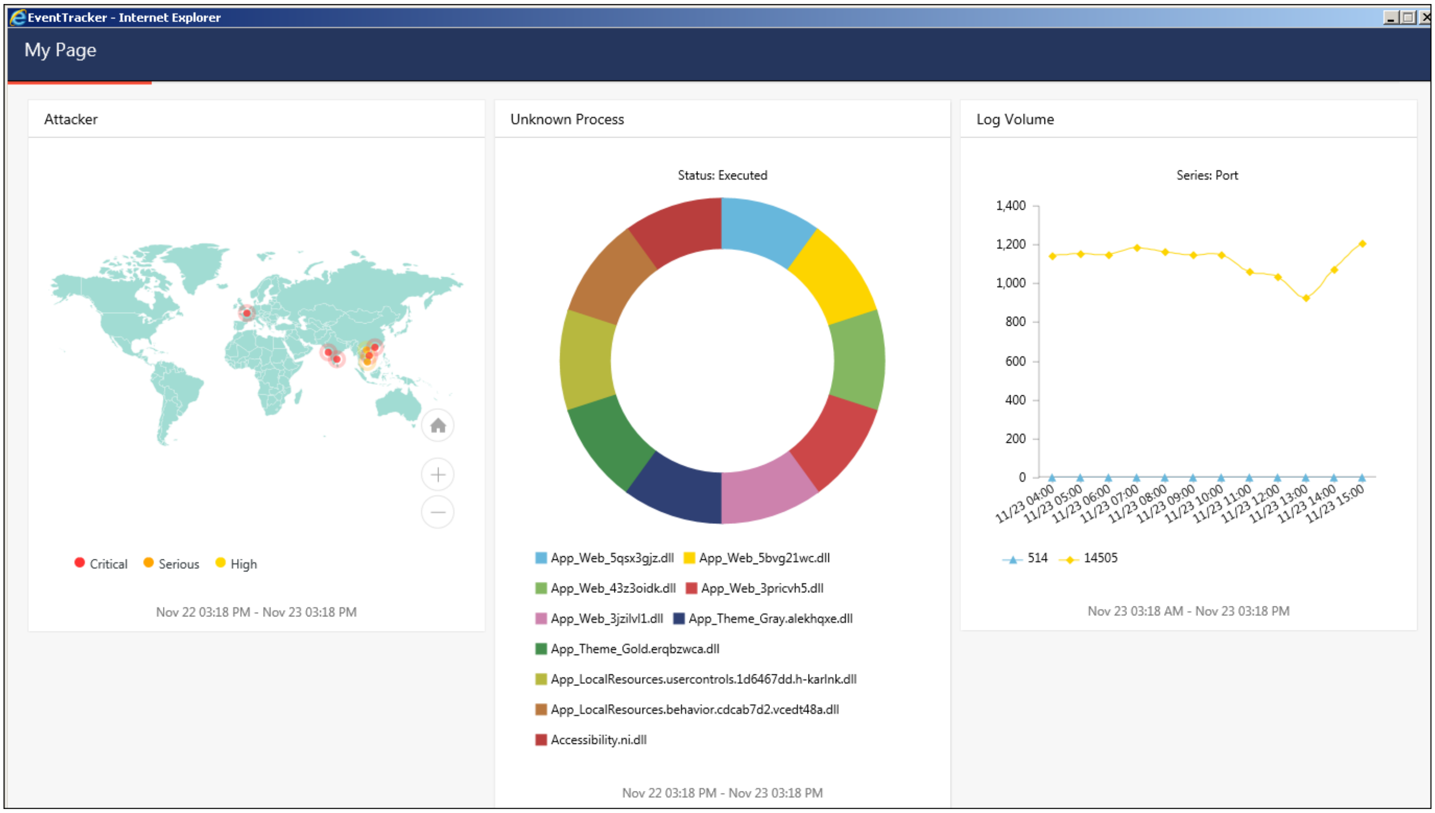


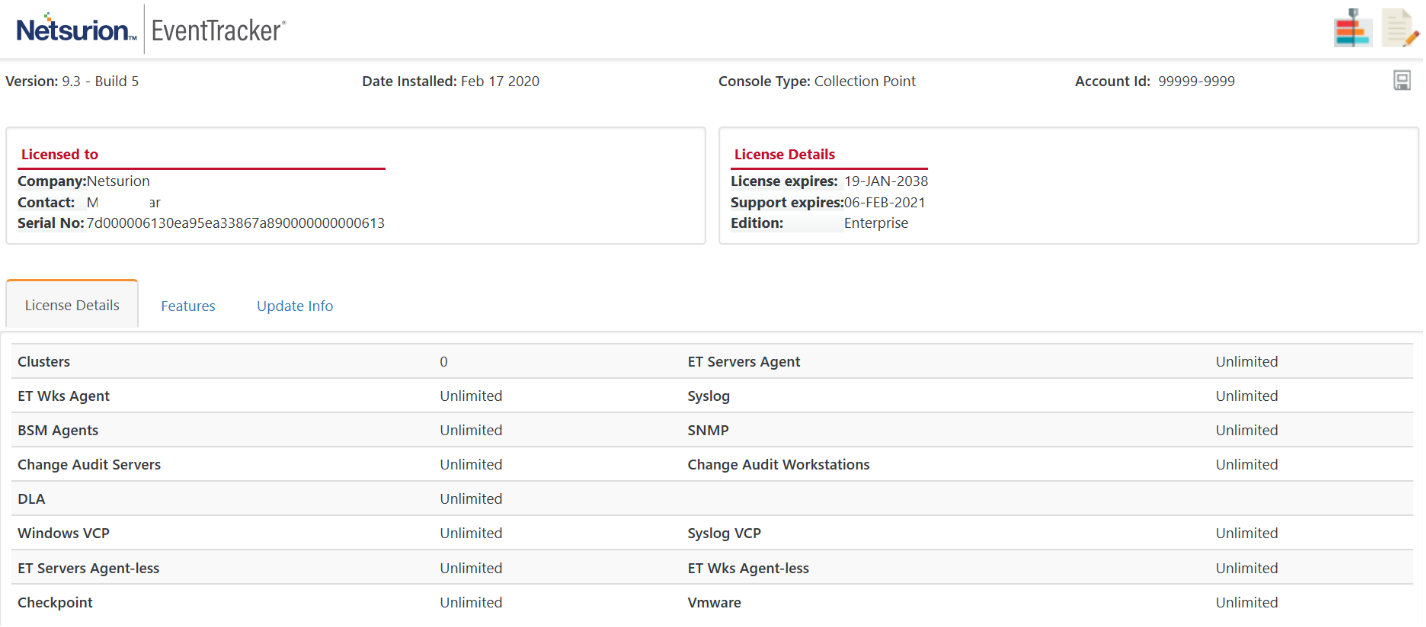
Figure 15

1.8 Help option

1.8.1 Licensing Details

1. Click your **Profile**, and then select **About** from the dropdown.

   License Details opens.



Version: 9.3 - Build 5 **Date Installed:** Feb 17 2020 **Console Type:** Collection Point **Account Id:** 99999-9999

Licensed to

Company: Netsurion
Contact: M ar
Serial No: 7d000006130ea95ea33867a890000000000613

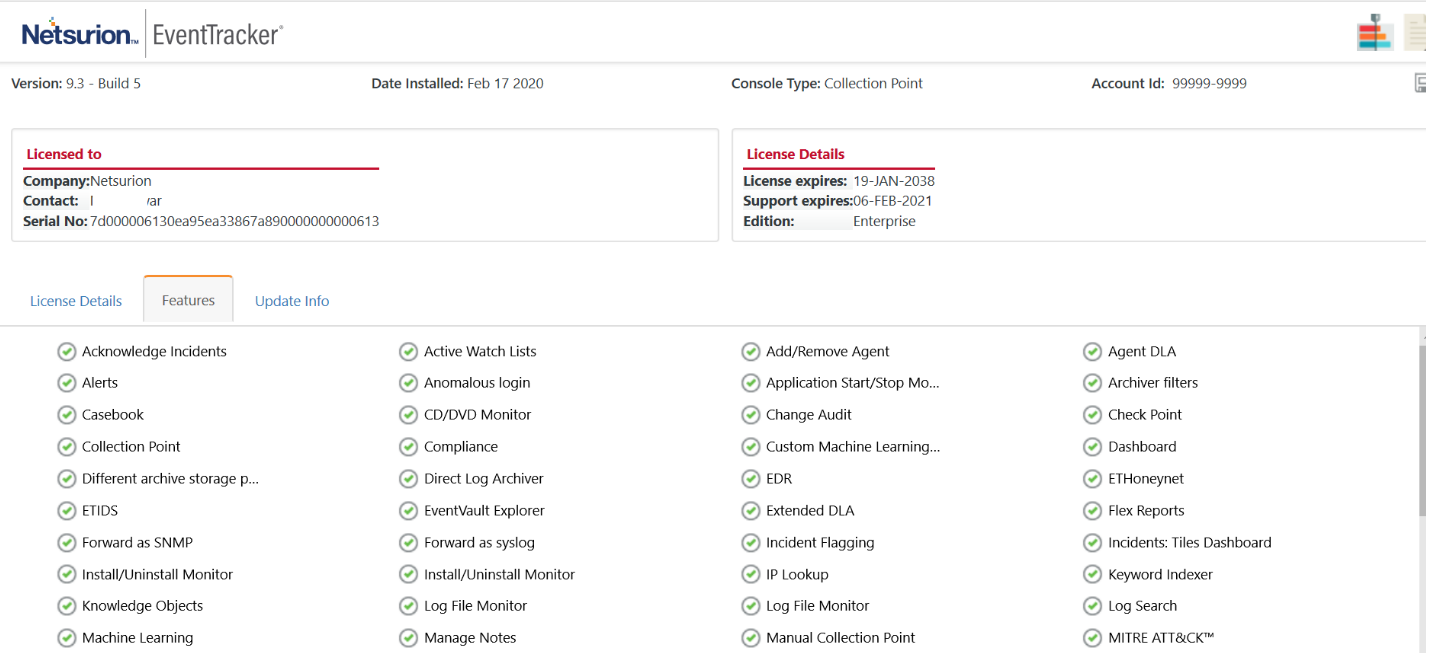
License Details

License expires: 19-JAN-2038
Support expires:06-FEB-2021
Edition: Enterprise

Clusters	0	ET Servers Agent	Unlimited
ET Wks Agent	Unlimited	Syslog	Unlimited
BSM Agents	Unlimited	SNMP	Unlimited
Change Audit Servers	Unlimited	Change Audit Workstations	Unlimited
DLA	Unlimited		
Windows VCP	Unlimited	Syslog VCP	Unlimited
ET Servers Agent-less	Unlimited	ET Wks Agent-less	Unlimited
Checkpoint	Unlimited	Vmware	Unlimited

Figure 16

2. Click the 🖫 icon to save the license details.
3. To view the features that have been installed, click **Features** tab.



Version: 9.3 - Build 5 **Date Installed:** Feb 17 2020 **Console Type:** Collection Point **Account Id:** 99999-9999

Licensed to

Company: Netsurion
Contact: I [redacted]ar
Serial No: 7d000006130ea95ea33867a890000000000613

License Details

License expires: 19-JAN-2038
Support expires:06-FEB-2021
Edition: Enterprise

- ✓ Acknowledge Incidents
- ✓ Alerts
- ✓ Casebook
- ✓ Collection Point
- ✓ Different archive storage p...
- ✓ ETIDS
- ✓ Forward as SNMP
- ✓ Install/Uninstall Monitor
- ✓ Knowledge Objects
- ✓ Machine Learning
- ✓ Active Watch Lists
- ✓ Anomalous login
- ✓ CD/DVD Monitor
- ✓ Compliance
- ✓ Direct Log Archiver
- ✓ EventVault Explorer
- ✓ Forward as syslog
- ✓ Install/Uninstall Monitor
- ✓ Log File Monitor
- ✓ Manage Notes
- ✓ Add/Remove Agent
- ✓ Application Start/Stop Mo...
- ✓ Change Audit
- ✓ Custom Machine Learning...
- ✓ EDR
- ✓ Extended DLA
- ✓ Incident Flagging
- ✓ IP Lookup
- ✓ Log File Monitor
- ✓ Manual Collection Point
- ✓ Agent DLA
- ✓ Archiver filters
- ✓ Check Point
- ✓ Dashboard
- ✓ ETHoneynet
- ✓ Flex Reports
- ✓ Incidents: Tiles Dashboard
- ✓ Keyword Indexer
- ✓ Log Search
- ✓ MITRE ATT&CK™

Figure 17

4. Click **Update Info** to view the updates installed, if any.

1.8.2 User Guide Details

1. Click the **Help** option.
   The EventTracker User Guide for the respective version displays.

1.9 Keeping the Tear Away feature functioning forever without being logged out

NOTE: This is applicable only for **IIS Webserver.**

Follow the steps mentioned below:

1. Go to **Start**> **All Programs**>**Internet Information Services (IIS) Manager**.
   OR,
2. Go to **Run** option and type **“inetmgr”** to open the **IIS Manager.**

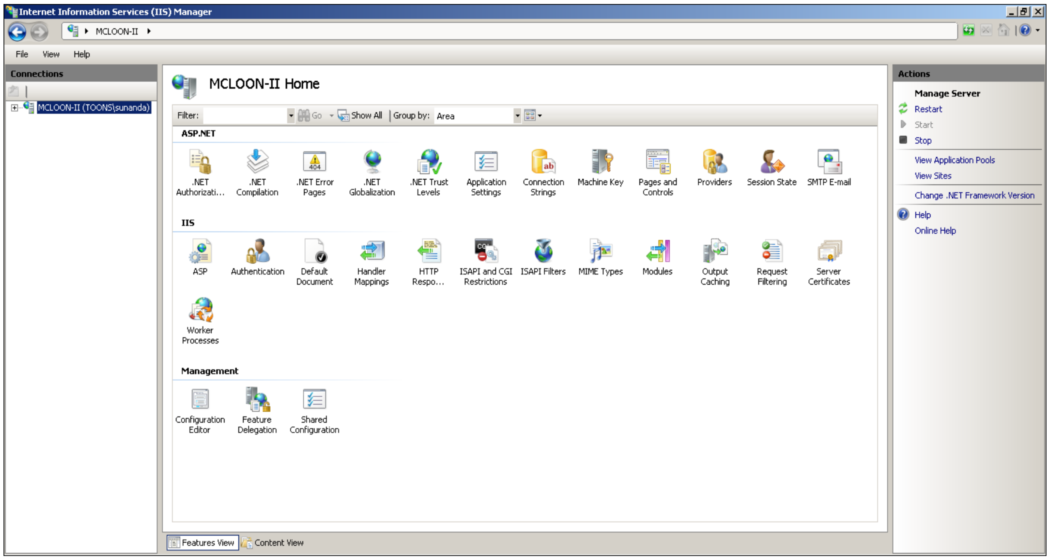
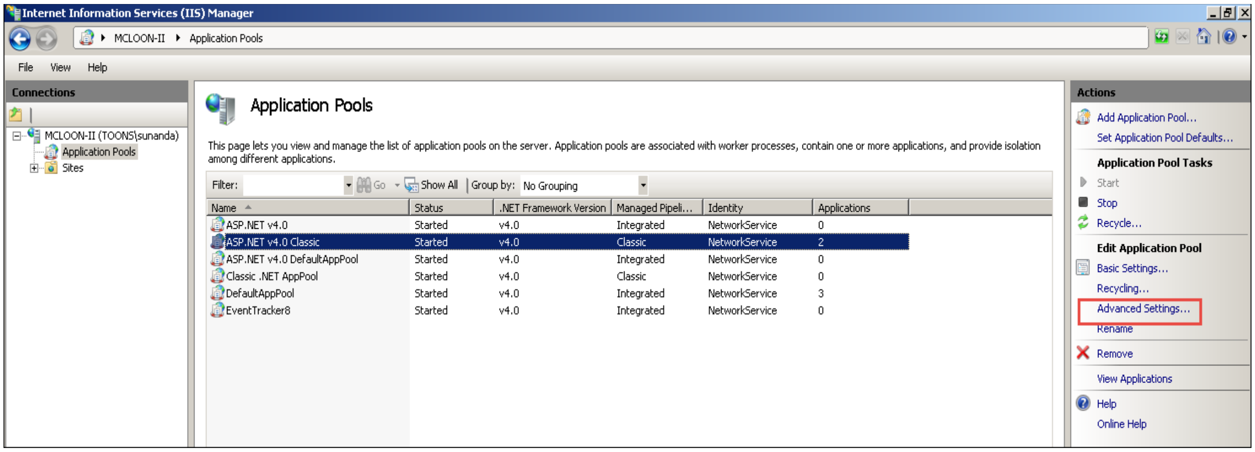


Figure 18

3. Select the **Application Pool** node available in the left pane and select **ASP .NET v4.0 Classic**.
4. Select the option **Advanced Settings…** in the Action pane as shown in the figure below:

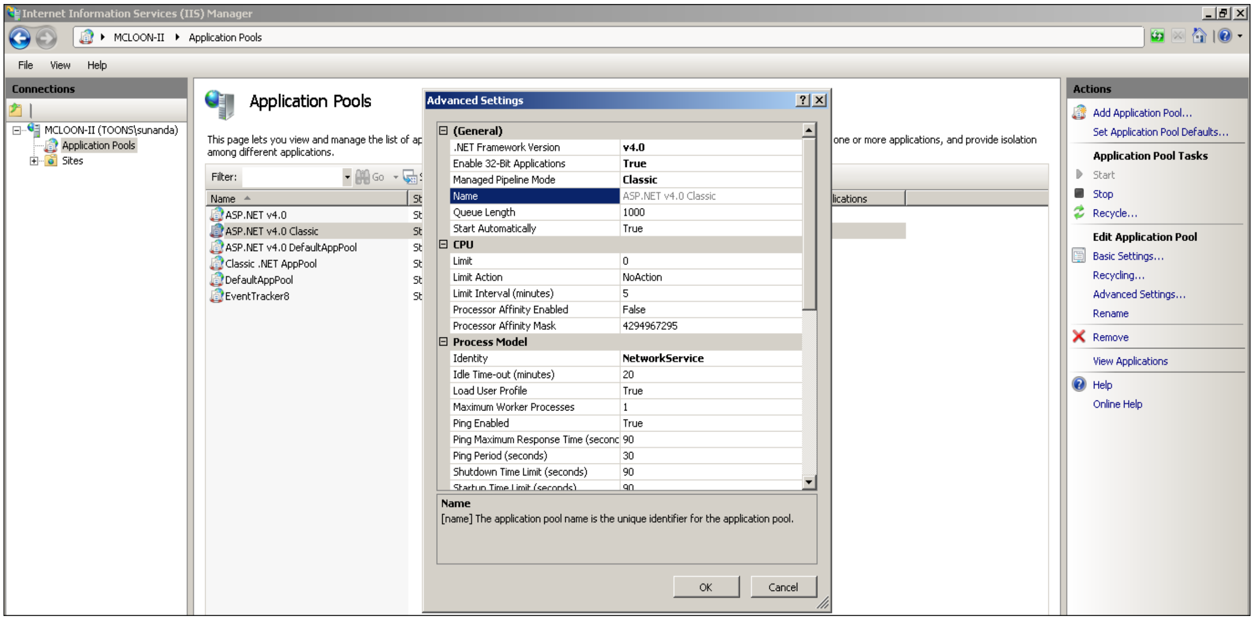


This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

Name	Status	.NET Framework Version	Managed Pipeli...	Identity	Applications
ASP.NET v4.0	Started	v4.0	Integrated	NetworkService	0
ASP.NET v4.0 Classic	Started	v4.0	Classic	NetworkService	2
ASP.NET v4.0 DefaultAppPool	Started	v4.0	Integrated	NetworkService	0
Classic .NET AppPool	Started	v4.0	Classic	NetworkService	0
DefaultAppPool	Started	v4.0	Integrated	NetworkService	3
EventTracker8	Started	v4.0	Integrated	NetworkService	0

Figure 19

The Advanced Settings window opens.



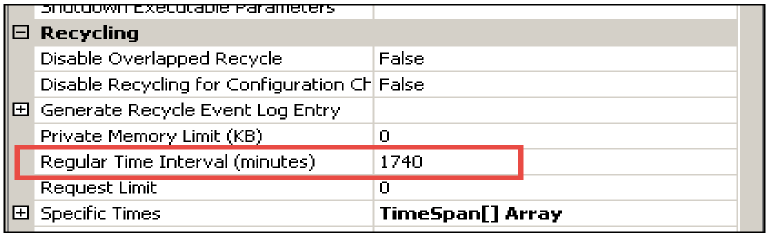
Advanced Settings

(General)	
.NET Framework Version	**v4.0**
Enable 32-Bit Applications	**True**
Managed Pipeline Mode	**Classic**
Name	ASP.NET v4.0 Classic
Queue Length	1000
Start Automatically	True
CPU	
Limit	0
Limit Action	NoAction
Limit Interval (minutes)	5
Processor Affinity Enabled	False
Processor Affinity Mask	4294967295
Process Model	
Identity	**NetworkService**
Idle Time-out (minutes)	20
Load User Profile	True
Maximum Worker Processes	1
Ping Enabled	True
Ping Maximum Response Time (seconc	90
Ping Period (seconds)	30
Shutdown Time Limit (seconds)	90
Startup Time Limit (seconds)	90

Name
[name] The application pool name is the unique identifier for the application pool.

Figure 20

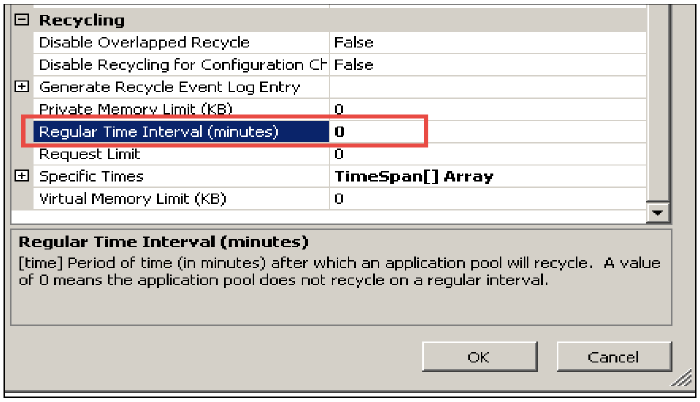
5. In the Recycling pane, the **Regular Time Interval (Minutes)** is **1740** (29 hours) by default.



Shutdown Executable Parameters	
Recycling	
Disable Overlapped Recycle	False
Disable Recycling for Configuration Ch	False
Generate Recycle Event Log Entry	
Private Memory Limit (KB)	0
Regular Time Interval (minutes)	1740
Request Limit	0
Specific Times	**TimeSpan[] Array**

Figure 21

6. Change it to 0 (Zero) and save the configuration and click **OK**.



Recycling	
Disable Overlapped Recycle	False
Disable Recycling for Configuration Ch	False
Generate Recycle Event Log Entry	
Private Memory Limit (KB)	0
Regular Time Interval (minutes)	**0**
Request Limit	0
Specific Times	**TimeSpan[] Array**
Virtual Memory Limit (KB)	0

Regular Time Interval (minutes)
[time] Period of time (in minutes) after which an application pool will recycle. A value of 0 means the application pool does not recycle on a regular interval.

Figure 22

7. Now, Reset the **IIS** and login to **EventTracker** web.
8. Click the **Tear Away** icon ☐.

9. Ensure you are in the News Page, for the tear away window to refresh every minute.

1.10 Updating EventTracker Users List

This option helps you in updating the EventTracker configuration, if

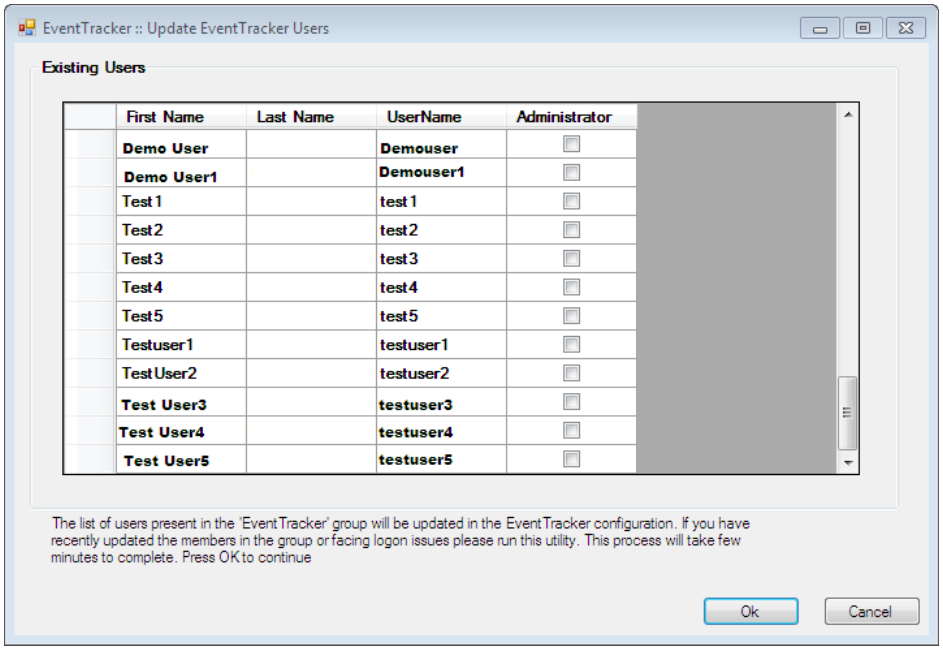
- New users are added to the "EventTracker" user group
- You face Log on issues

1.10.1 Updating Users List

1 Click **Start,** select **All Programs,** and then select **Prism Microsystems.**

2 Select **EventTracker,** and then select **Update Users List**.

EventTracker opens **Update EventTracker** Users console.



EventTracker :: Update EventTracker Users

Existing Users

First Name	Last Name	UserName	Administrator
Demo User		Demouser	□
Demo User1		Demouser1	□
Test1		test1	□
Test2		test2	□
Test3		test3	□
Test4		test4	□
Test5		test5	□
Testuser1		testuser1	□
TestUser2		testuser2	□
Test User3		testuser3	□
Test User4		testuser4	□
Test User5		testuser5	□

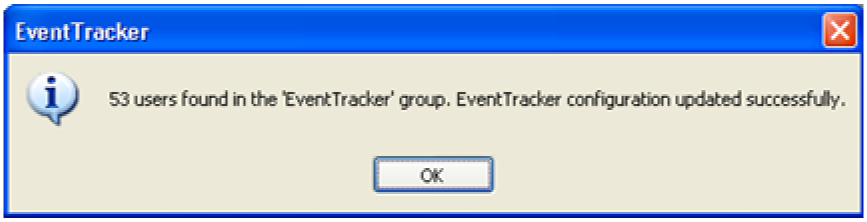
The list of users present in the 'EventTracker' group will be updated in the EventTracker configuration. If you have recently updated the members in the group or facing logon issues please run this utility. This process will take few minutes to complete. Press OK to continue

Figure 23

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 **Error! Reference source not found.** section.

3 Click **Ok**.

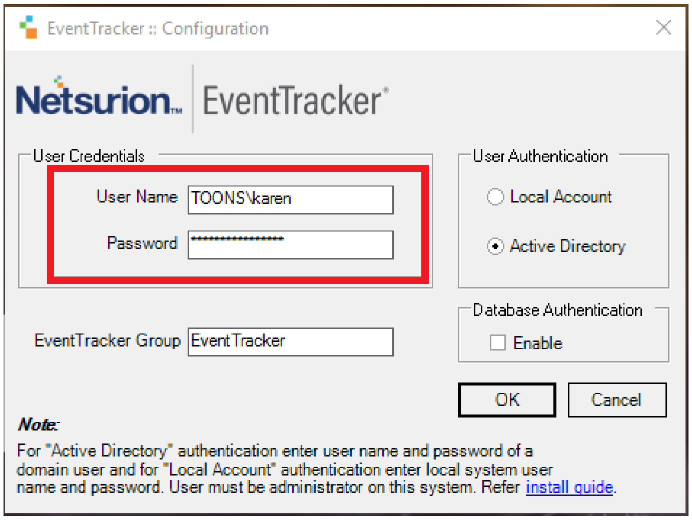
EventTracker updates 'EventTracker Configuration' and the success message appears.



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

Figure 24

NOTE:
If the user with which EventTracker Configuration runs has changed the password, it is mandatory to re-run the EventTracker Configuration with the updated password.



User Credentials

User Name: TOONS\karen

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

User Authentication

○ Local Account

● Active Directory

Database Authentication

□ Enable

EventTracker Group: EventTracker

Note:
For "Active Directory" authentication enter user name and password of a domain user and for "Local Account" authentication enter local system user name and password. User must be administrator on this system. Refer install guide.

Figure 25

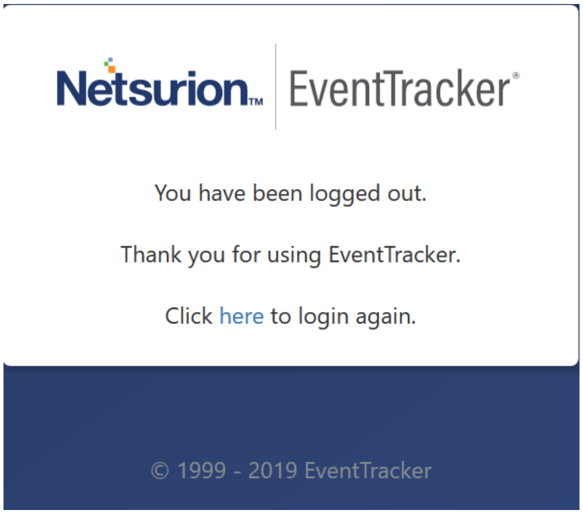
1. To find '**EventTracker Configuration'**, click **Start**, select All **Programs**.
2. Select **Prism Microsystems**, select **EventTracker**, and then select **EventTracker Configuration.**
3. Enter appropriate credentials and then select **OK.**

1.11 Exiting EventTracker

This option enables you to log out of EventTracker.

A) To exit EventTracker, click Log out .

To logs out of EventTracker.



You have been logged out.

Thank you for using EventTracker.

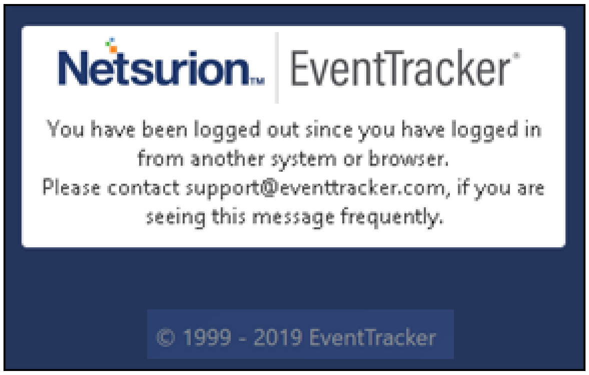
Click here to login again.

© 1999 - 2019 EventTracker

Figure 26

🗎 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.



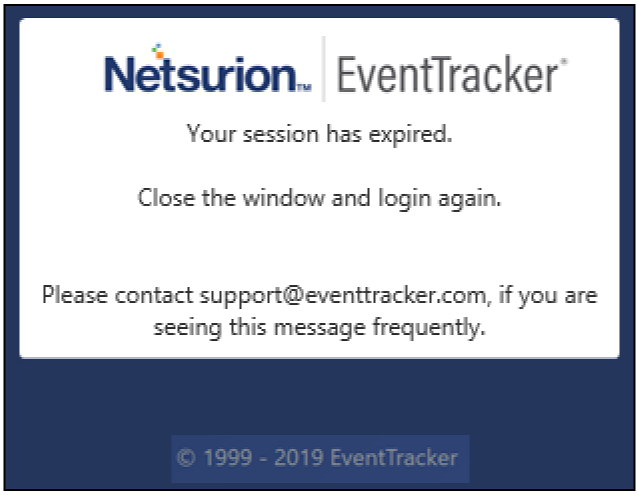
You have been logged out since you have logged in from another system or browser.
Please contact support@eventtracker.com, if you are seeing this message frequently.

© 1999 - 2019 EventTracker

Figure 27

🗎 NOTE

When there is no user interaction for a specified period, EventTracker logs out the user.



Your session has expired.

Close the window and login again.

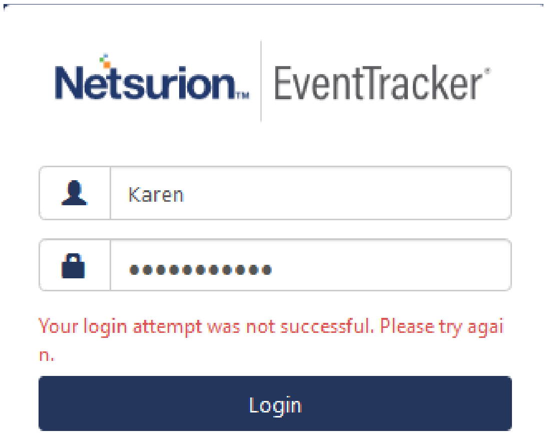
Please contact support@eventtracker.com, if you are seeing this message frequently.

© 1999 - 2019 EventTracker

Figure 28

🗎 NOTE

EventTracker denies access, when a user tries to log on without appropriate access permissions and privileges.



Karen

●●●●●●●●●●●

Your login attempt was not successful. Please try agai n.

Figure 29

2. Dashboard

In this chapter, you will learn about:

- Home
- My Dashboard
- Threats
  - Attacks and Targets
  - Processes
- Incidents
- Machine Learning
- Change Audit
- Compliance

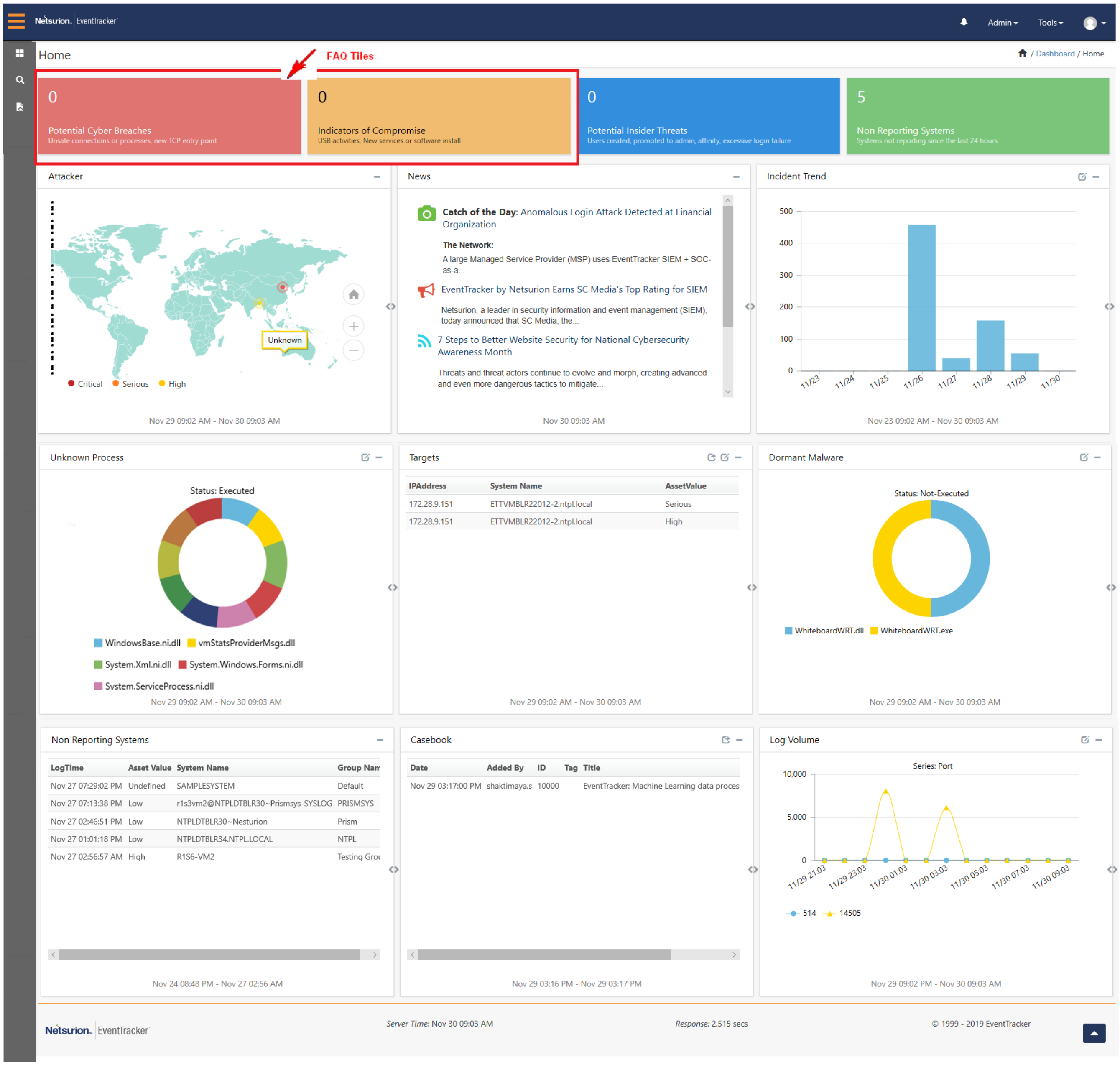
2.1 Overview of the Home Dashboard

Home Dashboard displays the below widgets by default:

- Incidents trend
- Attackers map
- Unknown/dormant malware
- Targets
- Non-reporting systems
- Casebook
- Log volume trend

NOTE: Edit option is not available for some of the custom dashlets such as Attackers, non-reporting system, and Casebook.

The user can re-arrange the dashlets as per requirement; make configuration changes by clicking the edit dashlet ✎ and can even click any of the interesting graphs for more information on the same.



Catch of the Day: Anomalous Login Attack Detected at Financial Organization

The Network:

A large Managed Service Provider (MSP) uses EventTracker SIEM + SOC-as-a...

EventTracker by Netsurion Earns SC Media's Top Rating for SIEM

Netsurion, a leader in security information and event management (SIEM), today announced that SC Media, the...

7 Steps to Better Website Security for National Cybersecurity Awareness Month

Threats and threat actors continue to evolve and morph, creating advanced and even more dangerous tactics to mitigate...

IPAddress	System Name	AssetValue
172.28.9.151	ETTVMBLR22012-2.ntpl.local	Serious
172.28.9.151	ETTVMBLR22012-2.ntpl.local	High

LogTime	Asset Value	System Name	Group Nam
Nov 27 07:29:02 PM	Undefined	SAMPLESYSTEM	Default
Nov 27 07:13:38 PM	Low	r1s3vm2@NTPLDTBLR30~Prismsys-SYSLOG	PRISMSYS
Nov 27 02:46:51 PM	Low	NTPLDTBLR30~Nesturion	Prism
Nov 27 01:01:18 PM	Low	NTPLDTBLR34.NTPL.LOCAL	NTPL
Nov 27 02:56:57 AM	High	R1S6-VM2	Testing Grou

Date	Added By	ID	Tag	Title
Nov 29 03:17:00 PM	shaktimaya.s	10000		EventTracker: Machine Learning data proces

Figure 30

2.2 Overview of My Dashboard

This option helps to view quick statistics and graphs like trend of events based on any flex persisted data. My dashboard is an enhanced feature, where the dashboard can be configured as well as customized according to user preferences.

With the introduction of CIM model, all the logs/events are now normalized and mapped to common schema for the last 7 days.

For Example: Just search with “**tags:"login failed"**” to get login failure results from any source (VPN, Active Directory, Firewall etc.) without worrying about event id or any other property.

2.2.1 Creating a Dashboard

1. To view My Dashboard, click **Dashboard**, and select **My Dashboard** from the dropdown list.
2. To add a dashboard, click add ⊕.

   EventTracker opens the Custom dashboard window.

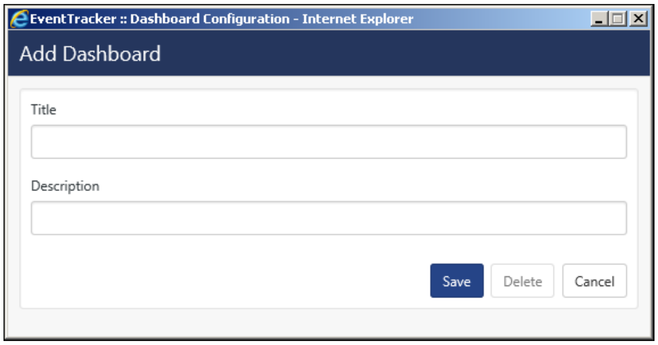


Figure 31

3. Enter Title and Description and click **Save**.
4. The customized dashboard gets added and is displayed.

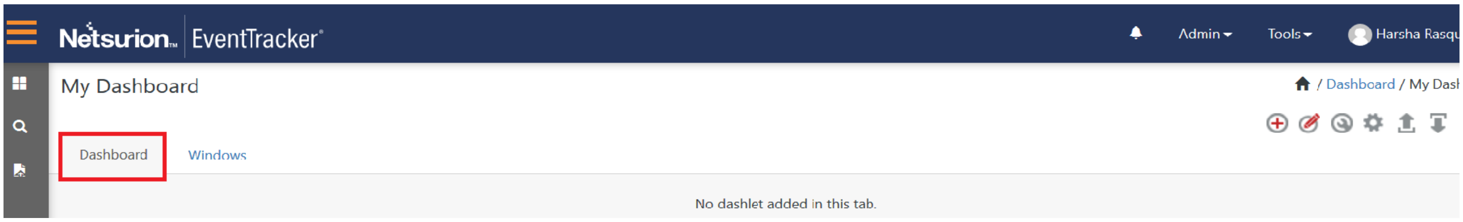
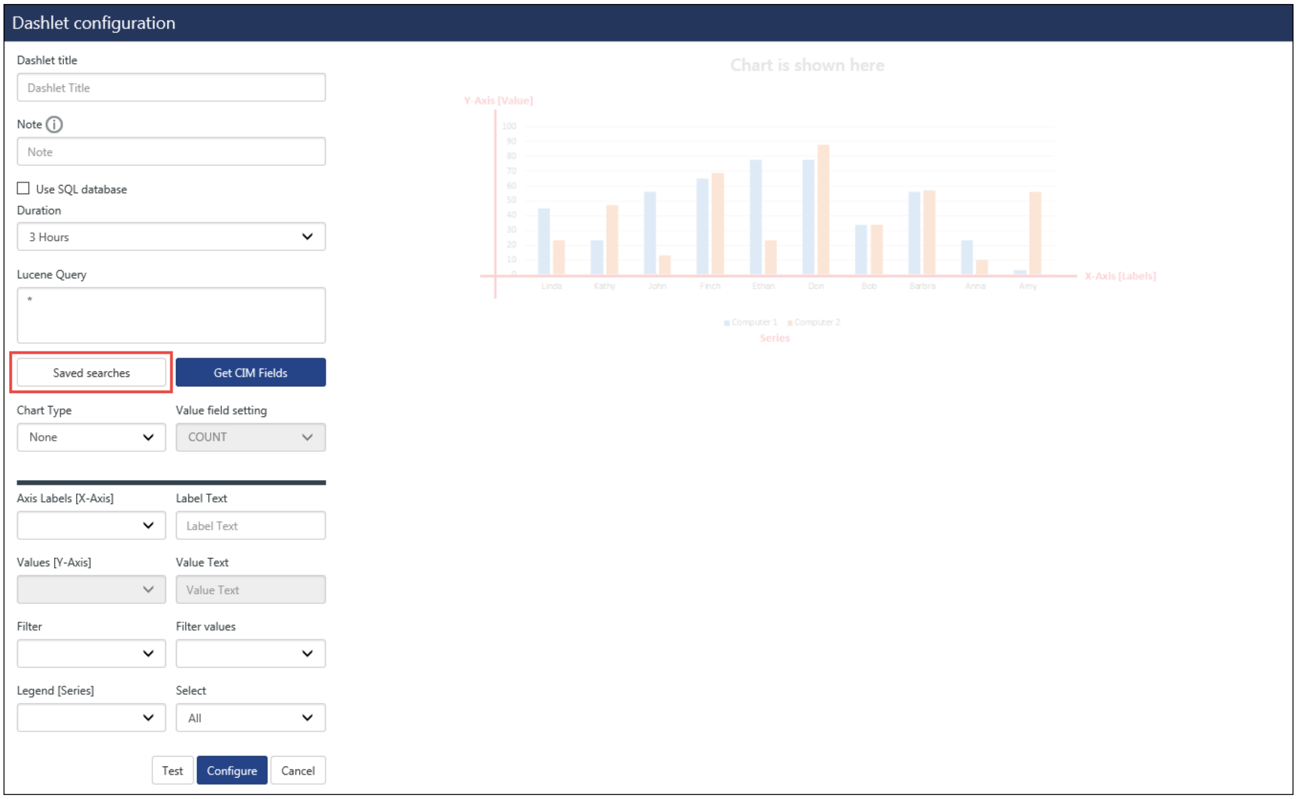


Figure 32

2.2.2 Configuring a Dashlet

1. For configuring a widget based on Flex persisted report, click **configure** ⚙.

   The Dashlet configuration page opens.



Dashlet configuration

Dashlet title: Dashlet Title

Note ⓘ: Note

☐ Use SQL database

Duration: 3 Hours

Lucene Query: *

Chart Type: None

Value field setting: COUNT

Axis Labels [X-Axis]:

Label Text: Label Text

Values [Y-Axis]:

Value Text: Value Text

Filter:

Filter values:

Legend [Series]:

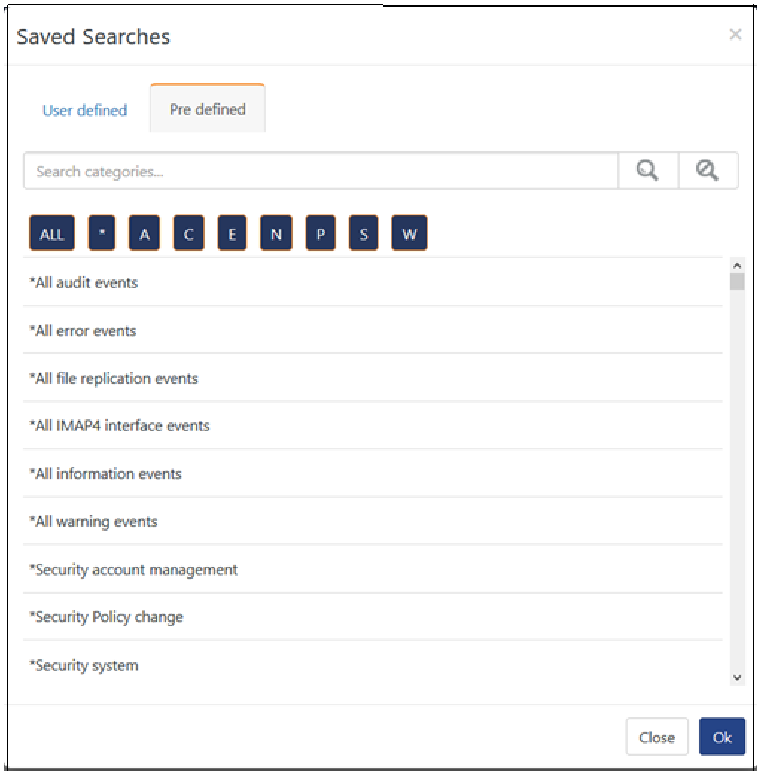
Select: All

Figure 33

Field	Implies
Dashlet Title	Enter the Dashlet Title
Use SQL Database	Check this if reports are to be fetched from Database.
Lucene Query	To create your own queries through its API and get the CIM fields.
Chart type	Select the graphical view option
Value field settings	Select from count/sum/average
Axis labels (X-axis)/ Values (Y-axis)	Plot the values from the dropdown options for the respective axis.
As of	Select the reports for Now/Recent.
Filtered Values	Select the values as per your requirement.
Legend	Select the series.

The user can create widgets from the pre-defined saved searches available.

a. Click **Save searches** as highlighted in the figure above.



Saved Searches

*All audit events

*All error events

*All file replication events

*All IMAP4 interface events

*All information events

*All warning events

*Security account management

*Security Policy change

*Security system

Figure 34

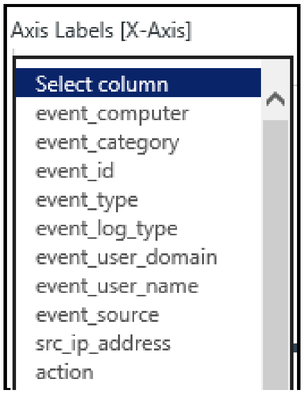
b. Select from the available list and then click **OK**.

c. Enter the required details and configure a widget for the selected saved search.

2.2.3 Creating a Dashlet using CIM fields

1. Enter the dashlet title, select the duration and click the **Get CIM fields** option. It will populate the CIM fields as a dropdown for the available options.

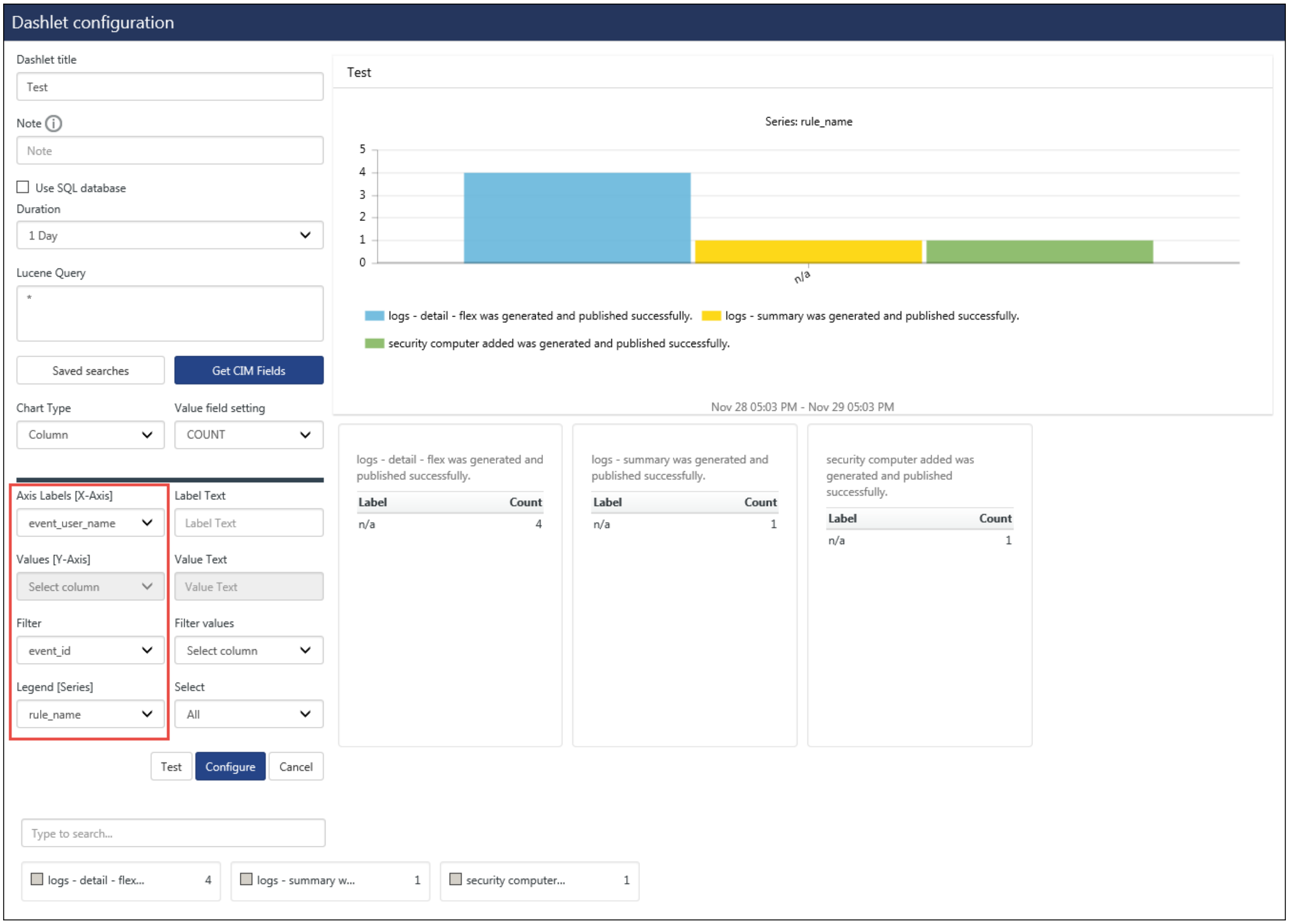
   For example: **Axis Labels: X-Axis**



Axis Labels [X-Axis]

Figure 35

2. Select the required fields from the available options and plot the graph for the widget.


Test
Series: rule_name
5
4
3
2
1
0
n/a
🟦 logs - detail - flex was generated and published successfully.
🟨 logs - summary was generated and published successfully.
🟩 security computer added was generated and published successfully.
Nov 28 05:03 PM - Nov 29 05:03 PM

Dashlet configuration

Dashlet title: Test

Note: Note

☐ Use SQL database

Duration: 1 Day

Lucene Query: *

Saved searches | Get CIM Fields

Chart Type: Column

Value field setting: COUNT

Axis Labels [X-Axis]: event_user_name

Label Text: Label Text

Values [Y-Axis]: Select column

Value Text: Value Text

Filter: event_id

Filter values: Select column

Legend [Series]: rule_name

Select: All

Test | Configure | Cancel

logs - detail - flex was generated and published successfully.

Label	Count
n/a	4

logs - summary was generated and published successfully.

Label	Count
n/a	1

security computer added was generated and published successfully.

Label	Count
n/a	1

Type to search...

☐ logs - detail - flex... 4 ☐ logs - summary w... 1 ☐ security computer... 1

Figure 36

3. Click **Test**.
   Verify the changes and click **Configure** to create the widget.

Now, for adding dashlets to the dashboard, click customize .

4. Select the configured widget and click **Add**.
   It is displayed in the Dashboard.

2.2.4 Creating a Dashlet using SQL Database

1. **Dashlet Title :** Flex Dashboard

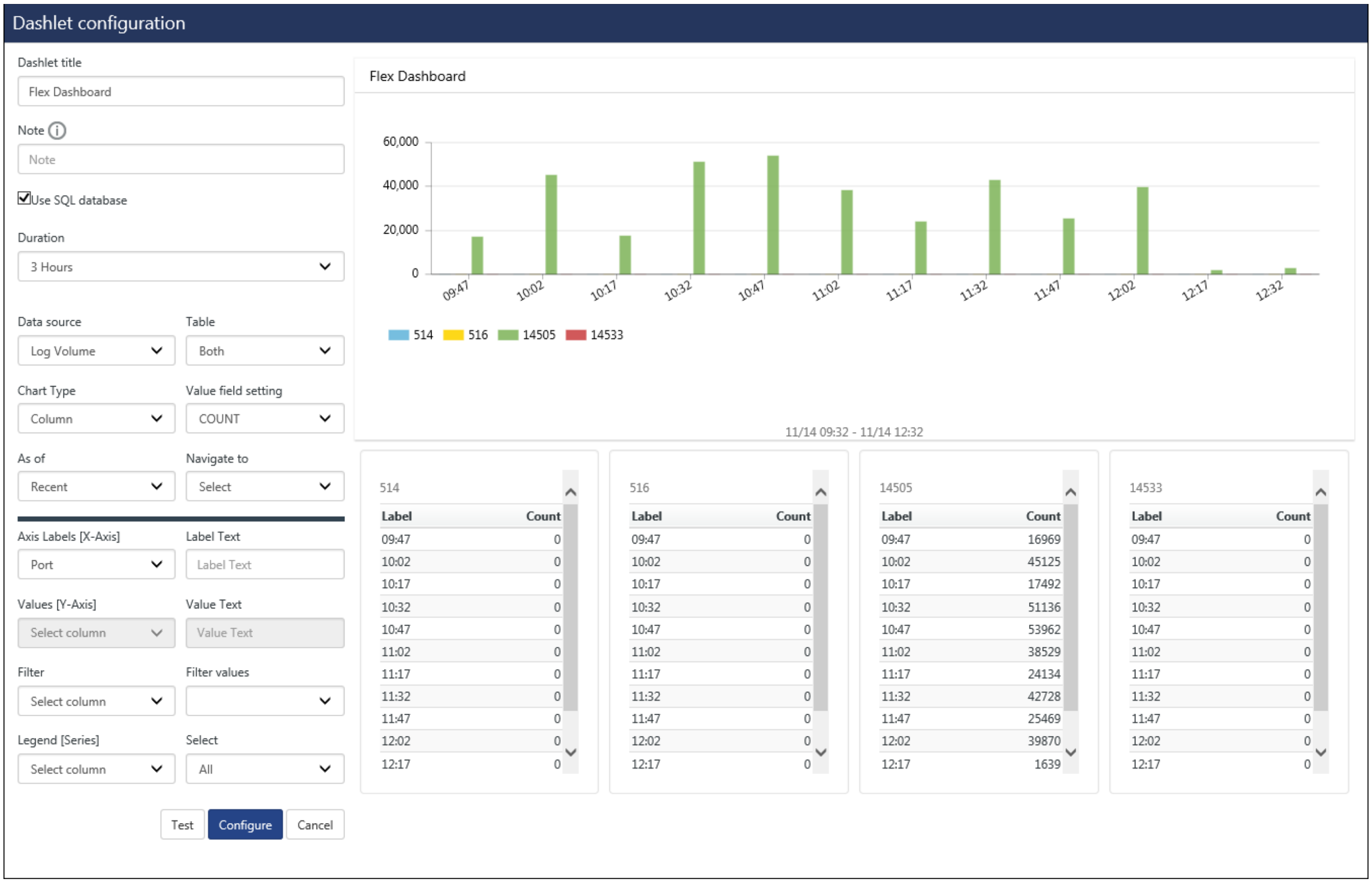
The **Use SQL Database** option is checked.

2. **Duration:** 3 hours
3. **Data source**: Log Volume
4. **Table**: Both
5. **Chart Type**: Column
6. **Axis labels (X-axis):** Port
7. In **Value field settings**: select from count/sum/average.

NOTE: The Values (Y-Axis) is disabled for the **Value Field Settings**: Count.

The available values is shown.

8. Click **Test**.



Dashlet title: Flex Dashboard

Note: Note

☑ Use SQL database

Duration: 3 Hours

Data source: Log Volume

Table: Both

Chart Type: Column

Value field setting: COUNT

As of: Recent

Navigate to: Select

Axis Labels [X-Axis]: Port

Label Text: Label Text

Values [Y-Axis]: Select column

Value Text: Value Text

Filter: Select column

Filter values:

Legend [Series]: Select column

Select: All

514

Label	Count
09:47	0
10:02	0
10:17	0
10:32	0
10:47	0
11:02	0
11:17	0
11:32	0
11:47	0
12:02	0
12:17	0

516

Label	Count
09:47	0
10:02	0
10:17	0
10:32	0
10:47	0
11:02	0
11:17	0
11:32	0
11:47	0
12:02	0
12:17	0

14505

Label	Count
09:47	16969
10:02	45125
10:17	17492
10:32	51136
10:47	53962
11:02	38529
11:17	24134
11:32	42728
11:47	25469
12:02	39870
12:17	1639

14533

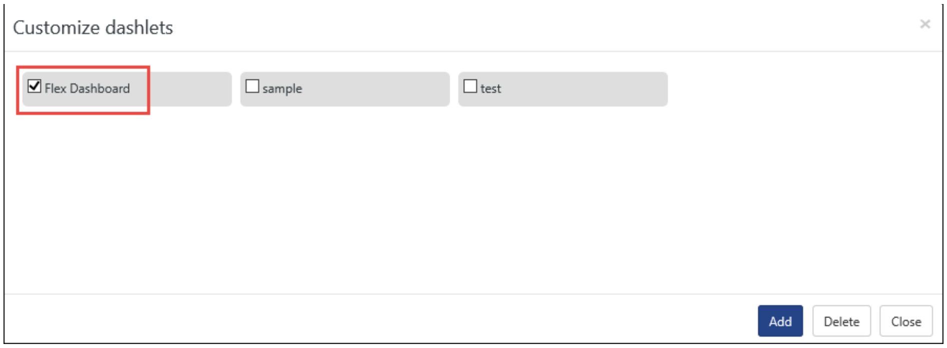
Label	Count
09:47	0
10:02	0
10:17	0
10:32	0
10:47	0
11:02	0
11:17	0
11:32	0
11:47	0
12:02	0
12:17	0

Figure 37

9. The Label with the counts gets displayed and the graph is also available.
10. After previewing the configured details, click **Configure**.

Now, for adding flex dashlets, click the customize icon .

11. Select the configured widget and click **Add**.

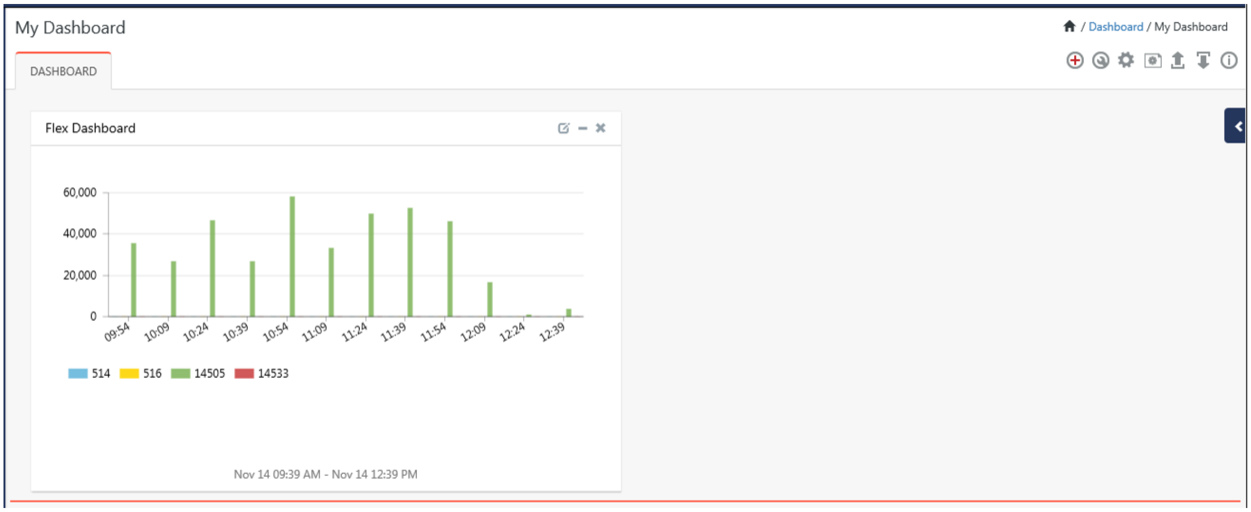


Customize dashlets

☑ Flex Dashboard □ sample □ test

Figure 38

The Dashlet gets added in your **Dashboard** tab titled as” Flex Dashboard”.



My Dashboard

Nov 14 09:39 AM - Nov 14 12:39 PM

Figure 39

12. Click on the graph to view the refined data.

Similarly, you can plot graph for **Chart Type**: Line/Donut/Stacked and Meter gauge and add them to your custom dashboard.

NOTE: You can create multiple dashboards and can add Customized dashlets. You can even re-arrange the dashboards according to requirements.

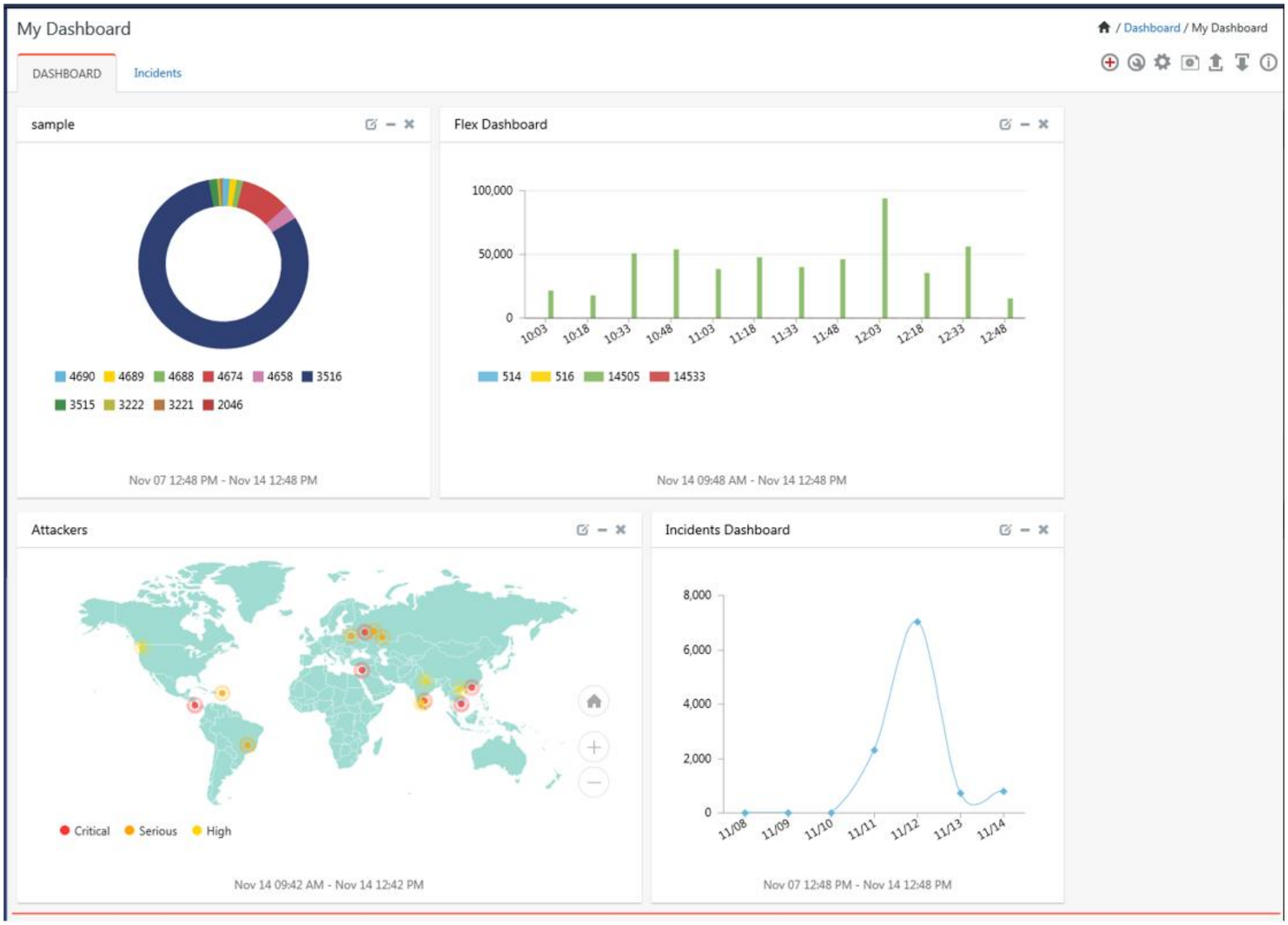


Figure 40

For Example:

There are two machines where Linux agent is installed, and it is forwarding samples every two seconds to the EventTracker. Now if the user wants to visualize Average Dist Queue length, following widget can be configured on the dashboard by selecting appropriate data source.

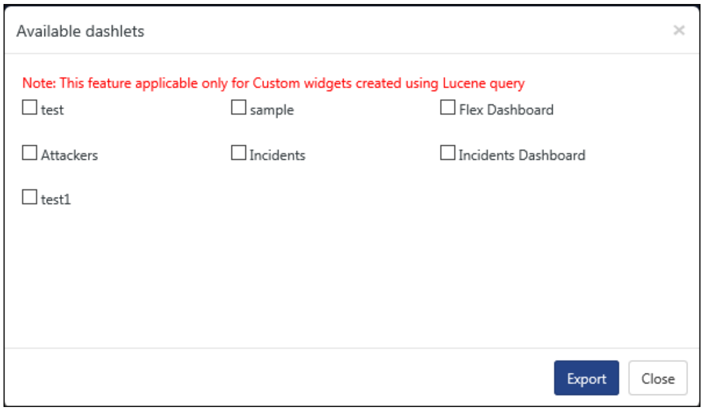
Chart Type	Function	X-Axis	Y-Axis	Legend
Meter gauge	Average(Default Select)	N/A	Avg. Disk queue length	Computer

Table 11

2.2.5 Exporting Dashlets

The configured Dashlet can be exported to excel format.

1) Click **Export** .
2) Select the dashlets to be exported and click **Export**.



Available dashlets

Note: This feature applicable only for Custom widgets created using Lucene query

□ test □ sample □ Flex Dashboard

□ Attackers □ Incidents □ Incidents Dashboard

□ test1

Figure 41

2.2.6 Importing Dashlets

1. Click **Import** . Browse the file and click **Import**.
   The dashlet gets imported.

   For more information on the Dashlet configuration, click **info** .

2.3 Attackers pane and Targets pane

2.3.1 Attackers pane

An IP address earns a negative reputation when it is found with suspicious activity, such as spam or viruses originating from that address. It is strongly recommended to perform a security audit on any of the systems that correspond to an IP address with a negative reputation, as those systems may have been compromised. Reputation score are measured from 0 to 100 and more the score more suspicious and dangerous it is.

Presently, EventTracker uses the services provided by **IP Void**, **IBM XFE and Borderware** to locate the Blacklisted IPs.

2.3.2 Targets pane

With the advent of the feature "Attackers" where the bad reputation IPs is pinned on the geolocation, it becomes necessary to display the information as to where these bad IPs have ventured into the network. The targets feature will suffice the requirement, displaying those targets within the enterprise which are being attacked, along with the details like-How (Port/Protocol), By Whom (IP/Host Name) and When/ How often.

There are two different ways of looking at same pair table data. The user can view it from the attacker dashboard - "who is attacking/how/what port" or from the targets dashboard- "what is being attacked/by who/which port".

In both the cases, user plays the defender - job where he can protect the assets, react in a timely way and defend in a proper manner.

For Geo-location, EventTracker is using the **IP Void** and **MaxMind GeoLite**.

NOTE: Attackers Dashboard feature uses the following websites:

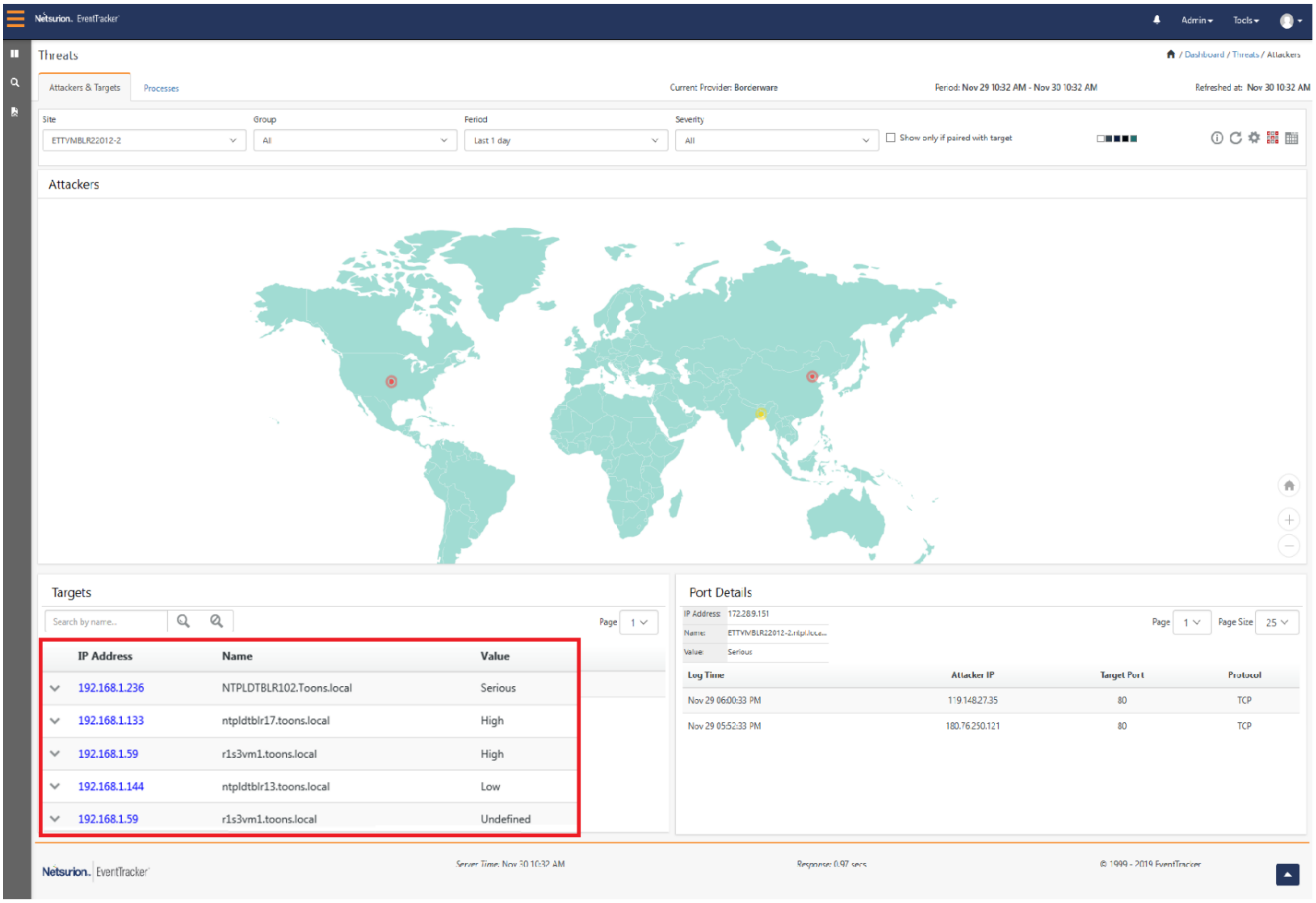
- **IP void**
- **IBM XFE**
- **Borderware**
- **IP Info**

NOTE:

- To get data populated on the Attackers Dashboard, access needs to be provided for these websites. Make sure that the above URLs are excluded from firewall.

For viewing the targets that has been attacked, scroll down to the **Targets** pane, as shown in the figure below:

The Targets will be shown in the left pane and the Port Details will be shown in the right pane.



Threats

🏠 / Dashboard / Threats / Attackers

Attackers & Targets | Processes

Current Provider: Borderware

Period: Nov 29 10:32 AM - Nov 30 10:32 AM

Refreshed at: Nov 30 10:32 AM

Site: ETTVMBLR22012-2 | Group: All | Period: Last 1 day | Severity: All | □ Show only if paired with target

Attackers

Targets

Search by name... | Page 1

	IP Address	Name	Value
⌄	192.168.1.236	NTPLDTBLR102.Toons.local	Serious
⌄	192.168.1.133	ntpldtblr17.toons.local	High
⌄	192.168.1.59	r1s3vm1.toons.local	High
⌄	192.168.1.144	ntpldtblr13.toons.local	Low
⌄	192.168.1.59	r1s3vm1.toons.local	Undefined

Port Details

IP Address: 172.28.9.151
Name: ETTVMBLR22012-2.ntpl.loca...
Value: Serious

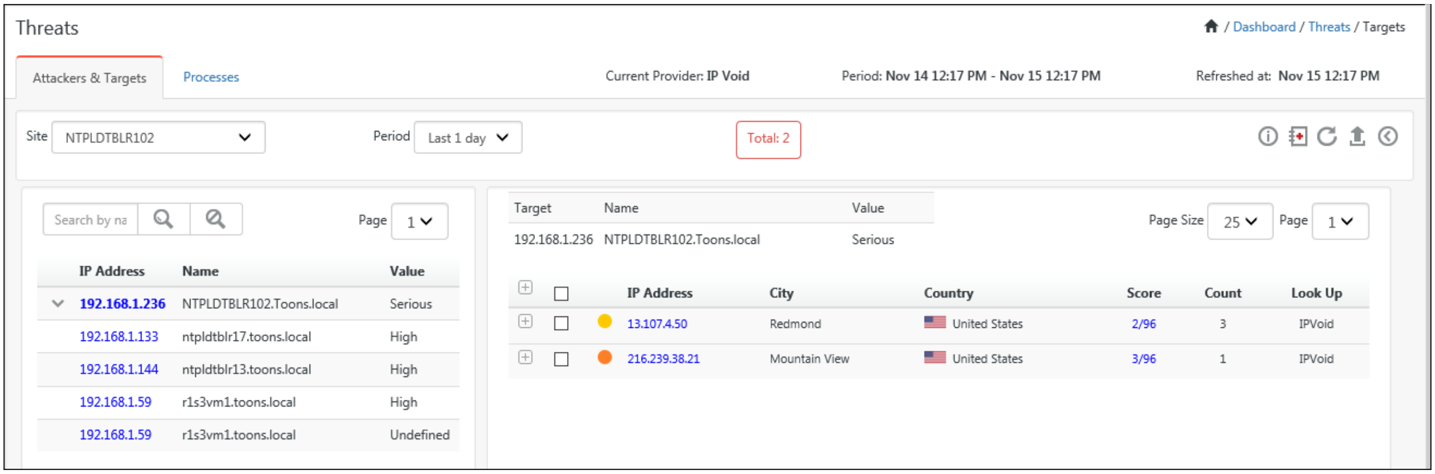
Page 1 | Page Size 25

Log Time	Attacker IP	Target Port	Protocol
Nov 29 06:00:33 PM	119.148.27.35	80	TCP
Nov 29 05:52:33 PM	180.76.250.121	80	TCP

Netsurion. EventTracker | Server Time: Nov 30 10:32 AM | Response: 0.97 secs | © 1999 - 2019 EventTracker

Figure 42

To view the Target data in detail, click the icon ▦.



Threats

🏠 / Dashboard / Threats / Targets

Attackers & Targets | Processes

Current Provider: IP Void

Period: Nov 14 12:17 PM - Nov 15 12:17 PM

Refreshed at: Nov 15 12:17 PM

Site: NTPLDTBLR102 | Period: Last 1 day | Total: 2

Search by na | Page 1

	IP Address	Name	Value
⌄	192.168.1.236	NTPLDTBLR102.Toons.local	Serious
	192.168.1.133	ntpldtblr17.toons.local	High
	192.168.1.144	ntpldtblr13.toons.local	High
	192.168.1.59	r1s3vm1.toons.local	High
	192.168.1.59	r1s3vm1.toons.local	Undefined

Target	Name	Value
192.168.1.236	NTPLDTBLR102.Toons.local	Serious

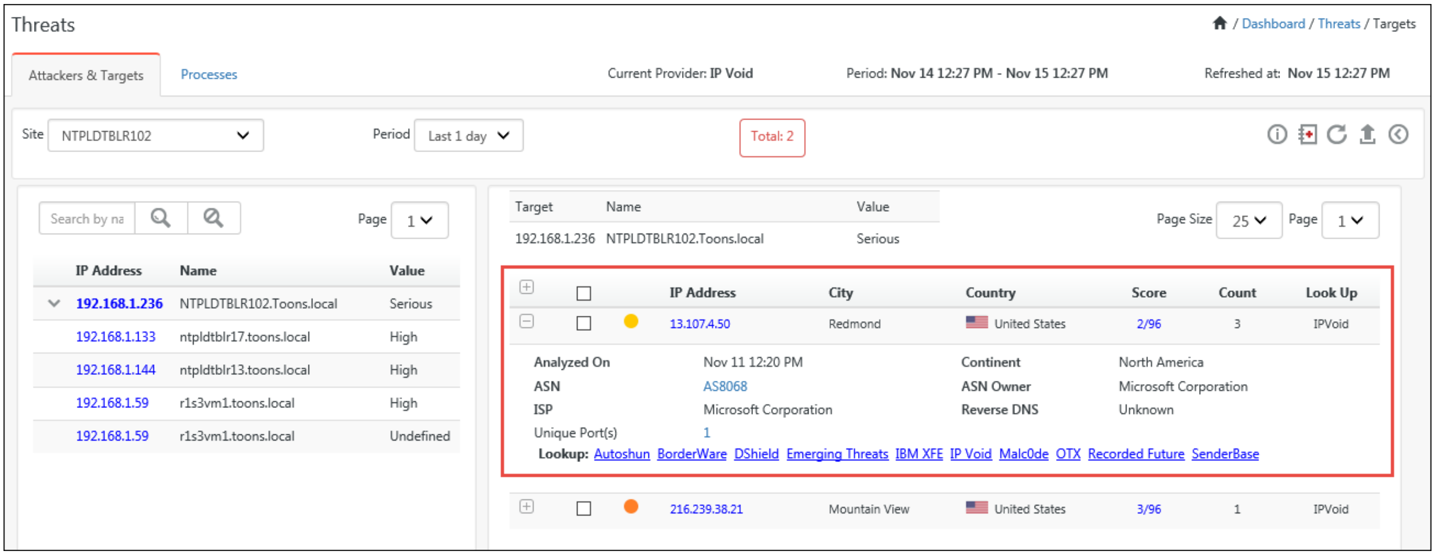
Page Size 25 | Page 1

⊞	□		IP Address	City	Country	Score	Count	Look Up
⊞	□	●	13.107.4.50	Redmond	United States	2/96	3	IPVoid
⊞	□	●	216.239.38.21	Mountain View	United States	3/96	1	IPVoid

Figure 43

The targets will show the attacks happening on the systems in the form of a pair table. The left pane will list down the multiple targets with their asset value and host name (if any). The respective attackers will be listed down in the right pane along with the critical reputation information.

To view other information related to the attackers in the Target dashboard, navigate to the right pane and click the icon ⊞ .



Threats

🏠 / Dashboard / Threats / Targets

Attackers & Targets | Processes

Current Provider: IP Void   Period: Nov 14 12:27 PM - Nov 15 12:27 PM   Refreshed at: Nov 15 12:27 PM

Site NTPLDTBLR102   Period Last 1 day   Total: 2

Search by na   Page 1

	IP Address	Name	Value
⌄	192.168.1.236	NTPLDTBLR102.Toons.local	Serious
	192.168.1.133	ntpldtblr17.toons.local	High
	192.168.1.144	ntpldtblr13.toons.local	High
	192.168.1.59	r1s3vm1.toons.local	High
	192.168.1.59	r1s3vm1.toons.local	Undefined

Target	Name	Value
192.168.1.236	NTPLDTBLR102.Toons.local	Serious

Page Size 25   Page 1

			IP Address	City	Country	Score	Count	Look Up
⊟	□	●	13.107.4.50	Redmond	United States	2/96	3	IPVoid

Analyzed On	Nov 11 12:20 PM	Continent	North America
ASN	AS8068	ASN Owner	Microsoft Corporation
ISP	Microsoft Corporation	Reverse DNS	Unknown
Unique Port(s)	1		

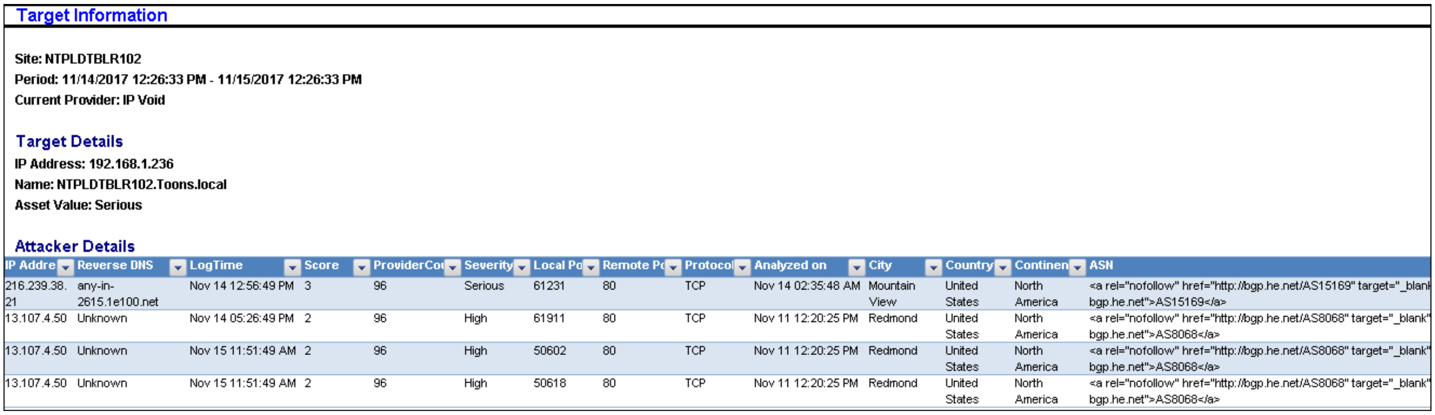
Lookup: Autoshun BorderWare DShield Emerging Threats IBM XFE IP Void Malc0de OTX Recorded Future SenderBase

			IP Address	City	Country	Score	Count	Look Up
⊞	□	●	216.239.38.21	Mountain View	United States	3/96	1	IPVoid

Figure 44

The user can further perform a Log Search Pair/Log Search Target for a respective target.

The target information can further be saved in the excel formal by click **Export** ⬆.



Target Information

Site: NTPLDTBLR102
Period: 11/14/2017 12:26:33 PM - 11/15/2017 12:26:33 PM
Current Provider: IP Void

Target Details

IP Address: 192.168.1.236
Name: NTPLDTBLR102.Toons.local
Asset Value: Serious

Attacker Details

IP Addre	Reverse DNS	LogTime	Score	ProviderCou	Severity	Local Po	Remote Po	Protocol	Analyzed on	City	Country	Continen	ASN
216.239.38.21	any-in-2615.1e100.net	Nov 14 12:56:49 PM	3	96	Serious	61231	80	TCP	Nov 14 02:35:48 AM	Mountain View	United States	North America	<a rel="nofollow" href="http://bgp.he.net/AS15169" target="_blank bgp.he.net">AS15169</a>
13.107.4.50	Unknown	Nov 14 05:26:49 PM	2	96	High	61911	80	TCP	Nov 11 12:20:25 PM	Redmond	United States	North America	<a rel="nofollow" href="http://bgp.he.net/AS8068" target="_blank" bgp.he.net">AS8068</a>
13.107.4.50	Unknown	Nov 15 11:51:49 AM	2	96	High	50602	80	TCP	Nov 11 12:20:25 PM	Redmond	United States	North America	<a rel="nofollow" href="http://bgp.he.net/AS8068" target="_blank" bgp.he.net">AS8068</a>
13.107.4.50	Unknown	Nov 15 11:51:49 AM	2	96	High	50618	80	TCP	Nov 11 12:20:25 PM	Redmond	United States	North America	<a rel="nofollow" href="http://bgp.he.net/AS8068" target="_blank" bgp.he.net">AS8068</a>

Figure 45

2.3.3 List of URLs for firewall proxy exclusion

1. https://api.xforce.ibmcloud.com/
2. http://ipinfo.io/

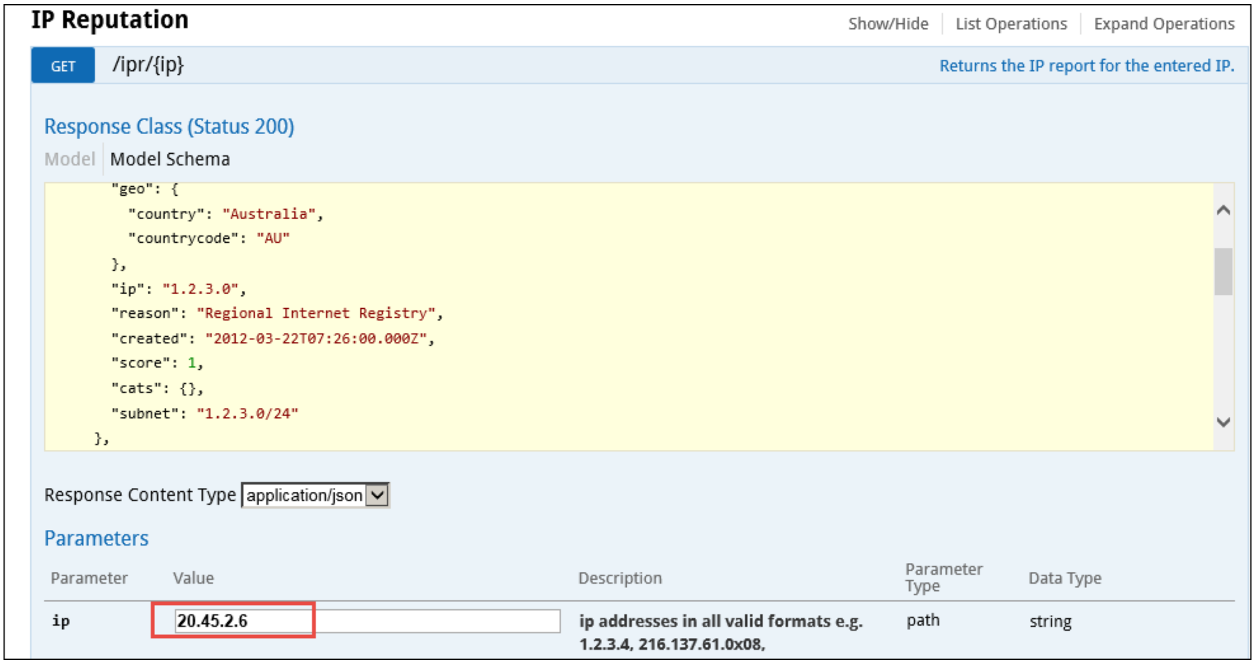
In Attackers,

1. http://www.ipvoid.com/
2. http://list.iblocklist.com/
3. http://www.borderware.com/
4. https://www.dshield.org/
5. https://rules.emergingthreats.net/
6. https://www.autoshun.org/files/
7. https://otx.alienvault.com/
8. https://www.senderbase.org/
9. http://certificates.eventtracker.com/

2.3.3.1 If the user tries to use the IP reputation provider "IBM-XFE", but the IP fails to resolve,

Follow the below mentioned steps:

1. Click the link: https://api.xforce.ibmcloud.com/doc/
2. Expand the **IP Reputation** option.
3. Click on **GET /ipr/{IP}**
4. In the **IP** field, enter the IP Address, as shown in the figure below:



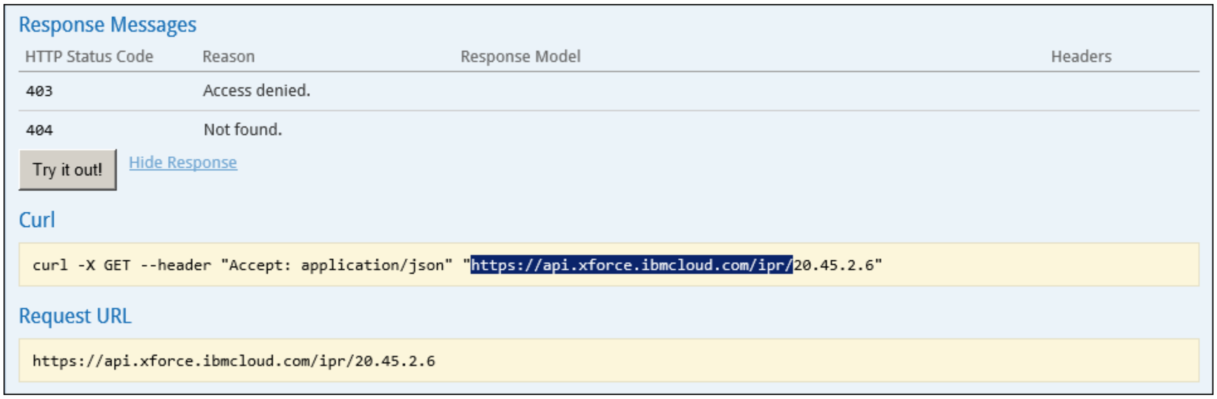
```
        "geo": {
          "country": "Australia",
          "countrycode": "AU"
        },
        "ip": "1.2.3.0",
        "reason": "Regional Internet Registry",
        "created": "2012-03-22T07:26:00.000Z",
        "score": 1,
        "cats": {},
        "subnet": "1.2.3.0/24"
      },
```

Response Content Type application/json

Parameter	Value	Description	Parameter Type	Data Type
ip	20.45.2.6	ip addresses in all valid formats e.g. 1.2.3.4, 216.137.61.0x08,	path	string

Figure 46

5. Click **Try It Out!**.
6. Copy the URL (Here: https://api.xforce.ibmcloud.com/)



Response Messages

HTTP Status Code	Reason	Response Model	Headers
403	Access denied.		
404	Not found.		

Curl

```
curl -X GET --header "Accept: application/json" "https://api.xforce.ibmcloud.com/ipr/20.45.2.6"
```

Request URL

```
https://api.xforce.ibmcloud.com/ipr/20.45.2.6
```

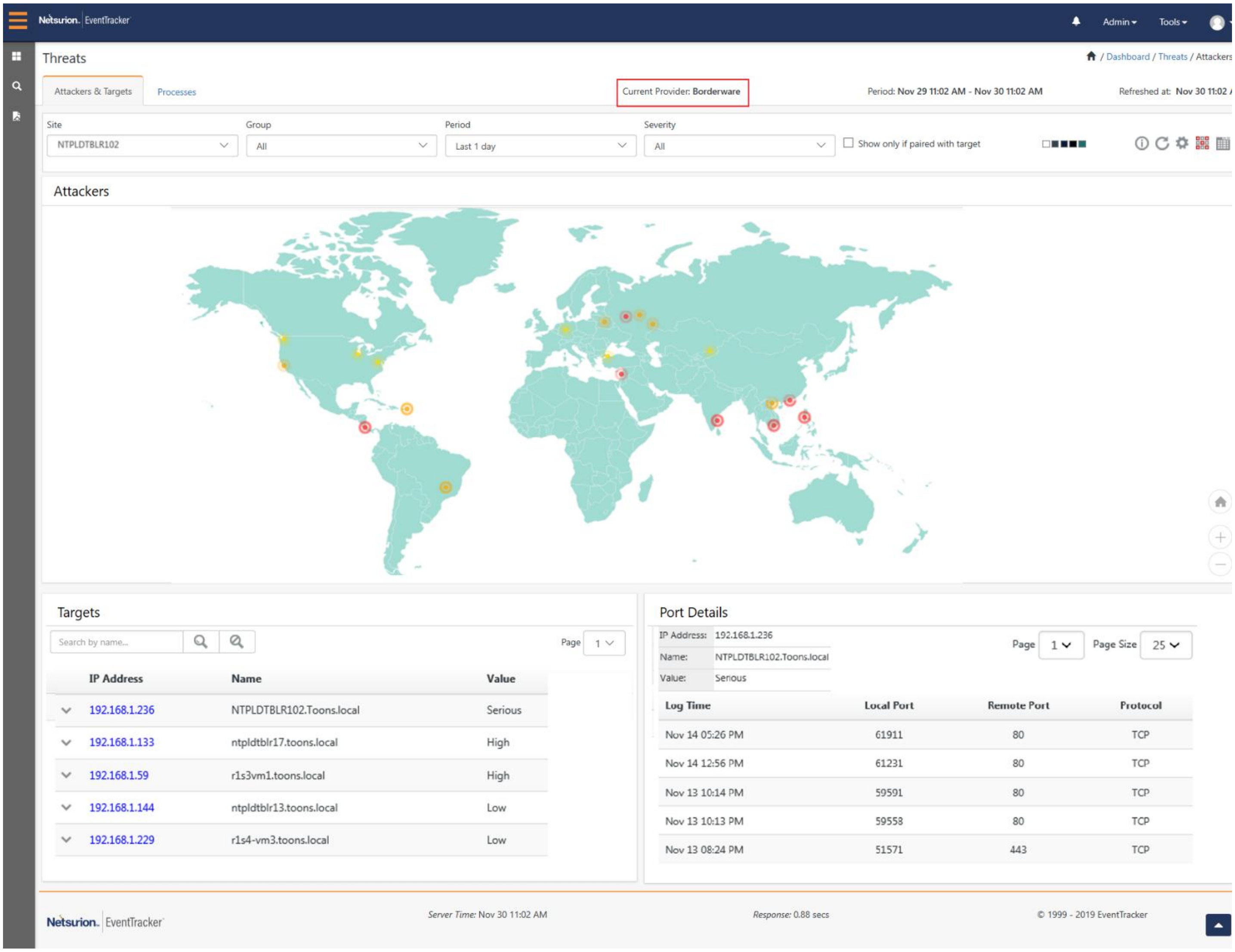
Figure 47

7. Now, open SQL Server Management Studio and expand **Databases**.
8. Expand **EventTrackerData** and then expand **Tables**.
9. Select the **IP_Provider_Engines** table, right-click and select **Edit Top 200 Rows.**
10. For **IBM-XFE, replace the existing URL with the copied URL (Here:** https://api.xforce.ibmcloud.com/)

The Attackers Dashboard option helps to view the Top 20 geographic location pins. Each of these top 20 pins may contain ‘N’ number of bad IPs. The summary of the IPs can also be viewed in a Tabular format.

1. To view Attackers Dashboard, click the **Dashboard** icon and select **Threats** from the dropdown list.

   Depending on the service provider selected in the Manager Configuration, the Attackers will be displayed.



Threats

⌂ / Dashboard / Threats / Attackers

Attackers & Targets | Processes

Current Provider: **Borderware**

Period: **Nov 29 11:02 AM - Nov 30 11:02 AM**

Refreshed at: **Nov 30 11:02**

Site: NTPLDTBLR102

Group: All

Period: Last 1 day

Severity: All

□ Show only if paired with target

Attackers

Targets

Search by name...

Page 1

	IP Address	Name	Value
⌄	192.168.1.236	NTPLDTBLR102.Toons.local	Serious
⌄	192.168.1.133	ntpldtblr17.toons.local	High
⌄	192.168.1.59	r1s3vm1.toons.local	High
⌄	192.168.1.144	ntpldtblr13.toons.local	Low
⌄	192.168.1.229	r1s4-vm3.toons.local	Low

Port Details

IP Address: 192.168.1.236

Name: NTPLDTBLR102.Toons.local

Value: Serious

Page 1 Page Size 25

Log Time	Local Port	Remote Port	Protocol
Nov 14 05:26 PM	61911	80	TCP
Nov 14 12:56 PM	61231	80	TCP
Nov 13 10:14 PM	59591	80	TCP
Nov 13 10:13 PM	59558	80	TCP
Nov 13 08:24 PM	51571	443	TCP

Netsurion. EventTracker

Server Time: Nov 30 11:02 AM

Response: 0.88 secs

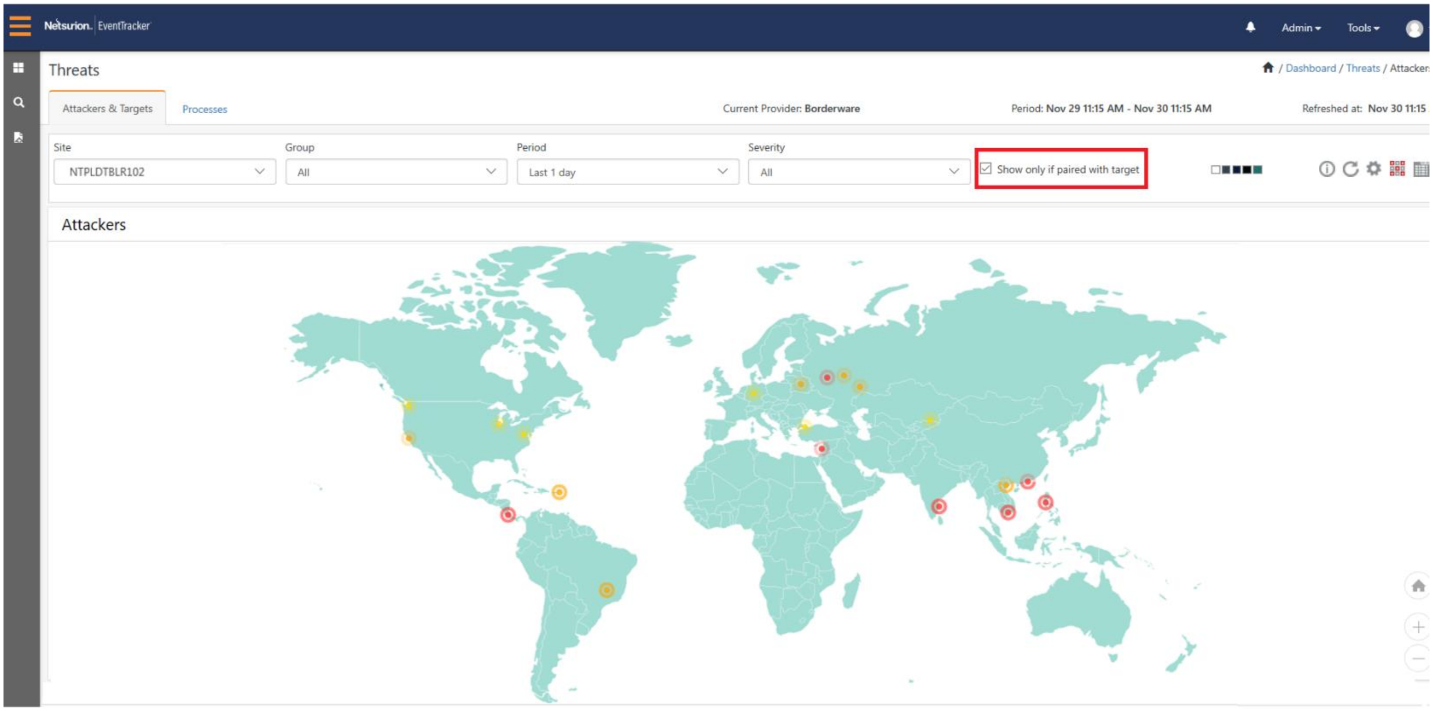
© 1999 - 2019 EventTracker

Figure 48

NOTE

The dashboard will populate data based on the default reputation service provider, i.e. Borderware. Once the user changes the service provider, the initial data will be intact and will continue populating data based on the new service provider, for the new IPs.

- Enable the checkbox **Show only if paired with target** to display only the paired IPs in the dashboard.



Threats

/ Dashboard / Threats / Attacker

Attackers & Targets | Processes

Current Provider: **Borderware** Period: **Nov 29 11:15 AM - Nov 30 11:15 AM** Refreshed at: **Nov 30 11:15**

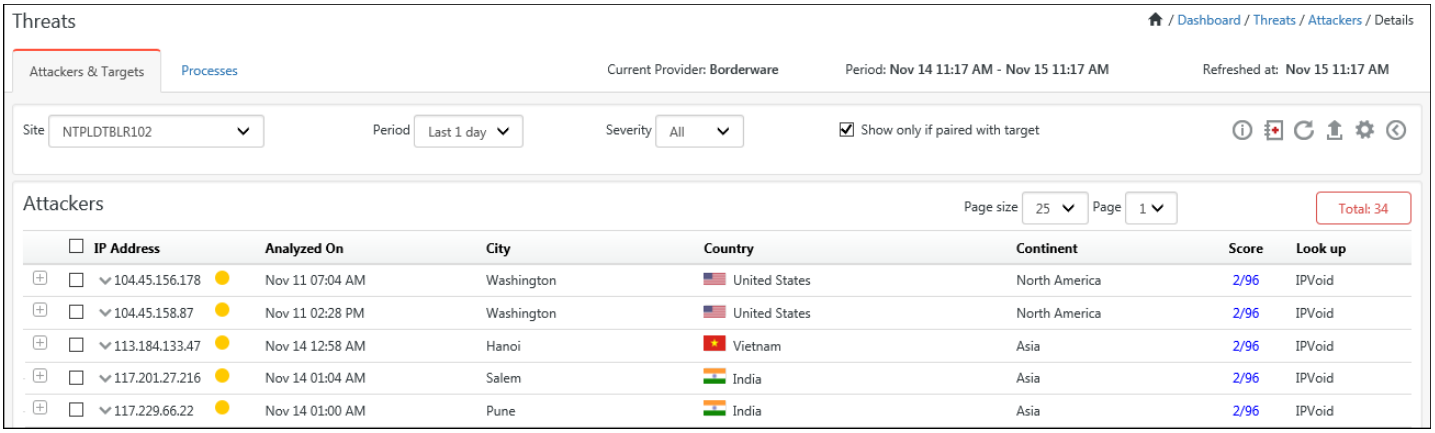
Site: NTPLDTBLR102 Group: All Period: Last 1 day Severity: All

☑ Show only if paired with target

Attackers

Figure 49

Similarly, you can get information for IP paired with targets in a tabular format, by enabling the checkbox and selecting the Tabular icon . This is shown in the figure below:


Threats

/ Dashboard / Threats / Attackers / Details

Attackers & Targets | Processes

Current Provider: **Borderware** Period: **Nov 14 11:17 AM - Nov 15 11:17 AM** Refreshed at: **Nov 15 11:17 AM**

Site: NTPLDTBLR102 Period: Last 1 day Severity: All ☑ Show only if paired with target

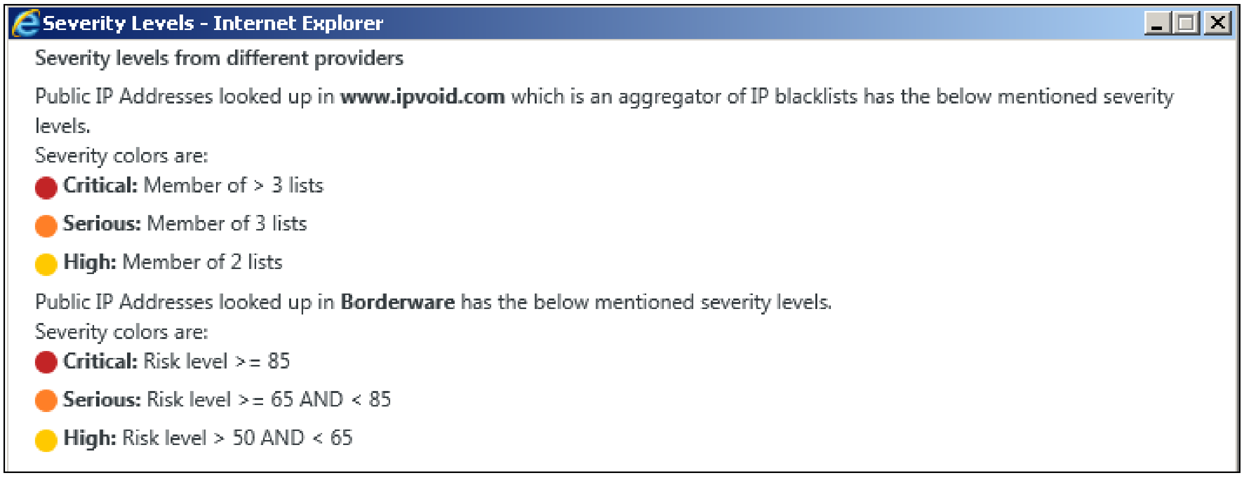
Attackers

Page size 25 Page 1 Total: 34

	☐ IP Address		Analyzed On	City	Country	Continent	Score	Look up
⊞	☐ 104.45.156.178	●	Nov 11 07:04 AM	Washington	United States	North America	2/96	IPVoid
⊞	☐ 104.45.158.87	●	Nov 11 02:28 PM	Washington	United States	North America	2/96	IPVoid
⊞	☐ 113.184.133.47	●	Nov 14 12:58 AM	Hanoi	Vietnam	Asia	2/96	IPVoid
⊞	☐ 117.201.27.216	●	Nov 14 01:04 AM	Salem	India	Asia	2/96	IPVoid
⊞	☐ 117.229.66.22	●	Nov 14 01:00 AM	Pune	India	Asia	2/96	IPVoid

Figure 50

- Severity implies the threat level of the IP Addresses, where the severity is calculated on list. Click the Information icon ⓘ to view the severity level of the different service providers.



Severity Levels - Internet Explorer

Severity levels from different providers

Public IP Addresses looked up in **www.ipvoid.com** which is an aggregator of IP blacklists has the below mentioned severity levels.

Severity colors are:

- 🔴 **Critical:** Member of > 3 lists
- 🟠 **Serious:** Member of 3 lists
- 🟡 **High:** Member of 2 lists

Public IP Addresses looked up in **Borderware** has the below mentioned severity levels.

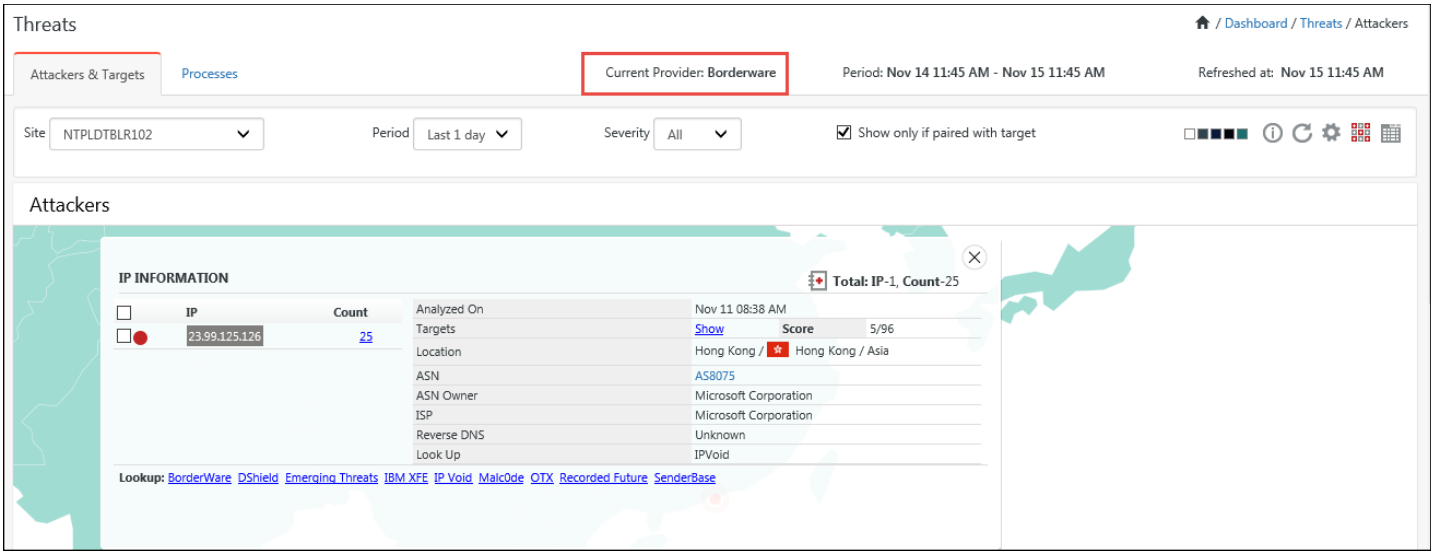
Severity colors are:

- 🔴 **Critical:** Risk level >= 85
- 🟠 **Serious:** Risk level >= 65 AND < 85
- 🟡 **High:** Risk level > 50 AND < 65

Figure 51

- Select an IP address and click **add Casebook** to add it to a New Casebook by selecting **Add New** or to an existing Casebook by selecting **Add to Existing**.
- Click the icon to refresh the dashboard.
- Click **Export** to export the details in a excel format.

2. To get the information about the bad IP, click on the respective location, as shown in the figure below:
   - For Service Provider**: Borderware**, the following information window will be displayed.



Threats

Dashboard / Threats / Attackers

Attackers & Targets | Processes

Current Provider: Borderware

Period: Nov 14 11:45 AM - Nov 15 11:45 AM

Refreshed at: Nov 15 11:45 AM

Site: NTPLDTBLR102 | Period: Last 1 day | Severity: All | ☑ Show only if paired with target

Attackers

IP INFORMATION

Total: IP-1, Count-25

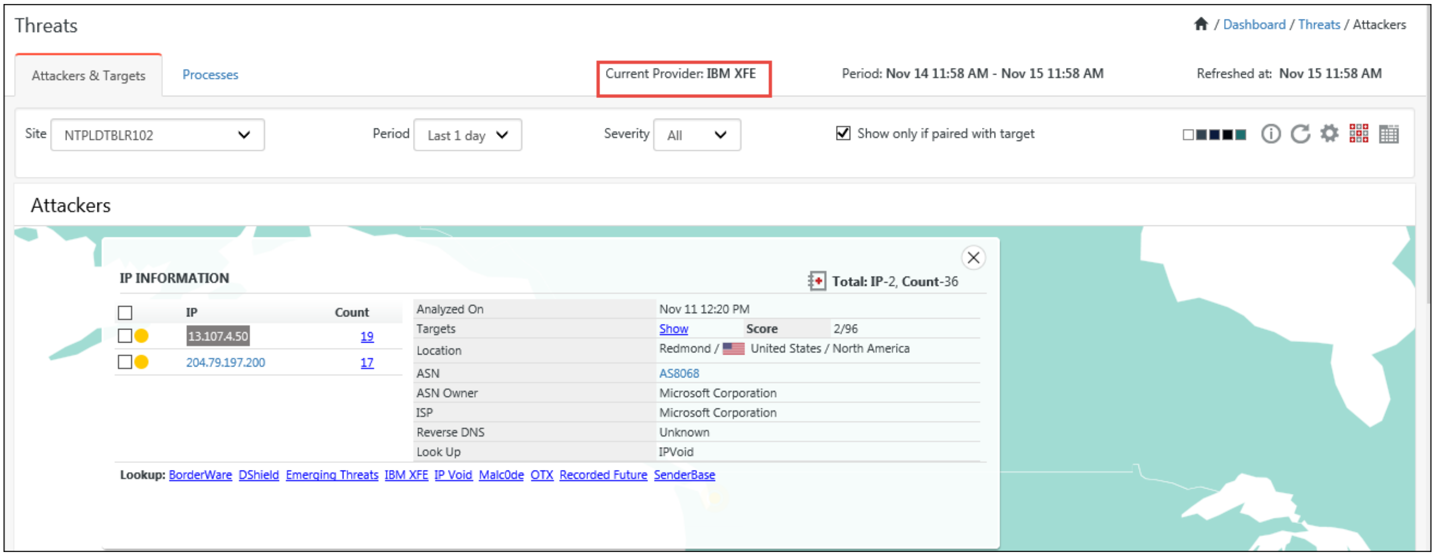
	IP	Count
□ ●	23.99.125.126	25

Analyzed On	Nov 11 08:38 AM		
Targets	Show	Score	5/96
Location	Hong Kong / Hong Kong / Asia		
ASN	AS8075		
ASN Owner	Microsoft Corporation		
ISP	Microsoft Corporation		
Reverse DNS	Unknown		
Look Up	IPVoid		

Lookup: BorderWare DShield Emerging Threats IBM XFE IP Void Malc0de OTX Recorded Future SenderBase

Figure 52

   - For Service Provider**: IBM XFE**, the following information window appears.



Threats

🏠 / Dashboard / Threats / Attackers

Attackers & Targets | Processes

Current Provider: IBM XFE

Period: Nov 14 11:58 AM - Nov 15 11:58 AM

Refreshed at: Nov 15 11:58 AM

Site NTPLDTBLR102 | Period Last 1 day | Severity All | ☑ Show only if paired with target

Attackers

IP INFORMATION

Total: IP-2, Count-36

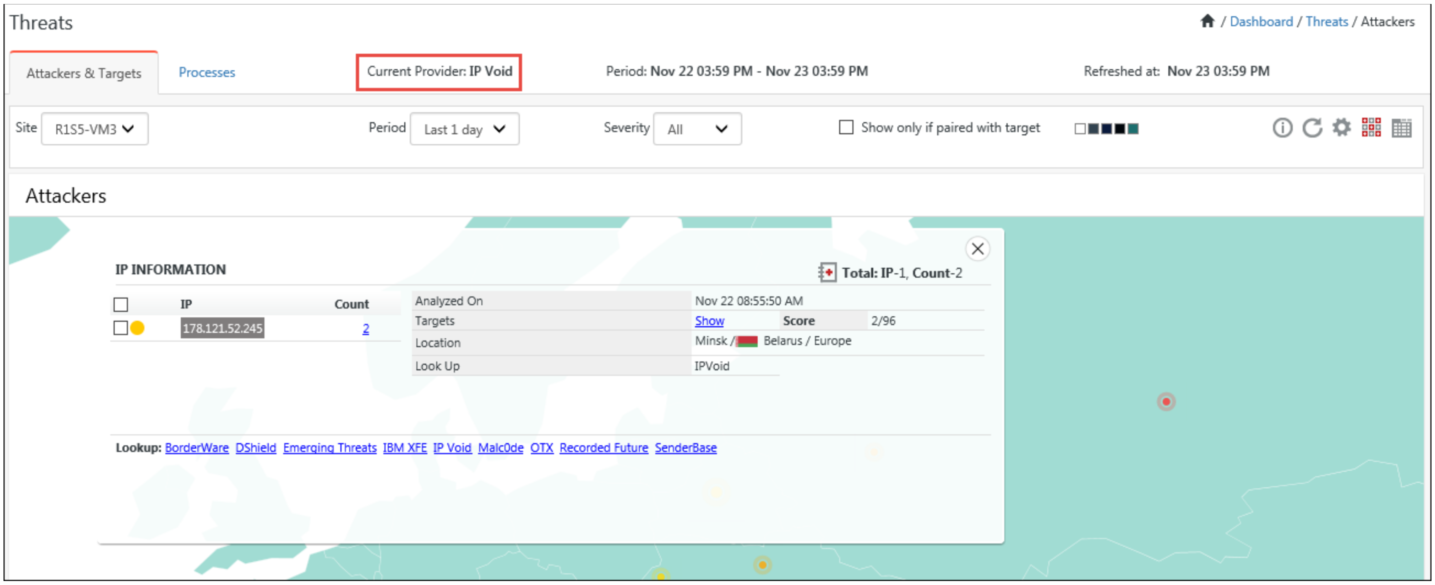
	IP	Count
□ ●	13.107.4.50	19
□ ●	204.79.197.200	17

Analyzed On	Nov 11 12:20 PM		
Targets	Show	Score	2/96
Location	Redmond / United States / North America		
ASN	AS8068		
ASN Owner	Microsoft Corporation		
ISP	Microsoft Corporation		
Reverse DNS	Unknown		
Look Up	IPVoid		

Lookup: BorderWare DShield Emerging Threats IBM XFE IP Void MalcOde OTX Recorded Future SenderBase

Figure 53

- For Service Provider**: IP Void** the following information window appears.



Threats

🏠 / Dashboard / Threats / Attackers

Attackers & Targets | Processes

Current Provider: IP Void

Period: Nov 22 03:59 PM - Nov 23 03:59 PM

Refreshed at: Nov 23 03:59 PM

Site R1S5-VM3 | Period Last 1 day | Severity All | □ Show only if paired with target

Attackers

IP INFORMATION

Total: IP-1, Count-2

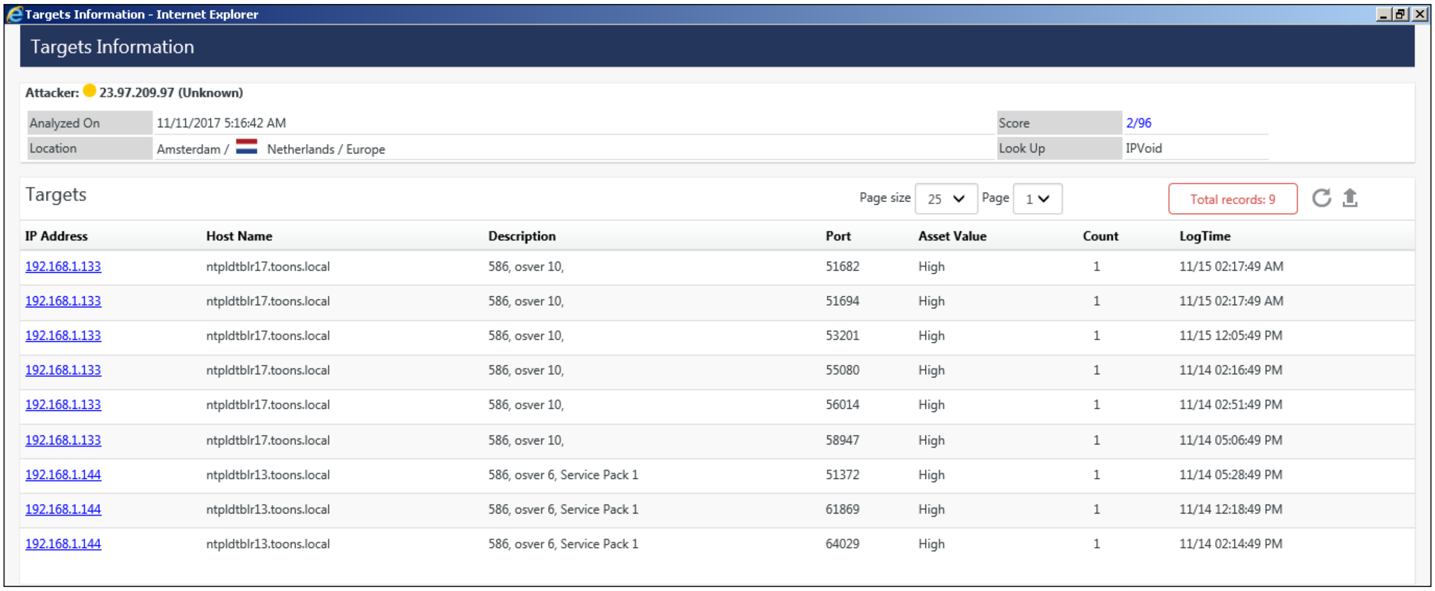
	IP	Count
□ ●	178.121.52.245	2

Analyzed On	Nov 22 08:55:50 AM		
Targets	Show	Score	2/96
Location	Minsk / Belarus / Europe		
Look Up	IPVoid		

Lookup: BorderWare DShield Emerging Threats IBM XFE IP Void MalcOde OTX Recorded Future SenderBase

Figure 54

1. To view the targets for the respective attackers, click the **Show** hyperlink.



Targets Information - Internet Explorer

Targets Information

Attacker: ● 23.97.209.97 (Unknown)

Analyzed On	11/11/2017 5:16:42 AM	Score	2/96
Location	Amsterdam / Netherlands / Europe	Look Up	IPVoid

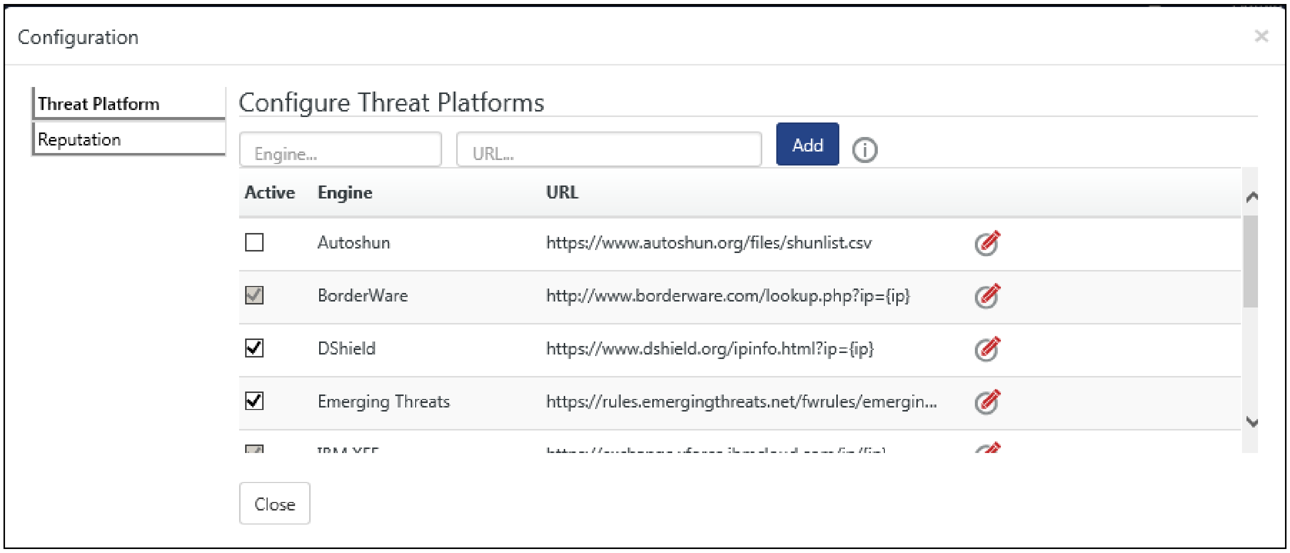
Targets

Page size 25 Page 1 Total records: 9

IP Address	Host Name	Description	Port	Asset Value	Count	LogTime
192.168.1.133	ntpldtblr17.toons.local	586, osver 10,	51682	High	1	11/15 02:17:49 AM
192.168.1.133	ntpldtblr17.toons.local	586, osver 10,	51694	High	1	11/15 02:17:49 AM
192.168.1.133	ntpldtblr17.toons.local	586, osver 10,	53201	High	1	11/15 12:05:49 PM
192.168.1.133	ntpldtblr17.toons.local	586, osver 10,	55080	High	1	11/14 02:16:49 PM
192.168.1.133	ntpldtblr17.toons.local	586, osver 10,	56014	High	1	11/14 02:51:49 PM
192.168.1.133	ntpldtblr17.toons.local	586, osver 10,	58947	High	1	11/14 05:06:49 PM
192.168.1.144	ntpldtblr13.toons.local	586, osver 6, Service Pack 1	51372	High	1	11/14 05:28:49 PM
192.168.1.144	ntpldtblr13.toons.local	586, osver 6, Service Pack 1	61869	High	1	11/14 12:18:49 PM
192.168.1.144	ntpldtblr13.toons.local	586, osver 6, Service Pack 1	64029	High	1	11/14 02:14:49 PM

Figure 55

2. For more information on the IP, click on the respective **Lookup** provider hyperlink.
3. For **IP Void,** when the configuration icon ⚙ is selected, the following window appears.
4. Click the **Threat Platform** option in the left pane.



Configuration

Threat Platform

Reputation

Configure Threat Platforms

Engine... URL... Add

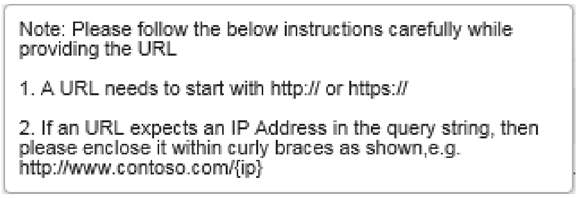
Active	Engine	URL
□	Autoshun	https://www.autoshun.org/files/shunlist.csv
☑	BorderWare	http://www.borderware.com/lookup.php?ip={ip}
☑	DShield	https://www.dshield.org/ipinfo.html?ip={ip}
☑	Emerging Threats	https://rules.emergingthreats.net/fwrules/emergin...
☑	IBM XFE	https://exchange.xforce.ibmcloud.com/ip/{ip}

Close

Figure 56

- The user can add custom threat Intelligence platforms by adding the name in the Engine Box and URL name in the URL box and click **Add**.
- The user can also unselect checkbox from the engine list available.
- A pop up message displays. Click **OK**.

- For editing a Engine name or URL, click Edit ✎.
- For more information, click information ⓘ.



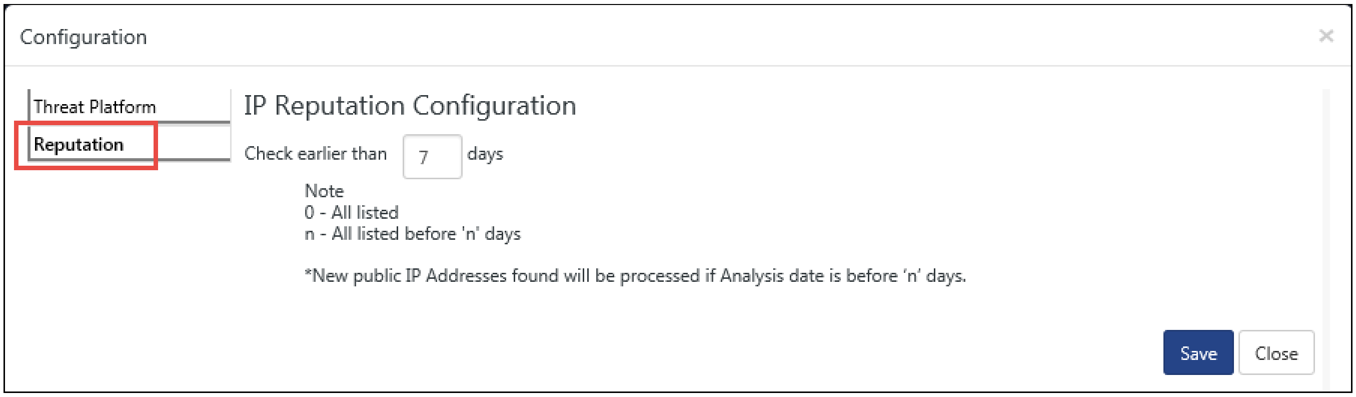
Note: Please follow the below instructions carefully while providing the URL

1. A URL needs to start with http:// or https://

2. If an URL expects an IP Address in the query string, then please enclose it within curly braces as shown,e.g. http://www.contoso.com/{ip}

Figure 57

5. Click the **Reputation** option and the following screen appears.



IP Reputation Configuration

Check earlier than 7 days

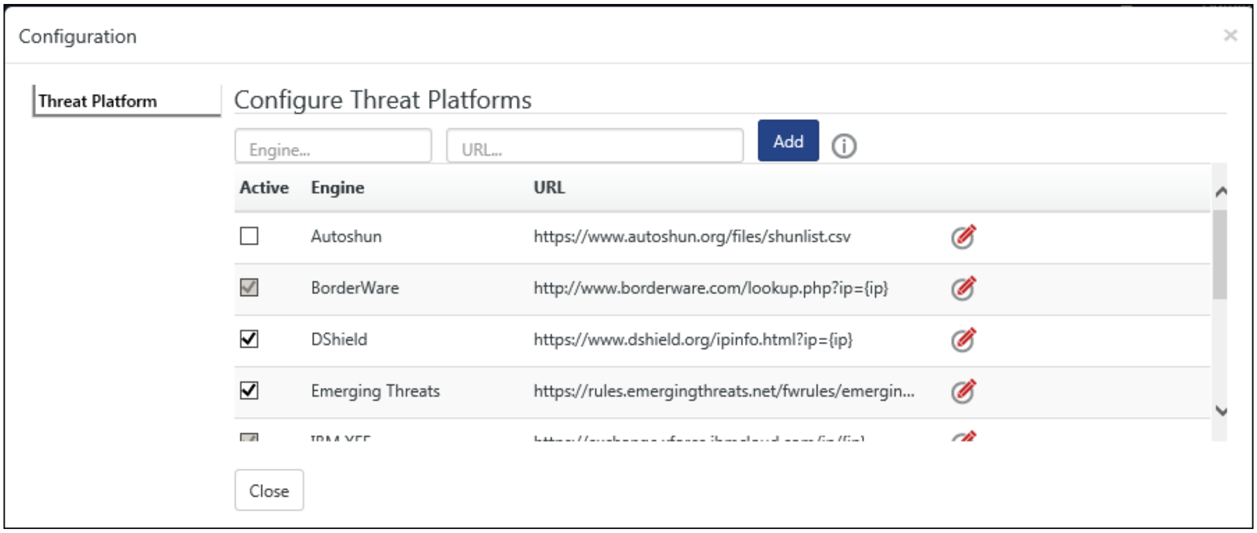
Note
0 - All listed
n - All listed before 'n' days

*New public IP Addresses found will be processed if Analysis date is before 'n' days.

Figure 58

- For tracking the earlier list of IP Reputation, enter the number of days in the **Check earlier than** field and click **Save**.

6. For **IBM XFE**, when the configuration icon ⚙ is selected, the following window appears.



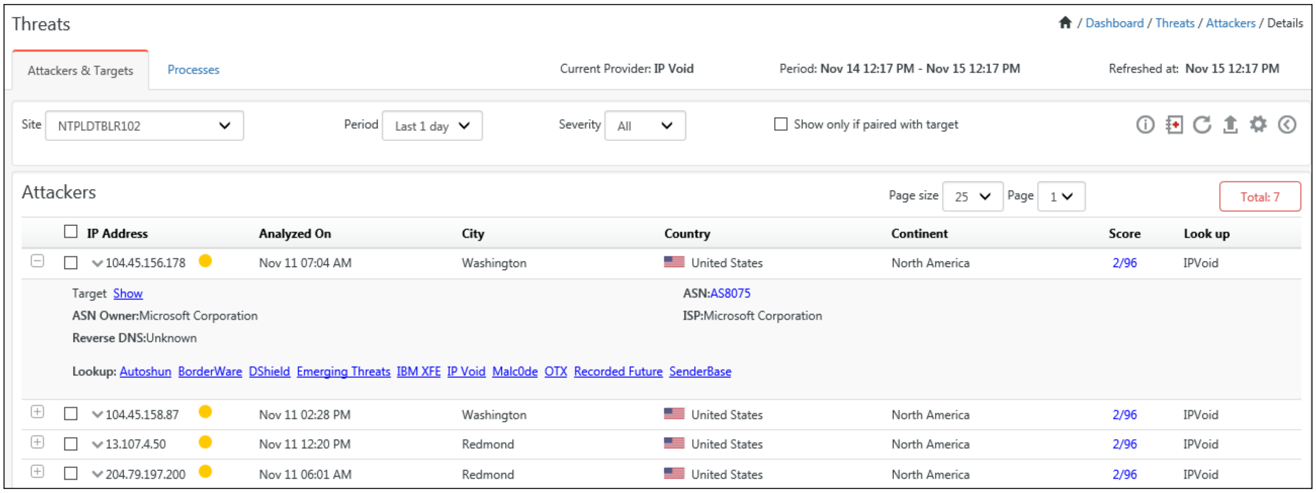
Configure Threat Platforms

Active	Engine	URL
☐	Autoshun	https://www.autoshun.org/files/shunlist.csv
☑	BorderWare	http://www.borderware.com/lookup.php?ip={ip}
☑	DShield	https://www.dshield.org/ipinfo.html?ip={ip}
☑	Emerging Threats	https://rules.emergingthreats.net/fwrules/emergin...
☑	IBM XFE	https://exchange.xforce.ibmcloud.com/ip/{ip}

Figure 59

- The user can add custom threat Intelligence platforms by adding the name in the Engine Box and URL name in the URL box and click **Add**.
- The user can unselect checkbox from the engine list available.
  A pop up message gets displayed. Click **OK**.
- For editing an Engine name or URL, click Edit ✎.
- For more information, click information ⓘ.

7. To get detailed information of the bad IPs, click Tabular view ▦ in the Attackers dashboard. The IPs is listed in a tabular format.
8. To view details about an IP, click ⊞



Current Provider: IP Void   Period: Nov 14 12:17 PM - Nov 15 12:17 PM   Refreshed at: Nov 15 12:17 PM

	□ IP Address		Analyzed On	City	Country	Continent	Score	Look up
⊟	□ 104.45.156.178	●	Nov 11 07:04 AM	Washington	United States	North America	2/96	IPVoid
⊞	□ 104.45.158.87	●	Nov 11 02:28 PM	Washington	United States	North America	2/96	IPVoid
⊞	□ 13.107.4.50	●	Nov 11 12:20 PM	Redmond	United States	North America	2/96	IPVoid
⊞	□ 204.79.197.200	●	Nov 11 06:01 AM	Redmond	United States	North America	2/96	IPVoid

Details of 104.45.156.178:

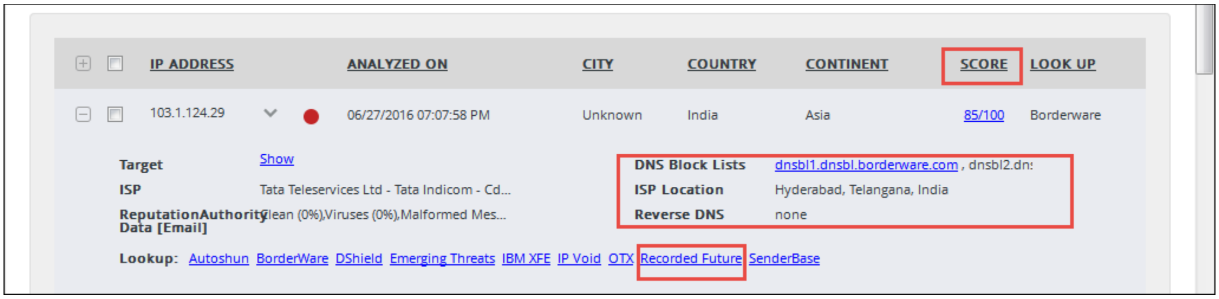
Target Show
ASN Owner:Microsoft Corporation
Reverse DNS:Unknown
ASN:AS8075
ISP:Microsoft Corporation

Lookup: Autoshun BorderWare DShield Emerging Threats IBM XFE IP Void Malc0de OTX Recorded Future SenderBase

Figure 60

5. Click on the IP dropdown icon ⌄ .
   - Select the **WHOIS** option for more information on the IP.
   - Select **Log Search**, for performing a search.

For Attackers >tabular data, the score column will get displayed along with DNS Block List and Lookup provider: **Recorded Future**. The figure is shown below:



⊞	□	IP ADDRESS			ANALYZED ON	CITY	COUNTRY	CONTINENT	SCORE	LOOK UP
⊟	□	103.1.124.29	⌄	●	06/27/2016 07:07:58 PM	Unknown	India	Asia	85/100	Borderware

Target Show
ISP Tata Teleservices Ltd - Tata Indicom - Cd...
ReputationAuthority Data [Email] Clean (0%),Viruses (0%),Malformed Mes...

DNS Block Lists dnsbl1.dnsbl.borderware.com , dnsbl2.dn:
ISP Location Hyderabad, Telangana, India
Reverse DNS none

Lookup: Autoshun BorderWare DShield Emerging Threats IBM XFE IP Void OTX Recorded Future SenderBase

Figure 61

2.4 Processes tab

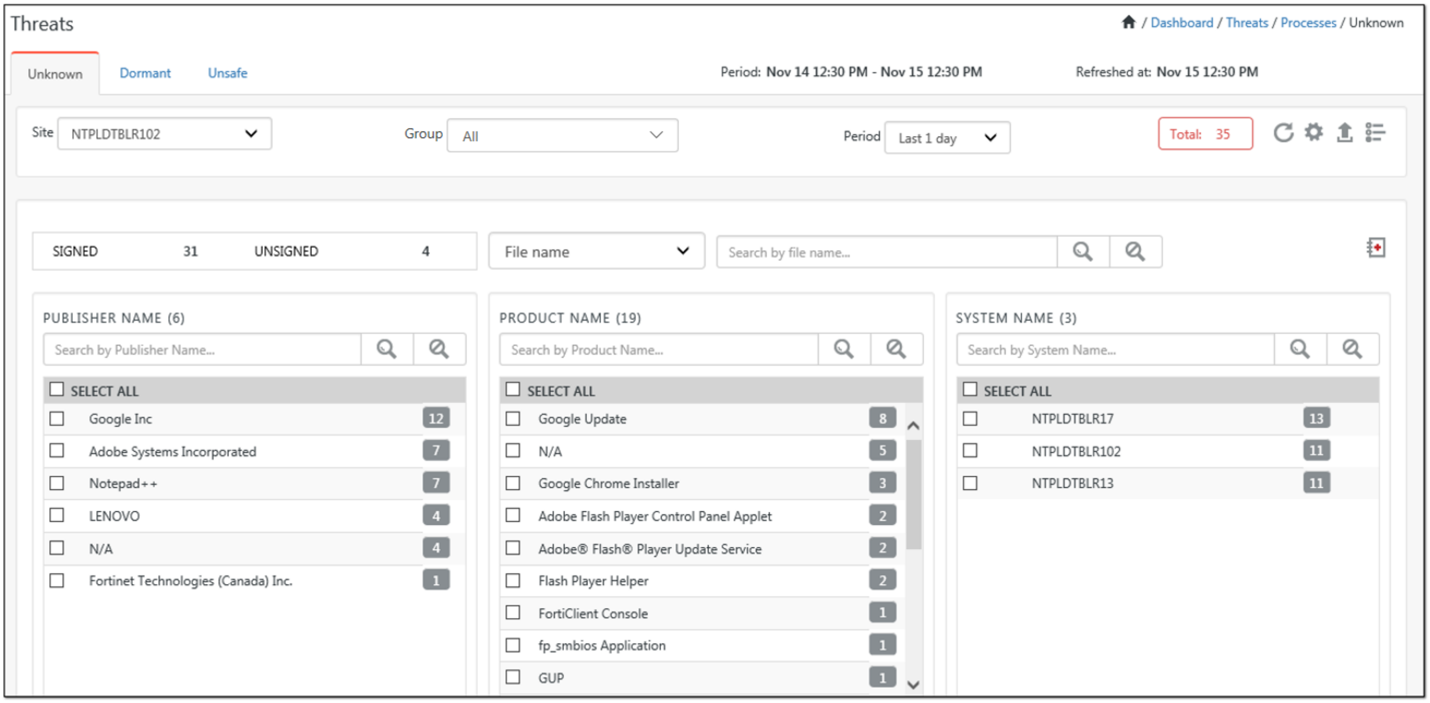
'Processes' is designed to interpret advanced threats and false positives which emerge within an enterprise. Whenever a new process is launched in a machine, it will look up for emerging threats, if any. The user will be able to filter the processes that are unknown based on Signature status. Also, the user will be able to filter the processes that are not digitally signed for which he might be interested. He can also add the processes to Dormant/Unsafe list as per requirement.

2.4.1 List of URLs for firewall proxy exclusion in Processes

1. https://www.virustotal.com
2. http://hashlib.leic.lumension.com
3. https://exchange.xforce.ibmcloud.com
4. nsrl.eventtracker.com: 9120

1. Navigate to the **Processes** tab.

   The Process dashboard opens with all the processes that are unknown.



Threats

/ Dashboard / Threats / Processes / Unknown

Unknown | Dormant | Unsafe

Period: Nov 14 12:30 PM - Nov 15 12:30 PM

Refreshed at: Nov 15 12:30 PM

Site: NTPLDTBLR102 | Group: All | Period: Last 1 day | Total: 35

SIGNED 31 | UNSIGNED 4 | File name | Search by file name...

PUBLISHER NAME (6)	
□ SELECT ALL	
□ Google Inc	12
□ Adobe Systems Incorporated	7
□ Notepad++	7
□ LENOVO	4
□ N/A	4
□ Fortinet Technologies (Canada) Inc.	1

PRODUCT NAME (19)	
□ SELECT ALL	
□ Google Update	8
□ N/A	5
□ Google Chrome Installer	3
□ Adobe Flash Player Control Panel Applet	2
□ Adobe® Flash® Player Update Service	2
□ Flash Player Helper	2
□ FortiClient Console	1
□ fp_smbios Application	1
□ GUP	1

SYSTEM NAME (3)	
□ SELECT ALL	
□ NTPLDTBLR17	13
□ NTPLDTBLR102	11
□ NTPLDTBLR13	11

Figure 62

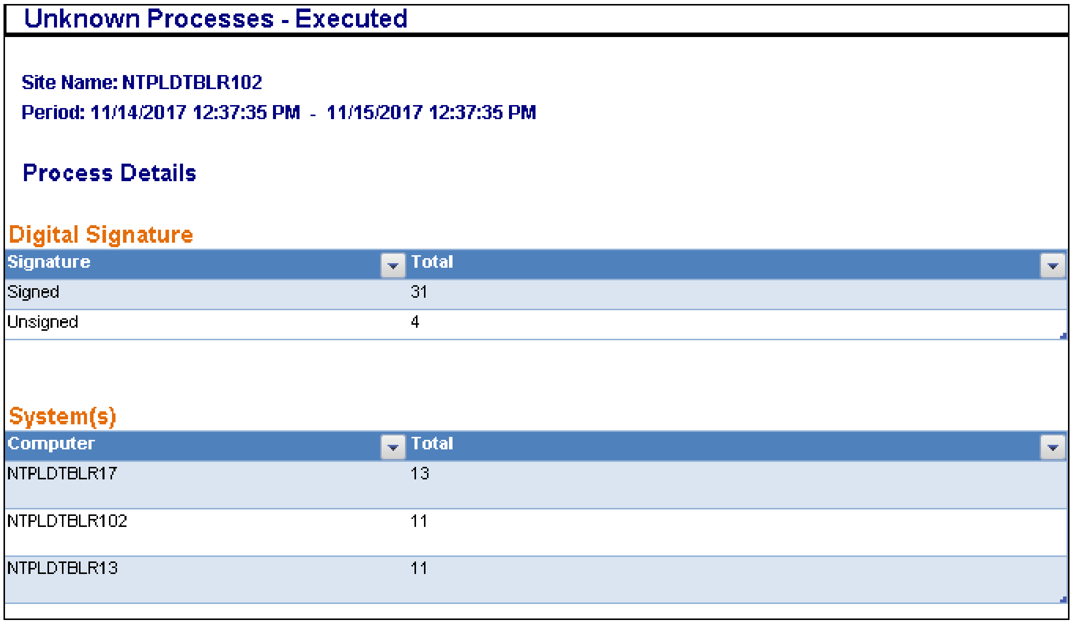
NOTE:

1. The **Processes** dashboard is added on feature and is available only on certified license.

2. The executed processes are displayed in the unknown tab and the processes that are unexecuted get listed in the dormant tab.

Processes Dashboard	
Field	Description
Sites	In a Collection Master, all sites are displayed. You cannot view this option in a Collection Point.
Period	Period can be selected for Last 1day/2day/3day/1 week/2 weeks/3 weeks/1 month/2 months/3 months/ All.
Signed/Unsigned	View the list of signed/unsigned status of the unknown process.
Publisher name	The name of the publisher appears.
Product name	The name of the products appears.
System name	The name of the systems appears.

2. Click **Casebook** to add a process to a new Casebook or an existing Casebook.
3. Use **Search** to search a **Publisher Name**/ **Product Name**/ **System Name**.
4. Use **Clear search criteria** to clear the search.
5. The user can select **refresh** to refresh data.
6. Click **Export** to get the list in excel format.



Unknown Processes - Executed

Site Name: NTPLDTBLR102
Period: 11/14/2017 12:37:35 PM - 11/15/2017 12:37:35 PM

Process Details

Digital Signature

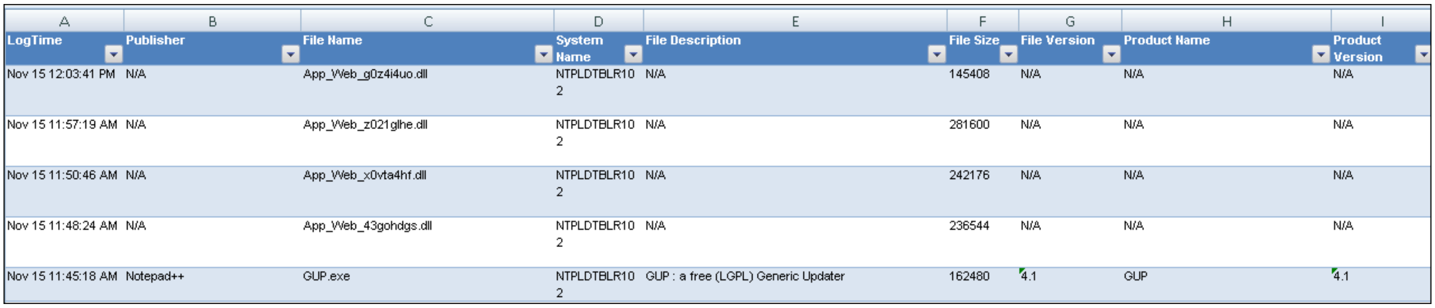
Signature	Total
Signed	31
Unsigned	4

System(s)

Computer	Total
NTPLDTBLR17	13
NTPLDTBLR102	11
NTPLDTBLR13	11

Figure 63

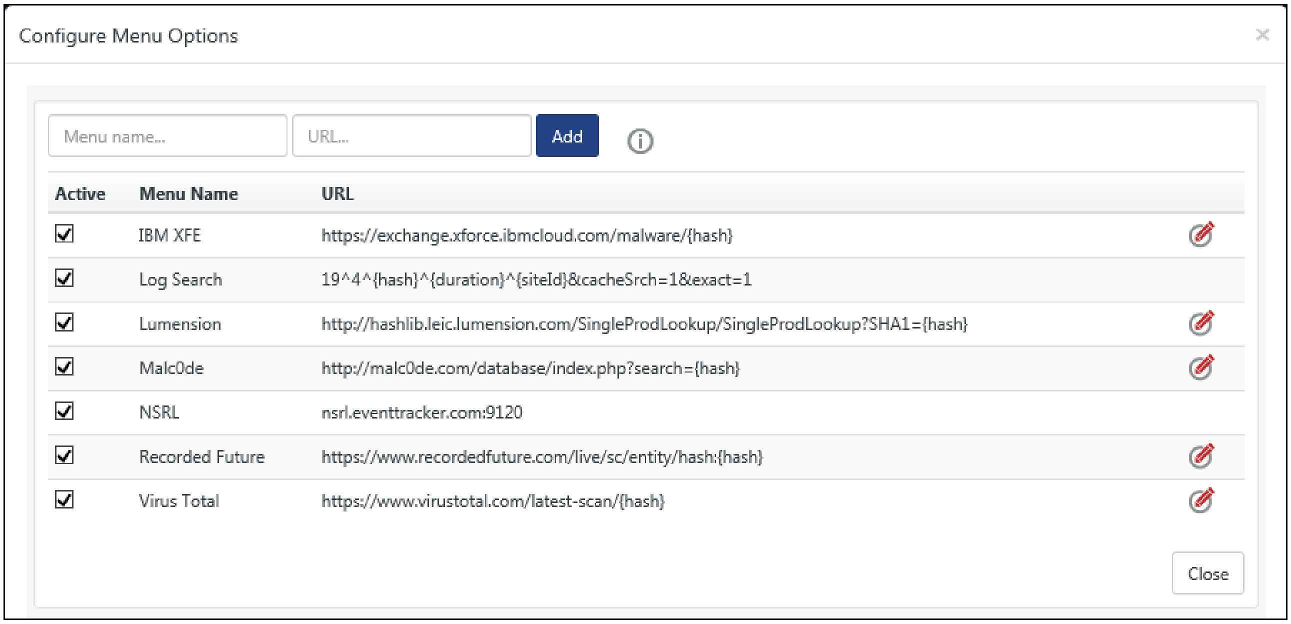
7. Click the **Detail** tab.



A	B	C	D	E	F	G	H	I
LogTime	Publisher	File Name	System Name	File Description	File Size	File Version	Product Name	Product Version
Nov 15 12:03:41 PM	N/A	App_Web_g0z4i4uo.dll	NTPLDTBLR102	N/A	145408	N/A	N/A	N/A
Nov 15 11:57:19 AM	N/A	App_Web_z021glhe.dll	NTPLDTBLR102	N/A	281600	N/A	N/A	N/A
Nov 15 11:50:46 AM	N/A	App_Web_x0vta4hf.dll	NTPLDTBLR102	N/A	242176	N/A	N/A	N/A
Nov 15 11:48:24 AM	N/A	App_Web_43gohdgs.dll	NTPLDTBLR102	N/A	236544	N/A	N/A	N/A
Nov 15 11:45:18 AM	Notepad++	GUP.exe	NTPLDTBLR102	GUP : a free (LGPL) Generic Updater	162480	4.1	GUP	4.1

Figure 64

8. When configuration ⚙ is selected, the following window opens.



Configure Menu Options

Active	Menu Name	URL	
☑	IBM XFE	https://exchange.xforce.ibmcloud.com/malware/{hash}	✎
☑	Log Search	19^4^{hash}^{duration}^{siteId}&cacheSrch=1&exact=1	
☑	Lumension	http://hashlib.leic.lumension.com/SingleProdLookup/SingleProdLookup?SHA1={hash}	✎
☑	Malc0de	http://malc0de.com/database/index.php?search={hash}	✎
☑	NSRL	nsrl.eventtracker.com:9120	
☑	Recorded Future	https://www.recordedfuture.com/live/sc/entity/hash:{hash}	✎
☑	Virus Total	https://www.virustotal.com/latest-scan/{hash}	✎

Figure 65

- The user can add custom threat Intelligence platforms by adding the name in the Engine Box and Url name in the URL box and click **Add**.
- The user can also unselect checkbox from the engine list available.
- A pop up message opens. Click **OK**.
- Click edit icon ✎ for making changes in the URL or engine name.
- For more information, click information ⓘ.

2.4.2 Unknown Process Filter

To reduce the noise in unknown process detection, the user can create and categorize a process as safe, based on the meta-data of the process. The user can create specific rules based on the attributes provided in Unknown Process filter wizard and can filter out the safe processes.

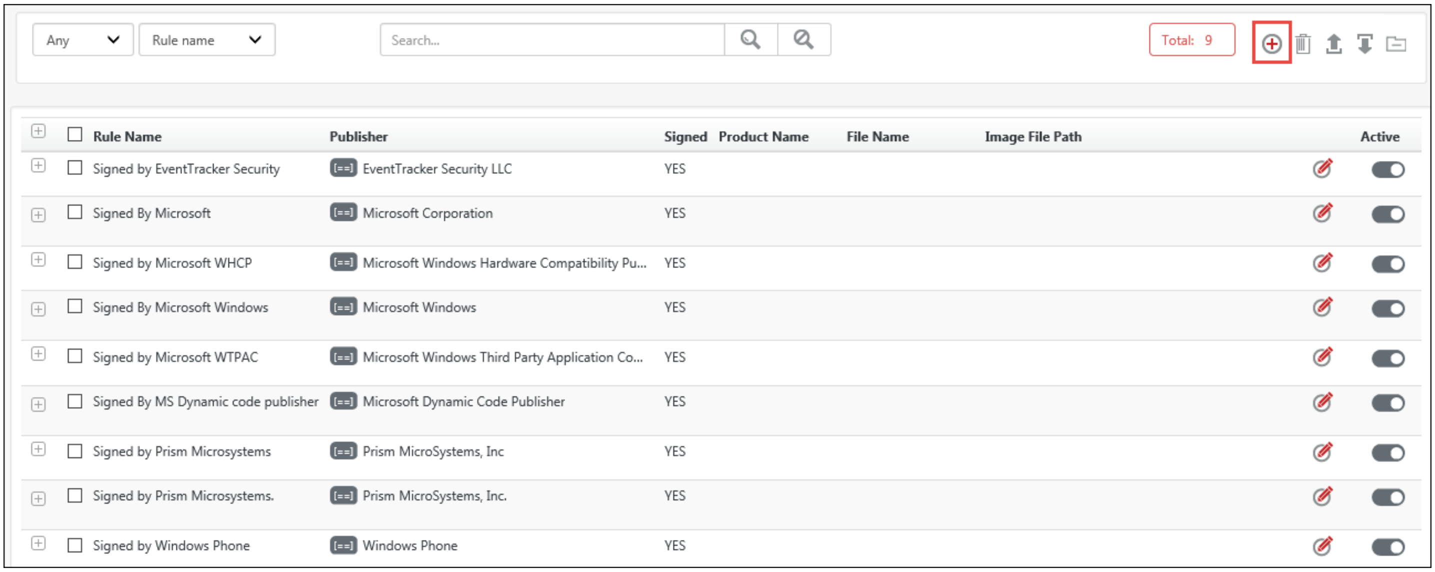
- To filter a process, click the icon ☰ in the Unknown process dashboard.

The Unknown process filter wizard appears.

NOTE

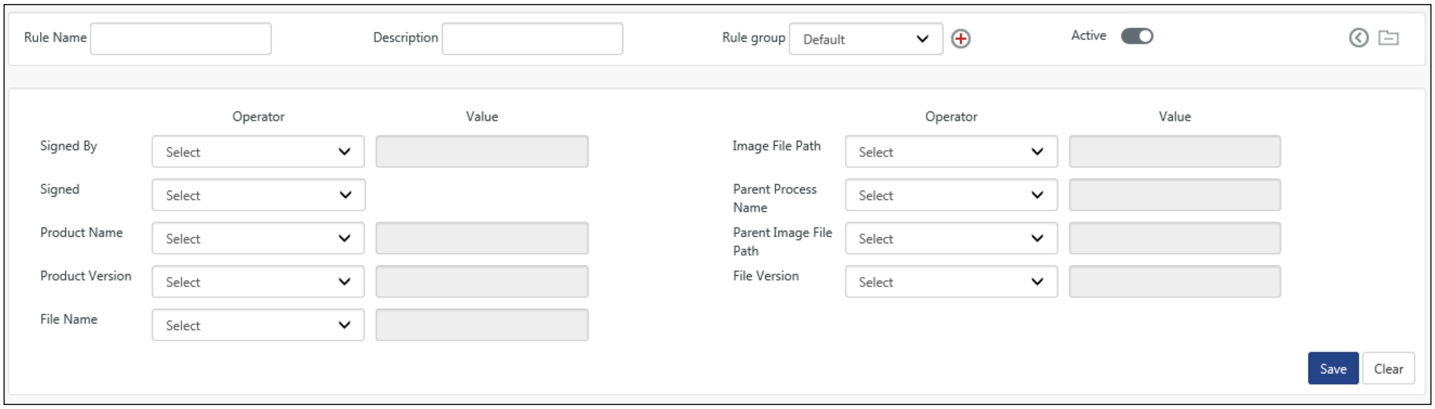
- By default, there are 9 Rules to filter out the EventTracker and Microsoft related files. These default rules help in reducing the noise.

- To add a new rule for filtering out a process, click add rule ⊕.



Rule Name	Publisher	Signed	Product Name	File Name	Image File Path	Active
Signed by EventTracker Security	EventTracker Security LLC	YES				
Signed By Microsoft	Microsoft Corporation	YES				
Signed by Microsoft WHCP	Microsoft Windows Hardware Compatibility Pu...	YES				
Signed By Microsoft Windows	Microsoft Windows	YES				
Signed by Microsoft WTPAC	Microsoft Windows Third Party Application Co...	YES				
Signed By MS Dynamic code publisher	Microsoft Dynamic Code Publisher	YES				
Signed by Prism Microsystems	Prism MicroSystems, Inc	YES				
Signed by Prism Microsystems.	Prism MicroSystems, Inc.	YES				
Signed by Windows Phone	Windows Phone	YES				

Figure 66



Rule Name Description Rule group Default Active

	Operator	Value		Operator	Value
Signed By	Select		Image File Path	Select	
Signed	Select		Parent Process Name	Select	
Product Name	Select		Parent Image File Path	Select	
Product Version	Select		File Version	Select	
File Name	Select				

Figure 67

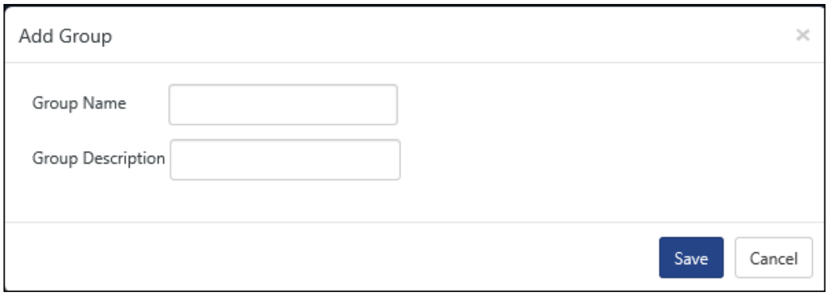
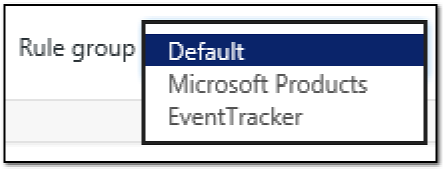
Unknown Process Filter	
Field	**Description**
Rule Name	Give a rule name.
Description	Add an appropriate description.
Add to Rule Group	Create group by clicking the add button ⊕.  Add Group × Group Name Group Description Save Cancel Click **Save**. To add rule to a group, click the dropdown list and select the group. 

Figure 68

- Select any of the provided attributes (**Publisher**/**Signed**/**Product Name**/**Product Version**/**File Name**/**Image File Path**/**Parent Process Name**/**Parent Image File Path**/**File Version**) to create a rule and filter out a safe process.

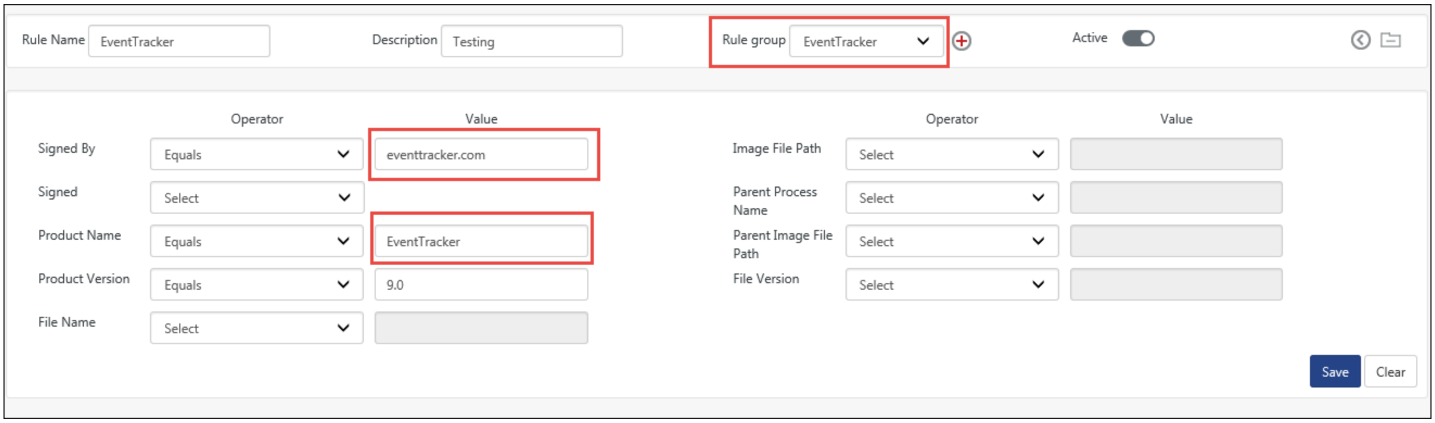
For Example: The user is flooded with unknown processes (Signed/Unsigned), and he wants to filter out the signed product “EventTracker” which is published by “EventTracker “, as a safe process.

The user can create a rule based on the above-mentioned criteria.

- Select the **Rule Name** as “EventTracker” and give a description.
- Select the relevant group from the dropdown list in the **Add to Rule Group** field.
- In **Publisher:** select operator (Equals/Contains/Regular Expression) from the drop-down list and enter the publisher name.
    - Here, we have selected “Equals”.
- Select the Signed field as “Yes”.

- Select the operator from the dropdown list and enter the product name. Here operator selected is “Equals”.
- After configuring the rule, click **Save**.

The figure is shown below:

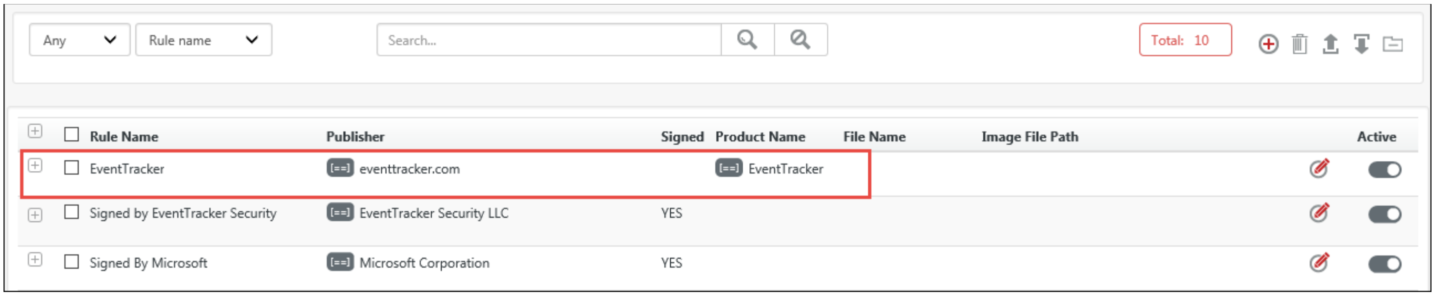


Rule Name: EventTracker
Description: Testing
Rule group: EventTracker
Active

	Operator	Value		Operator	Value
Signed By	Equals	eventtracker.com	Image File Path	Select	
Signed	Select		Parent Process Name	Select	
Product Name	Equals	EventTracker	Parent Image File Path	Select	
Product Version	Equals	9.0	File Version	Select	
File Name	Select				

Figure 69

The rule gets listed.



Rule Name	Publisher	Signed	Product Name	File Name	Image File Path	Active
EventTracker	eventtracker.com		EventTracker			
Signed by EventTracker Security	EventTracker Security LLC	YES				
Signed By Microsoft	Microsoft Corporation	YES				

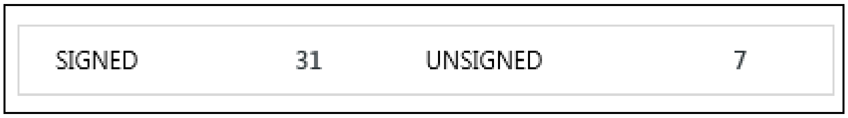
Figure 70

Once the rule gets activated, the processes related to the digitally signed product “EventTra cker” of Publisher “EventTracker”, will be marked as safe and will not be displayed in the Unknown Process Dashboard.

- To edit the rule click edit ✎ and to de-active the rule, uncheck the **Active** box.
- To export the rule, click export ⬆ and to import rule click import ⬇.
- To go back to the Unknown Process Dashboard, click the icon 🗀 .

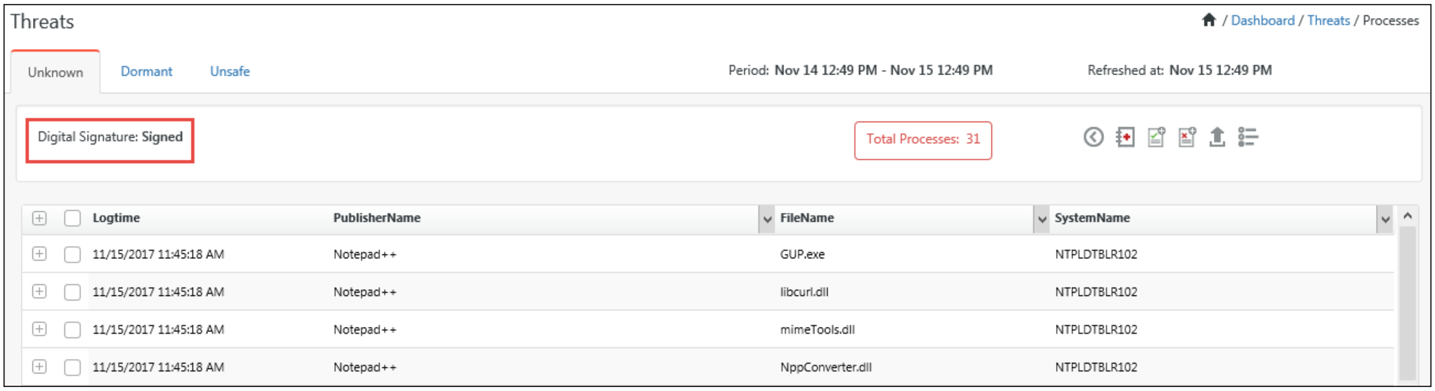
2.4.3 Digital Signature (Signed/Unsigned)

1. Click the **SIGNED**/ **UNSIGNED** hyperlink and it will list all the signed/unsigned unknown processes.



SIGNED 31 UNSIGNED 7

Figure 71



Threats

/ Dashboard / Threats / Processes

Unknown Dormant Unsafe

Period: Nov 14 12:49 PM - Nov 15 12:49 PM

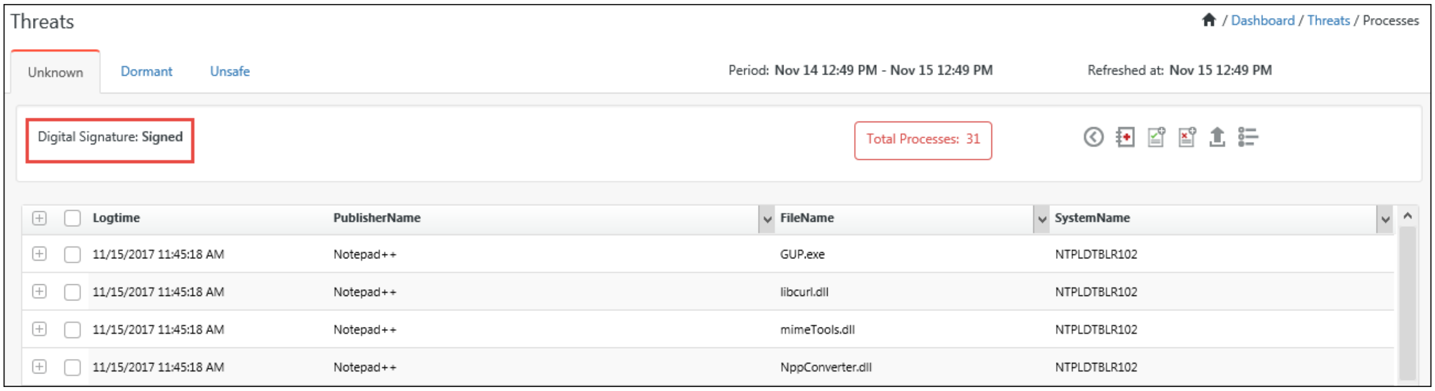
Refreshed at: Nov 15 12:49 PM

Digital Signature: Signed

Total Processes: 31

Logtime	PublisherName	FileName	SystemName
11/15/2017 11:45:18 AM	Notepad++	GUP.exe	NTPLDTBLR102
11/15/2017 11:45:18 AM	Notepad++	libcurl.dll	NTPLDTBLR102
11/15/2017 11:45:18 AM	Notepad++	mimeTools.dll	NTPLDTBLR102
11/15/2017 11:45:18 AM	Notepad++	NppConverter.dll	NTPLDTBLR102

Figure 72



Threats

/ Dashboard / Threats / Processes

Unknown Dormant Unsafe

Period: Nov 14 12:49 PM - Nov 15 12:49 PM

Refreshed at: Nov 15 12:49 PM

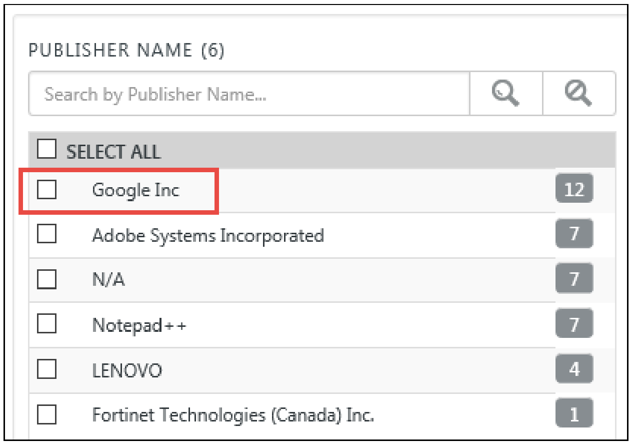
Digital Signature: Signed

Total Processes: 31

Logtime	PublisherName	FileName	SystemName
11/15/2017 11:45:18 AM	Notepad++	GUP.exe	NTPLDTBLR102
11/15/2017 11:45:18 AM	Notepad++	libcurl.dll	NTPLDTBLR102
11/15/2017 11:45:18 AM	Notepad++	mimeTools.dll	NTPLDTBLR102
11/15/2017 11:45:18 AM	Notepad++	NppConverter.dll	NTPLDTBLR102

Figure 73

2. Get the process detail by selecting any **Publisher Name**. (For e.g. Google Inc.).



PUBLISHER NAME (6)

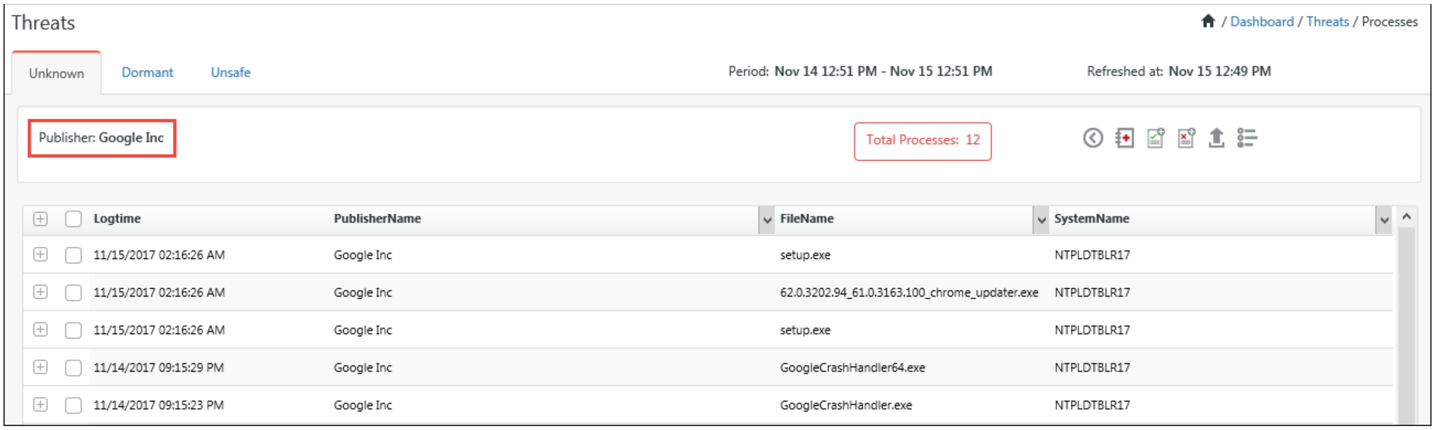
Search by Publisher Name...

□ SELECT ALL

□ Google Inc	12
□ Adobe Systems Incorporated	7
□ N/A	7
□ Notepad++	7
□ LENOVO	4
□ Fortinet Technologies (Canada) Inc.	1

Figure 74

The Detail window appears.



Threats

🏠 / Dashboard / Threats / Processes

Unknown Dormant Unsafe

Period: Nov 14 12:51 PM - Nov 15 12:51 PM

Refreshed at: Nov 15 12:49 PM

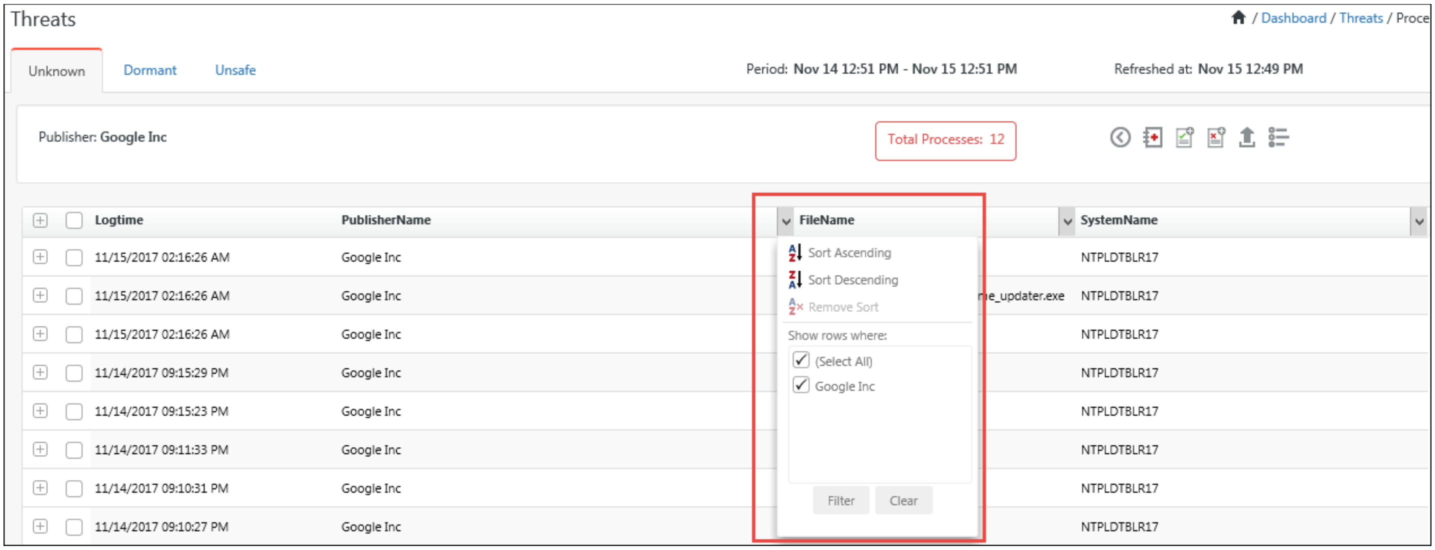
Publisher: Google Inc

Total Processes: 12

⊞	□	Logtime	PublisherName	FileName	SystemName
⊞	□	11/15/2017 02:16:26 AM	Google Inc	setup.exe	NTPLDTBLR17
⊞	□	11/15/2017 02:16:26 AM	Google Inc	62.0.3202.94_61.0.3163.100_chrome_updater.exe	NTPLDTBLR17
⊞	□	11/15/2017 02:16:26 AM	Google Inc	setup.exe	NTPLDTBLR17
⊞	□	11/14/2017 09:15:29 PM	Google Inc	GoogleCrashHandler64.exe	NTPLDTBLR17
⊞	□	11/14/2017 09:15:23 PM	Google Inc	GoogleCrashHandler.exe	NTPLDTBLR17

Figure 75

3. In the same way, the user can get the Process detail, selecting the desired **Product Name** or the **System Name**, in the Unknown process dashboard.
4. The user can also **Sort** and **Filter** the process as per requirement.



Threats

🏠 / Dashboard / Threats / Proce

Unknown Dormant Unsafe

Period: Nov 14 12:51 PM - Nov 15 12:51 PM

Refreshed at: Nov 15 12:49 PM

Publisher: Google Inc

Total Processes: 12

⊞	□	Logtime	PublisherName	FileName	SystemName
⊞	□	11/15/2017 02:16:26 AM	Google Inc		NTPLDTBLR17
⊞	□	11/15/2017 02:16:26 AM	Google Inc	ne_updater.exe	NTPLDTBLR17
⊞	□	11/15/2017 02:16:26 AM	Google Inc		NTPLDTBLR17
⊞	□	11/14/2017 09:15:29 PM	Google Inc		NTPLDTBLR17
⊞	□	11/14/2017 09:15:23 PM	Google Inc		NTPLDTBLR17
⊞	□	11/14/2017 09:11:33 PM	Google Inc		NTPLDTBLR17
⊞	□	11/14/2017 09:10:31 PM	Google Inc		NTPLDTBLR17
⊞	□	11/14/2017 09:10:27 PM	Google Inc		NTPLDTBLR17

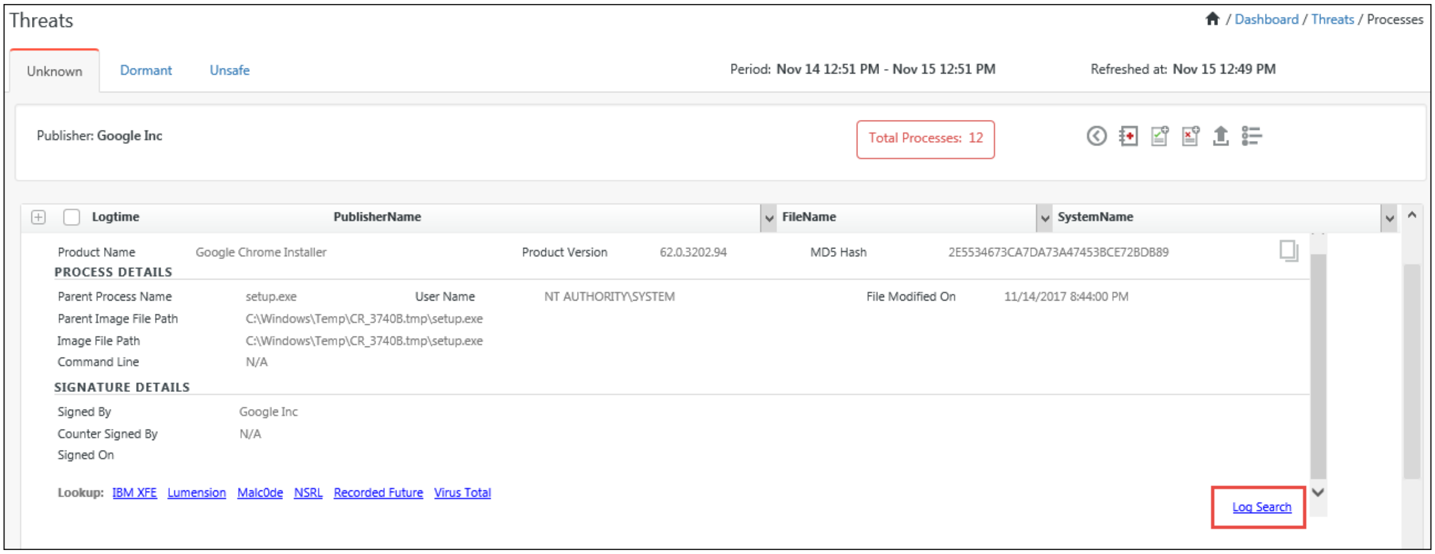
Figure 76

5. To export the details for selected file name, select it and then click Export ⬆.

2.4.4 Log Search for a process

In the Process file detail window, expand a process.

The below figure appears:



Period: Nov 14 12:51 PM - Nov 15 12:51 PM

Refreshed at: Nov 15 12:49 PM

Publisher: Google Inc

Product Name Google Chrome Installer Product Version 62.0.3202.94 MD5 Hash 2E5534673CA7DA73A47453BCE72BDB89

PROCESS DETAILS

Parent Process Name setup.exe User Name NT AUTHORITY\SYSTEM File Modified On 11/14/2017 8:44:00 PM

Parent Image File Path C:\Windows\Temp\CR_3740B.tmp\setup.exe

Image File Path C:\Windows\Temp\CR_3740B.tmp\setup.exe

Command Line N/A

SIGNATURE DETAILS

Signed By Google Inc

Counter Signed By N/A

Signed On

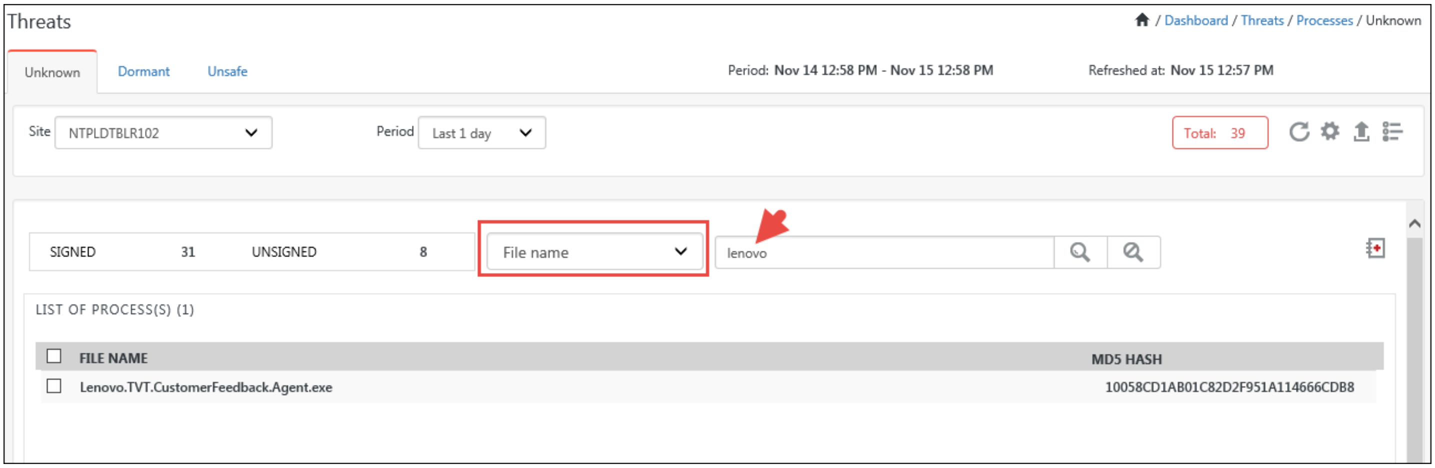
Figure 77

- Click the **Log Search** link, to perform a search.
- The users can also lookup for these unknown processes against the service providers i.e. **IBM XFE**/ **Lumension / NSRL/ VirusTotal, etc.** and by selecting the respective hyperlink. If the user is still not satisfied with the severity results for the process, he can use the unique MD5 Hash to search the severity of the process in some other Service provider.

2.4.5 Searching using File Name/ MD5 Hash

File Name

- To search using the File name, select **File name** from the dropdown list and then enter the name of the file in the search box and click search 🔍.



Period: Nov 14 12:58 PM - Nov 15 12:58 PM

Refreshed at: Nov 15 12:57 PM

Site NTPLDTBLR102 Period Last 1 day Total: 39

SIGNED 31 UNSIGNED 8 File name lenovo

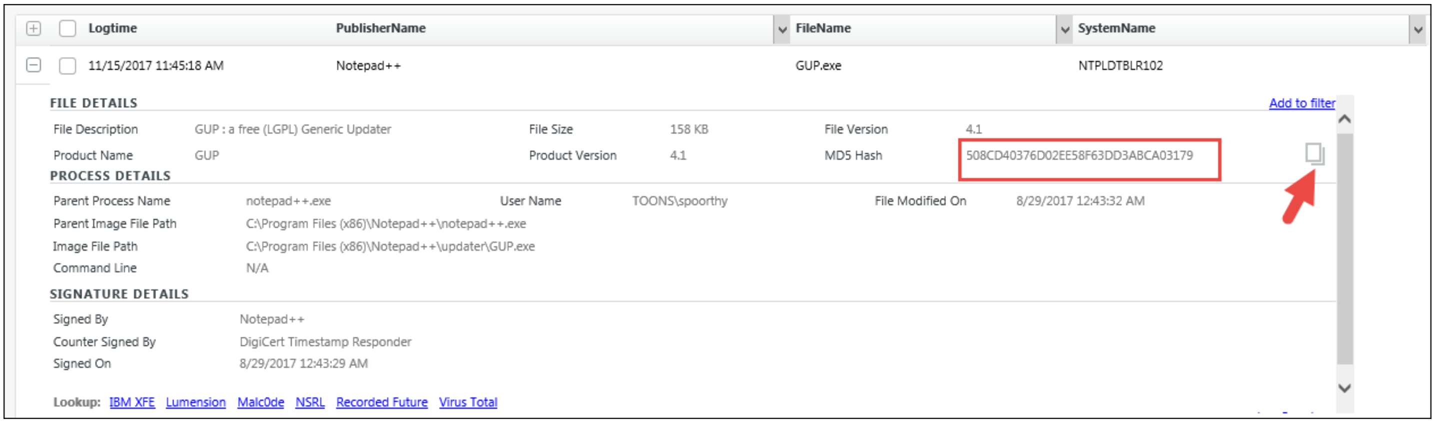
□	FILE NAME	MD5 HASH
□	Lenovo.TVT.CustomerFeedback.Agent.exe	10058CD1AB01C82D2F951A114666CDB8

Figure 78

MD5 Hash

- Copy the MD5 Hash unique code by clicking the icon ❐ .

  This is shown in the figure below:



⊞ ☐ Logtime	PublisherName	FileName	SystemName
⊟ ☐ 11/15/2017 11:45:18 AM	Notepad++	GUP.exe	NTPLDTBLR102

FILE DETAILS

Add to filter

File Description	GUP : a free (LGPL) Generic Updater	File Size	158 KB	File Version	4.1
Product Name	GUP	Product Version	4.1	MD5 Hash	508CD40376D02EE58F63DD3ABCA03179

PROCESS DETAILS

Parent Process Name	notepad++.exe	User Name	TOONS\spoorthy	File Modified On	8/29/2017 12:43:32 AM
Parent Image File Path	C:\Program Files (x86)\Notepad++\notepad++.exe				
Image File Path	C:\Program Files (x86)\Notepad++\updater\GUP.exe				
Command Line	N/A				

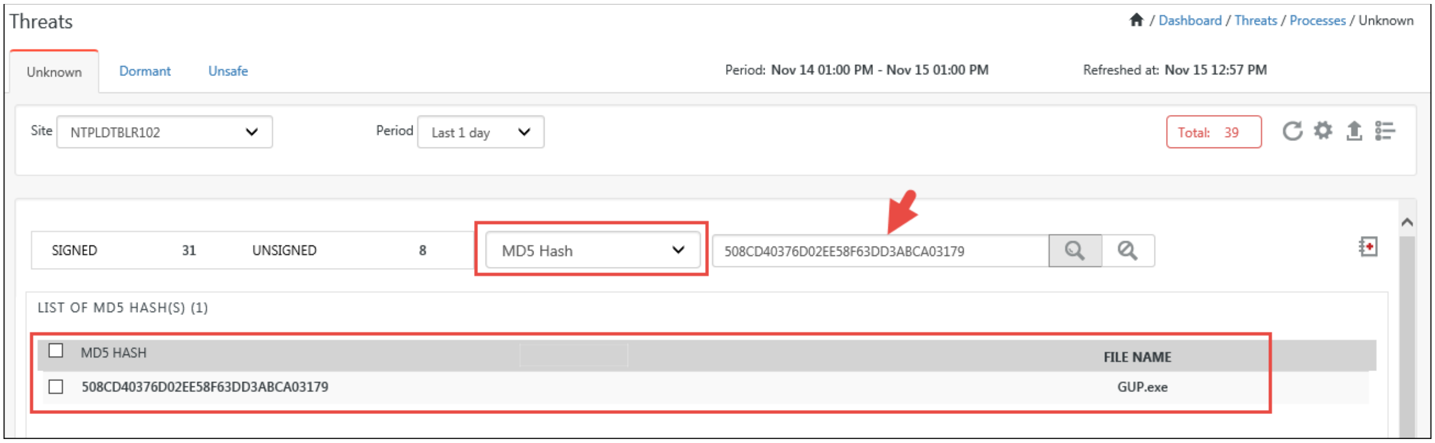
SIGNATURE DETAILS

Signed By	Notepad++
Counter Signed By	DigiCert Timestamp Responder
Signed On	8/29/2017 12:43:29 AM

Lookup: IBM XFE Lumension Malc0de NSRL Recorded Future Virus Total

Figure 79

- Now to perform a search using the MD5 hash, select MD 5 Hash from the drop-down list and paste the unique code in the search box.
- Click Search 🔍.
  The list opens.



Threats

Period: Nov 14 01:00 PM - Nov 15 01:00 PM

Refreshed at: Nov 15 12:57 PM

Site NTPLDTBLR102

Period Last 1 day

Total: 39

SIGNED 31 UNSIGNED 8

MD5 Hash

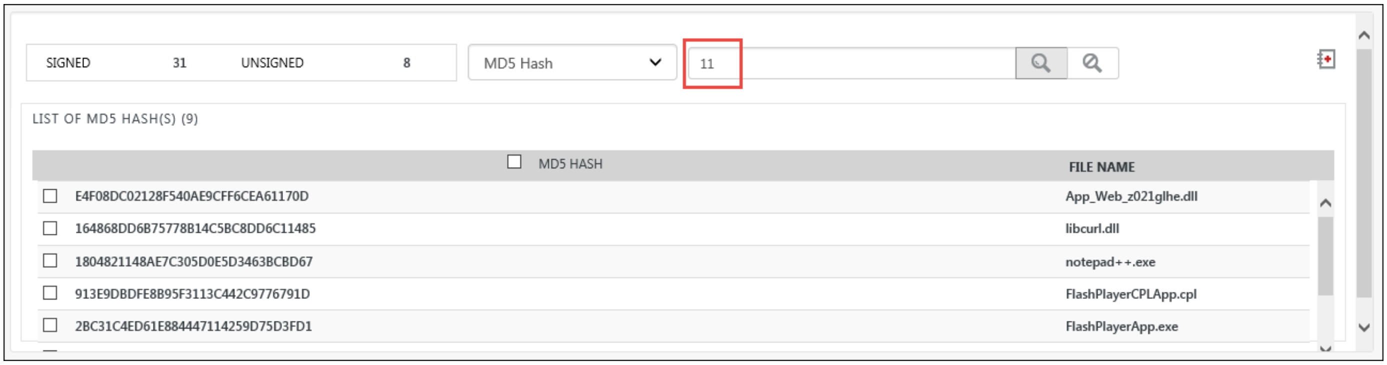
508CD40376D02EE58F63DD3ABCA03179

LIST OF MD5 HASH(S) (1)

☐ MD5 HASH	FILE NAME
☐ 508CD40376D02EE58F63DD3ABCA03179	GUP.exe

Figure 80

- The user can also simply type the random code details to perform a search.



SIGNED 31 UNSIGNED 8

MD5 Hash

11

LIST OF MD5 HASH(S) (9)

☐ MD5 HASH	FILE NAME
☐ E4F08DC02128F540AE9CFF6CEA61170D	App_Web_z021glhe.dll
☐ 164868DD6B75778B14C5BC8DD6C11485	libcurl.dll
☐ 1804821148AE7C305D0E5D3463BCBD67	notepad++.exe
☐ 913E9DBDFE8B95F3113C442C9776791D	FlashPlayerCPLApp.cpl
☐ 2BC31C4ED61E884447114259D75D3FD1	FlashPlayerApp.exe

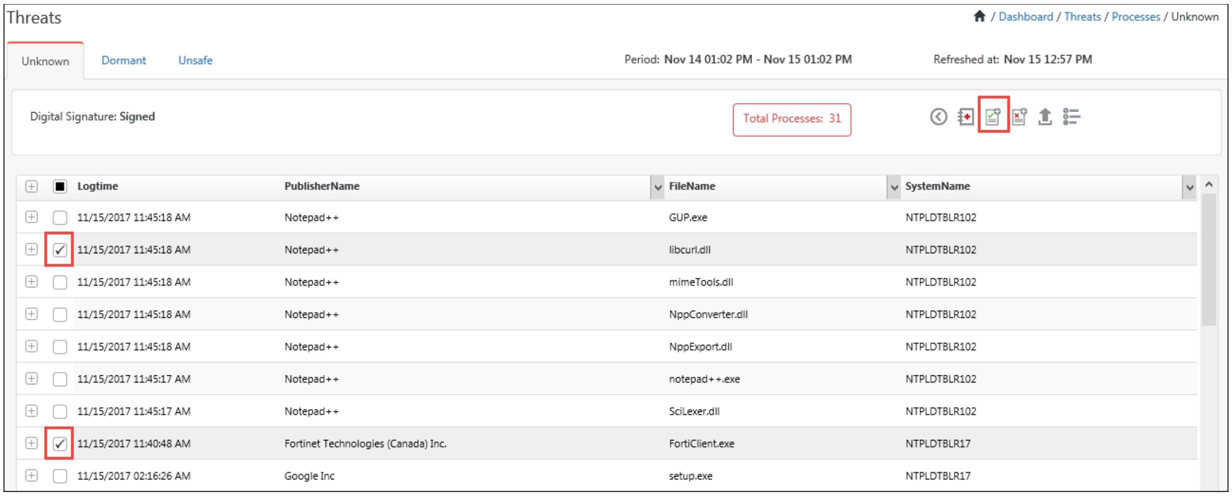
Figure 81

2.4.6 Adding to Safe List/Unsafe List

- To add a process to the safe list, use the icon .

It is added in the safe list under the feature Active Watch List.

For e.g. If the user wants to move the "**csc.exe**" in to the safe list, select the checkbox and click the Add to safe list icon .



Threats

/ Dashboard / Threats / Processes / Unknown

Unknown Dormant Unsafe

Period: Nov 14 01:02 PM - Nov 15 01:02 PM

Refreshed at: Nov 15 12:57 PM

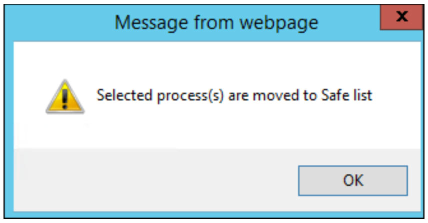
Digital Signature: Signed

Total Processes: 31

■ Logtime	PublisherName	FileName	SystemName
☐ 11/15/2017 11:45:18 AM	Notepad++	GUP.exe	NTPLDTBLR102
☑ 11/15/2017 11:45:18 AM	Notepad++	libcurl.dll	NTPLDTBLR102
☐ 11/15/2017 11:45:18 AM	Notepad++	mimeTools.dll	NTPLDTBLR102
☐ 11/15/2017 11:45:18 AM	Notepad++	NppConverter.dll	NTPLDTBLR102
☐ 11/15/2017 11:45:18 AM	Notepad++	NppExport.dll	NTPLDTBLR102
☐ 11/15/2017 11:45:17 AM	Notepad++	notepad++.exe	NTPLDTBLR102
☐ 11/15/2017 11:45:17 AM	Notepad++	SciLexer.dll	NTPLDTBLR102
☑ 11/15/2017 11:40:48 AM	Fortinet Technologies (Canada) Inc.	FortiClient.exe	NTPLDTBLR17
☐ 11/15/2017 02:16:26 AM	Google Inc	setup.exe	NTPLDTBLR17

Figure 82

The below message gets appears:



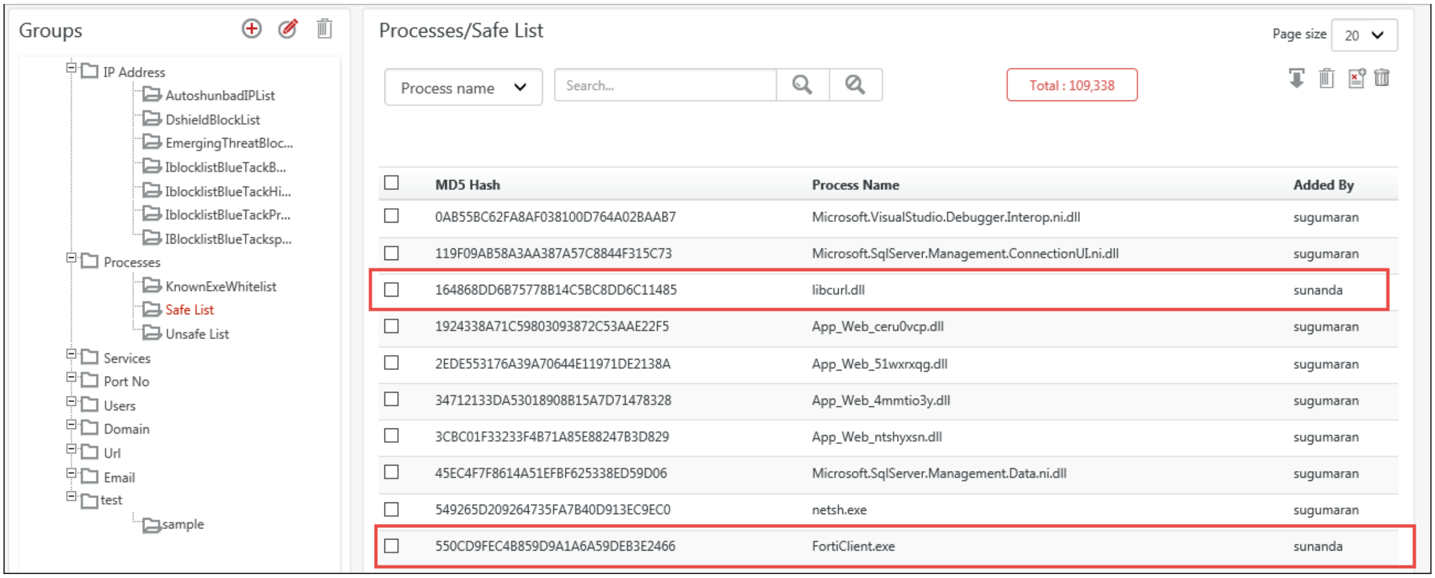
Message from webpage

Selected process(s) are moved to Safe list

OK

Figure 83

- Go to **Admin**> **Active Watch List**.
  - It will get added under the Safe list in **Admin**>**Active Watch List**.



□	MD5 Hash	Process Name	Added By
□	0AB55BC62FA8AF038100D764A02BAAB7	Microsoft.VisualStudio.Debugger.Interop.ni.dll	sugumaran
□	119F09AB58A3AA387A57C8844F315C73	Microsoft.SqlServer.Management.ConnectionUI.ni.dll	sugumaran
□	164868DD6B75778B14C5BC8DD6C11485	libcurl.dll	sunanda
□	1924338A71C59803093872C53AAE22F5	App_Web_ceru0vcp.dll	sugumaran
□	2EDE553176A39A70644E11971DE2138A	App_Web_51wxrxqg.dll	sugumaran
□	34712133DA53018908B15A7D71478328	App_Web_4mmtio3y.dll	sugumaran
□	3CBC01F33233F4B71A85E88247B3D829	App_Web_ntshyxsn.dll	sugumaran
□	45EC4F7F8614A51EFBF625338ED59D06	Microsoft.SqlServer.Management.Data.ni.dll	sugumaran
□	549265D209264735FA7B40D913EC9EC0	netsh.exe	sugumaran
□	550CD9FEC4B859D9A1A6A59DEB3E2466	FortiClient.exe	sunanda

Figure 84

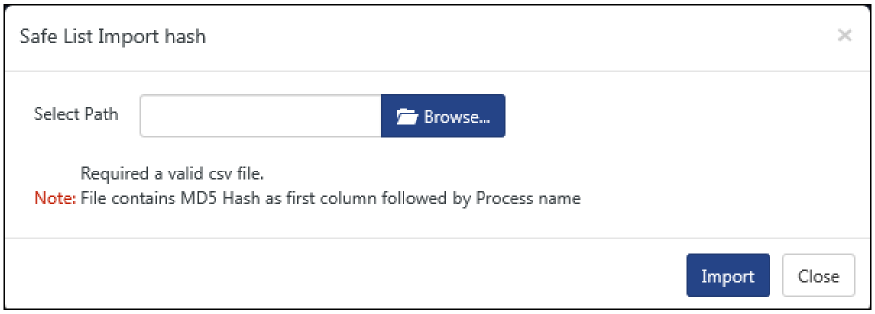
- Click the move to unsafe icon to move it unsafe list.
- The Delete All icon will delete all the processes.
- To delete a process or multiple processes, select the processes and click Delete icon .

NOTE: The user can follow the same process to add a process or multiple processes to the unsafe list by clicking the Add to unsafe list icon .

2.4.7 Importing Process to Safe List/Unsafe List

To Import,

- Click Import .



Required a valid csv file.

Note: File contains MD5 Hash as first column followed by Process name

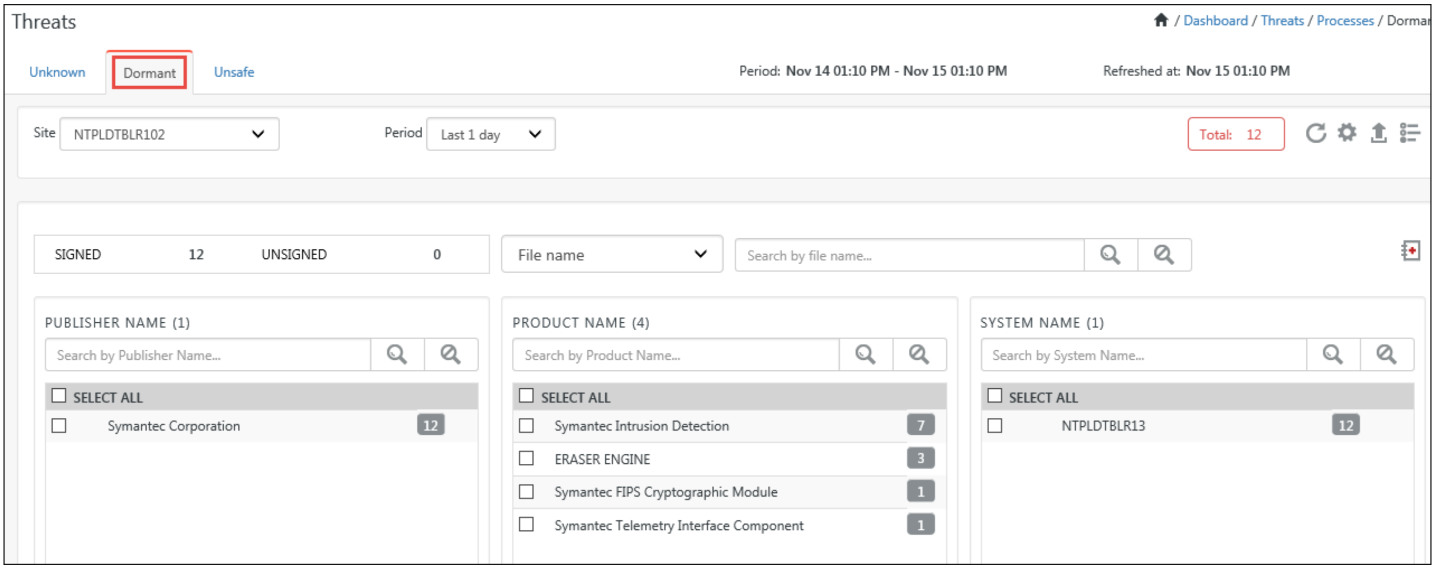
Figure 85

- Browse the path and select Import ⤓.

NOTE: The file should be a valid CSV file containing MD5 Hash as first column and Process name as second column.

2.5 Dormant tab

The dormant tab displays all the process which were not been executed.



Threats

🏠 / Dashboard / Threats / Processes / Dormar

Unknown | Dormant | Unsafe

Period: Nov 14 01:10 PM - Nov 15 01:10 PM

Refreshed at: Nov 15 01:10 PM

Site: NTPLDTBLR102

Period: Last 1 day

Total: 12

SIGNED 12 UNSIGNED 0

File name

Search by file name...

PUBLISHER NAME (1)

Search by Publisher Name...

□ SELECT ALL

□	Symantec Corporation	12

PRODUCT NAME (4)

Search by Product Name...

□ SELECT ALL

□	Symantec Intrusion Detection	7
□	ERASER ENGINE	3
□	Symantec FIPS Cryptographic Module	1
□	Symantec Telemetry Interface Component	1

SYSTEM NAME (1)

Search by System Name...

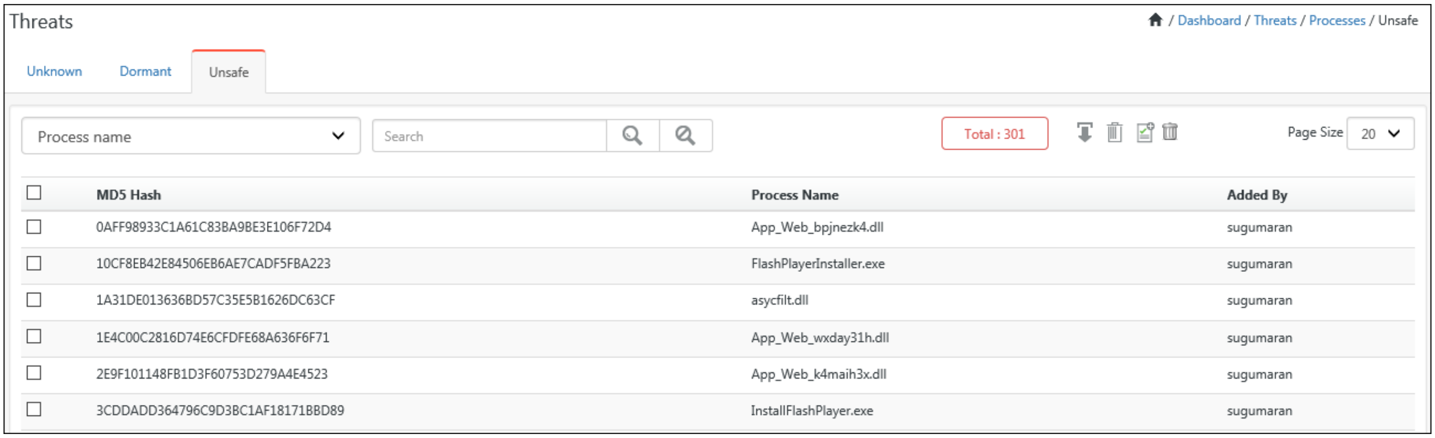
□ SELECT ALL

□	NTPLDTBLR13	12

Figure 86

2.6 Unsafe processes

The unsafe processes get listed in this page.



Threats

🏠 / Dashboard / Threats / Processes / Unsafe

Unknown | Dormant | Unsafe

Process name

Search

Total : 301

Page Size 20

□	MD5 Hash	Process Name	Added By
□	0AFF98933C1A61C83BA9BE3E106F72D4	App_Web_bpjnezk4.dll	sugumaran
□	10CF8EB42E84506EB6AE7CADF5FBA223	FlashPlayerInstaller.exe	sugumaran
□	1A31DE013636BD57C35E5B1626DC63CF	asycfilt.dll	sugumaran
□	1E4C00C2816D74E6CFDFE68A636F6F71	App_Web_wxday31h.dll	sugumaran
□	2E9F101148FB1D3F60753D279A4E4523	App_Web_k4maih3x.dll	sugumaran
□	3CDDADD364796C9D3BC1AF18171BBD89	InstallFlashPlayer.exe	sugumaran

Figure 87

2.7 Incidents tab

- Incidents Dashboard
- Dashboard view
- Graphical view
- Tabular view
- Advanced search
- Tile View

2.7.1 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.

The Incidents Dashboard of a Collection Master (CM) now provides critical information about Collection Points (CP) also. You can sort the machines based on the Collection Points or Risk. By Default, Incidents Dashboard displays All Sites sorted based on Collection Points or Risk. It displays all the sites in which major incidents have occurred.

2.7.1.1 Analyzing incidents dashboard

1 Log on to **EventTracker,** under **Dashboard,** select the **Incidents** option.

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, Incidents Dashboard displays All Sites sorted based on Collection Points or Risk (By Default, Incidents Dashboard displays All Sites sorted by Risk in CM).

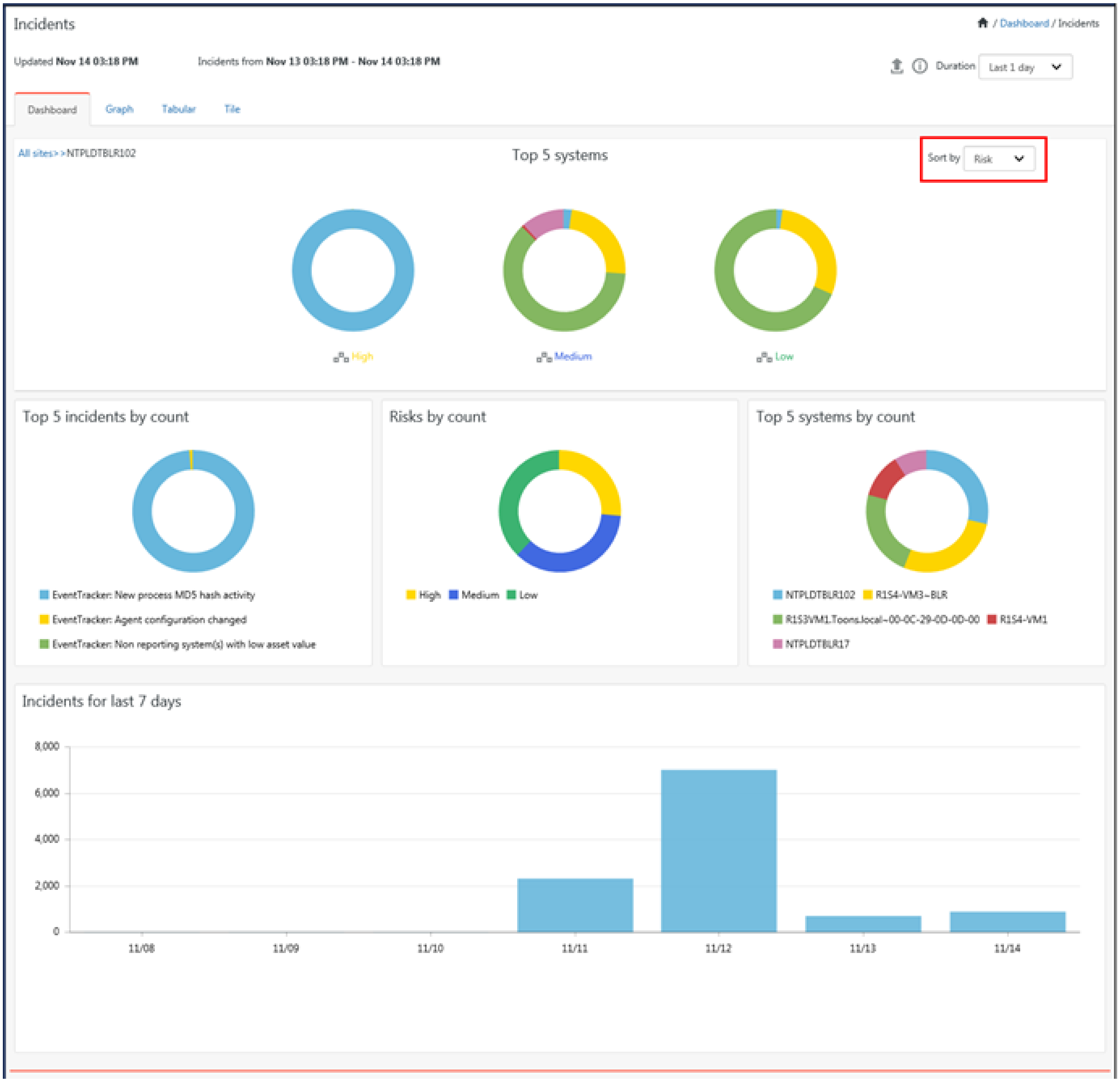
- You can sort the machines based on the Collection Points or Risk (We can sort by Risk/Sites in a CM and in the CP and standard by Risk/Systems)

- By default, EventTracker displays the incidents that are generated for past 24 hours in the Top 5 systems by Risk. (Top 5 sites by risk in the CM and top 5 systems by risk in the CP and Standard). It also displays the Incident for the last 7 days.

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

- In Top 5 incidents by Risk pane, it provides details about the incidents that have been identified based on the severity (It is risks by count and can be classified as Critical, Serious, High, Medium, and 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.
- Now if you select any Collection Point or Collection Master node in Top 5 sites by risk pane, you can further drill down to view the incidents/alerts generated at the respective individual systems.



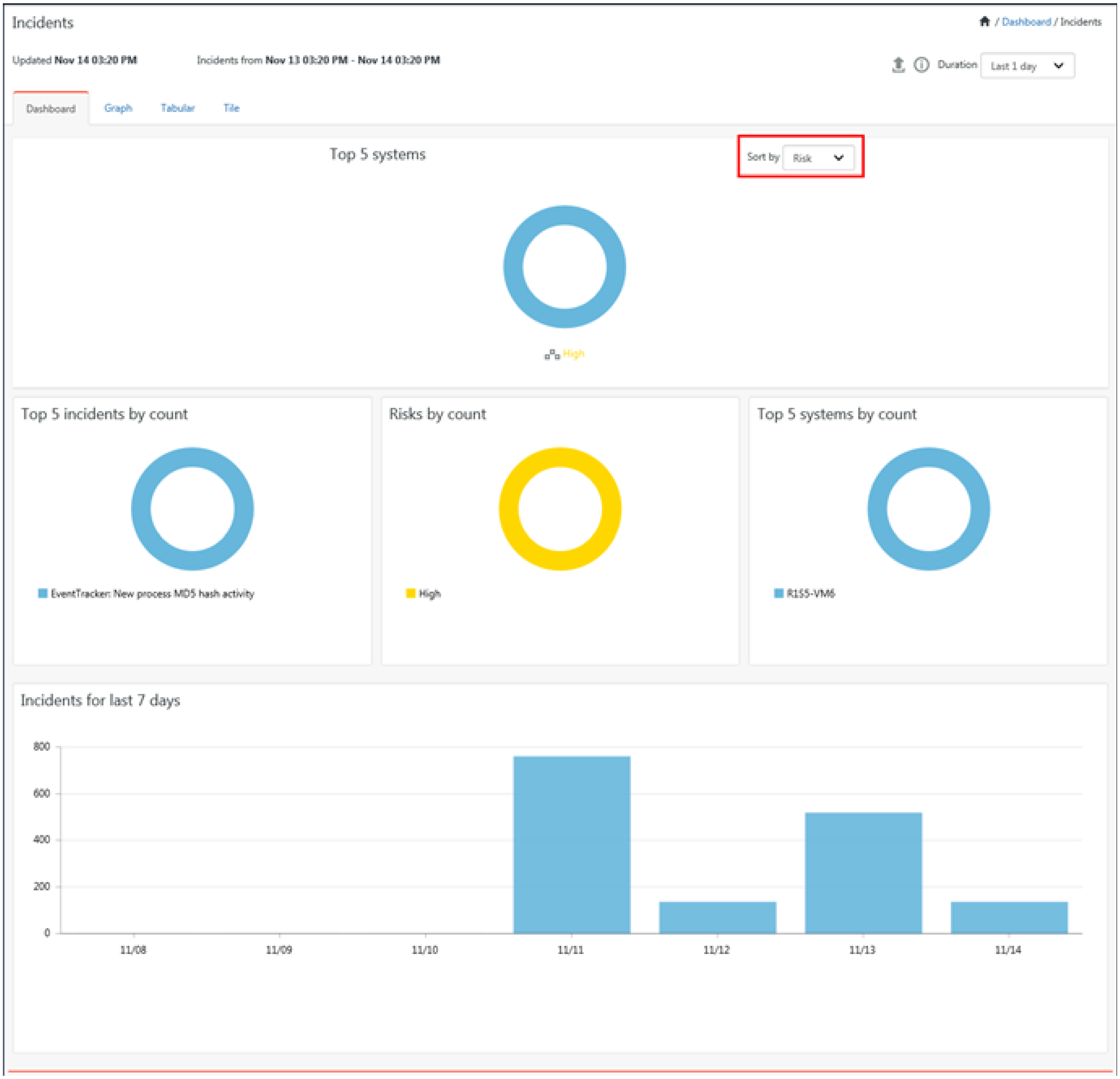
Updated **Nov 14 03:18 PM**

Incidents from **Nov 13 03:18 PM - Nov 14 03:18 PM**

Duration Last 1 day

Sort by Risk

Figure 88



Incidents

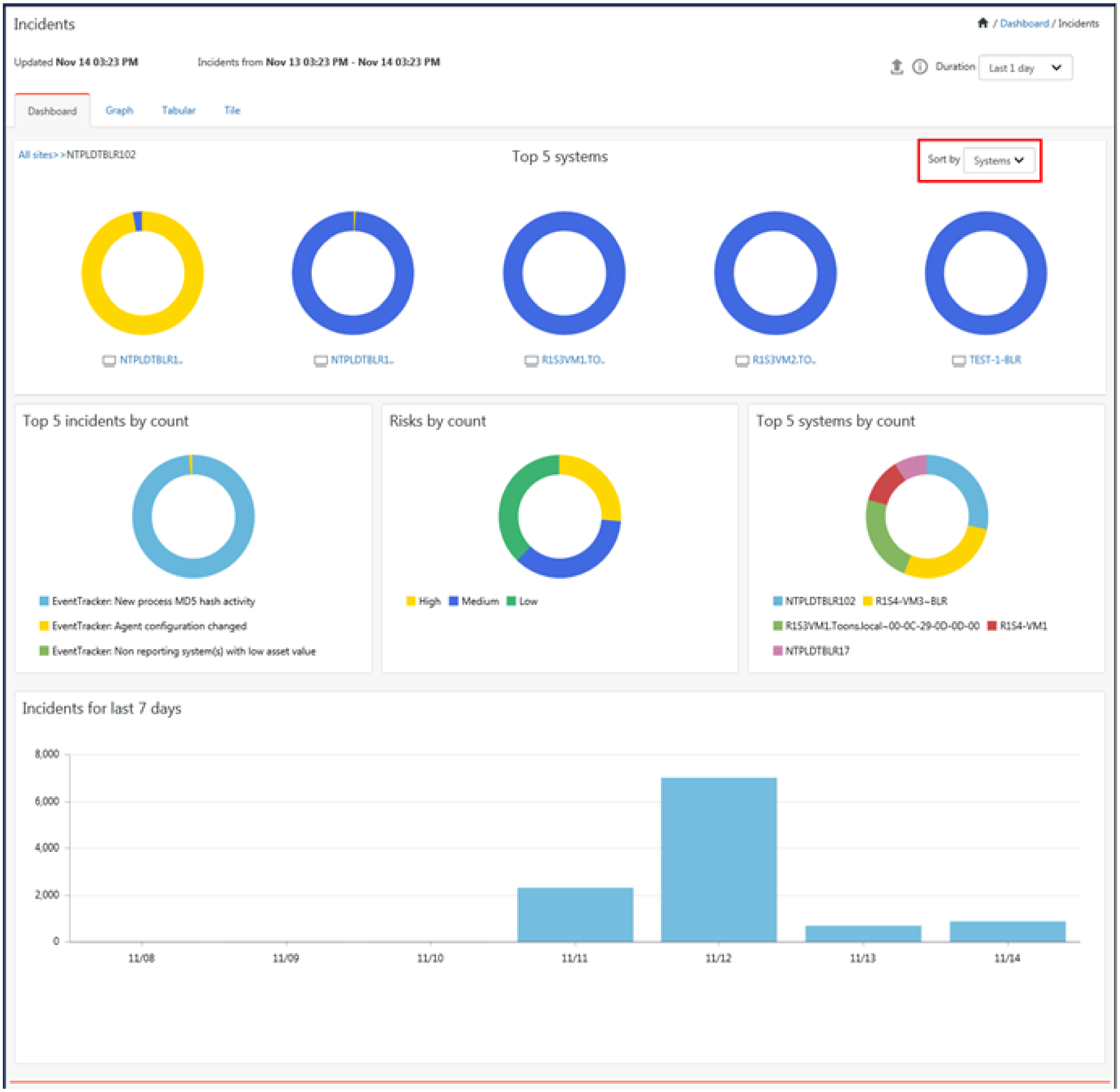
🏠 / Dashboard / Incidents

Updated **Nov 14 03:20 PM** Incidents from **Nov 13 03:20 PM - Nov 14 03:20 PM**

Duration: Last 1 day

Figure 89

2 In a Collection Master, click 品 hyperlink and **All sites** are displayed.



Updated **Nov 14 03:23 PM** Incidents from **Nov 13 03:23 PM - Nov 14 03:23 PM**

Duration: Last 1 day

Figure 90

3 To view systems by risk, click **Sort by** drop down, and then select **Risk.**
You can view sites by risk in a CM and in the CP it will be systems.

4 To view by systems, click **Sort by** drop down, and then select **Sites**.
You can view sites in a CM and in CP it will be systems.

5 To view the duration of incident details, click **Duration** drop down, and then select the required option.

2.7.1.2 Exporting incidents dashboard to excel

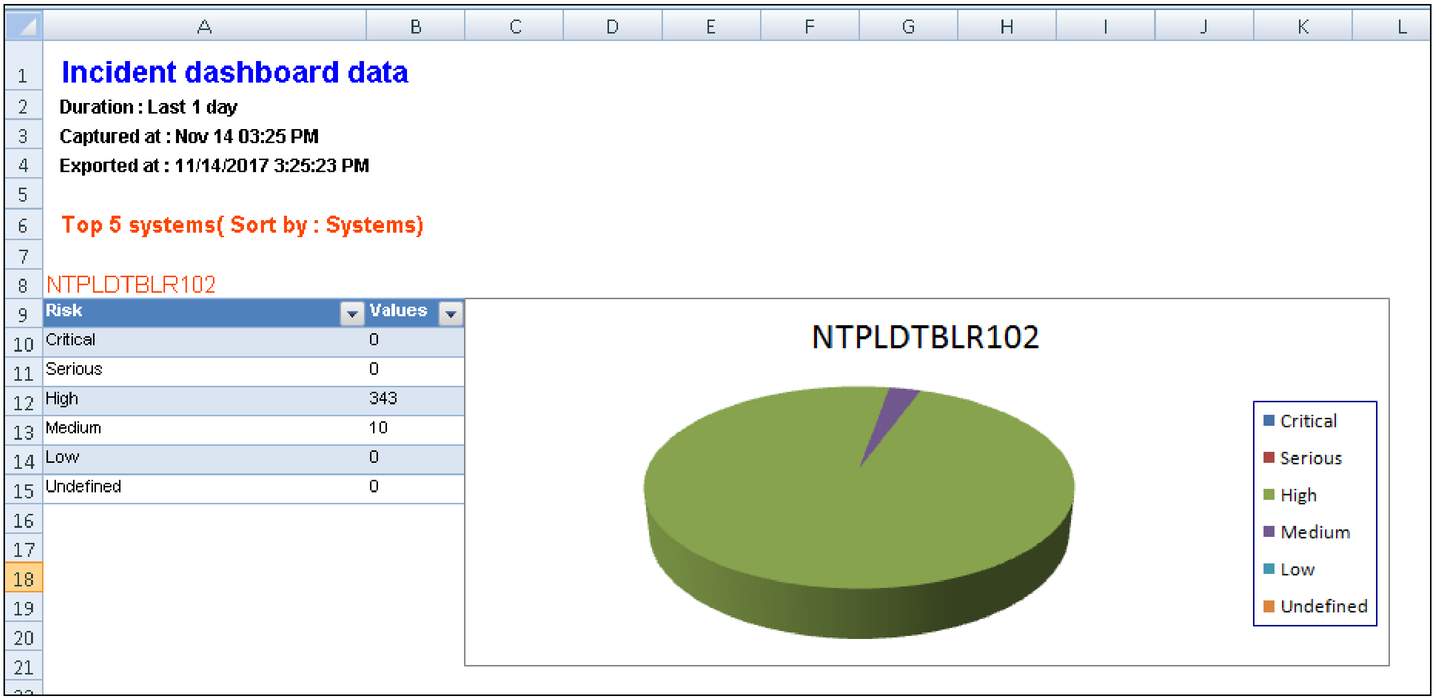
a. To view the summary of incidents dashboard in excel, click **Export** to export the data.

b. To view the file on local drive, click **Save**.

(OR)

To open the file directly, click **Open**.

A sample report is shown in the picture below.



Incident dashboard data

Duration : Last 1 day

Captured at : Nov 14 03:25 PM

Exported at : 11/14/2017 3:25:23 PM

Top 5 systems(Sort by : Systems)

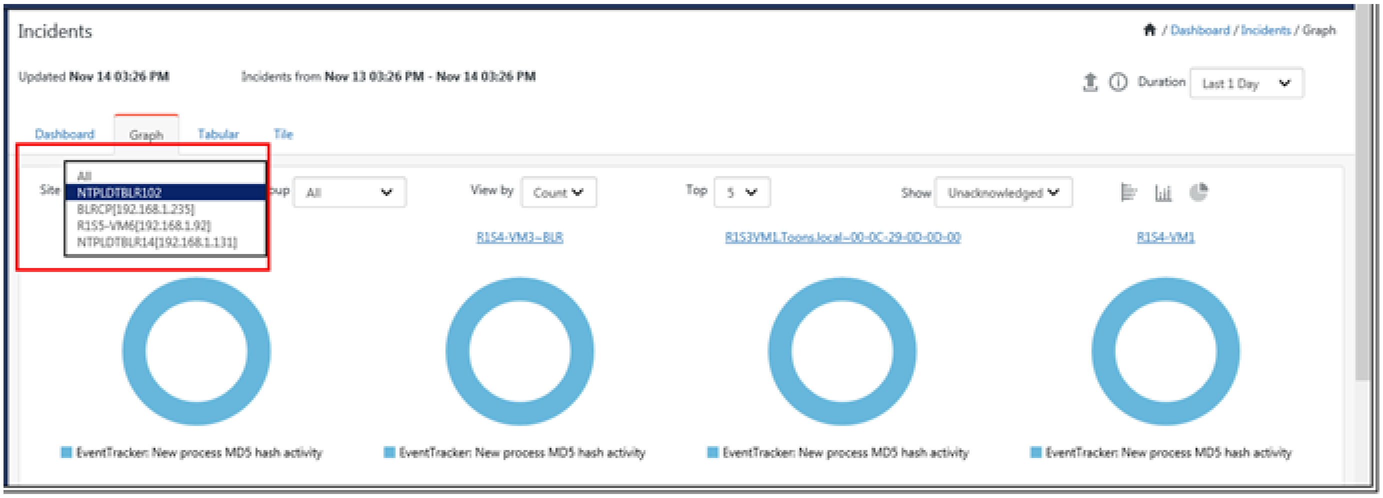
NTPLDTBLR102

Risk	Values
Critical	0
Serious	0
High	343
Medium	10
Low	0
Undefined	0

Figure 91

2.7.2 Graphical View

1. Select **Graph** tab.



Incidents

Updated Nov 14 03:26 PM

Incidents from Nov 13 03:26 PM - Nov 14 03:26 PM

Duration: Last 1 Day

Site: NTPLDTBLR102

Group: All

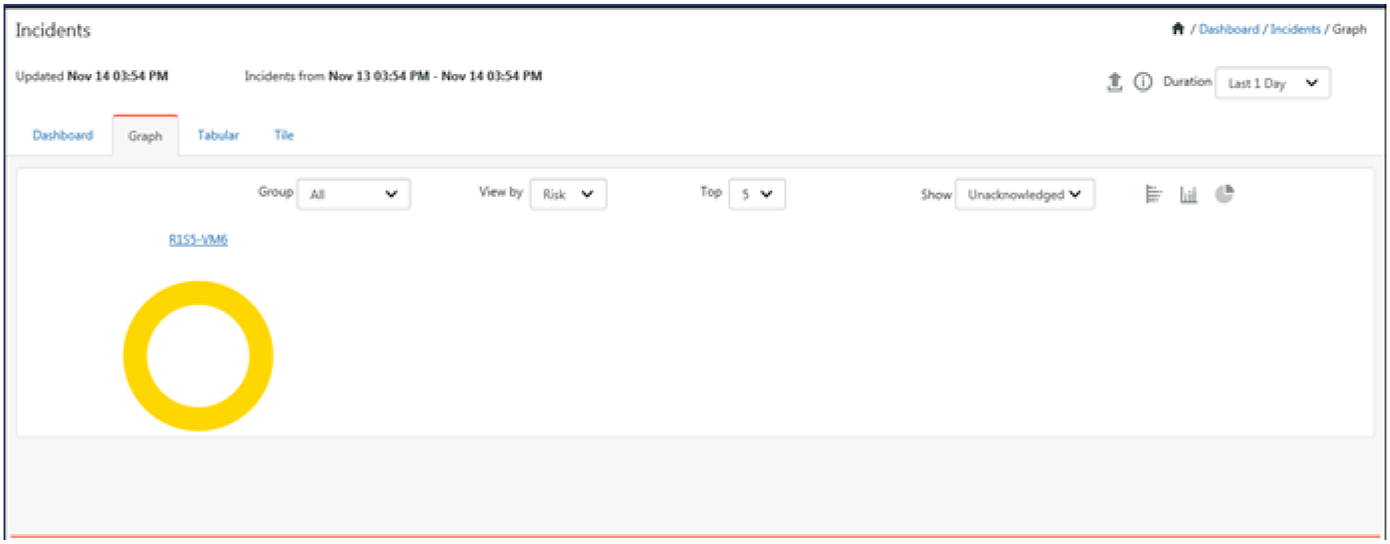
View by: Count

Top: 5

Show: Unacknowledged

/ Dashboard / Incidents / Graph
Dashboard
Graph
Tabular
Tile
All
NTPLDTBLR102
BLRCP[192.168.1.235]
R1S5-VM6[192.168.1.92]
NTPLDTBLR14[192.168.1.131]
R1S4-VM3~BLR
R1S3VM1.Toons.local~00-0C-29-0D-0D-00
R1S4-VM1
EventTracker: New process MD5 hash activity
EventTracker: New process MD5 hash activity
EventTracker: New process MD5 hash activity
EventTracker: New process MD5 hash activity

Figure 92



Incidents

Updated Nov 14 03:54 PM

Incidents from Nov 13 03:54 PM - Nov 14 03:54 PM

Duration: Last 1 Day

Group: All

View by: Risk

Top: 5

Show: Unacknowledged

Figure 93

The graphical view pane will list the Top 5 unacknowledged incidents by Risk or Count. The pictorial representation can be viewed in donut, bar or stacked bar graph.

Incidents Dashboard – Graphical View	
Field	**Description**
Sites	In a Collection Master, all sites are displayed. You cannot view this option in a Collection Point.
Group	In a Collection Point, enterprise system groups are listed in this drop-down list. By default, EventTracker selects the ALL option. NOTE: You cannot view this option in a Collection Master.
View By	View data by risk or count.
Top	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.
Acknowledged	Select this option to see the list of incidents that are acknowledged. By default, the dashboard displays only the unacknowledged incidents.

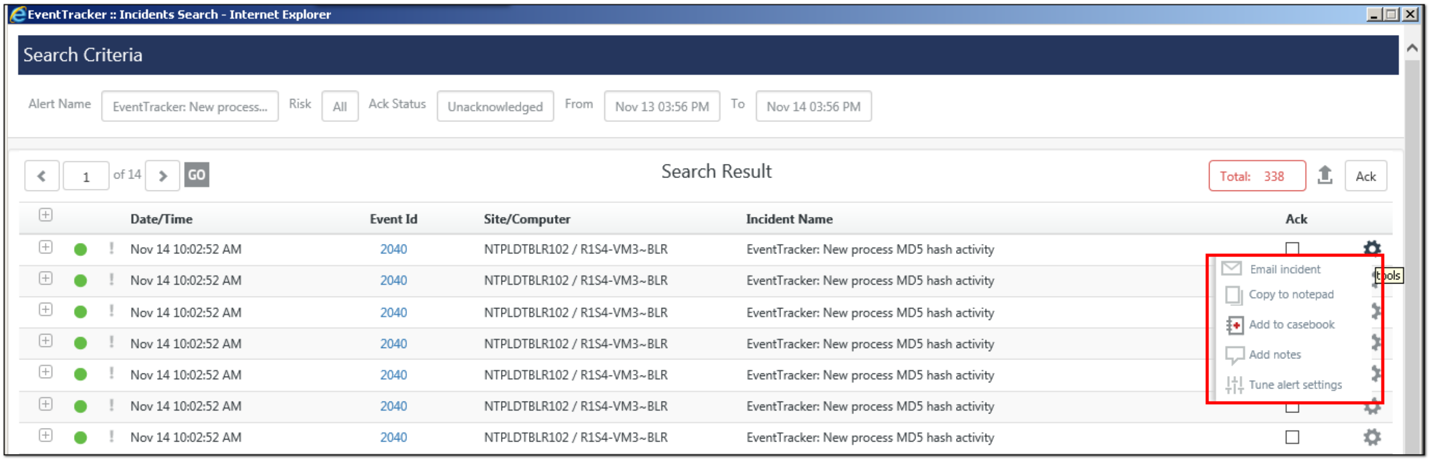
Table 12

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

2.7.3 Searching Incidents

1 To view the total incidents occurred on a particular system; click a graph in ‘**Incidents’** or ‘**Graph’** tab.

   Search Incidents Window opens.



EventTracker :: Incidents Search - Internet Explorer

Search Criteria

Alert Name: EventTracker: New process... Risk: All Ack Status: Unacknowledged From: Nov 13 03:56 PM To: Nov 14 03:56 PM

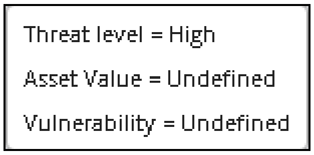
Search Result

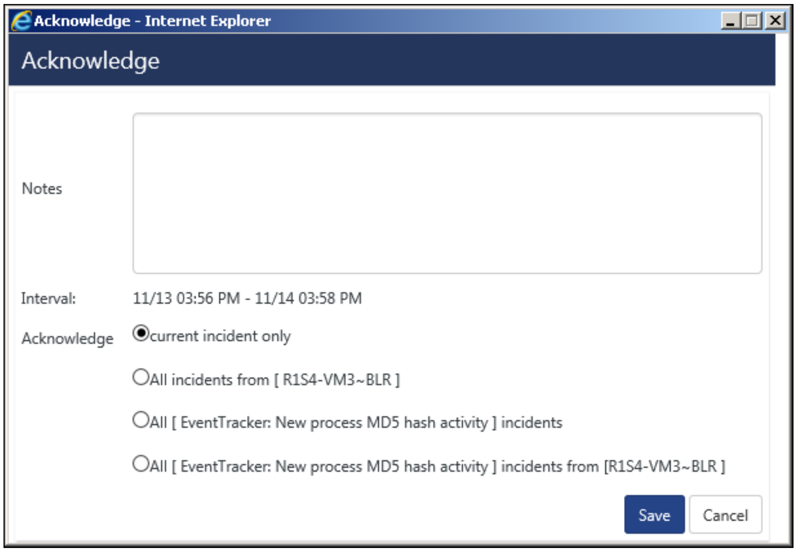
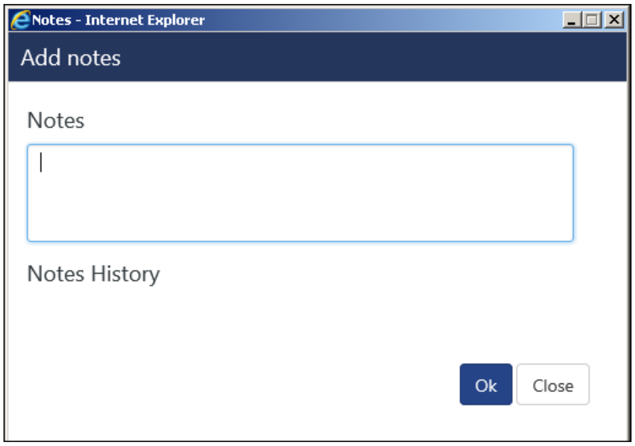
1 of 14 GO

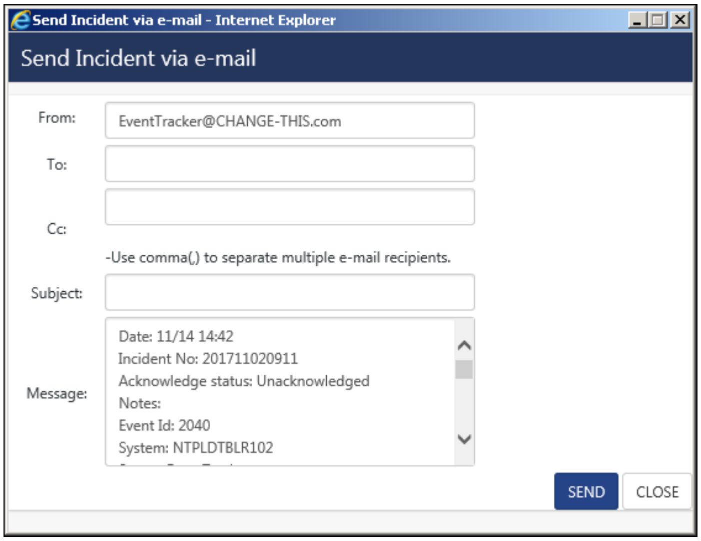
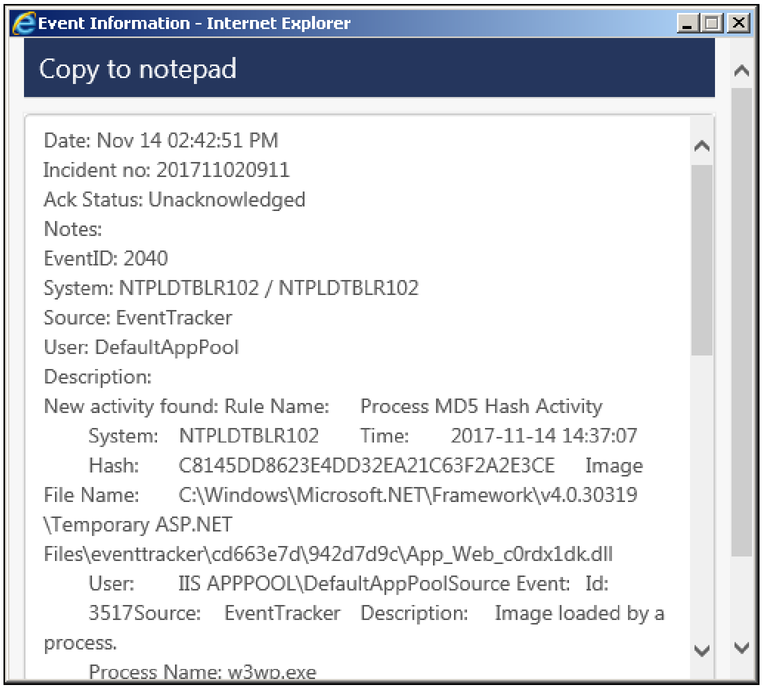
Total: 338

Date/Time	Event Id	Site/Computer	Incident Name	Ack
Nov 14 10:02:52 AM	2040	NTPLDTBLR102 / R1S4-VM3~BLR	EventTracker: New process MD5 hash activity	□
Nov 14 10:02:52 AM	2040	NTPLDTBLR102 / R1S4-VM3~BLR	EventTracker: New process MD5 hash activity	
Nov 14 10:02:52 AM	2040	NTPLDTBLR102 / R1S4-VM3~BLR	EventTracker: New process MD5 hash activity	
Nov 14 10:02:52 AM	2040	NTPLDTBLR102 / R1S4-VM3~BLR	EventTracker: New process MD5 hash activity	
Nov 14 10:02:52 AM	2040	NTPLDTBLR102 / R1S4-VM3~BLR	EventTracker: New process MD5 hash activity	
Nov 14 10:02:52 AM	2040	NTPLDTBLR102 / R1S4-VM3~BLR	EventTracker: New process MD5 hash activity	□
Nov 14 10:02:52 AM	2040	NTPLDTBLR102 / R1S4-VM3~BLR	EventTracker: New process MD5 hash activity	□

Figure 94

Field	Description
Date/Time	Date and time on which the incident occurred.
Incident #	A unique number assigned for each generated incident. 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.
Risk	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. For example:  Threat level = High Asset Value = Undefined Vulnerability = Undefined **When the vulnerability scanner(s) (ex: 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).**
Event Id	Event identifier associated with the generated alert.
System	The system name where the incident occurred.
Log Type	The event/incident recorded in the following logs i.e. Application, Security, System logs.
Source	The source of the event. This can be the name of a program, a system component, or an individual component of a large program.
User	The user name of the user that was logged on when the incident occurred.
Description	A brief description about the incident occurred.

Ack status	**Check this option to acknowledge the incident.** **EventTracker opens Bulk Acknowledge window.**  Acknowledge - Internet Explorer Acknowledge Notes Interval: 11/13 03:56 PM - 11/14 03:58 PM Acknowledge ● current incident only ○ All incidents from [R1S4-VM3~BLR] ○ All [EventTracker: New process MD5 hash activity] incidents ○ All [EventTracker: New process MD5 hash activity] incidents from [R1S4-VM3~BLR] Save Cancel **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 Save to save the information.**
Add Notes	**a) Click Add Notes.**  Notes - Internet Explorer Add notes Notes Notes History Ok Close 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.

Email Incident ✉	Email an incident including current Notes and Ack status. Click Email.  Send Incident via e-mail From: EventTracker@CHANGE-THIS.com To: Cc: -Use comma(,) to separate multiple e-mail recipients. Subject: Message: Date: 11/14 14:42 Incident No: 201711020911 Acknowledge status: Unacknowledged Notes: Event Id: 2040 System: NTPLDTBLR102 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 -> Email Configuration.
Copy to Notepad ❐	Click Copy to notepad icon. Event Information window opens with Event details.  Copy to notepad Date: Nov 14 02:42:51 PM Incident no: 201711020911 Ack Status: Unacknowledged Notes: EventID: 2040 System: NTPLDTBLR102 / NTPLDTBLR102 Source: EventTracker User: DefaultAppPool Description: New activity found: Rule Name: Process MD5 Hash Activity System: NTPLDTBLR102 Time: 2017-11-14 14:37:07 Hash: C8145DD8623E4DD32EA21C63F2A2E3CE Image File Name: C:\Windows\Microsoft.NET\Framework\v4.0.30319 \Temporary ASP.NET Files\eventtracker\cd663e7d\942d7d9c\App_Web_c0rdx1dk.dll User: IIS APPPOOL\DefaultAppPoolSource Event: Id: 3517Source: EventTracker Description: Image loaded by a process. Process Name: w3wp.exe

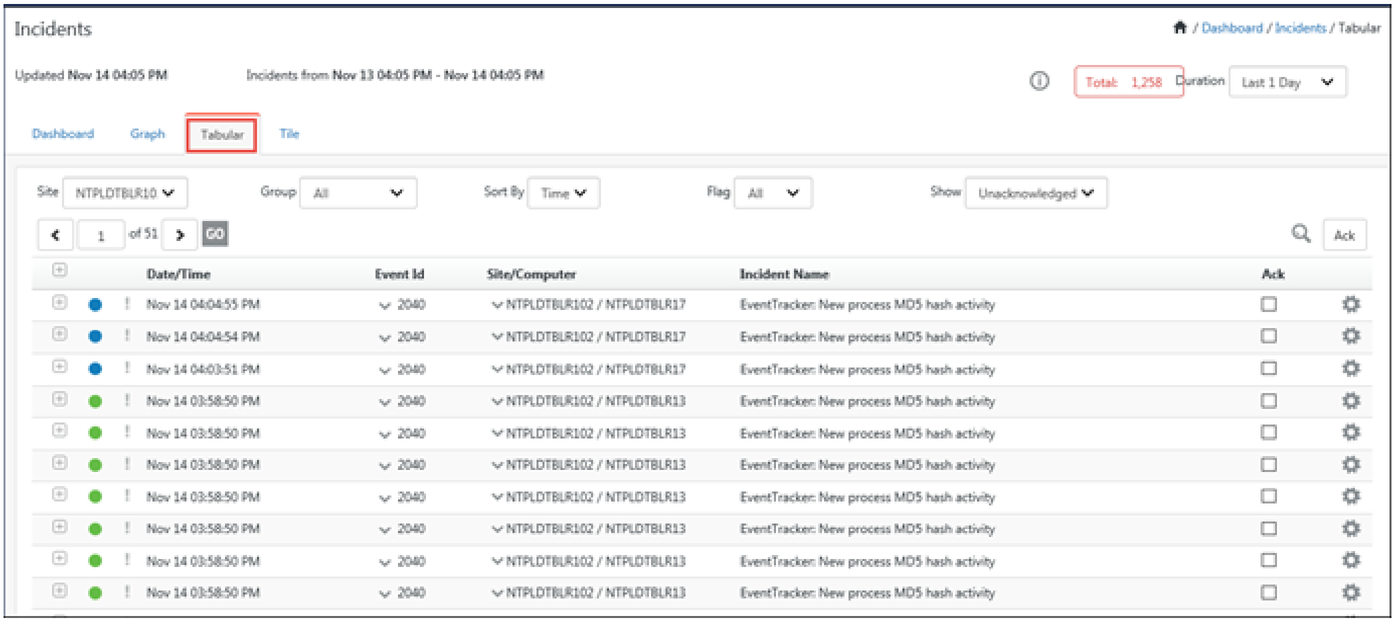
⬆	Click the icon to export the incident details in 'Excel' format.
🎚	EventTracker :: Alert Configuration window opens. For detail information please refer Alerts
📕	Click Casebook icon to view data in Casebook. For detail information please refer Casebook.

Table 13

2.7.4 Viewing incidents in Tabular View

1. Click the **Incident** menu, and then click **Tabular** tab.

   By default, EventTracker opens the unacknowledged incidents that are generated for past 24 hours. To view only the acknowledged incidents, click **Acknowledged** option from the drop-down box, as highlighted in the figure.



Incidents

🏠 / Dashboard / Incidents / Tabular

Updated Nov 14 04:05 PM

Incidents from Nov 13 04:05 PM - Nov 14 04:05 PM

Total: 1,258

Duration: Last 1 Day

Dashboard | Graph | Tabular | Tile

Site: NTPLDTBLR10

Group: All

Sort By: Time

Flag: All

Show: Unacknowledged

1 of 51 GO

Ack

⊞			Date/Time	Event Id	Site/Computer	Incident Name	Ack	
⊞	●	!	Nov 14 04:04:55 PM	2040	NTPLDTBLR102 / NTPLDTBLR17	EventTracker: New process MD5 hash activity	□	⚙
⊞	●	!	Nov 14 04:04:54 PM	2040	NTPLDTBLR102 / NTPLDTBLR17	EventTracker: New process MD5 hash activity	□	⚙
⊞	●	!	Nov 14 04:03:51 PM	2040	NTPLDTBLR102 / NTPLDTBLR17	EventTracker: New process MD5 hash activity	□	⚙
⊞	●	!	Nov 14 03:58:50 PM	2040	NTPLDTBLR102 / NTPLDTBLR13	EventTracker: New process MD5 hash activity	□	⚙
⊞	●	!	Nov 14 03:58:50 PM	2040	NTPLDTBLR102 / NTPLDTBLR13	EventTracker: New process MD5 hash activity	□	⚙
⊞	●	!	Nov 14 03:58:50 PM	2040	NTPLDTBLR102 / NTPLDTBLR13	EventTracker: New process MD5 hash activity	□	⚙
⊞	●	!	Nov 14 03:58:50 PM	2040	NTPLDTBLR102 / NTPLDTBLR13	EventTracker: New process MD5 hash activity	□	⚙
⊞	●	!	Nov 14 03:58:50 PM	2040	NTPLDTBLR102 / NTPLDTBLR13	EventTracker: New process MD5 hash activity	□	⚙
⊞	●	!	Nov 14 03:58:50 PM	2040	NTPLDTBLR102 / NTPLDTBLR13	EventTracker: New process MD5 hash activity	□	⚙
⊞	●	!	Nov 14 03:58:50 PM	2040	NTPLDTBLR102 / NTPLDTBLR13	EventTracker: New process MD5 hash activity	□	⚙

Figure 95

2. Click' ⊞ ' symbol to view detail information i.e. **Event Id, Source, Event Type, Description**.
3. Click **Flag** ! to change the status of the incident.

Flag icon	Description
! GRAY	No action has been taken
! RED	Relevant action is required for that particular incident to solve an issue
! GREEN	Checked the incident and necessary action has been taken care of.

Table 14

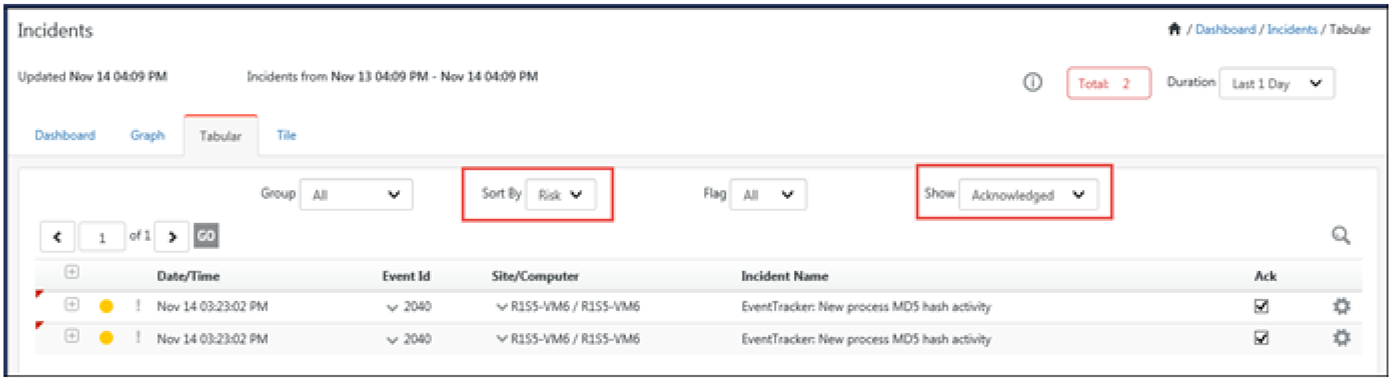
4. To acknowledge all incidents that have occurred, click **Ack** checkbox for the incident and then the **Ack**.

   This feature acknowledges the incidents present only in the same page.

   Bulk Acknowledge window opens.

5. Enter comments and then click **Save**.
6. To view the incidents that have been acknowledged, select the **Acknowledged** option from the drop-down box.

All the acknowledged incidents will be visible in Tabular View by selecting the **Acknowledged** option.



Incidents

Updated Nov 14 04:09 PM — Incidents from Nov 13 04:09 PM - Nov 14 04:09 PM — Total: 2 — Duration: Last 1 Day

Group: All — Sort By: Risk — Flag: All — Show: Acknowledged

			Date/Time	Event Id	Site/Computer	Incident Name	Ack
⊞	●	!	Nov 14 03:23:02 PM	2040	R1S5-VM6 / R1S5-VM6	EventTracker: New process MD5 hash activity	☑
⊞	●	!	Nov 14 03:23:02 PM	2040	R1S5-VM6 / R1S5-VM6	EventTracker: New process MD5 hash activity	☑

Figure 96

7. Click **Add Notes** to add comments about a incident.
8. Click **Email** to mail an incident.
9. Click **Casebook** to update data in Casebook.

   A Casebook message opens.

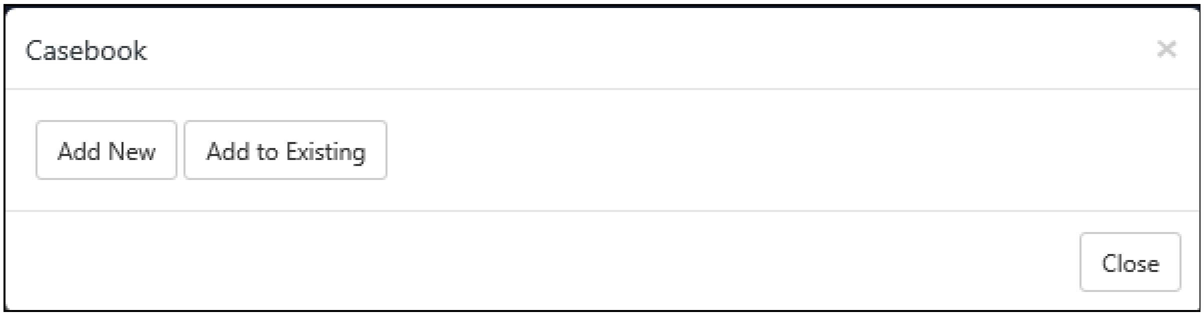
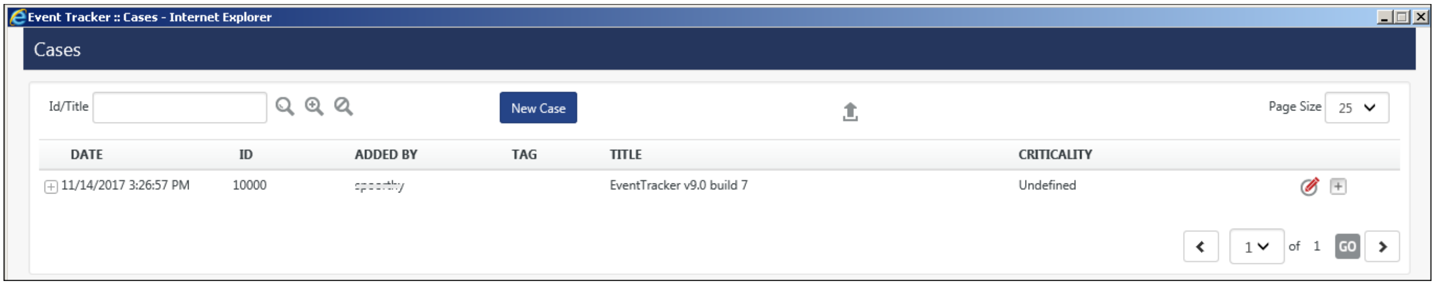


Figure 97

10. To add a new Casebook entry, click **Add new**.
11. To add to an existing Casebook, click **Add to existing**.

    Casebook window opens.



DATE	ID	ADDED BY	TAG	TITLE	CRITICALITY
11/14/2017 3:26:57 PM	10000	[redacted]		EventTracker v9.0 build 7	Undefined

Figure 98

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

    For detailed information about Casebook, refer Casebook.

2.7.5 Log Search feature

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

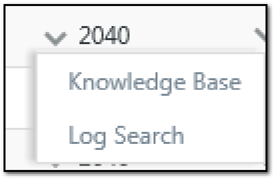


Figure 99

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

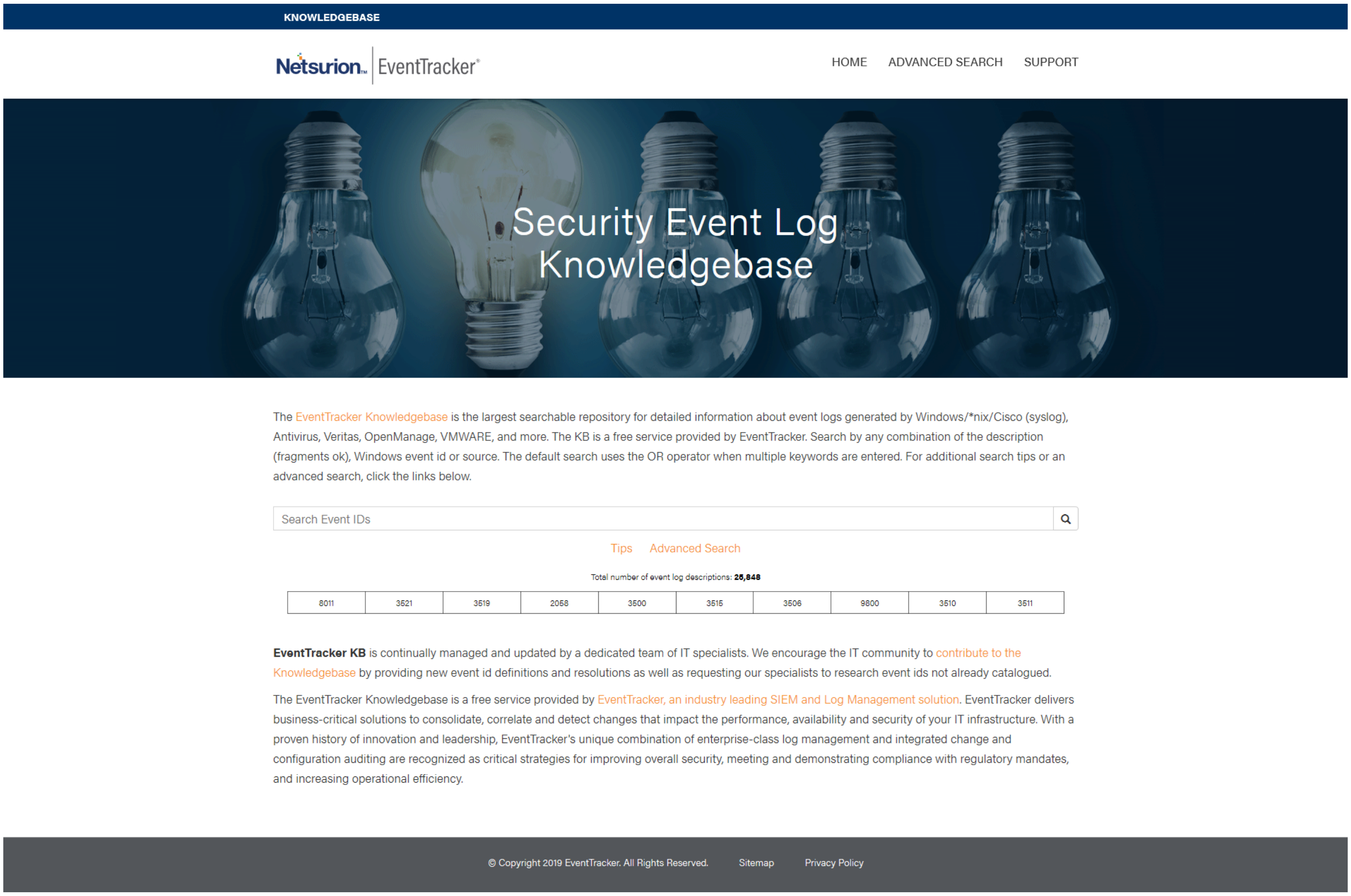
For more information on log search, refer https://www.netsurion.com/Corporate/media/Corporate/Files/Support-Docs/Feature-Guide-Log-Search-v8x.pdf document.

🗎 NOTE

In a collection master UI Tabular view, Log Search will not be shown for collection points.
For detail information on Alert configuration, refer Alerts.

2.8 Knowledge Base option

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



The EventTracker Knowledgebase is the largest searchable repository for detailed information about event logs generated by Windows/*nix/Cisco (syslog), Antivirus, Veritas, OpenManage, VMWARE, and more. The KB is a free service provided by EventTracker. Search by any combination of the description (fragments ok), Windows event id or source. The default search uses the OR operator when multiple keywords are entered. For additional search tips or an advanced search, click the links below.

Search Event IDs

Tips Advanced Search

Total number of event log descriptions: **25,848**

8011	3521	3519	2058	3500	3515	3506	9800	3510	3511

EventTracker KB is continually managed and updated by a dedicated team of IT specialists. We encourage the IT community to contribute to the Knowledgebase by providing new event id definitions and resolutions as well as requesting our specialists to research event ids not already catalogued.

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.

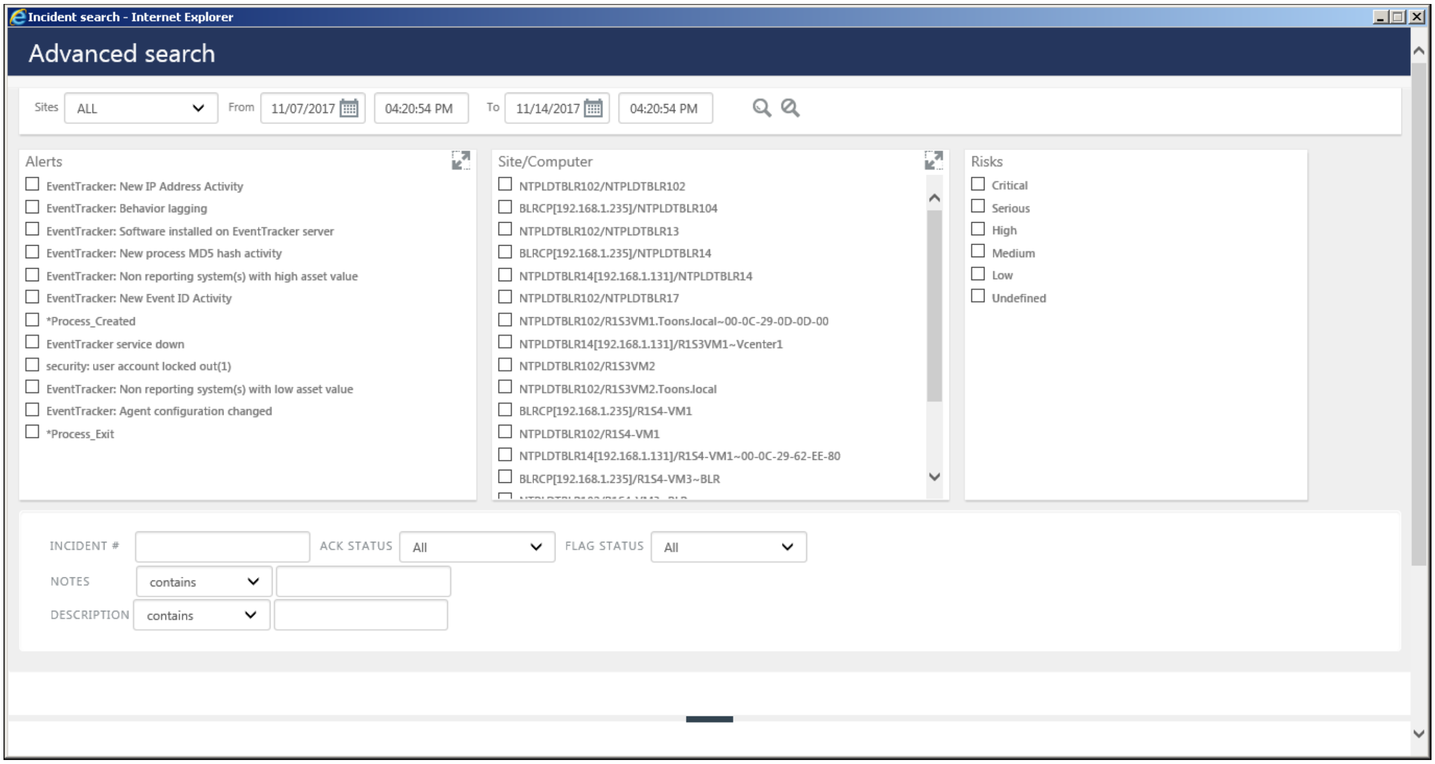
© Copyright 2019 EventTracker. All Rights Reserved. Sitemap Privacy Policy

Figure 100

2.9 Advanced Search

1. Click **Advanced Search** 🔍

Advanced Search window opens.



Incident search - Internet Explorer

Advanced search

Sites ALL From 11/07/2017 04:20:54 PM To 11/14/2017 04:20:54 PM

Alerts

- □ EventTracker: New IP Address Activity
- □ EventTracker: Behavior lagging
- □ EventTracker: Software installed on EventTracker server
- □ EventTracker: New process MD5 hash activity
- □ EventTracker: Non reporting system(s) with high asset value
- □ EventTracker: New Event ID Activity
- □ *Process_Created
- □ EventTracker service down
- □ security: user account locked out(1)
- □ EventTracker: Non reporting system(s) with low asset value
- □ EventTracker: Agent configuration changed
- □ *Process_Exit

Site/Computer

- □ NTPLDTBLR102/NTPLDTBLR102
- □ BLRCP[192.168.1.235]/NTPLDTBLR104
- □ NTPLDTBLR102/NTPLDTBLR13
- □ BLRCP[192.168.1.235]/NTPLDTBLR14
- □ NTPLDTBLR14[192.168.1.131]/NTPLDTBLR14
- □ NTPLDTBLR102/NTPLDTBLR17
- □ NTPLDTBLR102/R1S3VM1.Toons.local~00-0C-29-0D-0D-00
- □ NTPLDTBLR14[192.168.1.131]/R1S3VM1~Vcenter1
- □ NTPLDTBLR102/R1S3VM2
- □ NTPLDTBLR102/R1S3VM2.Toons.local
- □ BLRCP[192.168.1.235]/R1S4-VM1
- □ NTPLDTBLR102/R1S4-VM1
- □ NTPLDTBLR14[192.168.1.131]/R1S4-VM1~00-0C-29-62-EE-80
- □ BLRCP[192.168.1.235]/R1S4-VM3~BLR

Risks

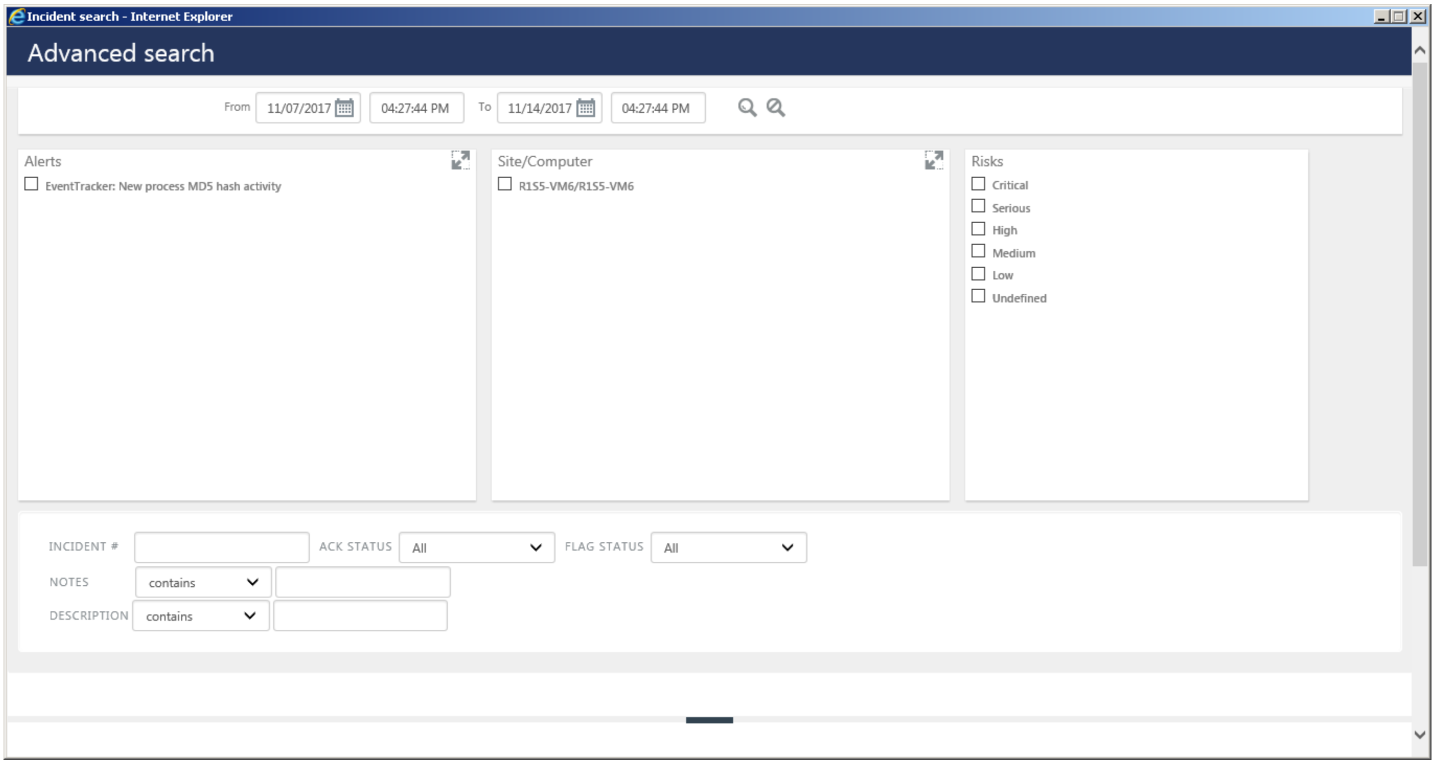
- □ Critical
- □ Serious
- □ High
- □ Medium
- □ Low
- □ Undefined

INCIDENT # ACK STATUS All FLAG STATUS All

NOTES contains

DESCRIPTION contains

Figure 101



From 11/07/2017 04:27:44 PM To 11/14/2017 04:27:44 PM

□ EventTracker: New process MD5 hash activity

□ R1S5-VM6/R1S5-VM6

□ Critical
□ Serious
□ High
□ Medium
□ Low
□ Undefined

INCIDENT #
ACK STATUS All
FLAG STATUS All
NOTES contains
DESCRIPTION contains

Figure 102

2. In Collection Master **Advanced Search** pane, select the required **Sites** from drop down.

   The Sites option is not available in a Collection Point.
3. Select / enter the required **Alert, Site/System, Risk, Incident#, Ack status, Flag Status, Notes, Description** fields.
4. If you want to grill down the search criteria, select **Contains/ does not contain** from **Notes** drop down and enter the note to list.
5. If you want to grill down the search criteria, select **Contains/ does not contain** from **Description** drop down and enter the description to list.
6. In **Duration** pane, enter **From:** and **To:** date fields.
7. Click **Search**.
8. To clear the search criteria, click 🔍.
9. To acknowledge all incidents that have occurred, click **Ack** hyperlink.

   This feature acknowledges the incidents present only in the same page.

2.10 Tile Dashboard

To make the Incidents feature more interactive, EventTracker now introduces a new dashboard named Tile Dashboard. This dashboard will help the user in getting the minute information related to the alert in a more precise way.

This new feature is provided to view the "Alert detail" in a tile format. This will show the number of "Incidents" generated for that "Alert", last occurred time of an incident, severity and number of actions taken for that alert, acknowledged/unacknowledged/Flagged and number of annotated counts.

Information will also be displayed for List, Trend (for 24 hrs) and E-mail Incident/Tune Alert Settings, by clicking the respective icons available.

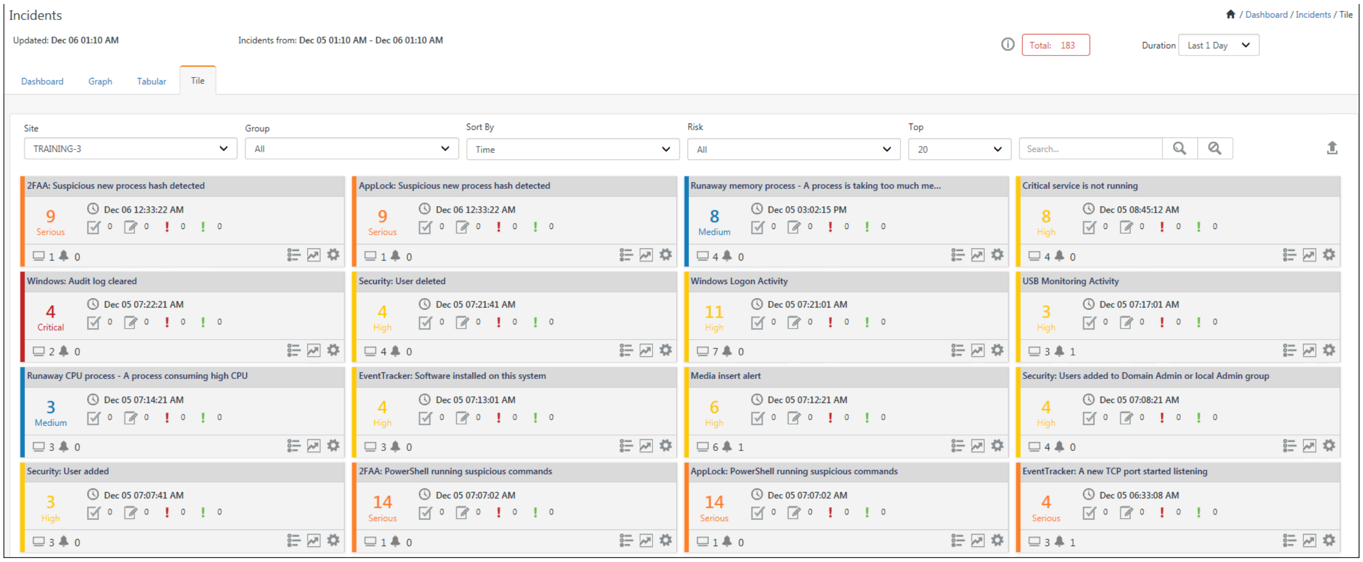
How is it Helpful?

1. Easily identify the Alert's and its details in a Tile view.
2. Add all the Event(s) to Casebook at a time.
3. Identify and view the type of action taken for the Alert.
4. Fine Tune the Alert and its details at a click.
5. Trend graph option to view the basic level details.

How it works?

- Login to **EventTracker** and navigate to **Incidents** in the Menu Bar.
- From the dropdown options, select **Tile View**.

The Tile Dashboard opens. It will show the data available in the Tabular options in a Tile format.



Incidents

Updated: Dec 06 01:10 AM

Incidents from: Dec 05 01:10 AM - Dec 06 01:10 AM

Total: 183

Duration: Last 1 Day

Site: TRAINING-3

Group: All

Sort By: Time

Risk: All

Top: 20

2FAA: Suspicious new process hash detected
9 Serious
Dec 06 12:33:22 AM
0 0 0 0
1 0

AppLock: Suspicious new process hash detected
9 Serious
Dec 06 12:33:22 AM
0 0 0 0
1 0

Runaway memory process - A process is taking too much me...
8 Medium
Dec 05 03:02:15 PM
0 0 0 0
4 0

Critical service is not running
8 High
Dec 05 08:45:12 AM
0 0 0 0
4 0

Windows: Audit log cleared
4 Critical
Dec 05 07:22:21 AM
0 0 0 0
2 0

Security: User deleted
4 High
Dec 05 07:21:41 AM
0 0 0 0
4 0

Windows Logon Activity
11 High
Dec 05 07:21:01 AM
0 0 0 0
7 0

USB Monitoring Activity
3 High
Dec 05 07:17:01 AM
0 0 0 0
3 1

Runaway CPU process - A process consuming high CPU
3 Medium
Dec 05 07:14:21 AM
0 0 0 0
3 0

EventTracker: Software installed on this system
4 High
Dec 05 07:13:01 AM
0 0 0 0
3 0

Media insert alert
6 High
Dec 05 07:12:21 AM
0 0 0 0
6 1

Security: Users added to Domain Admin or local Admin group
4 High
Dec 05 07:08:21 AM
0 0 0 0
4 0

Security: User added
3 High
Dec 05 07:07:41 AM
0 0 0 0
3 0

2FAA: PowerShell running suspicious commands
14 Serious
Dec 05 07:07:02 AM
0 0 0 0
1 0

AppLock: PowerShell running suspicious commands
14 Serious
Dec 05 07:07:02 AM
0 0 0 0
1 0

EventTracker: A new TCP port started listening
4 Serious
Dec 05 06:33:08 AM
0 0 0 0
3 1

Figure 103

NOTE: In Collection Master, any Collection Point selected from the **Site:** dropdown will not display the **Alert Action** icon 🔔 and the **Tune Alert settings** option on the Tools icon ⚙.

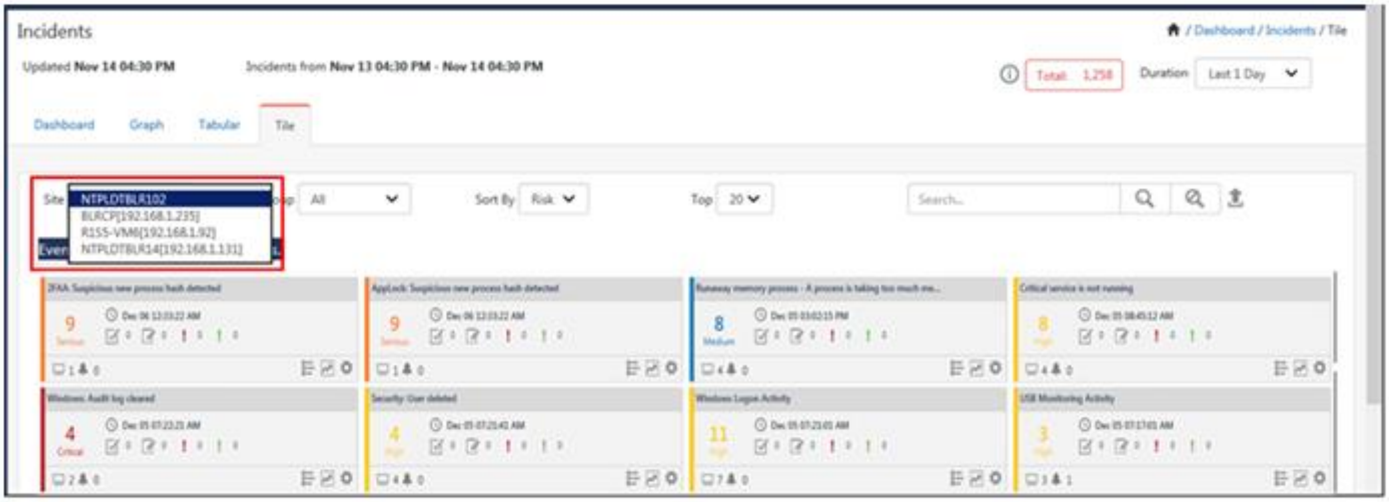

Incidents
Updated Nov 14 04:30 PM
Incidents from Nov 13 04:30 PM - Nov 14 04:30 PM
/ Dashboard / Incidents / Tile
Total: 1,258
Duration
Last 1 Day
Dashboard
Graph
Tabular
Tile
Site
NTPLDTBLR102
BLRCP[192.168.1.235]
R155-VM6[192.168.1.92]
NTPLDTBLR14[192.168.1.131]
All
Sort By
Risk
Top
20
Search...
2FAA: Suspicious new process hash detected
AppLock: Suspicious new process hash detected
Runaway memory process - A process is taking too much me...
Critical service is not running
Windows: Audit log cleared
Security: User deleted
Windows Logon Activity
USB Monitoring Activity
9
9
8
8
4
4
11
3

Figure 104

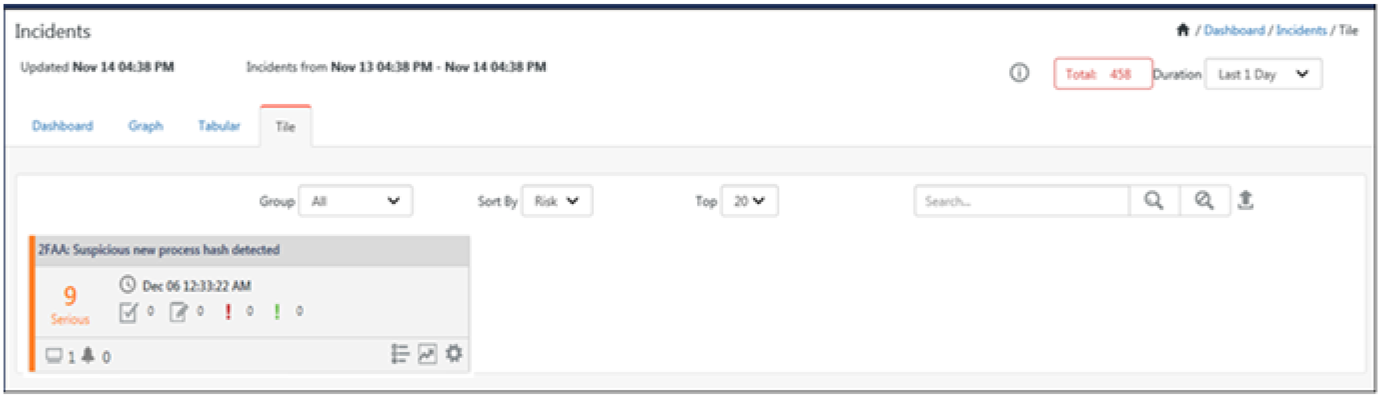
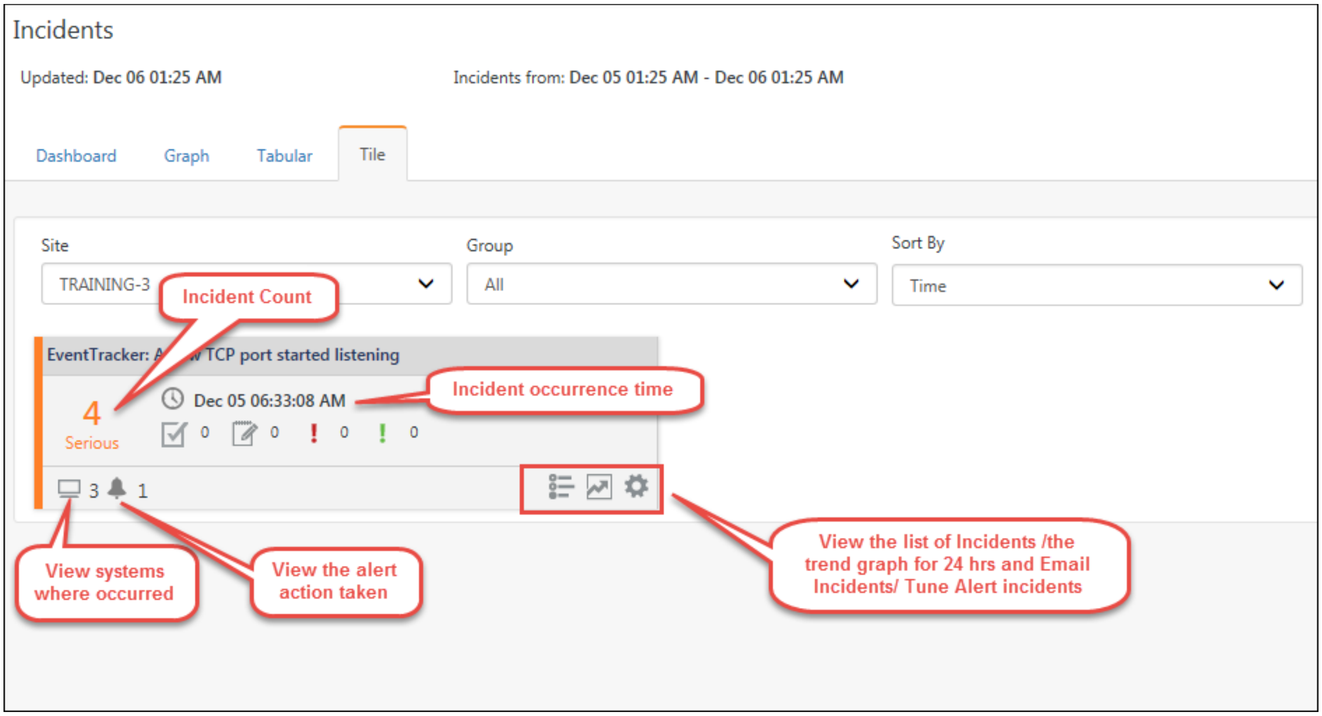


Figure 105

Incidents Dashboard – Tile View	
Field	**Description**
Sites	In a Collection Master, all sites are displayed. You cannot view this option in a Collection Point.
Group	In a Collection Point, enterprise system groups are listed in this drop-down list. By default, EventTracker selects the ALL option. **NOTE**: You cannot view this option in a Collection Master.
Sort By	View data by risk or time.
Top	By default, top 5 alerts with more incidents are displayed in the pane. You can select up to top 20 alerts for displaying in the top pane.

Click the respective icons for more information. The figure is shown below:



Incidents

Updated: Dec 06 01:25 AM

Incidents from: Dec 05 01:25 AM - Dec 06 01:25 AM

Site: TRAINING-3

Group: All

Sort By: Time

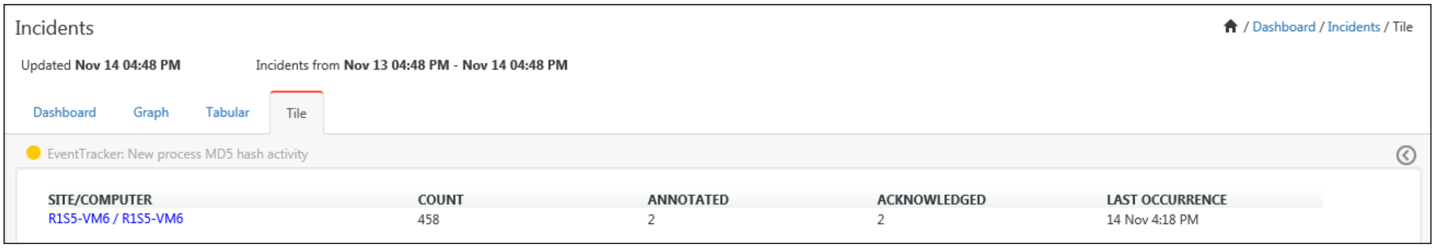
EventTracker: A new TCP port started listening

Dec 05 06:33:08 AM

Dashboard
Graph
Tabular
Tile
Incident Count
Incident occurrence time
4
Serious
0
0
0
0
3
1
View systems where occurred
View the alert action taken
View the list of Incidents /the trend graph for 24 hrs and Email Incidents/ Tune Alert incidents

Figure 106

- Click the systems 🖥 to view the systems where occurred.
- Click the system hyperlink and it will redirect you to the search result.



Incidents

🏠 / Dashboard / Incidents / Tile

Updated **Nov 14 04:48 PM** Incidents from **Nov 13 04:48 PM - Nov 14 04:48 PM**

Dashboard Graph Tabular Tile

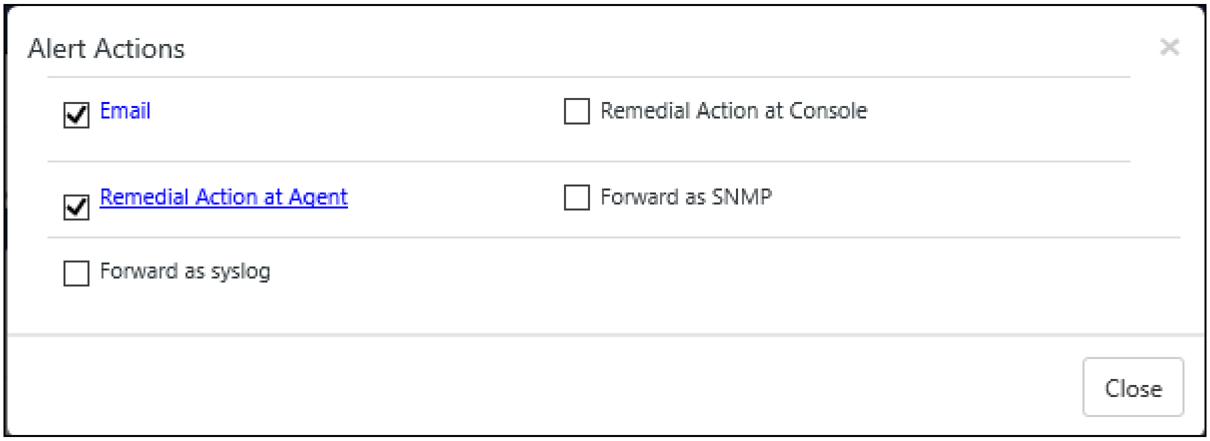
● EventTracker: New process MD5 hash activity

SITE/COMPUTER	COUNT	ANNOTATED	ACKNOWLEDGED	LAST OCCURRENCE
R1S5-VM6 / R1S5-VM6	458	2	2	14 Nov 4:18 PM

Figure 107

- Click notification 🔔 to view the alert action taken.

NOTE: The configured alert actions will display as a hyperlink and will be checked. The figure is shown below:



Alert Actions

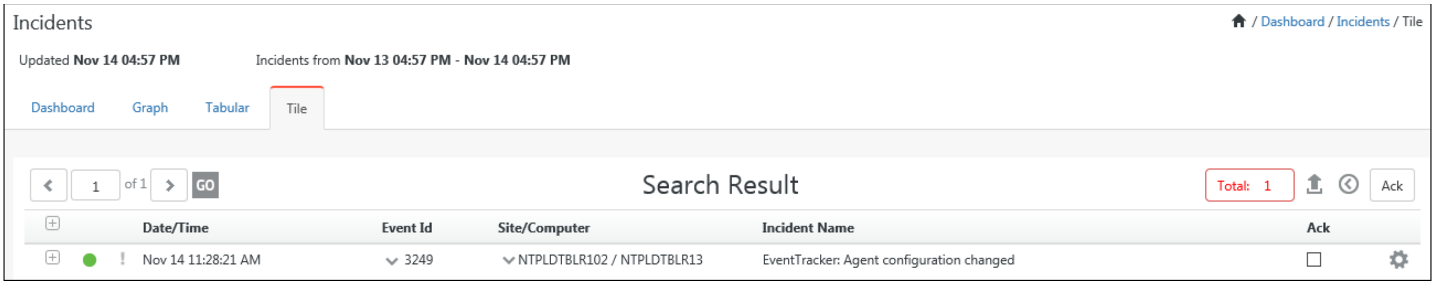
☑ Email ☐ Remedial Action at Console

☑ Remedial Action at Agent ☐ Forward as SNMP

☐ Forward as syslog

Figure 108

- To view the search list of the incident, click list icon ☰.



Incidents

🏠 / Dashboard / Incidents / Tile

Updated **Nov 14 04:57 PM** Incidents from **Nov 13 04:57 PM - Nov 14 04:57 PM**

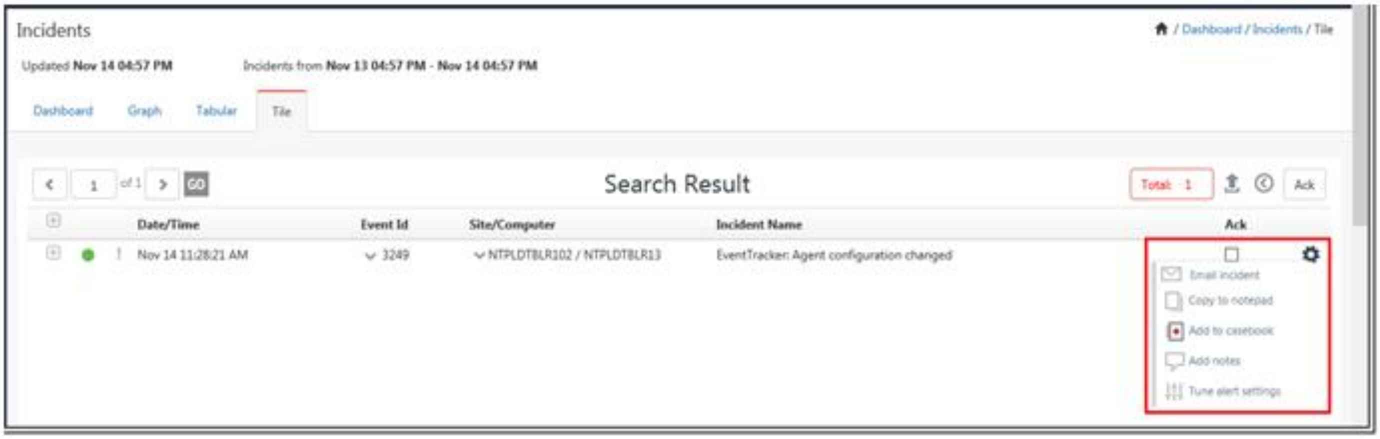
Dashboard Graph Tabular Tile

Search Result

Date/Time	Event Id	Site/Computer	Incident Name	Ack
Nov 14 11:28:21 AM	3249	NTPLDTBLR102 / NTPLDTBLR13	EventTracker: Agent configuration changed	☐

Figure 109

- The user can further click **tool** ⚙ for an incident and select any of the dropdown options displayed in the figure below:



Incidents

🏠 / Dashboard / Incidents / Tile

Updated **Nov 14 04:57 PM** Incidents from **Nov 13 04:57 PM - Nov 14 04:57 PM**

Search Result

⊞			Date/Time	Event Id	Site/Computer	Incident Name	Ack
⊞	●	!	Nov 14 11:28:21 AM	3249	NTPLDTBLR102 / NTPLDTBLR13	EventTracker: Agent configuration changed	□

Figure 110

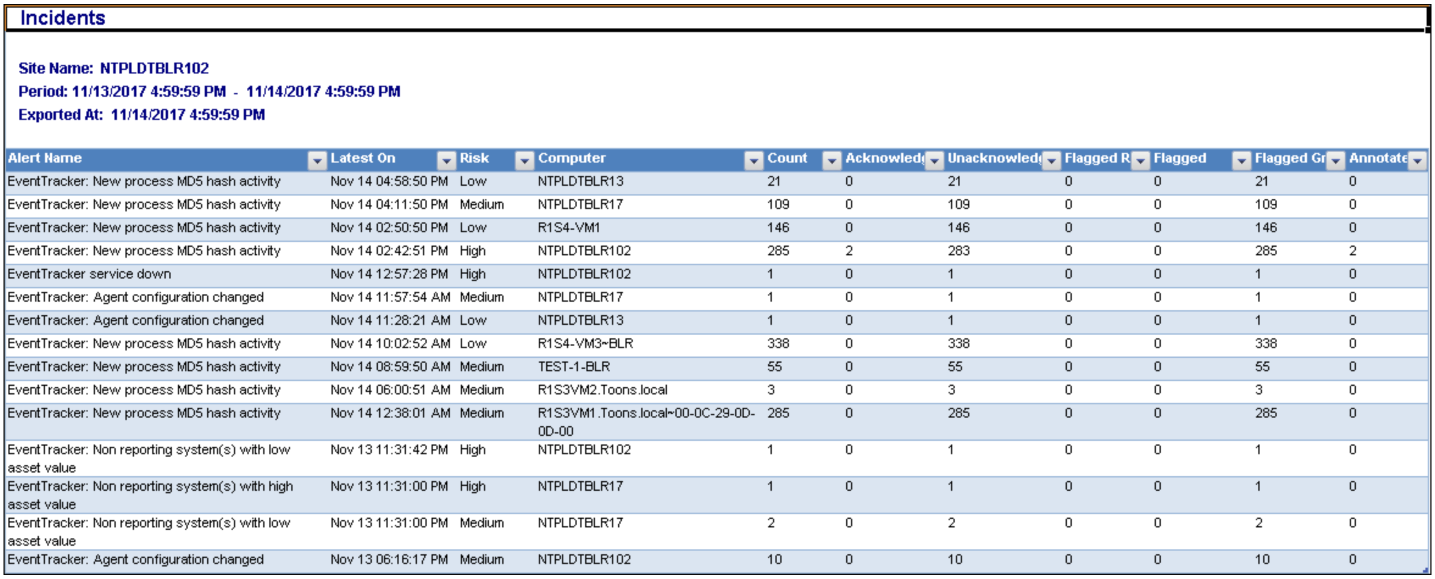
In the Tile Dashboard,

- Click trend graph , to view the incidents for the last 24 hrs.
- To e-mail the incident, click the icon and select **E-mail Incident** option from the dropdown list.
- To tune the alert settings, select the **Tune alert settings**.

To view the status of the incident,

- Click ☑ icon to view the acknowledged incident(s).
- This icon opens the count of the annotated incidents. Annotated incidents here means the incidents where comments were been added.
- The Flag Red icon ! and Flag Green icon ! shows the respective counts for the same.

To view all the Alert details in an excel format, click Export icon.



Incidents

Site Name: NTPLDTBLR102
Period: 11/13/2017 4:59:59 PM - 11/14/2017 4:59:59 PM
Exported At: 11/14/2017 4:59:59 PM

Alert Name	Latest On	Risk	Computer	Count	Acknowledg	Unacknowledg	Flagged R	Flagged	Flagged Gr	Annotate
EventTracker: New process MD5 hash activity	Nov 14 04:58:50 PM	Low	NTPLDTBLR13	21	0	21	0	0	21	0
EventTracker: New process MD5 hash activity	Nov 14 04:11:50 PM	Medium	NTPLDTBLR17	109	0	109	0	0	109	0
EventTracker: New process MD5 hash activity	Nov 14 02:50:50 PM	Low	R1S4-VM1	146	0	146	0	0	146	0
EventTracker: New process MD5 hash activity	Nov 14 02:42:51 PM	High	NTPLDTBLR102	285	2	283	0	0	285	2
EventTracker service down	Nov 14 12:57:28 PM	High	NTPLDTBLR102	1	0	1	0	0	1	0
EventTracker: Agent configuration changed	Nov 14 11:57:54 AM	Medium	NTPLDTBLR17	1	0	1	0	0	1	0
EventTracker: Agent configuration changed	Nov 14 11:28:21 AM	Low	NTPLDTBLR13	1	0	1	0	0	1	0
EventTracker: New process MD5 hash activity	Nov 14 10:02:52 AM	Low	R1S4-VM3~BLR	338	0	338	0	0	338	0
EventTracker: New process MD5 hash activity	Nov 14 08:59:50 AM	Medium	TEST-1-BLR	55	0	55	0	0	55	0
EventTracker: New process MD5 hash activity	Nov 14 06:00:51 AM	Medium	R1S3VM2.Toons.local	3	0	3	0	0	3	0
EventTracker: New process MD5 hash activity	Nov 14 12:38:01 AM	Medium	R1S3VM1.Toons.local~00-0C-29-0D-0D-00	285	0	285	0	0	285	0
EventTracker: Non reporting system(s) with low asset value	Nov 13 11:31:42 PM	High	NTPLDTBLR102	1	0	1	0	0	1	0
EventTracker: Non reporting system(s) with high asset value	Nov 13 11:31:00 PM	High	NTPLDTBLR17	1	0	1	0	0	1	0
EventTracker: Non reporting system(s) with low asset value	Nov 13 11:31:00 PM	Medium	NTPLDTBLR17	2	0	2	0	0	2	0
EventTracker: Agent configuration changed	Nov 13 06:16:17 PM	Medium	NTPLDTBLR102	10	0	10	0	0	10	0

Figure 111

2.10.1 Tiles Flip

If total incident count is equal to the acknowledged count, then tile will be flipped informing that this tile is of least importance.

A user visiting Tiles dashboard will be interested to know incidents which are important to him and needs attention. In the current scenario, such incident might be scattered and difficult to find.

Tile Flip for those tile(s) will make the process hassle-free so that other incidents get noticed.

NOTE: The auto refresh time for tiles is set to 120 seconds, by default.

2.11 Machine Learning

- Monitor Machine Learning Dashlet
- Add Machine Learning Dashlets
- Reset Personalization
- Volume Analysis
- Analyze Windows Logon
- Analyze Windows Application
- Analyze EventID
- Analyze IP Address
- Analyze Windows Network
- Analyze Windows Process
- Analyze Windows Runaway Process

- Analyze System
- Analyze Windows Interactive Logon Activity
- Analyze Windows User Location Affinity

EventTracker's Machine Learning provides you dashlets with the predefined set of job and allows you to add **custom** dashlets created with your own job 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.

The Machine Learning dashboard can be configured to display data across sites (i.e. Collection Points reporting to Collection Master) i.e. it is possible to view data in Collection Master for individual Collection Points, if configured. CP sends Machine Learning analysis data periodically to CM every 10 minutes and the CM stores the data for each CP.

2.11.1 Monitor Machine Learning Dashlet

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

EventTracker addresses this issue with its Machine Learning Activity, a dashboard that automatically provides information about unusual activity by:

- Continuously monitoring the event log stream
- Performing a combination of statistical and Machine Learning
- 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

NOTE

A job is a set of rules based on which new activities and Anomalies are identified in an Environment.

Machine Learning	**Windows Audit Policy and Acct Mgt**
	Windows Applications
	Event ID
	IP Address
	Windows Logon Failure
	Windows Network
	Windows Process
	Windows RunAway Process
	Windows Software Install
	System
	USB
	Windows Logon
	Windows Interactive Logon Activities
	Windows User Location Affinity
	Unique Process Hash

Table 15

NOTE

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

2.11.2 Adding Machine Learning Dashlets

This option helps to add dashlets to view Machine Learning Activity. Machine Learning dashboard displays machine activities through default dashlets. Using **Customize** option the Machine Learning dashlets can be added to the dashboard. Also new Machine Learning dashlet can be added by creating custom **Machine Learning Jobs**.

1 Navigate to Dashboard icon and click “**Machine Learning**”.

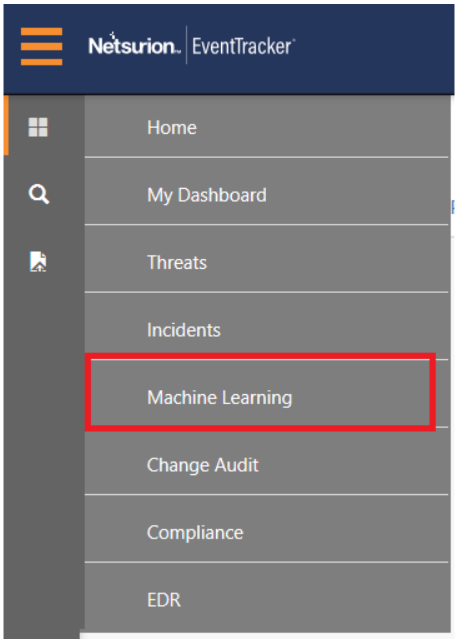
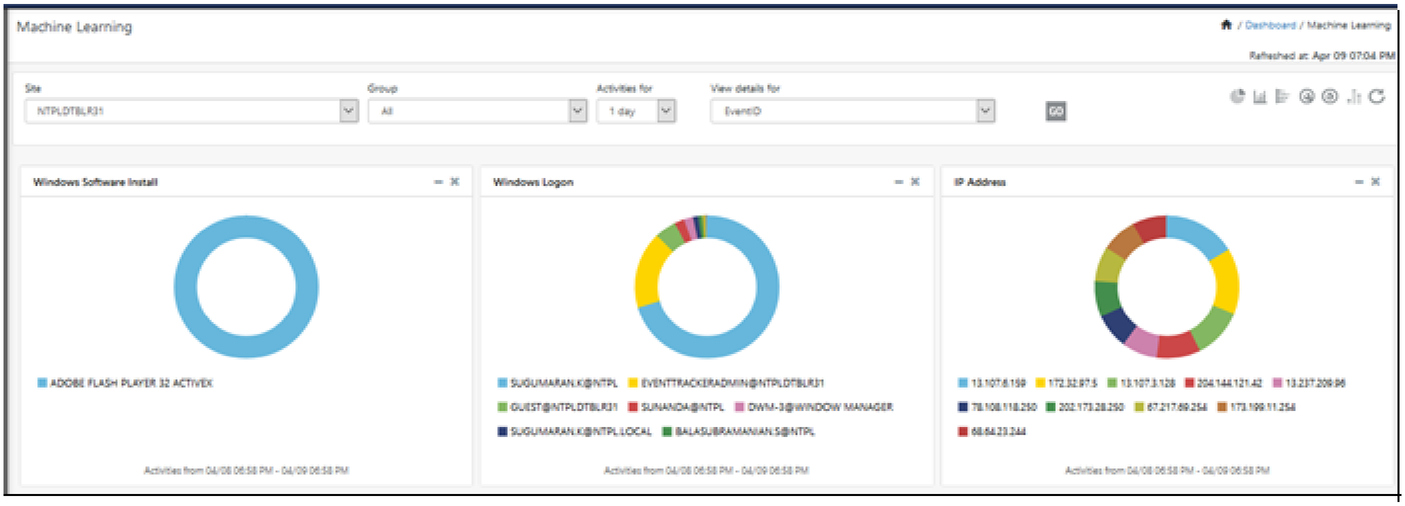


Figure 112

EventTracker opens the Machine Learning dashboard with default dashlets.


Machine Learning

Site: NTPLDTBLR31

Group: All

Activities for: 1 day

View details for: EventID

Refreshed at: Apr 09 07:04 PM

Figure 113

2 Select **Activities for** drop down and select the required number of days.

The data will be displayed as per the number of days selected. This option helps in viewing activity for specified duration.

NOTE: The activities for number of days depend on **Purge Frequency** set in **Machine Learning Settings** i.e.

a. Click the **Admin** dropdown, select **Machine Learning Settings**.

b. In **Purge Frequency** pane, select **Purge user data older than** option, select number of **days** from the drop down, and then click **OK**.

3 In the dashboard, click the icon in the right-hand side corner to customize the dashlet.

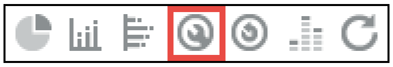
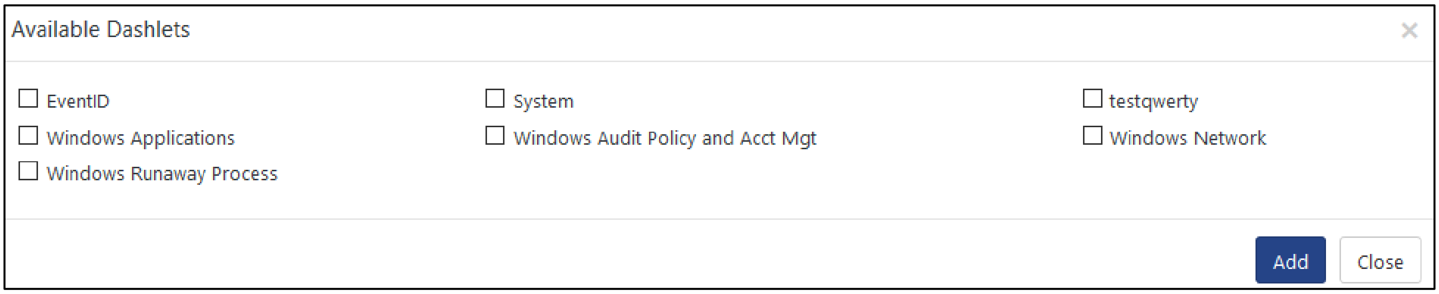


Figure 114

EventTracker opens the **Available Dashlets** dialog box.



Available Dashlets ×

□ EventID
□ Windows Applications
□ Windows Runaway Process
□ System
□ Windows Audit Policy and Acct Mgt
□ testqwerty
□ Windows Network

Add Close

Figure 115

4 Check the required activity option, and then click **Add**.

EventTracker adds the selected dashlets to the dashboard.

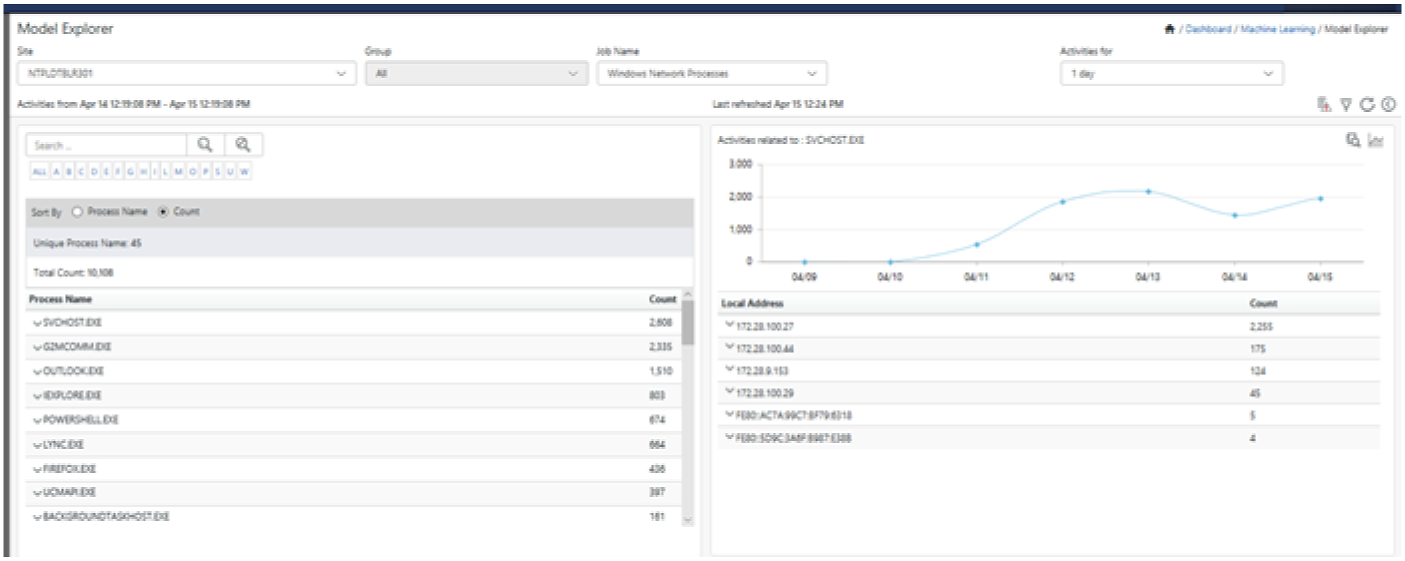
Important to Know

- Move the mouse pointer over a donut or the legend to view tooltip.
- Click a donut or legend.
- EventTracker moves you through Model Explorer Dashboard.

5 Click the corresponding **Donut/Bar/Stacked Bar** graph.

EventTracker opens the respective Model Explorer page.

Ex: Window Network Processes.


Model Explorer
/ Dashboard / Machine Learning / Model Explorer
Search ...
ALL A B C D E F G H I L M O P S U W
Sort By ○ Process Name ● Count
3,000
2,000
1,000
0
04/09
04/10
04/11
04/12
04/13
04/14
04/15

Site: NTPLDTBLR301

Group: All

Job Name: Windows Network Processes

Activities for: 1 day

Activities from Apr 14 12:19:08 PM - Apr 15 12:19:08 PM

Last refreshed Apr 15 12:24 PM

Unique Process Name: 45

Total Count: 10,108

Process Name	Count
SVCHOST.EXE	2,808
G2MCOMM.EXE	2,335
OUTLOOK.EXE	1,510
IEXPLORE.EXE	803
POWERSHELL.EXE	674
LYNC.EXE	664
FIREFOX.EXE	436
UCMAPI.EXE	397
BACKGROUNDTASKHOST.EXE	181

Activities related to : SVCHOST.EXE

Local Address	Count
172.28.100.27	2,255
172.28.100.44	175
172.28.9.153	124
172.28.100.29	45
FE80::ACTA:99C7:BF79:6318	5
FE80::5D9C:3A6F:8987:E388	4

Figure 116

- First pane **Activities for** shows activity details and weekly trend of activities
- Second pane **Activities for Process Name** shows top five Network Processes.
- Third pane **Anomalies in user occurrence** shows anomalous activities, helps to monitor abnormal user activities"
- Fourth pane **New Process Name observed** shows process activities
- **Left pane** displays the list of Extracted value based on the configured Machine Learning Jobs.

A. Click a hyperlink in the alphabetical list.

(OR)

B. Type the search phrase in the search field, and then click **Search** 🔍 \

EventTracker opens the list of searched criteria.

2.11.2.1 Log Search and Add to filter list

To do a Log Search, move the mouse pointer over a field in **Process Name column/IP Address**. From the drop down, click **Log Search**. For more details regarding Log Search, refer https://www.netsurion.com/Corporate/media/Corporate/Files/Support-Docs/Feature-Guide-Log-Search-v8x.pdf

A. To filter or ignore activities for the specified entity, select **Add to filter list**.

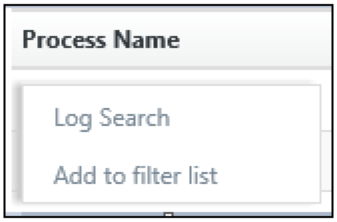
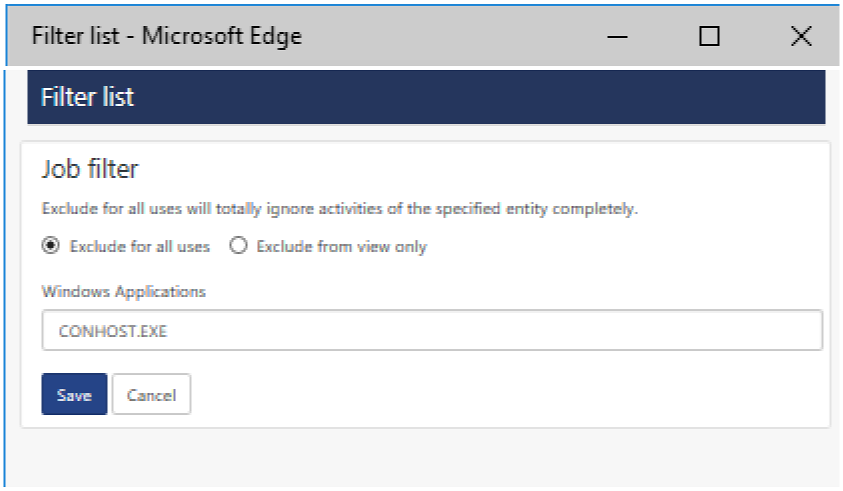


Figure 117

Filter list window opens.


Filter list - Microsoft Edge

Filter list

Job filter

Exclude for all uses will totally ignore activities of the specified entity completely.

● Exclude for all uses ○ Exclude from view only

Windows Applications

CONHOST.EXE

Figure 118

B. Select the required option and then click **Save**.

2.11.3 Resetting Personalization

This option helps to reset the dashboard with default dashlets.

1 In **Machine Learning,** click **Reset personalization** .

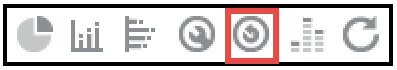


Figure 119

EventTracker displays the confirmation message box.

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

EventTracker removes the custom dashboard that you have added.

2.11.4 Volume Analysis option

This option provides a summary of total enterprise activities, which provides the distinct count of the activities and the total count of its occurrences. Machine Learning Volume analysis helps to analyze machine learning activity log volume.

1 In the **Machine Learning dashboard**, click the icon to select **Machine Learning Volume Analysis** option.

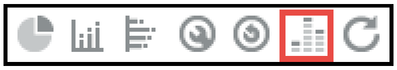
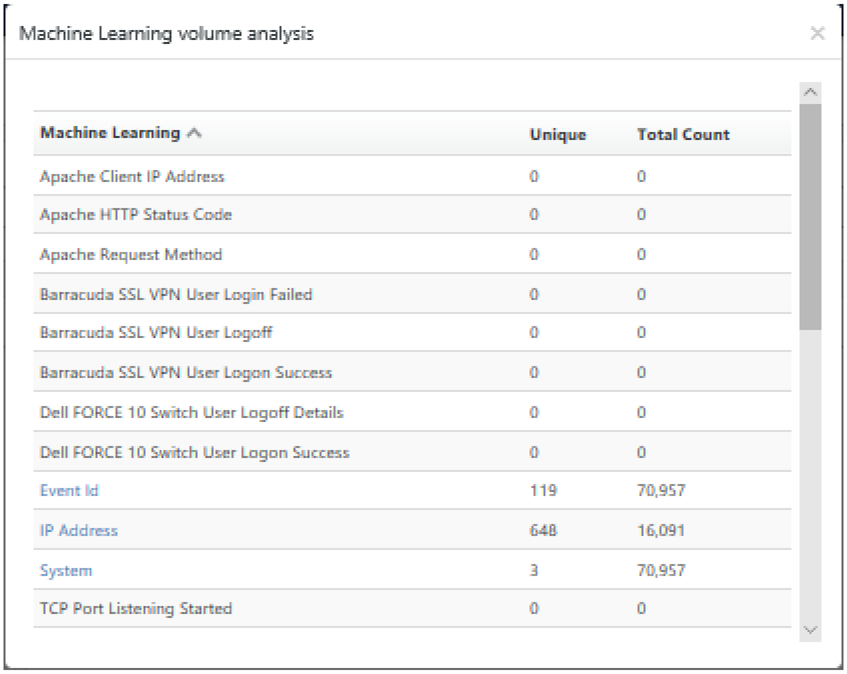


Figure 120

2 EventTracker opens the **Machine Learning Volume** Analysis dialog box.



Machine Learning volume analysis

Machine Learning	Unique	Total Count
Apache Client IP Address	0	0
Apache HTTP Status Code	0	0
Apache Request Method	0	0
Barracuda SSL VPN User Login Failed	0	0
Barracuda SSL VPN User Logoff	0	0
Barracuda SSL VPN User Logon Success	0	0
Dell FORCE 10 Switch User Logoff Details	0	0
Dell FORCE 10 Switch User Logon Success	0	0
Event Id	119	70,957
IP Address	648	16,091
System	3	70,957
TCP Port Listening Started	0	0

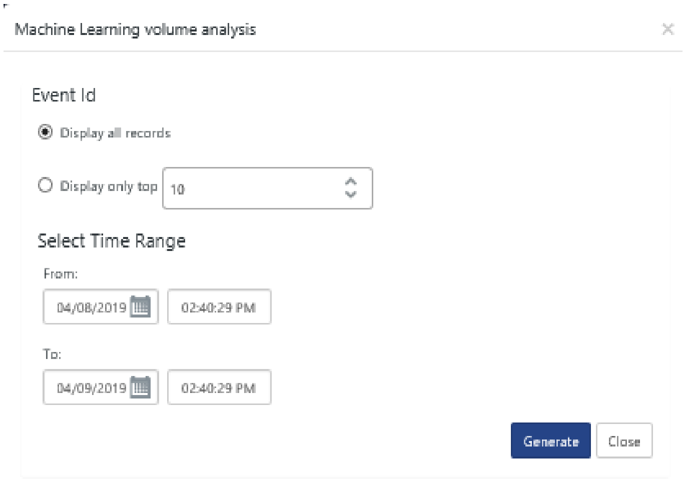
Figure 121

Field	Description
MACHINE LEARNING	List of activities. Click Machine Learning to sort the list in ascending or descending order.
UNIQUE	Count of unique activities.
TOTAL COUNT	Total count of occurrences with respect to unique activities.

Table 122

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

4 Select **Event ID Activity** options, set appropriate time range, and then click **Generate**.



Machine Learning volume analysis

Event Id

● Display all records

○ Display only top 10

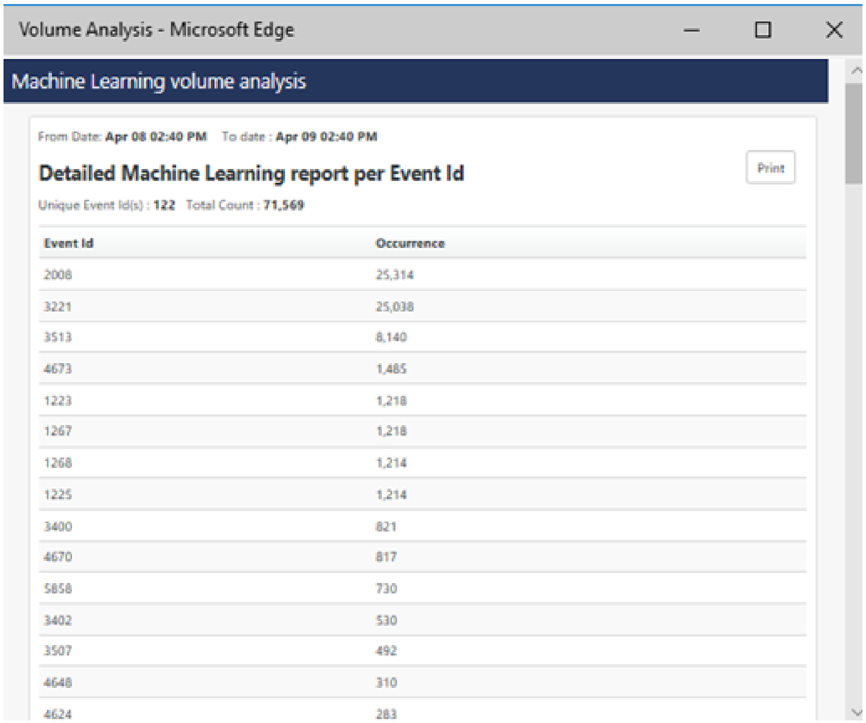
Select Time Range

From: 04/08/2019 02:40:29 PM

To: 04/09/2019 02:40:29 PM

Figure 123

EventTracker opens the consolidated list of activities.



Machine Learning volume analysis

From Date: **Apr 08 02:40 PM** To date : **Apr 09 02:40 PM**

Detailed Machine Learning report per Event Id

Unique Event Id(s) : **122** Total Count : **71,569**

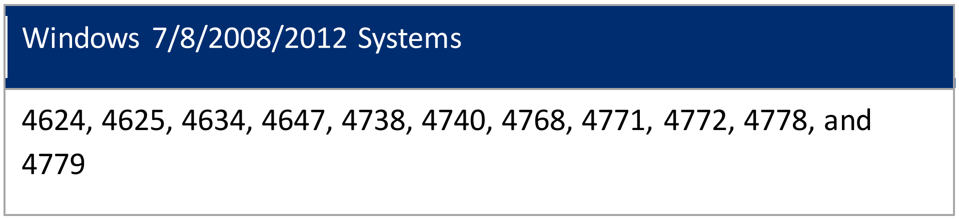
Event Id	Occurrence
2008	25,314
3221	25,038
3513	8,140
4673	1,485
1223	1,218
1267	1,218
1268	1,214
1225	1,214
3400	821
4670	817
5858	730
3402	530
3507	492
4648	310
4624	283

Figure 124

5 Click the **Print** hyperlink to print the report.

2.11.5 Analyzing Windows Logon

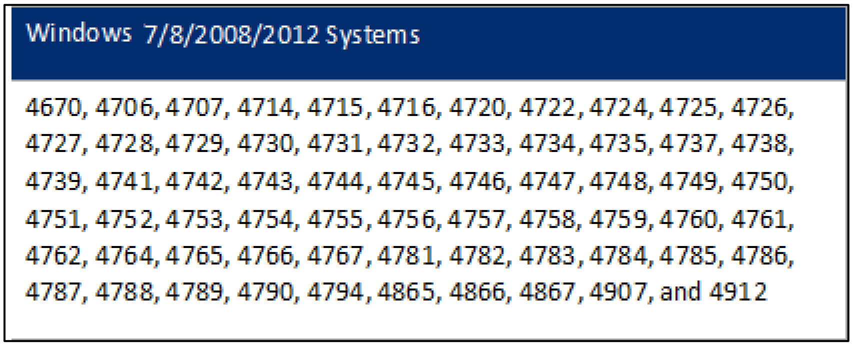
Windows Logon



Windows 7/8/2008/2012 Systems
4624, 4625, 4634, 4647, 4738, 4740, 4768, 4771, 4772, 4778, and 4779

Figure 125

Windows Audit Policy and Account Management

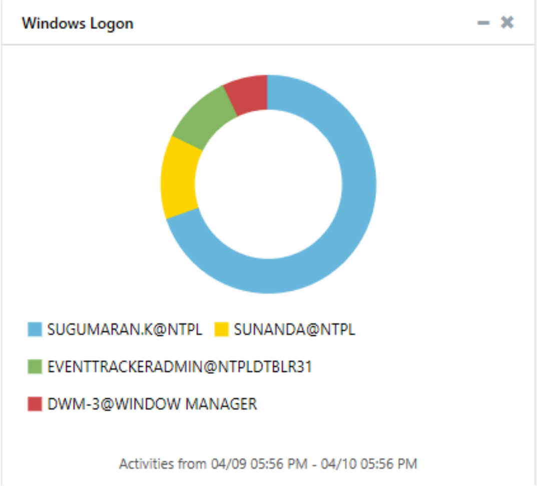


Windows 7/8/2008/2012 Systems
4670, 4706, 4707, 4714, 4715, 4716, 4720, 4722, 4724, 4725, 4726, 4727, 4728, 4729, 4730, 4731, 4732, 4733, 4734, 4735, 4737, 4738, 4739, 4741, 4742, 4743, 4744, 4745, 4746, 4747, 4748, 4749, 4750, 4751, 4752, 4753, 4754, 4755, 4756, 4757, 4758, 4759, 4760, 4761, 4762, 4764,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

Figure 126

2.11.6 Analyzing Windows Logon

1. Click **Windows Logon / Windows Audit Policy and Acct Mgt** donut chart to view the details.



Activities from 04/09 05:56 PM - 04/10 05:56 PM

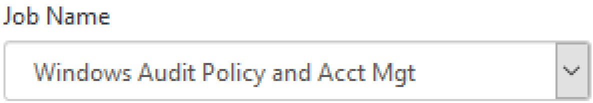
Figure 127

(OR)

Click the corresponding **Donut/Bar/Stacked Bar graph**. EventTracker opens the respective Model Explorer page.

(OR)

In **Job Name** drop down, select **Windows Logon / Windows Audit Policy and Acct Mgt**.



Job Name

Windows Audit Policy and Acct Mgt

Figure 128

2.11.7 Analyzing Windows Application

This option helps you analyze Application activity.

1. Event ID considered under this activity is **3221**. To analyze **Windows Application Activity,** click donut chart to view application activity details per system.

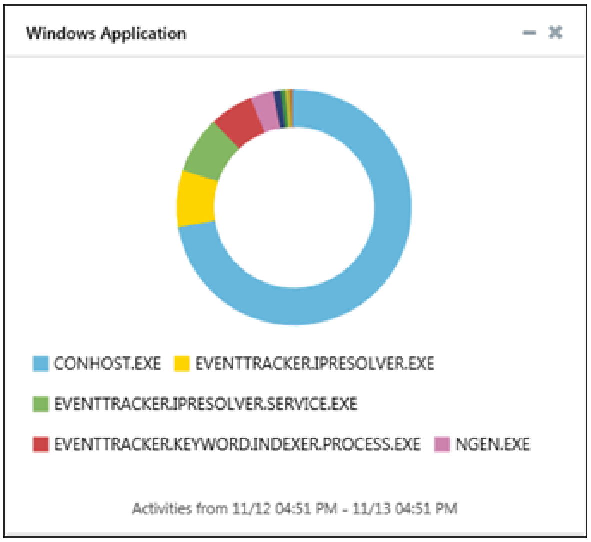

Windows Application
CONHOST.EXE
EVENTTRACKER.IPRESOLVER.EXE
EVENTTRACKER.IPRESOLVER.SERVICE.EXE
EVENTTRACKER.KEYWORD.INDEXER.PROCESS.EXE
NGEN.EXE
Activities from 11/12 04:51 PM - 11/13 04:51 PM

Figure 129

(OR)

From **Job Name** dropdown, select **Windows Applications** option, and then click GO.

EventTracker opens the respective Model Explorer page.

2.11.8 Analyzing EventID Activity

This option helps you analyze events by occurrence.

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

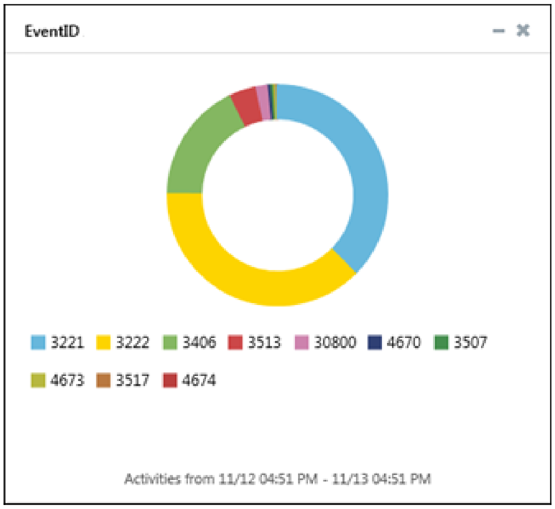


Figure 130

(OR)

From **Job Name** dropdown, select **Event ID** option, and then click GO .

EventTracker opens the “**Model Explorer page**” page.

2.12 Analyze IP Address

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** donut to view Model Explorer details for IP address activities.

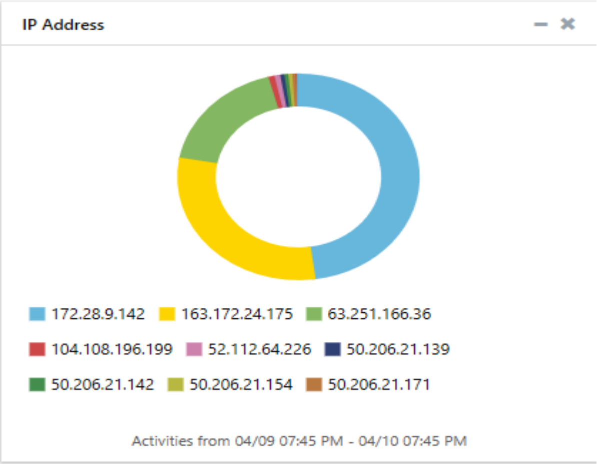


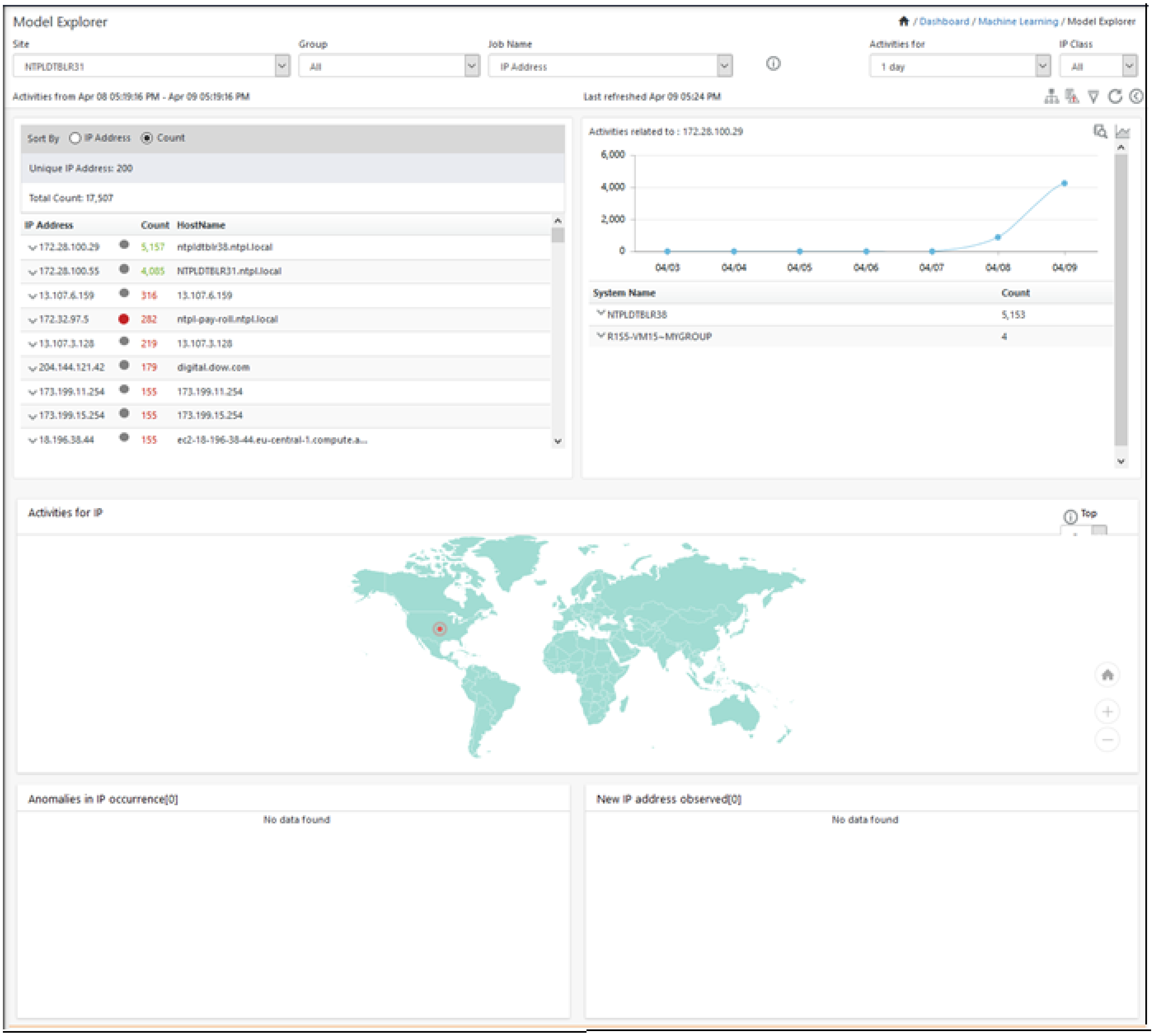
Figure 131

(OR)

From **Job Name** dropdown, select **IP Address** option and then click GO .

EventTracker opens the respective Model Explorer page.

By default, **IP Class** dropdown displays all IP addresses.



Model Explorer

/ Dashboard / Machine Learning / Model Explorer

Site: NTPLDTBLR31 | Group: All | Job Name: IP Address | Activities for: 1 day | IP Class: All

Activities from Apr 08 05:19:16 PM - Apr 09 05:19:16 PM

Last refreshed Apr 09 05:24 PM

Sort By ○ IP Address ● Count

Unique IP Address: 200

Total Count: 17,507

IP Address		Count	HostName
172.28.100.29	●	5,157	ntpldtblr38.ntpl.local
172.28.100.55	●	4,085	NTPLDTBLR31.ntpl.local
13.107.6.159	●	316	13.107.6.159
172.32.97.5	●	282	ntpl-pay-roll.ntpl.local
13.107.3.128	●	219	13.107.3.128
204.144.121.42	●	179	digital.dow.com
173.199.11.254	●	155	173.199.11.254
173.199.15.254	●	155	173.199.15.254
18.196.38.44	●	155	ec2-18-196-38-44.eu-central-1.compute.a...

Activities related to : 172.28.100.29

System Name	Count
NTPLDTBLR38	5,153
R155-VM15~MYGROUP	4

Activities for IP

Anomalies in IP occurrence[0]

No data found

New IP address observed[0]

No data found

Figure 132

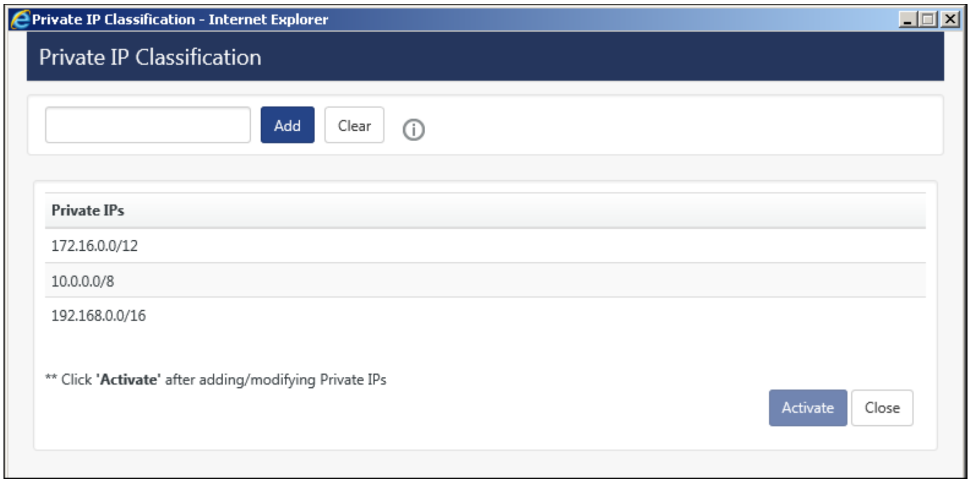
2 To view only Private or Public IP addresses, click the **IP Class** drop-down and then select **Private** or **Public** respectively.

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.

4 Click **Classification** .

All private IP addresses are displayed. You can also enter IP address in CIDR format which is explained below. Please refer Filter List section.



Private IP Classification - Internet Explorer

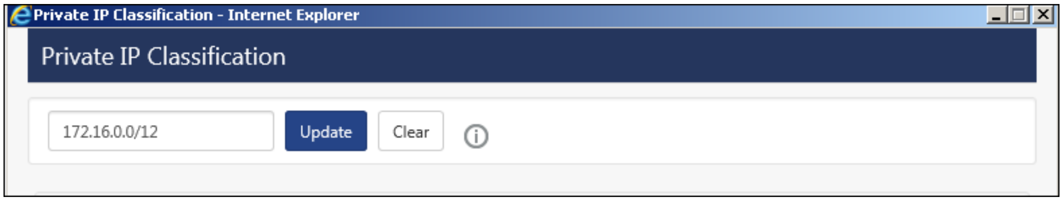
Private IP Classification

Private IPs
172.16.0.0/12
10.0.0.0/8
192.168.0.0/16

** Click '**Activate**' after adding/modifying Private IPs

Figure 133

5 Select any private IP address and then click **Update**.



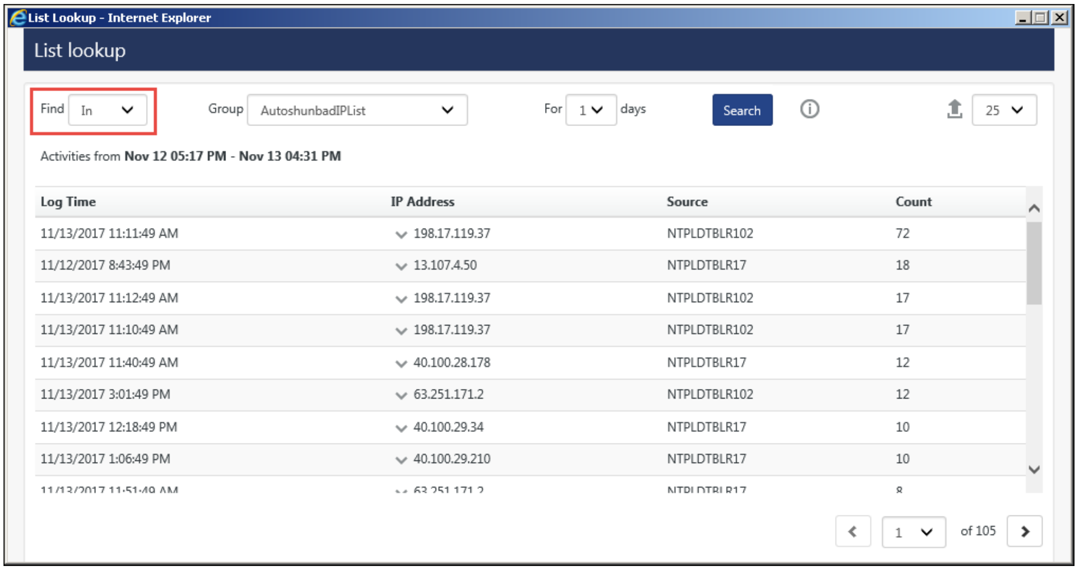
Private IP Classification - Internet Explorer

Private IP Classification

172.16.0.0/12

Figure 134

6 Click **List Lookup** to monitor unknown/blacklisted IP addresses that have logged into the network.



Find: In
Group: AutoshunbadIPList
For 1 days
25

Activities from **Nov 12 05:17 PM - Nov 13 04:31 PM**

Log Time	IP Address	Source	Count
11/13/2017 11:11:49 AM	198.17.119.37	NTPLDTBLR102	72
11/12/2017 8:43:49 PM	13.107.4.50	NTPLDTBLR17	18
11/13/2017 11:12:49 AM	198.17.119.37	NTPLDTBLR102	17
11/13/2017 11:10:49 AM	198.17.119.37	NTPLDTBLR102	17
11/13/2017 11:40:49 AM	40.100.28.178	NTPLDTBLR17	12
11/13/2017 3:01:49 PM	63.251.171.2	NTPLDTBLR102	12
11/13/2017 12:18:49 PM	40.100.29.34	NTPLDTBLR17	10
11/13/2017 1:06:49 PM	40.100.29.210	NTPLDTBLR17	10
11/13/2017 11:51:49 AM	63.251.171.2	NTPLDTBLR17	8

1 of 105

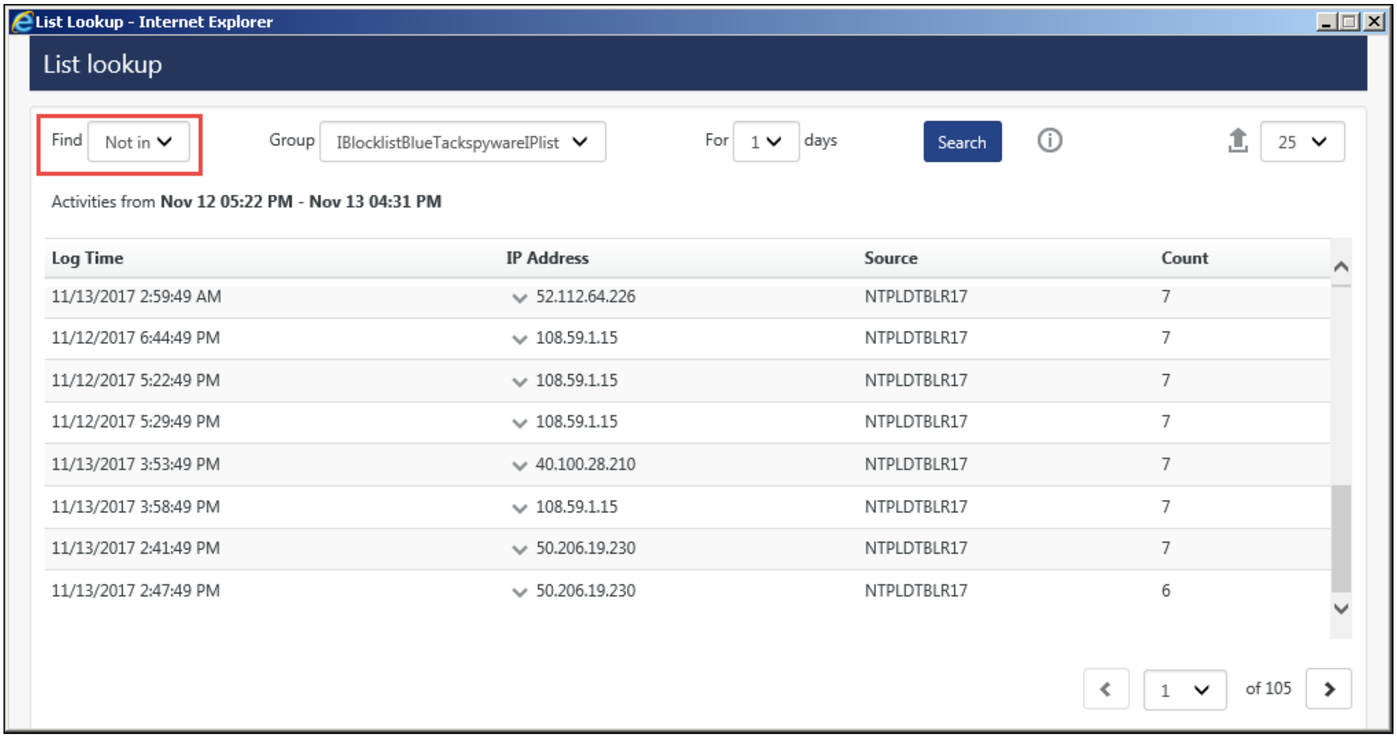
Figure 135

This list is generated from Active Watch List. Refer Admin menu -> Active Watch List.

If you select 'In' from Find: drop down, the processes that are found in Active Watch List group opens.

7 Click **Information** ⓘ to view detail information.

8 To view IP Addresses that are not available in Active Watch List, select **Not in** from **Find:** drop down.



Find: Not in
Group: IBlocklistBlueTackspywareIPlist
For 1 days
25

Activities from **Nov 12 05:22 PM - Nov 13 04:31 PM**

Log Time	IP Address	Source	Count
11/13/2017 2:59:49 AM	52.112.64.226	NTPLDTBLR17	7
11/12/2017 6:44:49 PM	108.59.1.15	NTPLDTBLR17	7
11/12/2017 5:22:49 PM	108.59.1.15	NTPLDTBLR17	7
11/12/2017 5:29:49 PM	108.59.1.15	NTPLDTBLR17	7
11/13/2017 3:53:49 PM	40.100.28.210	NTPLDTBLR17	7
11/13/2017 3:58:49 PM	108.59.1.15	NTPLDTBLR17	7
11/13/2017 2:41:49 PM	50.206.19.230	NTPLDTBLR17	7
11/13/2017 2:47:49 PM	50.206.19.230	NTPLDTBLR17	6

1 of 105

Figure 136

If you select 'Not in', the processes that are NOT available in Active Watch List group opens.

9 Click the **IP address** dropdown in the left pane/ third pane/ fourth pane / List Lookup, and then select **Whois**.

Whois option is provided to resolve **WAN IP** addresses and to know the owner details.

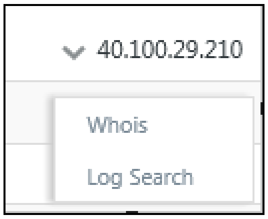
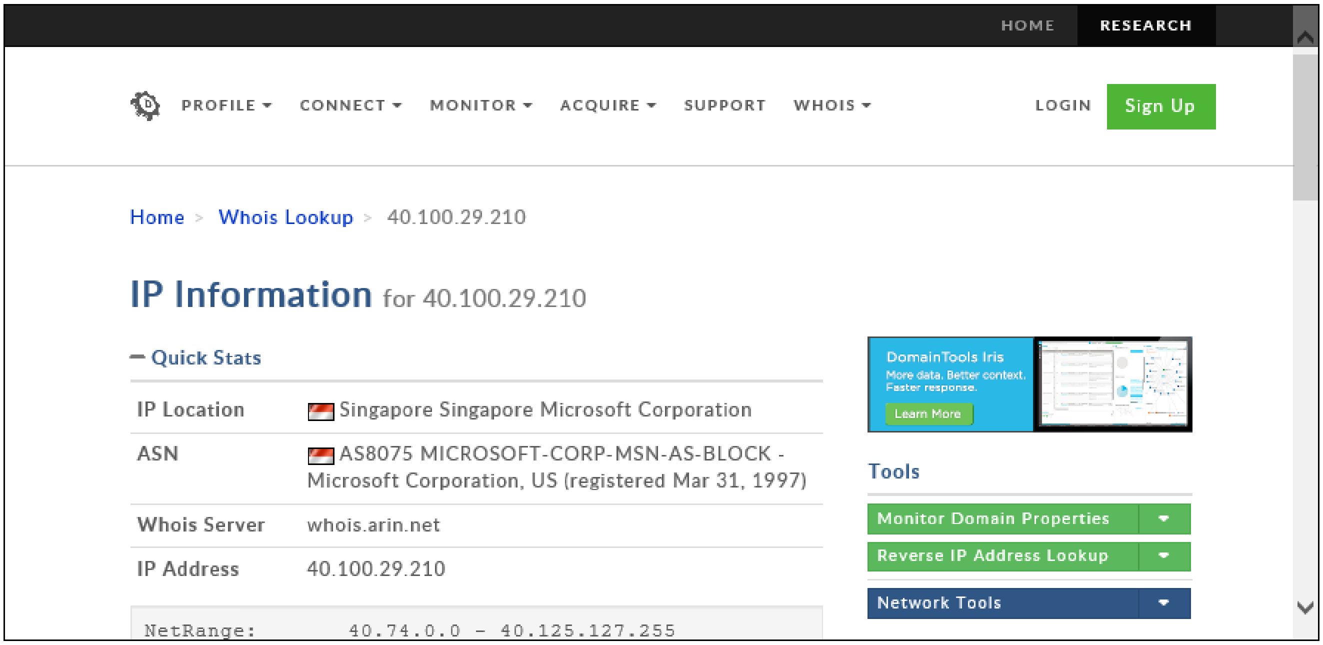


Figure 137

EventTracker moves you through the '**DomainTools**' Web site.


HOME
RESEARCH
PROFILE
CONNECT
MONITOR
ACQUIRE
SUPPORT
WHOIS
LOGIN
Sign Up
Home > Whois Lookup > 40.100.29.210
IP Information for 40.100.29.210
Quick Stats
DomainTools Iris
More data. Better context. Faster response.
Learn More
Tools
Monitor Domain Properties
Reverse IP Address Lookup
Network Tools

IP Location	Singapore Singapore Microsoft Corporation
ASN	AS8075 MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation, US (registered Mar 31, 1997)
Whois Server	whois.arin.net
IP Address	40.100.29.210

```
NetRange:        40.74.0.0 - 40.125.127.255
```

Figure 138

2.12.1 Filter List

1. Click **Filter** ▽ .
   Filter List window opens.

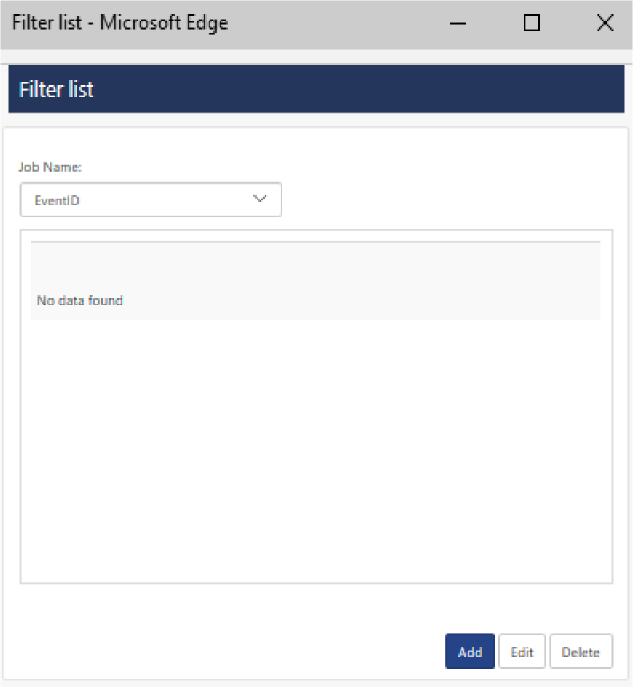
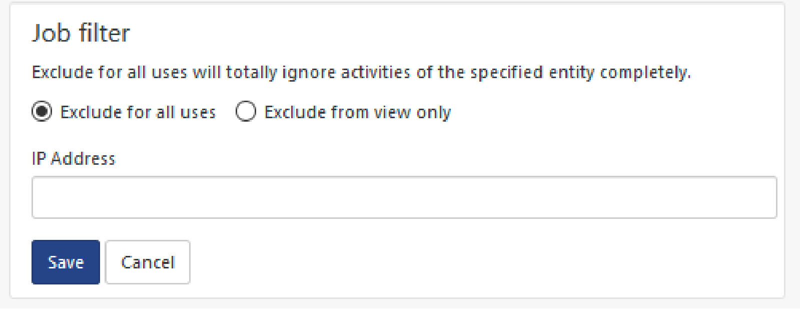


Figure 139

2. Click **Add**.

   Job filter pane opens.



Job filter

Exclude for all uses will totally ignore activities of the specified entity completely.

● Exclude for all uses ○ Exclude from view only

IP Address

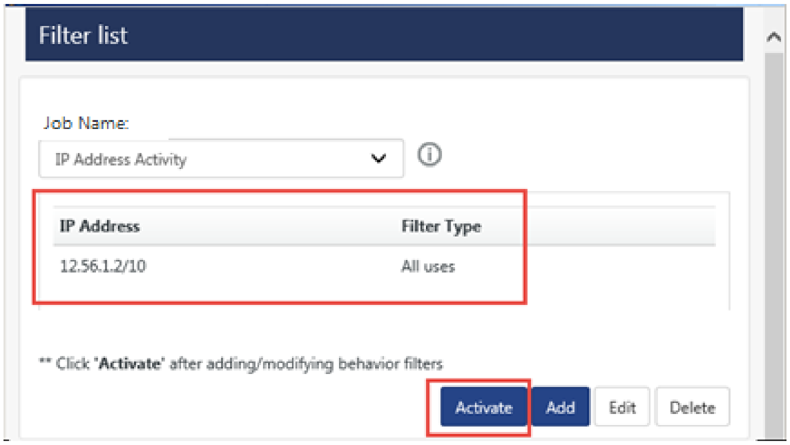
Figure 140

You now have an option to enter IP address in CIDR (Classless Inter-Domain Routing) format also. Ex: 12.56.1.2/10.

CIDR is a way to allocate and specify the Internet addresses used in inter-domain routing more flexibly than with the original system of Internet Protocol (IP) address classes.

The number of addresses of a subnet defined by the mask or prefix can be calculated as $2^{\text{address size - prefix size}}$, in which the address size is 128 for IPv6 and 32 for IPv4. For example, in IPv4, a prefix size of /29 gives: $2^{10-2} = 2^{8} = 256$ addresses.

3. To exclude an IP address from being monitored in **Filter list** pane, select **Exclude for all uses** or **Exclude from view only** option.
4. In **Filter list** pane, enter the required **IP Address** in the box and then select the **Save** button.
   Ex: In our example to exclude 12.56.1.2/10 from being monitored, enter this IP address and then click Save. Hence the activities of IP address 12.56.1.2/10 will be completely ignored.



Filter list

Job Name: IP Address Activity

IP Address	Filter Type
12.56.1.2/10	All uses

** Click '**Activate**' after adding/modifying behavior filters

Figure 141

5. Click **Activate**.

2.12.2 Analyzing Windows Network

This option helps you analyze network activities.

Event ID's considered under this activity are **3512** and **3513**. Whenever 3512 and 3513 events are received, remote IP address and remote port information is extracted from the event, and its count is maintaine d.

1 Click **Windows Network** donut chart to view activity details of devices like printers, routers over the respective network.

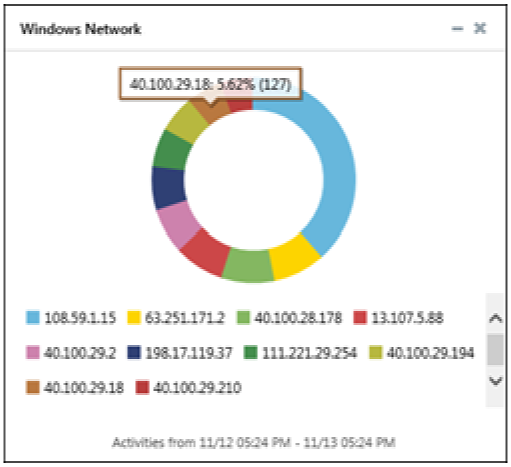


Figure 142

(OR)

From **Job Name** dropdown, select **Windows Network** option, and then click GO .

EventTracker opens the respective Model Explorer page.

2.12.3 Analyzing Windows Process

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, username, domain name, and computer name are extracted from the 'Event Description'.

1. To analyze process by occurrence, click the **Windows Process** donut chart to view process utilization activities details.

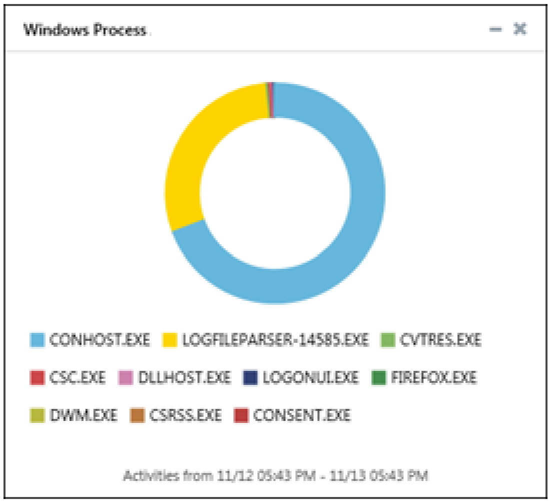


Figure 143

(OR)

From **Job Name** dropdown, select **Windows Process** option, and then click GO .

EventTracker opens the respective Model Explorer page.

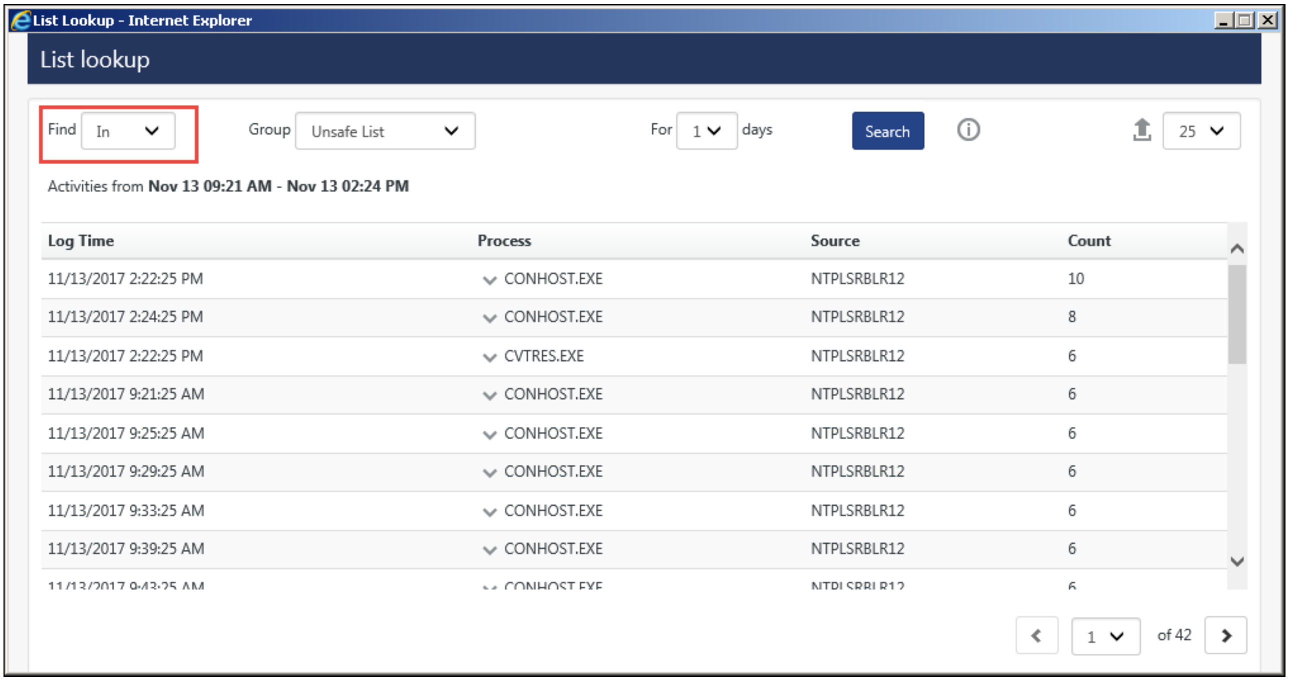
2. Click **ListLookup** to view malicious processes that can harm the system.

   ListLookup window opens.

3. In **Find:** drop down, select **In** or **Not in**, select the required **Group:** and duration.

   If you select **'In'**, the processes that are found in Active Watch List group displays.

4. Click **Search**.



Find: In | Group: Unsafe List | For: 1 days

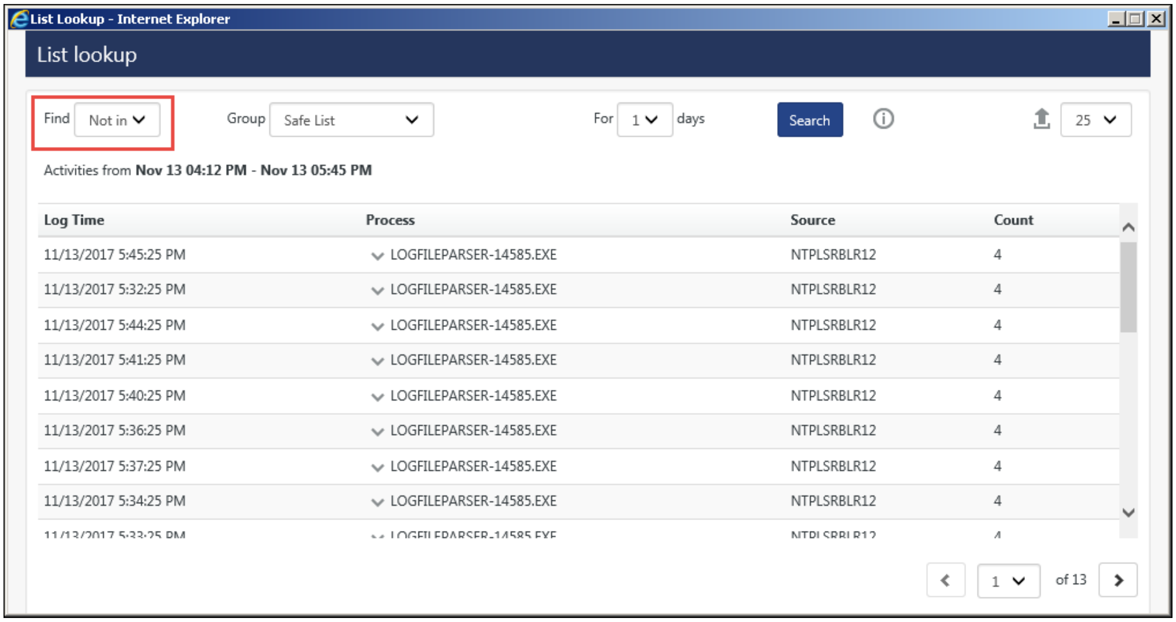
Activities from **Nov 13 09:21 AM - Nov 13 02:24 PM**

Log Time	Process	Source	Count
11/13/2017 2:22:25 PM	CONHOST.EXE	NTPLSRBLR12	10
11/13/2017 2:24:25 PM	CONHOST.EXE	NTPLSRBLR12	8
11/13/2017 2:22:25 PM	CVTRES.EXE	NTPLSRBLR12	6
11/13/2017 9:21:25 AM	CONHOST.EXE	NTPLSRBLR12	6
11/13/2017 9:25:25 AM	CONHOST.EXE	NTPLSRBLR12	6
11/13/2017 9:29:25 AM	CONHOST.EXE	NTPLSRBLR12	6
11/13/2017 9:33:25 AM	CONHOST.EXE	NTPLSRBLR12	6
11/13/2017 9:39:25 AM	CONHOST.EXE	NTPLSRBLR12	6
11/13/2017 9:43:25 AM	CONHOST.EXE	NTPLSRBLR12	6

Figure 144

5. Click **Information** ⓘ to view additional information.
6. In **Find:** drop down, select **Not In,** select the required **Group:** and the duration.

   If you select **'Not in'**, the processes that are NOT available in Active Watch List group opens.
7. Click **Search**.



Find: Not in | Group: Safe List | For: 1 days

Activities from **Nov 13 04:12 PM - Nov 13 05:45 PM**

Log Time	Process	Source	Count
11/13/2017 5:45:25 PM	LOGFILEPARSER-14585.EXE	NTPLSRBLR12	4
11/13/2017 5:32:25 PM	LOGFILEPARSER-14585.EXE	NTPLSRBLR12	4
11/13/2017 5:44:25 PM	LOGFILEPARSER-14585.EXE	NTPLSRBLR12	4
11/13/2017 5:41:25 PM	LOGFILEPARSER-14585.EXE	NTPLSRBLR12	4
11/13/2017 5:40:25 PM	LOGFILEPARSER-14585.EXE	NTPLSRBLR12	4
11/13/2017 5:36:25 PM	LOGFILEPARSER-14585.EXE	NTPLSRBLR12	4
11/13/2017 5:37:25 PM	LOGFILEPARSER-14585.EXE	NTPLSRBLR12	4
11/13/2017 5:34:25 PM	LOGFILEPARSER-14585.EXE	NTPLSRBLR12	4
11/13/2017 5:33:25 PM	LOGFILEPARSER-14585.EXE	NTPLSRBLR12	4

Figure 145

8. Click **Process** drop down.

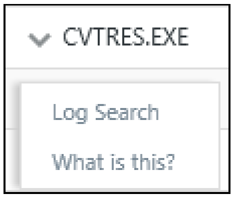


Figure 146

9. To perform a search, click **Log Search** link.
10. To know more details about a process, click **What is this?** Link.
    You will be redirected to the link http://www.processlibrary.com/ automatically.
11. To filter any process from the list, click **Add to filter list** link.

    This list is generated from Active Watch List. For detail information refer Admin menu -> Active Watch List.

2.12.4 Analyzing Windows Runaway Process

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 **Windows Runaway Process** donut chart to view per runaway process activity details.

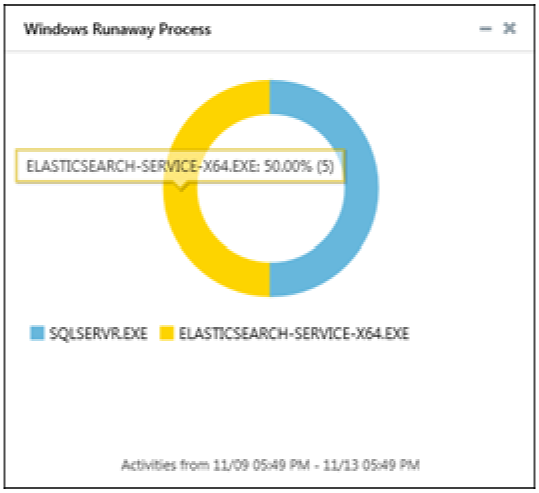

Windows Runaway Process
ELASTICSEARCH-SERVICE-X64.EXE: 50.00% (5)
SQLSERVR.EXE
ELASTICSEARCH-SERVICE-X64.EXE
Activities from 11/09 05:49 PM - 11/13 05:49 PM

Figure 147

(OR)

From **Job Name** dropdown, select **Windows Runaway Process** option, and then click the GO icon.

EventTracker opens the respective Model Explorer page.

2.12.5 Analyzing System

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

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

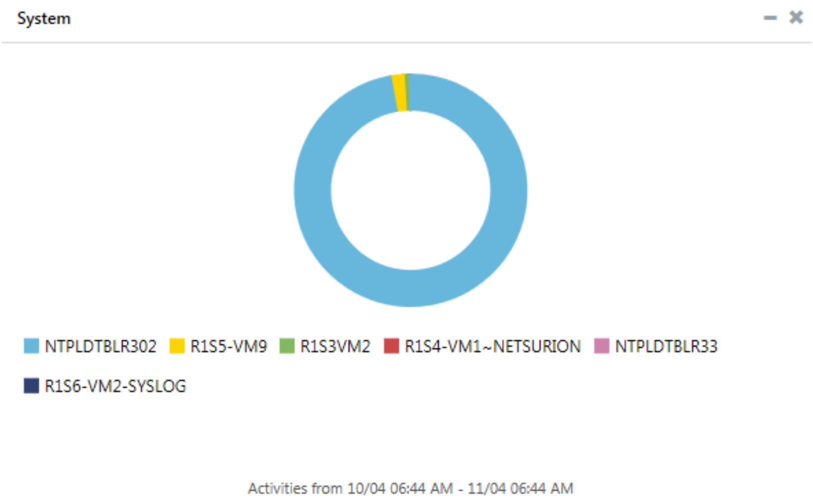


Figure 148

(OR)

From **Job Name** dropdown, select **Software** option, and then click the GO icon.

EventTracker opens the respective Model Explorer page.

2.12.5.1 Monitoring USB

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.

2.12.6 Analyzing Windows Interactive Logon Activity

This dashboard will display data for 2 types of Logon in Windows Logon Activity.

- RDP (Remote Desktop Users) – Logon Type 10
- Interactive Users – Logon Type 2

The graphical representation can be viewed by them in Machine Learning Dashboard which is like Incidents Dashboard.

2.12.6.1 Viewing Windows Interactive Logon Activity

1. Event ID considered under this activity is **4624**. To analyze events, click the **Windows Interactive Logon Activity** pie chart to view per event activity details.

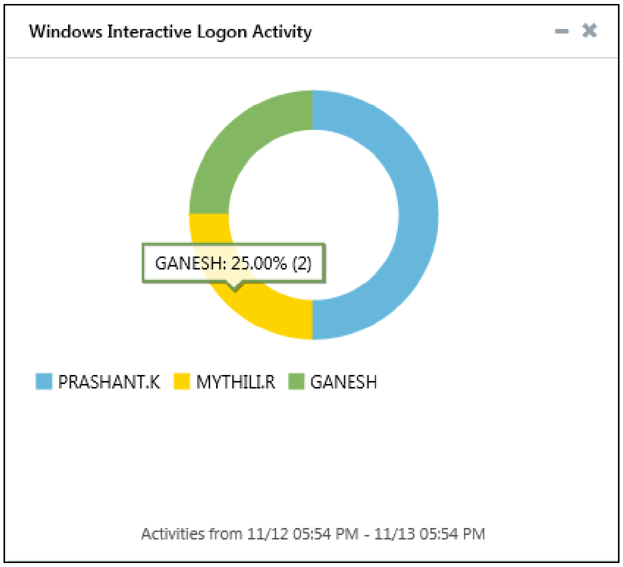

Windows Interactive Logon Activity
GANESH: 25.00% (2)
PRASHANT.K
MYTHILI.R
GANESH
Activities from 11/12 05:54 PM - 11/13 05:54 PM

Figure 149

(OR)

From **Job Name** dropdown, select **Windows Interactive Logon Activity** option, and then click **Go** icon.

EventTracker opens the respective Model Explorer page.

> 🗎 NOTE
>
> This will not be visible for users of other Logon Types.

2.12.7 Analyzing Windows User Location Affinity

This dashboard will display all windows interactive logon related events along with the pattern that occurs on any domain controller or windows machine in the network.

NOTE: The dashlet will support 2003, 2008 and 2012 domains.

The graphical representation can be viewed by them in Behavior Dashboard which is similar to Incidents Dashboard.

2.12.7.1 Viewing Windows User Location Affinity

1. To analyze events, click the **Windows user location affinity** donut graph to view per event activity details.

NOTE: This Machine Learning Job will only get displayed in the dropdown list of dashboards, when the user enables the **display in dashboard** option by editing the rule under Machine Learning Job.

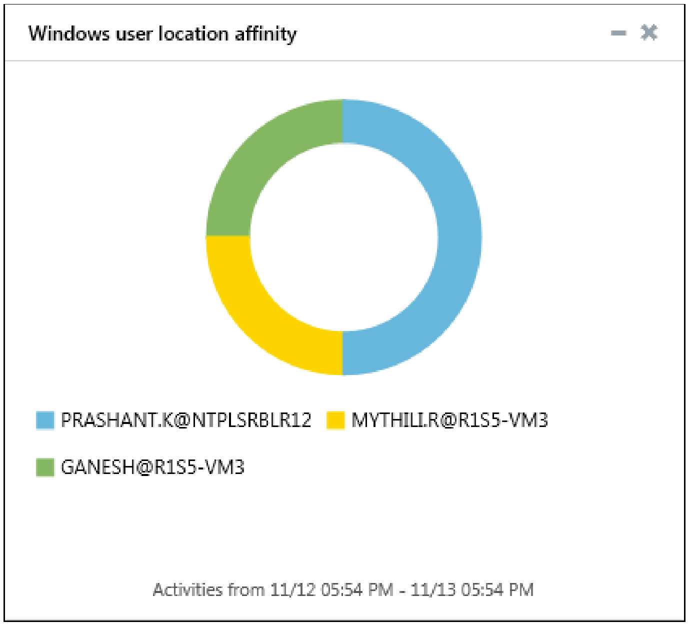
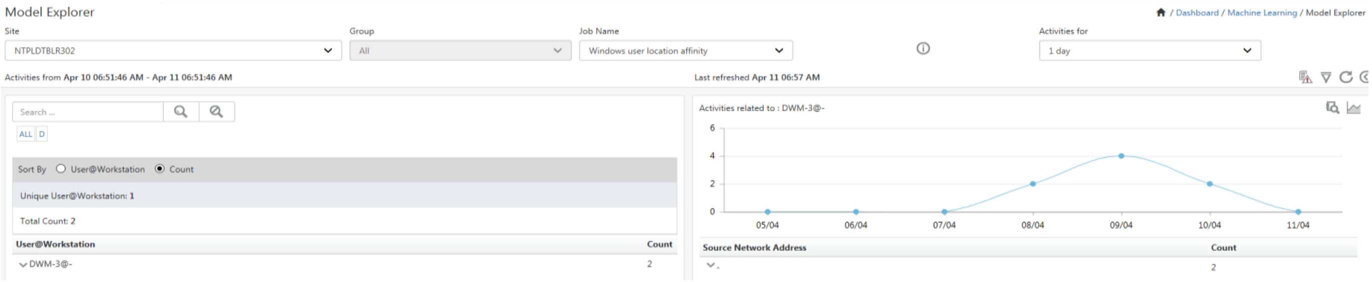

Windows user location affinity
PRASHANT.K@NTPLSRBLR12
MYTHILI.R@R1S5-VM3
GANESH@R1S5-VM3
Activities from 11/12 05:54 PM - 11/13 05:54 PM

Figure 150

(OR)

From **Job Name** dropdown, select **Windows user location affinity** option, and then click **Go** .

EventTracker opens the respective Model Explorer page.


Model Explorer

/ Dashboard / Machine Learning / Model Explorer

Site: NTPLDTBLR302

Group: All

Job Name: Windows user location affinity

Activities for: 1 day

Activities from Apr 10 06:51:46 AM - Apr 11 06:51:46 AM

Last refreshed Apr 11 06:57 AM

Sort By ○ User@Workstation ● Count

Unique User@Workstation: 1

Total Count: 2

User@Workstation	Count
DWM-3@-	2

Activities related to : DWM-3@-

Source Network Address	Count
-	2

Figure 151

2.13 Change Audit

- Change Audit Dashboard
- Last Changes
- Policy Dashboard
- Change Policies

2.13.1 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.

2.13.2 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.

2.13.3 Viewing Change Audit dashboard

1. Log on to EventTracker.
2. Click **Dashboard** and then select **Change Audit.**

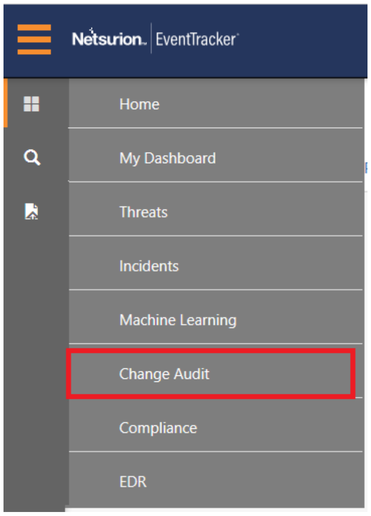


Figure 152

EventTracker opens the Change Audit Dashboard.

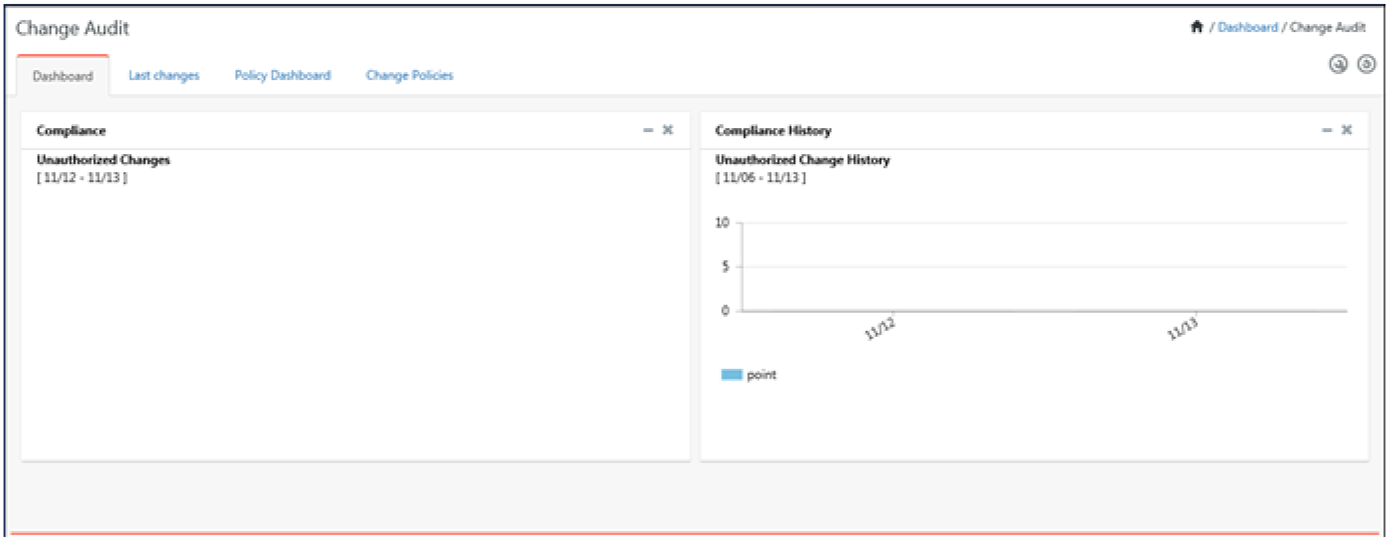
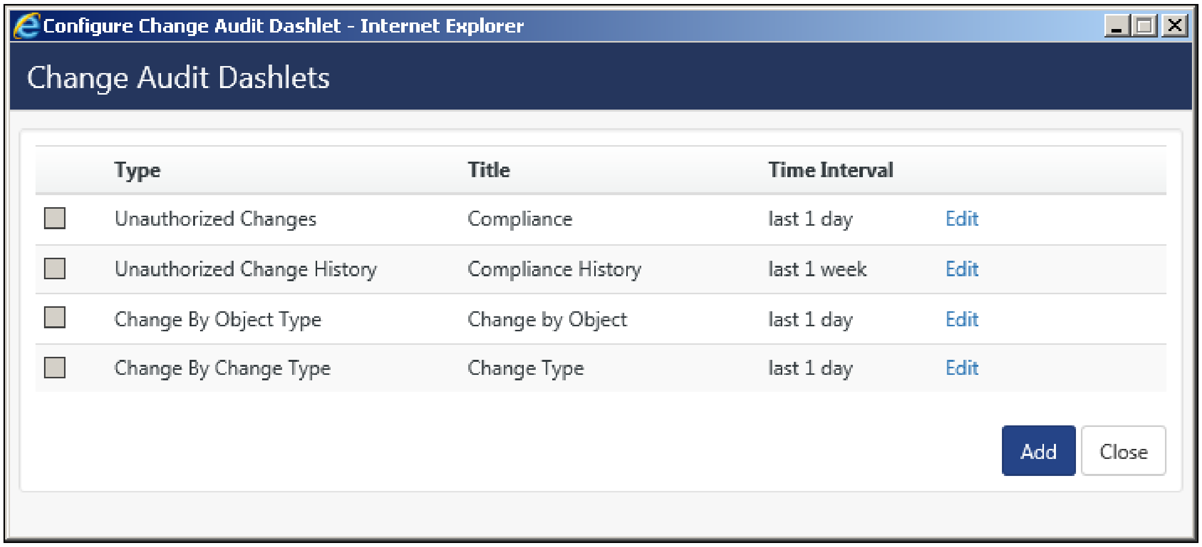


Figure 153

3. Click **Customize** .

EventTracker opens the Change Audit Dashlets pop-up window.



Configure Change Audit Dashlet - Internet Explorer

Change Audit Dashlets

	Type	Title	Time Interval	
□	Unauthorized Changes	Compliance	last 1 day	Edit
□	Unauthorized Change History	Compliance History	last 1 week	Edit
□	Change By Object Type	Change by Object	last 1 day	Edit
□	Change By Change Type	Change Type	last 1 day	Edit

Figure 154

4. Click **Edit** to edit the Title or Time Interval settings, and then click **Update**.
5. Select the required **Change Audit Dashlets** and then click **Add**.

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

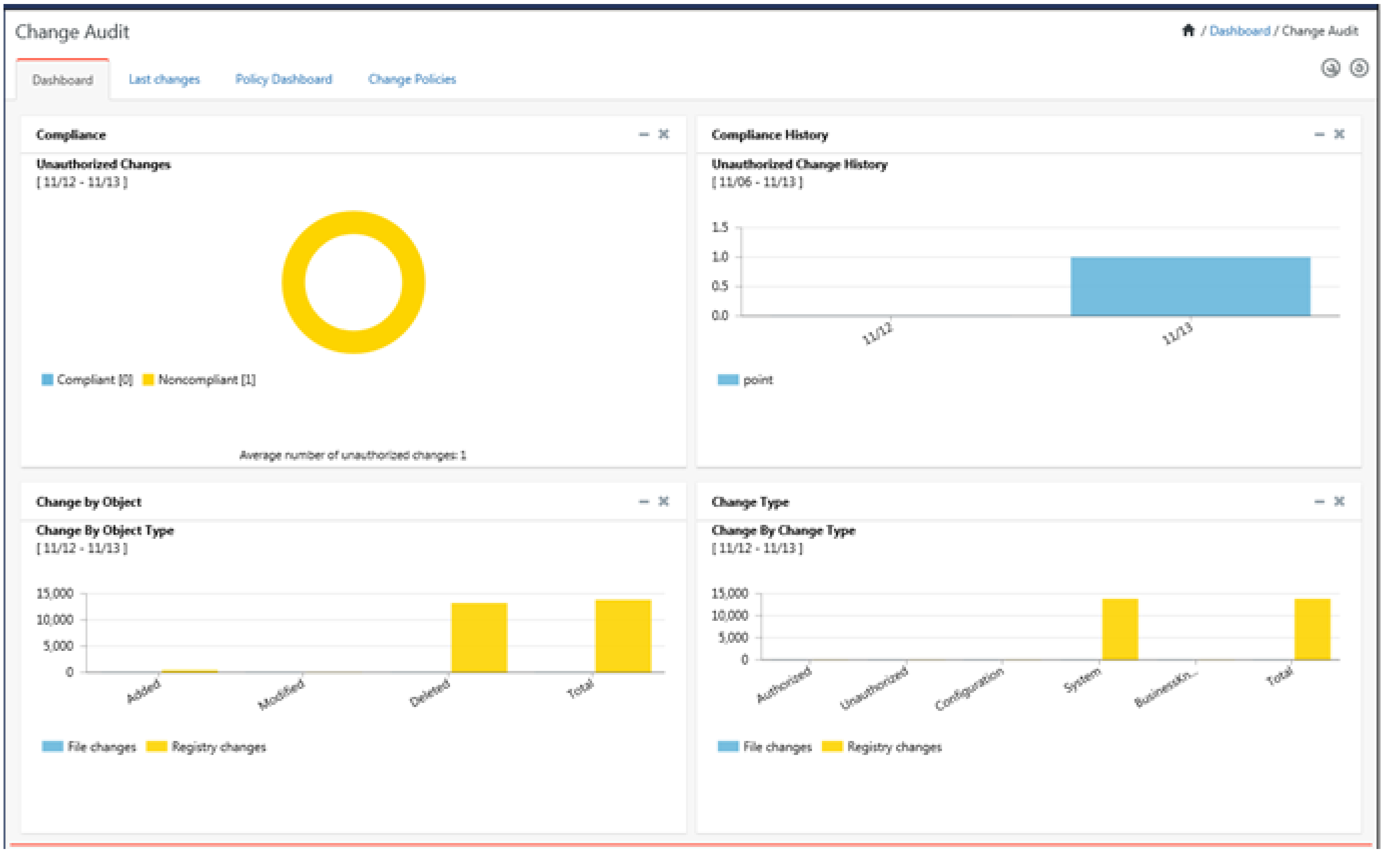
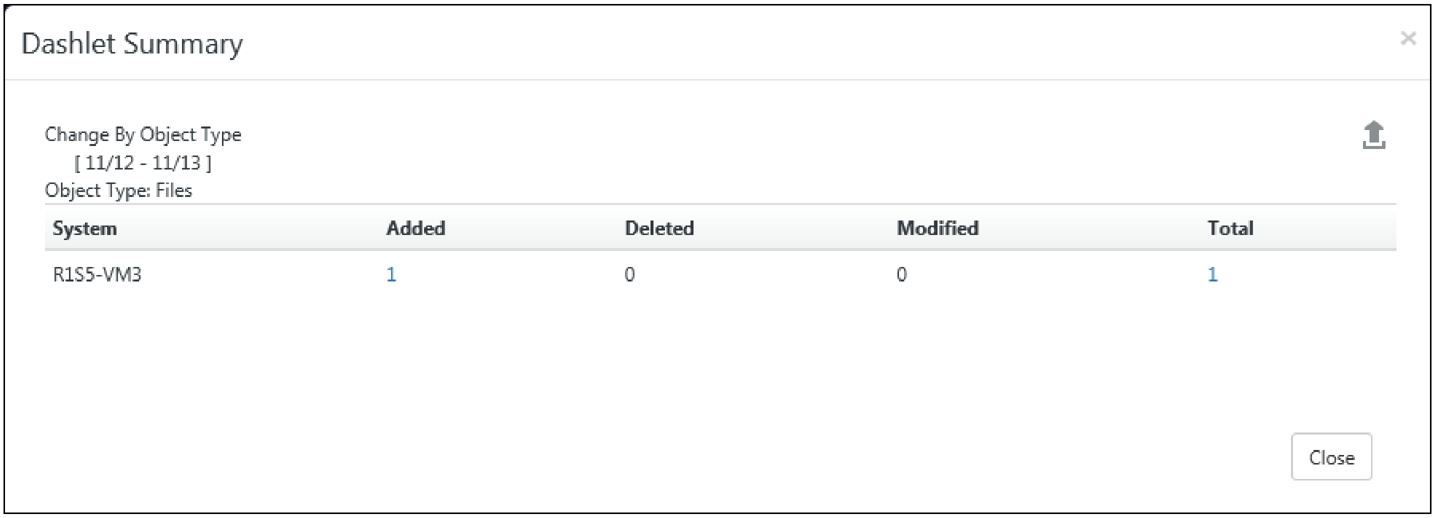


Figure 155

6. Click any graph or a legend to view respective Dashlet summary.

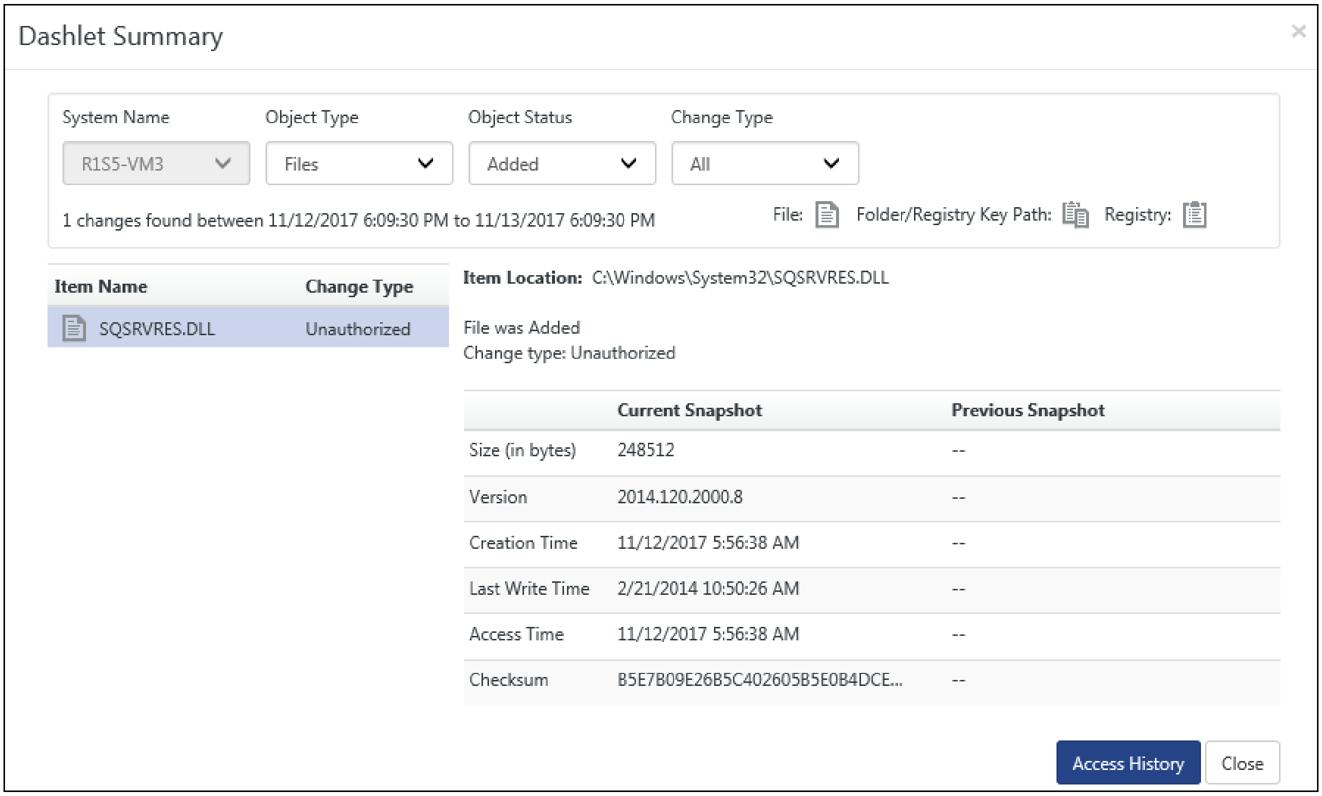


Change By Object Type
[11/12 - 11/13]
Object Type: Files

System	Added	Deleted	Modified	Total
R1S5-VM3	1	0	0	1

Figure 156

7. Click any hyperlink to view respective change details.



System Name: R1S5-VM3
Object Type: Files
Object Status: Added
Change Type: All

1 changes found between 11/12/2017 6:09:30 PM to 11/13/2017 6:09:30 PM

File: Folder/Registry Key Path: Registry:

Item Name	Change Type
SQSRVRES.DLL	Unauthorized

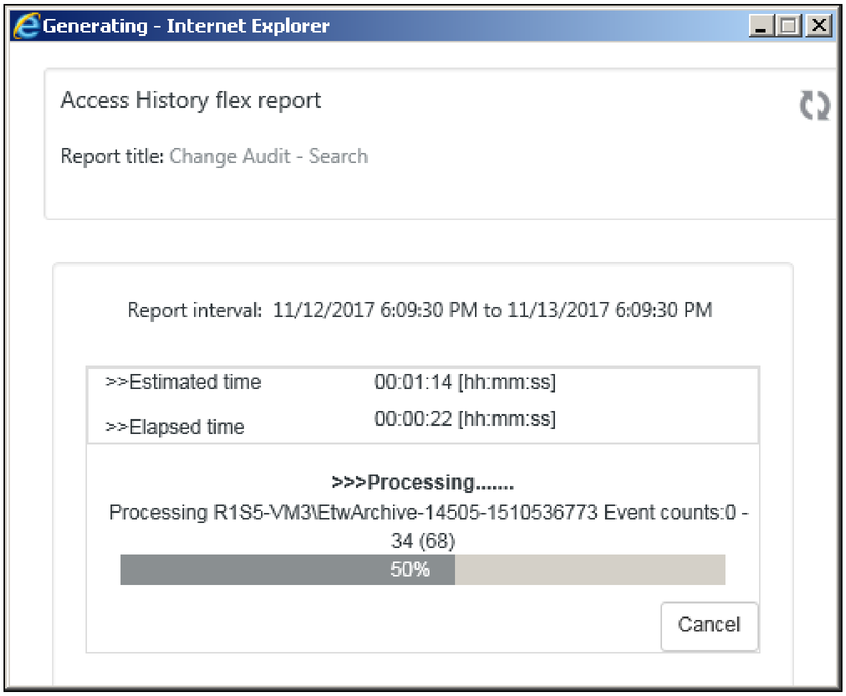
Item Location: C:\Windows\System32\SQSRVRES.DLL

File was Added
Change type: Unauthorized

	Current Snapshot	Previous Snapshot
Size (in bytes)	248512	--
Version	2014.120.2000.8	--
Creation Time	11/12/2017 5:56:38 AM	--
Last Write Time	2/21/2014 10:50:26 AM	--
Access Time	11/12/2017 5:56:38 AM	--
Checksum	B5E7B09E26B5C402605B5E0B4DCE...	--

Figure 157

8. Select **Access History**.



Access History flex report

Report title: Change Audit - Search

Report interval: 11/12/2017 6:09:30 PM to 11/13/2017 6:09:30 PM

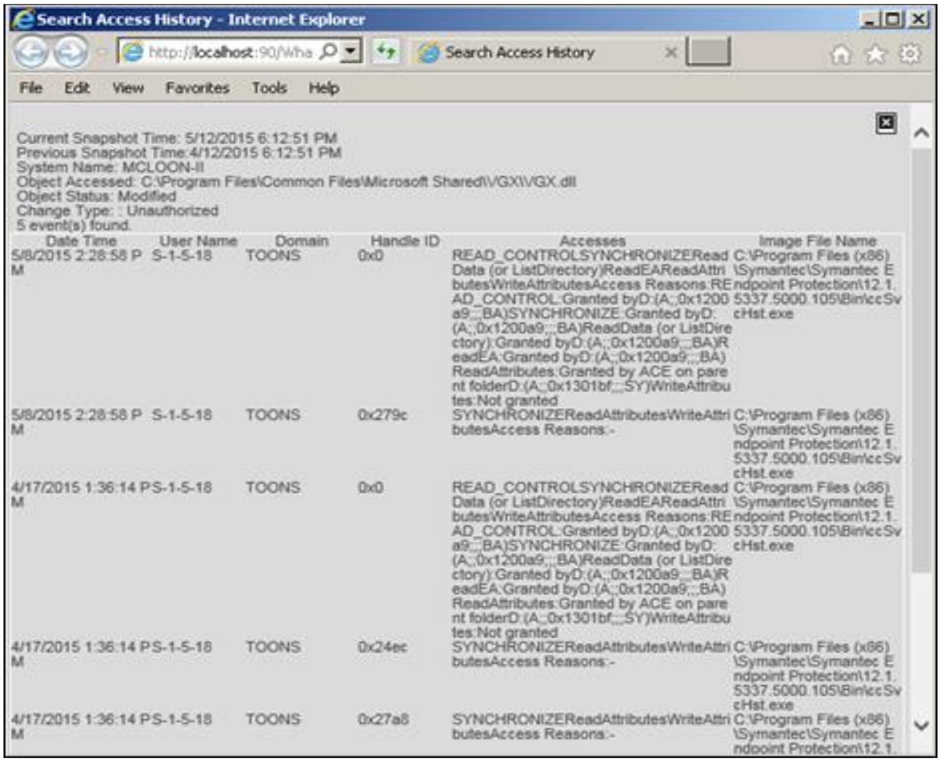
>>Estimated time	00:01:14 [hh:mm:ss]
>>Elapsed time	00:00:22 [hh:mm:ss]

>>>Processing.......

Processing R1S5-VM3\EtwArchive-14505-1510536773 Event counts:0 - 34 (68)

Figure 158

Access History flex report opens.



Current Snapshot Time: 5/12/2015 6:12:51 PM
Previous Snapshot Time:4/12/2015 6:12:51 PM
System Name: MCLOON-II
Object Accessed: C:\Program Files\Common Files\Microsoft Shared\VGX\VGX.dll
Object Status: Modified
Change Type: : Unauthorized
5 event(s) found.

Date Time	User Name	Domain	Handle ID	Accesses	Image File Name
5/8/2015 2:28:58 PM	S-1-5-18	TOONS	0x0	READ_CONTROLSYNCHRONIZEReadData (or ListDirectory)ReadEAReadAttributesWriteAttributesAccess Reasons:READ_CONTROL:Granted byD:(A;;0x1200a9;;;BA)SYNCHRONIZE:Granted byD:(A;;0x1200a9;;;BA)ReadData (or ListDirectory):Granted byD:(A;;0x1200a9;;;BA)ReadEA:Granted byD:(A;;0x1200a9;;;BA)ReadAttributes:Granted by ACE on parent folderD:(A;;0x1301bf;;;SY)WriteAttributes:Not granted	C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\12.1.5337.5000.105\Bin\ccSvcHst.exe
5/8/2015 2:28:58 PM	S-1-5-18	TOONS	0x279c	SYNCHRONIZEReadAttributesWriteAttributesAccess Reasons:-	C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\12.1.5337.5000.105\Bin\ccSvcHst.exe
4/17/2015 1:36:14 PM	S-1-5-18	TOONS	0x0	READ_CONTROLSYNCHRONIZEReadData (or ListDirectory)ReadEAReadAttributesWriteAttributesAccess Reasons:READ_CONTROL:Granted byD:(A;;0x1200a9;;;BA)SYNCHRONIZE:Granted byD:(A;;0x1200a9;;;BA)ReadData (or ListDirectory):Granted byD:(A;;0x1200a9;;;BA)ReadEA:Granted byD:(A;;0x1200a9;;;BA)ReadAttributes:Granted by ACE on parent folderD:(A;;0x1301bf;;;SY)WriteAttributes:Not granted	C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\12.1.5337.5000.105\Bin\ccSvcHst.exe
4/17/2015 1:36:14 PM	S-1-5-18	TOONS	0x24ec	SYNCHRONIZEReadAttributesWriteAttributesAccess Reasons:-	C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\12.1.5337.5000.105\Bin\ccSvcHst.exe
4/17/2015 1:36:14 PM	S-1-5-18	TOONS	0x27a8	SYNCHRONIZEReadAttributesWriteAttributesAccess Reasons:-	C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\12.1.

Figure 159

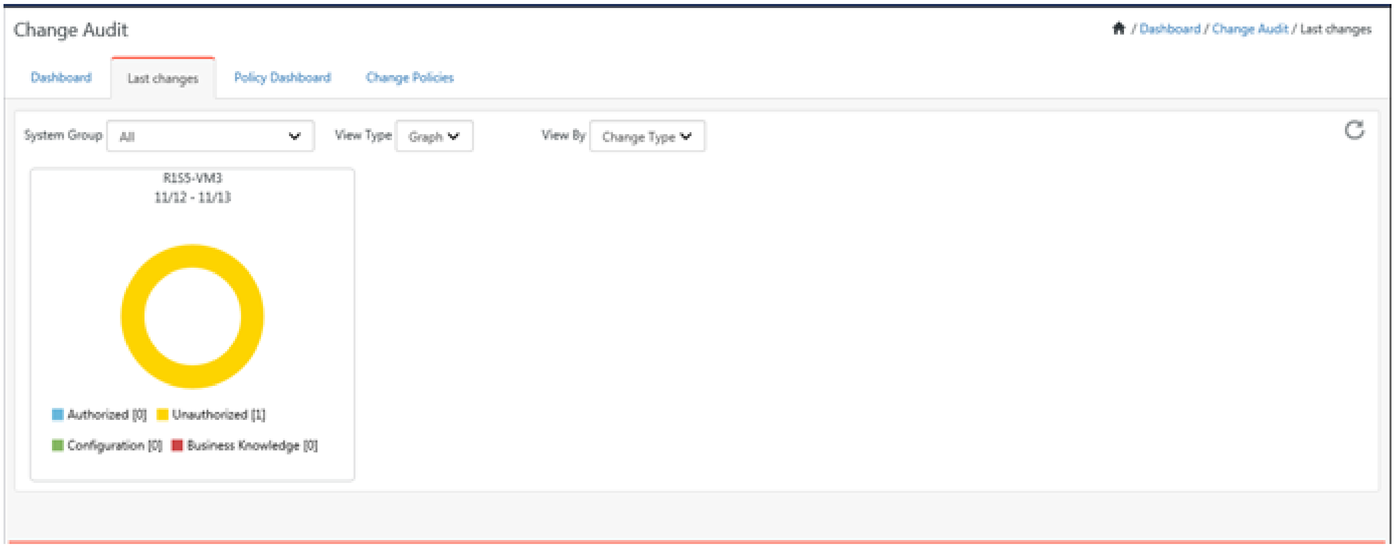
9. Click **Export** icon to export data to excel.

2.14 Last Changes tab

Last changes display the summary of snapshot comparison results.

a. Click **Last changes** tab.

EventTracker opens the Last changes tab.



System Group: All
View Type: Graph
View By: Change Type

Figure 160

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.

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

Fields	Description
Authorized	Detected changes that can be matched with an approved change request.
Unauthorized	Detected changes that cannot be matched to an approved change request.
Configuration	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.
Business Knowledge	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.

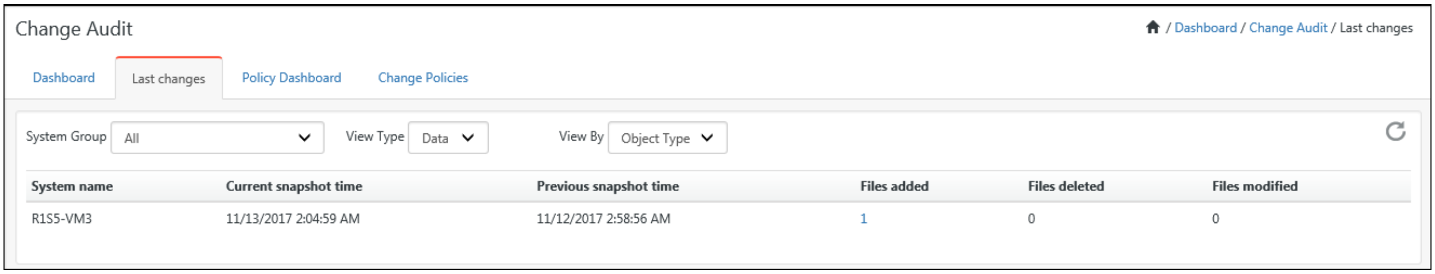
Table 17

2.14.1 Viewing 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 opens the statistical data of **Change Type/Object Type.**



Change Audit

/ Dashboard / Change Audit / Last changes

System Group: All

View Type: Data

View By: Object Type

System name	Current snapshot time	Previous snapshot time	Files added	Files deleted	Files modified
R1S5-VM3	11/13/2017 2:04:59 AM	11/12/2017 2:58:56 AM	1	0	0

Figure 161

2.14.2 Viewing 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 opens the default chart view summary of **Change Type/Object Type.**

2.15 Setting Dashboard Preferences

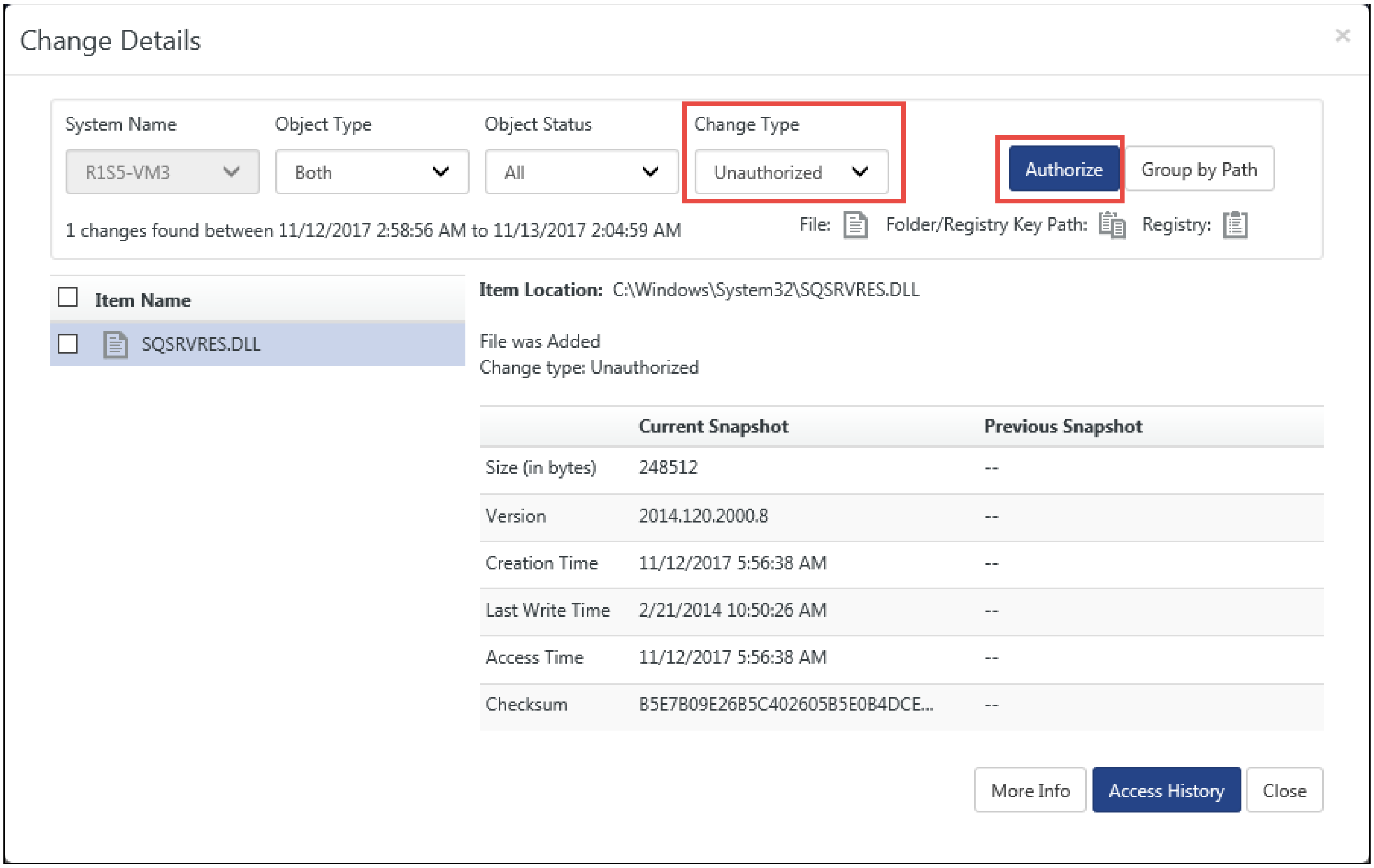
To set Dashboard preferences, refer EventTracker Control Panel -> Change Audit.

2.15.1 Authorizing 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 donut section under **View Type - Graph**.

   EventTracker opens 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 **Authorize**.



System Name: R1S5-VM3
Object Type: Both
Object Status: All
Change Type: Unauthorized

1 changes found between 11/12/2017 2:58:56 AM to 11/13/2017 2:04:59 AM

☐	Item Name
☐	SQSRVRES.DLL

Item Location: C:\Windows\System32\SQSRVRES.DLL

File was Added
Change type: Unauthorized

	Current Snapshot	Previous Snapshot
Size (in bytes)	248512	--
Version	2014.120.2000.8	--
Creation Time	11/12/2017 5:56:38 AM	--
Last Write Time	2/21/2014 10:50:26 AM	--
Access Time	11/12/2017 5:56:38 AM	--
Checksum	B5E7B09E26B5C402605B5E0B4DCE...	--

Figure 162

EventTracker opens the Authorization comment window.

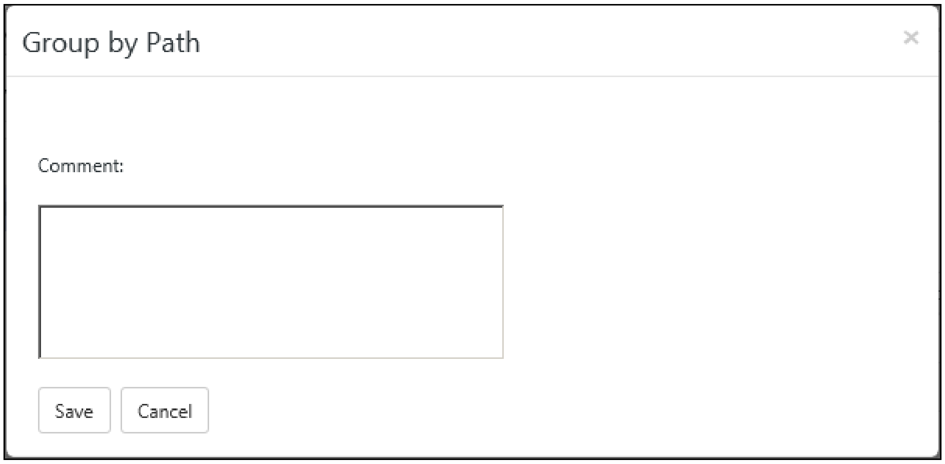


Figure 163

6. Type the reason why the selected item needs authorization in the **Authorization comment** field for future reference.

   This field is not mandatory.

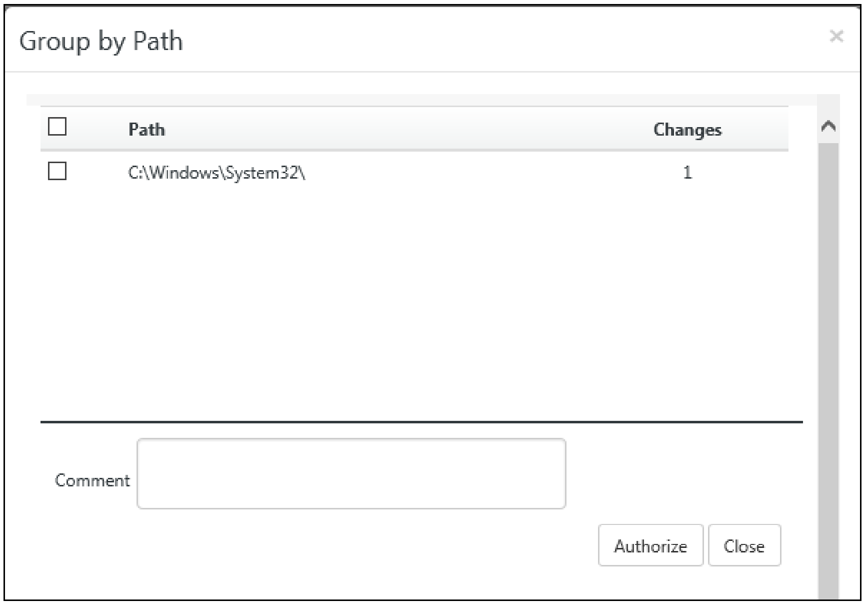
7. Click **Save**.

   EventTracker opens the confirmation message pop-up window.

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 opens the Group by Path window.



Group by Path

□	Path	Changes
□	C:\Windows\System32\	1

Figure 164

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 **Authorize**.

🗎 NOTE

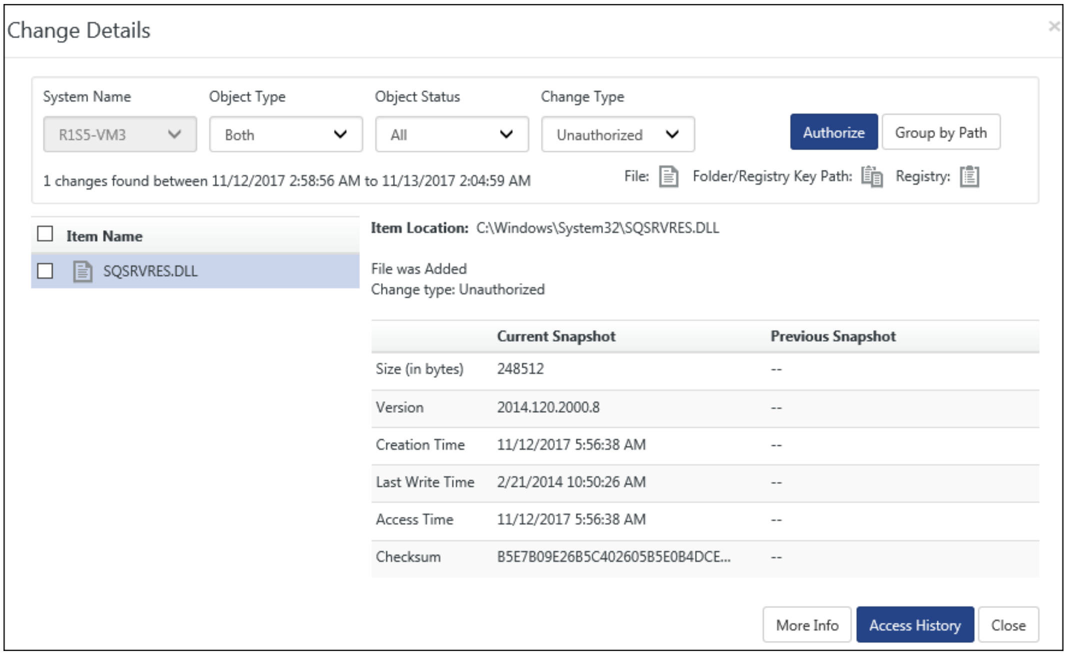
EventTracker enables Authorize button only for unauthorized items.
EventTracker displays the “Authorize” button when changes to “Unauthorized” items (*.exe, *.ocx, *.dll, *.sys, *.drv, *.msc, *.cpl, and *.vxd) are detected.
EventTracker displays the “More Info” button when new/modified/deleted DLLs and EXEs are detected.

2.15.2 Viewing 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) .



Change Details

System Name: R1S5-VM3
Object Type: Both
Object Status: All
Change Type: Unauthorized

1 changes found between 11/12/2017 2:58:56 AM to 11/13/2017 2:04:59 AM

☐ **Item Name**
☐ SQSRVRES.DLL

Item Location: C:\Windows\System32\SQSRVRES.DLL

File was Added
Change type: Unauthorized

	Current Snapshot	Previous Snapshot
Size (in bytes)	248512	--
Version	2014.120.2000.8	--
Creation Time	11/12/2017 5:56:38 AM	--
Last Write Time	2/21/2014 10:50:26 AM	--
Access Time	11/12/2017 5:56:38 AM	--
Checksum	B5E7B09E26B5C402605B5E0B4DCE...	--

Figure 165

1 Select an Item Name and then click **Access History**.

  EventTracker opens the progress bar.
  EventTracker opens the access history of the selected item in a pop-up window.

2 Click **Export** to export the report into Excel format.

2.15.3 Viewing Additional Information on Files

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

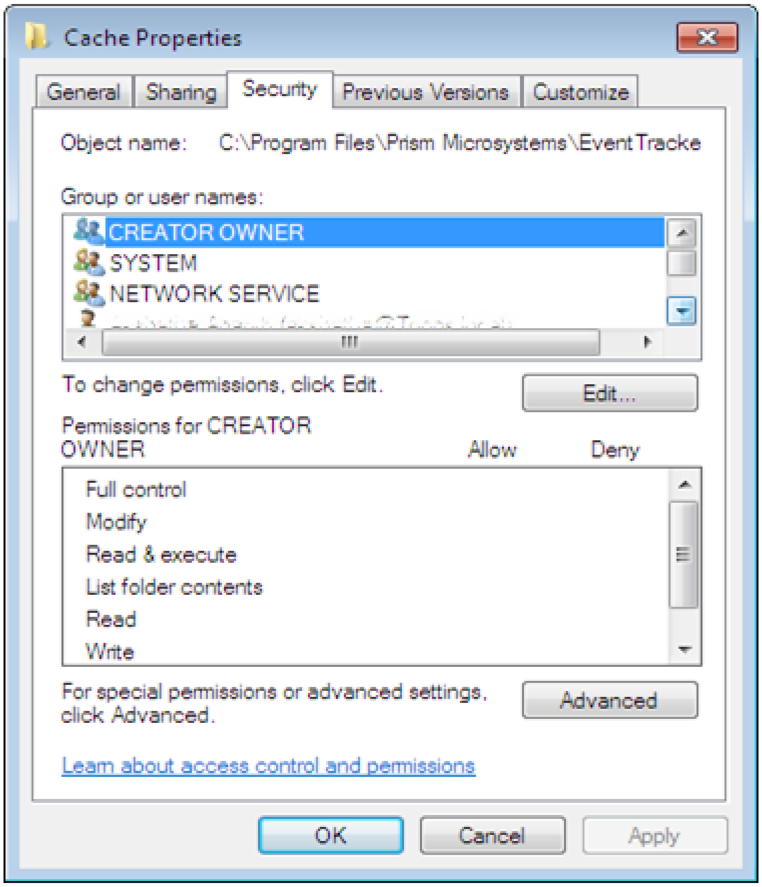
EventTracker redirects to http://www.processlibrary.com Web site.

2.16 Enabling 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.



Cache Properties

Object name: C:\Program Files\Prism Microsystems\EventTracke

Group or user names:

- CREATOR OWNER
- SYSTEM
- NETWORK SERVICE

To change permissions, click Edit.

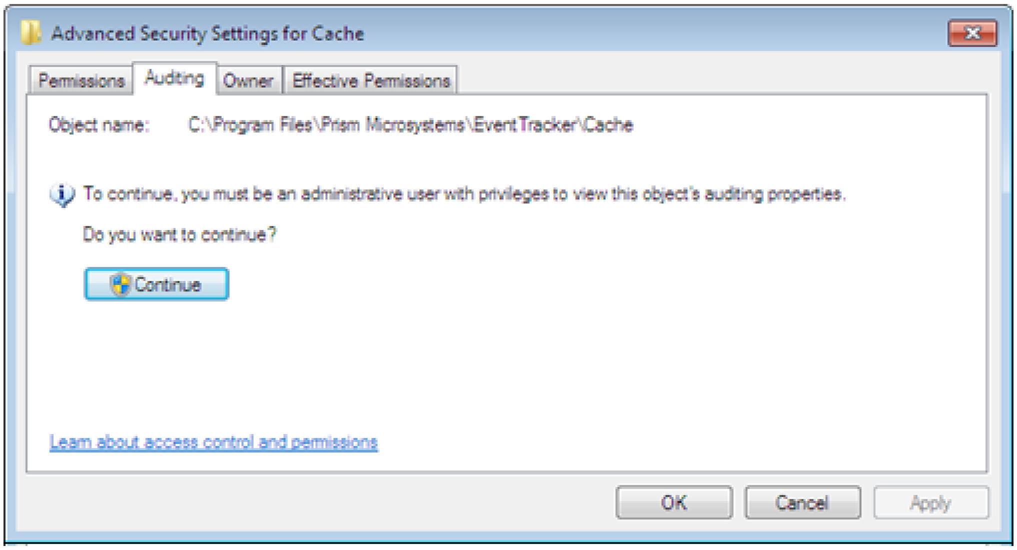
Permissions for CREATOR OWNER

	Allow	Deny
Full control		
Modify		
Read & execute		
List folder contents		
Read		
Write		

For special permissions or advanced settings, click Advanced.

Figure 166

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



Advanced Security Settings for Cache

Object name: C:\Program Files\Prism Microsystems\EventTracker\Cache

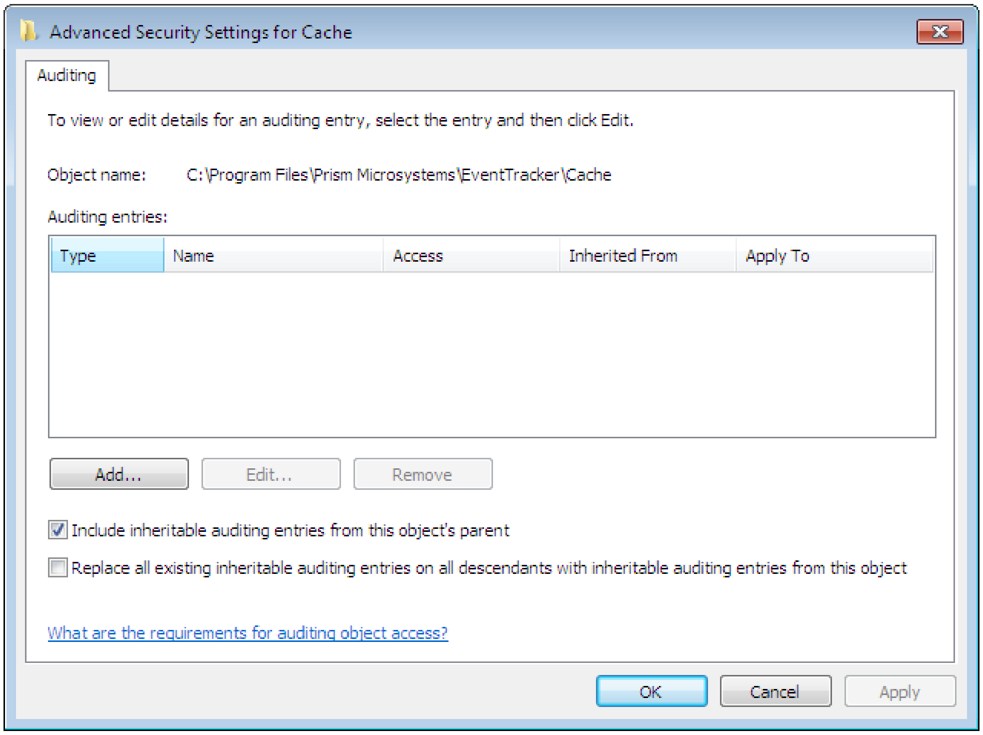
To continue, you must be an administrative user with privileges to view this object's auditing properties.

Do you want to continue?

Figure 167

4. Click **Continue.**

   Advance Security Settings for Cache window opens.



Advanced Security Settings for Cache

To view or edit details for an auditing entry, select the entry and then click Edit.

Object name: C:\Program Files\Prism Microsystems\EventTracker\Cache

Auditing entries:

Type	Name	Access	Inherited From	Apply To

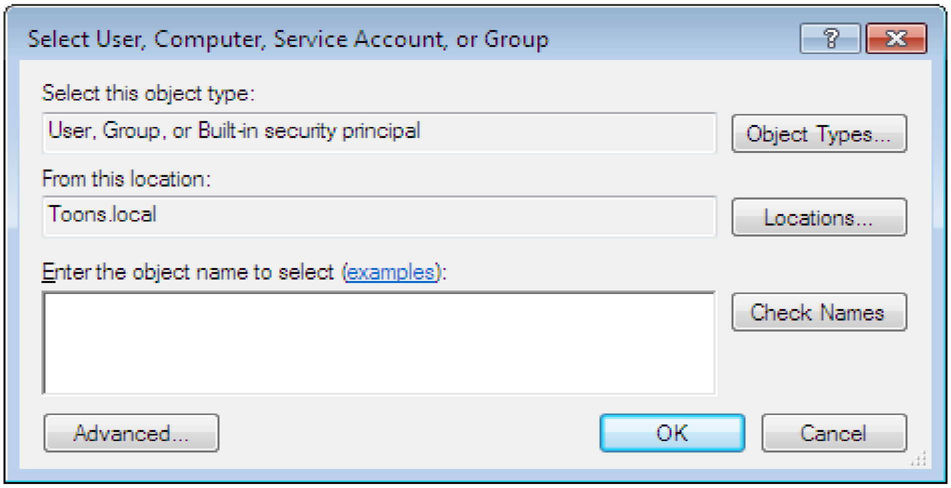
☑ Include inheritable auditing entries from this object's parent

□ Replace all existing inheritable auditing entries on all descendants with inheritable auditing entries from this object

Figure 168

5. Click **Add**.

   Select User, Computer, Service Account, or Group window is opens.



Select User, Computer, Service Account, or Group

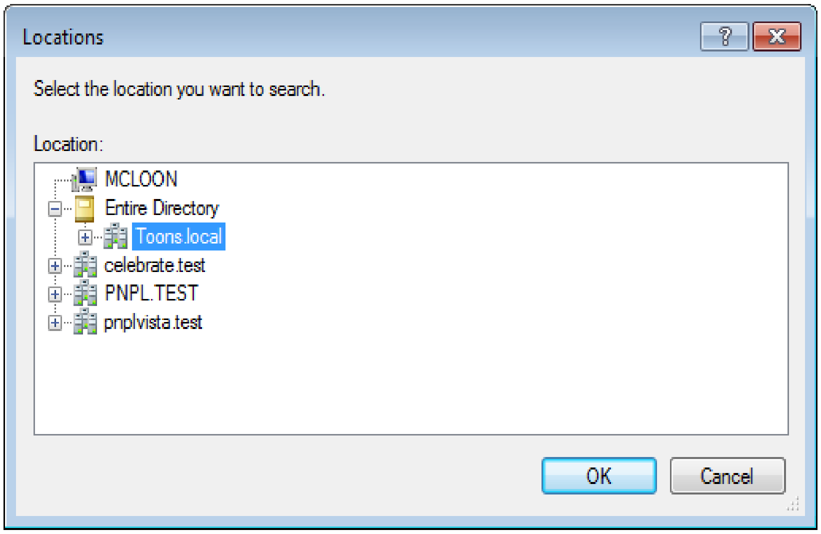
Select this object type:
User, Group, or Built-in security principal

From this location:
Toons.local

Enter the object name to select (examples):

Figure 169

6. To select the location from where you want to add users, click **Locations**.



Locations

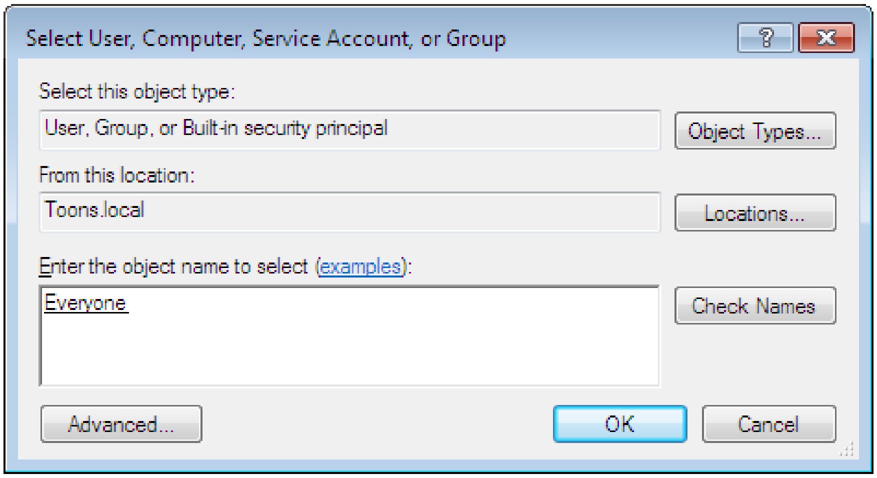
Select the location you want to search.

Location:

Figure 170

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



Select User, Computer, Service Account, or Group

Select this object type:
User, Group, or Built-in security principal

From this location:
Toons.local

Enter the object name to select (examples):
Everyone

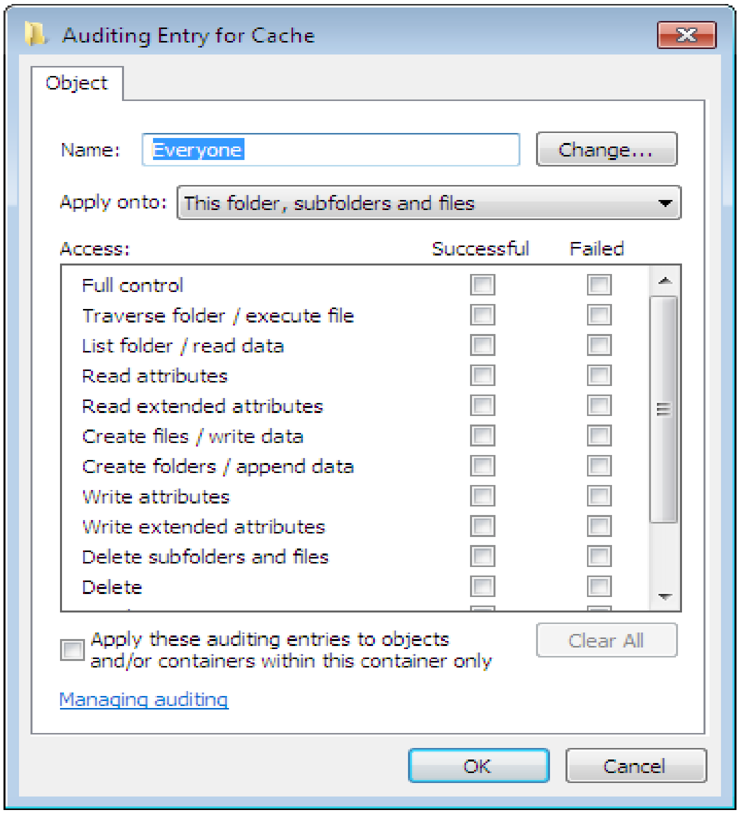
Figure 171

9. Click **Check Names**.

   If the username is valid, the username 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 opens.



Auditing Entry for Cache

Object

Name: Everyone

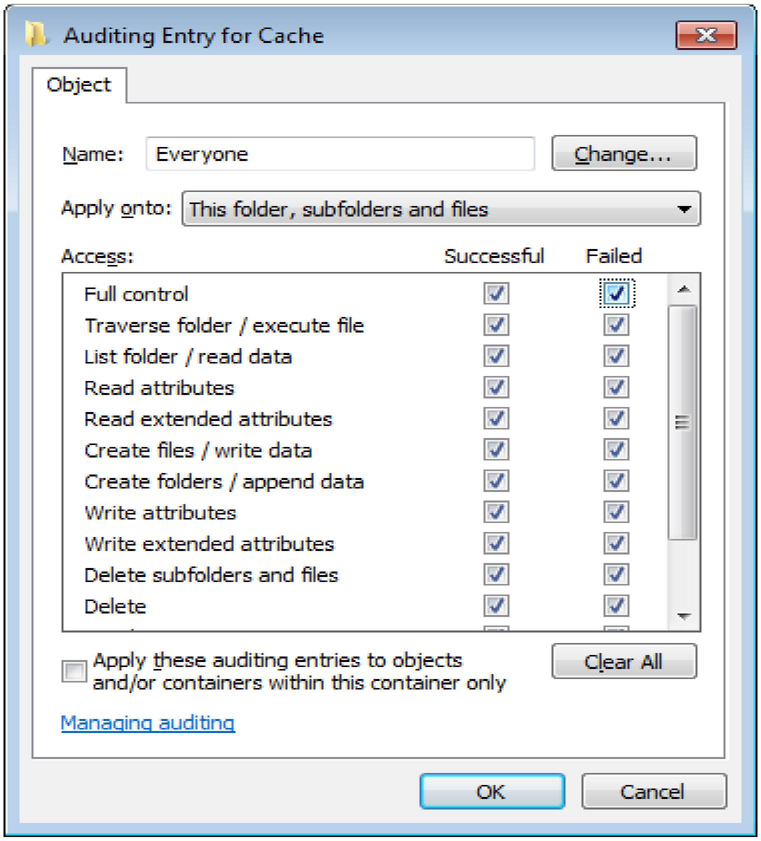
Apply onto: This folder, subfolders and files

Access:	Successful	Failed
Full control	☐	☐
Traverse folder / execute file	☐	☐
List folder / read data	☐	☐
Read attributes	☐	☐
Read extended attributes	☐	☐
Create files / write data	☐	☐
Create folders / append data	☐	☐
Write attributes	☐	☐
Write extended attributes	☐	☐
Delete subfolders and files	☐	☐
Delete	☐	☐

☐ Apply these auditing entries to objects and/or containers within this container only

Figure 172

11. Select **Full Control** under **Successful** and **Failed**.



Auditing Entry for Cache

Name: Everyone

Apply onto: This folder, subfolders and files

Access:	Successful	Failed
Full control	☑	☑
Traverse folder / execute file	☑	☑
List folder / read data	☑	☑
Read attributes	☑	☑
Read extended attributes	☑	☑
Create files / write data	☑	☑
Create folders / append data	☑	☑
Write attributes	☑	☑
Write extended attributes	☑	☑
Delete subfolders and files	☑	☑
Delete	☑	☑

☐ Apply these auditing entries to objects and/or containers within this container only

Figure 173

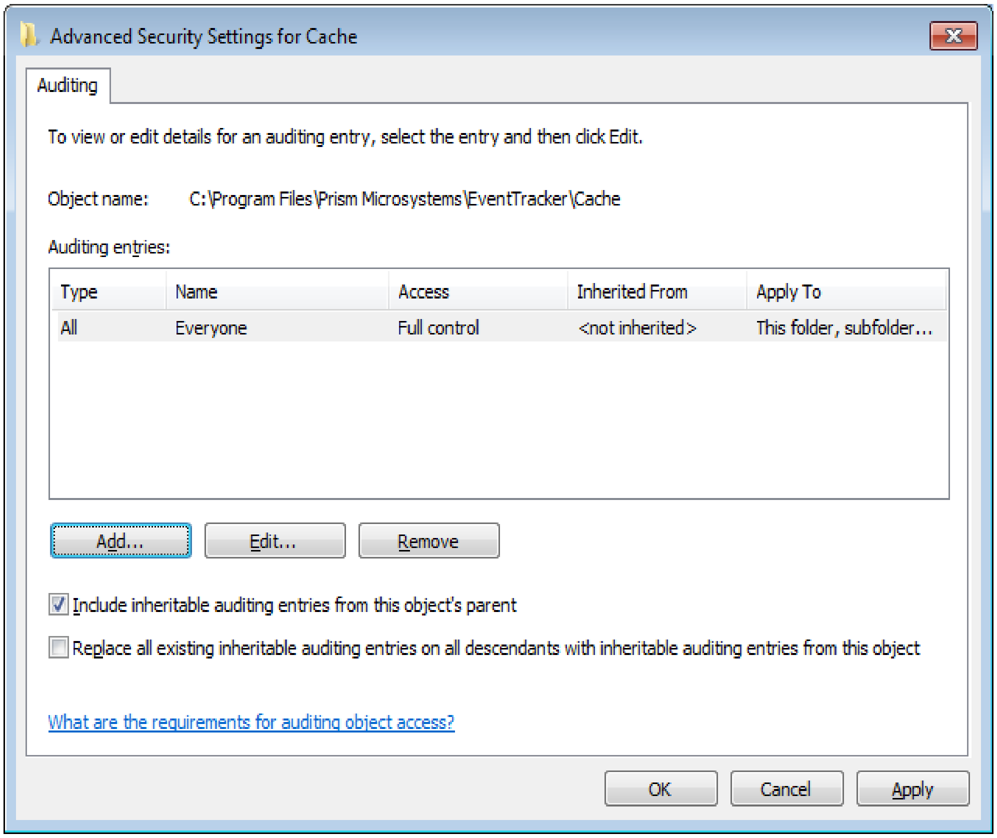
12. All other checkboxes are also selected automatically when you select **Full Control** checkbox.

NOTE

Select the Access options as per your requirement.

13. Click **OK**.

Advanced Security Settings for Cache window displays with the newly added user.



Advanced Security Settings for Cache

Auditing

To view or edit details for an auditing entry, select the entry and then click Edit.

Object name: C:\Program Files\Prism Microsystems\EventTracker\Cache

Auditing entries:

Type	Name	Access	Inherited From	Apply To
All	Everyone	Full control	<not inherited>	This folder, subfolder...

☑ Include inheritable auditing entries from this object's parent

□ Replace all existing inheritable auditing entries on all descendants with inheritable auditing entries from this object

What are the requirements for auditing object access?

Figure 174

14. Click **Apply,** and then click **OK**.

🗎 NOTE

Similarly, you can enable auditing on files.

2.17 Policy Dashboard tab

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

1. In **Policy Dashboard** tab, click **Configure** ⚙ .

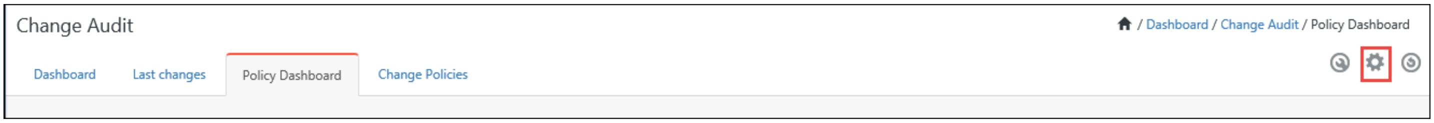
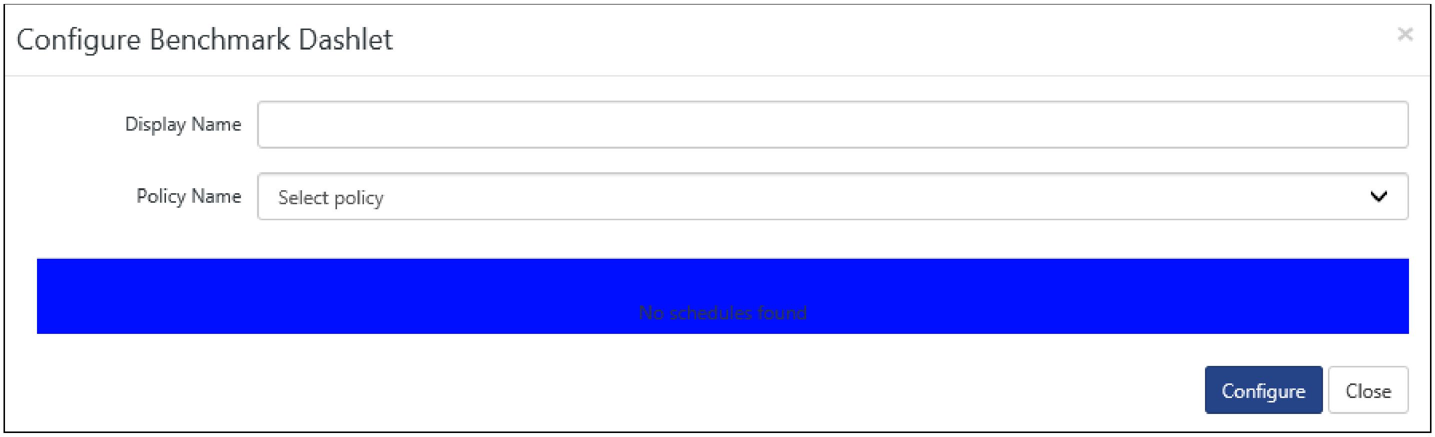


Figure 175

EventTracker opens the Configure Benchmark Dashlets pop-up window.



Configure Benchmark Dashlet

Display Name

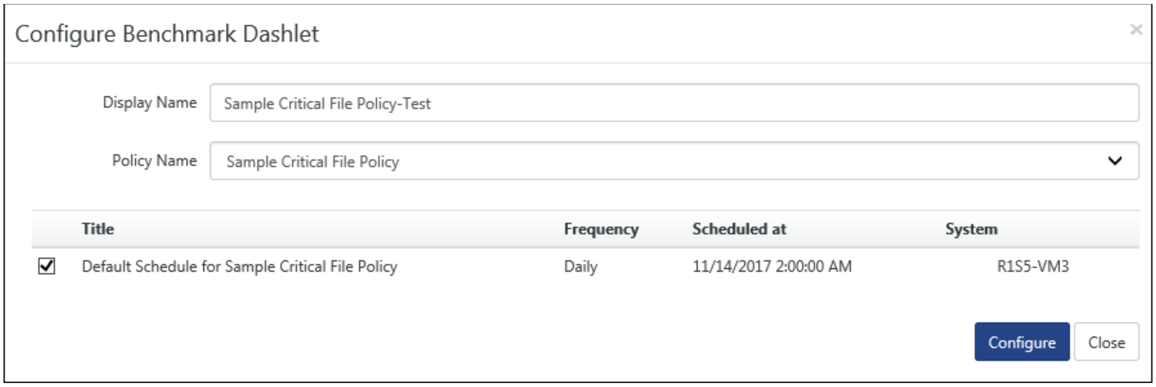
Policy Name: Select policy

No schedules found

Figure 176

2. Type a comprehensible name in the **Display Name** field.
3. Select a policy from the **Policy Name** field.

   EventTracker displays the **Configure Benchmark Dashlet** pop-up window with Schedule details of the selected Policy.



Configure Benchmark Dashlet

Display Name: Sample Critical File Policy-Test

Policy Name: Sample Critical File Policy

	Title	Frequency	Scheduled at	System
☑	Default Schedule for Sample Critical File Policy	Daily	11/14/2017 2:00:00 AM	R1S5-VM3

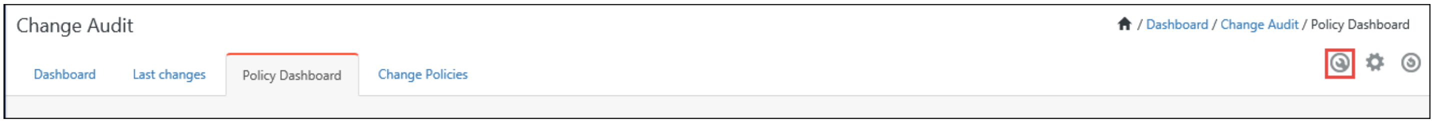
Figure 177

4. Click the checkbox to select the Schedule(s), and then click **Configure**.

2.17.1 Customizing the Policies Dashboard

This option helps to customize the dashboard with configured Dashlets.

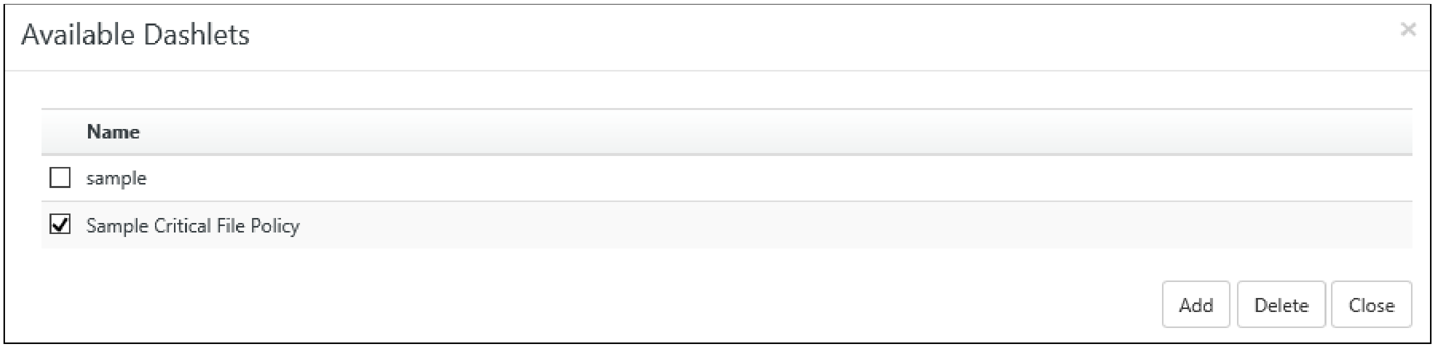
1) In **Change Audit** menu, click the **Policy Dashboard** drop down and then click **Customize** .



Change Audit

Figure 178

EventTracker opens the Available Dashlets pop-up window.



Available Dashlets

	Name
□	sample
☑	Sample Critical File Policy

Figure 179

2) Click the checkbox to select the Dashlet(s), and then click **Add**.

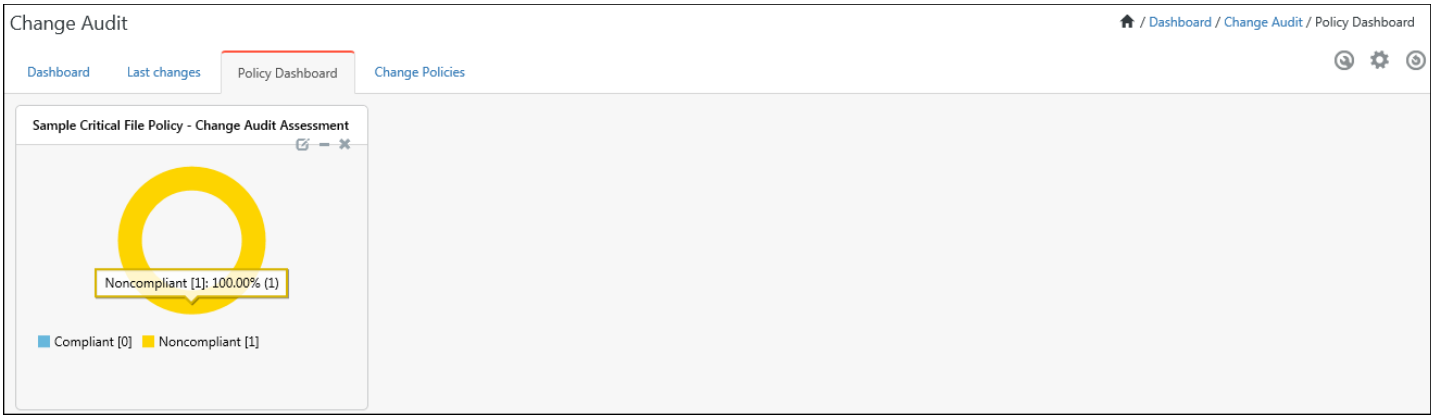
   EventTracker adds the Dashlet(s) to the Dashboard.

   OR

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

   EventTracker deletes the dashlet(s).

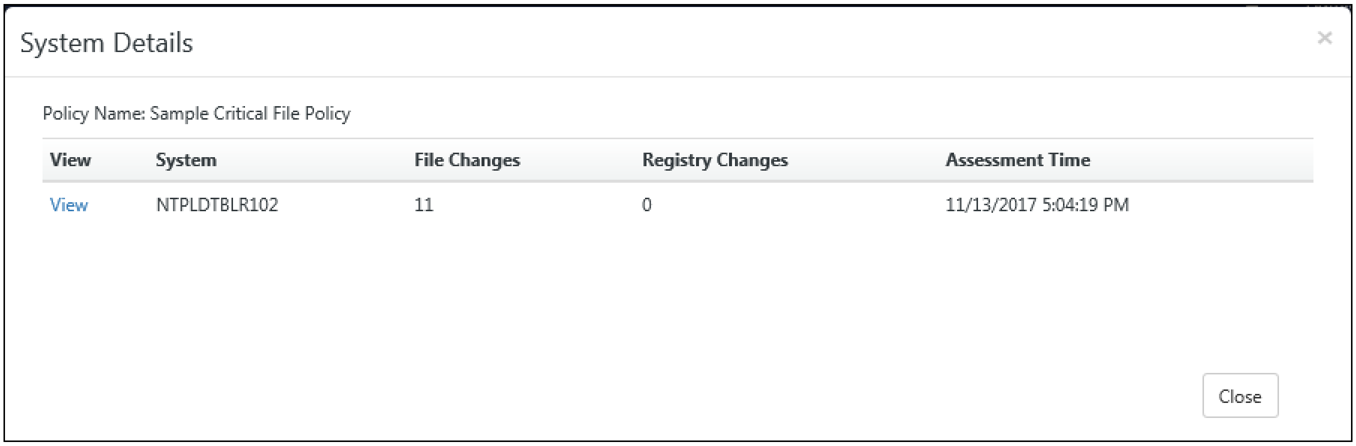
3) Click a donut chart or a legend to view respective system details.



Change Audit
/ Dashboard / Change Audit / Policy Dashboard
Dashboard
Last changes
Policy Dashboard
Change Policies
Sample Critical File Policy - Change Audit Assessment
Noncompliant [1]: 100.00% (1)
Compliant [0]
Noncompliant [1]

Figure 180

EventTracker opens the System Details Pop-up window.



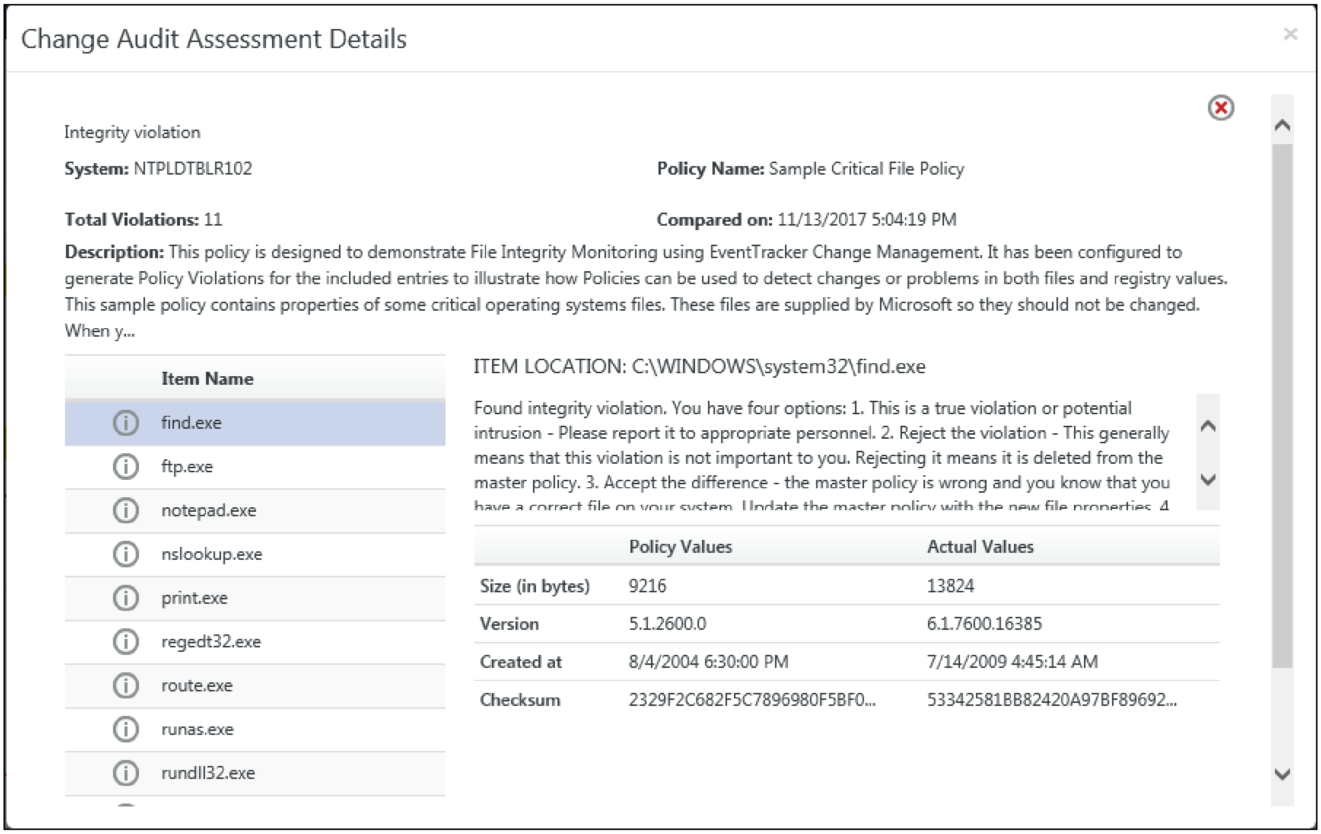
System Details

Policy Name: Sample Critical File Policy

View	System	File Changes	Registry Changes	Assessment Time
View	NTPLDTBLR102	11	0	11/13/2017 5:04:19 PM

Figure 181

4) Click the **View** hyperlink to view **Change Audit Assessment Details**.



Change Audit Assessment Details

Integrity violation

System: NTPLDTBLR102

Policy Name: Sample Critical File Policy

Total Violations: 11

Compared on: 11/13/2017 5:04:19 PM

Description: This policy is designed to demonstrate File Integrity Monitoring using EventTracker Change Management. It has been configured to generate Policy Violations for the included entries to illustrate how Policies can be used to detect changes or problems in both files and registry values. This sample policy contains properties of some critical operating systems files. These files are supplied by Microsoft so they should not be changed. When y...

Item Name
find.exe
ftp.exe
notepad.exe
nslookup.exe
print.exe
regedt32.exe
route.exe
runas.exe
rundll32.exe

ITEM LOCATION: C:\WINDOWS\system32\find.exe

Found integrity violation. You have four options: 1. This is a true violation or potential intrusion - Please report it to appropriate personnel. 2. Reject the violation - This generally means that this violation is not important to you. Rejecting it means it is deleted from the master policy. 3. Accept the difference - the master policy is wrong and you know that you have a correct file on your system. Update the master policy with the new file properties. 4

	Policy Values	Actual Values
Size (in bytes)	9216	13824
Version	5.1.2600.0	6.1.7600.16385
Created at	8/4/2004 6:30:00 PM	7/14/2009 4:45:14 AM
Checksum	2329F2C682F5C7896980F5BF0...	53342581BB82420A97BF89692...

Figure 182

2.18 EventTracker Inventory Manager

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

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

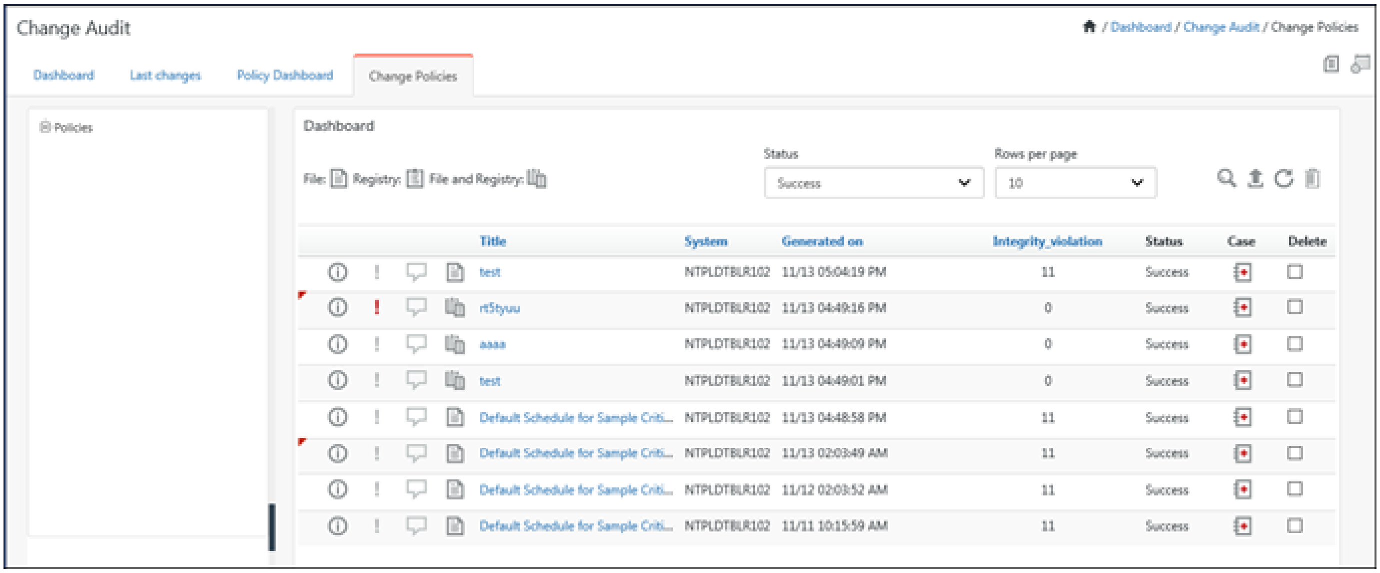
For detail information please refer EventTracker Control Panel -> Change Audit.

2.19 Change Policies tab

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

1 Click the **Change policies** tab.

Policy details opens in dashboard.



Status: Success

Rows per page: 10

Title	System	Generated on	Integrity_violation	Status	Case	Delete
test	NTPLDTBLR102	11/13 05:04:19 PM	11	Success	⊞	☐
rt5tyuu	NTPLDTBLR102	11/13 04:49:16 PM	0	Success	⊞	☐
aaaa	NTPLDTBLR102	11/13 04:49:09 PM	0	Success	⊞	☐
test	NTPLDTBLR102	11/13 04:49:01 PM	0	Success	⊞	☐
Default Schedule for Sample Criti...	NTPLDTBLR102	11/13 04:48:58 PM	11	Success	⊞	☐
Default Schedule for Sample Criti...	NTPLDTBLR102	11/13 02:03:49 AM	11	Success	⊞	☐
Default Schedule for Sample Criti...	NTPLDTBLR102	11/12 02:03:52 AM	11	Success	⊞	☐
Default Schedule for Sample Criti...	NTPLDTBLR102	11/11 10:15:59 AM	11	Success	⊞	☐

Figure 183

Icon	Represents
📄	File changes found.
📋	Registry changes found.
📑	File and registry changes found.
ⓘ	Information icon
💬	Notes icon
⊞	Casebook icon

Table 18

Field	Description
Title	Select any title to view policy comparison results for that period and integrity violation details on the Dashboard.
Status	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.
Delete	Select the checkbox against the policy comparison result and then click this button.

Table 19

2. Click **Information** ⓘ to view Policy Details.
3. Click the **Flag** ! to change status of that policy.

Flag Icon	Represents
! GRAY	Un-flagged and no action has been taken
! RED	Flagged and relevant action is required for that particular incident to solve an issue.
! GREEN	Checked the incident and necessary action has been taken care of

Table 20

4. Click **Notes** 💬 to enter relevant information about the respective policy.
5. Click any **Title** hyperlink to view Integrity violation details.
6. To add data to a Casebook, click **Casebook** .
   Casebook window opens to add to a new or existing Casebook.

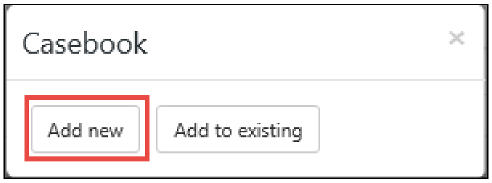


Figure 184

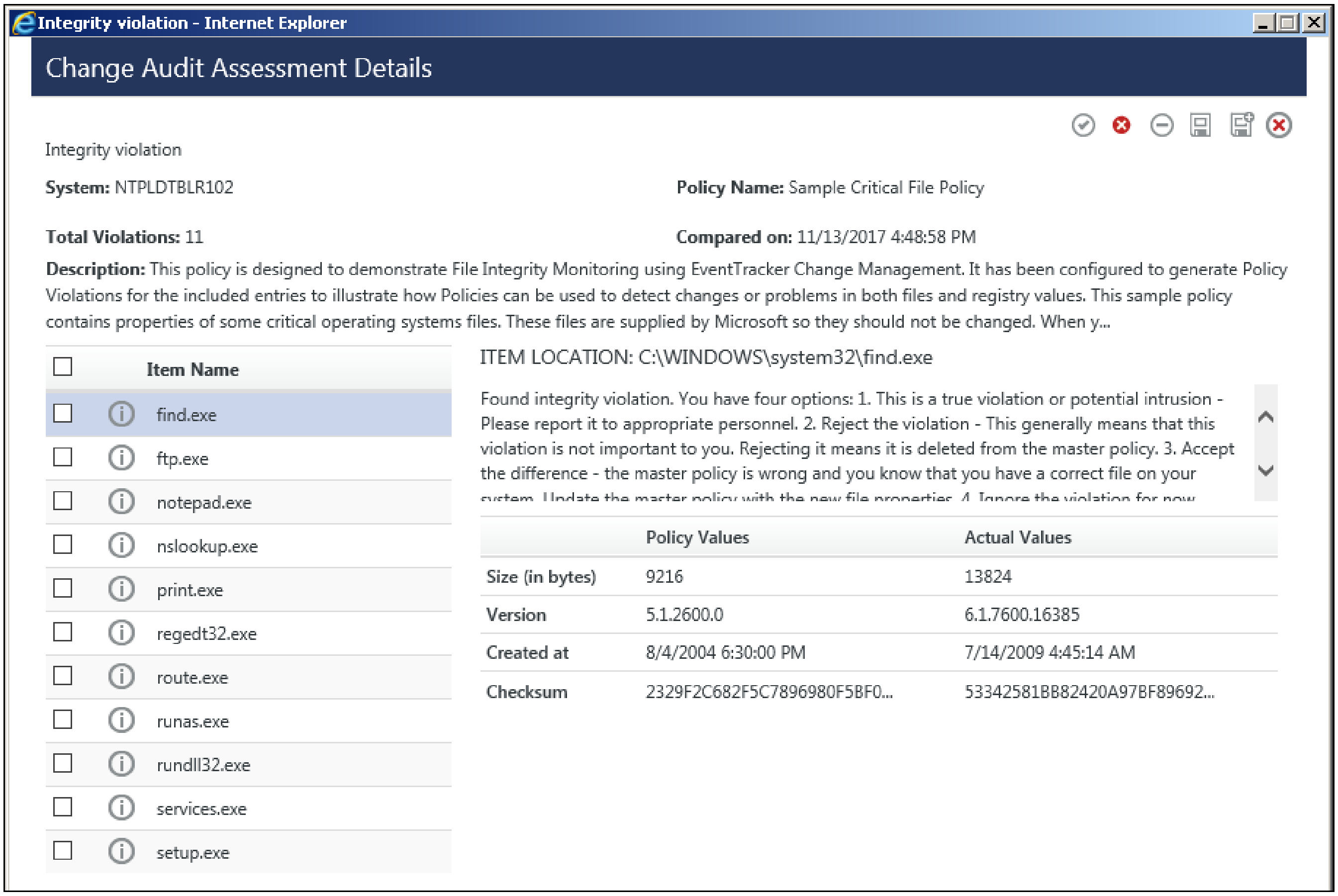
7. To create a new Casebook, click **Add new** Casebook.
8. To add data to a new casebook, click **Add to existing** Casebook.

   For more details regarding usage of Casebook, refer Casebook.
9. To delete a policy, select the **Delete** option and then click the **Delete** button.

2.19.1 Analyzing Policy Comparison Results

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

   EventTracker opens the Policy Comparison Results page.



Change Audit Assessment Details

Integrity violation

System: NTPLDTBLR102

Policy Name: Sample Critical File Policy

Total Violations: 11

Compared on: 11/13/2017 4:48:58 PM

Description: This policy is designed to demonstrate File Integrity Monitoring using EventTracker Change Management. It has been configured to generate Policy Violations for the included entries to illustrate how Policies can be used to detect changes or problems in both files and registry values. This sample policy contains properties of some critical operating systems files. These files are supplied by Microsoft so they should not be changed. When y...

□		Item Name
□	ⓘ	find.exe
□	ⓘ	ftp.exe
□	ⓘ	notepad.exe
□	ⓘ	nslookup.exe
□	ⓘ	print.exe
□	ⓘ	regedt32.exe
□	ⓘ	route.exe
□	ⓘ	runas.exe
□	ⓘ	rundll32.exe
□	ⓘ	services.exe
□	ⓘ	setup.exe

ITEM LOCATION: C:\WINDOWS\system32\find.exe

Found integrity violation. You have four options: 1. This is a true violation or potential intrusion - Please report it to appropriate personnel. 2. Reject the violation - This generally means that this violation is not important to you. Rejecting it means it is deleted from the master policy. 3. Accept the difference - the master policy is wrong and you know that you have a correct file on your system. Update the master policy with the new file properties. 4. Ignore the violation for now

	Policy Values	Actual Values
Size (in bytes)	9216	13824
Version	5.1.2600.0	6.1.7600.16385
Created at	8/4/2004 6:30:00 PM	7/14/2009 4:45:14 AM
Checksum	2329F2C682F5C7896980F5BF0...	53342581BB82420A97BF89692...

Figure 185

Fields	Description
System	Name of the target system where the policy is compared
Policy Name	Name of the policy compared on the target system.
Total Violations	Total number of violations detected.
Compared on	Date and time when the policy was compared.
Description	Description of the policy.
Item Name	Name of the policy item.
Policy Values	Values of the policy item selected in the left pane when the policy was configured.
Actual Values	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.
Item Description	Description of the item selected in e left pane is displayedat the bottom of the right pane.

Table 21

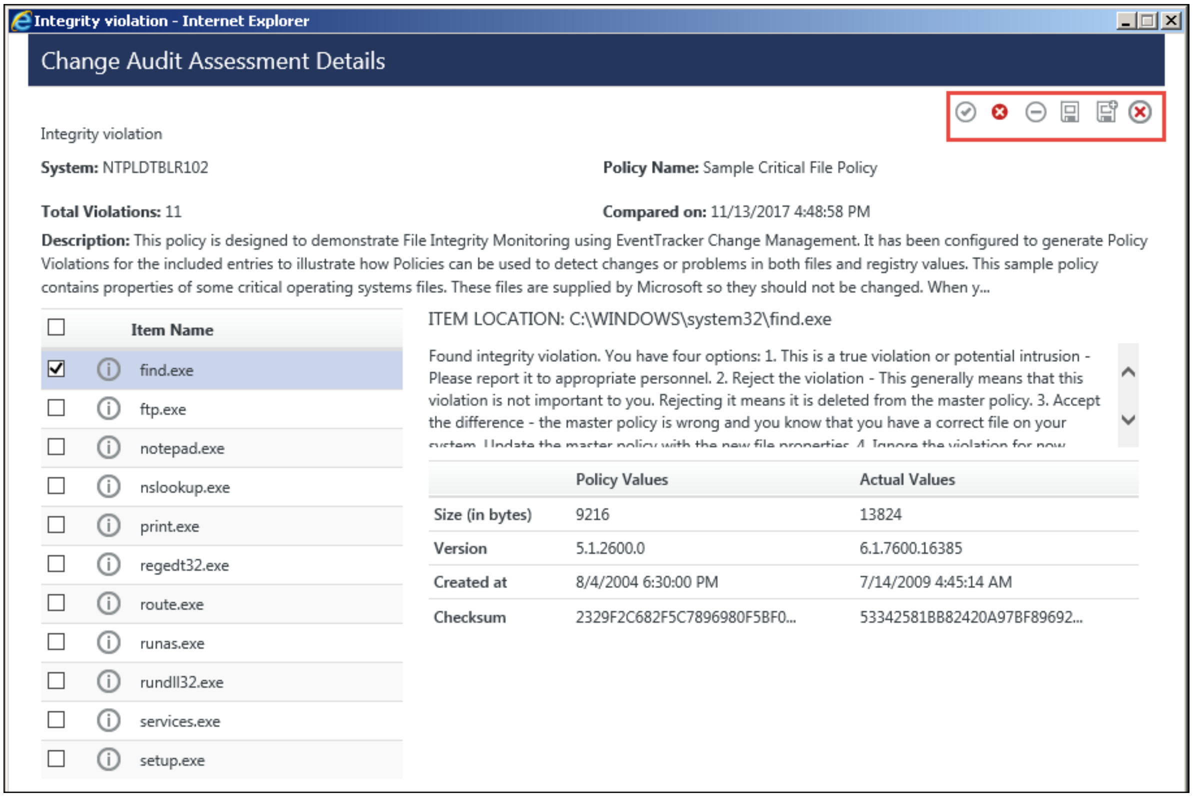
Fields	Description
Accept	If changes are found for the selected item, you can update the master policy with the new value.
Reject	If you find an item to be irrelevant to the present context, you can select and remove that item from the master policy.
Ignore	When you generate a report, ignored items will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

Table 22

Icon	Represents
✓	Items accepted.
⊖	Items ignored.
✖	Items rejected.

Table 23

b. Click the **Item Name** to **Accept**, **Reject** or **Ignore** the integrity violation.



Integrity violation - Internet Explorer

Change Audit Assessment Details

Integrity violation

System: NTPLDTBLR102

Policy Name: Sample Critical File Policy

Total Violations: 11

Compared on: 11/13/2017 4:48:58 PM

Description: This policy is designed to demonstrate File Integrity Monitoring using EventTracker Change Management. It has been configured to generate Policy Violations for the included entries to illustrate how Policies can be used to detect changes or problems in both files and registry values. This sample policy contains properties of some critical operating systems files. These files are supplied by Microsoft so they should not be changed. When y...

☐		Item Name
☑	ⓘ	find.exe
☐	ⓘ	ftp.exe
☐	ⓘ	notepad.exe
☐	ⓘ	nslookup.exe
☐	ⓘ	print.exe
☐	ⓘ	regedt32.exe
☐	ⓘ	route.exe
☐	ⓘ	runas.exe
☐	ⓘ	rundll32.exe
☐	ⓘ	services.exe
☐	ⓘ	setup.exe

ITEM LOCATION: C:\WINDOWS\system32\find.exe

Found integrity violation. You have four options: 1. This is a true violation or potential intrusion - Please report it to appropriate personnel. 2. Reject the violation - This generally means that this violation is not important to you. Rejecting it means it is deleted from the master policy. 3. Accept the difference - the master policy is wrong and you know that you have a correct file on your system. Update the master policy with the new file properties. 4. Ignore the violation for now

	Policy Values	Actual Values
Size (in bytes)	9216	13824
Version	5.1.2600.0	6.1.7600.16385
Created at	8/4/2004 6:30:00 PM	7/14/2009 4:45:14 AM
Checksum	2329F2C682F5C7896980F5BF0...	53342581BB82420A97BF89692...

Figure 186

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 What Changed -> Create Configuration Policy.

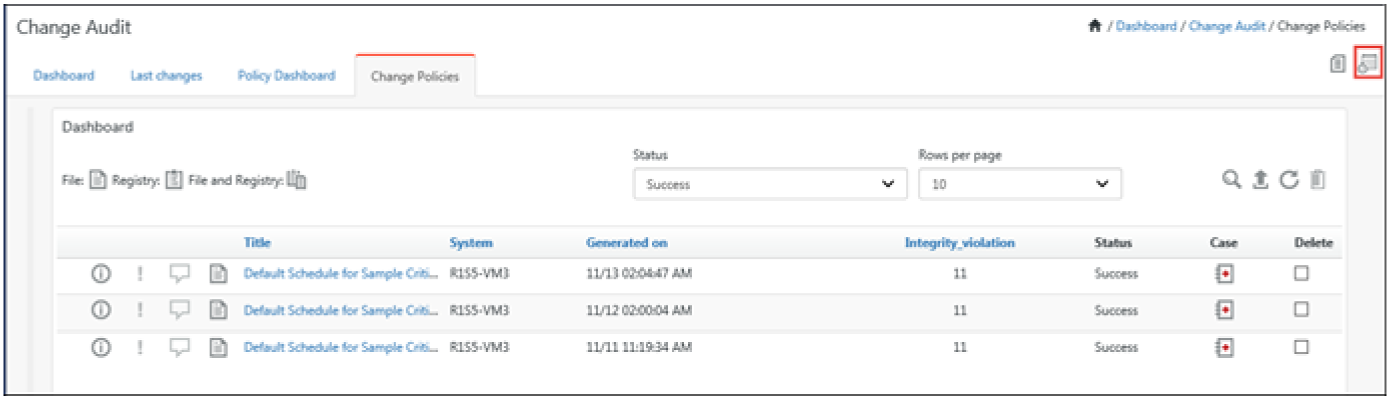
2.20 Scheduling Change Assessment

This option helps you schedule change assessment.

1 To schedule Change Assessment, click **Scheduled Reports** in the right-hand corner, and then click **New Schedule** ⊕.

(OR)

Click **Policies** in the tree pane, click the gear icon and then select **Add Scheduled**.



Change Audit

🏠 / Dashboard / Change Audit / Change Policies

Dashboard

File: Registry: File and Registry:

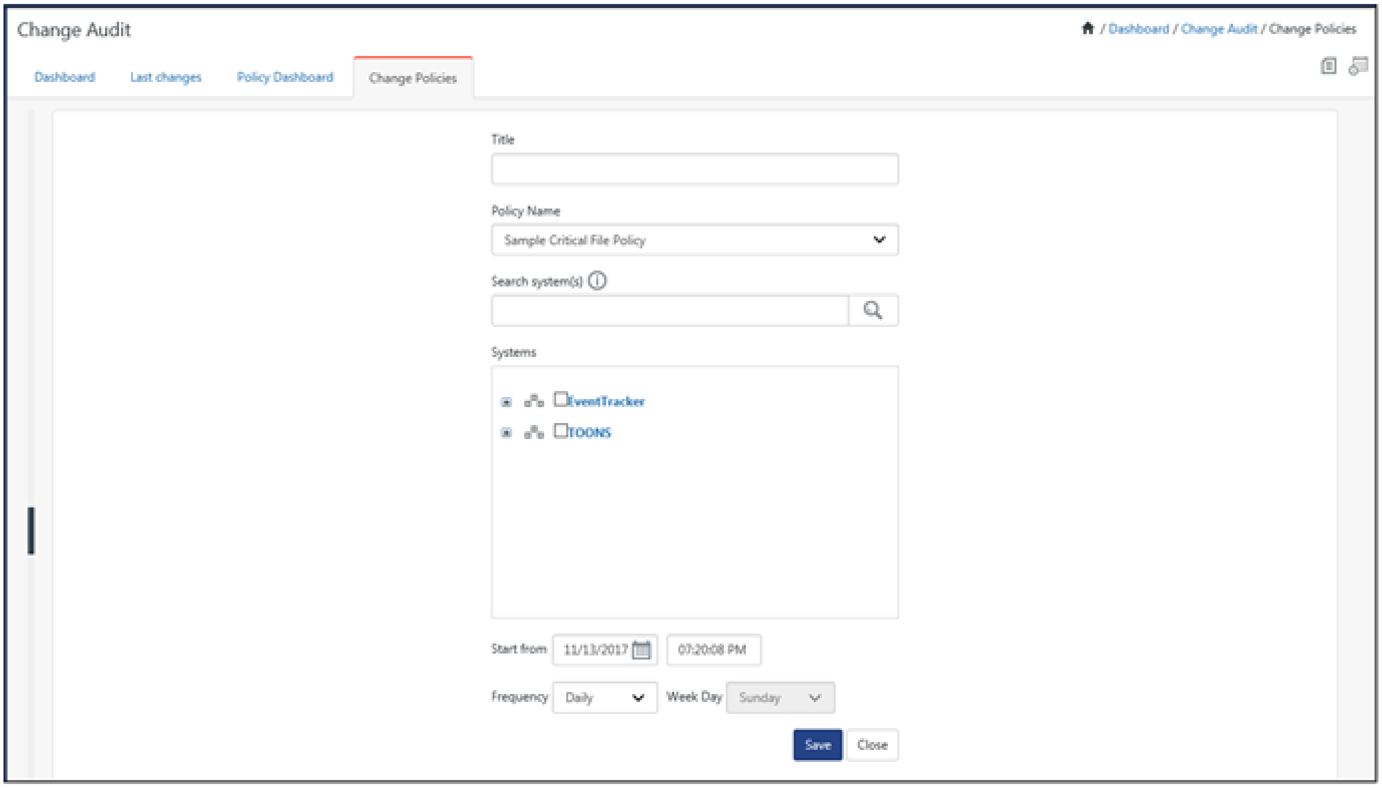
Status: Success

Rows per page: 10

				Title	System	Generated on	Integrity_violation	Status	Case	Delete
ⓘ	!			Default Schedule for Sample Criti...	R1S5-VM3	11/13 02:04:47 AM	11	Success		□
ⓘ	!			Default Schedule for Sample Criti...	R1S5-VM3	11/12 02:00:04 AM	11	Success		□
ⓘ	!			Default Schedule for Sample Criti...	R1S5-VM3	11/11 11:19:34 AM	11	Success		□

Figure 187

EventTracker opens the Scheduled page.



Change Audit

🏠 / Dashboard / Change Audit / Change Policies

Title:

Policy Name: Sample Critical File Policy

Search system(s) ⓘ

Systems

⊞ □ EventTracker

⊞ □ TOONS

Start from: 11/13/2017 07:20:08 PM

Frequency: Daily Week Day: Sunday

Figure 188

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 opens 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 Weekday drop-down list only when you select the Weekly option from the Frequency drop-down list.

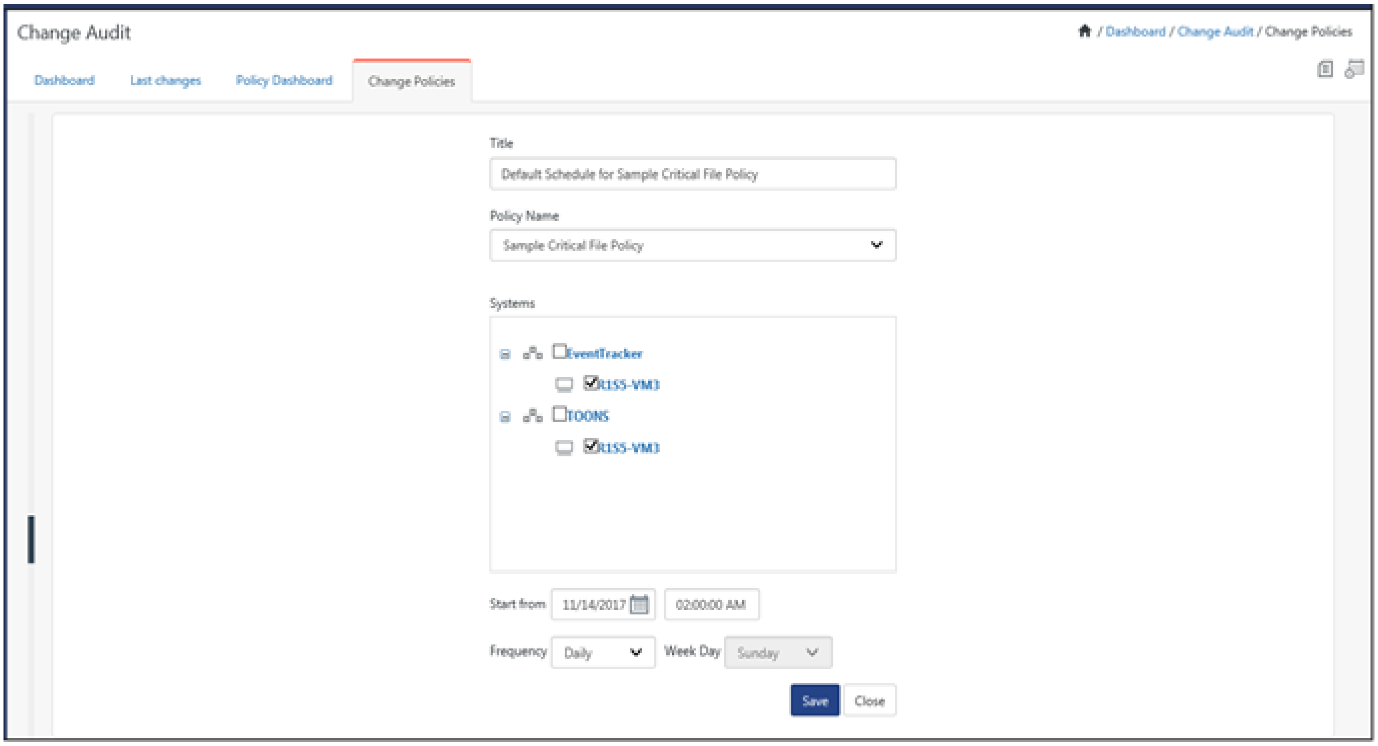
7 Click **Save**.

2.20.1 Editing Change Assessment Schedules

This option helps you edit Change Assessment schedules.

1 To Edit Change Assessment schedules, select a scheduled policy by clicking the scheduled reports icon .

2 Select the policy and click on **Edit** .



Change Audit

Title: Default Schedule for Sample Critical File Policy

Policy Name: Sample Critical File Policy

Systems

- ☐ EventTracker
  - ☑ R155-VM3
- ☐ TOONS
  - ☑ R155-VM3

Start from: 11/14/2017 02:00:00 AM

Frequency: Daily Week Day: Sunday

Figure 189

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

2.20.2 Running Schedules on Demand

This option helps you run schedules on demand.

a. To run the schedules on demand, select a scheduled policy in the bottom pane, and then select **Run Now**.

EventTracker opens the message box with appropriate message.

2.20.3 Deleting Scheduled policies

This option helps to delete schedules.

a) To delete a scheduled policy, select any scheduled policy in the bottom pane, and then select **Delete**.

EventTracker displays the confirmation message box.

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

2.21 Compliance Dashboard

The Compliance dashboard will display data related to the PCI DSS and NIST 800 171 Compliance by default.

Select the **Dashboard** icon and select **Compliance** from the dropdown list.

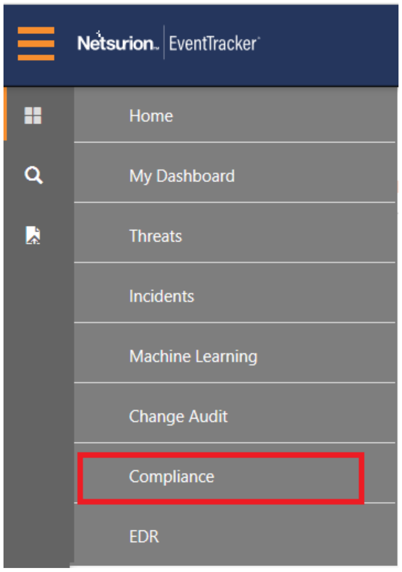
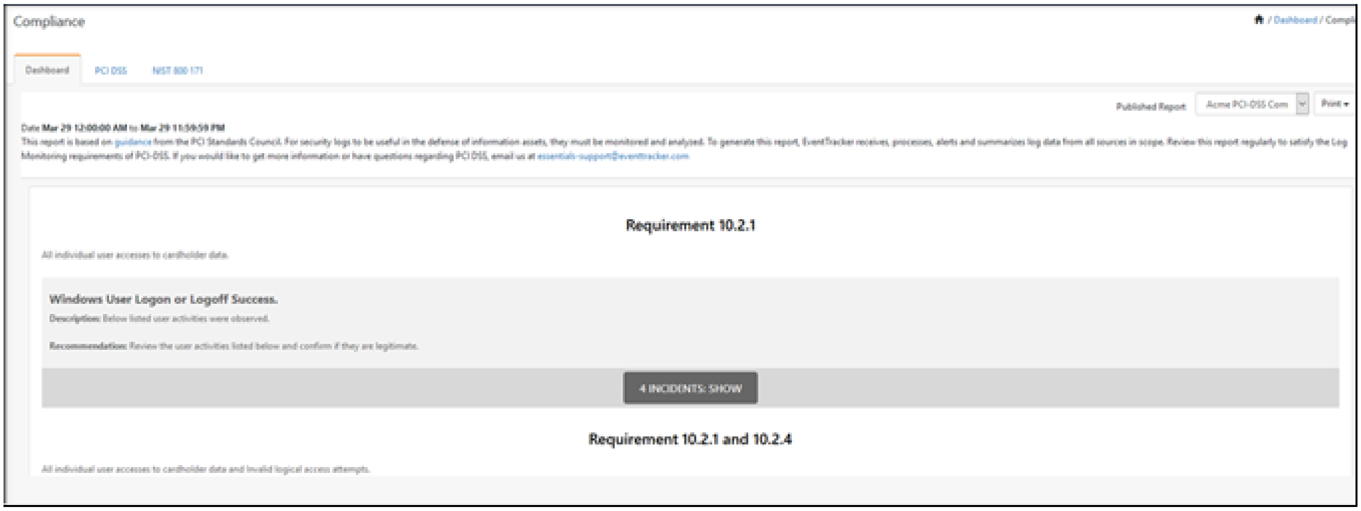


Figure 190

The Compliance Dashboard gets displayed with the available data.

From v9.1, the user will be able to view compliance summary reports details under the Dashboard tab. If the user has configured compliance summary report, then only the below screen will be displayed:



Compliance

🏠 / Dashboard / Compl

Dashboard PCI DSS NIST 800 171

Published Report Acme PCI-DSS Com Print ▾

Date **Mar 29 12:00:00 AM** to **Mar 29 11:59:59 PM**
This report is based on guidance from the PCI Standards Council. For security logs to be useful in the defense of information assets, they must be monitored and analyzed. To generate this report, EventTracker receives, processes, alerts and summarizes log data from all sources in scope. Review this report regularly to satisfy the Log Monitoring requirements of PCI-DSS. If you would like to get more information or have questions regarding PCI DSS, email us at essentials-support@eventtracker.com

Requirement 10.2.1

All individual user accesses to cardholder data.

Windows User Logon or Logoff Success.
Description: Below listed user activities were observed.

Recommendation: Review the user activities listed below and confirm if they are legitimate.

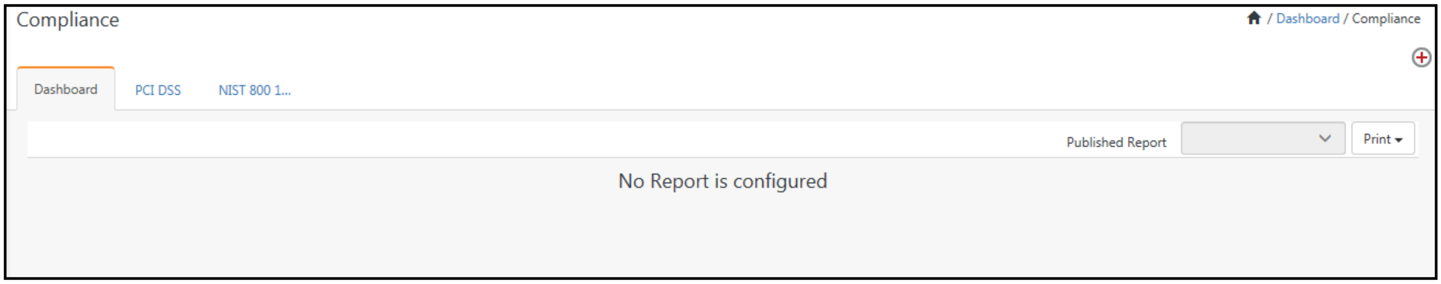
4 INCIDENTS: SHOW

Requirement 10.2.1 and 10.2.4

All individual user accesses to cardholder data and Invalid logical access attempts.

Figure 191

If no Compliance summary report is configured, the Dashboard will be displayed as shown below:



Compliance

🏠 / Dashboard / Compliance

⊕

Dashboard PCI DSS NIST 800 1...

Published Report [ ] Print ▾

No Report is configured

Figure 192

You also have Default Dashboards for PCI-DSS and NIST 800 171 in the respective tabs.

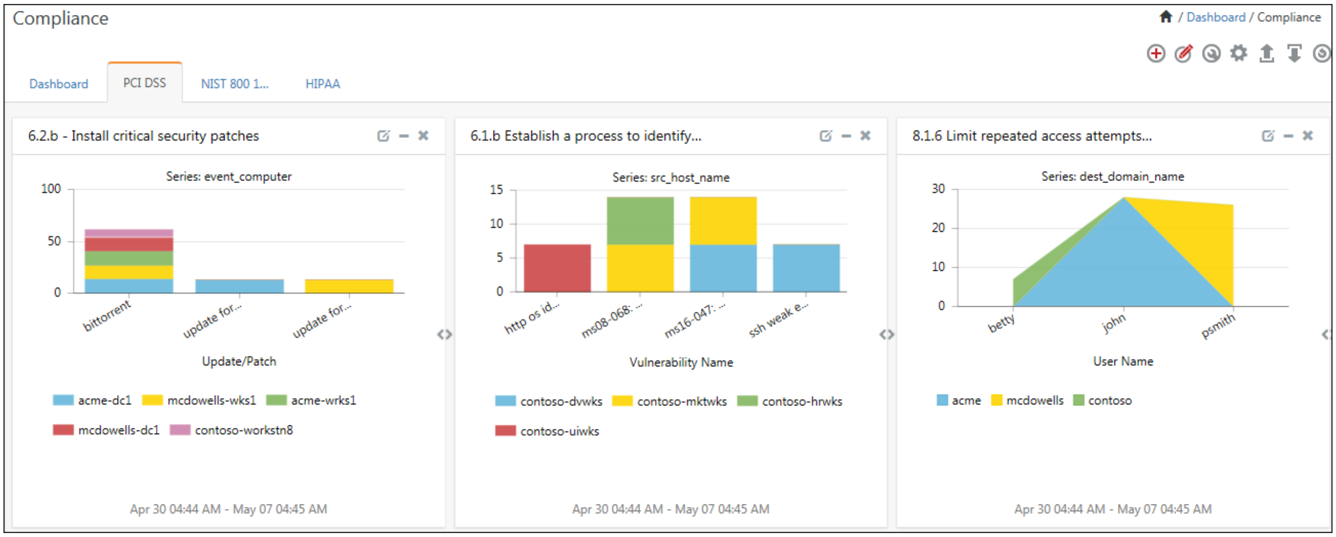


Figure 193

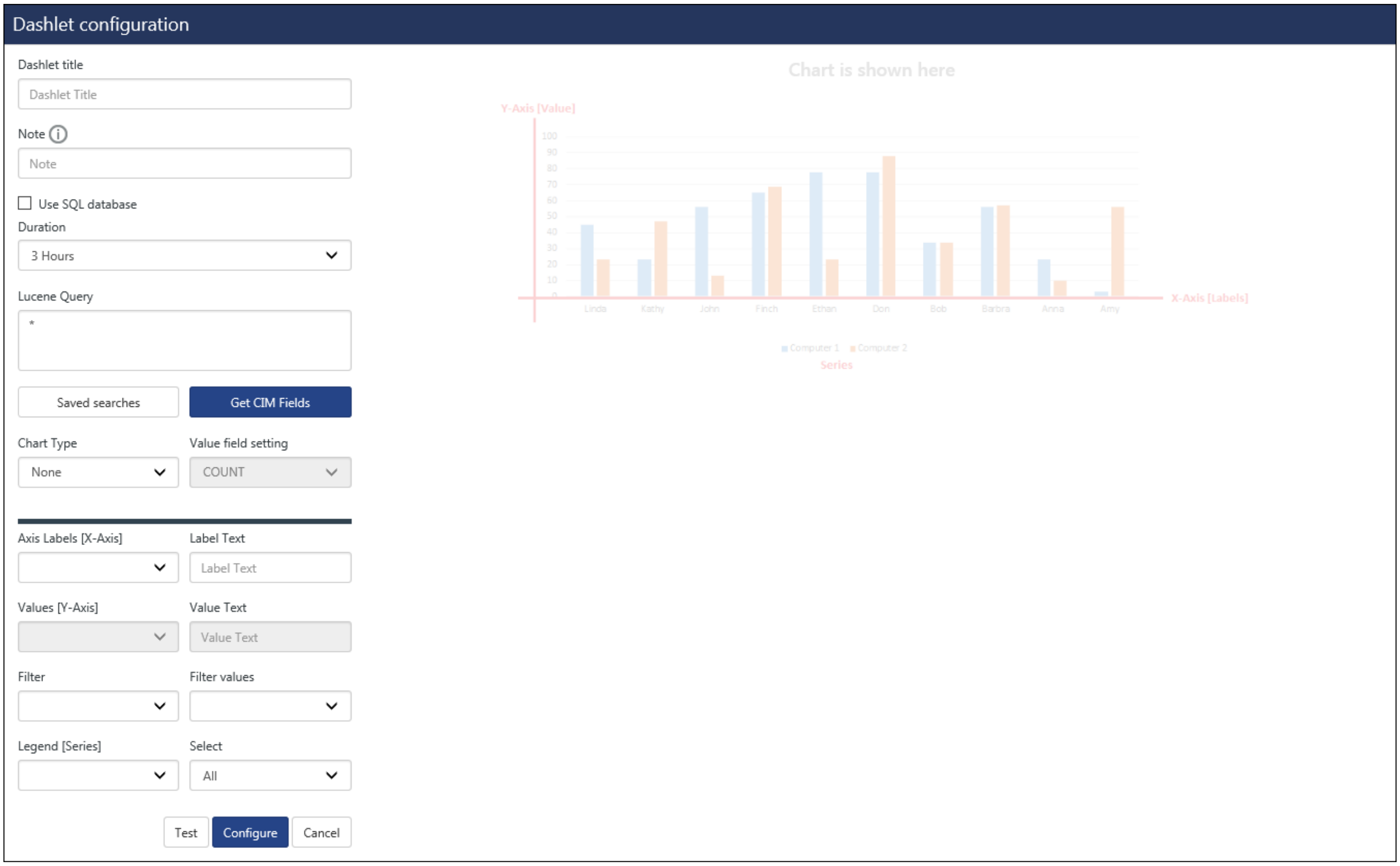
2.21.1 Creating a Dashboard

To create a Dashboard, click the ⊕ icon. Enter a Title and description, if required.

The Dashboard gets created.

Click	To
✎	Edit Dashboard
🔧	Customize Dashlet
⚙	Configure Dashlet
⤒	Export details
⤓	Import details
↺	Reset configuration

To configure a dashlet, click Gear ⚙ .



Dashlet configuration

Dashlet title: Dashlet Title

Note ⓘ: Note

☐ Use SQL database

Duration: 3 Hours

Lucene Query: *

Chart Type: None

Value field setting: COUNT

Axis Labels [X-Axis]:

Label Text: Label Text

Values [Y-Axis]:

Value Text: Value Text

Filter:

Filter values:

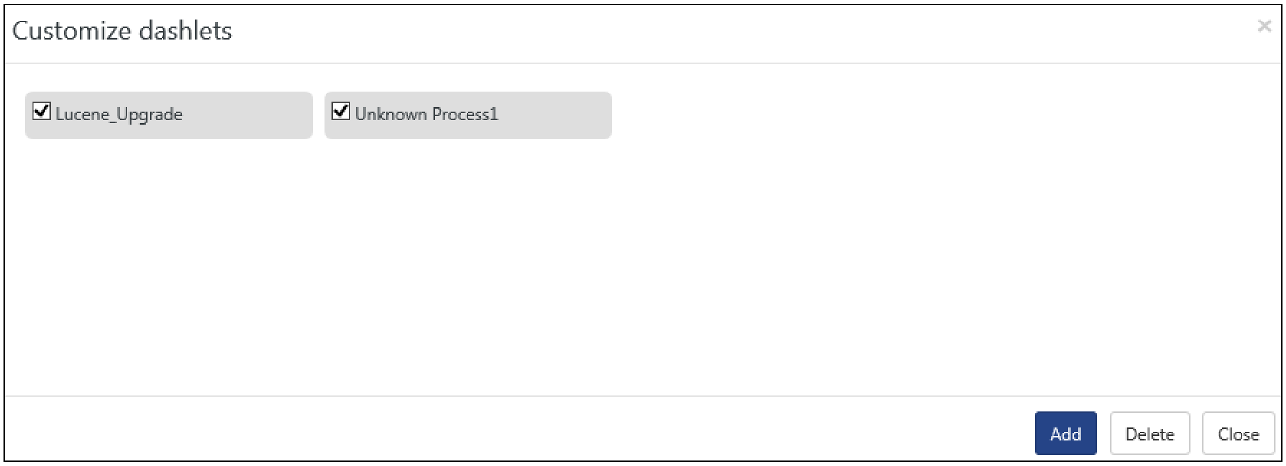
Legend [Series]:

Select: All

Figure 194

For more information to configure a dashlet, refer: Configure a Dashlet

To customize a dashlet, click **customize** .



Customize dashlets

☑ Lucene_Upgrade

☑ Unknown Process1

Figure 195

Click **Add**. The dashlets gets added in the created dashboard.

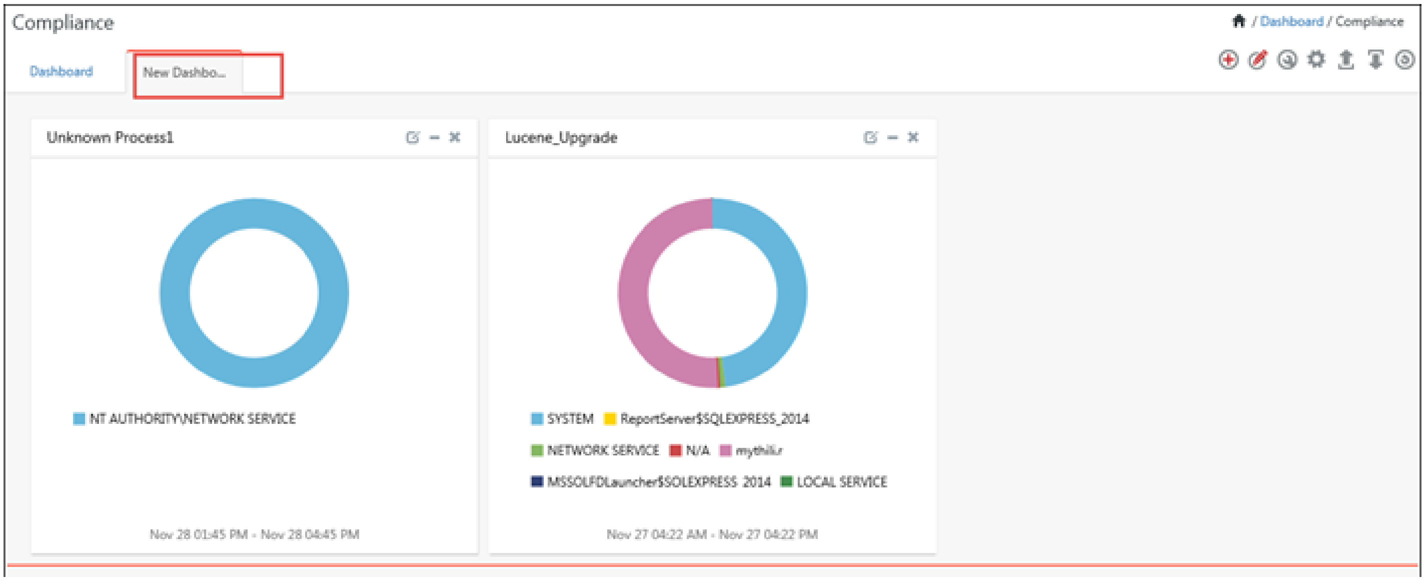
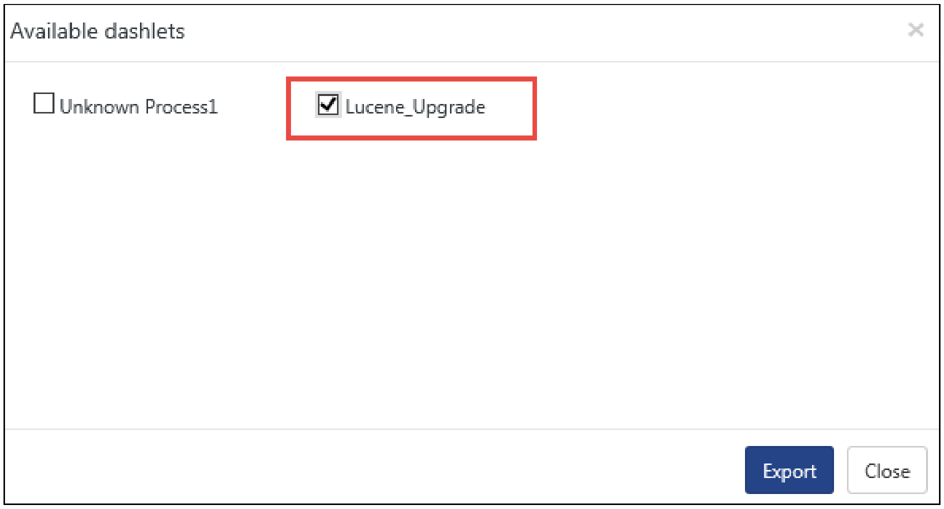

Compliance
/ Dashboard / Compliance
Dashboard
New Dashbo...
Unknown Process1
NT AUTHORITY\NETWORK SERVICE
Nov 28 01:45 PM - Nov 28 04:45 PM
Lucene_Upgrade
SYSTEM
ReportServer$SQLEXPRESS_2014
NETWORK SERVICE
N/A
mythili.r
MSSOLFDLauncher$SOLEXPRESS 2014
LOCAL SERVICE
Nov 27 04:22 AM - Nov 27 04:22 PM

Figure 196

To export the configuration, click Export . Select the dashlets and click **Export**.



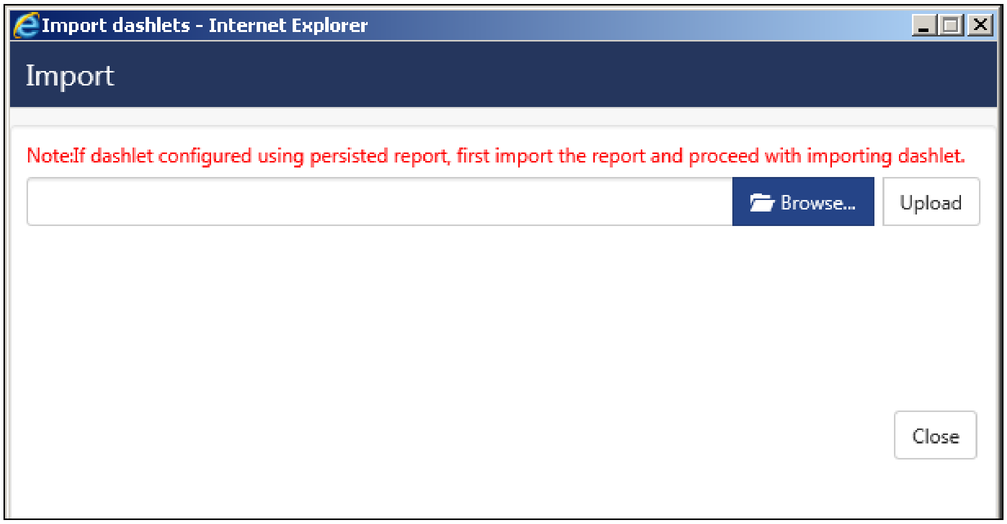
Available dashlets

☐ Unknown Process1

☑ Lucene_Upgrade

Figure 197

To import configuration, click import .



Note:If dashlet configured using persisted report, first import the report and proceed with importing dashlet.

Figure 198

Two more tabs have been provided for "PCI-DSS" and "NIST 800-171" in the Compliance Dashboard. The tabs will display the respective compliance reports.

PCI-DSS	NIST 800-171
PCI DSS - 10.2.3 Access to all audit trails	NIST 800-171 - 3.1.7 Prevent non-privileged users from executing privileged functions and audit the execution of such functions
PCI DSS - 10.2.5.a Verify use of identification and authentication mechanisms is logged	NIST 800-171 - 3.1.8 Limit unsuccessful logon attempts
PCI DSS - 10.2.5.b Verify all elevation of privileges is logged	NIST 800-171 - 3.11.2 Scan for vulnerabilities in the information system and applications periodically
PCI DSS - 10.2.6 Initialization, stopping, or pausing of the audit logs	NIST 800-171 - 3.3.8 Protect audit information and audit tools from unauthorized access
PCI DSS - 6.1.b Establish a process to identify security vulnerabilities	NIST 800-171 - 3.4.9 Control and monitor user-installed software
PCI DSS - 6.2.b Install critical security patches	NIST 800-171 - 3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and nonprivileged accounts
PCI DSS - 8.1.6 Limit repeated access attempts by locking out the user	

3. Search

In this chapter, you will learn about:

- Basic Search
- Advanced Search

3.1 Searching 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**

The user can also perform a search using the Elastic search.

3.1.1 Basic search

For basic search, select from the saved searches available or enter a lucene query to perform a basic search. The left pane will list the trending items (if any).

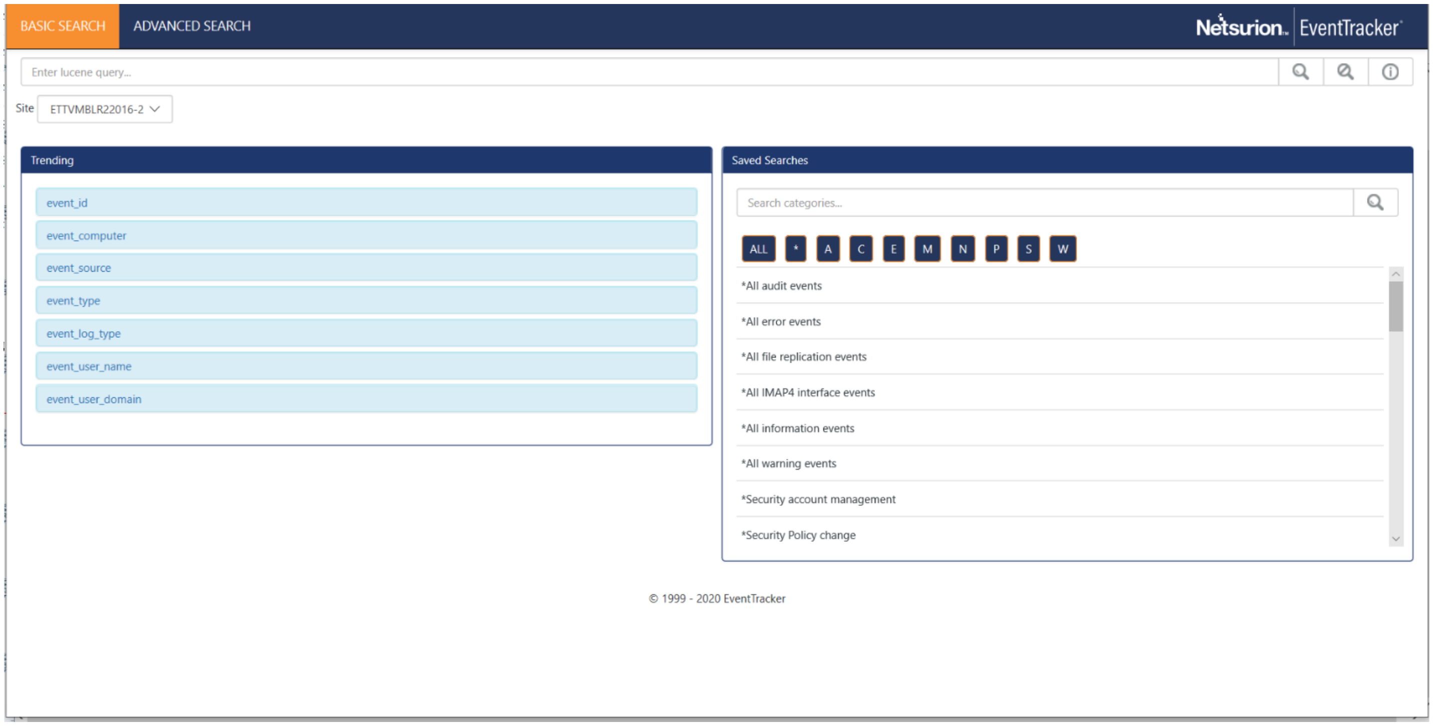
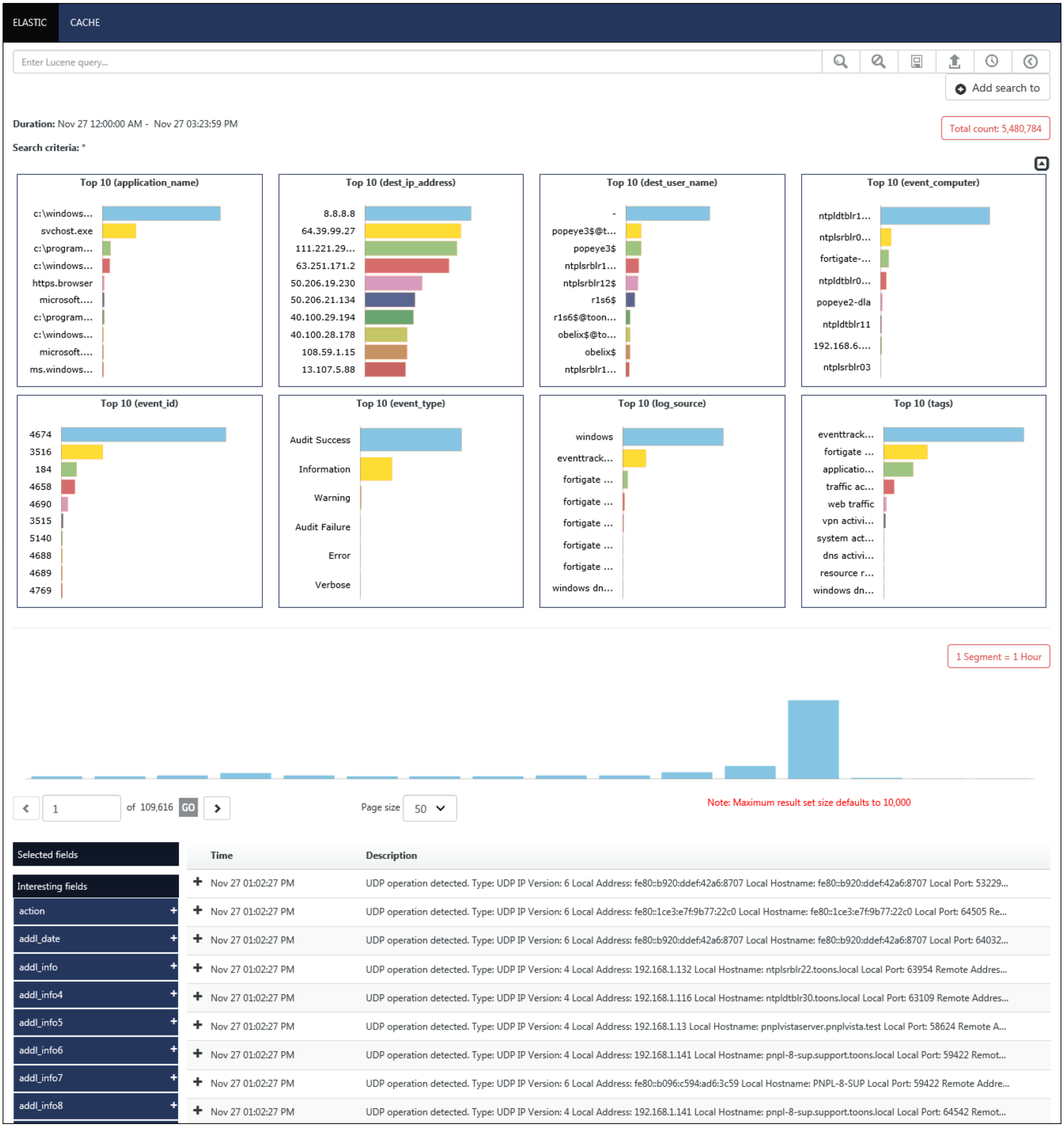


Figure 199

1. Select any of the items (e.g.: User: network service) for performing basic search from the Trending today pane.
2. For, performing a search on the logs processed on the current day, click the **logs processed today** hyperlink to view all logs processed since 12:00 A.M till current time.



Duration: Nov 27 12:00:00 AM - Nov 27 03:23:59 PM

Search criteria: *

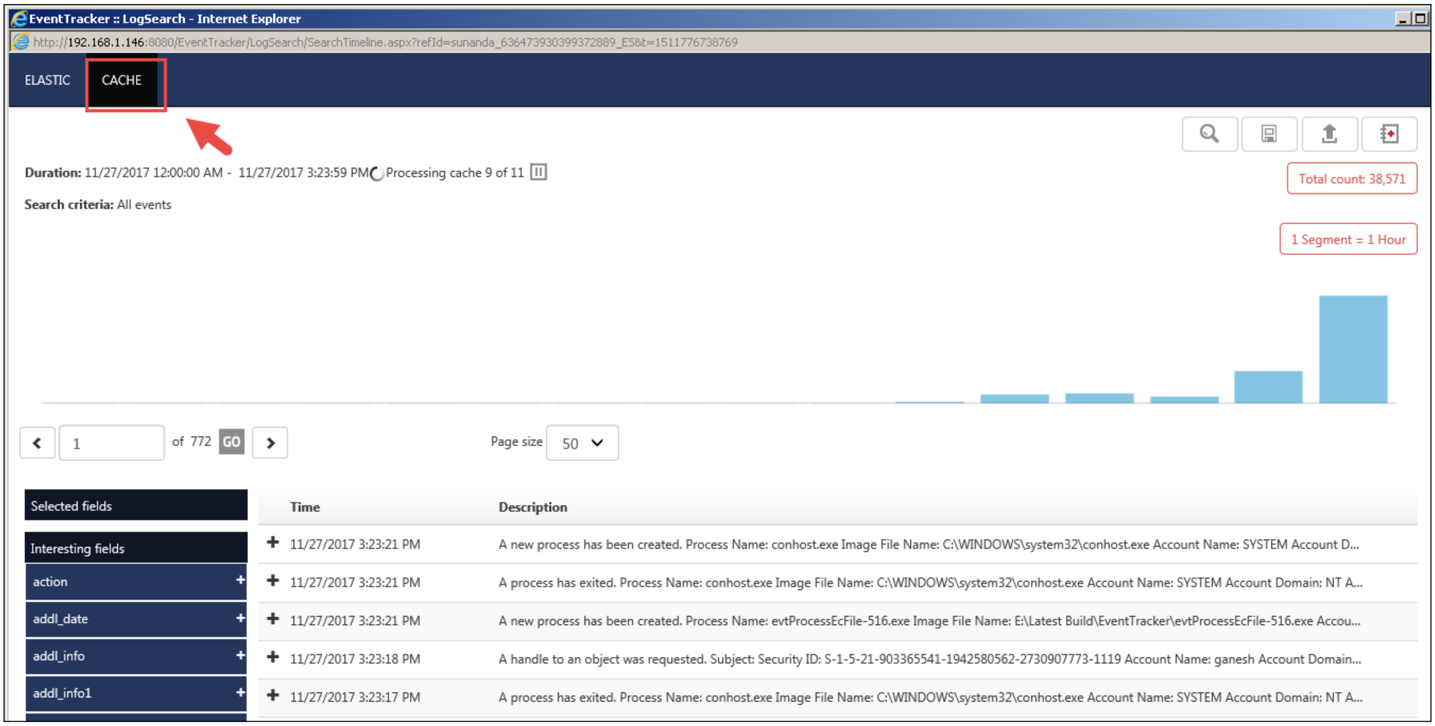
Total count: 5,480,784

1 of 109,616

Note: Maximum result set size defaults to 10,000

Time	Description
Nov 27 01:02:27 PM	UDP operation detected. Type: UDP IP Version: 6 Local Address: fe80::b920:ddef:42a6:8707 Local Hostname: fe80::b920:ddef:42a6:8707 Local Port: 53229...
Nov 27 01:02:27 PM	UDP operation detected. Type: UDP IP Version: 6 Local Address: fe80::1ce3:e7f:9b77:22c0 Local Hostname: fe80::1ce3:e7f:9b77:22c0 Local Port: 64505 Re...
Nov 27 01:02:27 PM	UDP operation detected. Type: UDP IP Version: 6 Local Address: fe80::b920:ddef:42a6:8707 Local Hostname: fe80::b920:ddef:42a6:8707 Local Port: 64032...
Nov 27 01:02:27 PM	UDP operation detected. Type: UDP IP Version: 4 Local Address: 192.168.1.132 Local Hostname: ntplsrblr22.toons.local Local Port: 63954 Remote Addres...
Nov 27 01:02:27 PM	UDP operation detected. Type: UDP IP Version: 4 Local Address: 192.168.1.116 Local Hostname: ntpldtblr30.toons.local Local Port: 63109 Remote Addres...
Nov 27 01:02:27 PM	UDP operation detected. Type: UDP IP Version: 4 Local Address: 192.168.1.13 Local Hostname: pnplvistaserver.pnplvista.test Local Port: 58624 Remote A...
Nov 27 01:02:27 PM	UDP operation detected. Type: UDP IP Version: 4 Local Address: 192.168.1.141 Local Hostname: pnpl-8-sup.support.toons.local Local Port: 59422 Remot...
Nov 27 01:02:27 PM	UDP operation detected. Type: UDP IP Version: 6 Local Address: fe80::b096:c594:ad6:3c59 Local Hostname: PNPL-8-SUP Local Port: 59422 Remote Addre...
Nov 27 01:02:27 PM	UDP operation detected. Type: UDP IP Version: 4 Local Address: 192.168.1.141 Local Hostname: pnpl-8-sup.support.toons.local Local Port: 64542 Remot...

Figure 200


EventTracker :: LogSearch - Internet Explorer
http://192.168.1.146:8080/EventTracker/LogSearch/SearchTimeline.aspx?refId=sunanda_636473930399372889_ES&t=1511776738769
ELASTIC
CACHE
Total count: 38,571
1 Segment = 1 Hour
of 772
GO
Page size
50
Selected fields
Interesting fields
action
addl_date
addl_info
addl_info1

Duration: 11/27/2017 12:00:00 AM - 11/27/2017 3:23:59 PM Processing cache 9 of 11

Search criteria: All events

Time	Description
11/27/2017 3:23:21 PM	A new process has been created. Process Name: conhost.exe Image File Name: C:\WINDOWS\system32\conhost.exe Account Name: SYSTEM Account D...
11/27/2017 3:23:21 PM	A process has exited. Process Name: conhost.exe Image File Name: C:\WINDOWS\system32\conhost.exe Account Name: SYSTEM Account Domain: NT A...
11/27/2017 3:23:21 PM	A new process has been created. Process Name: evtProcessEcFile-516.exe Image File Name: E:\Latest Build\EventTracker\evtProcessEcFile-516.exe Accou...
11/27/2017 3:23:18 PM	A handle to an object was requested. Subject: Security ID: S-1-5-21-903365541-1942580562-2730907773-1119 Account Name: ganesh Account Domain...
11/27/2017 3:23:17 PM	A process has exited. Process Name: conhost.exe Image File Name: C:\WINDOWS\system32\conhost.exe Account Name: SYSTEM Account Domain: NT A...

Figure 200

3.2 Searching from Elastic

3.2.1 Advanced Search

Note: To understand the usage of the new system selection interface introduced in feature update 9.3.3 as part of update ET93U20-031, please refer to New System Selection Interface User Guide.

Here the search result is performed using the Elastic Search. The user can write a lucene query for searching or can select from the fields available in the "**Search In**" box.

For example, if the user wants to search for event source and event id and filter event computer. They can either write a lucene query such as: "**event_source:(*EVENTTRACKER*) AND event_id:(3240 || 2040 || 2037) AND NOT event_computer:(*-DLA)**" to perform a search.

The user can choose the **duration** and can also select from the **system tree** in the left pane.

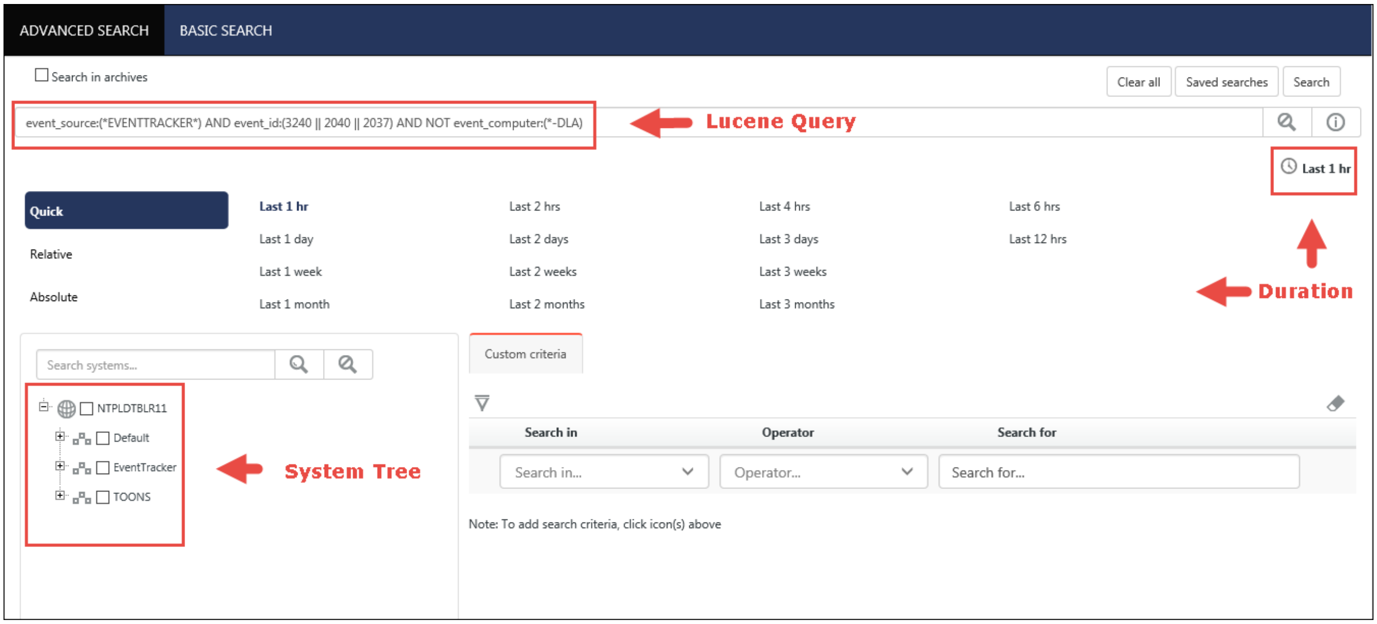
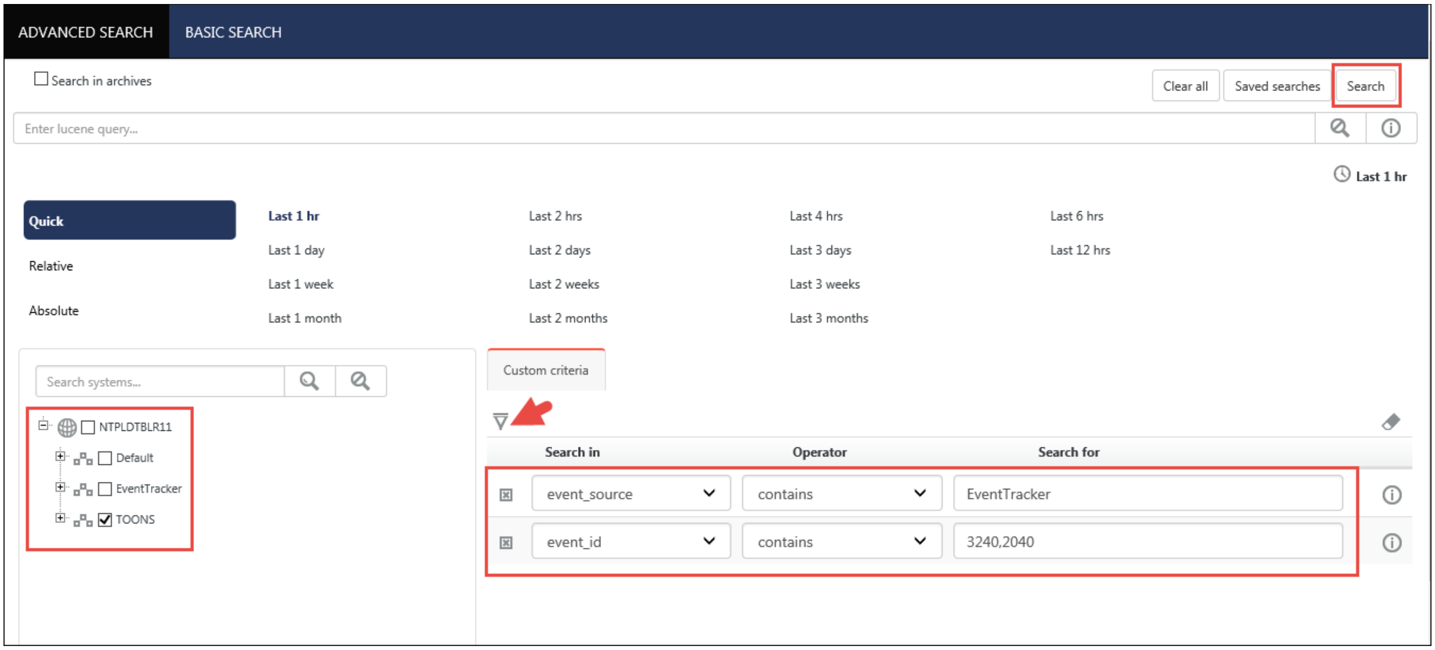


Figure 201

Click **Search**.

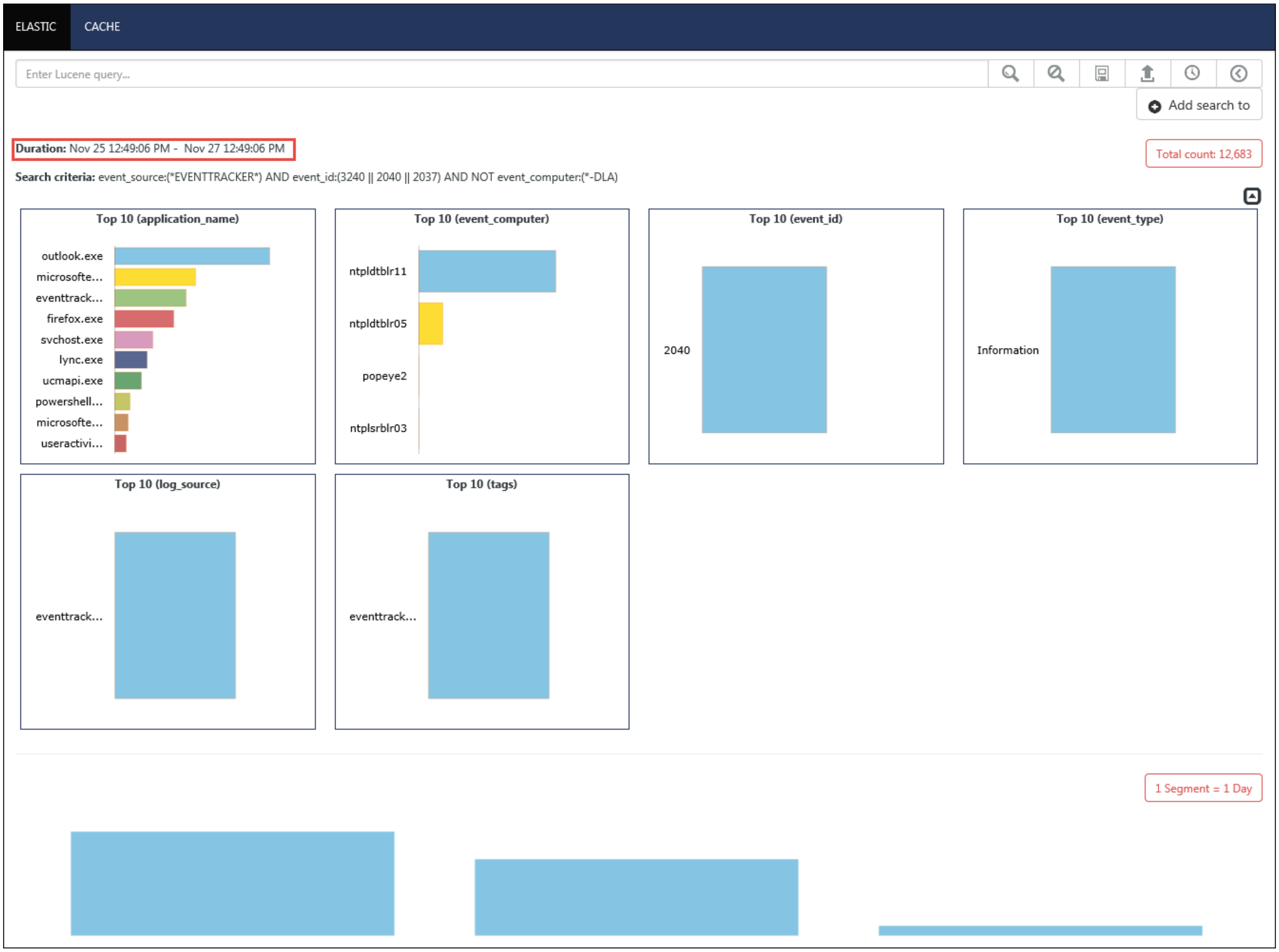
OR, they can even select from the dropdown option in the **Search In** field. Select the Add Search criteria icon ⊽. Select from the available option and create the search criteria.



Search in	Operator	Search for
event_source	contains	EventTracker
event_id	contains	3240,2040

Figure 202

It will display the total count in a graph format in the top pane and the search results displaying with the interesting fields in the bottom pane.



Duration: Nov 25 12:49:06 PM - Nov 27 12:49:06 PM

Total count: 12,683

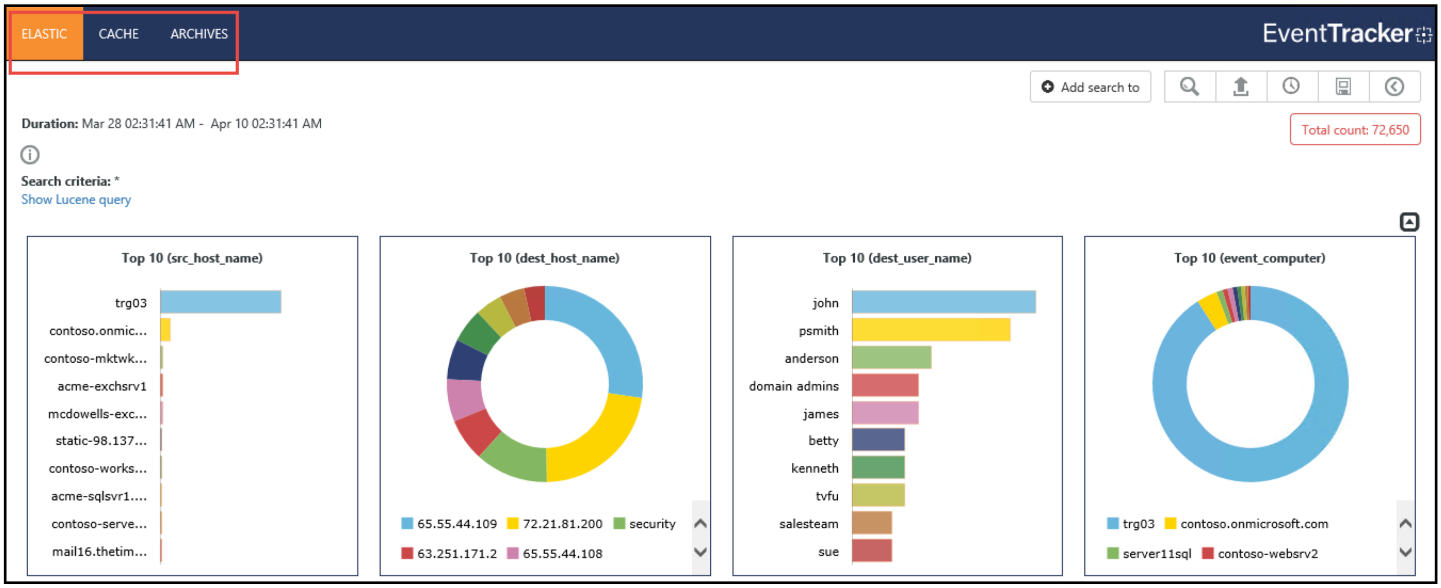
Search criteria: event_source:(*EVENTTRACKER*) AND event_id:(3240 || 2040 || 2037) AND NOT event_computer:(*-DLA)

Figure 203

3.3 Three tabs - Elastic, Cache and Archives in Log search result window

When log volume is more, and the data is not indexed in the selected duration, the 3 tabs in search helps to show the entire data without any miss.

For example: Suppose the elastic purge is set to 7 days and if user try to do elastic search for last 2 weeks data, then 1-week data will be shown Elastic tab, the mdb’s which are available in cache folder and are not indexed cabs data will be shown in the Cache tab and second week cabs data will be shown in Archives tab.

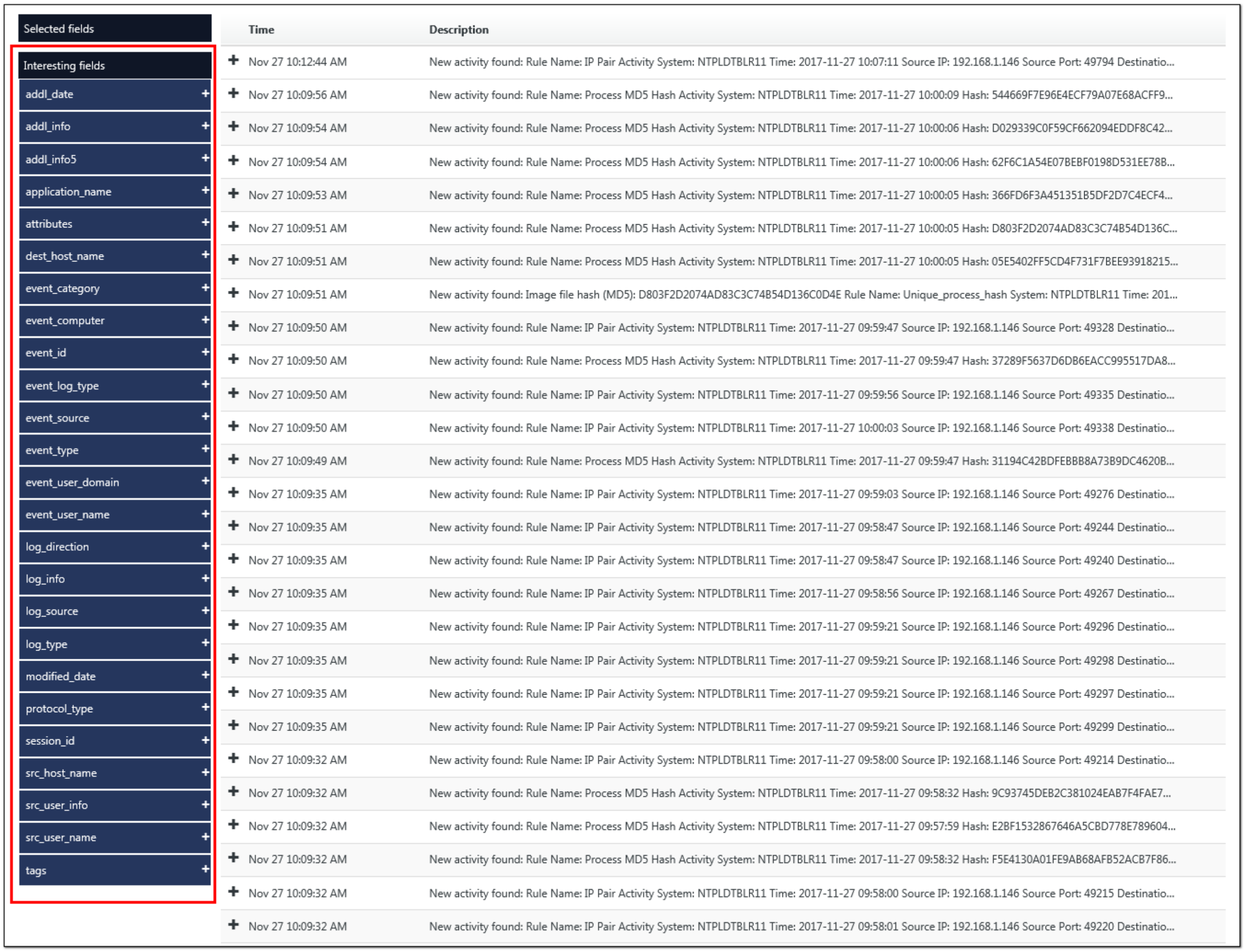


Duration: Mar 28 02:31:41 AM - Apr 10 02:31:41 AM

Search criteria: *

Figure 204

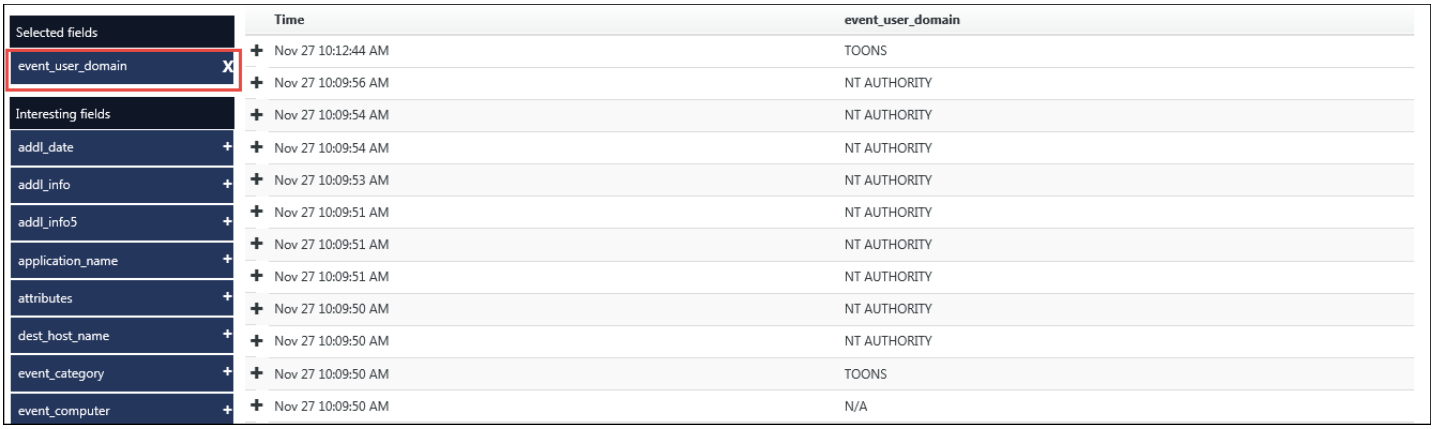
Click	To
🔍	Search
🔍	Clear Search
💾	Save the search results
⬆	Export the results
🕒	Refine on Time duration
◀	Go back to Advanced search



Time	Description
Nov 27 10:12:44 AM	New activity found: Rule Name: IP Pair Activity System: NTPLDTBLR11 Time: 2017-11-27 10:07:11 Source IP: 192.168.1.146 Source Port: 49794 Destinatio...
Nov 27 10:09:56 AM	New activity found: Rule Name: Process MD5 Hash Activity System: NTPLDTBLR11 Time: 2017-11-27 10:00:09 Hash: 544669F7E96E4ECF79A07E68ACFF9...
Nov 27 10:09:54 AM	New activity found: Rule Name: Process MD5 Hash Activity System: NTPLDTBLR11 Time: 2017-11-27 10:00:06 Hash: D029339C0F59CF662094EDDF8C42...
Nov 27 10:09:54 AM	New activity found: Rule Name: Process MD5 Hash Activity System: NTPLDTBLR11 Time: 2017-11-27 10:00:06 Hash: 62F6C1A54E07BEBF0198D531EE78B...
Nov 27 10:09:53 AM	New activity found: Rule Name: Process MD5 Hash Activity System: NTPLDTBLR11 Time: 2017-11-27 10:00:05 Hash: 366FD6F3A451351B5DF2D7C4ECF4...
Nov 27 10:09:51 AM	New activity found: Rule Name: Process MD5 Hash Activity System: NTPLDTBLR11 Time: 2017-11-27 10:00:05 Hash: D803F2D2074AD83C3C74B54D136C...
Nov 27 10:09:51 AM	New activity found: Rule Name: Process MD5 Hash Activity System: NTPLDTBLR11 Time: 2017-11-27 10:00:05 Hash: 05E5402FF5CD4F731F7BEE93918215...
Nov 27 10:09:51 AM	New activity found: Image file hash (MD5): D803F2D2074AD83C3C74B54D136C0D4E Rule Name: Unique_process_hash System: NTPLDTBLR11 Time: 201...
Nov 27 10:09:50 AM	New activity found: Rule Name: IP Pair Activity System: NTPLDTBLR11 Time: 2017-11-27 09:59:47 Source IP: 192.168.1.146 Source Port: 49328 Destinatio...
Nov 27 10:09:50 AM	New activity found: Rule Name: Process MD5 Hash Activity System: NTPLDTBLR11 Time: 2017-11-27 09:59:47 Hash: 37289F5637D6DB6EACC995517DA8...
Nov 27 10:09:50 AM	New activity found: Rule Name: IP Pair Activity System: NTPLDTBLR11 Time: 2017-11-27 09:59:56 Source IP: 192.168.1.146 Source Port: 49335 Destinatio...
Nov 27 10:09:50 AM	New activity found: Rule Name: IP Pair Activity System: NTPLDTBLR11 Time: 2017-11-27 10:00:03 Source IP: 192.168.1.146 Source Port: 49338 Destinatio...
Nov 27 10:09:49 AM	New activity found: Rule Name: Process MD5 Hash Activity System: NTPLDTBLR11 Time: 2017-11-27 09:59:47 Hash: 31194C42BDFEBBB8A73B9DC4620B...
Nov 27 10:09:35 AM	New activity found: Rule Name: IP Pair Activity System: NTPLDTBLR11 Time: 2017-11-27 09:59:03 Source IP: 192.168.1.146 Source Port: 49276 Destinatio...
Nov 27 10:09:35 AM	New activity found: Rule Name: IP Pair Activity System: NTPLDTBLR11 Time: 2017-11-27 09:58:47 Source IP: 192.168.1.146 Source Port: 49244 Destinatio...
Nov 27 10:09:35 AM	New activity found: Rule Name: IP Pair Activity System: NTPLDTBLR11 Time: 2017-11-27 09:58:47 Source IP: 192.168.1.146 Source Port: 49240 Destinatio...
Nov 27 10:09:35 AM	New activity found: Rule Name: IP Pair Activity System: NTPLDTBLR11 Time: 2017-11-27 09:58:56 Source IP: 192.168.1.146 Source Port: 49267 Destinatio...
Nov 27 10:09:35 AM	New activity found: Rule Name: IP Pair Activity System: NTPLDTBLR11 Time: 2017-11-27 09:59:21 Source IP: 192.168.1.146 Source Port: 49296 Destinatio...
Nov 27 10:09:35 AM	New activity found: Rule Name: IP Pair Activity System: NTPLDTBLR11 Time: 2017-11-27 09:59:21 Source IP: 192.168.1.146 Source Port: 49298 Destinatio...
Nov 27 10:09:35 AM	New activity found: Rule Name: IP Pair Activity System: NTPLDTBLR11 Time: 2017-11-27 09:59:21 Source IP: 192.168.1.146 Source Port: 49297 Destinatio...
Nov 27 10:09:35 AM	New activity found: Rule Name: IP Pair Activity System: NTPLDTBLR11 Time: 2017-11-27 09:59:21 Source IP: 192.168.1.146 Source Port: 49299 Destinatio...
Nov 27 10:09:32 AM	New activity found: Rule Name: IP Pair Activity System: NTPLDTBLR11 Time: 2017-11-27 09:58:00 Source IP: 192.168.1.146 Source Port: 49214 Destinatio...
Nov 27 10:09:32 AM	New activity found: Rule Name: Process MD5 Hash Activity System: NTPLDTBLR11 Time: 2017-11-27 09:58:32 Hash: 9C93745DEB2C381024EAB7F4FAE7...
Nov 27 10:09:32 AM	New activity found: Rule Name: Process MD5 Hash Activity System: NTPLDTBLR11 Time: 2017-11-27 09:57:59 Hash: E2BF1532867646A5CBD778E789604...
Nov 27 10:09:32 AM	New activity found: Rule Name: Process MD5 Hash Activity System: NTPLDTBLR11 Time: 2017-11-27 09:58:32 Hash: F5E4130A01FE9AB68AFB52ACB7F86...
Nov 27 10:09:32 AM	New activity found: Rule Name: IP Pair Activity System: NTPLDTBLR11 Time: 2017-11-27 09:58:00 Source IP: 192.168.1.146 Source Port: 49215 Destinatio...
Nov 27 10:09:32 AM	New activity found: Rule Name: IP Pair Activity System: NTPLDTBLR11 Time: 2017-11-27 09:58:01 Source IP: 192.168.1.146 Source Port: 49220 Destinatio...

Figure 205

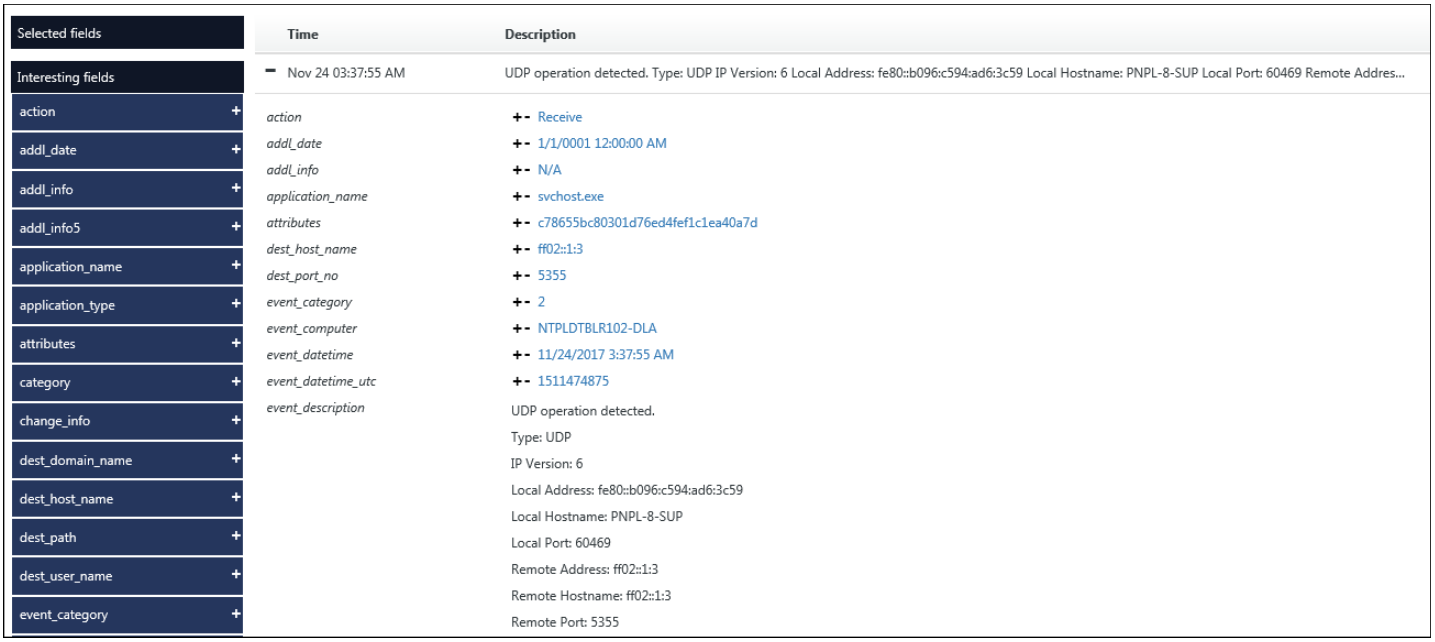
To add the interesting fields and get the results based on it, click the ➕ icon for the respective field.



Time	event_user_domain
Nov 27 10:12:44 AM	TOONS
Nov 27 10:09:56 AM	NT AUTHORITY
Nov 27 10:09:54 AM	NT AUTHORITY
Nov 27 10:09:54 AM	NT AUTHORITY
Nov 27 10:09:53 AM	NT AUTHORITY
Nov 27 10:09:51 AM	NT AUTHORITY
Nov 27 10:09:51 AM	NT AUTHORITY
Nov 27 10:09:51 AM	NT AUTHORITY
Nov 27 10:09:50 AM	NT AUTHORITY
Nov 27 10:09:50 AM	NT AUTHORITY
Nov 27 10:09:50 AM	TOONS
Nov 27 10:09:50 AM	N/A

Figure 206

To get detail related to a search entity, click **Expand**.



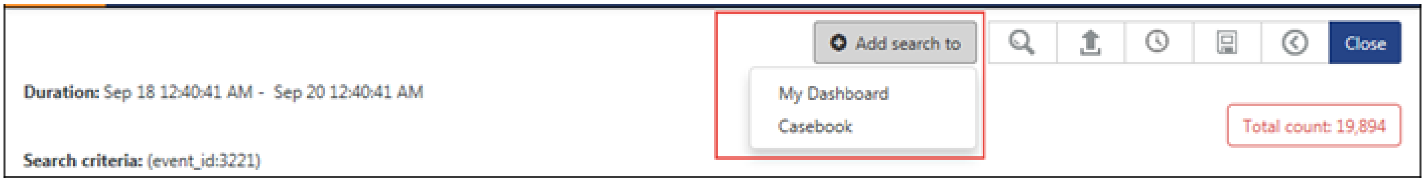
Time	Description
− Nov 24 03:37:55 AM	UDP operation detected. Type: UDP IP Version: 6 Local Address: fe80::b096:c594:ad6:3c59 Local Hostname: PNPL-8-SUP Local Port: 60469 Remote Addres...

action	+- Receive
addl_date	+- 1/1/0001 12:00:00 AM
addl_info	+- N/A
application_name	+- svchost.exe
attributes	+- c78655bc80301d76ed4fef1c1ea40a7d
dest_host_name	+- ff02::1:3
dest_port_no	+- 5355
event_category	+- 2
event_computer	+- NTPLDTBLR102-DLA
event_datetime	+- 11/24/2017 3:37:55 AM
event_datetime_utc	+- 1511474875
event_description	UDP operation detected. Type: UDP IP Version: 6 Local Address: fe80::b096:c594:ad6:3c59 Local Hostname: PNPL-8-SUP Local Port: 60469 Remote Address: ff02::1:3 Remote Hostname: ff02::1:3 Remote Port: 5355

Figure 207

3.3.1 Add Search to Dashboard/Casebook

To add the search results to Dashboard or casebook, click the "**Add search to**" option.



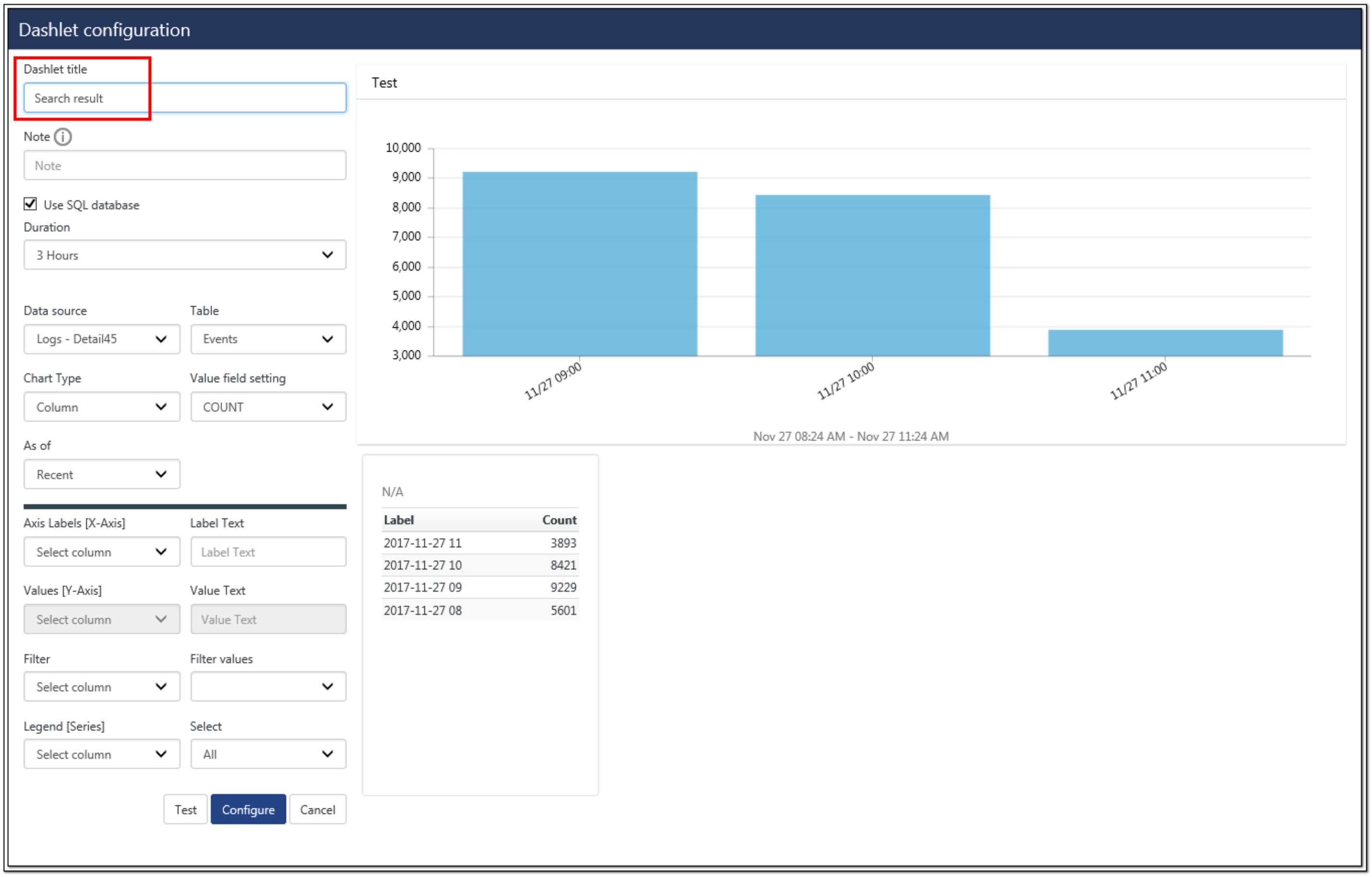
Duration: Sep 18 12:40:41 AM - Sep 20 12:40:41 AM

Search criteria: (event_id:3221)

Total count: 19,894

Figure 208

a. Select the **Dashboard** option and configure a dashlet for the same. An example is shown below:



Dashlet configuration

Dashlet title: Search result

Note: Note

☑ Use SQL database

Duration: 3 Hours

Data source: Logs - Detail45

Table: Events

Chart Type: Column

Value field setting: COUNT

As of: Recent

Axis Labels [X-Axis]: Select column

Label Text: Label Text

Values [Y-Axis]: Select column

Value Text: Value Text

Filter: Select column

Filter values:

Legend [Series]: Select column

Select: All

N/A

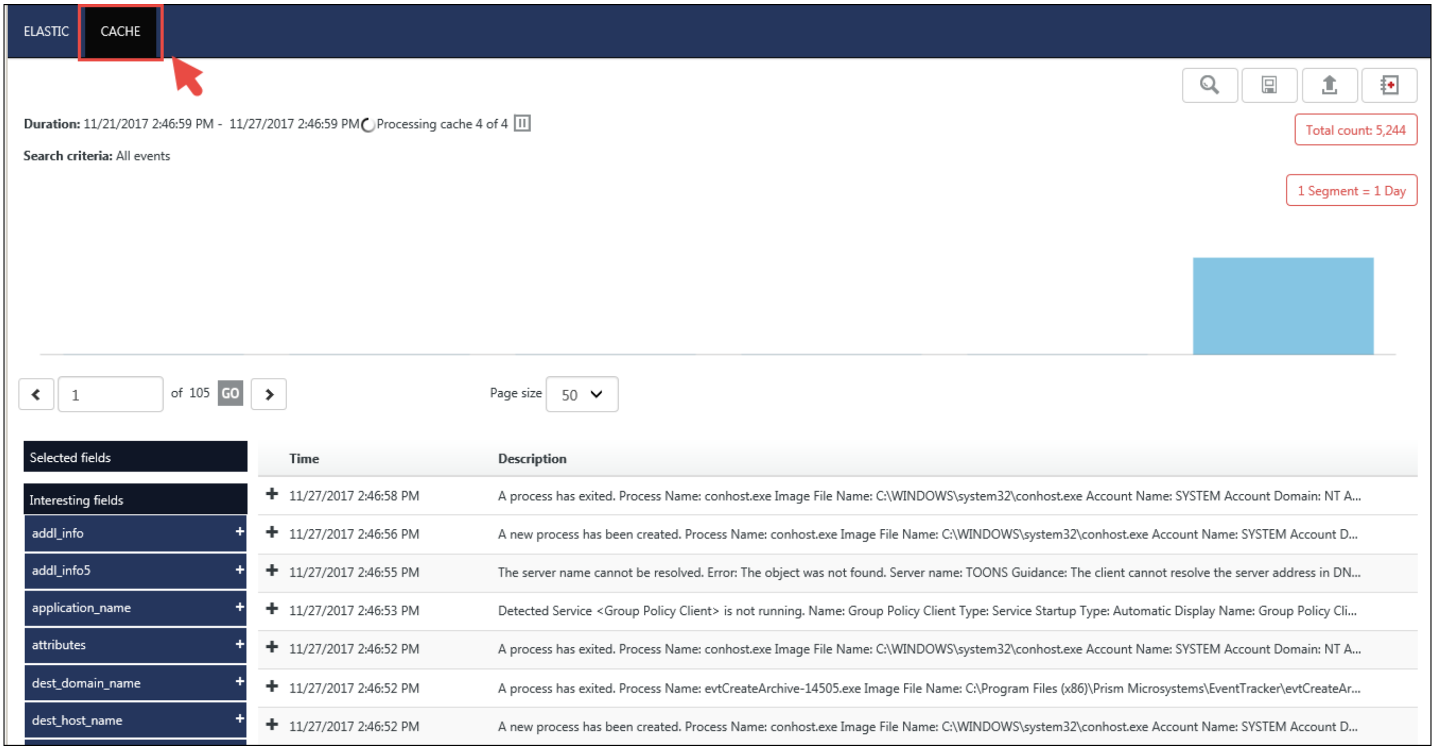
Label	Count
2017-11-27 11	3893
2017-11-27 10	8421
2017-11-27 09	9229
2017-11-27 08	5601

Figure 209

b. Select the **Casebook** option and add the result of new or existing casebook.

The user can also view the search results from the cache.

To do this, navigate to the **CACHE** tab and view the results.



Duration: 11/21/2017 2:46:59 PM - 11/27/2017 2:46:59 PM Processing cache 4 of 4

Search criteria: All events

Total count: 5,244

1 Segment = 1 Day

1 of 105 GO

Page size 50

Selected fields
Interesting fields
addl_info +
addl_info5 +
application_name +
attributes +
dest_domain_name +
dest_host_name +

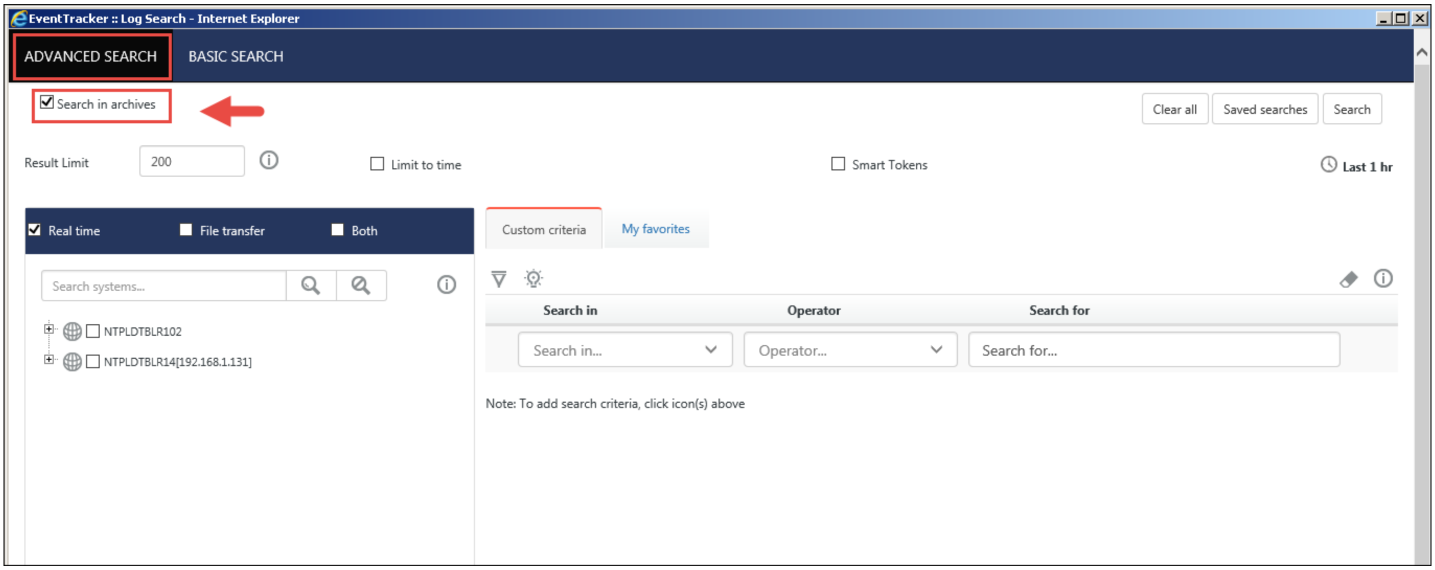
	Time	Description
+	11/27/2017 2:46:58 PM	A process has exited. Process Name: conhost.exe Image File Name: C:\WINDOWS\system32\conhost.exe Account Name: SYSTEM Account Domain: NT A...
+	11/27/2017 2:46:56 PM	A new process has been created. Process Name: conhost.exe Image File Name: C:\WINDOWS\system32\conhost.exe Account Name: SYSTEM Account D...
+	11/27/2017 2:46:55 PM	The server name cannot be resolved. Error: The object was not found. Server name: TOONS Guidance: The client cannot resolve the server address in DN...
+	11/27/2017 2:46:53 PM	Detected Service <Group Policy Client> is not running. Name: Group Policy Client Type: Service Startup Type: Automatic Display Name: Group Policy Cli...
+	11/27/2017 2:46:52 PM	A process has exited. Process Name: conhost.exe Image File Name: C:\WINDOWS\system32\conhost.exe Account Name: SYSTEM Account Domain: NT A...
+	11/27/2017 2:46:52 PM	A process has exited. Process Name: evtCreateArchive-14505.exe Image File Name: C:\Program Files (x86)\Prism Microsystems\EventTracker\evtCreateAr...
+	11/27/2017 2:46:52 PM	A new process has been created. Process Name: conhost.exe Image File Name: C:\WINDOWS\system32\conhost.exe Account Name: SYSTEM Account D...

Figure 210

3.4 Searching from Archives

3.4.1 Advanced Search

For advanced search from the cache, check the "**Search in Archives**" option.



☑ Search in archives

Result Limit 200

□ Limit to time

□ Smart Tokens

Last 1 hr

☑ Real time □ File transfer □ Both

Search systems...

□ NTPLDTBLR102

□ NTPLDTBLR14[192.168.1.131]

Search in... Operator... Search for...

Note: To add search criteria, click icon(s) above

Figure 211

Add Search criteria and **Save Search criteria** are some features that have been added and are explained below.

3.4.2 Adding Search Criteria

In Advanced Log search, you can search using regular expression.

1. Click **Add search criteria** ▽ .
2. In **Search in** drop down menu, select **EventID**.

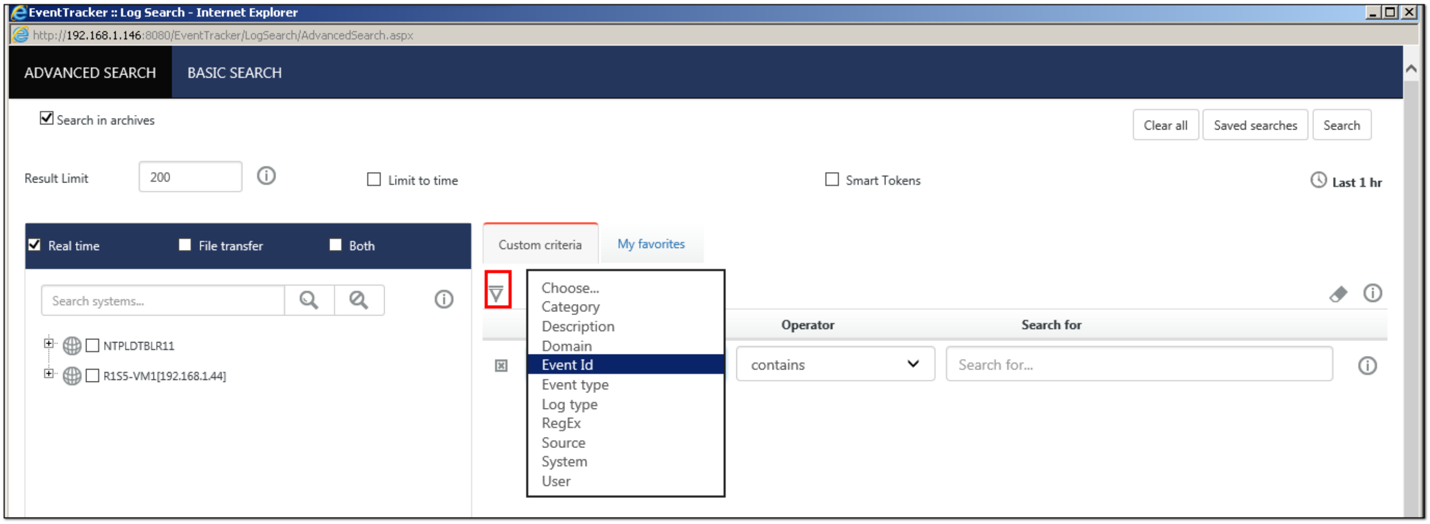


Figure 212

3. Select Operator drop down.

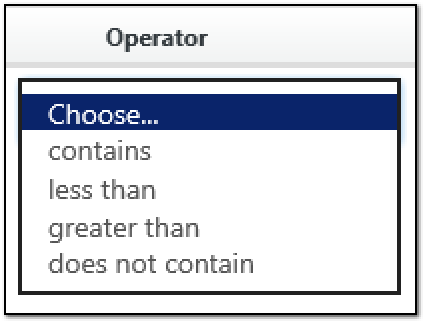
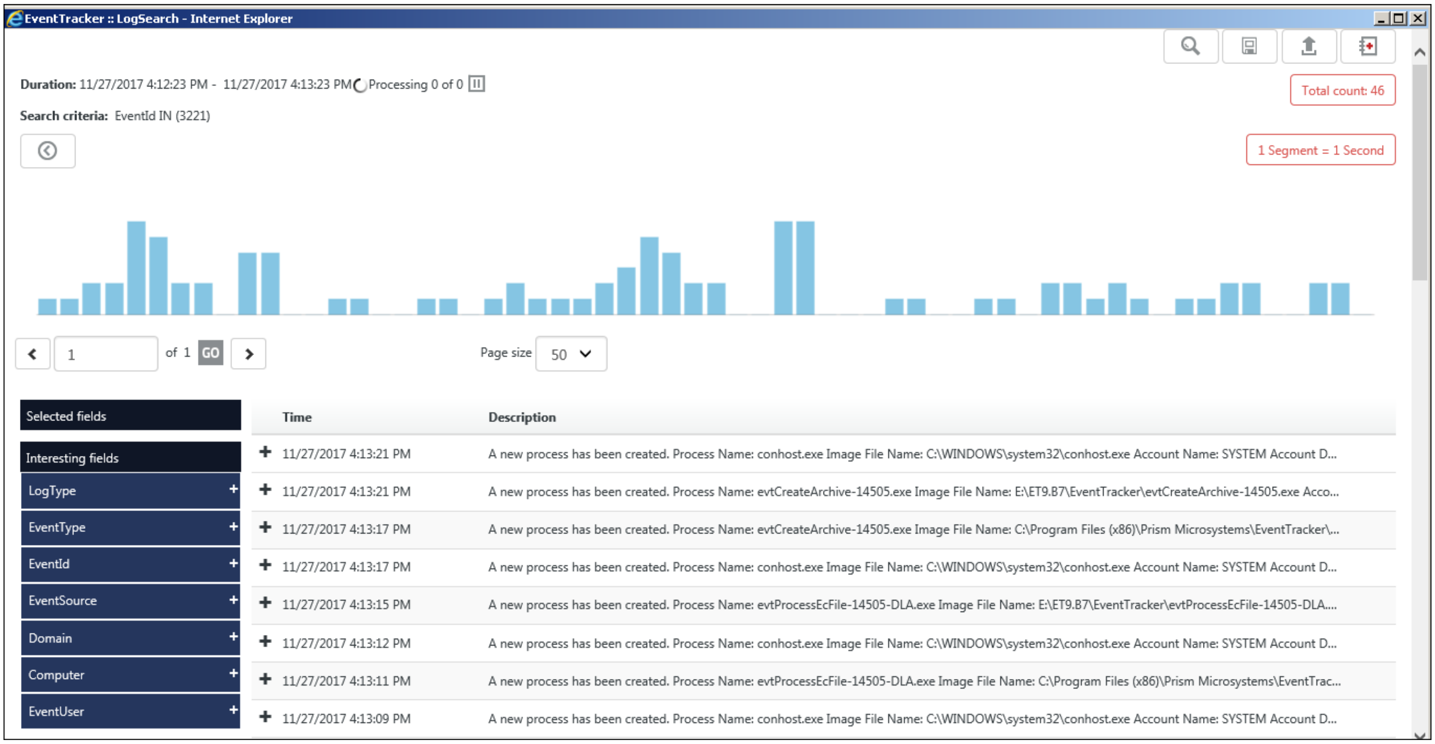


Figure 213

4. Enter search criteria in Search for box. (for e.g. : 3221)
5. Click Help ⓘ icon for additional information.
6. Click Search.



Duration: 11/27/2017 4:12:23 PM - 11/27/2017 4:13:23 PM Processing 0 of 0

Search criteria: EventId IN (3221)

Page size 50

	Time	Description
+	11/27/2017 4:13:21 PM	A new process has been created. Process Name: conhost.exe Image File Name: C:\WINDOWS\system32\conhost.exe Account Name: SYSTEM Account D...
+	11/27/2017 4:13:21 PM	A new process has been created. Process Name: evtCreateArchive-14505.exe Image File Name: E:\ET9.B7\EventTracker\evtCreateArchive-14505.exe Acco...
+	11/27/2017 4:13:17 PM	A new process has been created. Process Name: evtCreateArchive-14505.exe Image File Name: C:\Program Files (x86)\Prism Microsystems\EventTracker\...
+	11/27/2017 4:13:17 PM	A new process has been created. Process Name: conhost.exe Image File Name: C:\WINDOWS\system32\conhost.exe Account Name: SYSTEM Account D...
+	11/27/2017 4:13:15 PM	A new process has been created. Process Name: evtProcessEcFile-14505-DLA.exe Image File Name: E:\ET9.B7\EventTracker\evtProcessEcFile-14505-DLA....
+	11/27/2017 4:13:12 PM	A new process has been created. Process Name: conhost.exe Image File Name: C:\WINDOWS\system32\conhost.exe Account Name: SYSTEM Account D...
+	11/27/2017 4:13:11 PM	A new process has been created. Process Name: evtProcessEcFile-14505-DLA.exe Image File Name: C:\Program Files (x86)\Prism Microsystems\EventTrac...
+	11/27/2017 4:13:09 PM	A new process has been created. Process Name: conhost.exe Image File Name: C:\WINDOWS\system32\conhost.exe Account Name: SYSTEM Account D...

Figure 214

The standard properties will list in the left pane and the search result in the right. Expand the interested entity and view the details.

The user can further include or exclude the standard properties and perform a pivoting based on the search criteria.

3.5 Smart Tokens

Every Knowledge Object that is defined has finite Smart Tokens. From a visualization and analytical perspective, only a few or specific Smart Tokens will be important, which needs to be searched. The Smart Token feature will make the searching process hassle-free and will also help in performing a filtered search to get the detailed information on a specific token, when required.

The Smart Token option remains disabled by default. The user needs to enable the option to continue with the search.

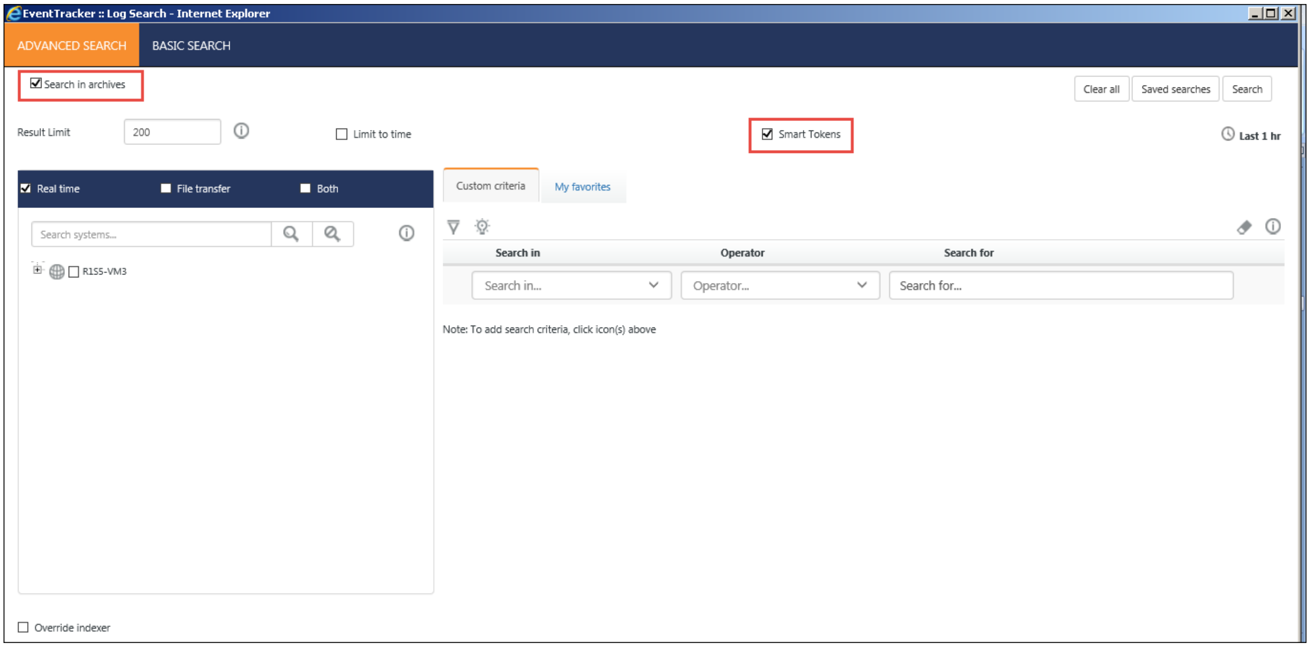
How to Perform a Search on Smart Tokens?

To perform a filtered search on Smart Tokens from the Knowledge Objects available, you need to follow the below mentioned steps:

Step 1: Click the search icon 🔍 from the EventTracker menu. The Log Search dialog box is displayed.

Step 2: Select the checkbox **"Search in archives"**. The smart token option is now visible.

Step 3: Enable the option "Smart Token" by clicking the check box.



☑ Search in archives

Result Limit 200

□ Limit to time

☑ Smart Tokens

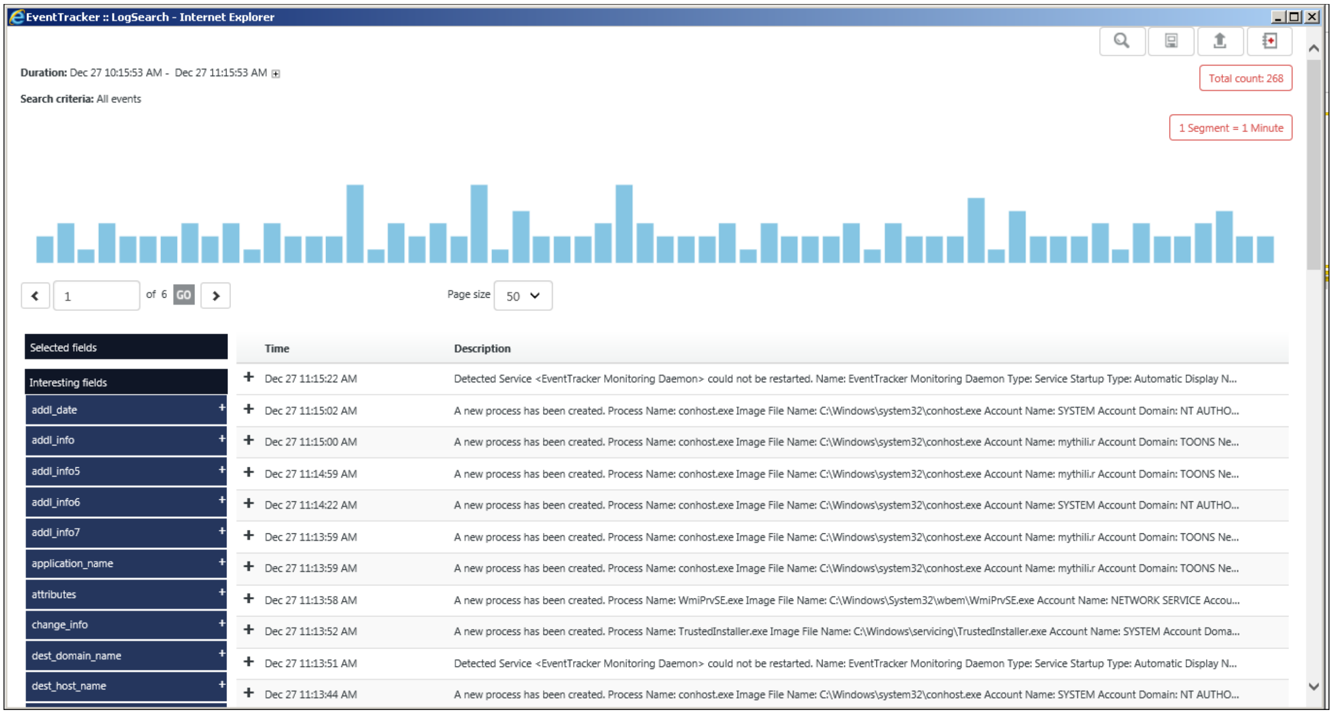
☑ Real time ■ File transfer ■ Both

Note: To add search criteria, click icon(s) above

□ Override indexer

Figure 215

Step 4: Perform a search. The search result gets displayed with all the interesting fields listed in the left pane.



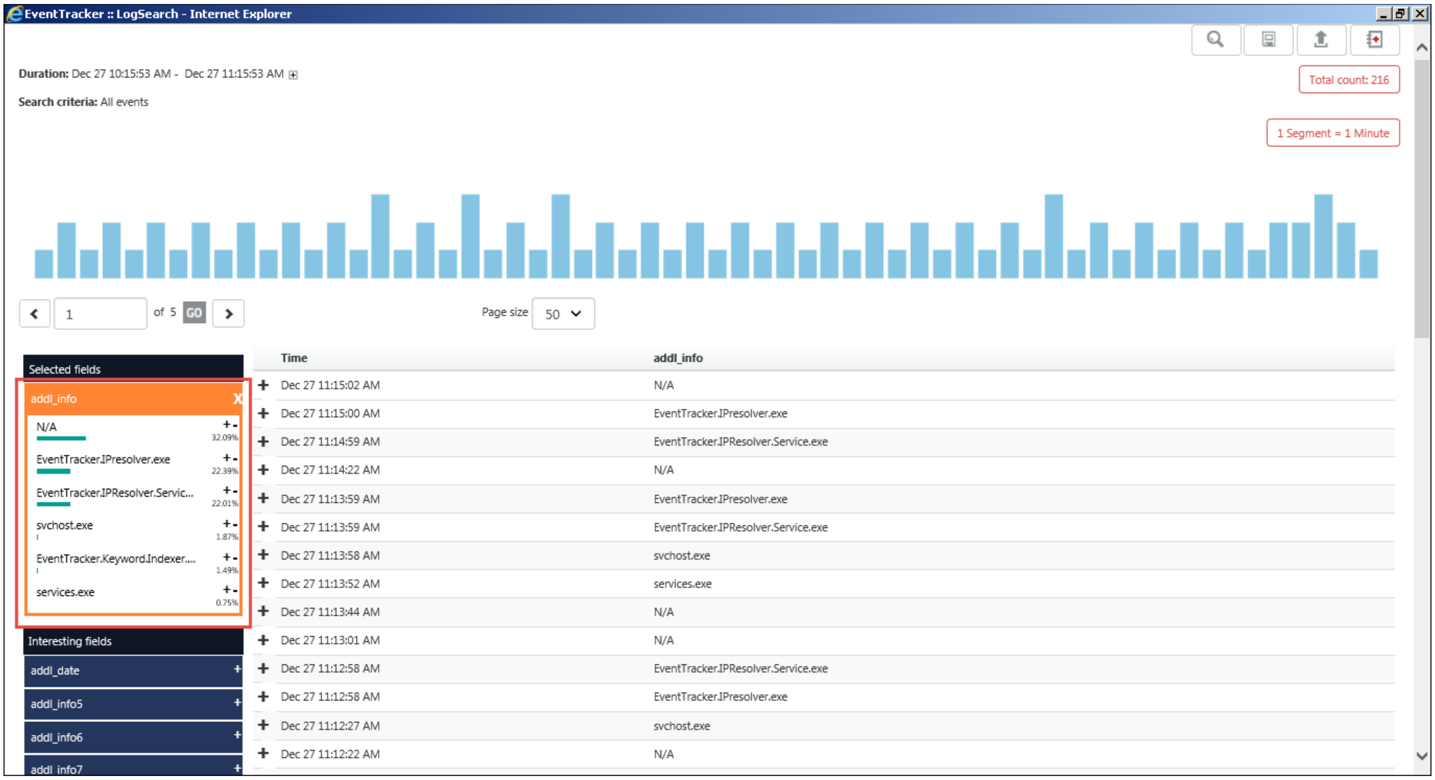
Duration: Dec 27 10:15:53 AM - Dec 27 11:15:53 AM

Search criteria: All events

Time	Description
Dec 27 11:15:22 AM	Detected Service <EventTracker Monitoring Daemon> could not be restarted. Name: EventTracker Monitoring Daemon Type: Service Startup Type: Automatic Display N...
Dec 27 11:15:02 AM	A new process has been created. Process Name: conhost.exe Image File Name: C:\Windows\system32\conhost.exe Account Name: SYSTEM Account Domain: NT AUTHO...
Dec 27 11:15:00 AM	A new process has been created. Process Name: conhost.exe Image File Name: C:\Windows\system32\conhost.exe Account Name: mythili.r Account Domain: TOONS Ne...
Dec 27 11:14:59 AM	A new process has been created. Process Name: conhost.exe Image File Name: C:\Windows\system32\conhost.exe Account Name: mythili.r Account Domain: TOONS Ne...
Dec 27 11:14:22 AM	A new process has been created. Process Name: conhost.exe Image File Name: C:\Windows\system32\conhost.exe Account Name: SYSTEM Account Domain: NT AUTHO...
Dec 27 11:13:59 AM	A new process has been created. Process Name: conhost.exe Image File Name: C:\Windows\system32\conhost.exe Account Name: mythili.r Account Domain: TOONS Ne...
Dec 27 11:13:59 AM	A new process has been created. Process Name: conhost.exe Image File Name: C:\Windows\system32\conhost.exe Account Name: mythili.r Account Domain: TOONS Ne...
Dec 27 11:13:58 AM	A new process has been created. Process Name: WmiPrvSE.exe Image File Name: C:\Windows\System32\wbem\WmiPrvSE.exe Account Name: NETWORK SERVICE Accou...
Dec 27 11:13:52 AM	A new process has been created. Process Name: TrustedInstaller.exe Image File Name: C:\Windows\servicing\TrustedInstaller.exe Account Name: SYSTEM Account Doma...
Dec 27 11:13:51 AM	Detected Service <EventTracker Monitoring Daemon> could not be restarted. Name: EventTracker Monitoring Daemon Type: Service Startup Type: Automatic Display N...
Dec 27 11:13:44 AM	A new process has been created. Process Name: conhost.exe Image File Name: C:\Windows\system32\conhost.exe Account Name: SYSTEM Account Domain: NT AUTHO...

Figure 216

Step 5: The interesting fields includes the different values and these fields can be further included or excluded in the search criteria.



Duration: Dec 27 10:15:53 AM - Dec 27 11:15:53 AM

Search criteria: All events

Selected fields

addl_info

N/A	+ -	32.09%
EventTracker.IPresolver.exe	+ -	22.39%
EventTracker.IPResolver.Servic...	+ -	22.01%
svchost.exe	+ -	1.87%
EventTracker.Keyword.Indexer....	+ -	1.49%
services.exe	+ -	0.75%

Interesting fields

- addl_date +
- addl_info5 +
- addl_info6 +
- addl_info7 +

Time	addl_info
Dec 27 11:15:02 AM	N/A
Dec 27 11:15:00 AM	EventTracker.IPresolver.exe
Dec 27 11:14:59 AM	EventTracker.IPResolver.Service.exe
Dec 27 11:14:22 AM	N/A
Dec 27 11:13:59 AM	EventTracker.IPresolver.exe
Dec 27 11:13:59 AM	EventTracker.IPResolver.Service.exe
Dec 27 11:13:58 AM	svchost.exe
Dec 27 11:13:52 AM	services.exe
Dec 27 11:13:44 AM	N/A
Dec 27 11:13:01 AM	N/A
Dec 27 11:12:58 AM	EventTracker.IPResolver.Service.exe
Dec 27 11:12:58 AM	EventTracker.IPresolver.exe
Dec 27 11:12:27 AM	svchost.exe
Dec 27 11:12:22 AM	N/A

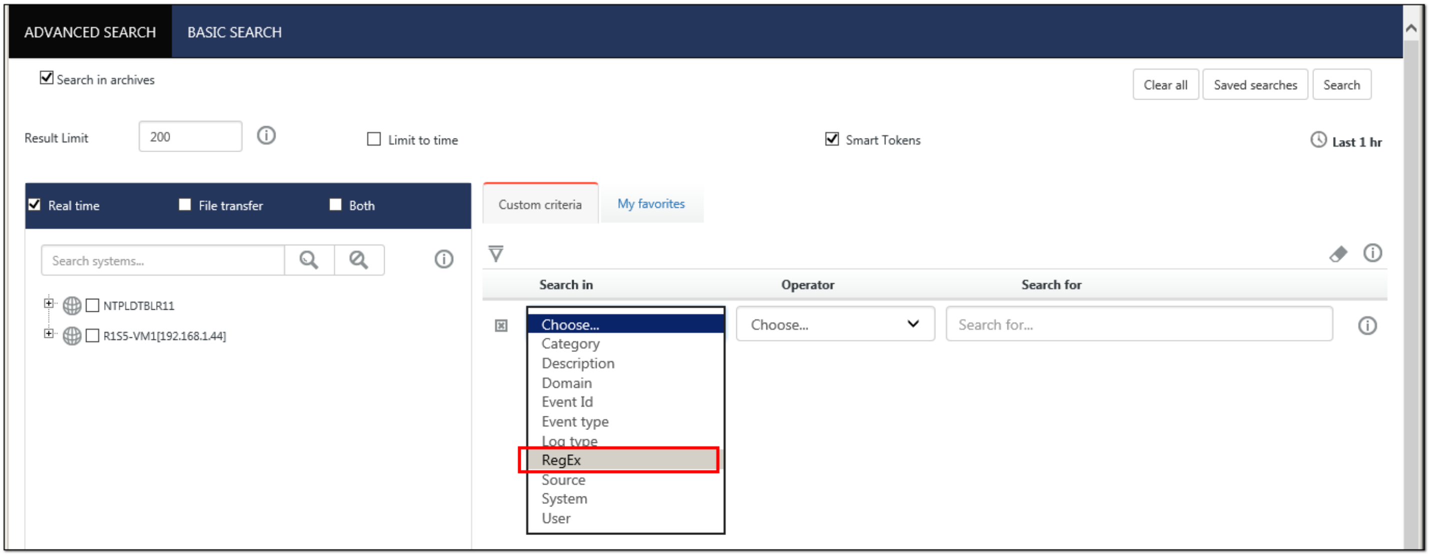
Figure 217

Pivoting can be done based on the interesting fields available in the left pane, which can be included + or excluded ☒ depending on the search criteria.

3.5.1 RegEx in Log Search

In Advanced Log search, you can search using regular expression.

1. Click **Add search criteria** ▽ .
2. In **Search in** drop down menu, select **RegEx**.



☑ Search in archives

Result Limit 200

□ Limit to time

☑ Smart Tokens

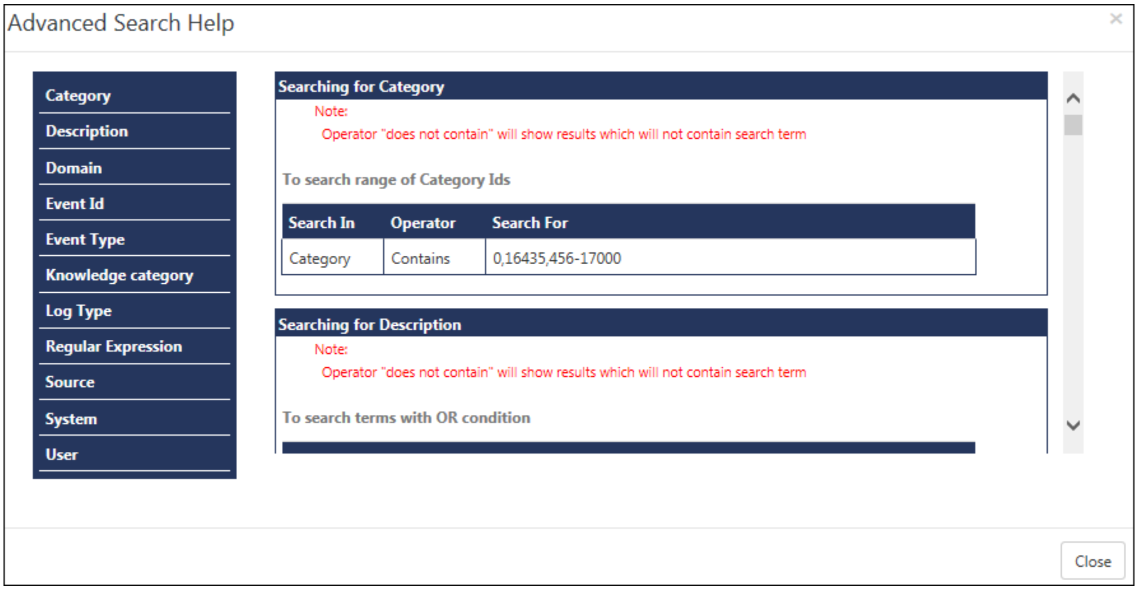
Last 1 hr

☑ Real time □ File transfer □ Both

Search for...

Figure 218

3. Select **Operator** drop down.
4. Enter search criteria in **Search for** box.
5. Click **Help** ⓘ for additional information.



Advanced Search Help

Searching for Category

Note:

Operator "does not contain" will show results which will not contain search term

To search range of Category Ids

Search In	Operator	Search For
Category	Contains	0,16435,456-17000

Searching for Description

Note:

Operator "does not contain" will show results which will not contain search term

To search terms with OR condition

Figure 219

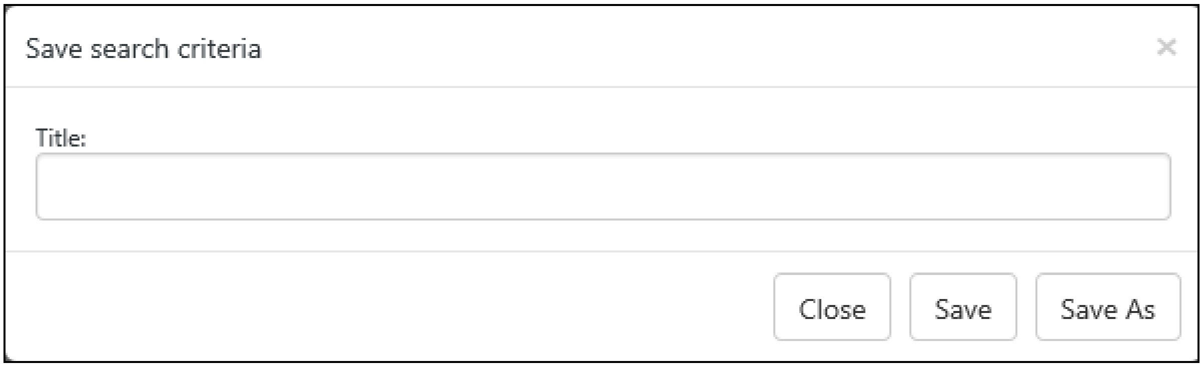
6. Click **Search**.

3.5.1.1 Saving Search Criteria

The search criteria can also be saved for viewing later.

- Click the 💾 icon for saving the filtered token criteria.
- Give a title and click **-<Save>-**.

  The search result will be saved.



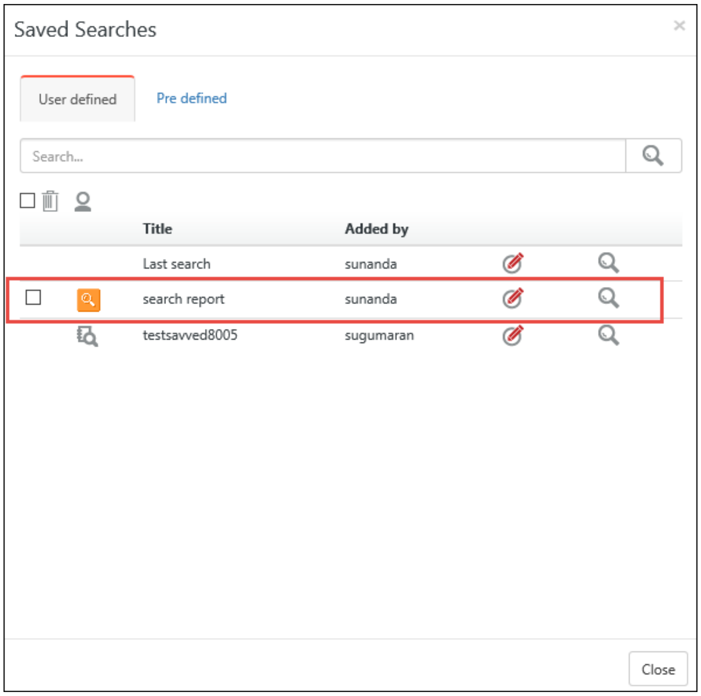
Save search criteria ×

Title:

Close | Save | Save As

Figure 220

- For viewing the saved search results, click on -<**Advanced Search**>- .In the Advanced Log Search window, click on the “**Saved searche**s” option.



Saved Searches ×

User defined | Pre defined

Search...

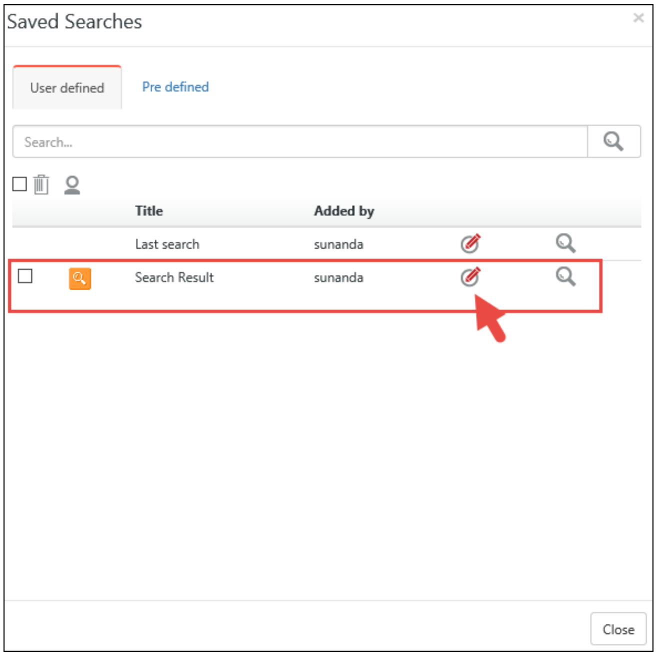
Title	Added by
Last search	sunanda
search report	sunanda
testsavved8005	sugumaran

Close

Figure 221

How to edit a Saved search?

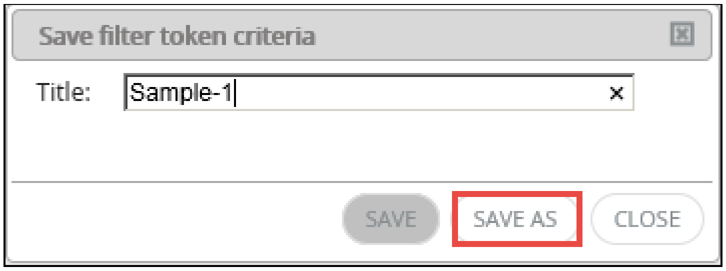
For editing the saved search criteria, click the **Saved search** hyperlink. The saved result opens.



	Title	Added by
	Last search	sunanda
□	Search Result	sunanda

Figure 222

- Click on the ✎ icon and start editing the saved searches.
- After editing and performing the search, the new search result can also be saved with a new title for viewing later.



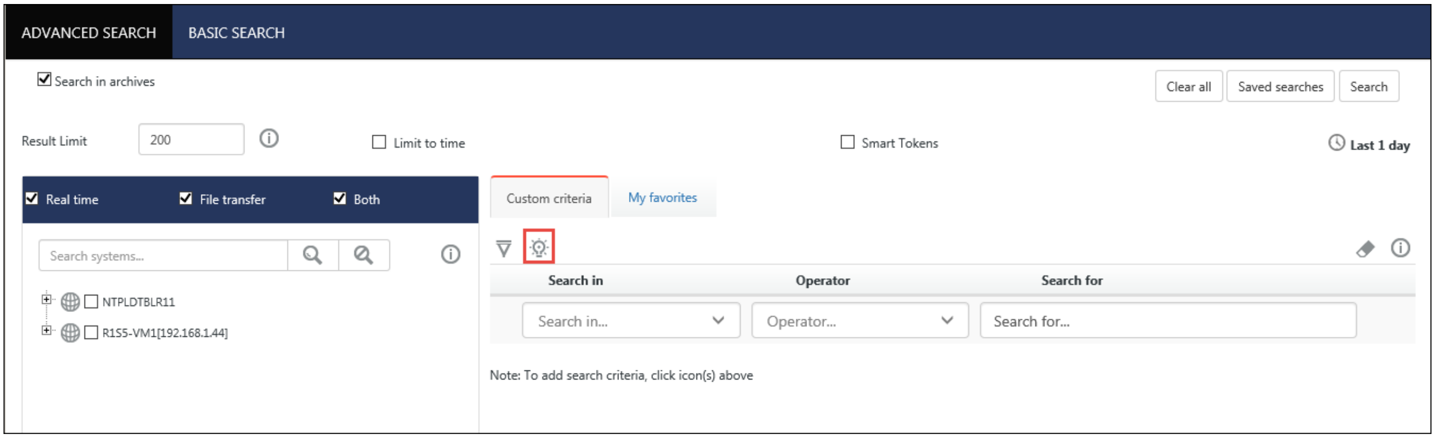
Title: Sample-1

Figure 223

How to Add Knowledge Objects?

For adding Knowledge objects and viewing a search result based on that, the below mentioned steps should be followed:

Step 1: Open the Advanced Log Search window.



☑ Search in archives

Result Limit 200

□ Limit to time

□ Smart Tokens

Last 1 day

☑ Real time ☑ File transfer ☑ Both

□ NTPLDTBLR11

□ R1S5-VM1[192.168.1.44]

Note: To add search criteria, click icon(s) above

Figure 224

Step 2: Click the icon ☼ to add knowledge object.

Step 3: Click '**Search**'.

The search page will be displayed and then you can further proceed in the same way for performing log search.

NOTE: Windows Standard Token is a default token offered by EventTracker in log search, which cannot be edited and saved.

4. Reports

In this chapter, you will learn about:

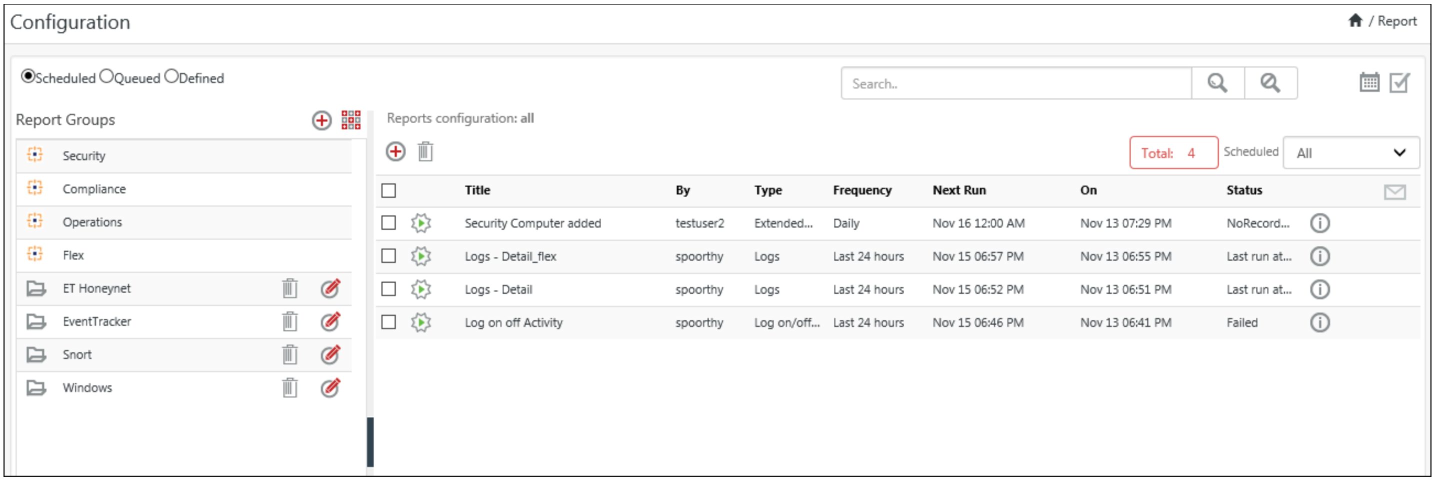
- Reports Configuration
- Reports Dashboard
- Generate different reports
  - On Demand
  - Queued
  - Scheduled
  - Defined
- Security/Operations/Compliance/Flex Reports/Alphabetical
- Reports Exception
- Reports Status
- Report Calendar
- Flex History

4.1 Reports Configuration

Note: To understand the usage of the new system selection interface introduced in feature update 9.3.3 as part of update ET93U20-031, please refer New System Selection Interface User Guide.

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 **New** ⊕ .
2. To view the respective **Security/Operation/Compliance/Flex Reports** that are configured, click the respective **Report groups**.



Configuration

/ Report

● Scheduled ○ Queued ○ Defined

Search..

Report Groups

- Security
- Compliance
- Operations
- Flex
- ET Honeynet
- EventTracker
- Snort
- Windows

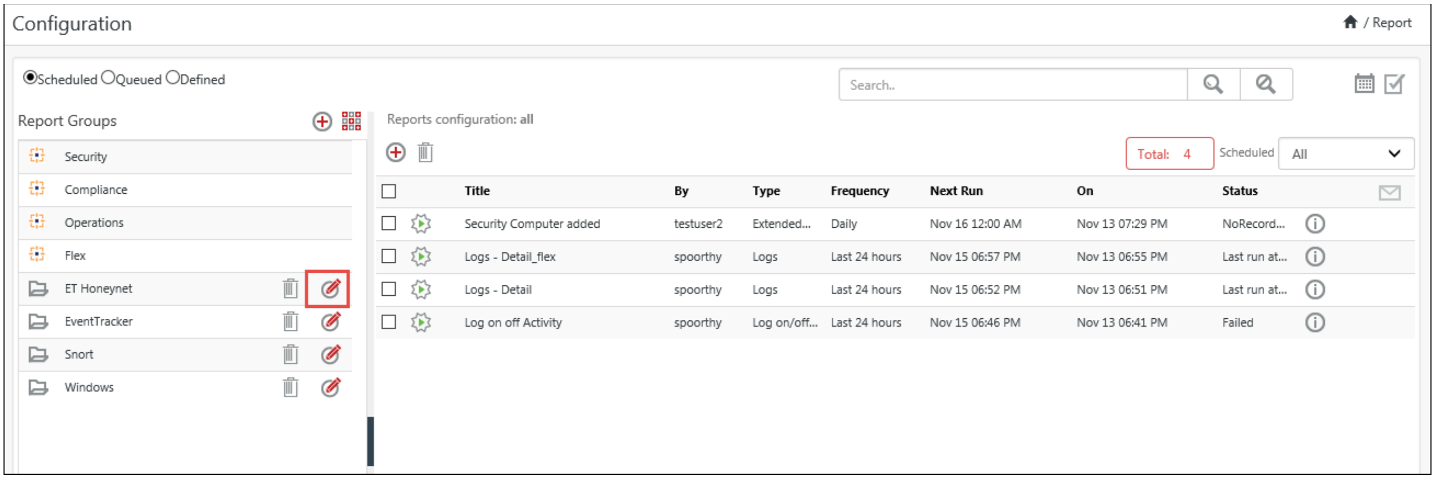
Reports configuration: all

Total: 4 Scheduled All

□		Title	By	Type	Frequency	Next Run	On	Status
□		Security Computer added	testuser2	Extended...	Daily	Nov 16 12:00 AM	Nov 13 07:29 PM	NoRecord...
□		Logs - Detail_flex	spoorthy	Logs	Last 24 hours	Nov 15 06:57 PM	Nov 13 06:55 PM	Last run at...
□		Logs - Detail	spoorthy	Logs	Last 24 hours	Nov 15 06:52 PM	Nov 13 06:51 PM	Last run at...
□		Log on off Activity	spoorthy	Log on/off...	Last 24 hours	Nov 15 06:46 PM	Nov 13 06:41 PM	Failed

Figure 225

3. To Edit or Delete a group in **Reports Configuration** tree, right-click any group, select **Edit** or **Delete** accordingly.



Configuration

/ Report

● Scheduled ○ Queued ○ Defined

Search..

Report Groups

- Security
- Compliance
- Operations
- Flex
- ET Honeynet
- EventTracker
- Snort
- Windows

Reports configuration: all

Total: 4 Scheduled All

□		Title	By	Type	Frequency	Next Run	On	Status
□		Security Computer added	testuser2	Extended...	Daily	Nov 16 12:00 AM	Nov 13 07:29 PM	NoRecord...
□		Logs - Detail_flex	spoorthy	Logs	Last 24 hours	Nov 15 06:57 PM	Nov 13 06:55 PM	Last run at...
□		Logs - Detail	spoorthy	Logs	Last 24 hours	Nov 15 06:52 PM	Nov 13 06:51 PM	Last run at...
□		Log on off Activity	spoorthy	Log on/off...	Last 24 hours	Nov 15 06:46 PM	Nov 13 06:41 PM	Failed

Figure 226

4. To email a report, click **Email** ✉ .
5. Select any report option and then click **Information** ⓘ 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 **Run Now** ▶ to run the respective **Scheduled/Queued/Defined** reports.
8. Select the **Scheduled** drop-down to run the report **All** / **Daily /Last 24 hours/ Twice Daily / Hourly / Weekly /Last 1 week/Once in a Week/Monthly.**
9. To search for a report, enter the search criteria and click **Search** 🔍 **.**
10. To delete a report, select any report and then click **Delete** 🗑 **.**
11. To view data about **Reports** in Calendar, click **Report Calendar** 📅 .
12. To view status about **Reports**, click **Report Status** ☑ .

4.2 Security/Operations/Compliance/Flex Reports/Alphabetical Reports/Favorites

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

2 Select **New** ⊕.

EventTracker opens the Reports page.

3 Select the required **Security/Operations/Compliance/Flex Reports /Alphabetical/Favorites** 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 are explained below.

4.2.1 Security reports

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.

4.2.2 Operations reports

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.

4.2.3 Compliance reports

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

4.2.4 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.

4.2.5 Favorites tab

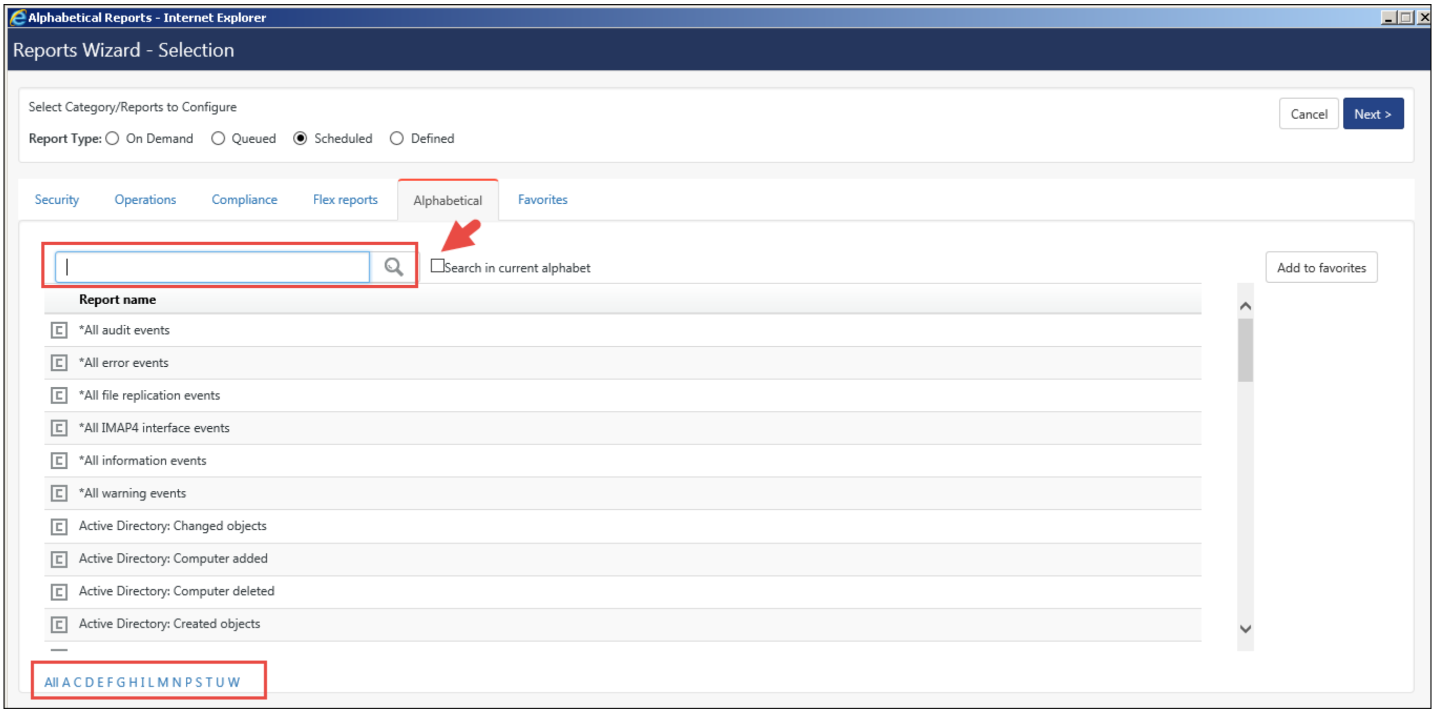
This tab will display all the category/reports/ flex reports that are added to the favorite list.

4.3 Generating Alphabetical Reports

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

2 Click **New** ⊕ in **Dashboard / Configuration**.

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


Alphabetical Reports - Internet Explorer
Reports Wizard - Selection
Cancel
Next >
Security
Operations
Compliance
Flex reports
Alphabetical
Favorites
Add to favorites
All A C D E F G H I L M N P S T U W

Select Category/Reports to Configure

Report Type: ○ On Demand ○ Queued ● Scheduled ○ Defined

□ Search in current alphabet

Report name
*All audit events
*All error events
*All file replication events
*All IMAP4 interface events
*All information events
*All warning events
Active Directory: Changed objects
Active Directory: Computer added
Active Directory: Computer deleted
Active Directory: Created objects

Figure 227

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 opens the Category/Reports/Flex Report searched for.

(OR)

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

6 Click **Next**>>.

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

🗎 NOTE

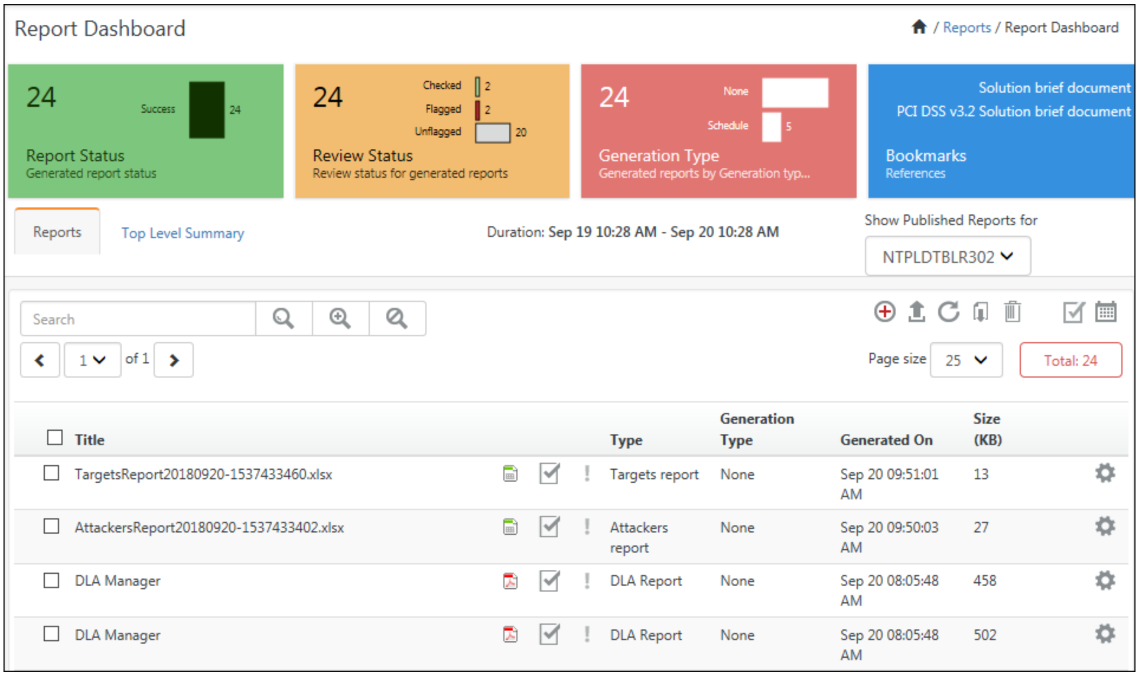
You can also add Category/Reports/Flex Report to the favorites list. To do this select a Category/Reports/Flex Report and then click Add to favorites. Similarly, you can generate Security, Operations, Flex and Compliance Reports.

4.4 Reports Dashboard page

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

1 Click **Reports,** and then click **Dashboard**.

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



Report Dashboard

/ Reports / Report Dashboard

24 Success 24 — Report Status — Generated report status

24 Checked 2, Flagged 2, Unflagged 20 — Review Status — Review status for generated reports

24 None, Schedule 5 — Generation Type — Generated reports by Generation typ...

Solution brief document
PCI DSS v3.2 Solution brief document
Bookmarks — References

Reports | Top Level Summary

Duration: Sep 19 10:28 AM - Sep 20 10:28 AM

Show Published Reports for: NTPLDTBLR302

Search

1 of 1

Page size 25 | Total: 24

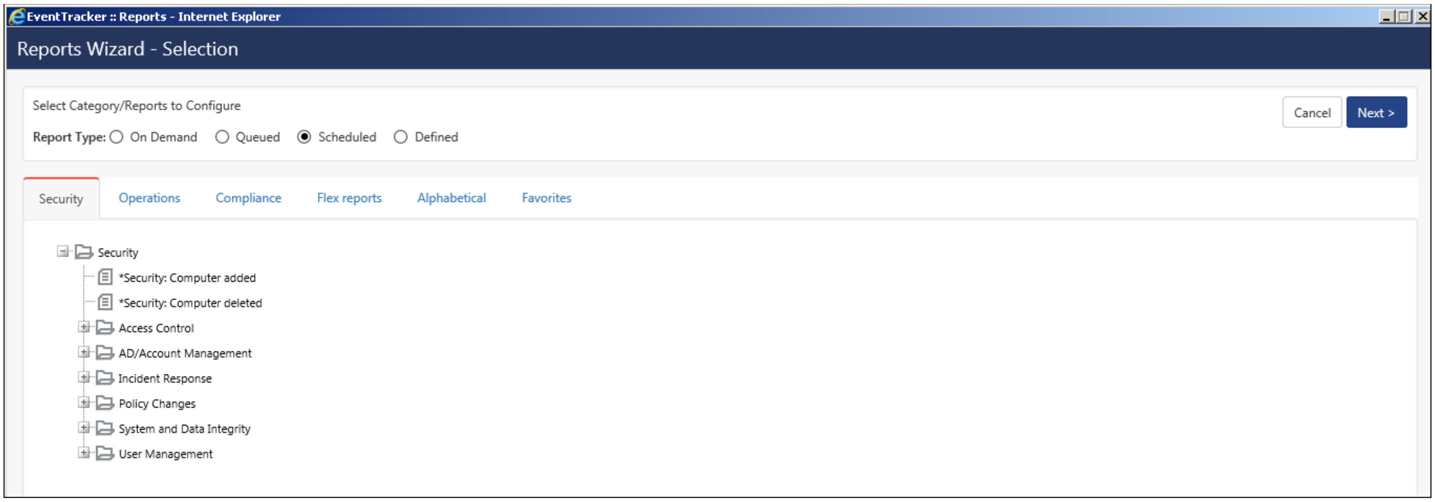
□	Title				Type	Generation Type	Generated On	Size (KB)	
□	TargetsReport20180920-1537433460.xlsx		☑	!	Targets report	None	Sep 20 09:51:01 AM	13	⚙
□	AttackersReport20180920-1537433402.xlsx		☑	!	Attackers report	None	Sep 20 09:50:03 AM	27	⚙
□	DLA Manager		☑	!	DLA Report	None	Sep 20 08:05:48 AM	458	⚙
□	DLA Manager		☑	!	DLA Report	None	Sep 20 08:05:48 AM	502	⚙

Figure 228

NOTE

In Reports, Export Type will only support for Excel, PDF and HTML.

2 Click **New** ⊕ in the **Report Dashboard** page, to generate the respective reports.



EventTracker :: Reports - Internet Explorer

Reports Wizard - Selection

Select Category/Reports to Configure

Report Type: ○ On Demand ○ Queued ● Scheduled ○ Defined

Cancel | Next >

Security | Operations | Compliance | Flex reports | Alphabetical | Favorites

- Security
  - *Security: Computer added
  - *Security: Computer deleted
  - Access Control
  - AD/Account Management
  - Incident Response
  - Policy Changes
  - System and Data Integrity
  - User Management

Figure 229

The detail 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.

Icon	Description
🗋	No record found
»	Processing report
☑	Report generated successfully
❌	Failed to generate report
☒	Cancelled report

Table 24

4 Click **Flag** ! to change the status of the report.

Flag Icon	Description
! GRAY	Un-flagged and no action has been taken
! RED	Flagged and relevant action is required for that particular incident to solve an issue
! GREEN	Checked the report and necessary action has been taken care of

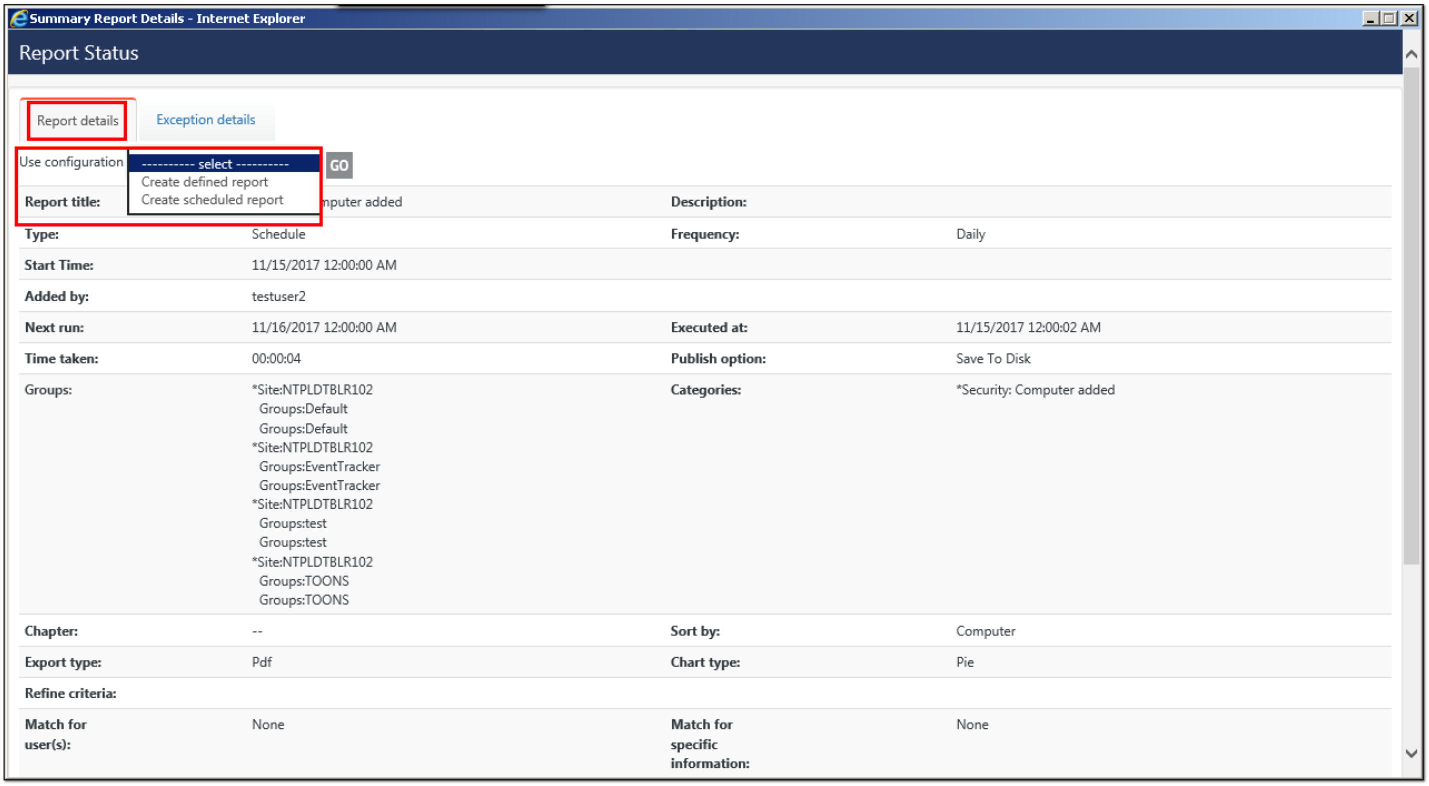
Table 25

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

Table 26

5 Select **Info** ⓘ from the gear icon in the right-hand corner for viewing Report **Details** and **Exception Details**.

Report details window opens by default.



Report title:	...mputer added	Description:	
Type:	Schedule	Frequency:	Daily
Start Time:	11/15/2017 12:00:00 AM		
Added by:	testuser2		
Next run:	11/16/2017 12:00:00 AM	Executed at:	11/15/2017 12:00:02 AM
Time taken:	00:00:04	Publish option:	Save To Disk
Groups:	*Site:NTPLDTBLR102 Groups:Default Groups:Default *Site:NTPLDTBLR102 Groups:EventTracker Groups:EventTracker *Site:NTPLDTBLR102 Groups:test Groups:test *Site:NTPLDTBLR102 Groups:TOONS Groups:TOONS	Categories:	*Security: Computer added
Chapter:	--	Sort by:	Computer
Export type:	Pdf	Chart type:	Pie
Refine criteria:			
Match for user(s):	None	Match for specific information:	None

Figure 230

a. Select **Use Configuration** drop-down, select **Create defined report** or **Create scheduled report**.

b. Select **Go** hyperlink.

c. Select **Exception Details** to view details about the exceptions generated.

d. Select **Flag for Follow up** 📝 to add more information.

6 Select on **Title** hyperlink to view details about the report in **PDF and Excel** format etc.
Summary Report Details window opens.

7 Select **Export** ⬆ to export data to excel.

8 Select **Casebook** from the drop-down list by clicking the ⚙ icon, to update data in Casebook.

A Casebook message opens.

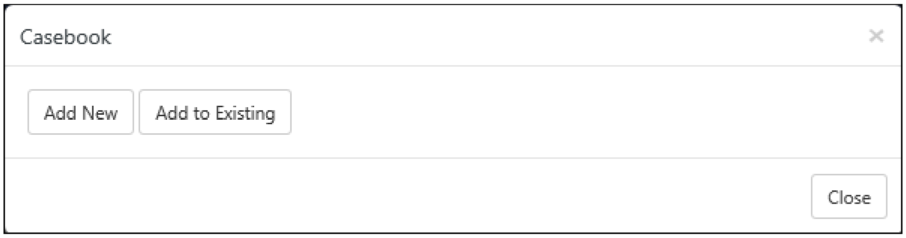


Figure 231

a) To add a new Casebook entry, click **Add new**.

b) To add to an existing Casebook, click **Add to existing**.

Casebook window opens.

c) Enter relevant data and then click **Save**.

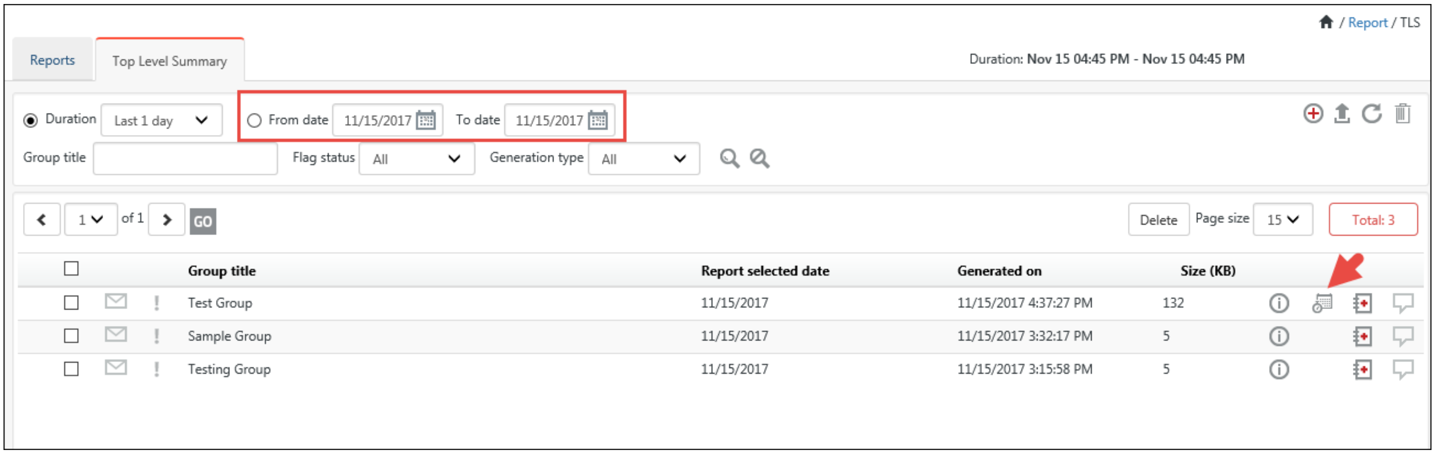
For detail information, refer Casebook.

9 Click **Notes** 💬 to add comments about a report.

10 For deleting any report, select the checkbox of the report and then click **Delete** to delete a report from the **Dashboard** view.

4.4.1 Top Level Summary tab

1 Click on the **Top-Level Summary** tab, to display the Top-Level Summary Data**.**
EventTracker: Top Level Summary Dashboard page opens.
The summary data of the generated scheduled reports is archived during report generation. Summary data is collected for specific type of reports like flex (log, log volume) and category-based reports only.



Duration: Nov 15 04:45 PM - Nov 15 04:45 PM

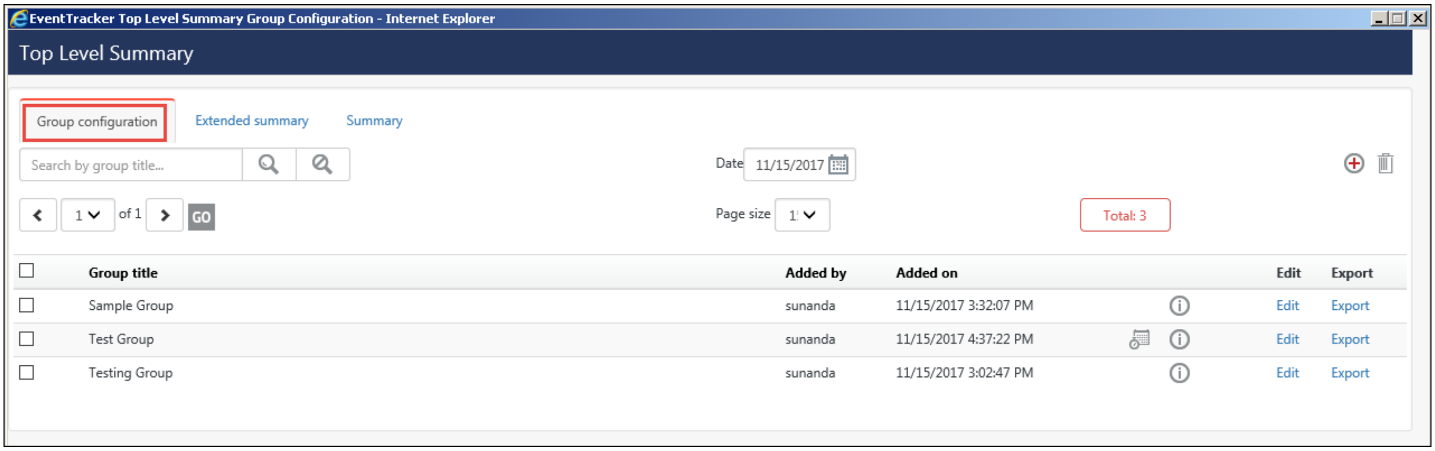
● Duration Last 1 day ○ From date 11/15/2017 To date 11/15/2017

Group title Flag status All Generation type All

□			Group title	Report selected date	Generated on	Size (KB)
□		!	Test Group	11/15/2017	11/15/2017 4:37:27 PM	132
□		!	Sample Group	11/15/2017	11/15/2017 3:32:17 PM	5
□		!	Testing Group	11/15/2017	11/15/2017 3:15:58 PM	5

Figure 232

- The **Top Level Summary** tab will display the scheduled and the on demand report groups that have been exported. The **scheduled** opens the scheduled report groups. The user can select the date range and search report as per requirement.
- For configuring a **Top Level Summary Group**, click **Group Configuration** ⊕ . EventTracker opens the Group Configuration Tab.
- Click **Add Group** to configure a Group.

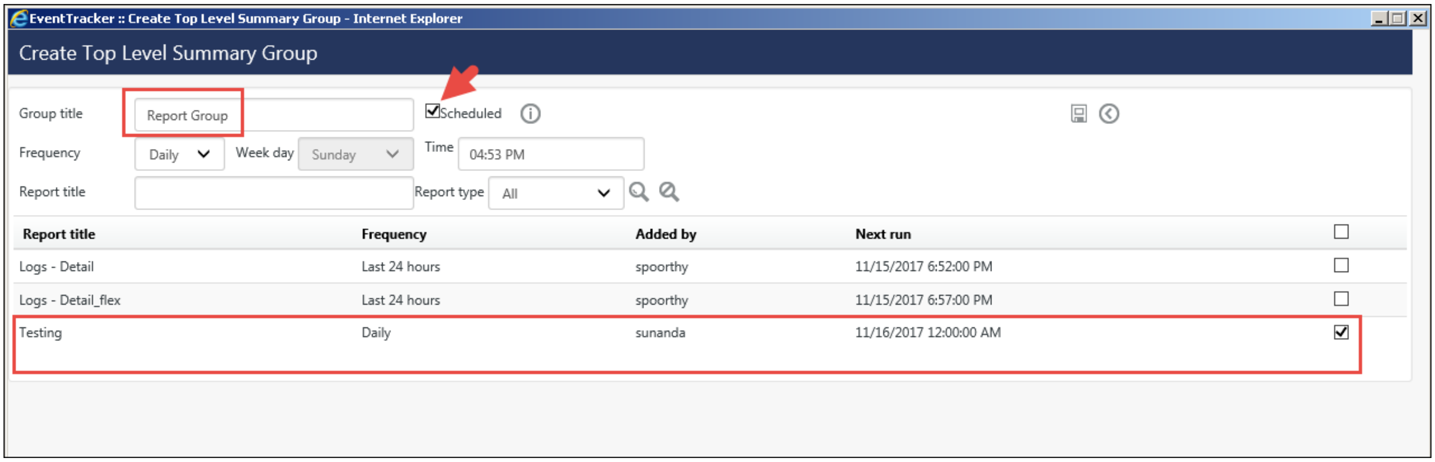


Date 11/15/2017

□	Group title	Added by	Added on	Edit	Export
□	Sample Group	sunanda	11/15/2017 3:32:07 PM	Edit	Export
□	Test Group	sunanda	11/15/2017 4:37:22 PM	Edit	Export
□	Testing Group	sunanda	11/15/2017 3:02:47 PM	Edit	Export

Figure 233

- Enter a **Group Title**; select the reports to be added under the group by clicking the checkbox and then click **Save**. Also select the checkbox Scheduled as shown in the figure below.



EventTracker :: Create Top Level Summary Group - Internet Explorer

Create Top Level Summary Group

Group title: Report Group ☑Scheduled

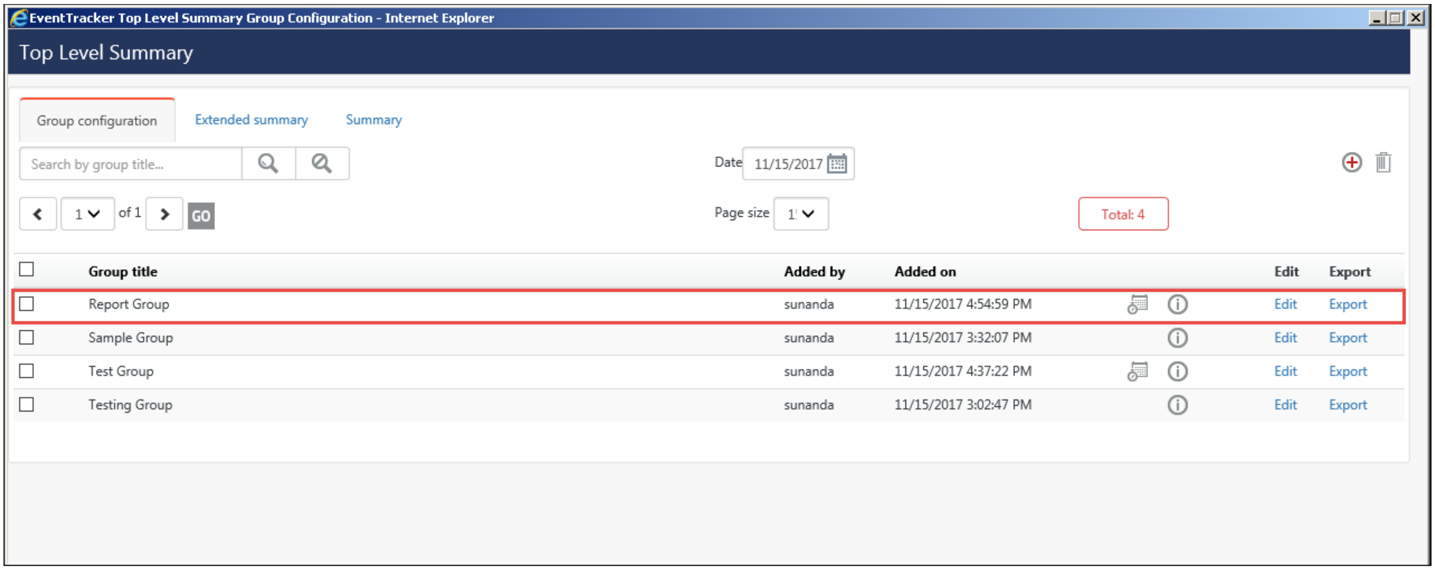
Frequency: Daily Week day: Sunday Time: 04:53 PM

Report title: Report type: All

Report title	Frequency	Added by	Next run	□
Logs - Detail	Last 24 hours	spoorthy	11/15/2017 6:52:00 PM	□
Logs - Detail_flex	Last 24 hours	spoorthy	11/15/2017 6:57:00 PM	□
Testing	Daily	sunanda	11/16/2017 12:00:00 AM	☑

Figure 234

The Group gets added and is displayed in the Group Configuration page.



EventTracker Top Level Summary Group Configuration - Internet Explorer

Top Level Summary

Group configuration | Extended summary | Summary

Search by group title...

Date: 11/15/2017

1 of 1 GO

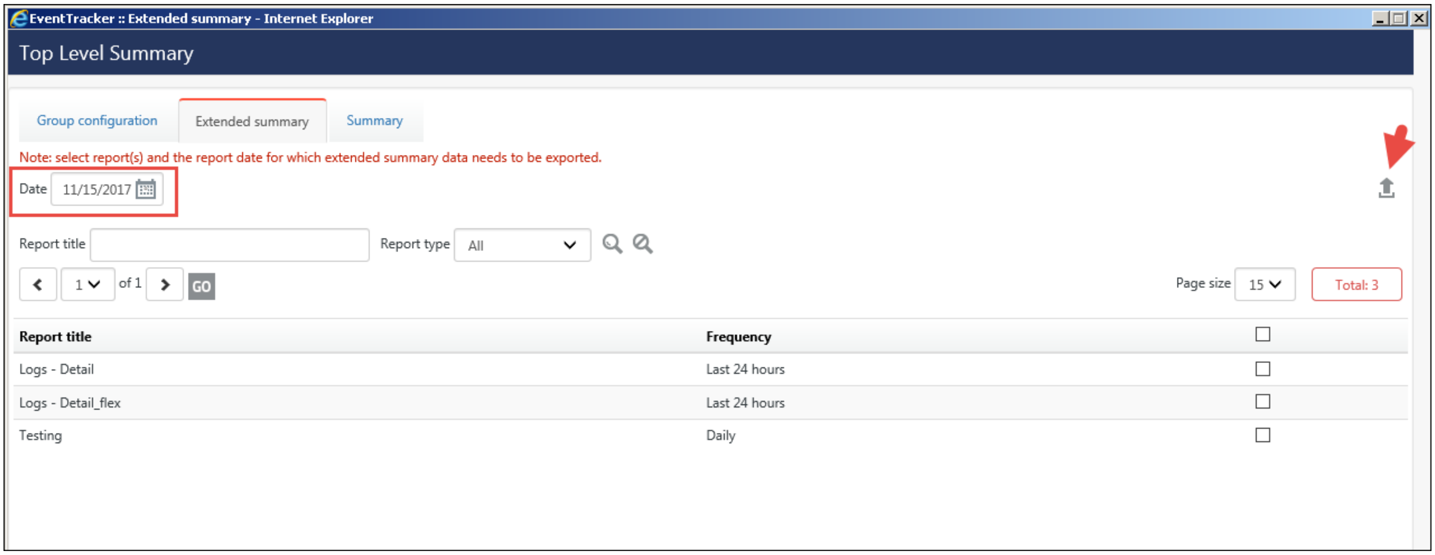
Page size: 1

Total: 4

□	Group title	Added by	Added on		Edit	Export
□	Report Group	sunanda	11/15/2017 4:54:59 PM		Edit	Export
□	Sample Group	sunanda	11/15/2017 3:32:07 PM		Edit	Export
□	Test Group	sunanda	11/15/2017 4:37:22 PM		Edit	Export
□	Testing Group	sunanda	11/15/2017 3:02:47 PM		Edit	Export

Figure 235

- In the **Extended summary** tab, the user can select the report(s) and the date for which the extended summary data needs to be exported.



Note: select report(s) and the report date for which extended summary data needs to be exported.

Date 11/15/2017

Report title

Report type All

1 of 1

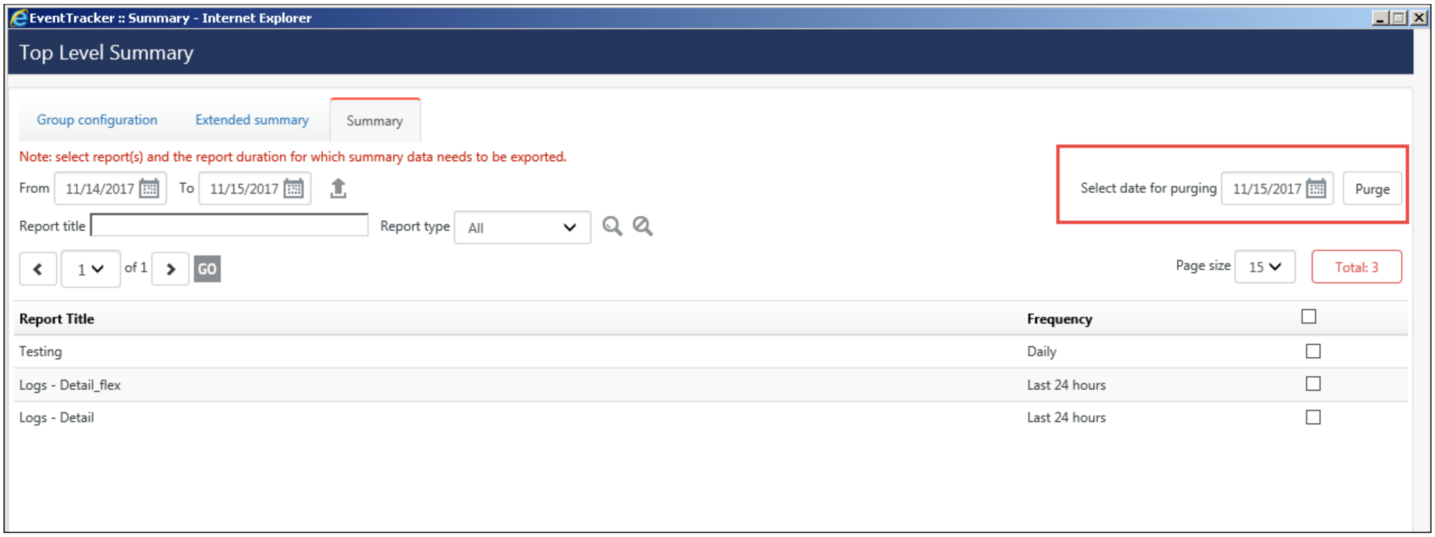
Page size 15

Total: 3

Report title	Frequency	□
Logs - Detail	Last 24 hours	□
Logs - Detail_flex	Last 24 hours	□
Testing	Daily	□

Figure 236

- In the **Summary** tab, select the report (s) and the date range that needs to be exported in to excel files.
- You can also purge the reports up to a selected date by using **Purge** from **Summary** tab.



Note: select report(s) and the report duration for which summary data needs to be exported.

From 11/14/2017 To 11/15/2017

Select date for purging 11/15/2017

Report title

Report type All

1 of 1

Page size 15

Total: 3

Report Title	Frequency	□
Testing	Daily	□
Logs - Detail_flex	Last 24 hours	□
Logs - Detail	Last 24 hours	□

Figure 237

2 To get an Extended Summary of the report, select the required Report titles and then select ⬆ **Export**.

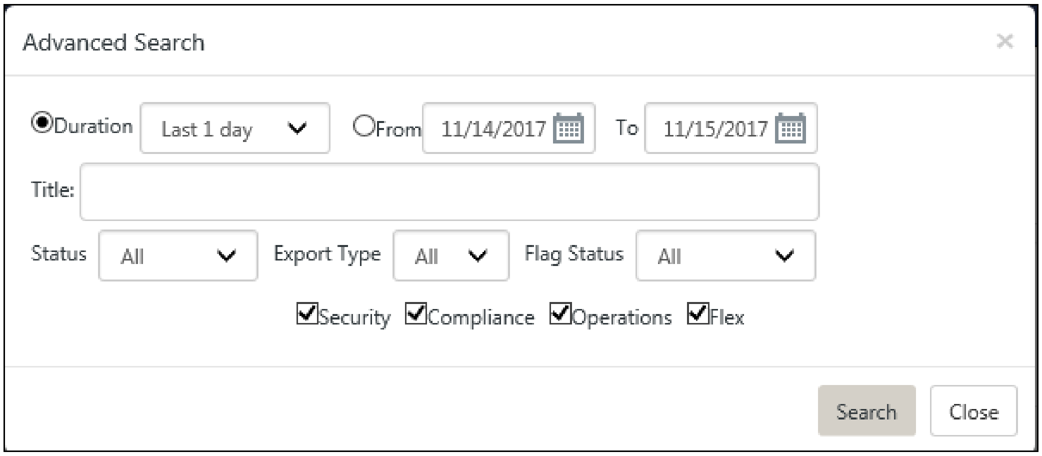
The selected reports are exported to an excel file.

3 To view data about **Reports** in Calendar, click **Report Calendar** ▦ icon.

4 To view status about **Reports**, click **Report Status** ☑ .

5 To search any report, enter relevant data in Search textbox and then click **Search**.

6 To perform an advance search, click **Advanced Search** in the **Report Dashboard** page.
Advanced Search window opens.



Advanced Search

● Duration: Last 1 day
○ From: 11/14/2017 To: 11/15/2017
Title:
Status: All
Export Type: All
Flag Status: All
☑ Security ☑ Compliance ☑ Operations ☑ Flex

Figure 238

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

4.5 Generating 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, click the **Reports** menu, and then select **Dashboard** or **Configuration**.

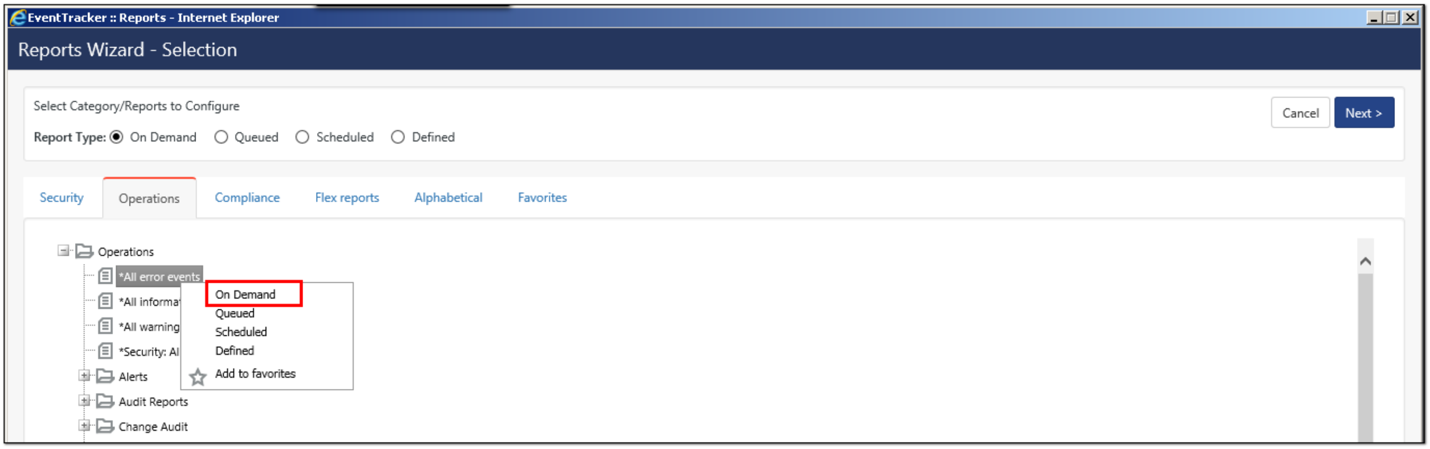
2 Click **New** in **Dashboard / Configuration**.

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 **Security** menu, select **All error events**, right-click **On Demand.**

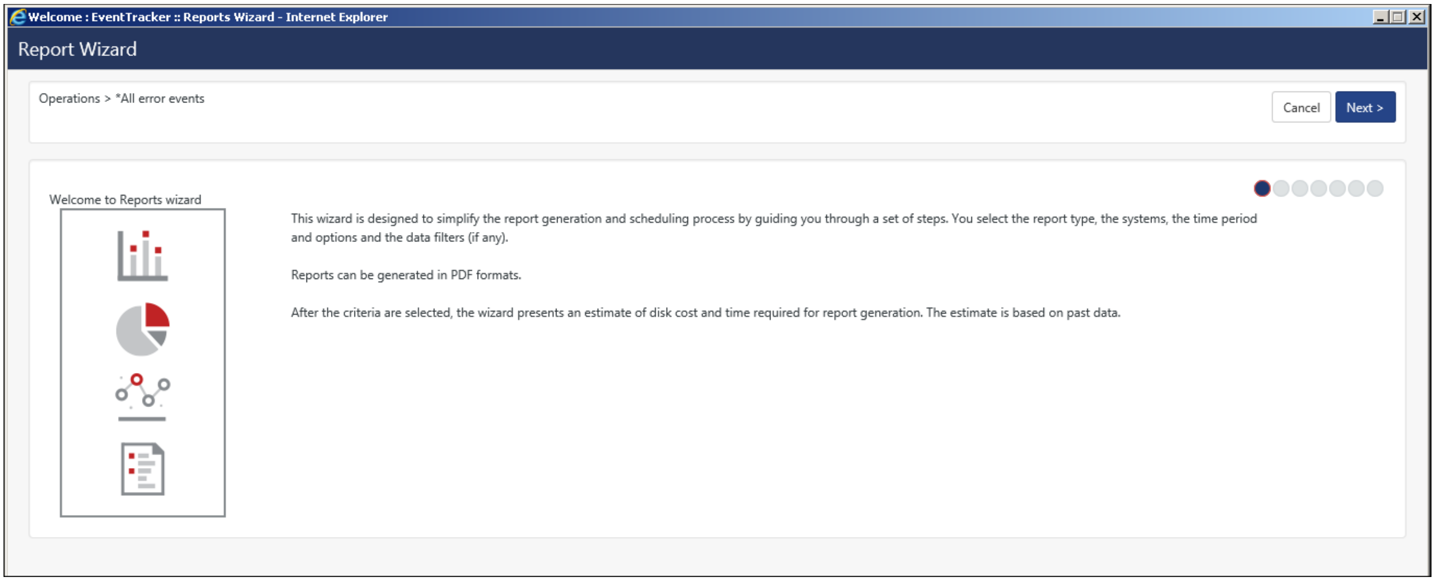


Select Category/Reports to Configure

Report Type: ● On Demand ○ Queued ○ Scheduled ○ Defined

Figure 239

EventTracker opens the Reports Wizard.


Welcome : EventTracker :: Reports Wizard - Internet Explorer
Report Wizard
Cancel
Next >
Welcome to Reports wizard

Operations > *All error events

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 formats.

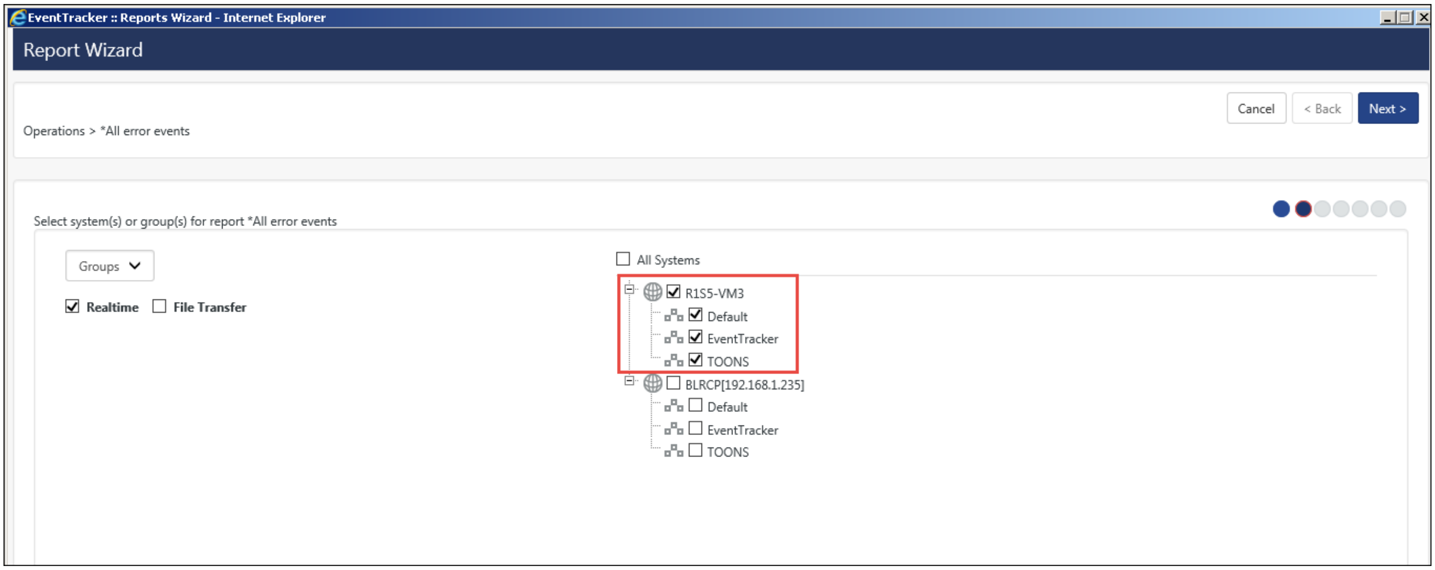
After the criteria are selected, the wizard presents an estimate of disk cost and time required for report generation. The estimate is based on past data.

Figure 240

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>>.**



EventTracker :: Reports Wizard - Internet Explorer

Report Wizard

Operations > *All error events

Select system(s) or group(s) for report *All error events

Groups

☑ Realtime ☐ File Transfer

☐ All Systems
- ☑ R1S5-VM3
  - ☑ Default
  - ☑ EventTracker
  - ☑ TOONS
- ☐ BLRCP[192.168.1.235]
  - ☐ Default
  - ☐ EventTracker
  - ☐ TOONS

Figure 241

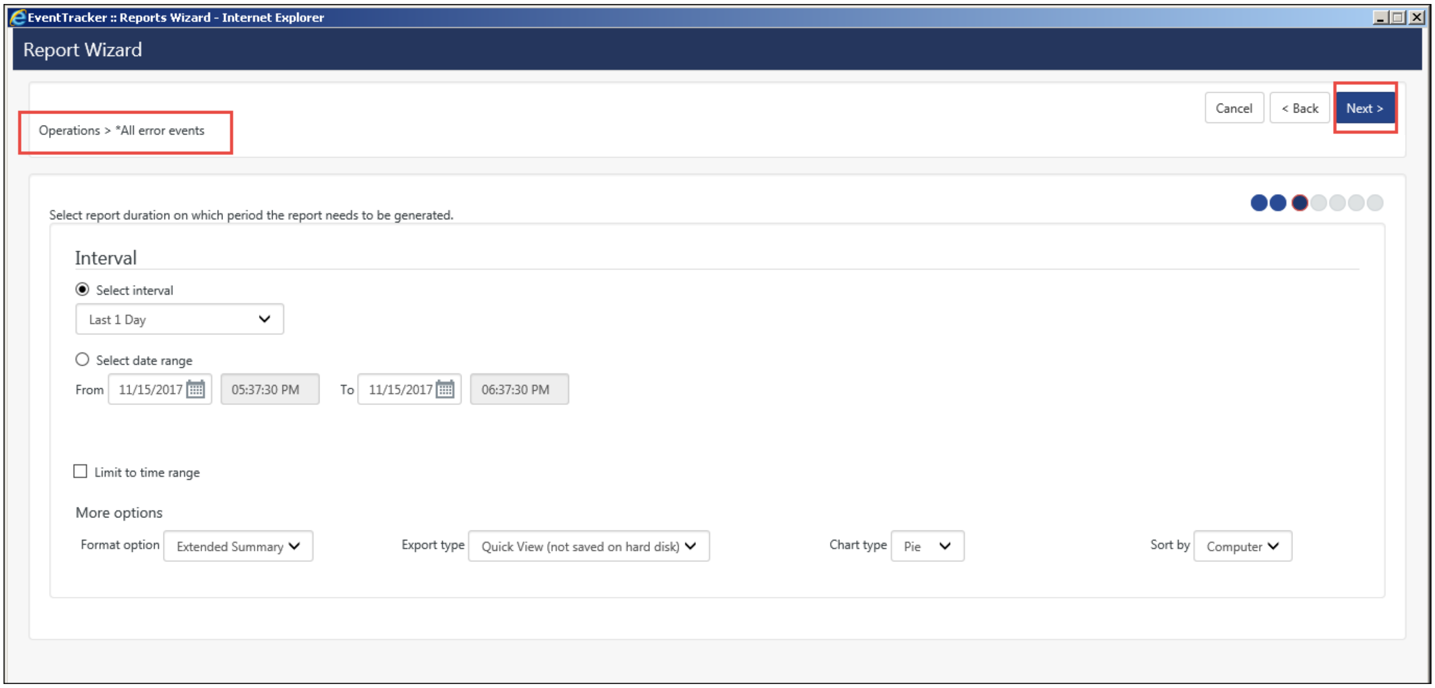
10 Select the required **Interval** and **Limit to time Range option.**

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. **Donut, Bar, Line graph).**

14 Select **Sort by (Computer or User).**



EventTracker :: Reports Wizard - Internet Explorer

Report Wizard

Operations > *All error events

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

Interval

● Select interval

Last 1 Day

○ Select date range

From 11/15/2017 05:37:30 PM To 11/15/2017 06:37:30 PM

☐ Limit to time range

More options

Format option: Extended Summary

Export type: Quick View (not saved on hard disk)

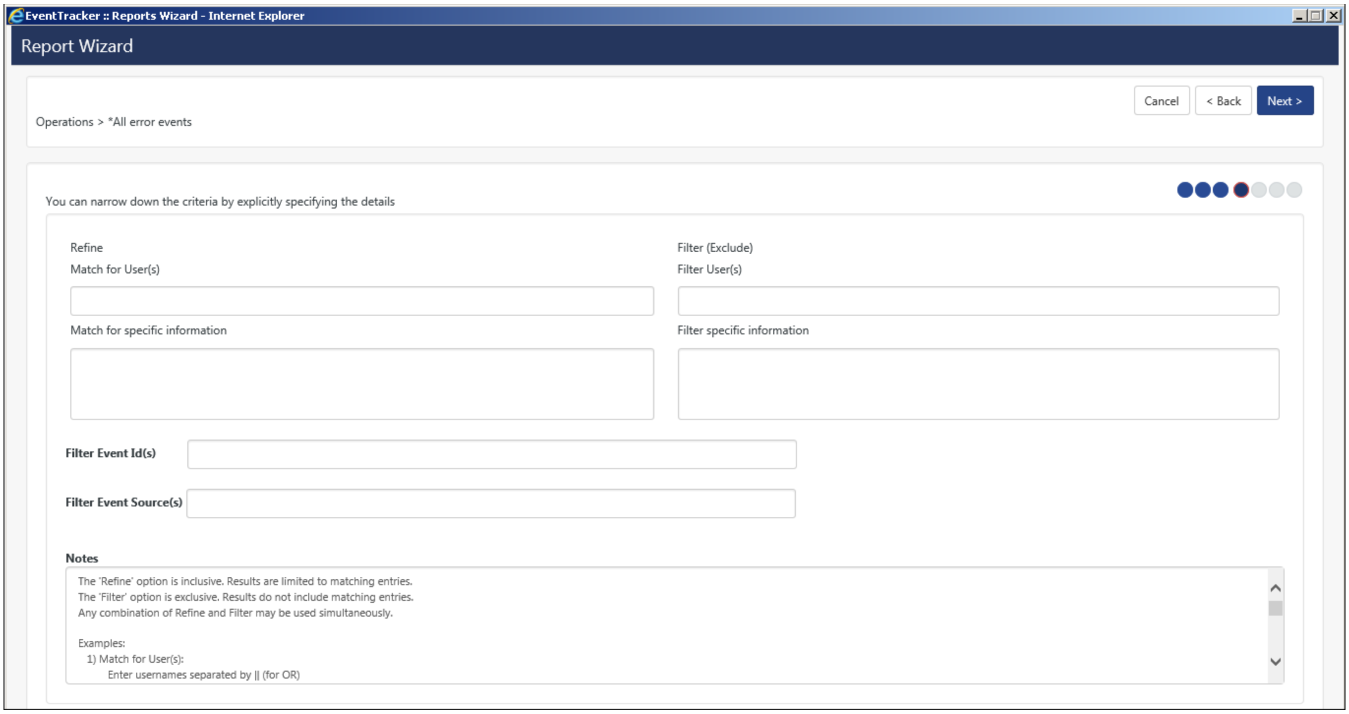
Chart type: Pie

Sort by: Computer

Figure 242

15 Click **Next>>**.

16 Enter the appropriate **Refine** and **Filter** details.



Operations > *All error events

You can narrow down the criteria by explicitly specifying the details

Refine
Match for User(s)

Match for specific information

Filter (Exclude)
Filter User(s)

Filter specific information

Filter Event Id(s)

Filter Event Source(s)

Notes

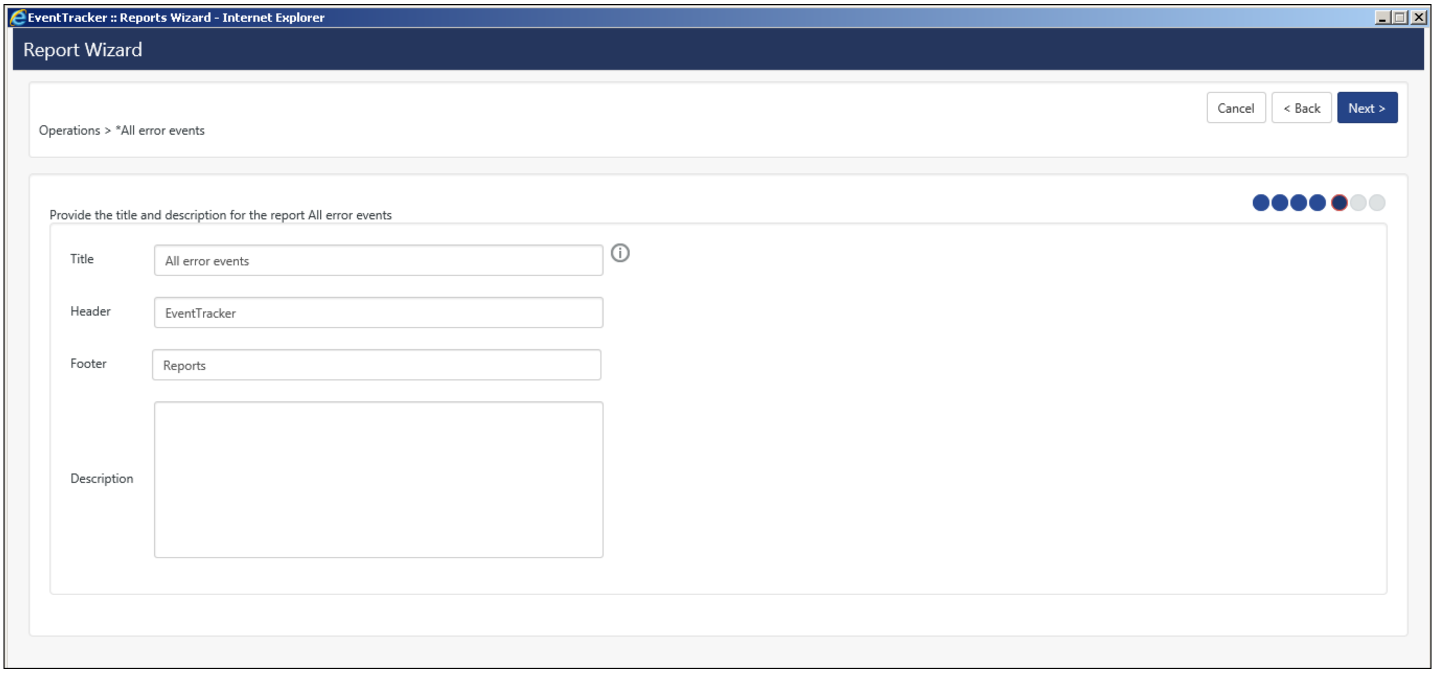
The 'Refine' option is inclusive. Results are limited to matching entries.
The 'Filter' option is exclusive. Results do not include matching entries.
Any combination of Refine and Filter may be used simultaneously.

Examples:
1) Match for User(s):
Enter usernames separated by || (for OR)

Figure 243

17 Click **Next>>**.

18 Enter the relevant **Title**, **Header**, **Footer**, and **Description** data.



Operations > *All error events

Provide the title and description for the report All error events

Title All error events

Header EventTracker

Footer Reports

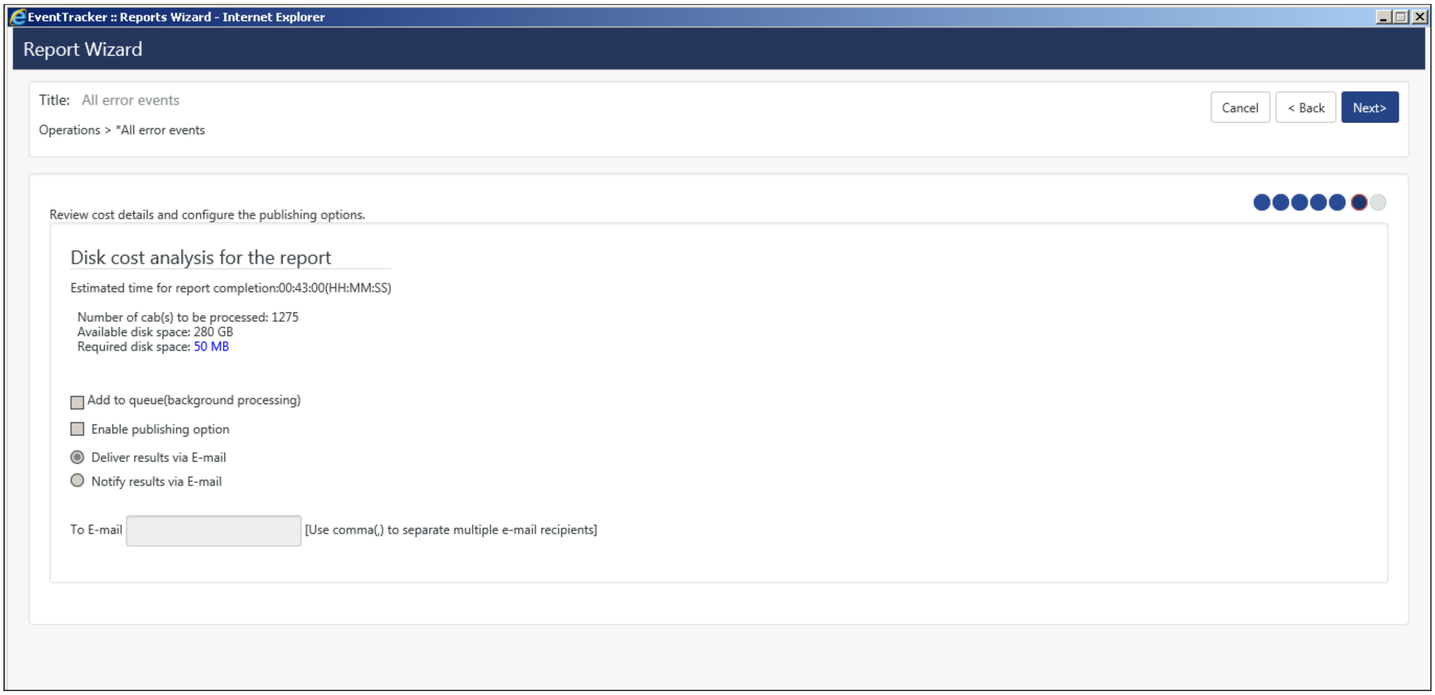
Description

Figure 244

19 Click **Next>>**.
Review cost details and configure the publishing options window opens.

NOTE

Publishing options are disabled because On Demand (foreground processing) has been selected.



Title: All error events

Operations > *All error events

Review cost details and configure the publishing options.

Disk cost analysis for the report

Estimated time for report completion:00:43:00(HH:MM:SS)

Number of cab(s) to be processed: 1275
Available disk space: 280 GB
Required disk space: 50 MB

□ Add to queue(background processing)

□ Enable publishing option

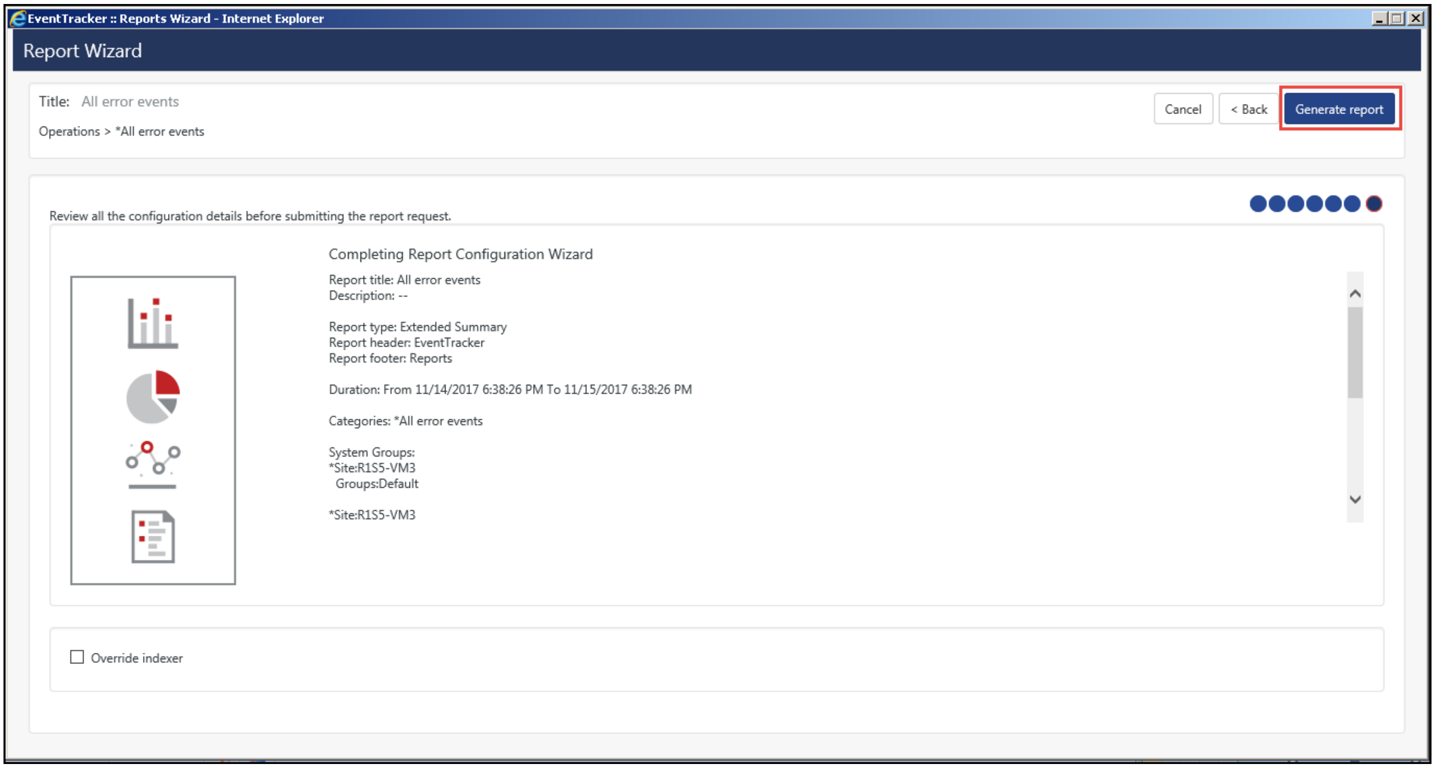
● Deliver results via E-mail

○ Notify results via E-mail

To E-mail [Use comma(,) to separate multiple e-mail recipients]

Figure 245

20 Click **Next>>**.
The last step of **Completing Report Configuration Wizard** opens.



Title: All error events

Operations > *All error events

Review all the configuration details before submitting the report request.

Completing Report Configuration Wizard

Report title: All error events
Description: --

Report type: Extended Summary
Report header: EventTracker
Report footer: Reports

Duration: From 11/14/2017 6:38:26 PM To 11/15/2017 6:38:26 PM

Categories: *All error events

System Groups:
*Site:R1S5-VM3
Groups:Default

*Site:R1S5-VM3

☐ Override indexer

Figure 246

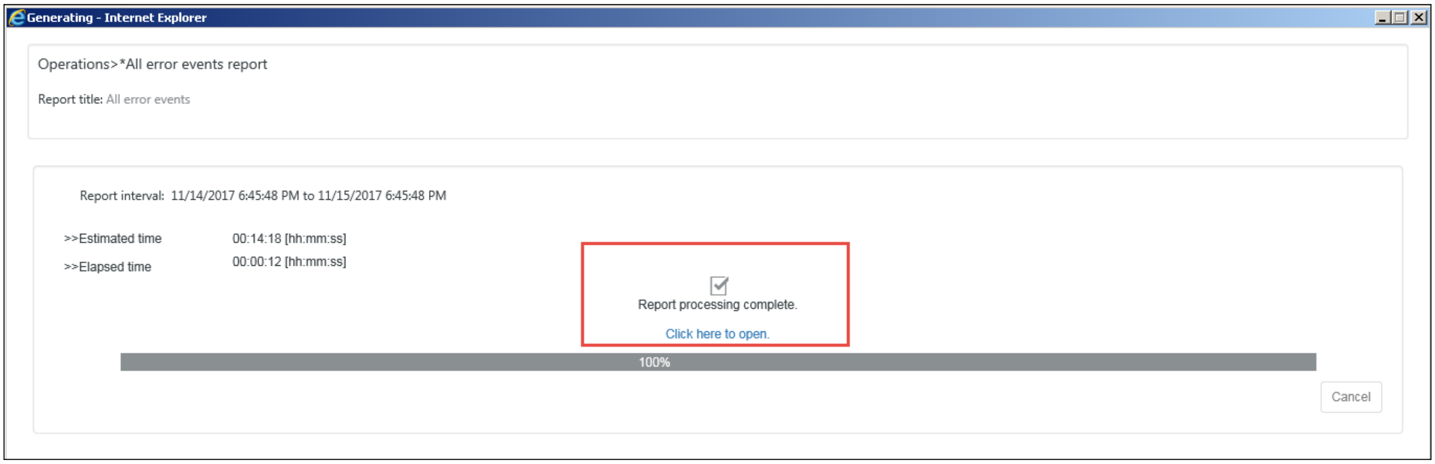
21 Select **Override indexer** if required, and then select **Generate Report.**

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 opens the initializing report queue and displays the summary of report generated.



Operations>*All error events report

Report title: All error events

Report interval: 11/14/2017 6:45:48 PM to 11/15/2017 6:45:48 PM

>>Estimated time 00:14:18 [hh:mm:ss]

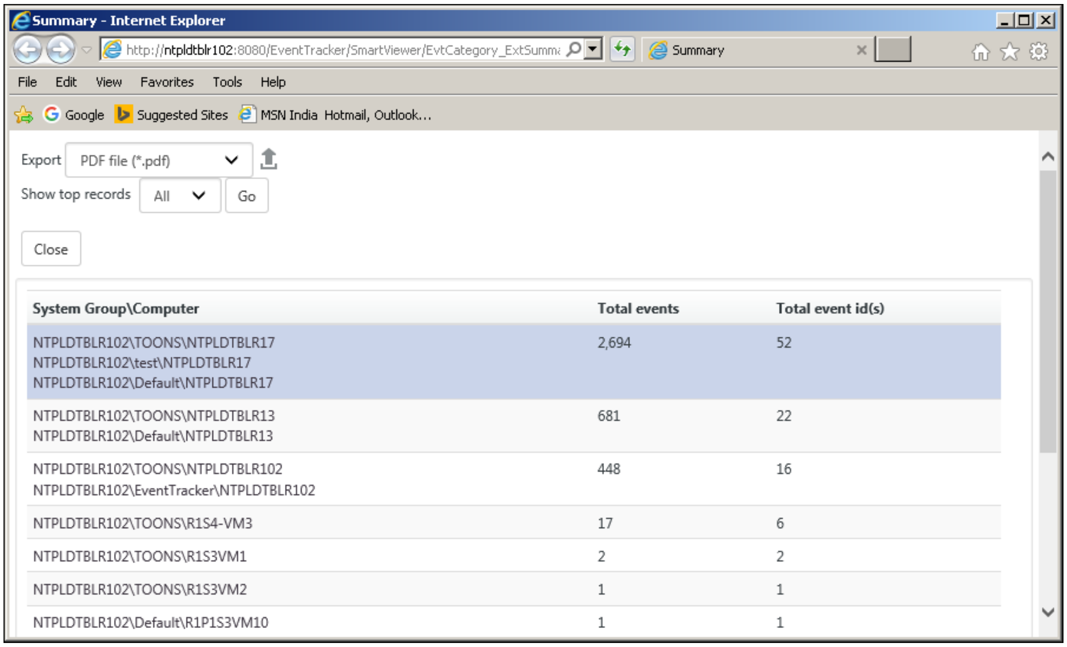
>>Elapsed time 00:00:12 [hh:mm:ss]

☑ Report processing complete.

Click here to open.

Figure 247

22 Click the hyperlink to view the report.


Summary - Internet Explorer
http://ntpldtblr102:8080/EventTracker/SmartViewer/EvtCategory_ExtSumm
Summary
File Edit View Favorites Tools Help
Google Suggested Sites MSN India Hotmail, Outlook...

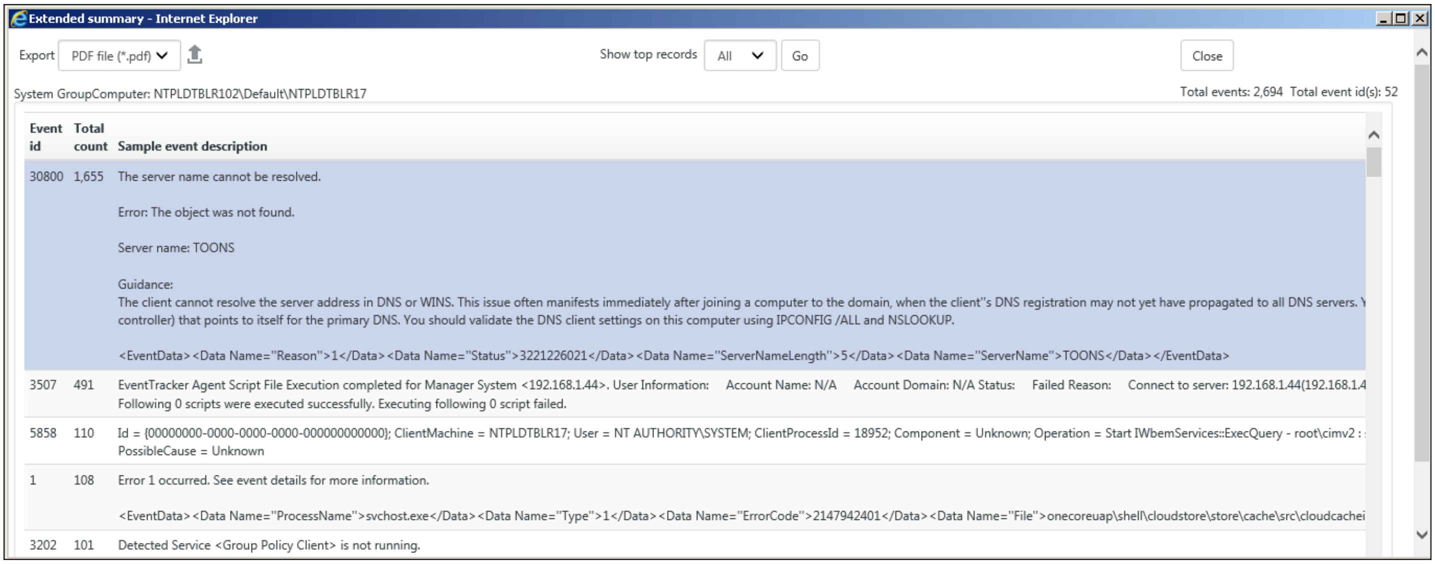
Export PDF file (*.pdf)

Show top records All Go

System Group\Computer	Total events	Total event id(s)
NTPLDTBLR102\TOONS\NTPLDTBLR17 NTPLDTBLR102\test\NTPLDTBLR17 NTPLDTBLR102\Default\NTPLDTBLR17	2,694	52
NTPLDTBLR102\TOONS\NTPLDTBLR13 NTPLDTBLR102\Default\NTPLDTBLR13	681	22
NTPLDTBLR102\TOONS\NTPLDTBLR102 NTPLDTBLR102\EventTracker\NTPLDTBLR102	448	16
NTPLDTBLR102\TOONS\R1S4-VM3	17	6
NTPLDTBLR102\TOONS\R1S3VM1	2	2
NTPLDTBLR102\TOONS\R1S3VM2	1	1
NTPLDTBLR102\Default\R1P1S3VM10	1	1

Figure 248

23 Select any one of the **System Group\Computer** hyperlinks to view detail information.



Extended summary - Internet Explorer

Export PDF file (*.pdf) Show top records All Go Close

System GroupComputer: NTPLDTBLR102\Default\NTPLDTBLR17

Total events: 2,694 Total event id(s): 52

Event id	Total count	Sample event description
30800	1,655	The server name cannot be resolved. Error: The object was not found. Server name: TOONS Guidance: The client cannot resolve the server address in DNS or WINS. This issue often manifests immediately after joining a computer to the domain, when the client''s DNS registration may not yet have propagated to all DNS servers. Y controller) that points to itself for the primary DNS. You should validate the DNS client settings on this computer using IPCONFIG /ALL and NSLOOKUP. <EventData><Data Name="Reason">1</Data><Data Name="Status">3221226021</Data><Data Name="ServerNameLength">5</Data><Data Name="ServerName">TOONS</Data></EventData>
3507	491	EventTracker Agent Script File Execution completed for Manager System <192.168.1.44>. User Information: Account Name: N/A Account Domain: N/A Status: Failed Reason: Connect to server: 192.168.1.44(192.168.1.4 Following 0 scripts were executed successfully. Executing following 0 script failed.
5858	110	Id = {00000000-0000-0000-0000-000000000000}; ClientMachine = NTPLDTBLR17; User = NT AUTHORITY\SYSTEM; ClientProcessId = 18952; Component = Unknown; Operation = Start IWbemServices::ExecQuery - root\cimv2 : PossibleCause = Unknown
1	108	Error 1 occurred. See event details for more information. <EventData><Data Name="ProcessName">svchost.exe</Data><Data Name="Type">1</Data><Data Name="ErrorCode">2147942401</Data><Data Name="File">onecoreuap\shell\cloudstore\store\cache\src\cloudcachei
3202	101	Detected Service <Group Policy Client> is not running.

Figure 249

4.6 Generating Queued Reports

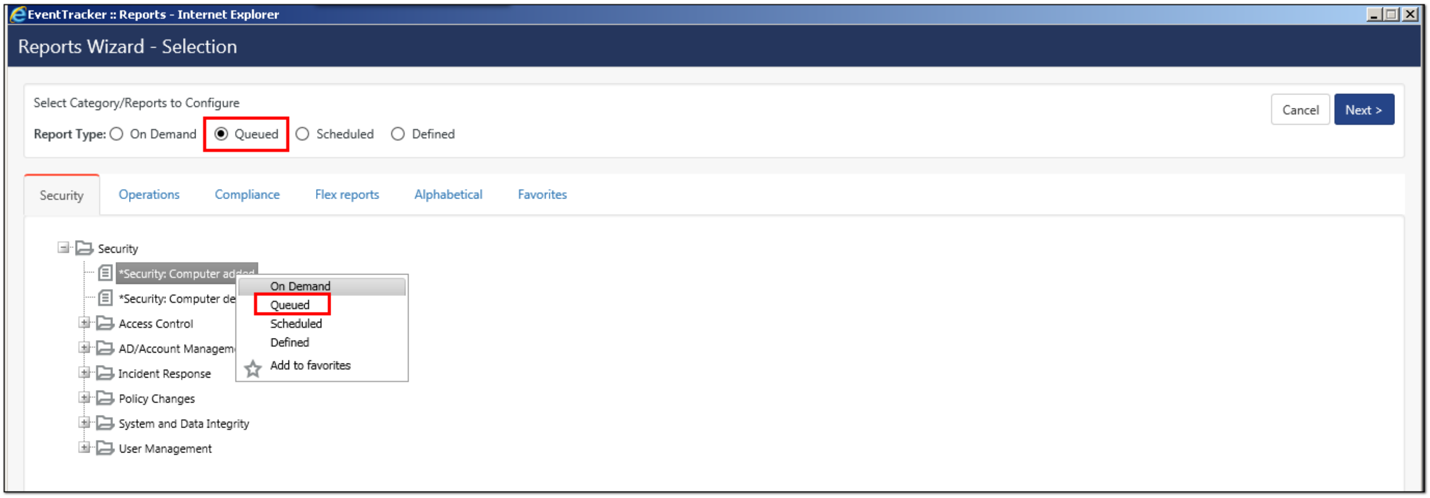
Reports that are generated in the background are called **Queued** reports.

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

2 Click **New** ⊕ 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** ▶ .



EventTracker :: Reports - Internet Explorer

Reports Wizard - Selection

Select Category/Reports to Configure

Report Type: ○ On Demand ● Queued ○ Scheduled ○ Defined

Figure 250

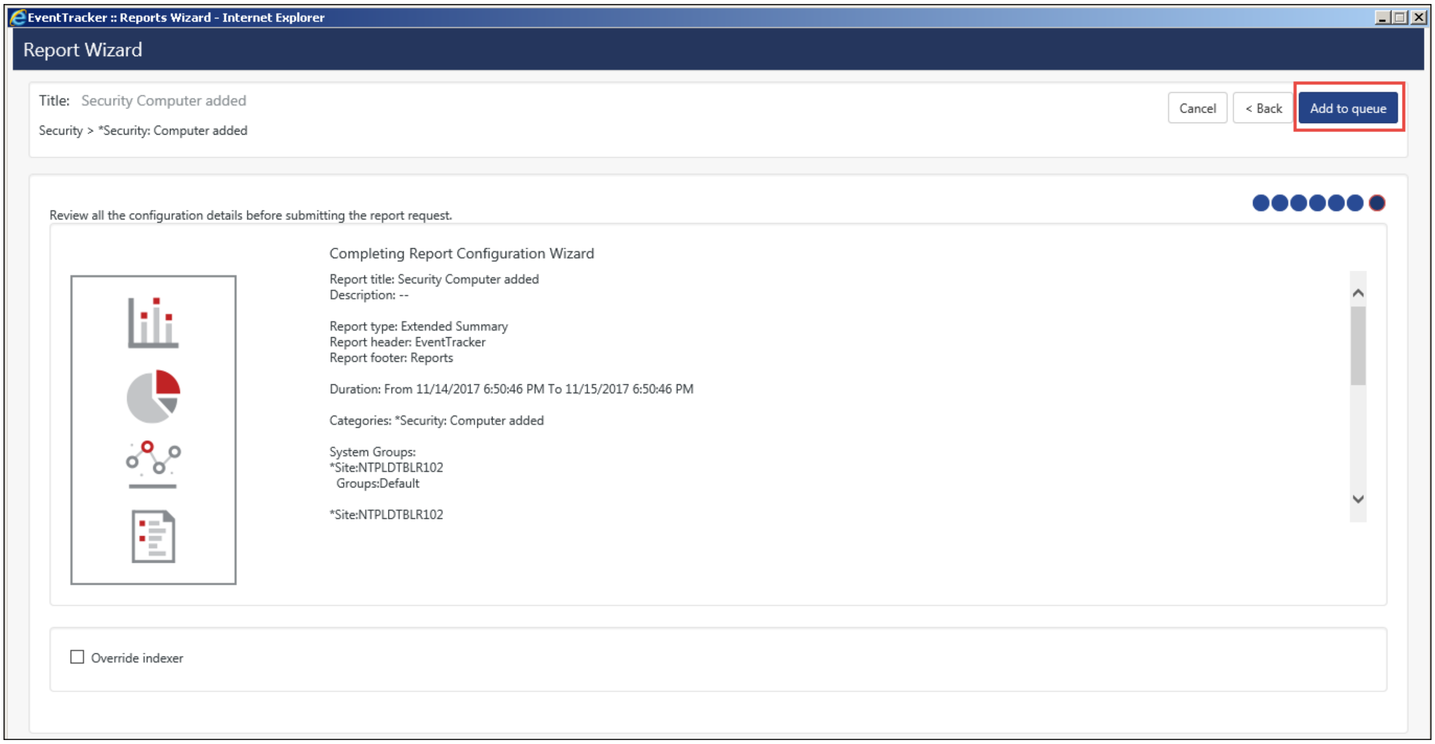
3 Select any one of the **Compliance / Security / Operations / Flex reports / Alphabetical** tab.

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 opens 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.
The last step of Reports Wizard opens.



Title: Security Computer added
Security > *Security: Computer added

Review all the configuration details before submitting the report request.

Completing Report Configuration Wizard
Report title: Security Computer added
Description: --

Report type: Extended Summary
Report header: EventTracker
Report footer: Reports

Duration: From 11/14/2017 6:50:46 PM To 11/15/2017 6:50:46 PM

Categories: *Security: Computer added

System Groups:
*Site:NTPLDTBLR102
Groups:Default

*Site:NTPLDTBLR102

☐ Override indexer

Figure 251

12 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.

4.7 Generating Scheduled Reports

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

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

2 Click **New** ⊕ 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**.
Example: In '**Flex Reports'** Report Tree, select **Logs**, select **Summary**. Report Type selected is **Scheduled**.

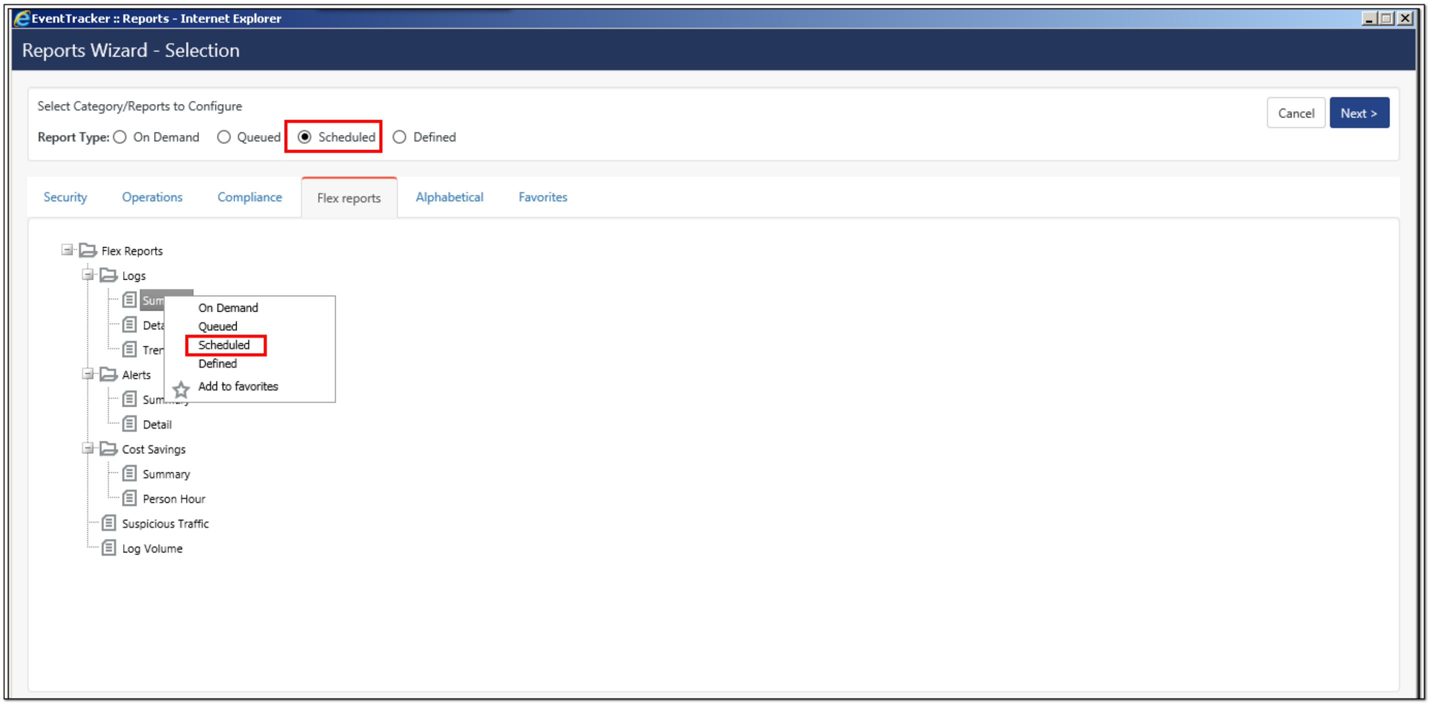


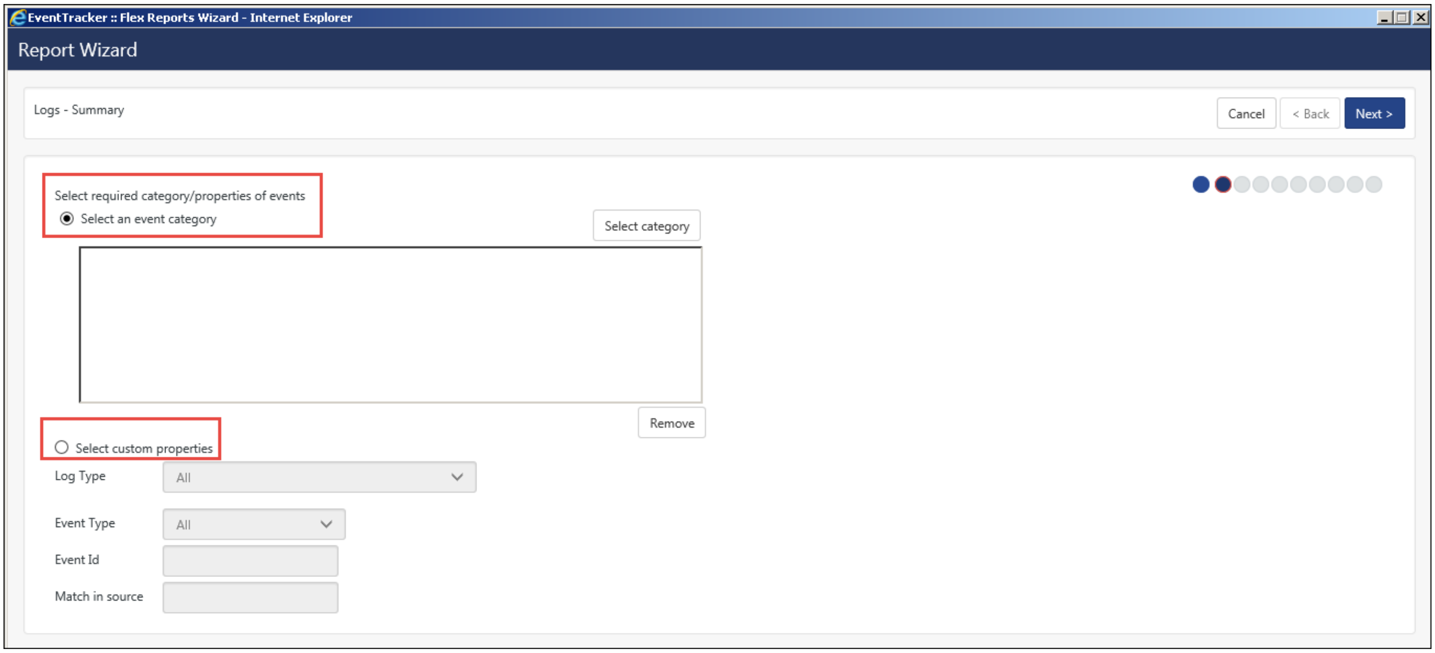
Figure 252

6 Click **Next.**

EventTracker opens the Reports Wizard.

7 Click **Next >>.**

8 Select the required **Select an event category** or **Select custom properties** option. Also select the required **Log Type**, and then click **Next >>** button.


EventTracker :: Flex Reports Wizard - Internet Explorer

Report Wizard

Logs - Summary

Select required category/properties of events

● Select an event category

○ Select custom properties

Log Type: All

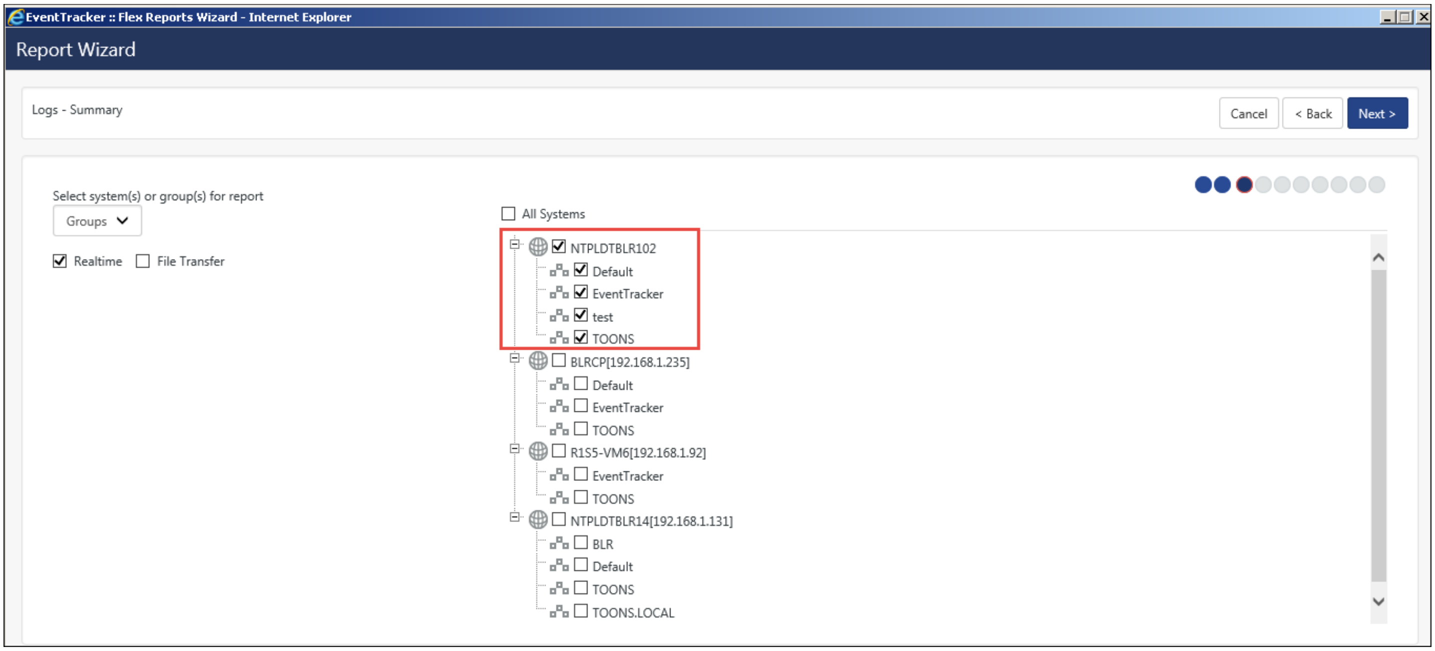
Event Type: All

Event Id

Match in source

Figure 253

9 In **Select system(s) or group(s) for report** pane, select the appropriate options and then click **Next>>.**


EventTracker :: Flex Reports Wizard - Internet Explorer

Report Wizard

Logs - Summary

Select system(s) or group(s) for report: Groups

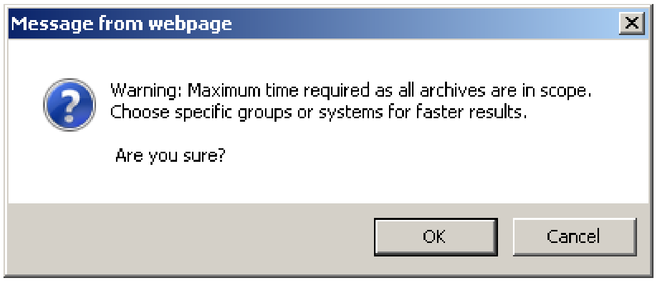
☑ Realtime ☐ File Transfer

☐ All Systems

- ☑ NTPLDTBLR102
  - ☑ Default
  - ☑ EventTracker
  - ☑ test
  - ☑ TOONS
- ☐ BLRCP[192.168.1.235]
  - ☐ Default
  - ☐ EventTracker
  - ☐ TOONS
- ☐ R1S5-VM6[192.168.1.92]
  - ☐ EventTracker
  - ☐ TOONS
- ☐ NTPLDTBLR14[192.168.1.131]
  - ☐ BLR
  - ☐ Default
  - ☐ TOONS
  - ☐ TOONS.LOCAL

Figure 254

A warning message opens.



Message from webpage

Warning: Maximum time required as all archives are in scope. Choose specific groups or systems for faster results.

Are you sure?

Figure 255

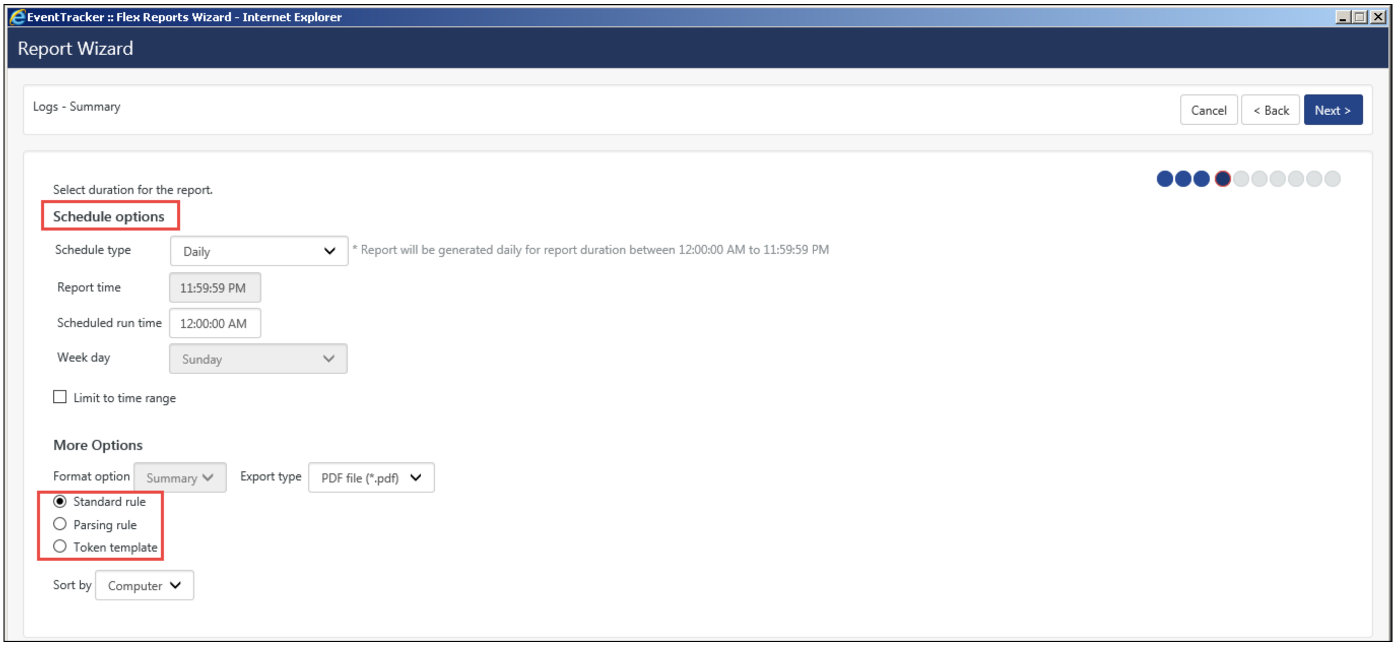
10 Click **OK**.

11 In **Select duration for the report** pane, select the appropriate **Schedule options (Schedule Type:, Report Time:, Schedule Run Time:,).**

Schedule type can be selected as **Daily/Last 24 hours/Twice Daily/Weekly/Last 1 Week/Once in a week/Hourly/Monthly.**

- "**Daily**" report type will have report time of 11:59:59 PM by default.
- For "**Last 24 hours**" type user can specify report time.
- "**Weekly**" selected report type will be from Sunday 12:00:00 AM to Next Saturday 11:59:59 PM.
- For "**Last 1 week**" Report type, user can select Report time, Scheduled run time and day of week and all other options remain same.
- If Schedule Type selected is **Monthly**, then an option to select date range and time range is provided i.e. **Limit to date range and Limit to time range.**

12 Select the required **Format option (Standard Rule, Parsing Rule, Token Template), Export type, Sort by Computer or User.**



EventTracker :: Flex Reports Wizard - Internet Explorer

Report Wizard

Logs - Summary

Select duration for the report.

Schedule options

Schedule type: Daily

* Report will be generated daily for report duration between 12:00:00 AM to 11:59:59 PM

Report time: 11:59:59 PM

Scheduled run time: 12:00:00 AM

Week day: Sunday

□ Limit to time range

More Options

Format option: Summary

Export type: PDF file (*.pdf)

● Standard rule

○ Parsing rule

○ Token template

Sort by: Computer

Figure 256

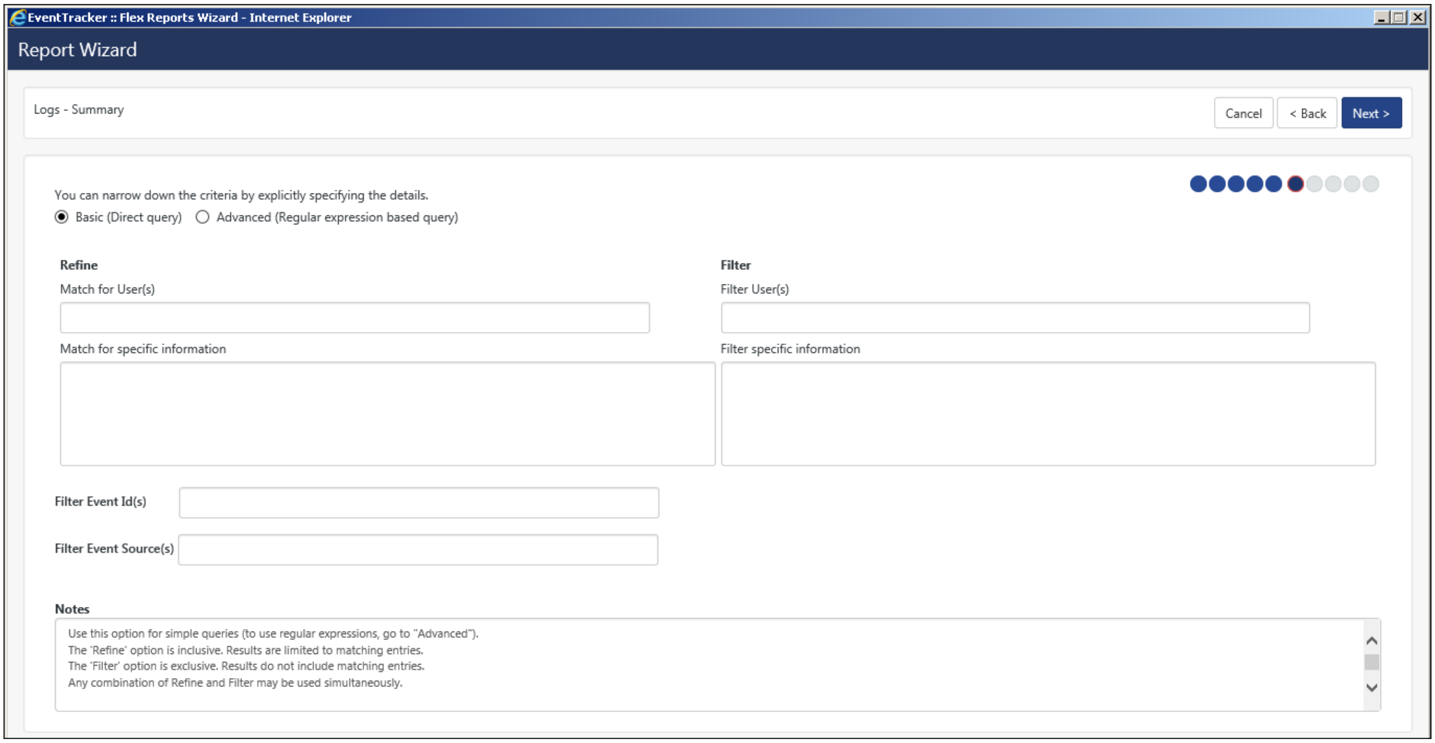
Parsing Rule and Token Template is explained in detail in Parsing Rules.

13 Click **Next>>.**

14 Select the required **Refine** and **Filter** Details.

NOTE

- The transferred TLS reports from Collection Point will not display the selected reports, on clicking the information icon in Collection Master, in case the main reports are selected for transferring in Collection Point.
- For a Fresh environment, i.e. v9.1, the user can generate report for only PDF and Excel export types. Even for Export Import Utility, the user can generate only PDF and Excel reports.
- For an upgrade from older version to v9.0, the earlier configured report (HTML and DOCX), the reports will be generated in HTML and DOCX export types, until the user edits the reports and saves the changed configuration. The user can also generate the earlier configured report (HTML & DOCX) in the newer version, by importing it from EventTracker Control Panel> Export Import Utility.



You can narrow down the criteria by explicitly specifying the details.

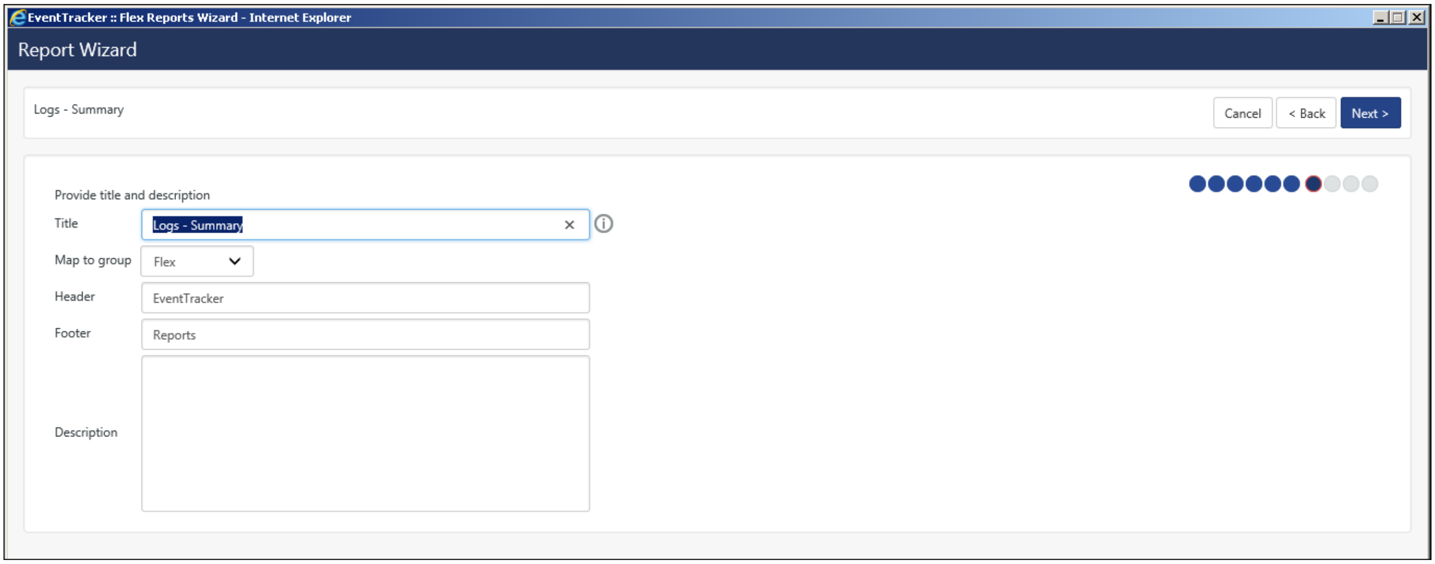
● Basic (Direct query) ○ Advanced (Regular expression based query)

Use this option for simple queries (to use regular expressions, go to "Advanced").
The 'Refine' option is inclusive. Results are limited to matching entries.
The 'Filter' option is exclusive. Results do not include matching entries.
Any combination of Refine and Filter may be used simultaneously.

Figure 257

15 Click **Next>>.**

16 Enter the appropriate **Title, Header** and **Footer** details.



Logs - Summary

Provide title and description

Title: Logs - Summary

Map to group: Flex

Header: EventTracker

Footer: Reports

Description:

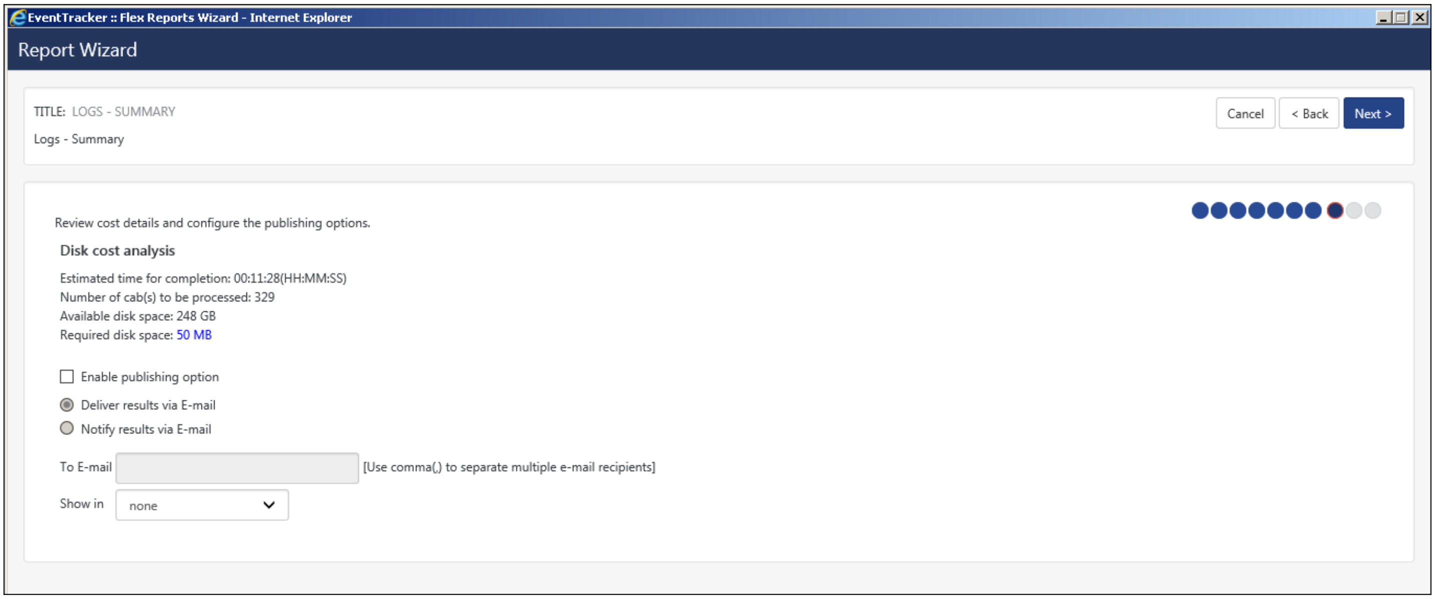
Figure 258

17 In **Map to group** drop-down, you can select the required groups.

18 Click **Next>>.**

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

20 Select **Update status via RSS:** feed drop down. Select **Show in Compliance Dashboard** if required.



TITLE: LOGS - SUMMARY

Logs - Summary

Review cost details and configure the publishing options.

Disk cost analysis

Estimated time for completion: 00:11:28(HH:MM:SS)
Number of cab(s) to be processed: 329
Available disk space: 248 GB
Required disk space: 50 MB

☐ Enable publishing option

● Deliver results via E-mail

○ Notify results via E-mail

To E-mail [Use comma(,) to separate multiple e-mail recipients]

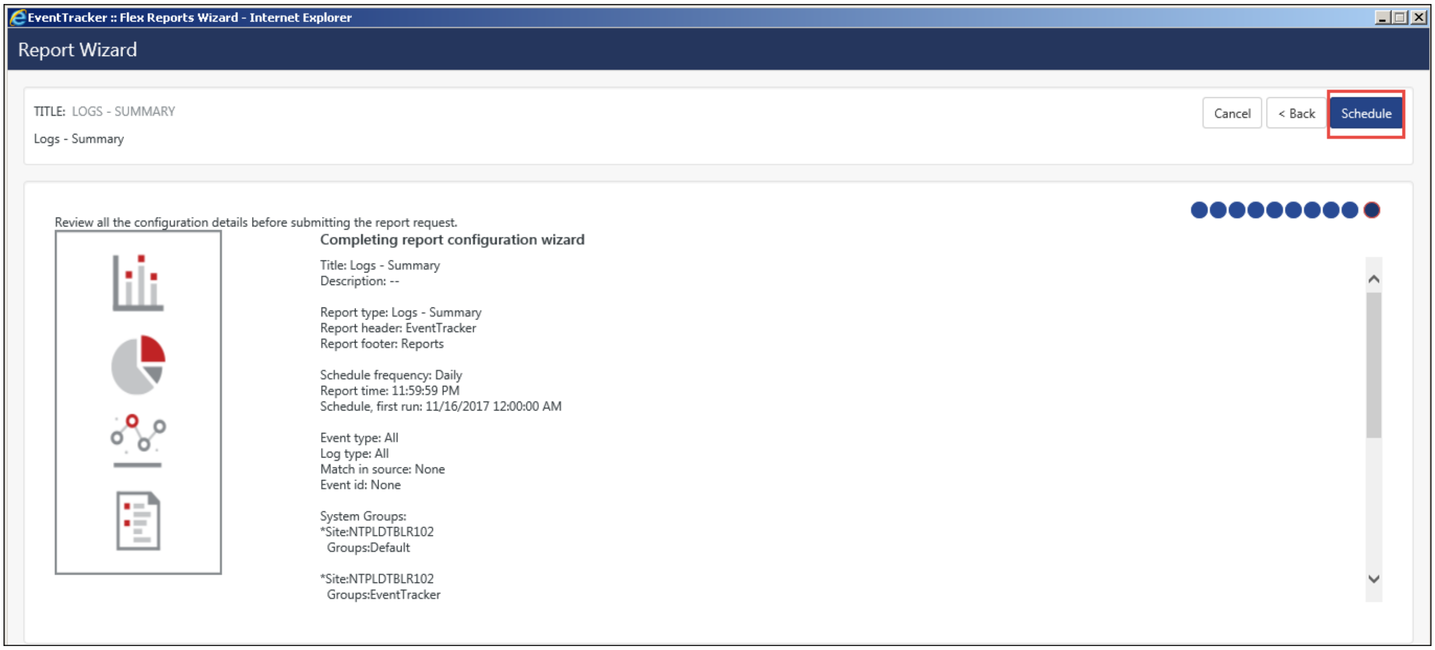
Show in: none

Figure 259

21 Click **Next>>.**

The last step of Report Configuration wizard displays.

22 Select **Schedule**.



TITLE: LOGS - SUMMARY
Logs - Summary

Review all the configuration details before submitting the report request.

Completing report configuration wizard

Title: Logs - Summary
Description: --

Report type: Logs - Summary
Report header: EventTracker
Report footer: Reports

Schedule frequency: Daily
Report time: 11:59:59 PM
Schedule, first run: 11/16/2017 12:00:00 AM

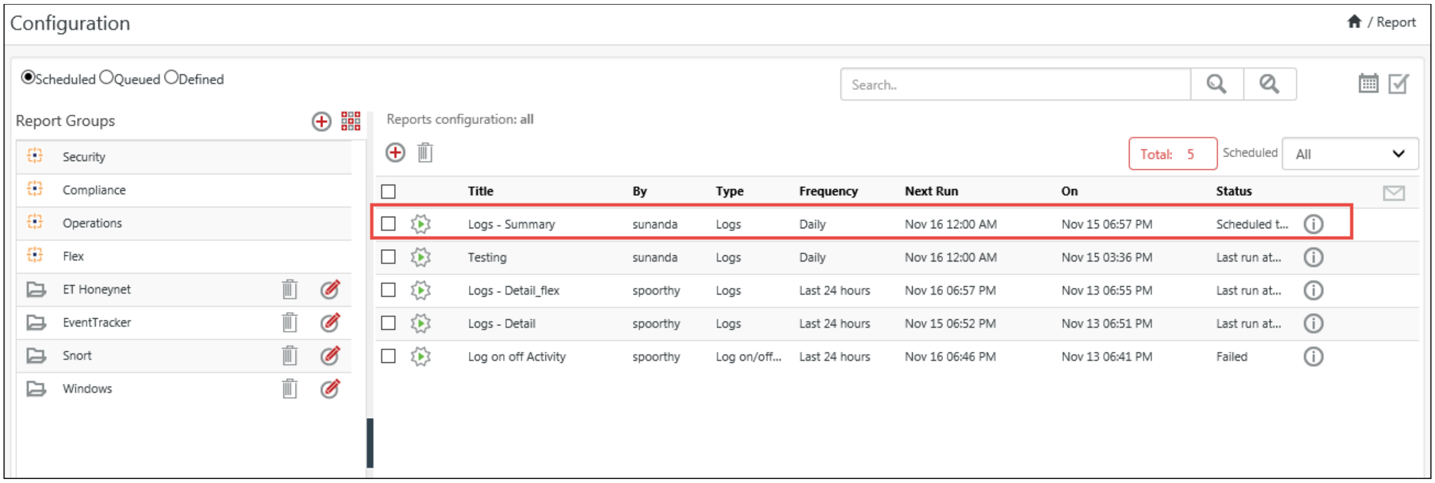
Event type: All
Log type: All
Match in source: None
Event id: None

System Groups:
*Site:NTPLDTBLR102
Groups:Default

*Site:NTPLDTBLR102
Groups:EventTracker

Figure 260

The corresponding report opens in the Reports Configuration.



	Title	By	Type	Frequency	Next Run	On	Status
□	Logs - Summary	sunanda	Logs	Daily	Nov 16 12:00 AM	Nov 15 06:57 PM	Scheduled t...
□	Testing	sunanda	Logs	Daily	Nov 16 12:00 AM	Nov 15 03:36 PM	Last run at...
□	Logs - Detail_flex	spoorthy	Logs	Last 24 hours	Nov 16 06:57 PM	Nov 13 06:55 PM	Last run at...
□	Logs - Detail	spoorthy	Logs	Last 24 hours	Nov 15 06:52 PM	Nov 13 06:51 PM	Last run at...
□	Log on off Activity	spoorthy	Log on/off...	Last 24 hours	Nov 16 06:46 PM	Nov 13 06:41 PM	Failed

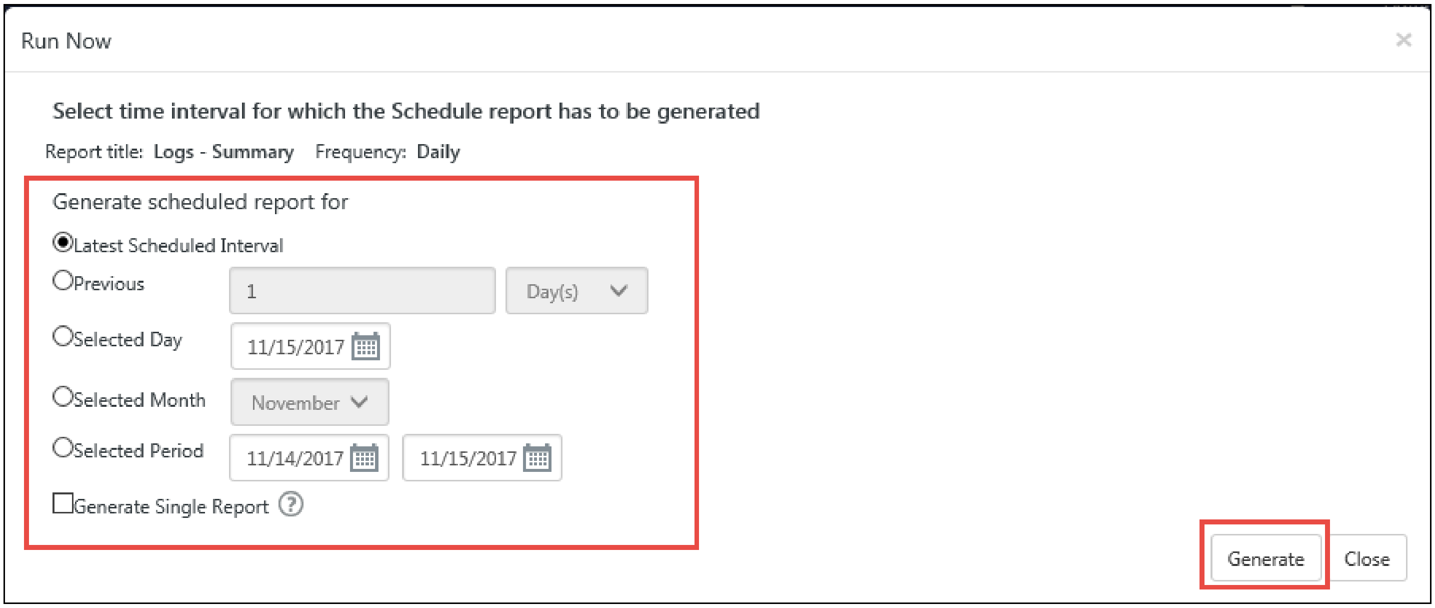
Figure 261

4.7.1 Scheduled Reports - Run Now

A new option has been added for the user to generate a single or multiple report based on the duration selected and the type (daily/weekly etc...) in scheduled reports. Instead of generating 7 daily reports for a week, a single consolidated report can be generated.

1. Select **Scheduled** option, and then select **Run Now** .

   Scheduled run now window opens:



Run Now

Select time interval for which the Schedule report has to be generated

Report title: Logs - Summary Frequency: Daily

Generate scheduled report for

● Latest Scheduled Interval

○ Previous 1 Day(s)

○ Selected Day 11/15/2017

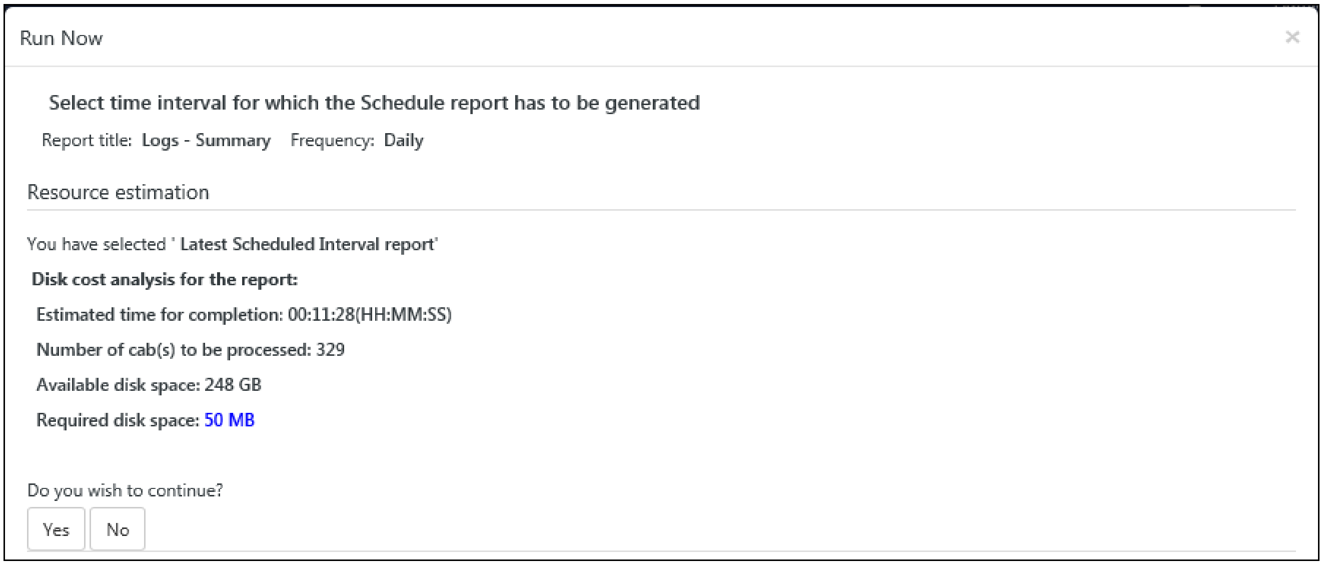
○ Selected Month November

○ Selected Period 11/14/2017 11/15/2017

□ Generate Single Report

Figure 262

2. In **Generate scheduled report for** pane, select the required duration.
   In our example we are selecting **Previous 4 weeks.**
3. Select **Generate Single Report option.**
4. Select **Help** ⓘ for additional information.
5. Select the **Generate** button.



Run Now

Select time interval for which the Schedule report has to be generated

Report title: Logs - Summary Frequency: Daily

Resource estimation

You have selected ' Latest Scheduled Interval report'

Disk cost analysis for the report:

Estimated time for completion: 00:11:28(HH:MM:SS)

Number of cab(s) to be processed: 329

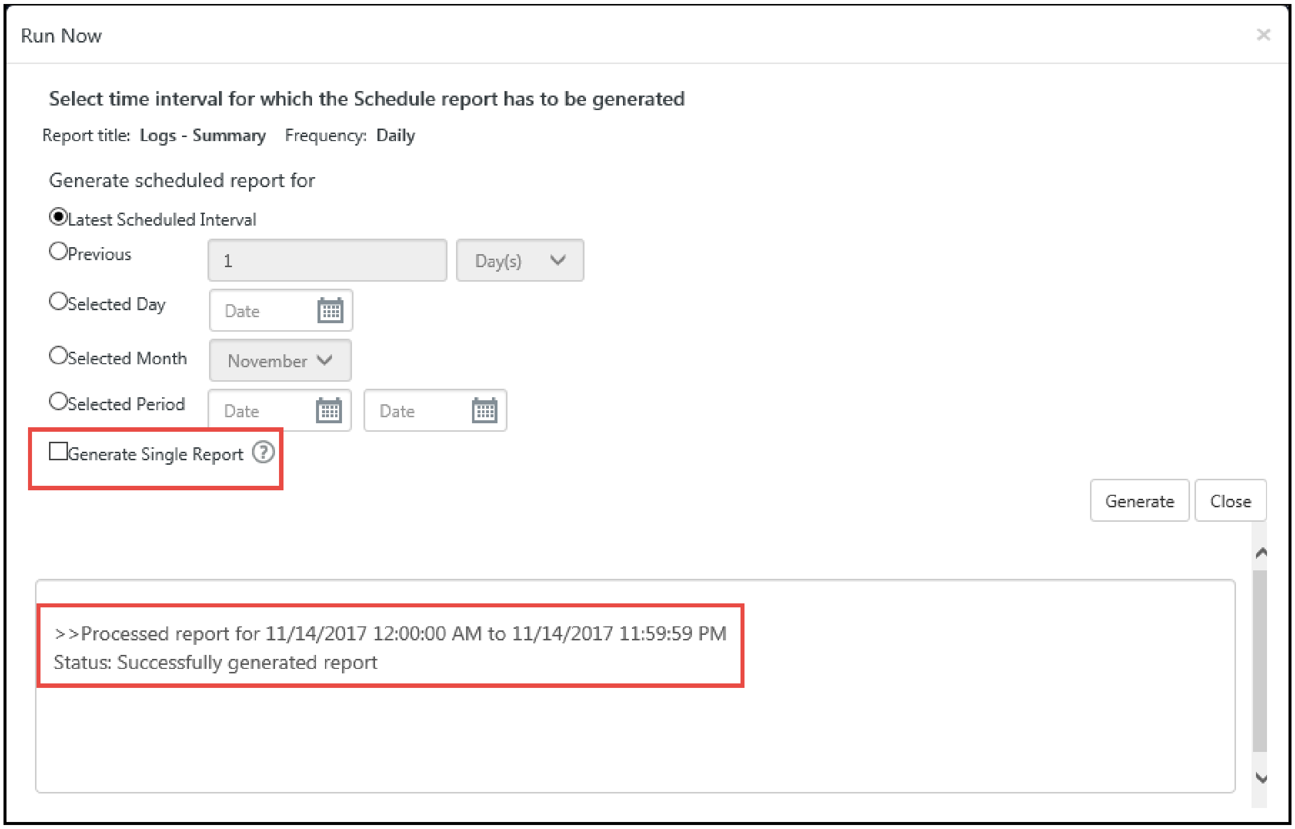
Available disk space: 248 GB

Required disk space: 50 MB

Do you wish to continue?

Figure 263

6. Verify **Resource estimation** and then select **Yes**.
   Once the report is generated successfully, a message opens.



Run Now

Select time interval for which the Schedule report has to be generated

Report title: Logs - Summary Frequency: Daily

Generate scheduled report for

● Latest Scheduled Interval

○ Previous 1 Day(s)

○ Selected Day Date

○ Selected Month November

○ Selected Period Date Date

□ Generate Single Report

```
>>Processed report for 11/14/2017 12:00:00 AM to 11/14/2017 11:59:59 PM
Status: Successfully generated report
```

Figure 264

You can view the result in Reports dashboard.

4.8 Generating defined reports

Defined reports are used to generate the reports immediately.

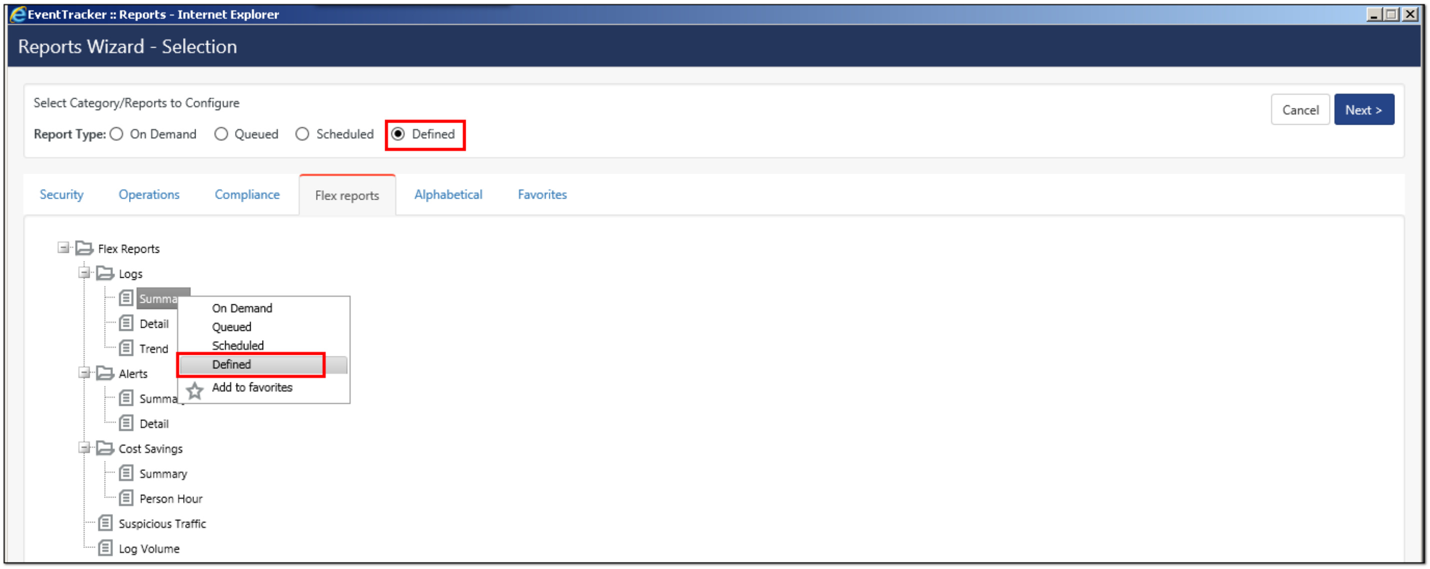
1 Log on to EventTracker and then click the **Reports** menu.

2 Click **New** ⊕ in **Dashboard / Configuration**.

3 Select **Defined**, and then select **New** ⊕ .

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.**



EventTracker :: Reports - Internet Explorer

Reports Wizard - Selection

Select Category/Reports to Configure

Report Type: ○ On Demand ○ Queued ○ Scheduled ● Defined

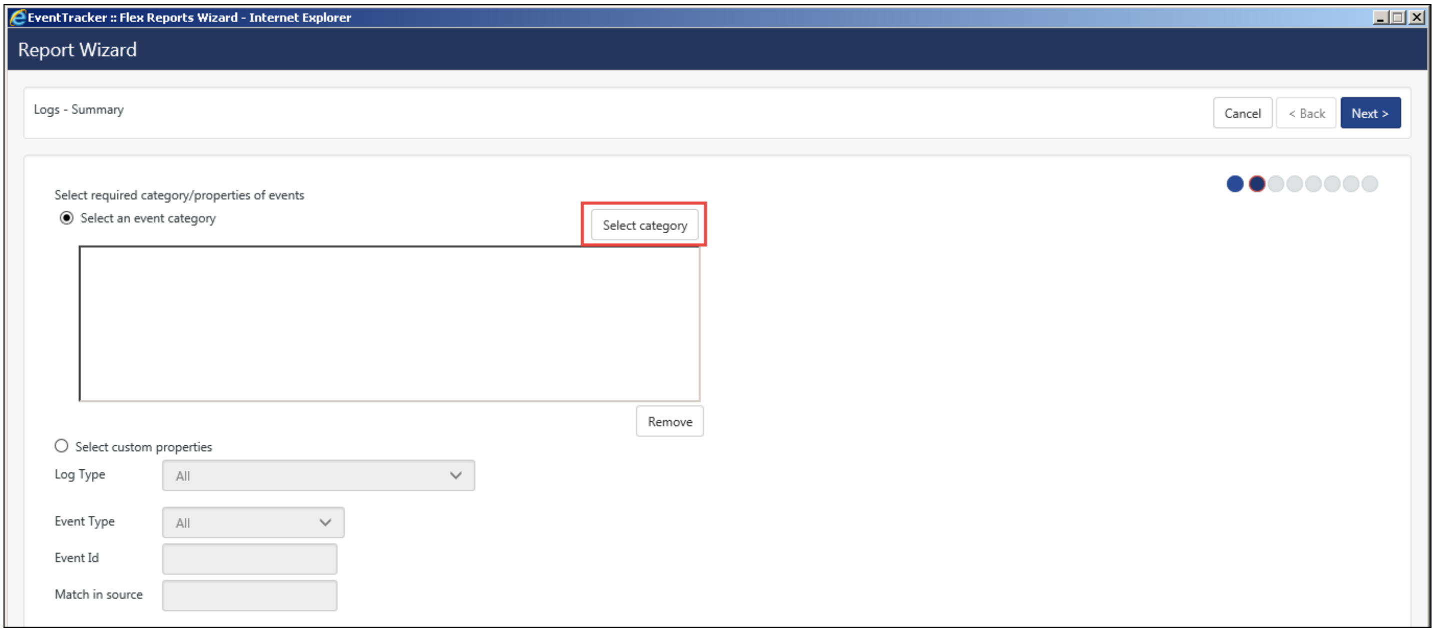
Figure 265

6 Select **Next**.

EventTracker opens the Reports Wizard.

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

a) If **Select and event category** is checked, then Click **Select Category** hyperlink.



EventTracker :: Flex Reports Wizard - Internet Explorer

Report Wizard

Logs - Summary

Select required category/properties of events

● Select an event category

○ Select custom properties

Log Type: All

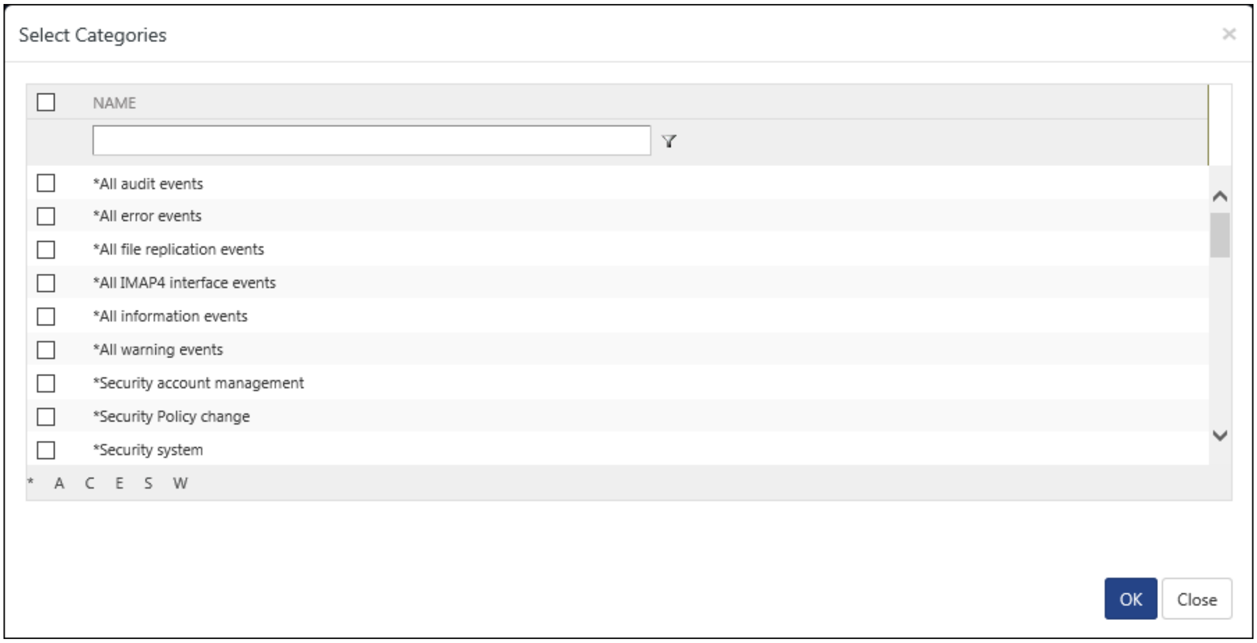
Event Type: All

Event Id:

Match in source:

Figure 266

Categories window opens.



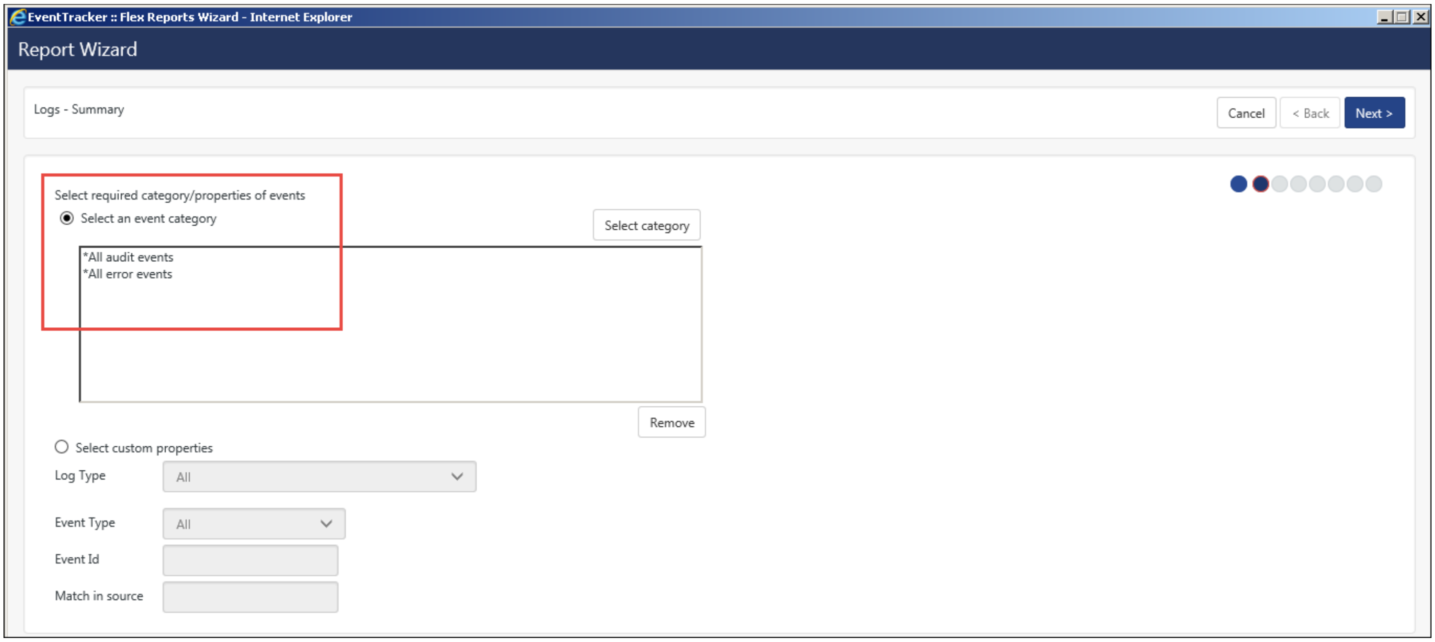
Select Categories

□	NAME
□	*All audit events
□	*All error events
□	*All file replication events
□	*All IMAP4 interface events
□	*All information events
□	*All warning events
□	*Security account management
□	*Security Policy change
□	*Security system

Figure 267

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

In this example, all categories are selected.



Select required category/properties of events

● Select an event category

*All audit events
*All error events

○ Select custom properties

Log Type: All

Event Type: All

Event Id:

Match in source:

Figure 268

(OR)

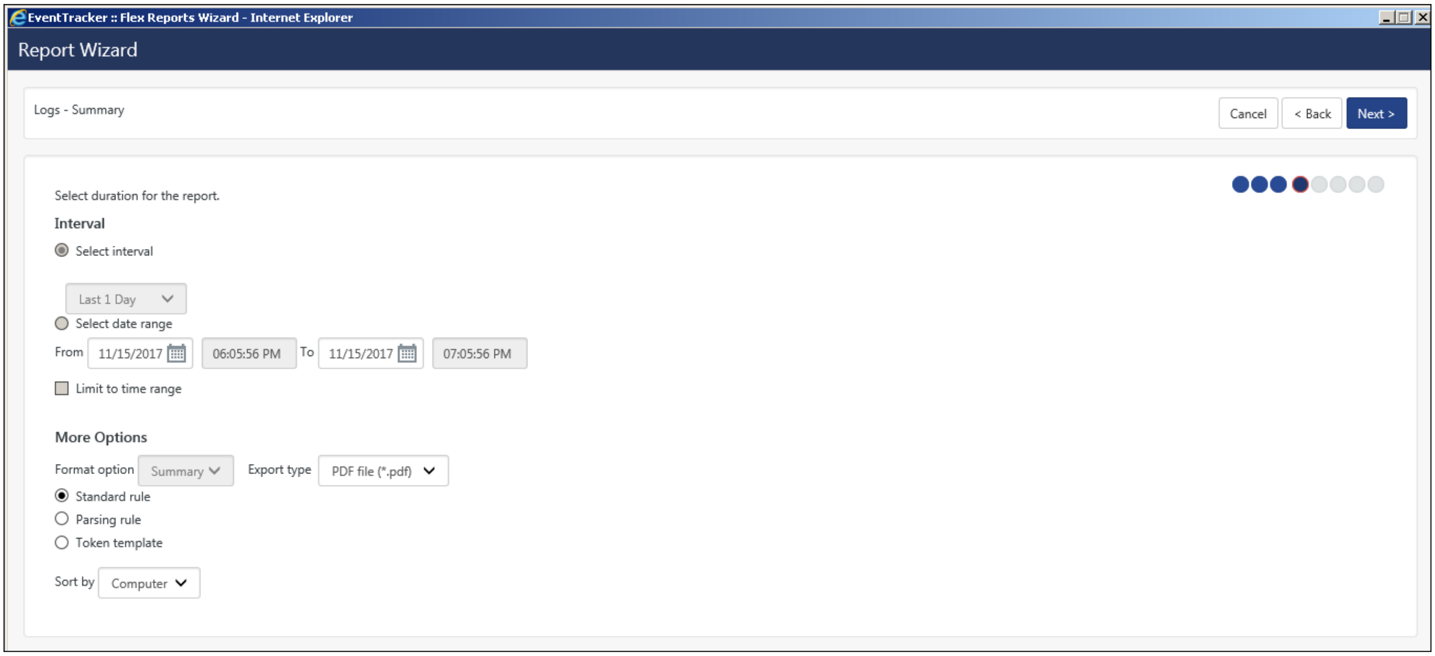
i. Select **Select custom properties** option.

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

8 Click **Next>>.**

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

10 Select the duration of the report.



Select duration for the report.

Interval

● Select interval

Last 1 Day

○ Select date range

From 11/15/2017 06:05:56 PM To 11/15/2017 07:05:56 PM

□ Limit to time range

More Options

Format option Summary Export type PDF file (*.pdf)

● Standard rule

○ Parsing rule

○ Token template

Sort by Computer

Figure 269

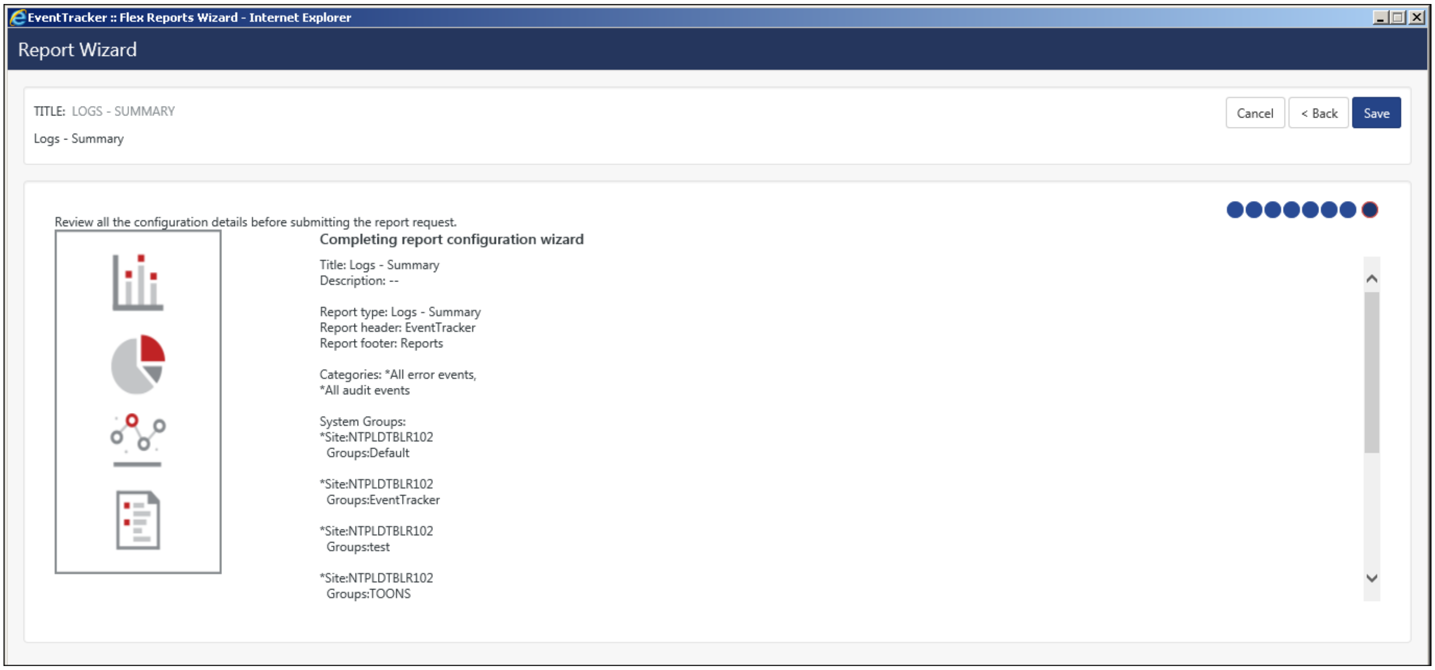
11 Select the required **Refine** and **Filter (Exclude)** details, and then click **Next>>.**

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

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

14 Select **Update status via RSS:** feed drop down. Select **Show in Compliance Dashboard** if required.

15 In the last step of Report Configuration Wizard, select **Save.**



TITLE: LOGS - SUMMARY
Logs - Summary

Review all the configuration details before submitting the report request.

Completing report configuration wizard

Title: Logs - Summary
Description: --

Report type: Logs - Summary
Report header: EventTracker
Report footer: Reports

Categories: *All error events,
*All audit events

System Groups:
*Site:NTPLDTBLR102
Groups:Default

*Site:NTPLDTBLR102
Groups:EventTracker

*Site:NTPLDTBLR102
Groups:test

*Site:NTPLDTBLR102
Groups:TOONS

Figure: 270

The corresponding report displays in **Security** window.

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

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

4.9 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 and Excel formats.

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

4.10 Reporting 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.

4.11 Refine and Filter Options

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

Field	Description
Refine: Use this option if you are looking for specific information.	
Match for User(s)	This field can take multiple strings separated by ||. || Stands for OR condition. Example- If you wish to generate a Log on/off Activity report for a specific user named "John" then, just enter John in the 'Match for User(s)' textbox. If you are looking for multiple users John, Leonard and Susan then, enter as John||Leonard||Susan.
Match for specific information	This field can take multiple strings separated with && or ||. && Stands for AND condition and || stands for OR condition. If you want to make a match on any of the special characters like "\", "^", "$", etc., then in the search string prefix this char with a backslash, like "\\" for a "\" and "\^" for a "^".Example- If you wish to generate a Printer Usage report for a specific printer named "FLR1PRINTER" then, just enter FLR1PRINTER in 'Filter for Specific Info' textbox. If you are wish to generate a Printer Usage report for a specific user "Susan", specific printer "FLR1PRINTER" and specific document "FinancialInfo.xls", you have to enter Susan in 'Match for User(s)' textbox and you have to enter FLR1PRINTER&&FinancialInfo.xls in 'Filter for Specific Info' textbox.
Filter (Exclude): Use this option if you want to ignore specific information.	
Filter User(s)	Type the user names to exclude from report generation.
Filter specific information	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.
Use this option if you do not wish to see specific Event Id(s) or Event Source(s)	
Filter Event Id(s)	Enter the Event ID(s), which you do not wish to see in the report. Use || as a separator to enter multiple Event Id(s).
Filter Event Source(s)	Enter the Event sources (s), which you do not wish to, see in the report. Use || as a separator to enter multiple Event Id(s).

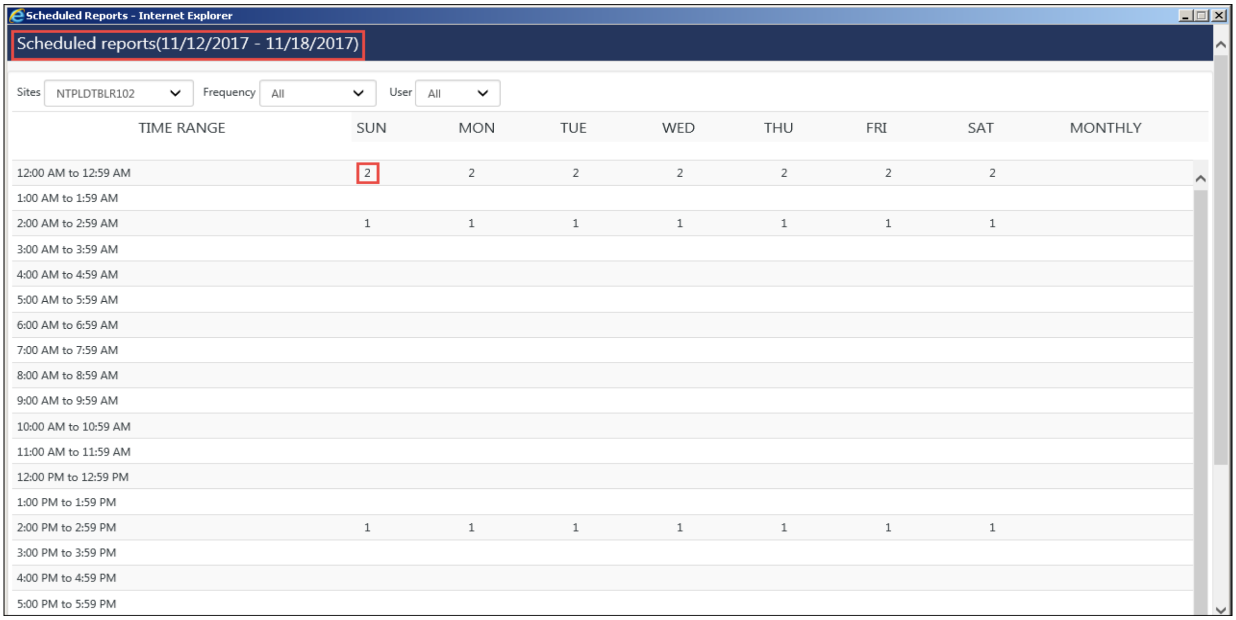
Table 27

4.12 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.

1 To access report calendar in **Reports Dashboard** or **Configuration**, click **Report Calendar** 📅 .

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



Scheduled Reports - Internet Explorer

Scheduled reports(11/12/2017 - 11/18/2017)

Sites: NTPLDTBLR102 Frequency: All User: All

TIME RANGE	SUN	MON	TUE	WED	THU	FRI	SAT	MONTHLY
12:00 AM to 12:59 AM	2	2	2	2	2	2	2	
1:00 AM to 1:59 AM								
2:00 AM to 2:59 AM	1	1	1	1	1	1	1	
3:00 AM to 3:59 AM								
4:00 AM to 4:59 AM								
5:00 AM to 5:59 AM								
6:00 AM to 6:59 AM								
7:00 AM to 7:59 AM								
8:00 AM to 8:59 AM								
9:00 AM to 9:59 AM								
10:00 AM to 10:59 AM								
11:00 AM to 11:59 AM								
12:00 PM to 12:59 PM								
1:00 PM to 1:59 PM								
2:00 PM to 2:59 PM	1	1	1	1	1	1	1	
3:00 PM to 3:59 PM								
4:00 PM to 4:59 PM								
5:00 PM to 5:59 PM								

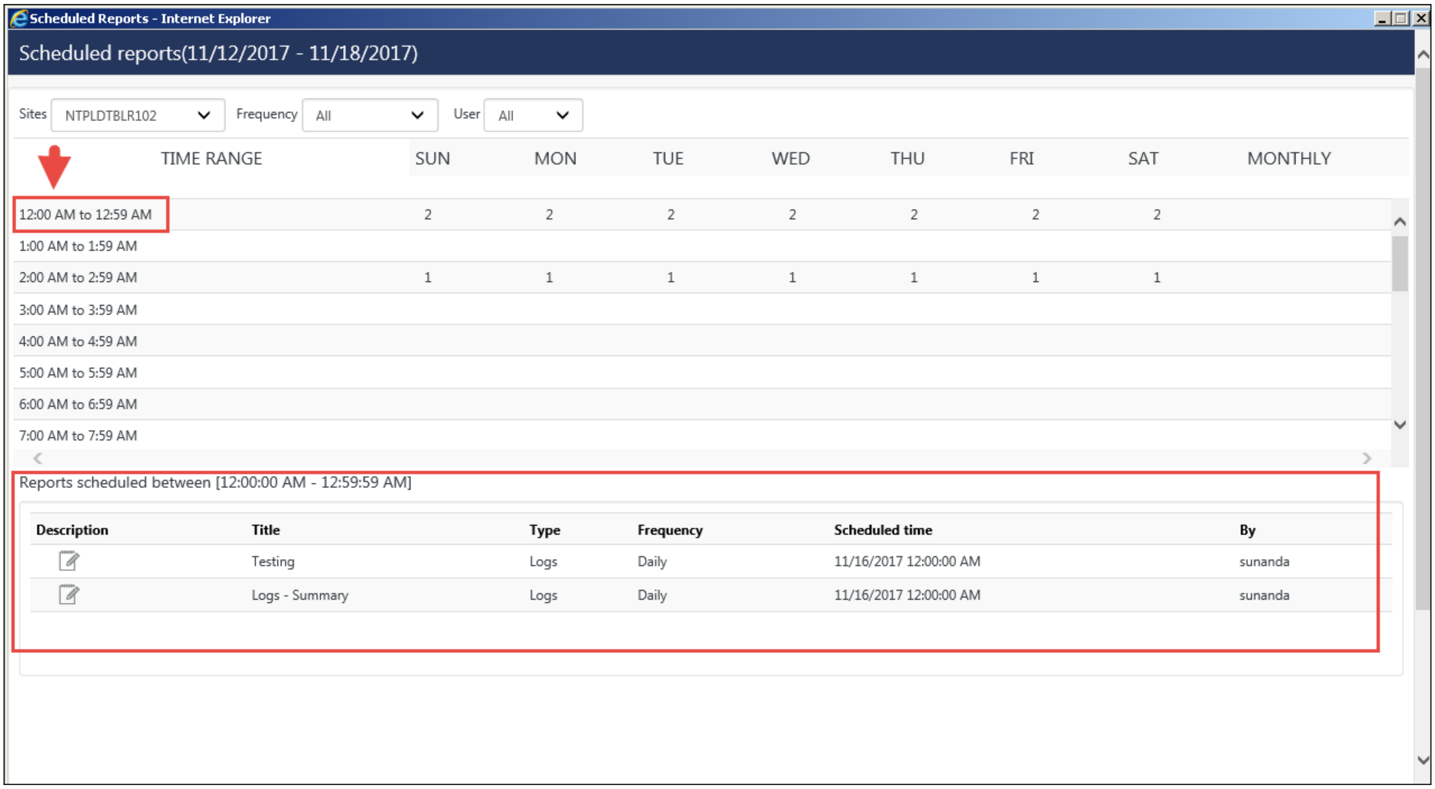
Figure 271

Click	To
Frequency	Select a frequency from this drop-down list to view respective reports.
Time range	To view reports scheduled in that time slot.
Day	To view reports scheduled on that day.
Show reports	EventTracker selects this checkbox and displays all reports schedules. Clear this checkbox and EventTracker displays only the reports schedules.
User	To view reports scheduled by a particular user

4.12.1 Viewing scheduled reports in time slot

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

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


Scheduled Reports - Internet Explorer
Scheduled reports(11/12/2017 - 11/18/2017)
Sites NTPLDTBLR102
Frequency All
User All

TIME RANGE	SUN	MON	TUE	WED	THU	FRI	SAT	MONTHLY
12:00 AM to 12:59 AM	2	2	2	2	2	2	2	
1:00 AM to 1:59 AM								
2:00 AM to 2:59 AM	1	1	1	1	1	1	1	
3:00 AM to 3:59 AM								
4:00 AM to 4:59 AM								
5:00 AM to 5:59 AM								
6:00 AM to 6:59 AM								
7:00 AM to 7:59 AM								

Reports scheduled between [12:00:00 AM - 12:59:59 AM]

Description	Title	Type	Frequency	Scheduled time	By
	Testing	Logs	Daily	11/16/2017 12:00:00 AM	sunanda
	Logs - Summary	Logs	Daily	11/16/2017 12:00:00 AM	sunanda

Figure 272

Click	To
Title	Title of the scheduled reports
Type	Type of the scheduled reports
Frequency	Frequency of the report generation
Scheduled Time	Date and time set for report generation
Configured By	Name of the user who configured the report

Table 28

2 Click ✎ to view the descriptions.

EventTracker opens read-only descriptions.

4.12.2 Viewing scheduled reports on a day

1 To view scheduled reports on a day, click the name of the day.

EventTracker opens the reports scheduled on that day.

2 To view scheduled reports on a day and a time slot, click the links at the intersection of Time range and Day.

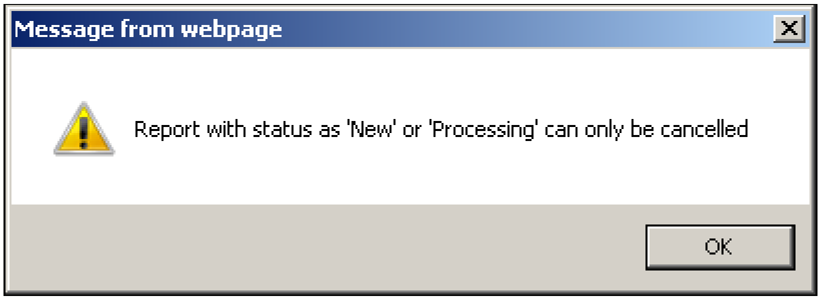
EventTracker opens the reports scheduled on that day and time slot.

4.13 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 **Report Status** ☑ .

EventTracker opens a message. Click OK.

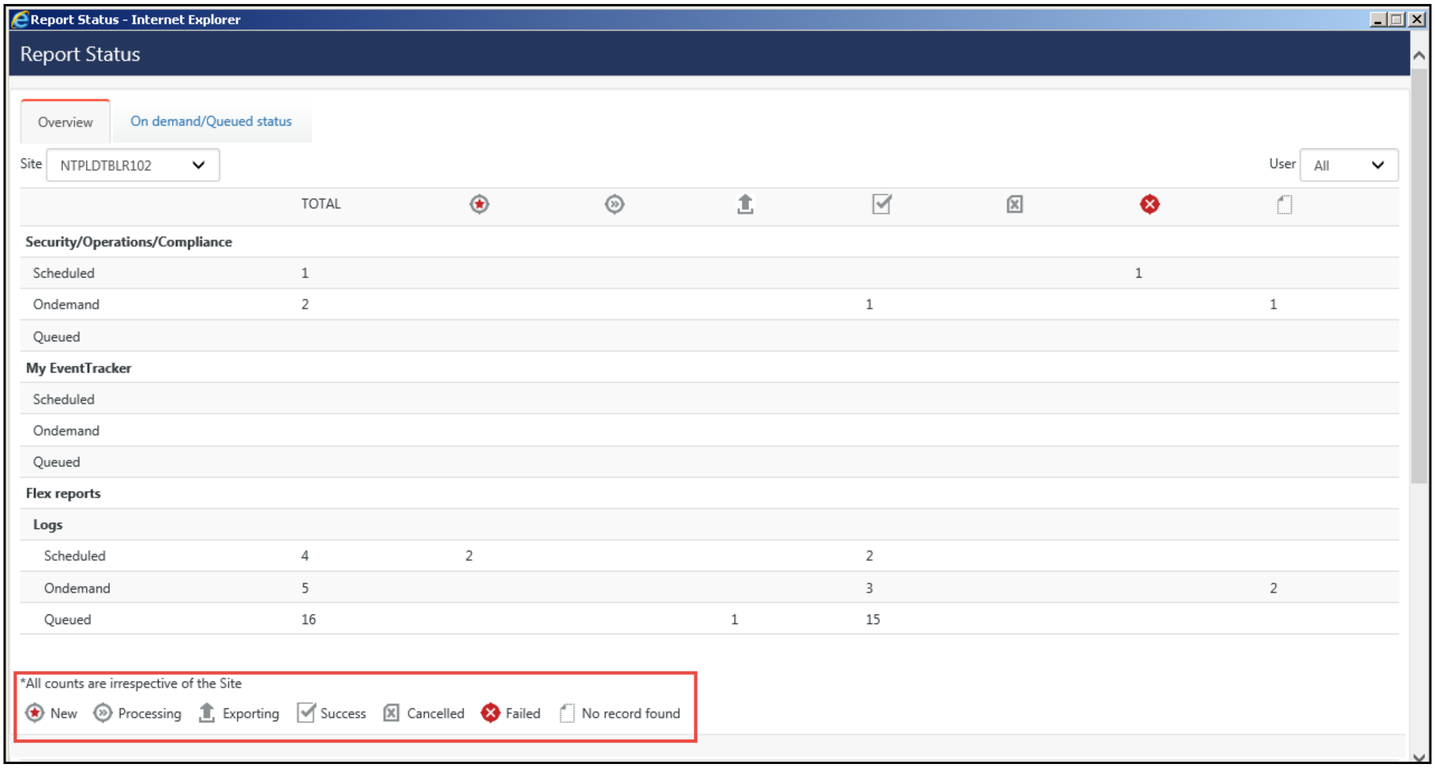


Message from webpage

Report with status as 'New' or 'Processing' can only be cancelled

Figure 273

EventTracker opens the **Report Status** Snapshot pop-up window.



Report Status - Internet Explorer

Report Status

Overview | On demand/Queued status

Site NTPLDTBLR102 | User All

	TOTAL	⊛	⊙	⬆	☑	☒	⊗	🗋
Security/Operations/Compliance								
Scheduled	1						1	
Ondemand	2				1			1
Queued								
My EventTracker								
Scheduled								
Ondemand								
Queued								
Flex reports								
Logs								
Scheduled	4	2			2			
Ondemand	5				3			2
Queued	16			1	15			

*All counts are irrespective of the Site

⊛ New ⊙ Processing ⬆ Exporting ☑ Success ☒ Cancelled ⊗ Failed 🗋 No record found

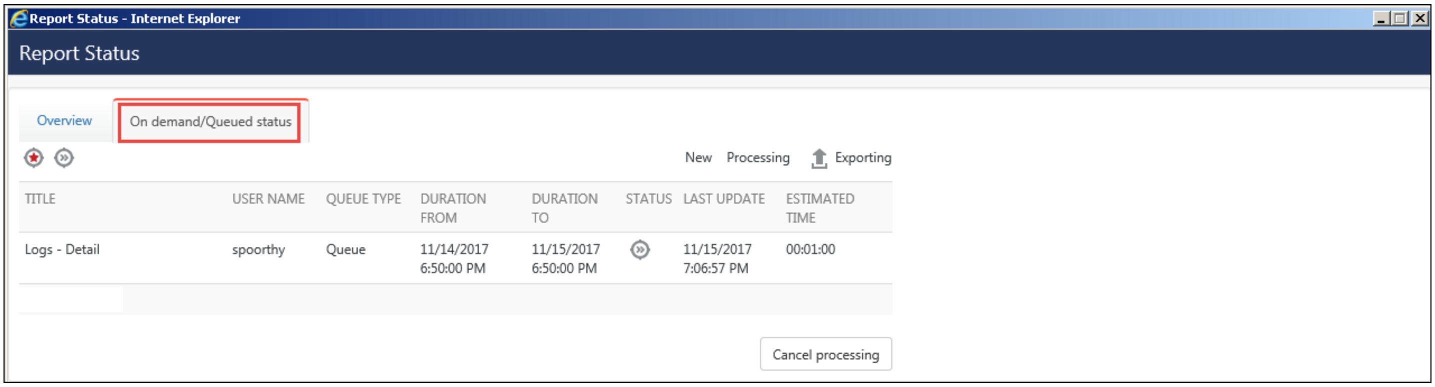
Figure 274

Field	Description
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 29

4.13.1 On Demand/Queued Status button

1. Click **On Demand/Queued Status**.
   Reports Status opens.



TITLE	USER NAME	QUEUE TYPE	DURATION FROM	DURATION TO	STATUS	LAST UPDATE	ESTIMATED TIME
Logs - Detail	spoorthy	Queue	11/14/2017 6:50:00 PM	11/15/2017 6:50:00 PM		11/15/2017 7:06:57 PM	00:01:00

Figure 275

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

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

4.14 Favorites tab

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

2 Click **New** ⊕ in **Dashboard / Configuration**.

3 Select **Alphabetical** tab.

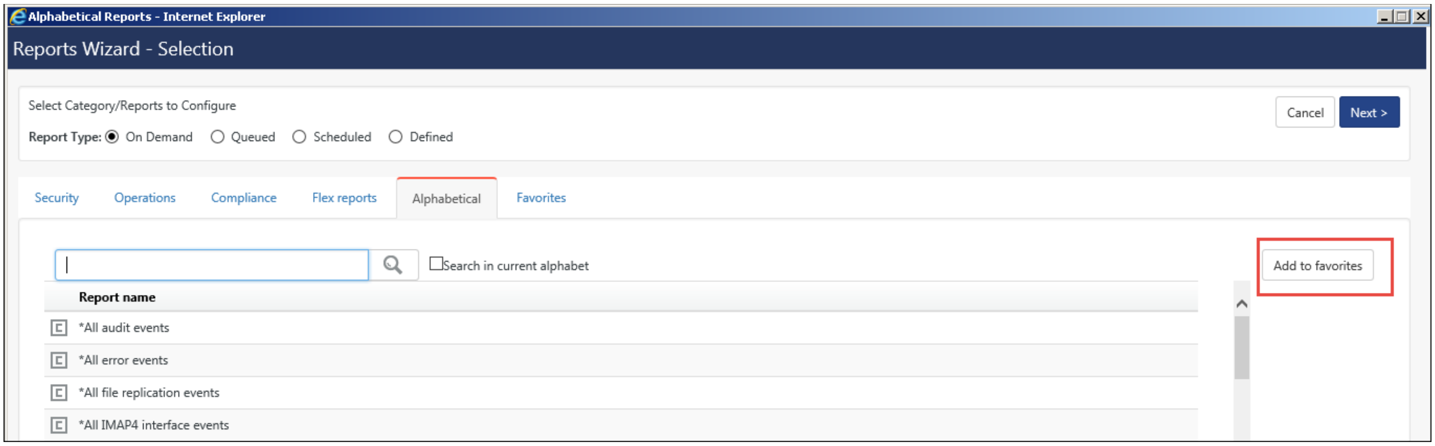
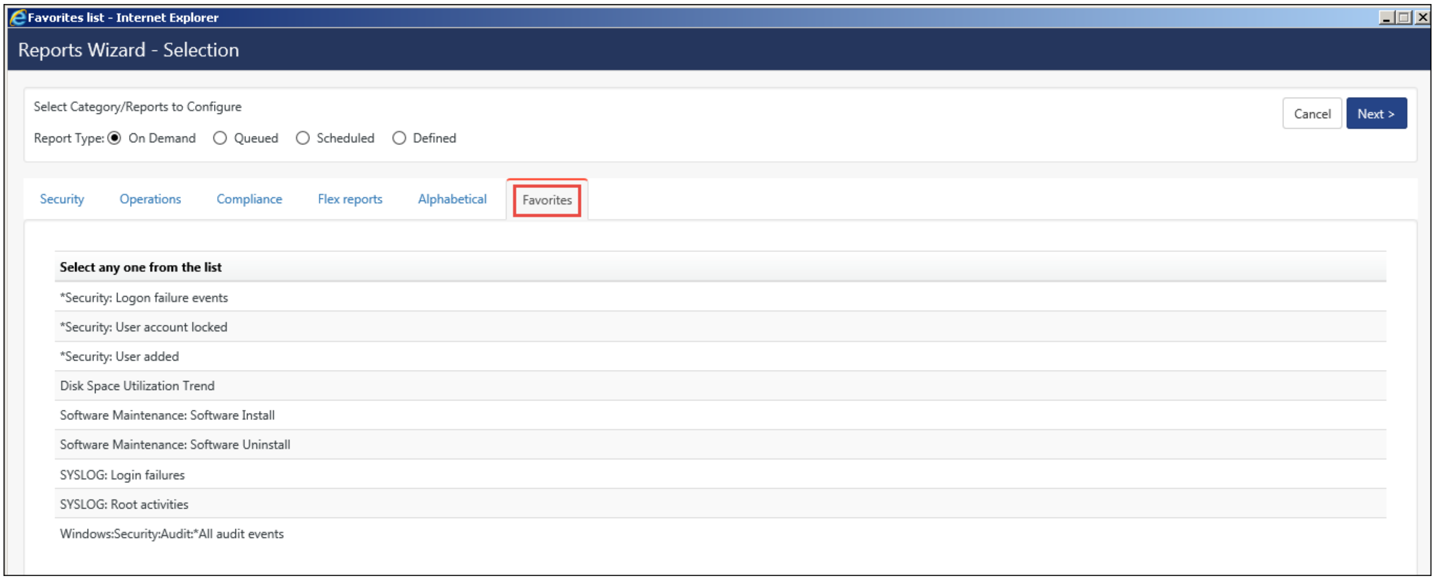

Alphabetical Reports - Internet Explorer
Reports Wizard - Selection
Select Category/Reports to Configure
Report Type: ● On Demand ○ Queued ○ Scheduled ○ Defined
Cancel
Next >
Security
Operations
Compliance
Flex reports
Alphabetical
Favorites
□Search in current alphabet
Add to favorites
Report name
*All audit events
*All error events
*All file replication events
*All IMAP4 interface events

Figure 276

4 Select any report and then select the **Add to Favorites** tab.

5 To view favorites, click the **Favorites** tab.


Favorites list - Internet Explorer
Reports Wizard - Selection
Select Category/Reports to Configure
Report Type: ● On Demand ○ Queued ○ Scheduled ○ Defined
Cancel
Next >
Security
Operations
Compliance
Flex reports
Alphabetical
Favorites

Select any one from the list
*Security: Logon failure events
*Security: User account locked
*Security: User added
Disk Space Utilization Trend
Software Maintenance: Software Install
Software Maintenance: Software Uninstall
SYSLOG: Login failures
SYSLOG: Root activities
Windows:Security:Audit:*All audit events

Figure 277

6 To generate a report, select any report and the **Report Type.**

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

4.14.1 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**

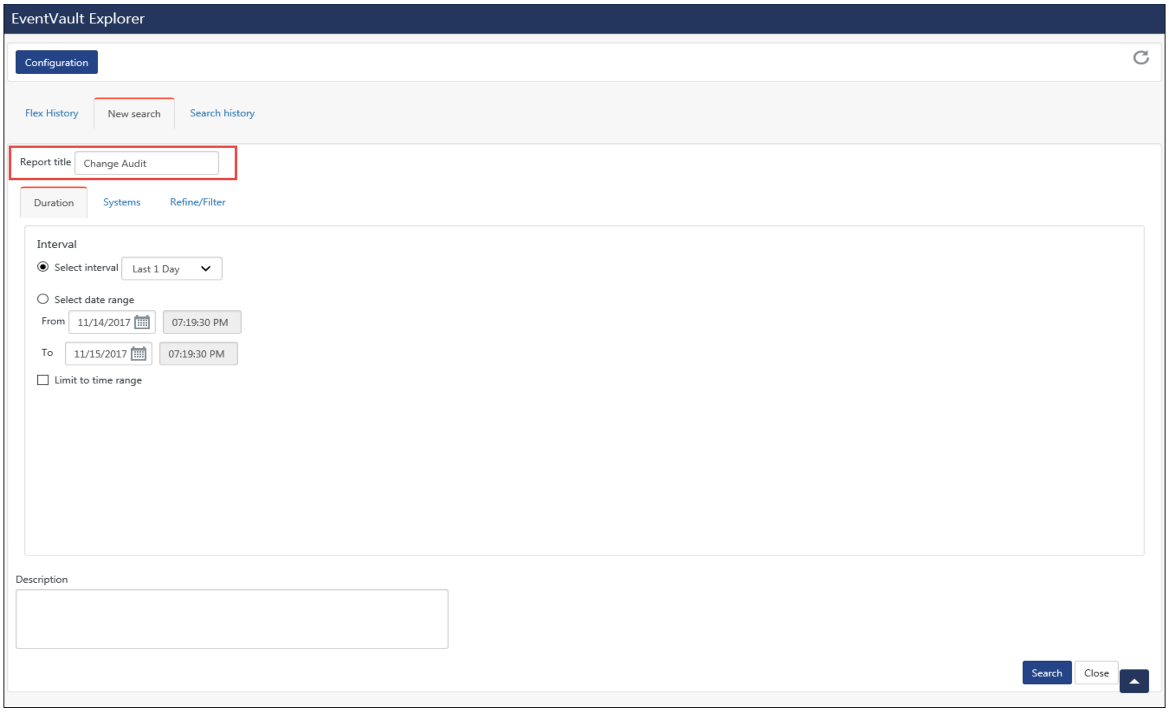
User can also configure EventVault Explorer to use remote SQL Server database. The reason is that the SQL Server Express Edition has maximum database size limitation of 4 GB. Hence, to overcome this limitation an option is provided to use Remote SQL Server, which can be SQL Server Enterprise Full Edition.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

4.14.2 Perform search in EventVault Explorer

This option helps you to search CAB files.

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

EventTracker opens the EventVault Explorer.



Report title: Change Audit

Interval

● Select interval: Last 1 Day

○ Select date range

From 11/14/2017 07:19:30 PM

To 11/15/2017 07:19:30 PM

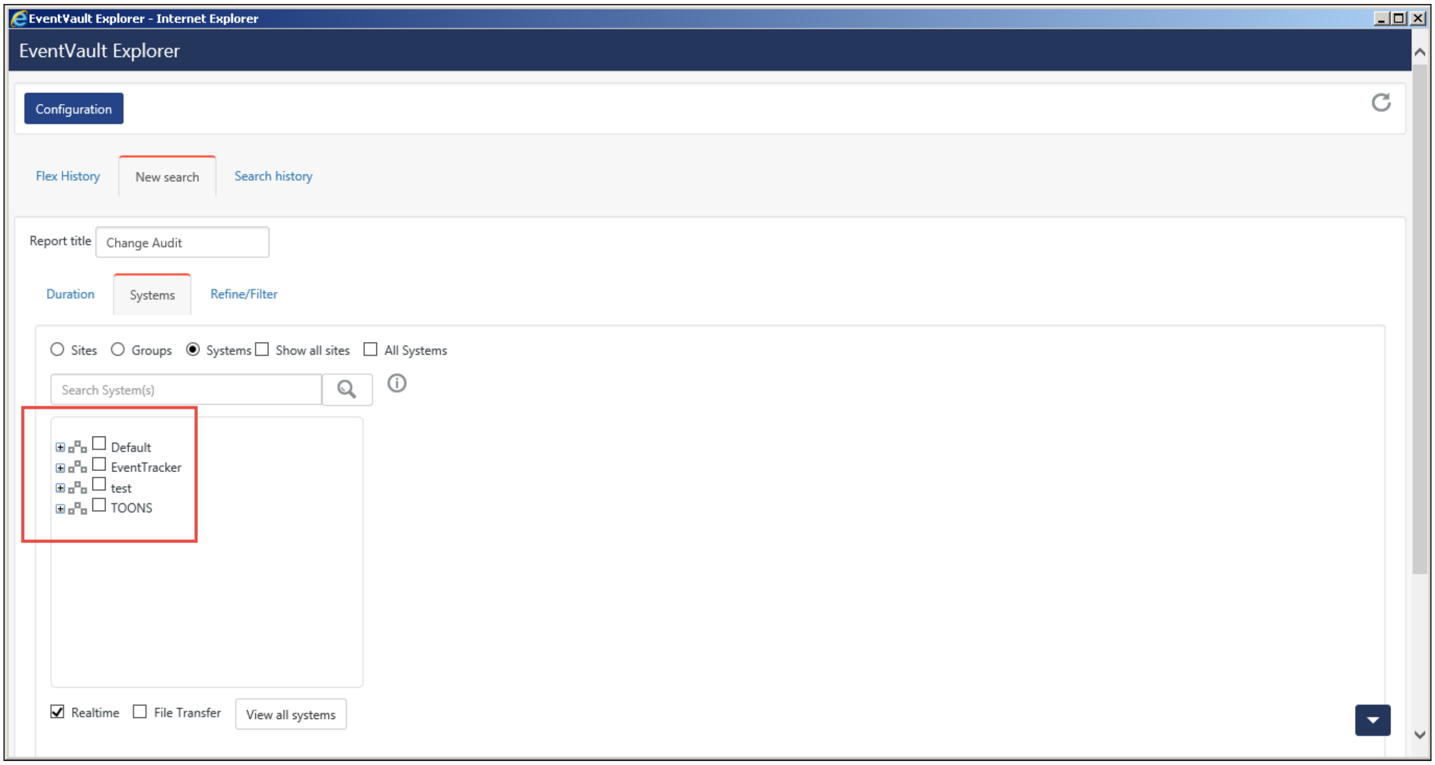
□ Limit to time range

Figure 278

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).**



Report title: Change Audit

○ Sites ○ Groups ● Systems □ Show all sites □ All Systems

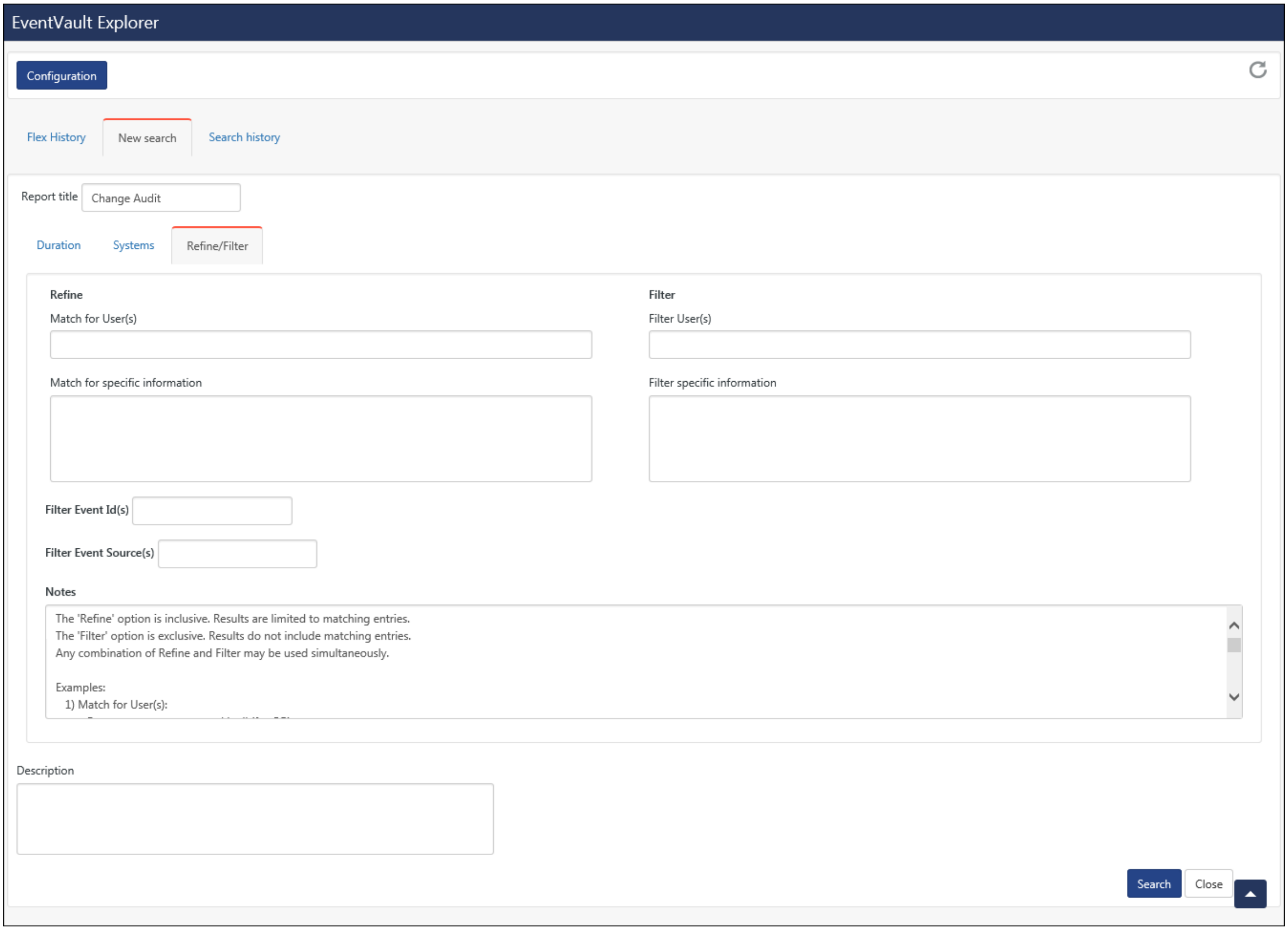
Search System(s)

□ Default
□ EventTracker
□ test
□ TOONS

☑ Realtime □ File Transfer

Figure 279

5 Set the **Refine / Filter** criteria.



Report title: Change Audit

The 'Refine' option is inclusive. Results are limited to matching entries.
The 'Filter' option is exclusive. Results do not include matching entries.
Any combination of Refine and Filter may be used simultaneously.

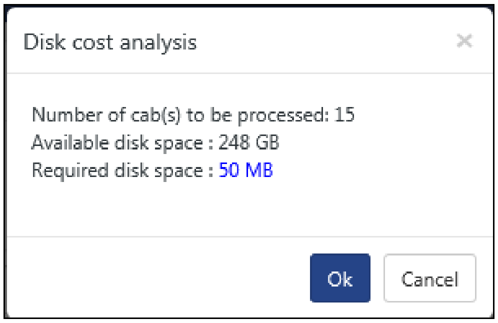
Examples:
1) Match for User(s):

Figure 280

6 Enter an appropriate **Description**.

7 Click **Search**.

EventTracker opens the Disk cost analysis pop-up window.



Number of cab(s) to be processed: 15
Available disk space : 248 GB
Required disk space : 50 MB

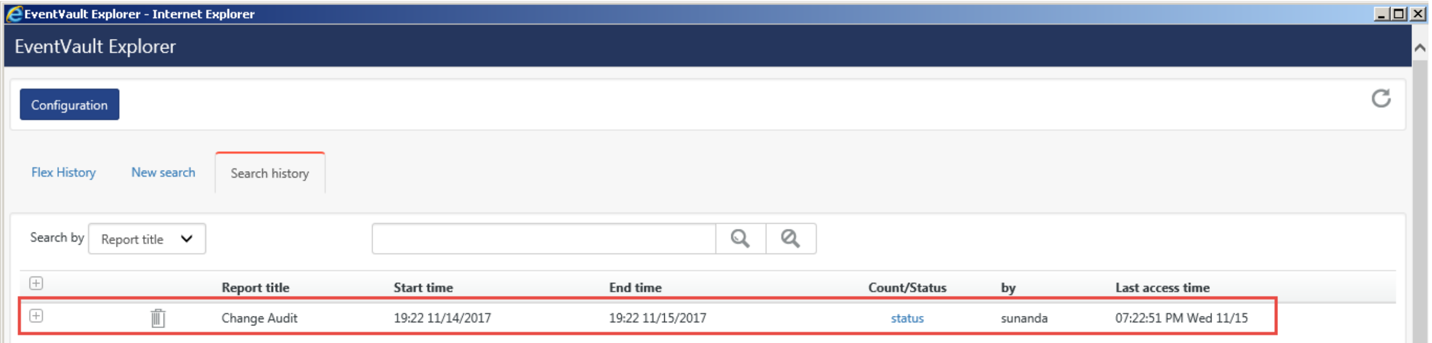
Figure 281

8 Click **OK**.

EventTracker opens 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**).

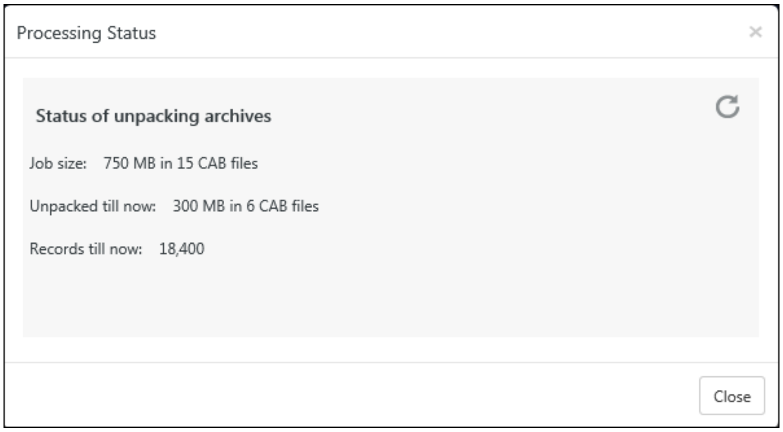


Report title	Start time	End time	Count/Status	by	Last access time
Change Audit	19:22 11/14/2017	19:22 11/15/2017	status	sunanda	07:22:51 PM Wed 11/15

Figure 282

10 Click the **Status** hyperlink.

EventTracker opens EventVault Explorer processing status window.



Status of unpacking archives

Job size: 750 MB in 15 CAB files

Unpacked till now: 300 MB in 6 CAB files

Records till now: 18,400

Figure 283

Status	For
Initializing	New request
Processing	Cab Extraction
Exception Occurred	Failed
Status of unpacking Archives	All the archives have been processed (unpacked) successfully.

Table 30

4.15 Flex report history

It provides detail 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, Event Type, Category, Domain, System, User and Description.

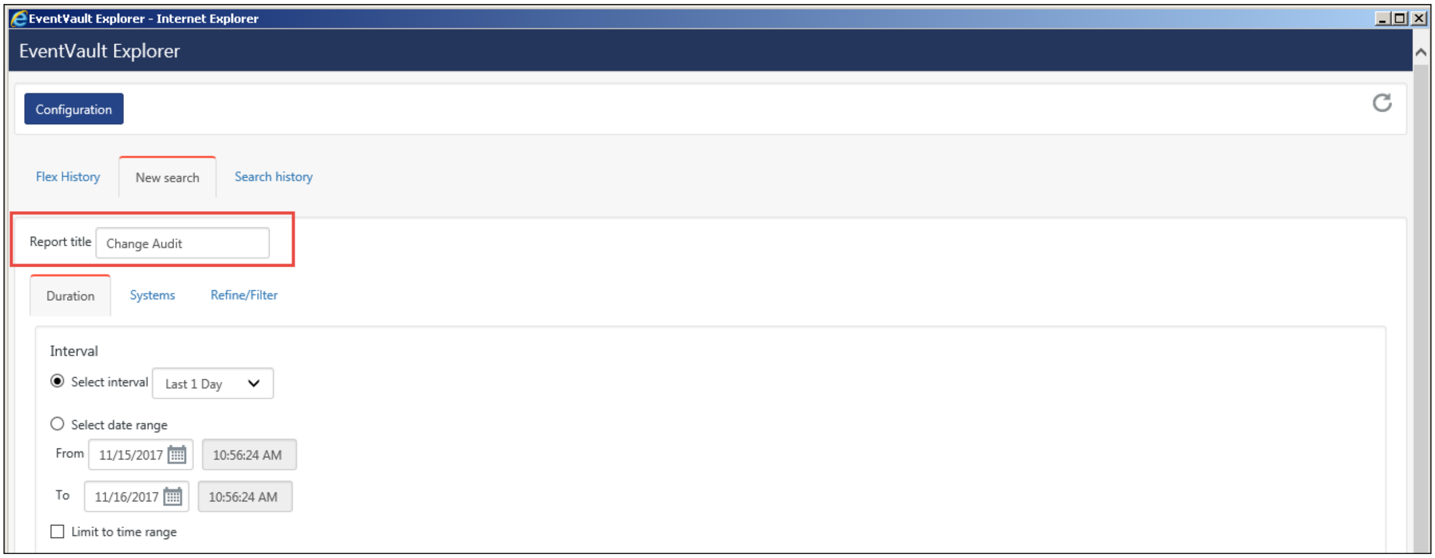
You can create and extract your own custom columns from the standard columns provided. The results can be extracted in an excel file since it supports all excel features. It allows you to browse through underlined data.

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 **Reports**, and then select **Explorer**.

EventTracker opens the EventVault Explorer.



Report title: Change Audit

Interval

● Select interval: Last 1 Day

○ Select date range

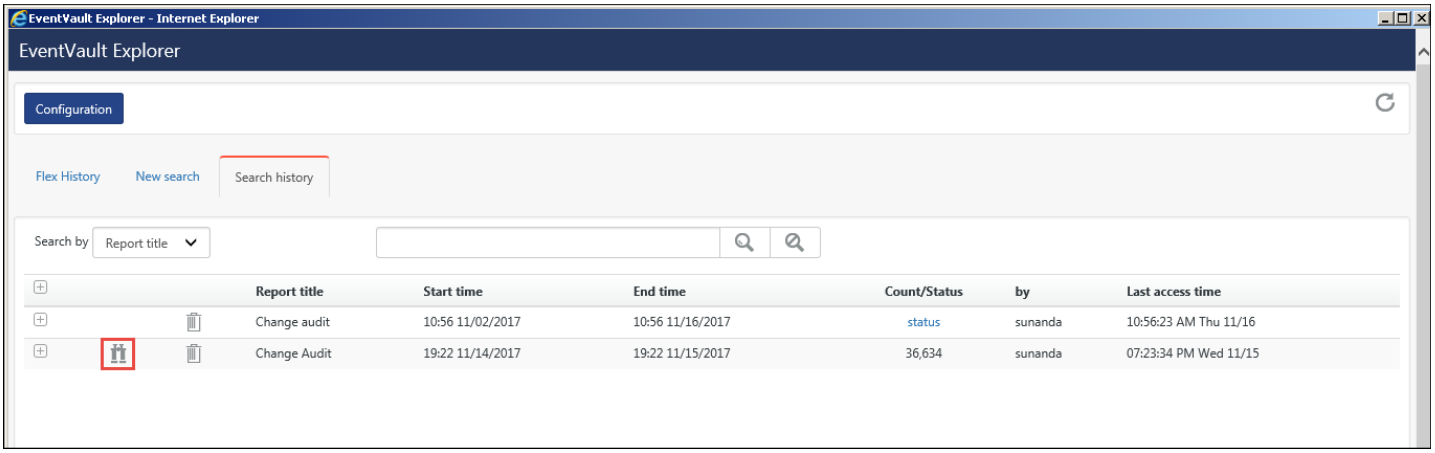
From 11/15/2017 10:56:24 AM

To 11/16/2017 10:56:24 AM

□ Limit to time range

Figure 284

2. Go to **New Search** tab; enter the **Report Title**, the **Date range/ Time range** and the **System Name.**



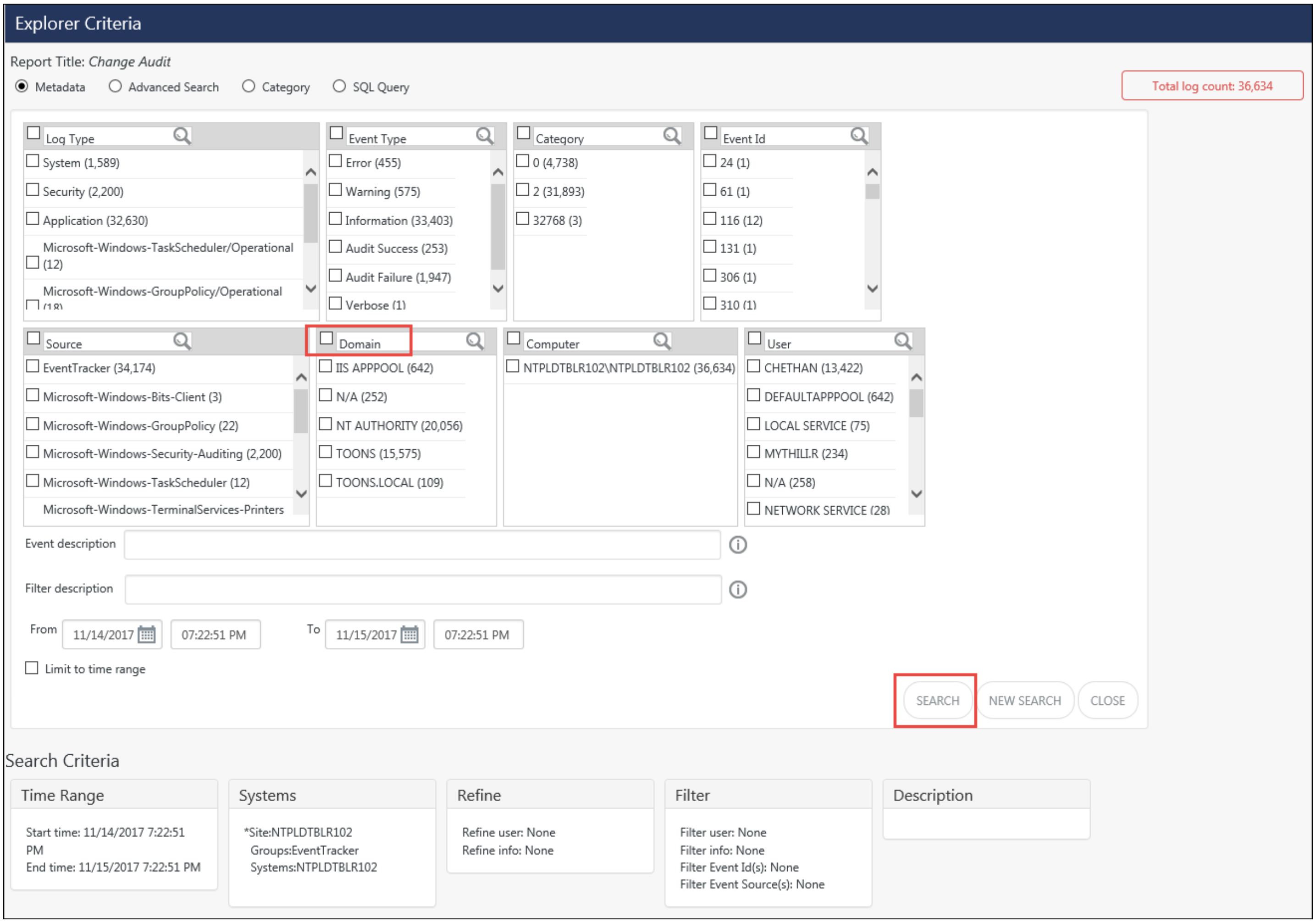
Search by: Report title

Report title	Start time	End time	Count/Status	by	Last access time
Change audit	10:56 11/02/2017	10:56 11/16/2017	status	sunanda	10:56:23 AM Thu 11/16
Change Audit	19:22 11/14/2017	19:22 11/15/2017	36,634	sunanda	07:23:34 PM Wed 11/15

Figure 285

4. Select **Explore** .

Flex Data Refine window opens.



Explorer Criteria

Report Title: *Change Audit*

● Metadata ○ Advanced Search ○ Category ○ SQL Query

Total log count: 36,634

□ Log Type
□ System (1,589)
□ Security (2,200)
□ Application (32,630)
□ Microsoft-Windows-TaskScheduler/Operational (12)
□ Microsoft-Windows-GroupPolicy/Operational (18)

□ Event Type
□ Error (455)
□ Warning (575)
□ Information (33,403)
□ Audit Success (253)
□ Audit Failure (1,947)
□ Verbose (1)

□ Category
□ 0 (4,738)
□ 2 (31,893)
□ 32768 (3)

□ Event Id
□ 24 (1)
□ 61 (1)
□ 116 (12)
□ 131 (1)
□ 306 (1)
□ 310 (1)

□ Source
□ EventTracker (34,174)
□ Microsoft-Windows-Bits-Client (3)
□ Microsoft-Windows-GroupPolicy (22)
□ Microsoft-Windows-Security-Auditing (2,200)
□ Microsoft-Windows-TaskScheduler (12)
Microsoft-Windows-TerminalServices-Printers

□ Domain
□ IIS APPPOOL (642)
□ N/A (252)
□ NT AUTHORITY (20,056)
□ TOONS (15,575)
□ TOONS.LOCAL (109)

□ Computer
□ NTPLDTBLR102\NTPLDTBLR102 (36,634)

□ User
□ CHETHAN (13,422)
□ DEFAULTAPPPOOL (642)
□ LOCAL SERVICE (75)
□ MYTHILI.R (234)
□ N/A (258)
□ NETWORK SERVICE (28)

Event description

Filter description

From 11/14/2017 07:22:51 PM To 11/15/2017 07:22:51 PM

□ Limit to time range

Search Criteria

Time Range
Start time: 11/14/2017 7:22:51 PM
End time: 11/15/2017 7:22:51 PM

Systems
*Site:NTPLDTBLR102
Groups:EventTracker
Systems:NTPLDTBLR102

Refine
Refine user: None
Refine info: None

Filter
Filter user: None
Filter info: None
Filter Event Id(s): None
Filter Event Source(s): None

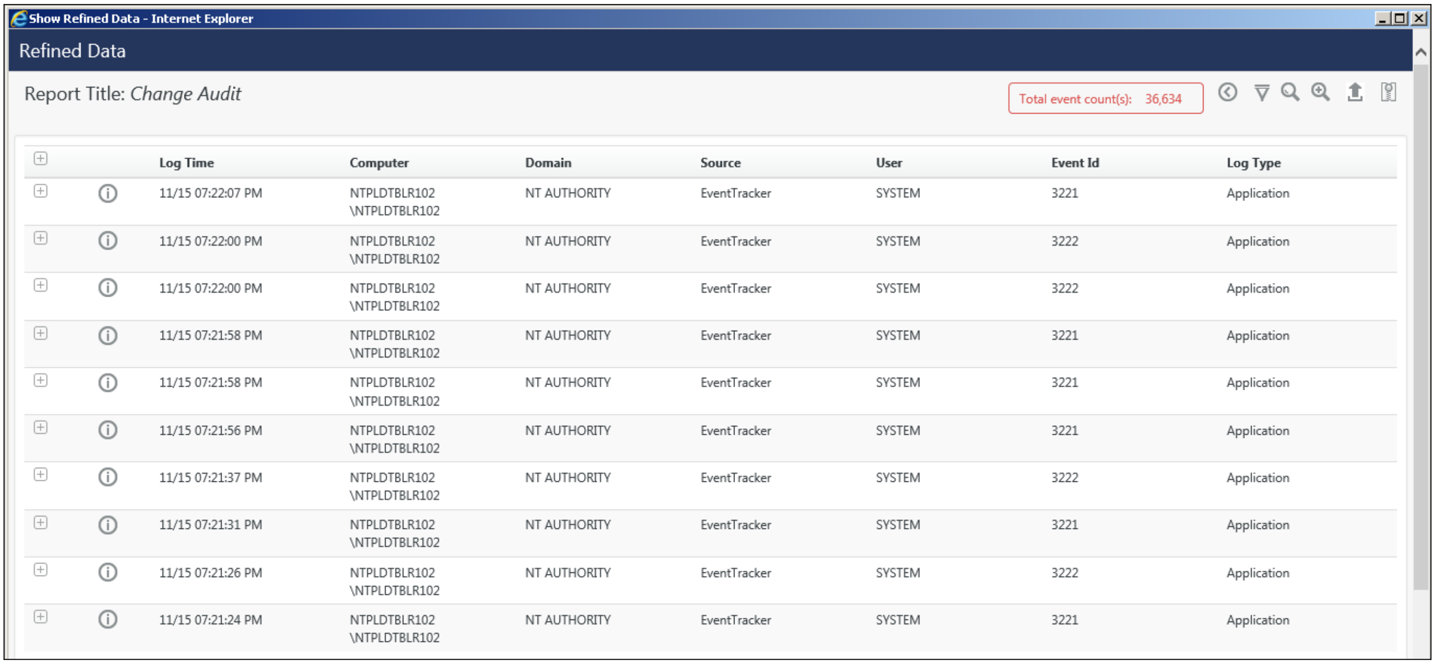
Description

Figure 286

5. Select the required options and then select **Search**.

   Ex: Select Domain option, and then click Search.

   Show Refined Data window opens.



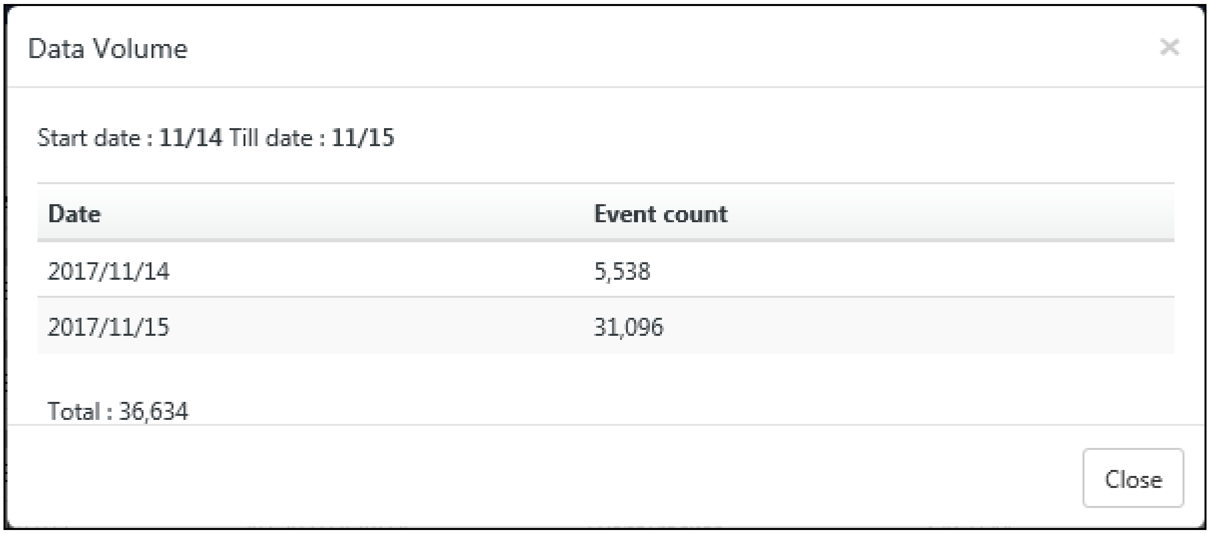
Report Title: *Change Audit*

Total event count(s): 36,634

		Log Time	Computer	Domain	Source	User	Event Id	Log Type
⊞	ⓘ	11/15 07:22:07 PM	NTPLDTBLR102 \NTPLDTBLR102	NT AUTHORITY	EventTracker	SYSTEM	3221	Application
⊞	ⓘ	11/15 07:22:00 PM	NTPLDTBLR102 \NTPLDTBLR102	NT AUTHORITY	EventTracker	SYSTEM	3222	Application
⊞	ⓘ	11/15 07:22:00 PM	NTPLDTBLR102 \NTPLDTBLR102	NT AUTHORITY	EventTracker	SYSTEM	3222	Application
⊞	ⓘ	11/15 07:21:58 PM	NTPLDTBLR102 \NTPLDTBLR102	NT AUTHORITY	EventTracker	SYSTEM	3221	Application
⊞	ⓘ	11/15 07:21:58 PM	NTPLDTBLR102 \NTPLDTBLR102	NT AUTHORITY	EventTracker	SYSTEM	3221	Application
⊞	ⓘ	11/15 07:21:56 PM	NTPLDTBLR102 \NTPLDTBLR102	NT AUTHORITY	EventTracker	SYSTEM	3221	Application
⊞	ⓘ	11/15 07:21:37 PM	NTPLDTBLR102 \NTPLDTBLR102	NT AUTHORITY	EventTracker	SYSTEM	3222	Application
⊞	ⓘ	11/15 07:21:31 PM	NTPLDTBLR102 \NTPLDTBLR102	NT AUTHORITY	EventTracker	SYSTEM	3221	Application
⊞	ⓘ	11/15 07:21:26 PM	NTPLDTBLR102 \NTPLDTBLR102	NT AUTHORITY	EventTracker	SYSTEM	3222	Application
⊞	ⓘ	11/15 07:21:24 PM	NTPLDTBLR102 \NTPLDTBLR102	NT AUTHORITY	EventTracker	SYSTEM	3221	Application

Figure 287

6. To view data volume, click **Data Volume** .



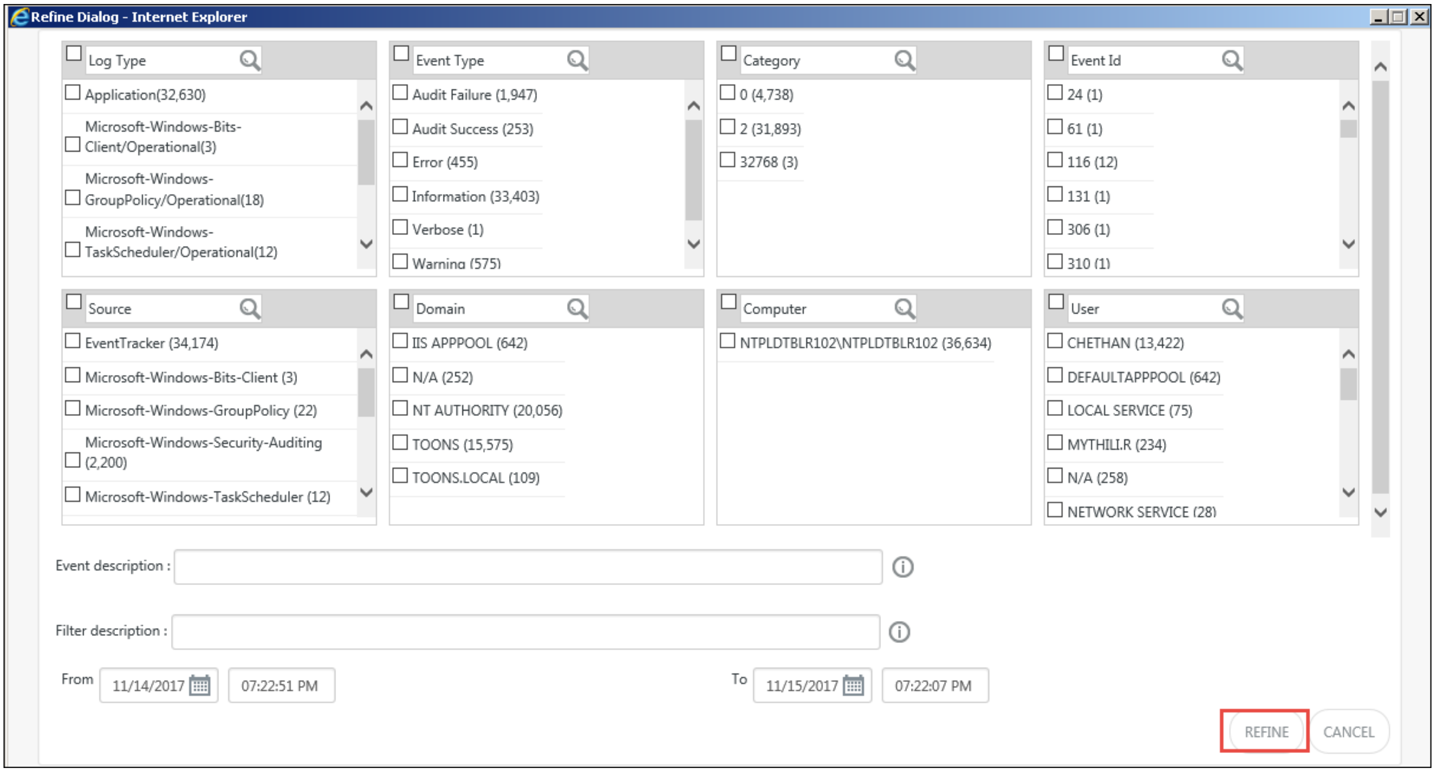
Start date : **11/14** Till date : **11/15**

Date	Event count
2017/11/14	5,538
2017/11/15	31,096

Total : 36,634

Figure 288

7. To refine and narrow down the search criteria, click **Refine**.
8. Click **Refine option**.
   Flex Refine Dialog opens.



□ Log Type
- □ Application(32,630)
- □ Microsoft-Windows-Bits-Client/Operational(3)
- □ Microsoft-Windows-GroupPolicy/Operational(18)
- □ Microsoft-Windows-TaskScheduler/Operational(12)

□ Event Type
- □ Audit Failure (1,947)
- □ Audit Success (253)
- □ Error (455)
- □ Information (33,403)
- □ Verbose (1)
- □ Warning (575)

□ Category
- □ 0 (4,738)
- □ 2 (31,893)
- □ 32768 (3)

□ Event Id
- □ 24 (1)
- □ 61 (1)
- □ 116 (12)
- □ 131 (1)
- □ 306 (1)
- □ 310 (1)

□ Source
- □ EventTracker (34,174)
- □ Microsoft-Windows-Bits-Client (3)
- □ Microsoft-Windows-GroupPolicy (22)
- □ Microsoft-Windows-Security-Auditing (2,200)
- □ Microsoft-Windows-TaskScheduler (12)

□ Domain
- □ IIS APPPOOL (642)
- □ N/A (252)
- □ NT AUTHORITY (20,056)
- □ TOONS (15,575)
- □ TOONS.LOCAL (109)

□ Computer
- □ NTPLDTBLR102\NTPLDTBLR102 (36,634)

□ User
- □ CHETHAN (13,422)
- □ DEFAULTAPPPOOL (642)
- □ LOCAL SERVICE (75)
- □ MYTHILI.R (234)
- □ N/A (258)
- □ NETWORK SERVICE (28)

Event description :

Filter description :

From 11/14/2017 07:22:51 PM To 11/15/2017 07:22:07 PM

Figure 289

10. Enter the relevant search criteria and then click **Refine**.
11. To return to flex history tab, click **Flex History**.
12. To search data, click **Search again**.
13. To export data to excel, click **Export**.

4.15.1 Configuring EventVault Explorer to use remote SQL Server

🗎 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, please 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 the remote system.

1. Click **'Reports'**, select **'Explorer'**.

   The **EventVault Explorer window** will appear on the screen.

🗎 NOTE

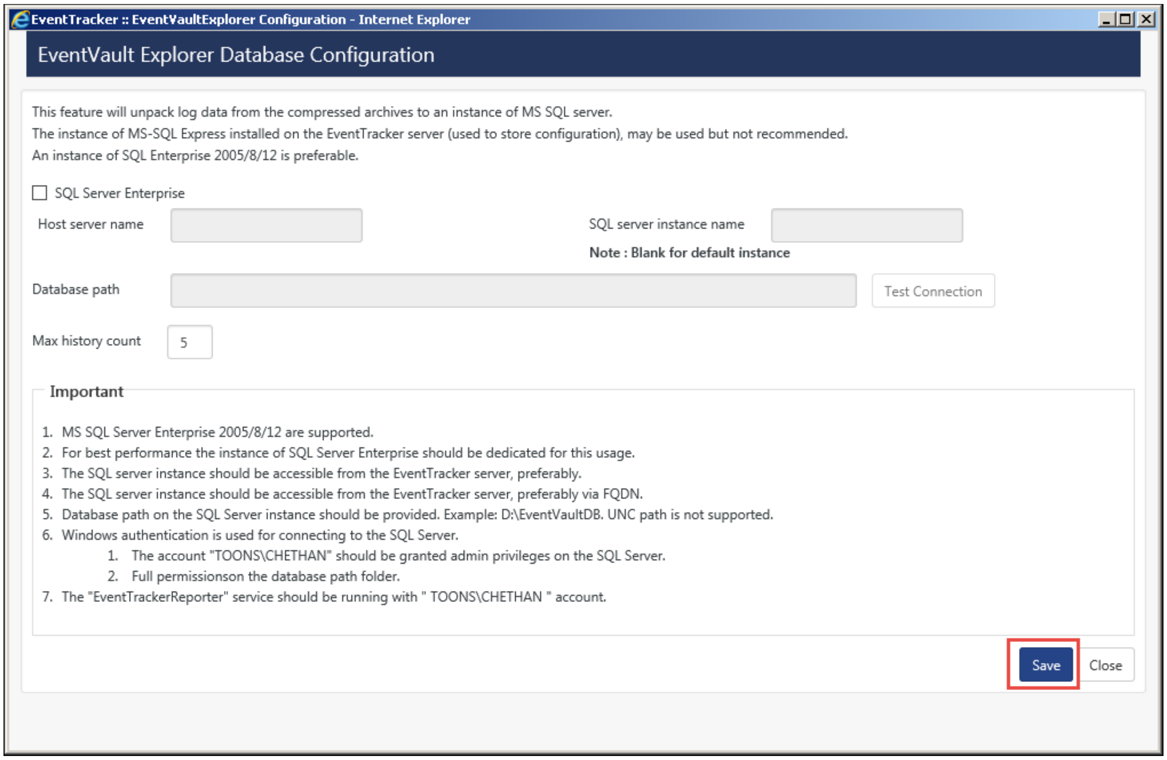
With the new User Interface enhancement provided in v8.3, the EventVault Explorer will now support the following changes:

- Faster Data loading
- Quick access to columns with the top records.
- Time Selection options (Quick, Relative and Absolute).
- Expand and Collapse for the available column option.
- Include/Exclude metadata from available columns.

For more information, refer the section- "**EventVault Explorer**" in the following link https://www.netsurion.com/Corporate/media/Corporate/Files/Support-Docs/Eventvault-explorer-Behavior-and-Tile-Dashboard-enhancement.pdf

2. Click **Configuration** hyperlink.

   EventVault Explorer Database Configuration window opens.


EventTracker :: EventVaultExplorer Configuration - Internet Explorer

EventVault Explorer Database Configuration

This feature will unpack log data from the compressed archives to an instance of MS SQL server.
The instance of MS-SQL Express installed on the EventTracker server (used to store configuration), may be used but not recommended.
An instance of SQL Enterprise 2005/8/12 is preferable.

☐ SQL Server Enterprise

Host server name

SQL server instance name

Note : Blank for default instance

Database path

Test Connection

Max history count 5

Important

1. MS SQL Server Enterprise 2005/8/12 are supported.
2. For best performance the instance of SQL Server Enterprise should be dedicated for this usage.
3. The SQL server instance should be accessible from the EventTracker server, preferably.
4. The SQL server instance should be accessible from the EventTracker server, preferably via FQDN.
5. Database path on the SQL Server instance should be provided. Example: D:\EventVaultDB. UNC path is not supported.
6. Windows authentication is used for connecting to the SQL Server.
   1. The account "TOONS\CHETHAN" should be granted admin privileges on the SQL Server.
   2. Full permissionson the database path folder.
7. The "EventTrackerReporter" service should be running with " TOONS\CHETHAN " account.

Figure 290

🗎 NOTE

For more details, refer EventVault Explorer – Introduction and Usage document.

4.16 Collection Point

4.16.1 Configuring Reports to Collection Masters

To send Collection Point generated reports to Collection Master, first the user must save the configuration (Refer: Collection Point/Collection Master)

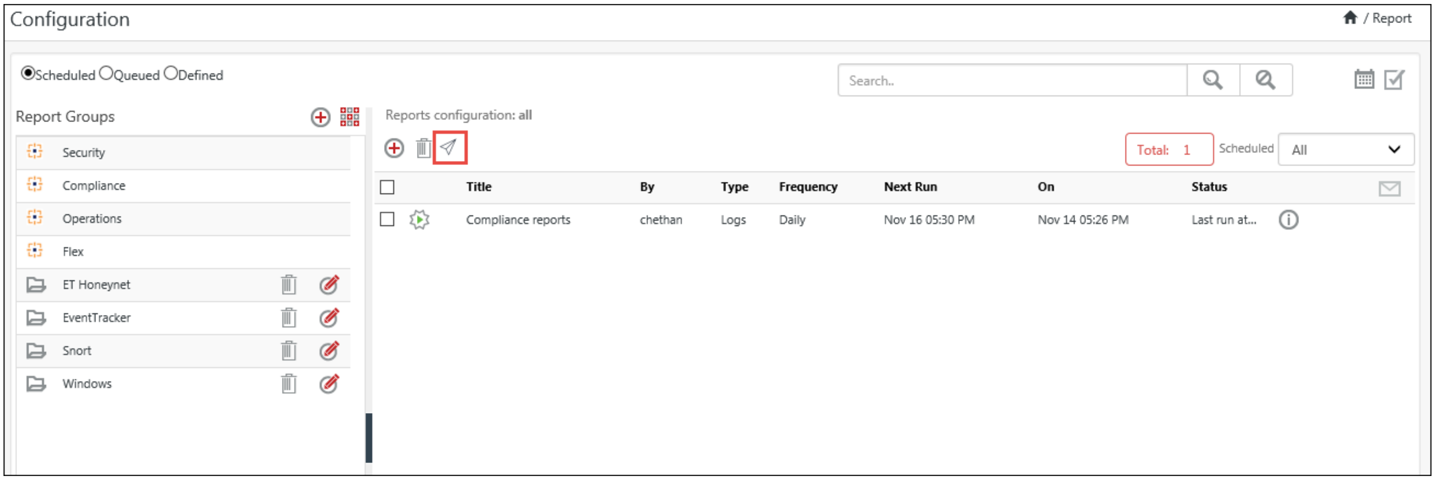
For the existing configured and saved reports, the **Send to Collection Master** icon will be available in **Reports Configuration** & **Top Level Summary**.

🗎 NOTE

The added notes for PDF report in Collection Point will not be transferred to Collection Master.

For configuring Reports,

- Click **Reports> Configuration**.
- Click **Send to Collection Master** .

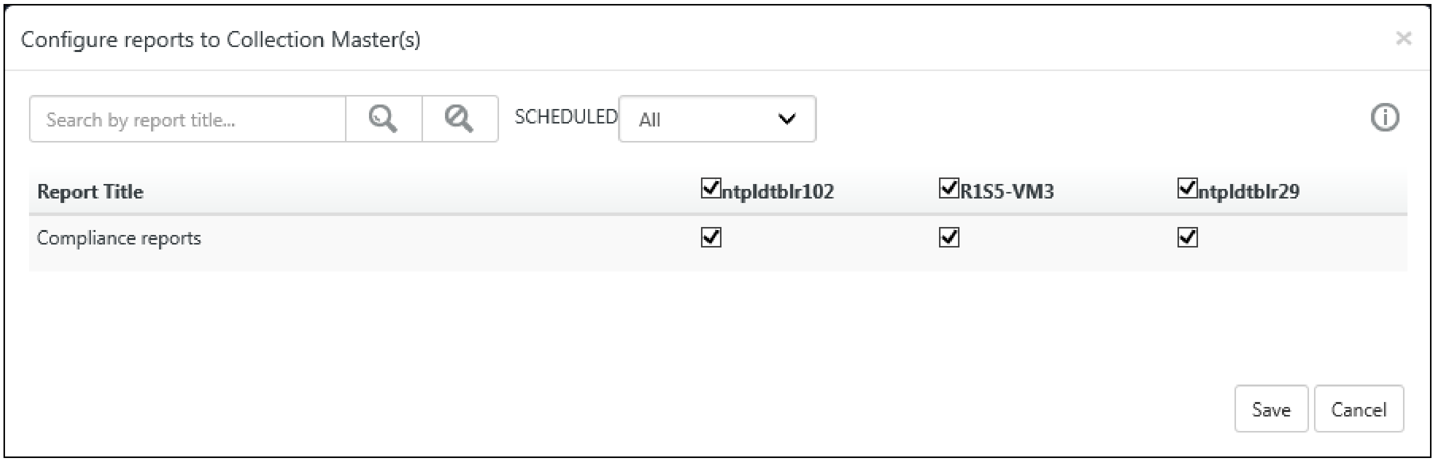


☐	Title	By	Type	Frequency	Next Run	On	Status
☐	Compliance reports	chethan	Logs	Daily	Nov 16 05:30 PM	Nov 14 05:26 PM	Last run at...

Figure 291

The configure reports to Collection Master window display.

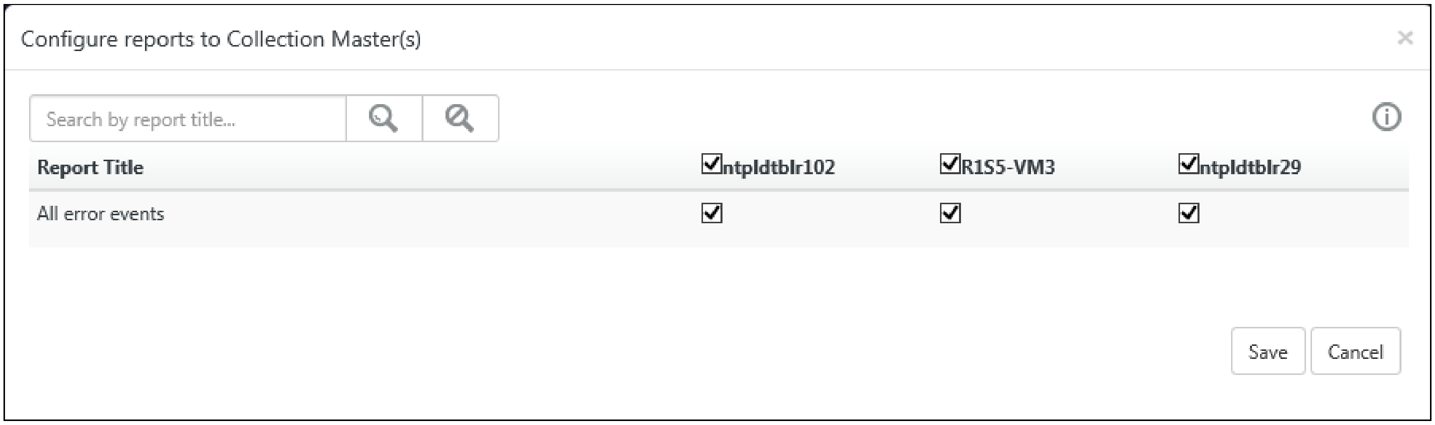
- Select the Collection Master(s), where the Collection Point generated report(s) needs to be forwarded.


Configure reports to Collection Master(s)
×
Search by report title...
SCHEDULED
All
Save
Cancel

Report Title	☑ntpldtblr102	☑R1S5-VM3	☑ntpldtblr29
Compliance reports	☑	☑	☑

Figure 292 (For Scheduled report type)

NOTE 1: For **Queued** Type report, the figure is shown below:

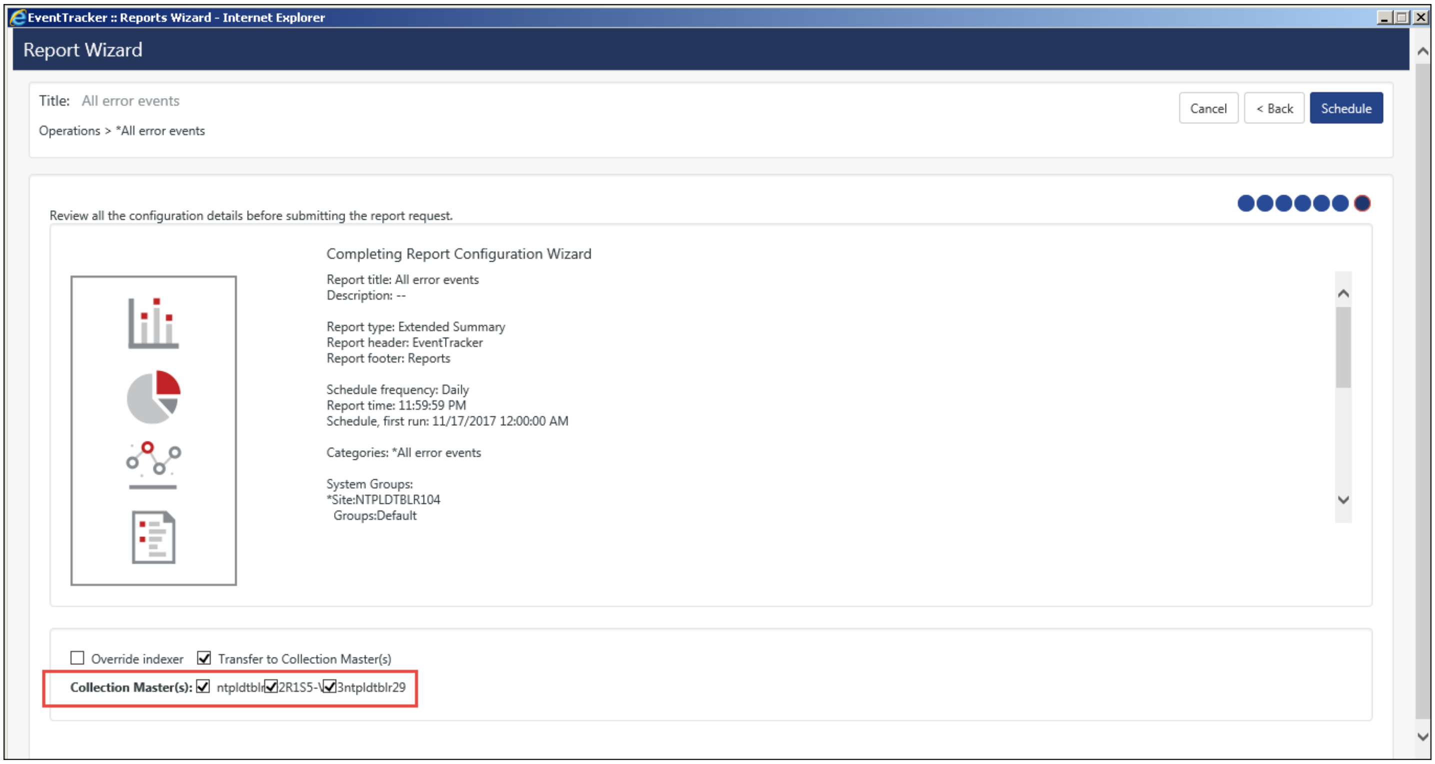

Configure reports to Collection Master(s)
×
Search by report title...
Save
Cancel

Report Title	☑ntpldtblr102	☑R1S5-VM3	☑ntpldtblr29
All error events	☑	☑	☑

Figure 293 (For Queued report type)

- Click **Save**.

NOTE 2: The user can also select the Collection Master (s) from the Report wizard in the Final step.



EventTracker :: Reports Wizard - Internet Explorer

Report Wizard

Title: All error events

Operations > *All error events

Review all the configuration details before submitting the report request.

Completing Report Configuration Wizard

Report title: All error events
Description: --

Report type: Extended Summary
Report header: EventTracker
Report footer: Reports

Schedule frequency: Daily
Report time: 11:59:59 PM
Schedule, first run: 11/17/2017 12:00:00 AM

Categories: *All error events

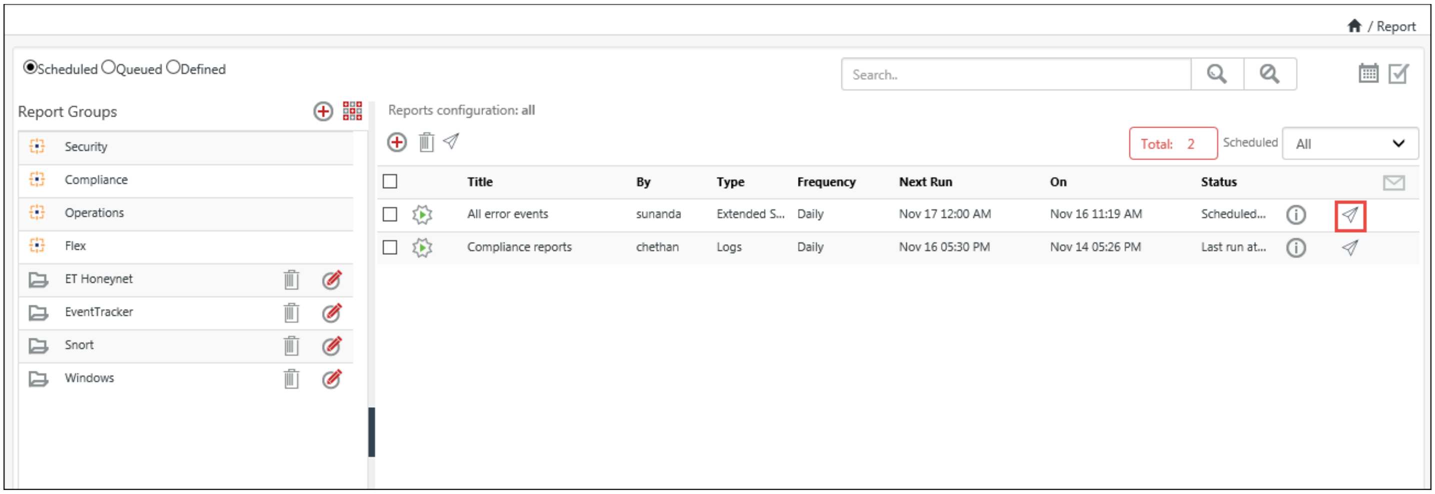
System Groups:
*Site:NTPLDTBLR104
Groups:Default

☐ Override indexer ☑ Transfer to Collection Master(s)

Collection Master(s): ☑ ntpldtblr☑2R1S5-\☑3ntpldtblr29

Figure 294

- The **Send to Collection Master** icon will be displayed for all the individual configured reports. The figure is shown below:



● Scheduled ○ Queued ○ Defined

Report Groups

- Security
- Compliance
- Operations
- Flex
- ET Honeynet
- EventTracker
- Snort
- Windows

Reports configuration: all

Total: 2 Scheduled All

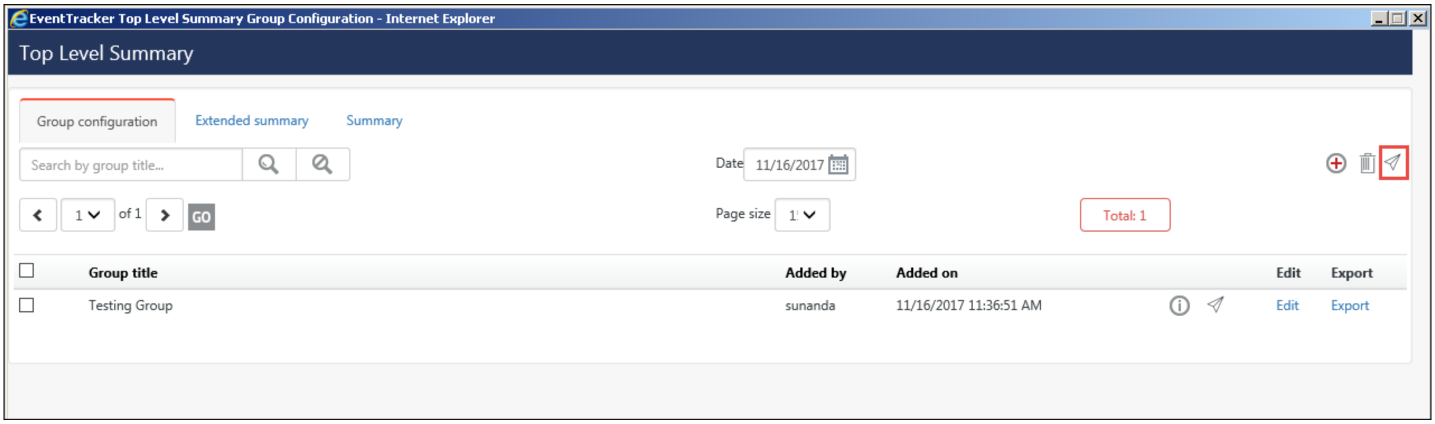
☐		Title	By	Type	Frequency	Next Run	On	Status		
☐		All error events	sunanda	Extended S...	Daily	Nov 17 12:00 AM	Nov 16 11:19 AM	Scheduled...	ⓘ	
☐		Compliance reports	chethan	Logs	Daily	Nov 16 05:30 PM	Nov 14 05:26 PM	Last run at...	ⓘ	

Figure 295

- To get the report(s) detail and history, click information ⓘ .

For configuring Top Level Summary,

- Click **Reports** > **Dashboard** > **Top Level Summary.**
- Click the group configuration icon ⊕ .
    - In the Top-Level Summary page, the **Send to Collection Master** ➢ , will be visible, for the existing group reports.



EventTracker Top Level Summary Group Configuration - Internet Explorer

Top Level Summary

Group configuration | Extended summary | Summary

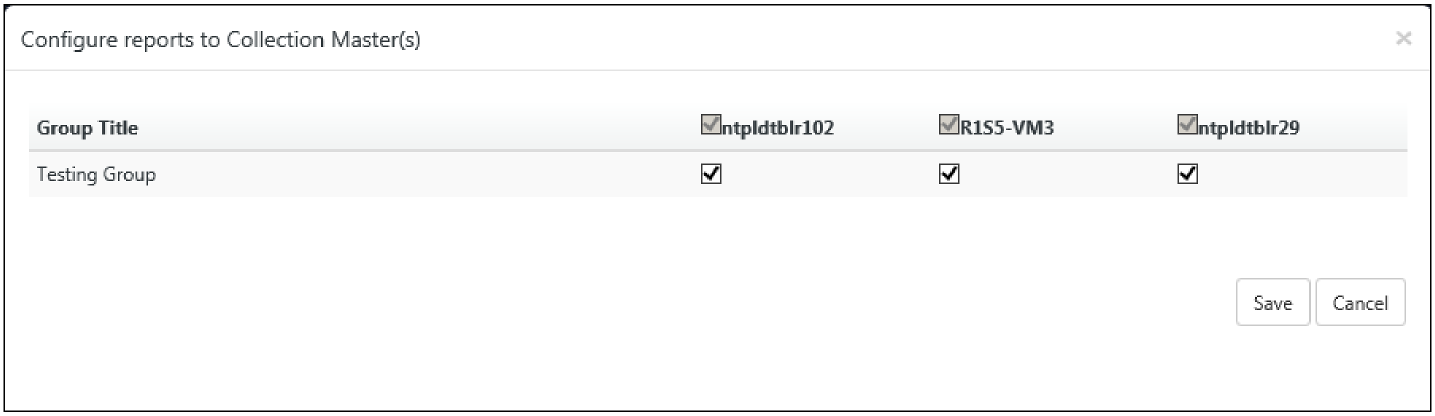
Search by group title... Date 11/16/2017

1 of 1 GO Page size 1 Total: 1

☐	Group title	Added by	Added on		Edit	Export
☐	Testing Group	sunanda	11/16/2017 11:36:51 AM	ⓘ ➢	Edit	Export

Figure 296

- Click the icon ➢ to forward the TLS reports to CM.
- Select the Collection Master(s) checkbox where you wish to forward the reports.



Configure reports to Collection Master(s)

Group Title	☑ntpldtblr102	☑R1S5-VM3	☑ntpldtblr29
Testing Group	☑	☑	☑

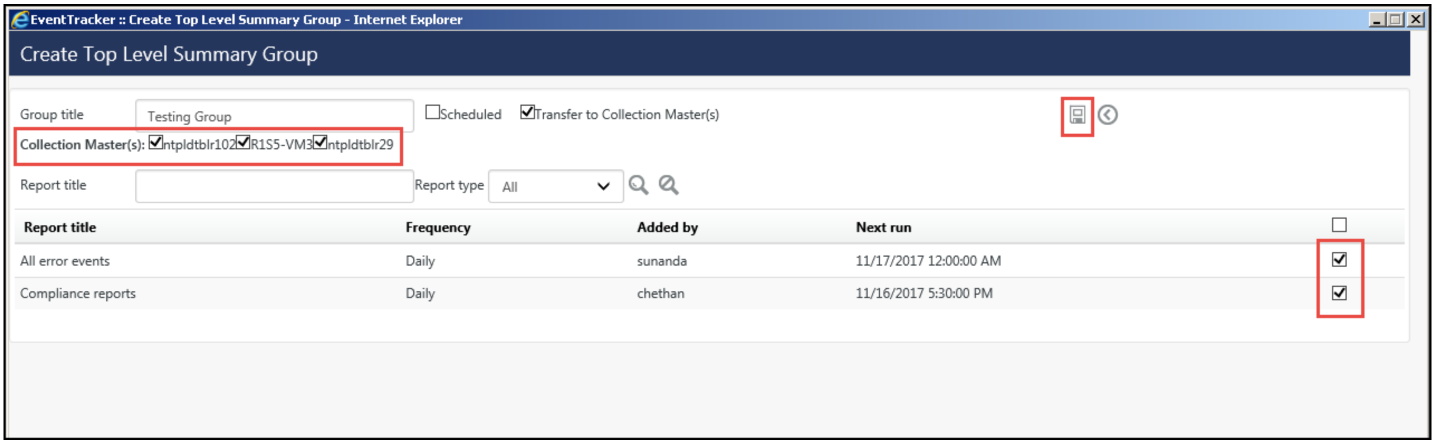
Save Cancel

Figure 297

- Click **Save**.

Also, while creating a new group in TLS, the user can send the group reports to the respective CM(s).

1. Click Add group ⊕ and create the group by selecting the reports.
2. Check the **Transfer to CM** checkbox and select the respective CM(s).
3. Click save 💾 after making the changes.
   This is shown in the figure below:



EventTracker :: Create Top Level Summary Group - Internet Explorer

Create Top Level Summary Group

Group title: Testing Group   ☐Scheduled   ☑Transfer to Collection Master(s)

Collection Master(s): ☑ntpldtblr102 ☑R1S5-VM3 ☑ntpldtblr29

Report title: Report type: All

Report title	Frequency	Added by	Next run	☐
All error events	Daily	sunanda	11/17/2017 12:00:00 AM	☑
Compliance reports	Daily	chethan	11/16/2017 5:30:00 PM	☑

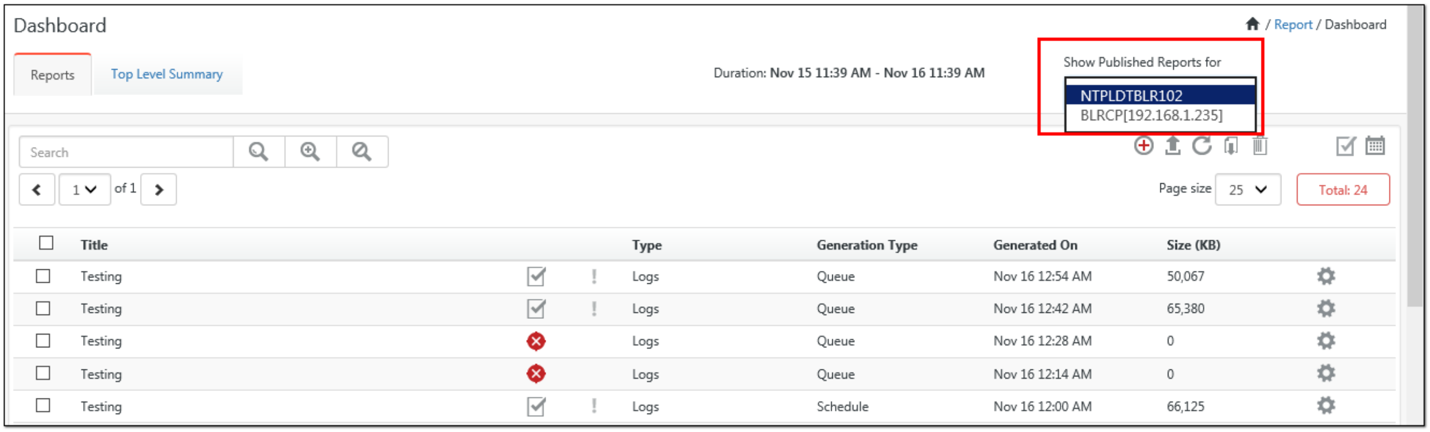
Figure 298

4.17 Collection Master

4.17.1 Viewing the CP generated reports

For Reports,

- Navigate to **Reports** > **Dashboard**.
- In the right-hand side, an option “**Show Published Report for**” is available.



Dashboard

Reports | Top Level Summary

Duration: Nov 15 11:39 AM - Nov 16 11:39 AM

Show Published Reports for: NTPLDTBLR102 / BLRCP[192.168.1.235]

/ Report / Dashboard

Search   1 of 1   Page size 25   Total: 24

☐	Title			Type	Generation Type	Generated On	Size (KB)	
☐	Testing	☑	!	Logs	Queue	Nov 16 12:54 AM	50,067	⚙
☐	Testing	☑	!	Logs	Queue	Nov 16 12:42 AM	65,380	⚙
☐	Testing	☒		Logs	Queue	Nov 16 12:28 AM	0	⚙
☐	Testing	☒		Logs	Queue	Nov 16 12:14 AM	0	⚙
☐	Testing	☑	!	Logs	Schedule	Nov 16 12:00 AM	66,125	⚙

Figure 299

NOTE

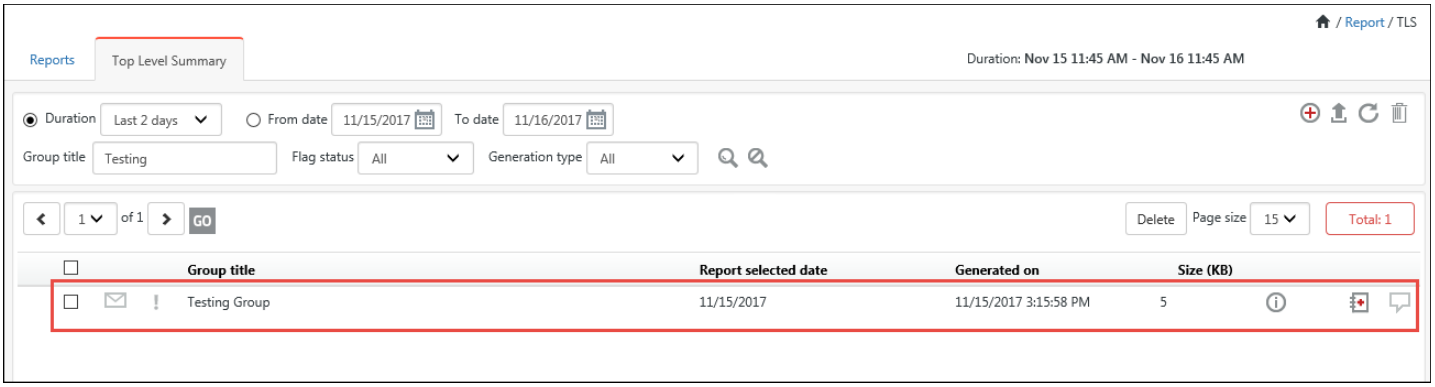
Click the ⚙ icon to add notes/add to Casebook or E-mail report. Refer: (Casebook).

- Select the Collection Point site from the drop-down list, for which you wish to view the report.

For Top Level Summary,

- In **Show Published reports for**, select the CP site from the dropdown box.

The report(s) opens.



Reports | Top Level Summary

Duration: Nov 15 11:45 AM - Nov 16 11:45 AM

● Duration: Last 2 days ○ From date: 11/15/2017 To date: 11/16/2017

Group title: Testing Flag status: All Generation type: All

			Group title	Report selected date	Generated on	Size (KB)
□		!	Testing Group	11/15/2017	11/15/2017 3:15:58 PM	5

Figure 300

5. Active Watch List

In this chapter, you will learn how to use:

- Active Watch List
- Create Groups
- Add new class
- Add a new pattern
- Import a list
- Delete a list/entity
- Link a group
- Move a group
- TAXII Server Configuration

5.1 Active Watch List

In large enterprise networks, network administrators have a busy schedule maintaining network and monitoring if nodes up and running 24/7.

There are many possible ways in which an enterprise network may be compromised. Like

- Users access various applications, web sites, and download some applications and install them.
- An external entity may access enterprise network, if it is connected to internet.

It will be a tedious task to monitor illegitimate activities unless an efficient monitoring or analysis tool is provided. In order to curb the irrelevant activities of users, we have introduced Active watch list feature where in all the actions can be monitored and necessary actions can be taken when required.

We can maintain a list of various classes and generate a list of activities of these entities.

To mention a few features,

- **IP Address:** An external access request from unknown IP
- **Port No:** If any external user is trying to connect to your local machine, then blacklisted port numbers can be tracked
- **Process**: Malicious processes can be monitored like Trojan.exe
- **Service**: Unknown service is being installed by users, which potentially degrade performance
- **IP Address and Port No:** In an enterprises network connected to internet, users may access data from outside the enterprise network. All the communication happens via IP addresses. Every request may not be legitimate; a hacker may also try to gain access to the network.

It is often necessary to know who is accessing the network. Is there any blacklisted IP address trying to access the network? How to audit IPs and publish such list of these IP activities?

Users can create list of IPs based on the security risk list done by some agencies like FBI, Google, etc or the enterprise itself may list certain IPs to monitor. Our application should provide a way to enlist IPs. Items in the IP list can be of any of the following format

- Wild character representation e.g. 123.234.*.12
- Range of IP e.g. 123.34.1-234
- CIDR format e.g. 123.45.78.34/26
- IP Address e.g. 123.45.67.4

Process: Often users download software's like Tools, Games, File Downloader which may harm system performance and compromise information. Such processes need to be tracked and alerted if the process is blacklisted, so that network administrator can take necessary actions.

Processes are executable files and always have '.exe' file extension. Some of these processes may harm performance and compromise information. Enlist any process name is executable (*.exe).

Service: There are numerous services available to download e.g. Desktop search by MS and Google, these processes frequently scan documents and keep them indexed for speedier search of documents. These are legitimate services because publishers are known. Many such services are available for download of which publisher and their purpose is unknown. Such process may harm performance and compromise information. It is necessary to keep audit of known and unknown services installed by user and check if any one of them is blacklisted.

Able to enlist service names which are alpha numeric text with valid set of special characters.

Users: Periodically companies may monitor certain employees who are suspected of malicious activities. It is necessary to monitor the logs generated having users from the monitored list.

Alpha numeric text with special chars allowed by active directory.

Serial Numbers: Serial numbers are associated with USB devices. USB memory sticks are major source of data theft; most of the enterprises disable USB drives. EventTracker's USB monitoring feature allows only registered (serial number) USB drives to connect.

5.1.1 Creating Active Watch List Groups

1. Log on to EventTracker.
2. Click the **Admin** menu, and then select **Active Watch List.**
   Active Watch List window opens.

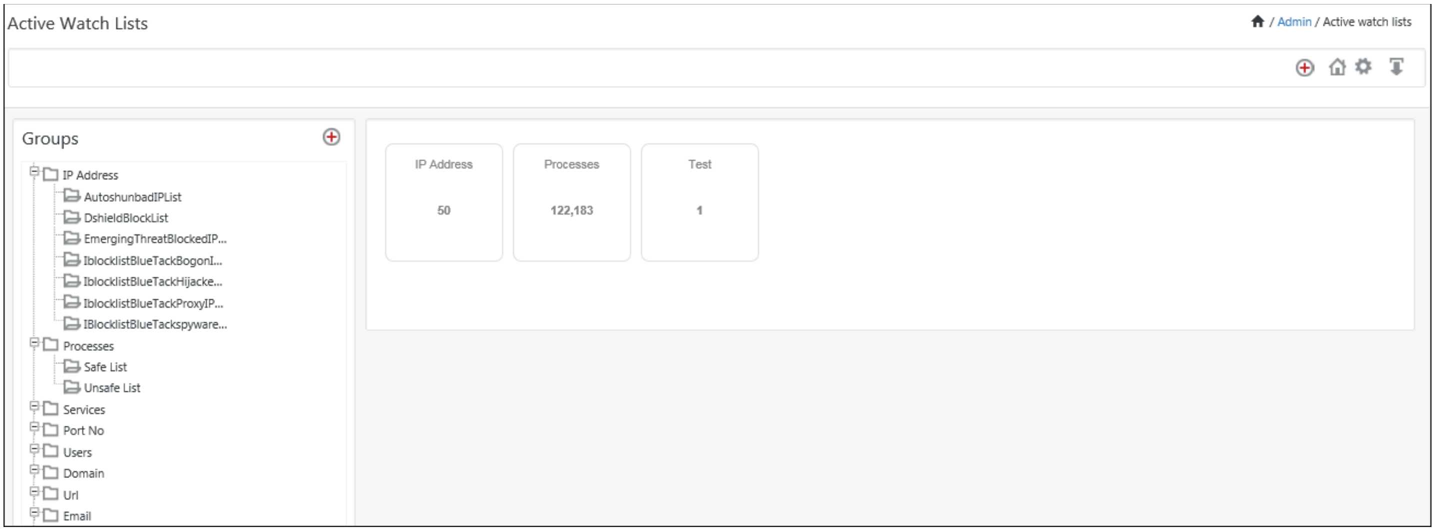

Active Watch Lists
/ Admin / Active watch lists
Groups
IP Address
AutoshunbadIPList
DshieldBlockList
EmergingThreatBlockedIP...
IblocklistBlueTackBogonI...
IblocklistBlueTackHijacke...
IblocklistBlueTackProxyIP...
IBlocklistBlueTackspyware...
Processes
Safe List
Unsafe List
Services
Port No
Users
Domain
Url
Email
IP Address
50
Processes
122,183
Test
1

Figure 301

3. To create a list for the respective groups, click ⊕ symbol.

Group window opens.

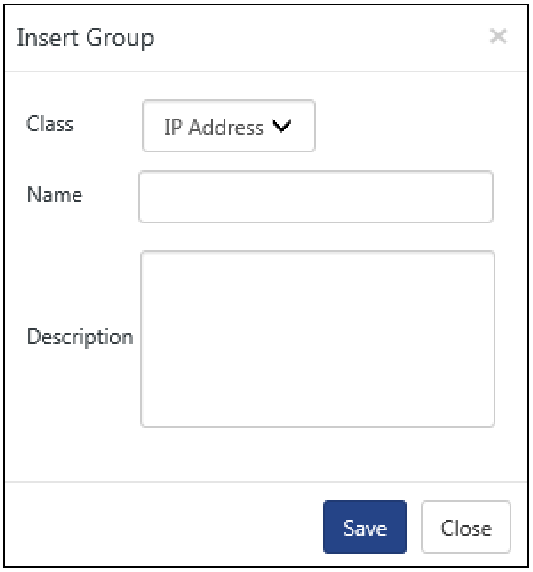


Figure 302

4. To select the respective class, select the **CLASS:** drop down list.

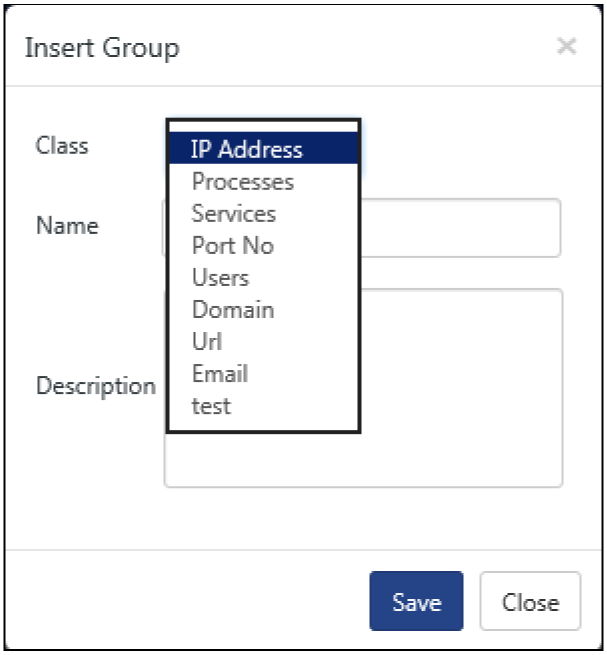


Figure 303

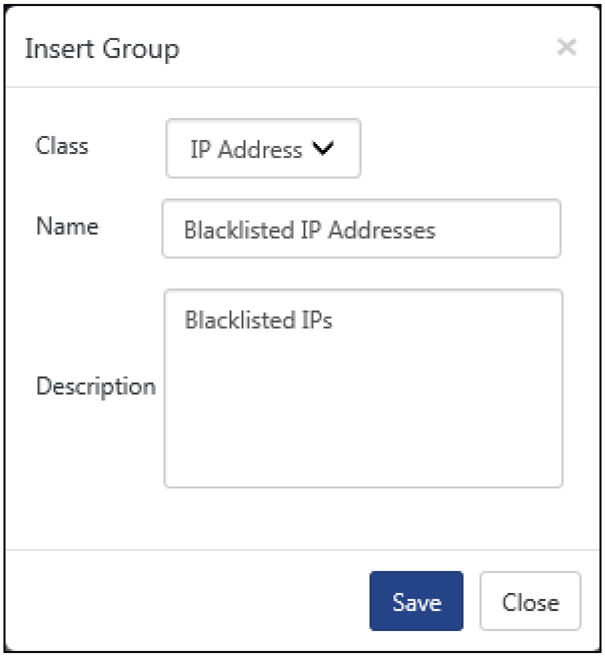
Field	Description
IP Address	Create a list of IP Addresses
Processes	Create a list of processes (executable files)
Services	Create a list of services
Port no	Create a list of port numbers
Users	Create a list of users

5. Select the required **CLASS**, enter an appropriate **NAME** and **DESCRIPTION**.
6. Click **SAVE**.

Ex: To create a list of blacklisted IP addresses.

a. In **CLASS:** drop down select **IP Address**, enter **NAME:** as '**BlackListed IP Addresses'**.

A group is created under IP Address list.


Insert Group

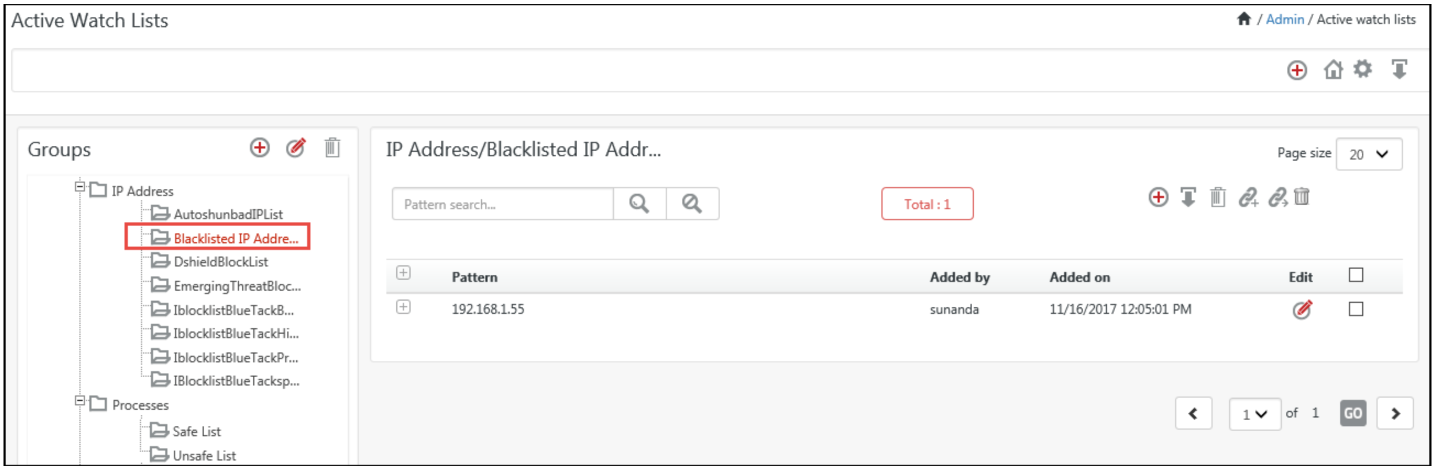
Class: IP Address

Name: Blacklisted IP Addresses

Description: Blacklisted IPs

Figure 304

You can view the created group in Active Watch List window.



Pattern	Added by	Added on	Edit	□
192.168.1.55	sunanda	11/16/2017 12:05:01 PM		□

Figure 305

b. Select the **Black Listed IP Addresses** link.

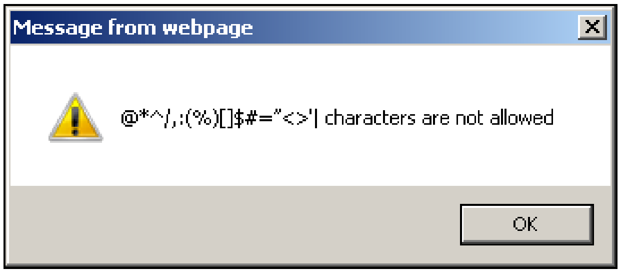
You can further continue to edit the groups and perform necessary actions like import, link and move which are explained in forthcoming sections.

Similarly, you can create a list of processes, services, port no, Users, Domain, URL etc.

7. To add a new group, click the ⊕ symbol in **GROUPS** pane and continue to add required groups for the necessary classes as explained above.

NOTE

If you enter a group name with special characters, then an error message opens.



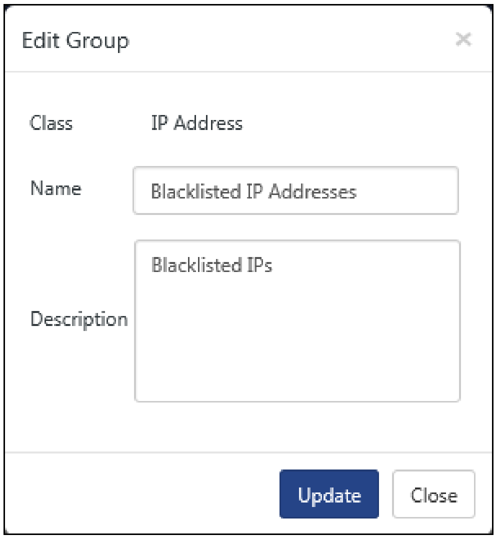
@*^/,:(%)[]$#="<>'| characters are not allowed

Figure 306

5.1.2 Editing Groups

1. To edit a group in **Groups** pane, click **Edit** ✎.

Group window opens.



Edit Group ×

Class IP Address

Name: Blacklisted IP Addresses

Description: Blacklisted IPs

Figure 307

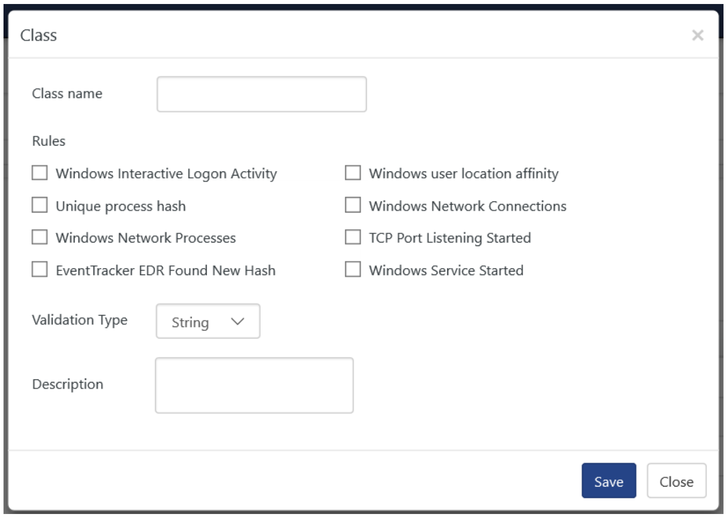
2. Enter relevant data and then click **Update**.

5.2 Adding a new class

To create a New Class,

1. Click **add** ⊕ icon in the right-hand corner.

   The Class window gets opens.



Class ×

Class name

Rules

- □ Windows Interactive Logon Activity
- □ Unique process hash
- □ Windows Network Processes
- □ EventTracker EDR Found New Hash
- □ Windows user location affinity
- □ Windows Network Connections
- □ TCP Port Listening Started
- □ Windows Service Started

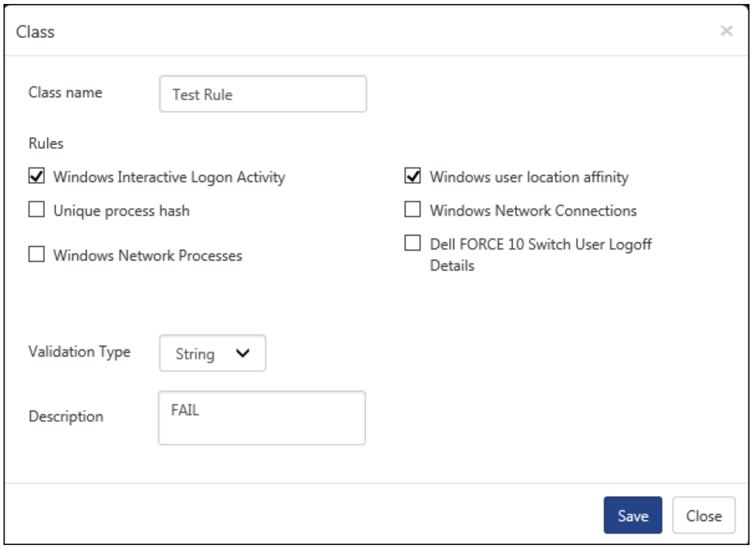
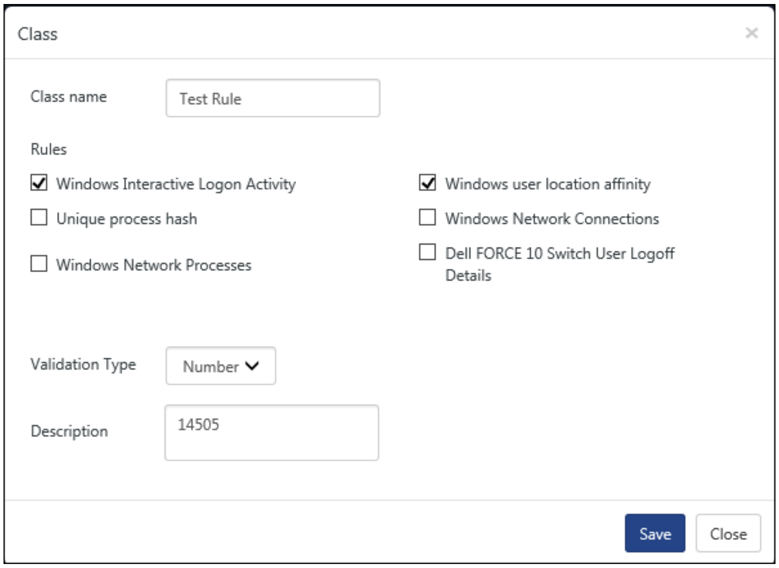
Validation Type: String

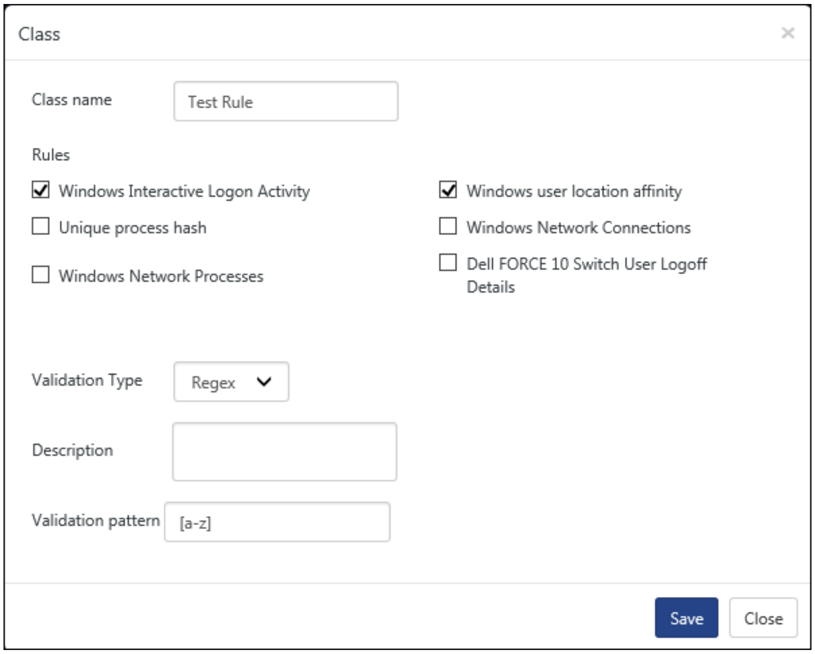
Description

Figure 308

2. Enter the Class name and select the Behavior Rule(s) checkbox that are to be mapped with the class.

3. Select the Validation Type from the dropdown list.

Field	Description
String	A String can be selected. Ex: FAIL  Class Class name: Test Rule Rules ☑ Windows Interactive Logon Activity ☑ Windows user location affinity ☐ Unique process hash ☐ Windows Network Connections ☐ Windows Network Processes ☐ Dell FORCE 10 Switch User Logoff Details Validation Type: String Description: FAIL
Number	A Number can be selected. Ex: 14505  Class Class name: Test Rule Rules ☑ Windows Interactive Logon Activity ☑ Windows user location affinity ☐ Unique process hash ☐ Windows Network Connections ☐ Windows Network Processes ☐ Dell FORCE 10 Switch User Logoff Details Validation Type: Number Description: 14505

Regex	A Regular Expression can be selected. Ex: [a-z] 

Class

Class name: Test Rule

Rules

☑ Windows Interactive Logon Activity
☑ Windows user location affinity
☐ Unique process hash
☐ Windows Network Connections
☐ Windows Network Processes
☐ Dell FORCE 10 Switch User Logoff Details

Validation Type: Regex

Description:

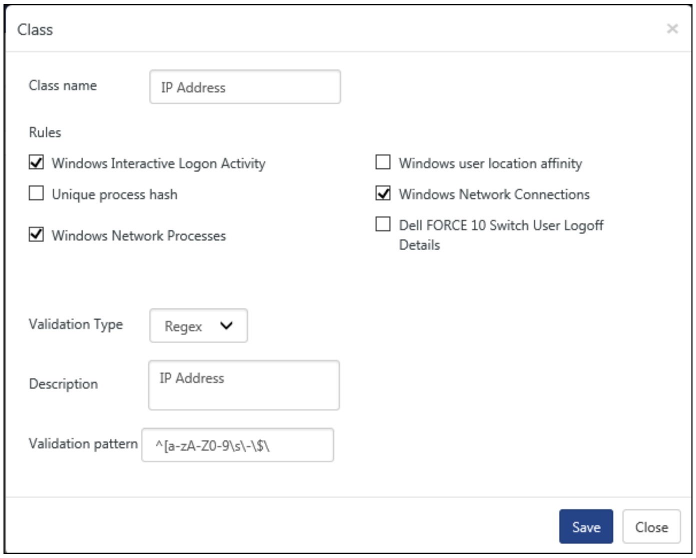
Validation pattern: [a-z]

5.2.1 Editing an Existing Class

To edit or modify an existing class,

1. Select the class and click **Edit** in the top right-hand side corner.

   The edit class window opens.



Class

Class name: IP Address

Rules

☑ Windows Interactive Logon Activity
☐ Windows user location affinity
☐ Unique process hash
☑ Windows Network Connections
☑ Windows Network Processes
☐ Dell FORCE 10 Switch User Logoff Details

Validation Type: Regex

Description: IP Address

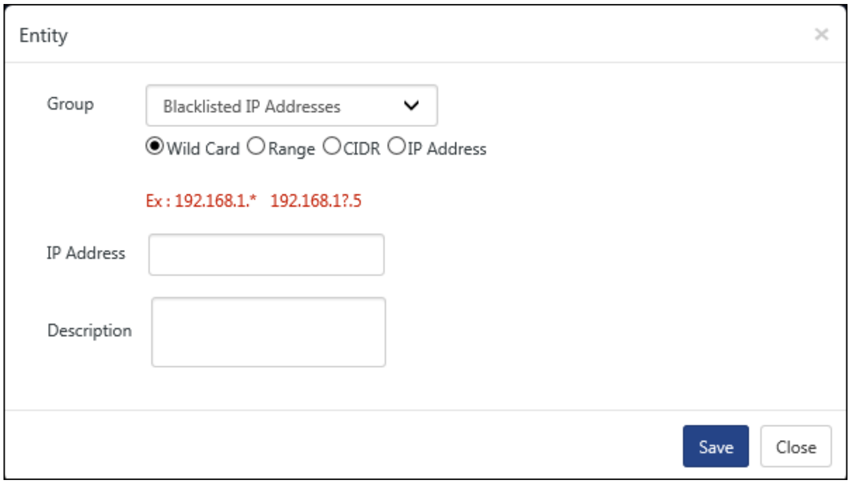
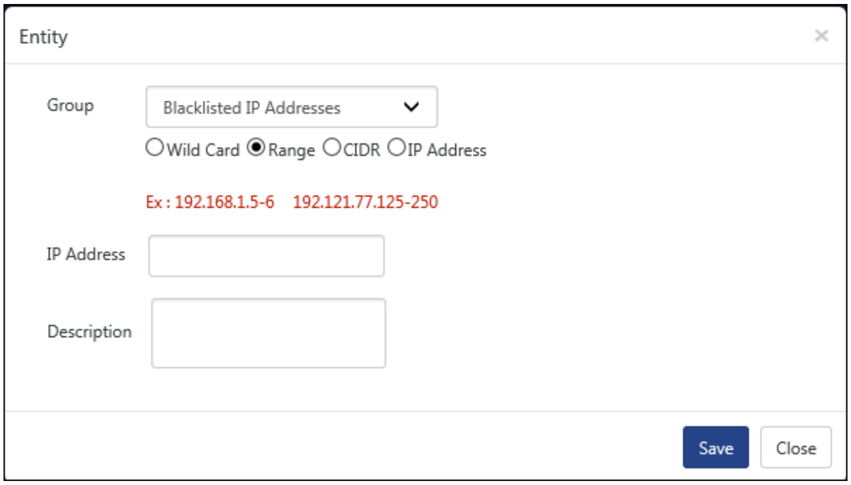
Validation pattern: ^[a-zA-Z0-9\s\-\$\

Figure 309

2. Make the changes required and click **Save**.

5.3 Adding a new pattern

1. Select the required group in **Groups** pane.
   Ex: BlackListed IP Addresses
2. To add a new pattern, select the ⊕ symbol in the right pane.
   Entity window opens.

Field	Description
Wild Card	A wild card entry can be entered. Ex: 13.34.34.*  Entity Group: Blacklisted IP Addresses ● Wild Card ○ Range ○ CIDR ○ IP Address Ex : 192.168.1.* 192.168.1?.5 IP Address Description Save Close
Range	A range of IP Addresses can be entered. Ex: 19.26.7.8-8  Entity Group: Blacklisted IP Addresses ○ Wild Card ● Range ○ CIDR ○ IP Address Ex : 192.168.1.5-6 192.121.77.125-250 IP Address Description Save Close

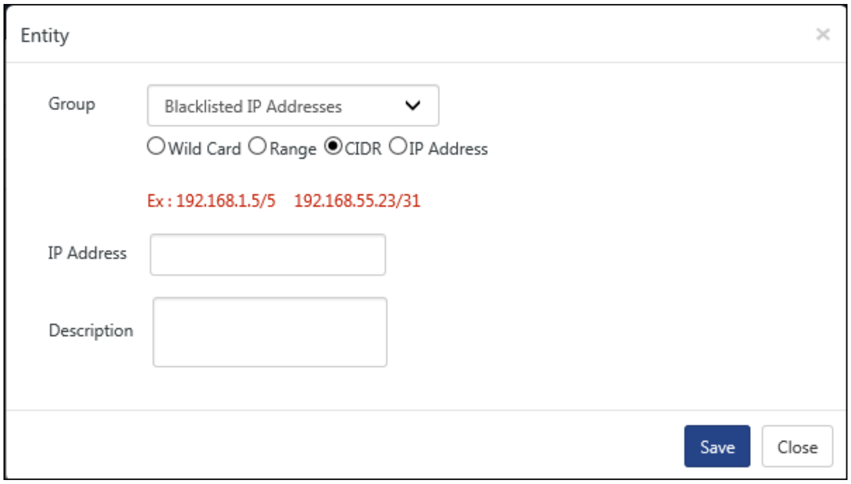
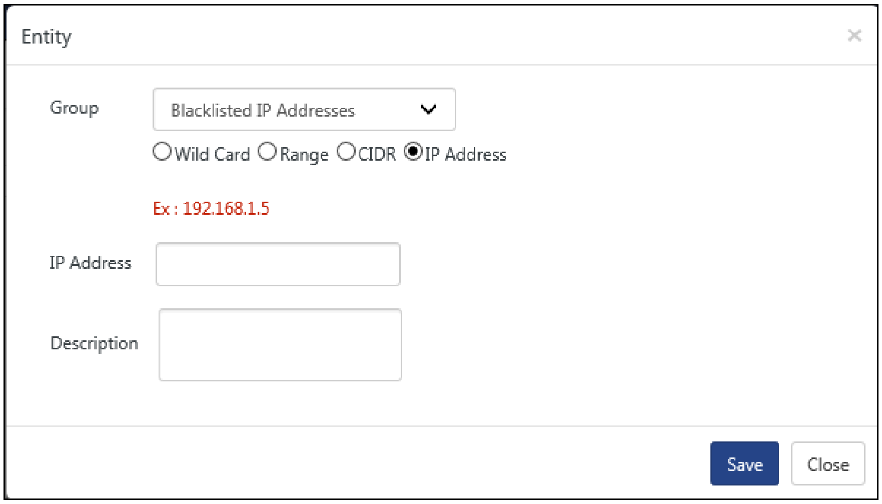
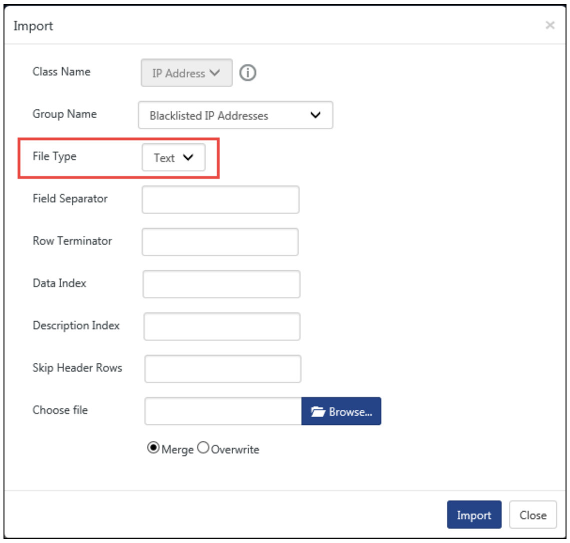
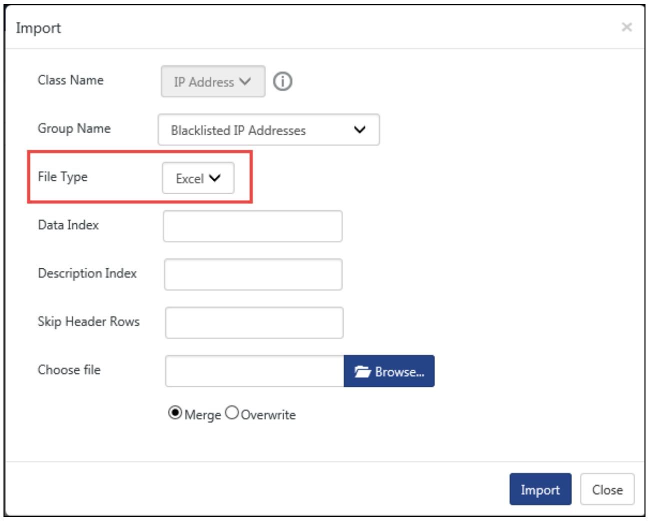
CIDR	IP addresses can be entered in CIDR format. Ex: 12.18.1.4/10  Entity Group: Blacklisted IP Addresses ○Wild Card ○Range ●CIDR ○IP Address Ex : 192.168.1.5/5 192.168.55.23/31 IP Address Description
IP Address	A valid IP address can be entered. Ex: 168.63.138.84  Entity Group: Blacklisted IP Addresses ○Wild Card ○Range ○CIDR ●IP Address Ex : 192.168.1.5 IP Address Description

Table 31

3. Enter the **IP Address:** in the required pattern and add a necessary **Description**.
4. Click **Save**.

5.4 Importing a list

1. To import a list of IP Addresses, click **Import** .
2. Select/enter correct values in the required fields. Click **Browse** and attach a **Text/CSV/Excel** file.

Field	Description	
Class Name	The class name in which you wish to import data is selected already.	
Group Name	Select the required group	
File Type	Text/CSV	a. Select the required File Type i.e. Text or CSV.  Import Class Name: IP Address ⓘ Group Name: Blacklisted IP Addresses File Type: Text Field Separator Row Terminator Data Index Description Index Skip Header Rows Choose file [Browse...] ● Merge ○ Overwrite [Import] [Close] b. Click ⓘ icon to know more details.
	Excel	c. Select File Type as Excel.  Import Class Name: IP Address ⓘ Group Name: Blacklisted IP Addresses File Type: Excel Data Index Description Index Skip Header Rows Choose file [Browse...] ● Merge ○ Overwrite [Import] [Close] d. Click ⓘ icon to know more details.
Field Separator		Space '\s', Tab '\t', semi colon ';', colon ':', comma ',' etc. NOTE: This option is not available in Excel File Type.

Row terminator	New line ‘\n’, Carriage Return ‘\r’ NOTE: This option is not available in Excel File Type.
Data Index	It is the columns that are been indexed. In Text/CSV File Type, you can enter only numbers. In Excel File Type, you can enter only alphabets.
Description Index	A valid number or Alphabet and this field is Optional. In Text/CSV File Type, you can enter only numbers. In Excel File Type, you can enter only alphabets.
Skip Header Rows	You can input a number.
Choose file	Click the Browse… button and select the file from local drive.
Merge/ Overwrite	You merge or overwrite an existing list. **NOTE**: If you click on merge, then the list will be merged with the existing one. If you click on overwrite then the previous list will be removed, and the new list will be updated.

Table 32

3. Select **Import**.

   The relevant data will be imported accordingly.

🗎 NOTE

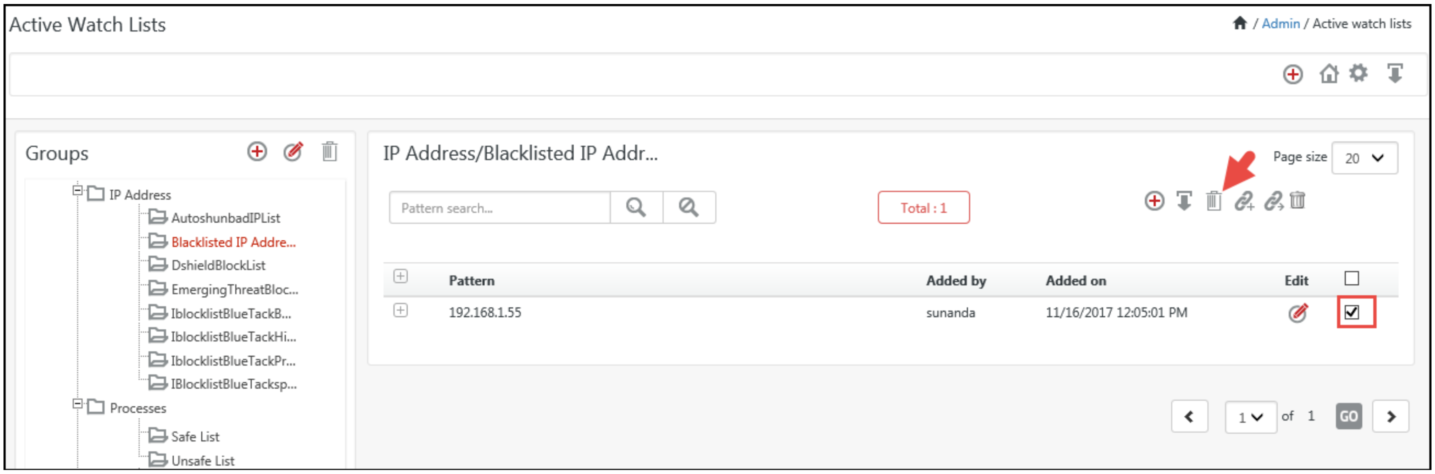
Duplicate entries are not imported.

5.4.1 Deleting a list/entity

1. To delete a pattern, select the required pattern option.

   Ex:

   To delete IP address, check the correct option.



Pattern	Added by	Added on	Edit	□
192.168.1.55	sunanda	11/16/2017 12:05:01 PM		☑

Figure 310

2. Click **Delete** .

   A message displays requesting for confirmation to delete.

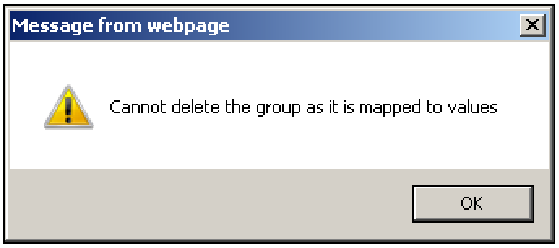
3. Click **OK**.

   A successful message opens.

   The relevant IP address is deleted from IP Address/Black Listed IP Addresses group.

NOTE

The same applies to a group also. If you want to delete a group, then you must first delete the list otherwise a warning message displays.



Cannot delete the group as it is mapped to values

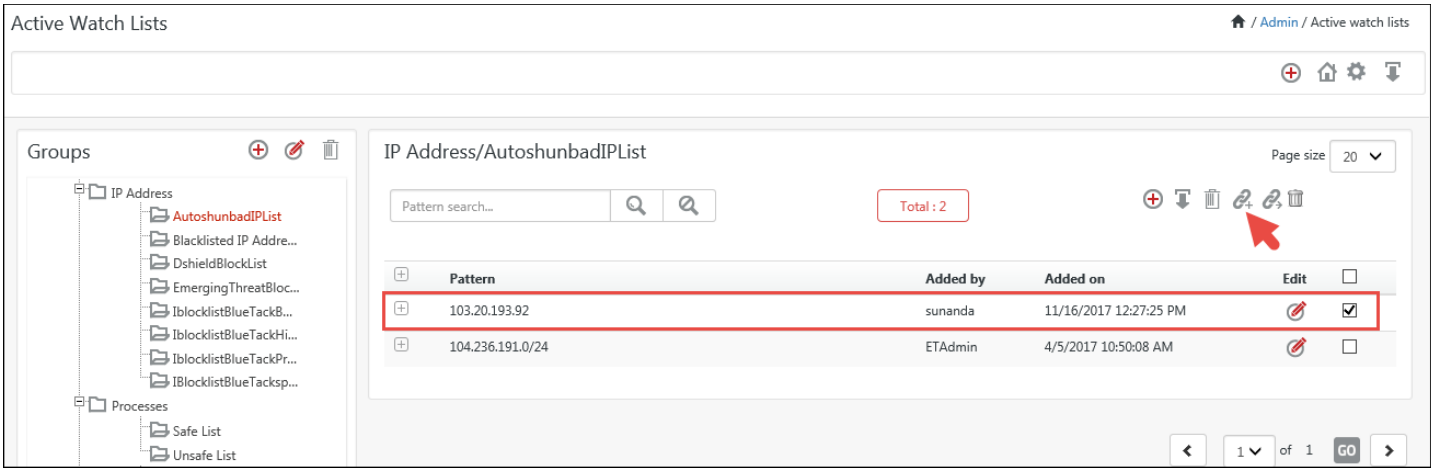
Figure 311

5.4.2 Linking to group

1. To link a pattern to another group,

   Ex:

   a. To link an IP address 103.20.193.92 from **AutoshunbadIPList** group to **New Group**, check the respective option and click **Link to group** .

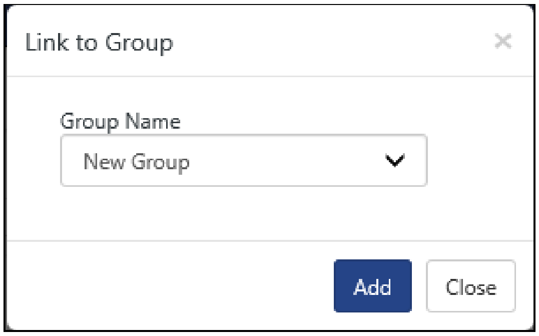


	Pattern	Added by	Added on	Edit	□
⊞	103.20.193.92	sunanda	11/16/2017 12:27:25 PM		☑
⊞	104.236.191.0/24	ETAdmin	4/5/2017 10:50:08 AM		□

Figure 312

Link to Group window opens:

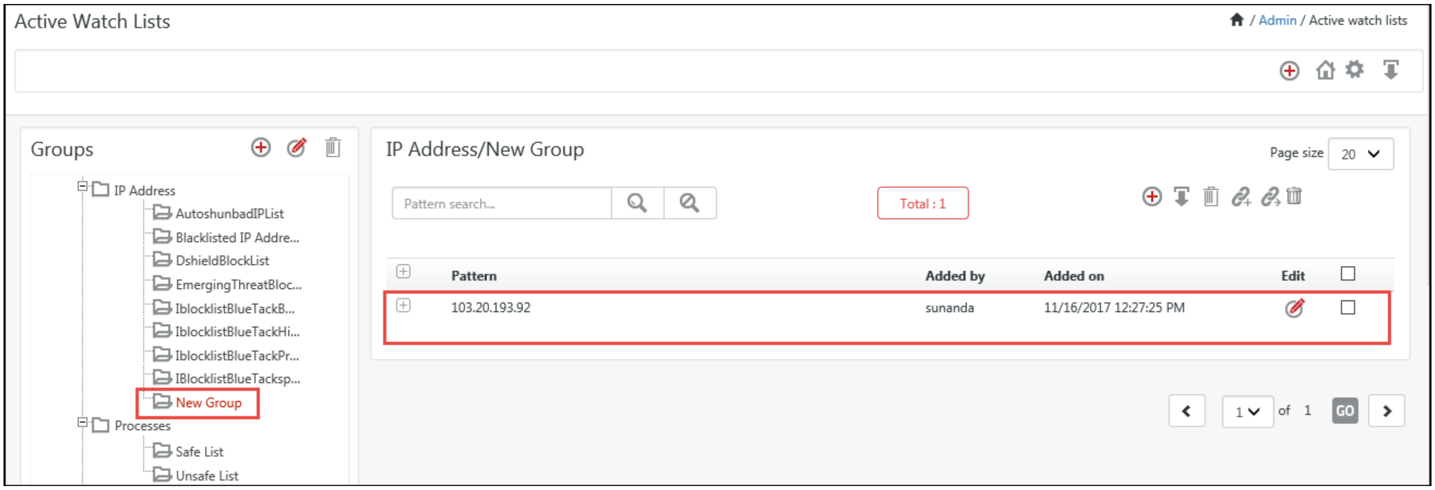
b. Select the **Group Name**, and then select **Add**.



Group Name: New Group

Figure 313

The IP address 103.20.193.92 is successfully linked to New Group.



	Pattern	Added by	Added on	Edit	□
⊞	103.20.193.92	sunanda	11/16/2017 12:27:25 PM		□

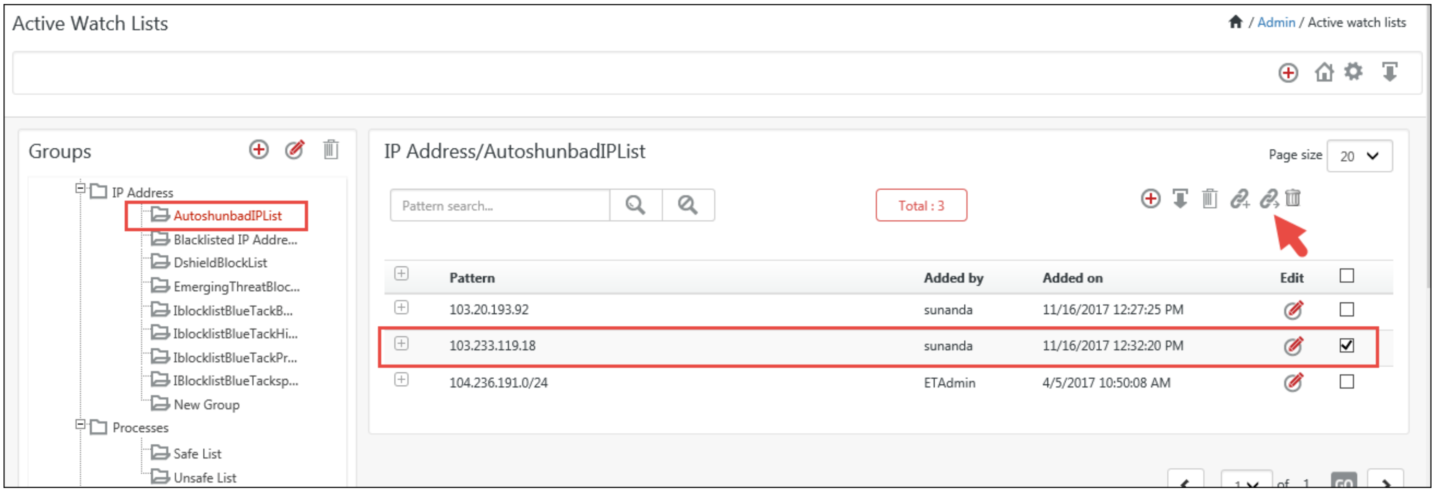
Figure 314

5.4.3 Moving to Group

1. To move a pattern to another group,

   Ex:

   a. To move the IP address 103.233.119.18 from **AutoshunbadIPList** group to **New Group**, check the required option and, click **Move to group** .

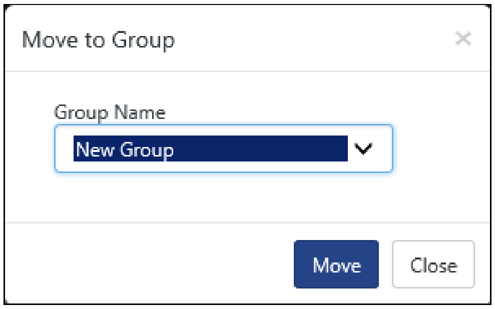


Pattern	Added by	Added on	Edit	□
103.20.193.92	sunanda	11/16/2017 12:27:25 PM		□
103.233.119.18	sunanda	11/16/2017 12:32:20 PM		☑
104.236.191.0/24	ETAdmin	4/5/2017 10:50:08 AM		□

Figure 315

   Move to group window opens.

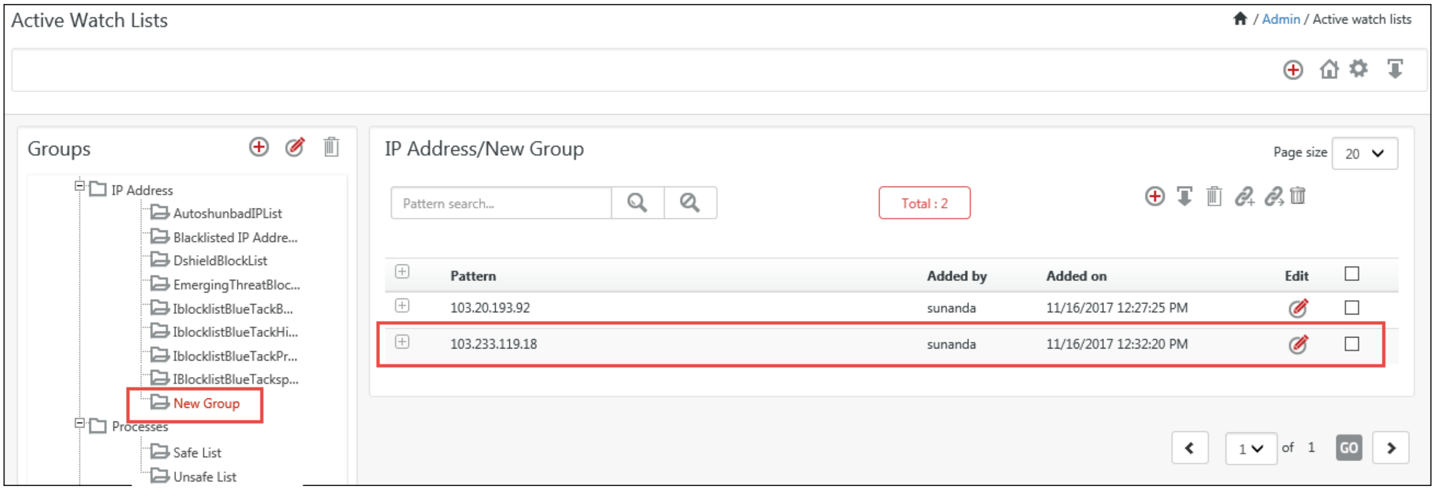
   b. Select the **Group Name**, and then select **Move**.



Group Name: New Group

Figure 316

   The IP address 103.233.119.18 is successfully moved to New Group.



Pattern	Added by	Added on	Edit	□
103.20.193.92	sunanda	11/16/2017 12:27:25 PM		□
103.233.119.18	sunanda	11/16/2017 12:32:20 PM		□

Figure 317

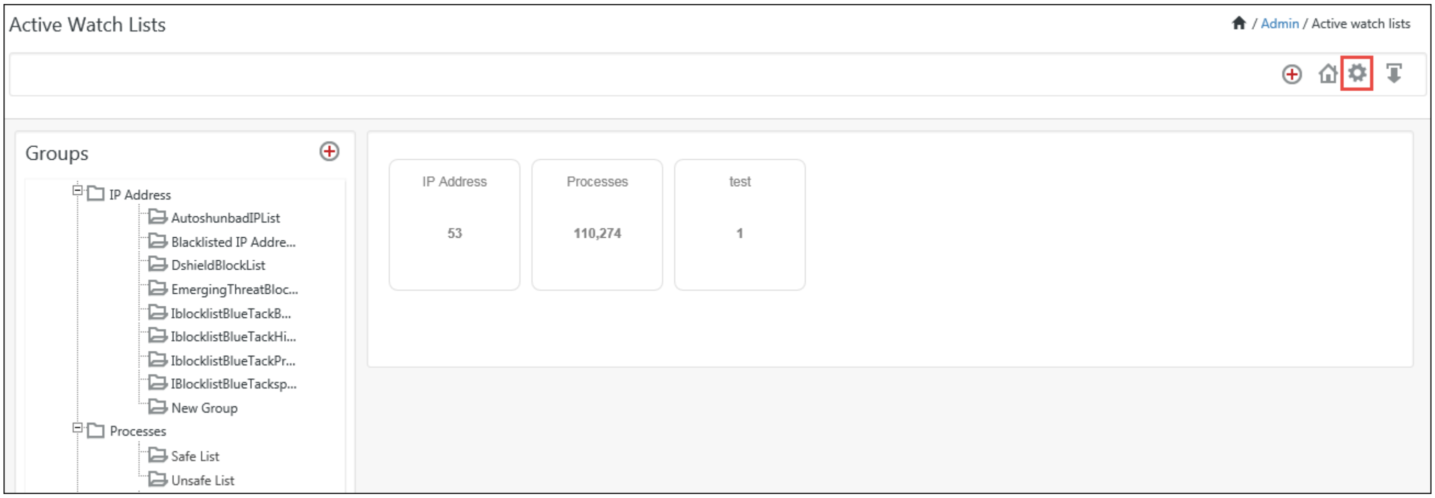
To monitor the usage of IP addresses and processes, please refer [Behavior -> IP Address Activity or Process Activity.]()

To learn more about the usage of entities in Active Watch List, command line usage etc, please refer https://www.netsurion.com/Corporate/media/Corporate/Files/Support-Docs/Active-Watch-List-and-its-Usage.pdf

5.5 TAXII Server Configuration

This feature will connect to any of the TAXII Server(s) to collect the Cyber Threat information to EventTracker.

To configure TAXII feeds, click the icon ⚙.



IP Address	Processes	test
53	110,274	1

Figure 318

The TAXII server configuration page opens. Click the **Add Feed**.

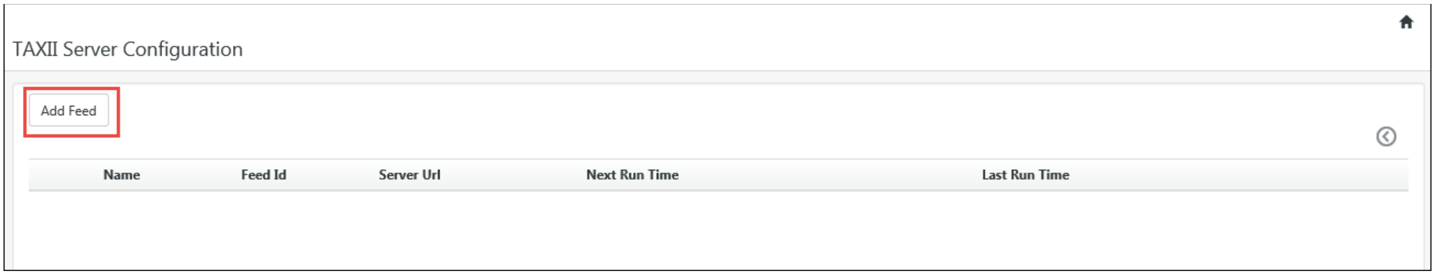


Figure 319

The Configuration page opens. Enter the configuration details.

1. **Name:** Provide a User-friendly name to identify the TAXII feed.

   Example: BlackListedIP

2. **Feed Id:** Feed Id/Collection Name available on TAXII server from which data needs to be fetched.

   Example: guest.MalwareDomainList_Hostlist

3. **Server URL**: Complete TAXII server endpoint URL.

   Example: http://hailataxii.com/taxii-discovery-service

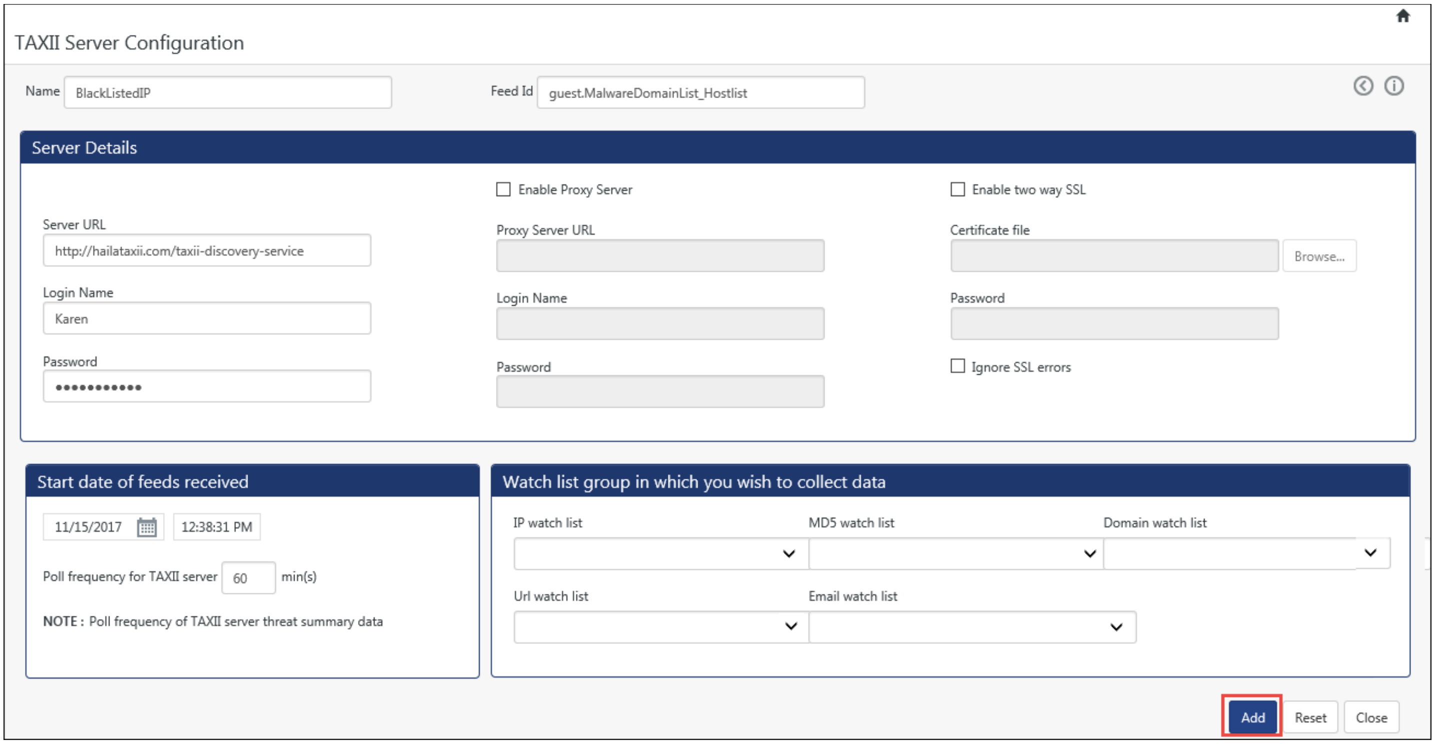
4. **Login Name:** Username that is to be used for authenticating with the TAXII server.
5. **Password:** Password that is to be used for authenticating with the TAXII server.
6. **Enable Proxy Server:** To use proxy for internet connectivity. (If the organization's internet connectivity is running with proxy connection).
7. **Proxy Server URL:** URL of the proxy server.
8. **Login Name:** Username that is to be used for authenticating with the Proxy server.
9. **Password:** Password that is to be used for authenticating with the Proxy server.
10. **Enable two way SSL:** To authenticate client for SSL using certificate.
11. **Certificate file:** Certificate file to be used for client-side SSL authentication.

    Example: G:\TAXIIServer\admin.p12

12. **Password:** Password for the client certificate file.
13. **Ignore SSL errors:** To ignore the SSL errors.
14. **From date:** By default, it will select the frequency of 24 hours and the current system time when the feed is added.
15. **From time:** System Current time (as explained above).
16. **Poll frequency for TAXII server:** This is the time interval used between each connection request to the TAXII server.

Below are the names of the watch list groups in which the user(s) wishes to collect the data. Default classes are IP Address, MD5, Domain, and URL.

- IP watch list
- MD5 watch list
- Domain watch list
- URL watch list



TAXII Server Configuration

Name: BlackListedIP Feed Id: guest.MalwareDomainList_Hostlist

Server Details

Server URL: http://hailataxii.com/taxii-discovery-service

Login Name: Karen

Password: ●●●●●●●●●●●

□ Enable Proxy Server

Proxy Server URL

Login Name

Password

□ Enable two way SSL

Certificate file

Password

□ Ignore SSL errors

Start date of feeds received

11/15/2017 12:38:31 PM

Poll frequency for TAXII server 60 min(s)

NOTE : Poll frequency of TAXII server threat summary data

Watch list group in which you wish to collect data

IP watch list

MD5 watch list

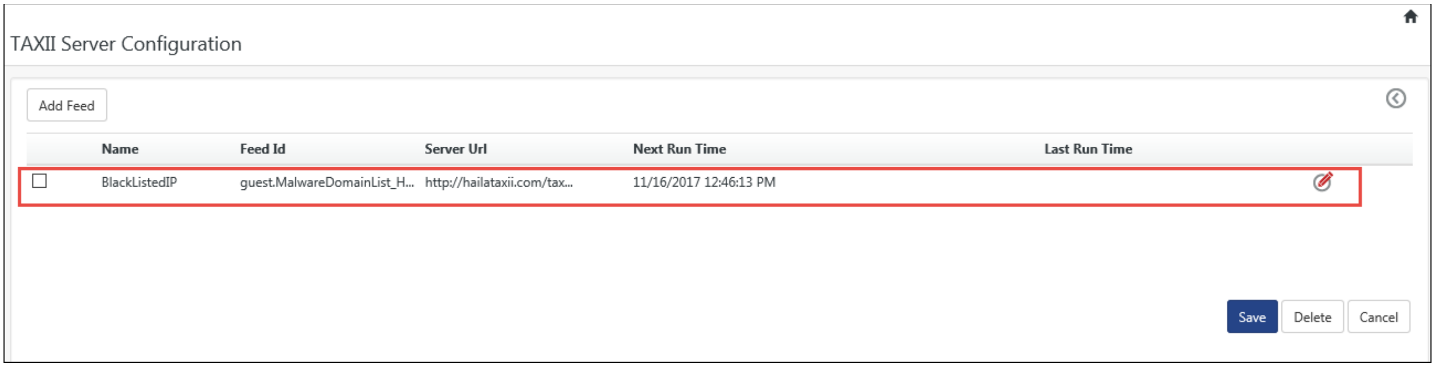
Domain watch list

Url watch list

Email watch list

Figure 320

The added TAXII configuration opens. Click **Save**.



TAXII Server Configuration

	Name	Feed Id	Server Url	Next Run Time	Last Run Time
□	BlackListedIP	guest.MalwareDomainList_H...	http://hailataxii.com/tax...	11/16/2017 12:46:13 PM	

Figure 321

6. Alerts

In this chapter, you will learn about:

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

6.1 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

6.2 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.

Risk	
T	Threat level (how severe the Alert is) assigned while creating Alerts.
A	Asset value of the system (how important or critical the computer is) set through the System Manager.
V	Vulnerability (how vulnerable the computer is) automatically updated using third party vulnerability assessment reports.

Table 33

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.

6.2.1 Alert Email Template feature

The **Alert Email Template** feature will now allow the user to extract the value from the event and prepare Alert description format based on selected email Template. The user will have an option to select the emai l template for the alert email.

To make the email more precise the user is allowed to customize the alert email using short description with plan text/HTML format as per their requirement.

6.2.2 Configuring Alerts with Active Watch List

The user(s) can configure alerts by extracting the values from the event and compare it against the Active Watch List. If the admin maintains a local black/white list data, he/she can configure the alerts and compare it with Active Watch list, based on which the alert will be triggered.

- Go to **Admin-> Alerts**. In the Alert Management page, click **Add Alert**.
- Enter the Alert name and the other required fields.

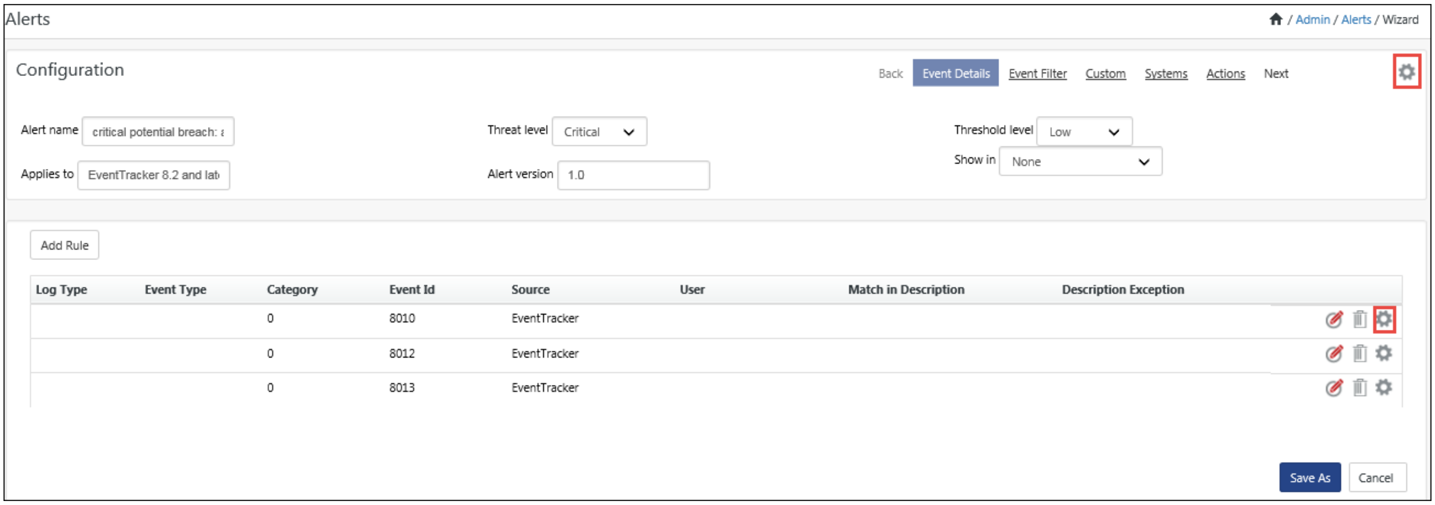
NOTE: Follow the steps in the document "**BDS Alert Configuration**" for extracting values.

In the below example, we have taken the extraction method as "**Regular Expression**" for Alert "**Critical Potential Breach from low reputation IP**".

- Configure the alert using Event level configuration or Alert level configuration.
- Go to **Admin-> Alerts**. In the Alert Management page, click **Add Alert**.
- Enter the Alert name and the other required fields.

In the below example, we have taken the extraction method as "**Regular Expression**" for Alert "**EventTracker: Critical Potential Breach from low reputation IP**".

- Configure the alert using Event level configuration or Alert level configuration.



Configuration

Alert name: critical potential breach: a

Applies to: EventTracker 8.2 and lat

Threat level: Critical

Alert version: 1.0

Threshold level: Low

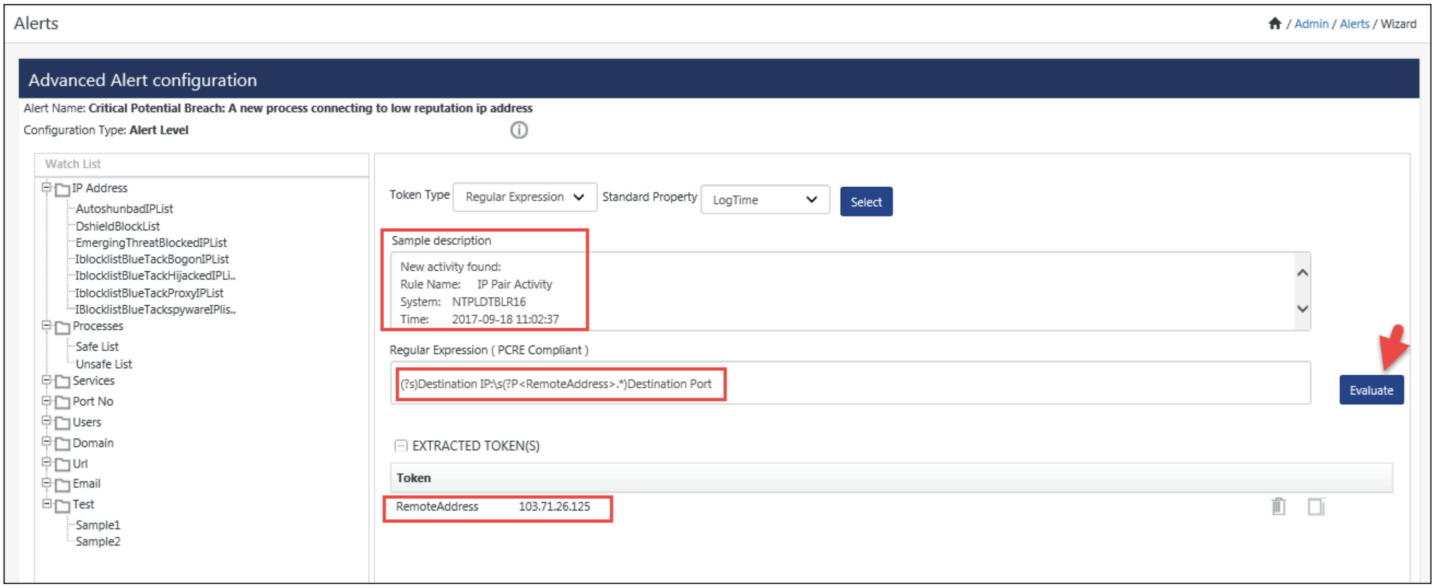
Show in: None

Log Type	Event Type	Category	Event Id	Source	User	Match in Description	Description Exception
		0	8010	EventTracker			
		0	8012	EventTracker			
		0	8013	EventTracker			

Figure 322

- Select the **Token Type** as Regular Expression.
- Enter the Sample Description, Regular Expression and a Short Description.

Here we have extracted the value "**RemoteAddress**".


Alerts
/ Admin / Alerts / Wizard
Advanced Alert configuration
Watch List
IP Address
AutoshunbadIPList
DshieldBlockList
EmergingThreatBlockedIPList
IblocklistBlueTackBogonIPList
IblocklistBlueTackHijackedIPLi..
IblocklistBlueTackProxyIPList
IBlocklistBlueTackspywareIPlis..
Processes
Safe List
Unsafe List
Services
Port No
Users
Domain
Url
Email
Test
Sample1
Sample2
Select
Evaluate

Alert Name: **Critical Potential Breach: A new process connecting to low reputation ip address**

Configuration Type: **Alert Level**

Token Type: Regular Expression

Standard Property: LogTime

Sample description

```
New activity found:
Rule Name:     IP Pair Activity
System:    NTPLDTBLR16
Time:      2017-09-18 11:02:37
```

Regular Expression (PCRE Compliant)

```
(?s)Destination IP:\s(?P<RemoteAddress>.*)Destination Port
```

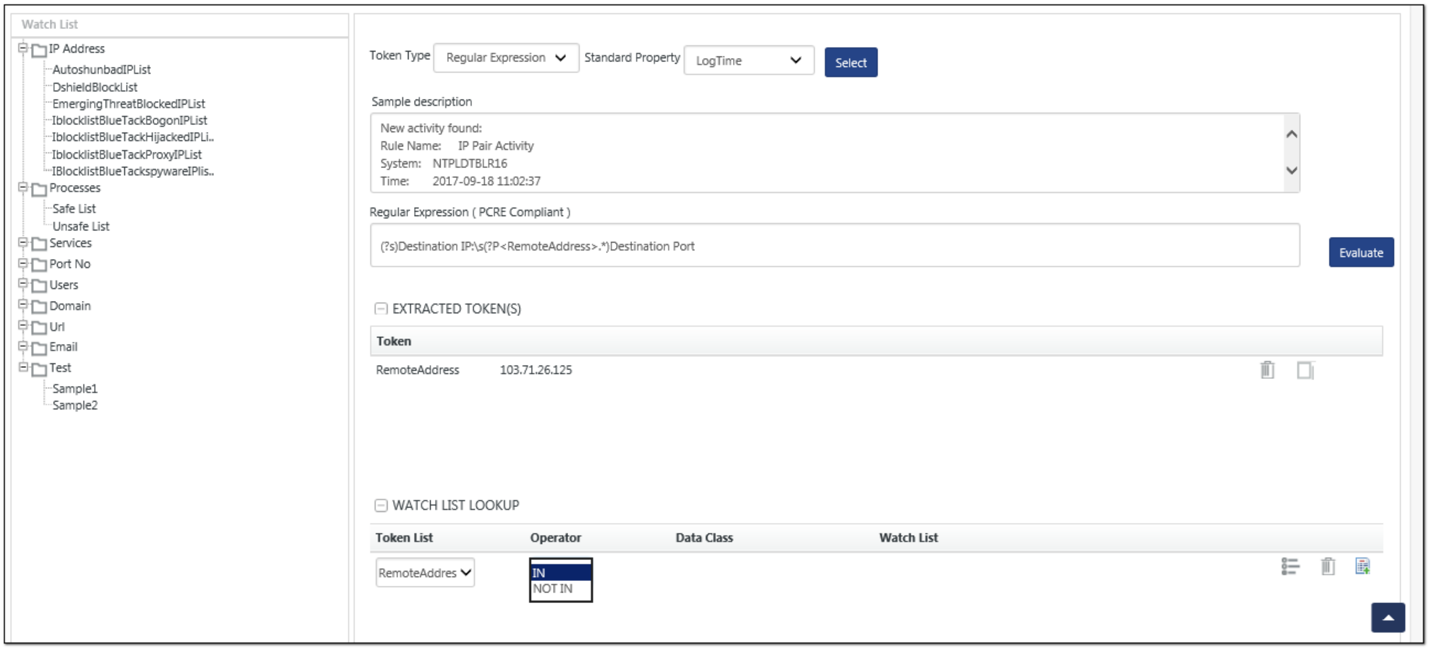
EXTRACTED TOKEN(S)

Token	
RemoteAddress	103.71.26.125

Figure 323

The extracted values is displayed in the Watch List Lookup pane.

- Click the lookup icon to add data class and watch list.



Watch List

- IP Address
  - AutoshunbadIPList
  - DshieldBlockList
  - EmergingThreatBlockedIPList
  - IblocklistBlueTackBogonIPList
  - IblocklistBlueTackHijackedIPLi..
  - IblocklistBlueTackProxyIPList
  - IBlocklistBlueTackspywareIPlis..
- Processes
  - Safe List
  - Unsafe List
- Services
- Port No
- Users
- Domain
- Url
- Email
- Test
  - Sample1
  - Sample2

Token Type: Regular Expression; Standard Property: LogTime; Select

Sample description

```
New activity found:
Rule Name:    IP Pair Activity
System:    NTPLDTBLR16
Time:    2017-09-18 11:02:37
```

Regular Expression (PCRE Compliant)

```
(?s)Destination IP:\s(?P<RemoteAddress>.*)Destination Port
```

Evaluate

EXTRACTED TOKEN(S)

Token	
RemoteAddress	103.71.26.125

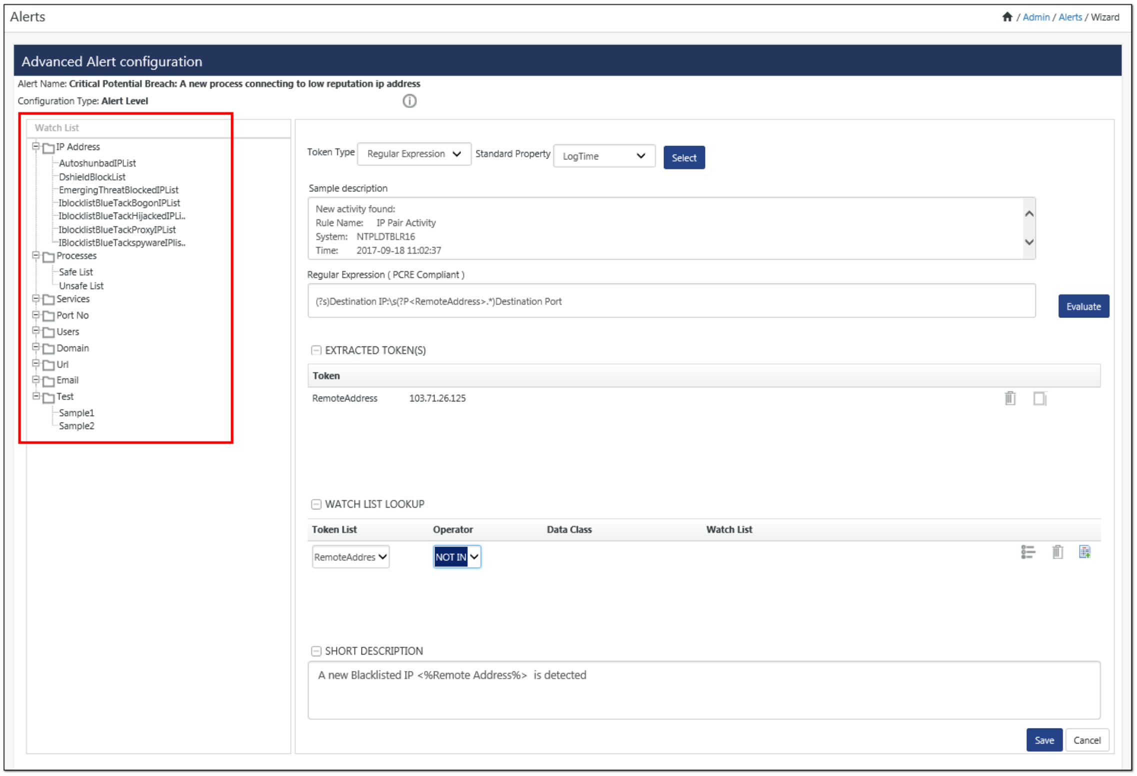
WATCH LIST LOOKUP

Token List	Operator	Data Class	Watch List
RemoteAddres	IN NOT IN		

Figure 324

From the Watch List tree, select the class or group to add to the watch list.

The user can also select Operator as IN or NOT IN as per the user preference.



Alerts

/ Admin / Alerts / Wizard

Advanced Alert configuration

Alert Name: **Critical Potential Breach: A new process connecting to low reputation ip address**

Configuration Type: **Alert Level**

Watch List

- IP Address
  - AutoshunbadIPList
  - DshieldBlockList
  - EmergingThreatBlockedIPList
  - IblocklistBlueTackBogonIPList
  - IblocklistBlueTackHijackedIPLi..
  - IblocklistBlueTackProxyIPList
  - IBlocklistBlueTackspywareIPlis..
- Processes
  - Safe List
  - Unsafe List
- Services
- Port No
- Users
- Domain
- Url
- Email
- Test
  - Sample1
  - Sample2

Token Type: Regular Expression; Standard Property: LogTime; Select

Sample description

```
New activity found:
Rule Name:    IP Pair Activity
System:    NTPLDTBLR16
Time:    2017-09-18 11:02:37
```

Regular Expression (PCRE Compliant)

```
(?s)Destination IP:\s(?P<RemoteAddress>.*)Destination Port
```

Evaluate

EXTRACTED TOKEN(S)

Token	
RemoteAddress	103.71.26.125

WATCH LIST LOOKUP

Token List	Operator	Data Class	Watch List
RemoteAddres	NOT IN		

SHORT DESCRIPTION

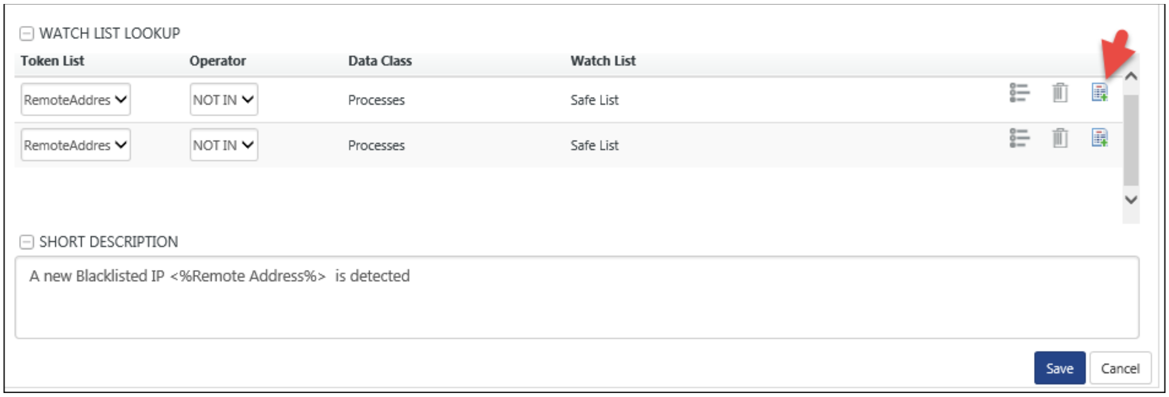
A new Blacklisted IP <%Remote Address%> is detected

Save Cancel

Figure 325

To add multiple lookup for the extracted token, click **clone** , to duplicate the record. Now the user can change the duplicated records as per requirement.

For example, we have taken the extracted token “**RemoteAddress**” and added the watch list “**Safe List**” by selecting it from the watch list tree.



⊟ WATCH LIST LOOKUP

Token List	Operator	Data Class	Watch List
RemoteAddres	NOT IN	Processes	Safe List
RemoteAddres	NOT IN	Processes	Safe List

⊟ SHORT DESCRIPTION

A new Blacklisted IP <%Remote Address%> is detected

Figure 326

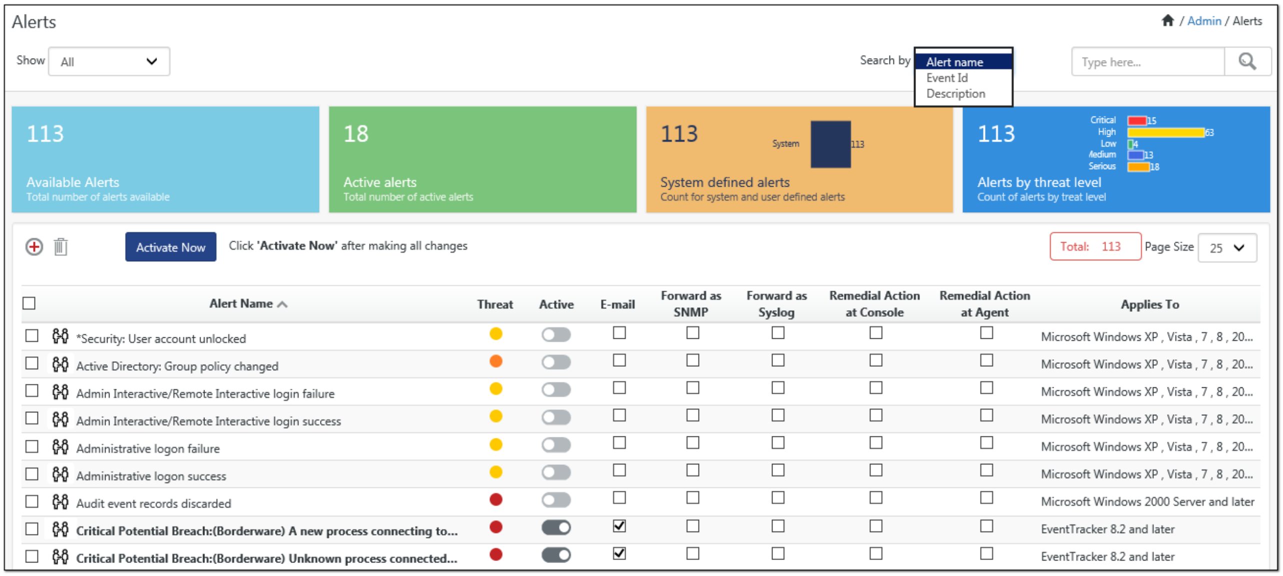
- To save the configuration, click **Save** and **Finish**.

6.3 Adding Custom Alerts

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

1 To add custom alerts, click **Admin**, and then click **Alerts**.

EventTracker opens **Alert Management** page.



Alerts

113 Available Alerts
Total number of alerts available

18 Active alerts
Total number of active alerts

113 System defined alerts
Count for system and user defined alerts

113 Alerts by threat level
Count of alerts by treat level

Click **'Activate Now'** after making all changes

Total: 113 Page Size 25

□	Alert Name	Threat	Active	E-mail	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
□	*Security: User account unlocked	●	○	□	□	□	□	□	Microsoft Windows XP , Vista , 7 , 8 , 20...
□	Active Directory: Group policy changed	●	○	□	□	□	□	□	Microsoft Windows XP , Vista , 7 , 8 , 20...
□	Admin Interactive/Remote Interactive login failure	●	○	□	□	□	□	□	Microsoft Windows XP , Vista , 7 , 8 , 20...
□	Admin Interactive/Remote Interactive login success	●	○	□	□	□	□	□	Microsoft Windows XP , Vista , 7 , 8 , 20...
□	Administrative logon failure	●	○	□	□	□	□	□	Microsoft Windows XP , Vista , 7 , 8 , 20...
□	Administrative logon success	●	○	□	□	□	□	□	Microsoft Windows XP , Vista , 7 , 8 , 20...
□	Audit event records discarded	●	○	□	□	□	□	□	Microsoft Windows 2000 Server and later
□	**Critical Potential Breach:(Borderware) A new process connecting to...**	●	●	☑	□	□	□	□	EventTracker 8.2 and later
□	**Critical Potential Breach:(Borderware) Unknown process connected...**	●	●	☑	□	□	□	□	EventTracker 8.2 and later

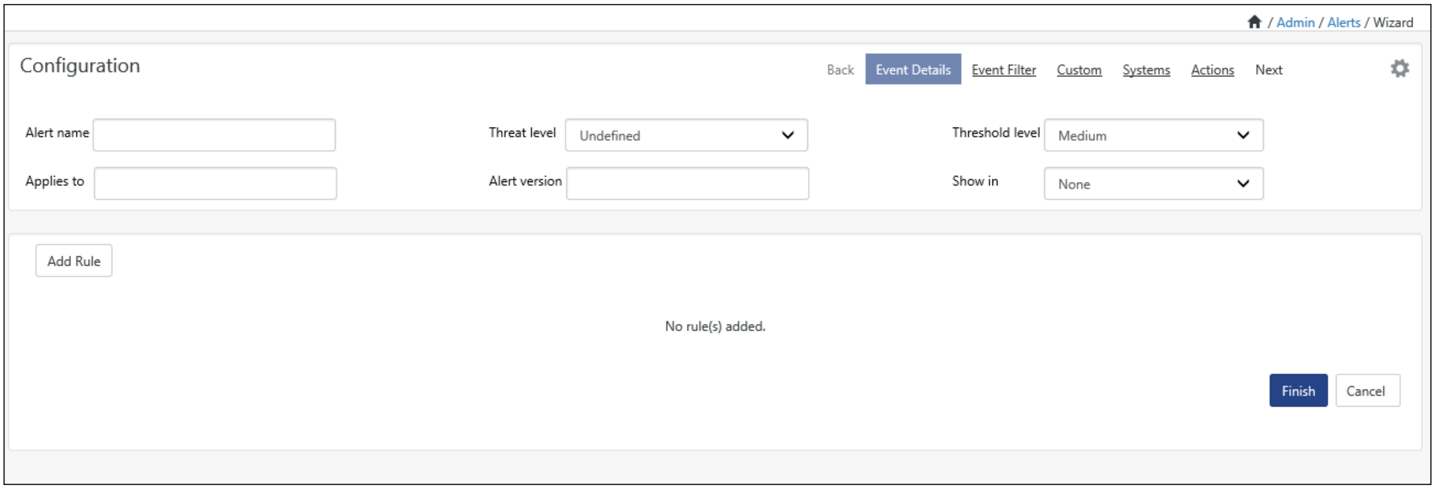
Figure 327

Field	Description
Search	Type the search string and then clicksearch icon 🔍. This helps to easily locate the alert you are looking for.
Search by	Search the alert by Alert Name/Event id/description option.
Page Size	Select an option from this drop-down list to display the maximum number of alerts in a page.
Alert Name	Name of the alert. Click the hyperlink to modify alert details.
Threat level	Severity of the alert.
Active	Select or clear the checkbox to activate or deactivate the alert.
E-mail	Select this checkbox to configure e-mail alert notification. The SMTP server should be configured to send Email.
Message	Select this checkbox to configure console message alert notification.
Forward as SNMP	Select this checkbox to forward alert notification as an SNMP trap.
Forward as SYSLOG	Select this checkbox to forward alert notification as a SYSLOG message.
Remedial Action at Console	Select this checkbox to configure custom action to be executed on receipt of an event at the manager side.
Remedial Action at Agent	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.
Activate Now	Click to activate the selected alert.
Add alert	Click to add custom alert.
Delete	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.

Table 34

2 On the **Alert Management** page, click the ⊕ **icon** to add new alert.

EventTracker opens the **Alert configuration** page.



Alert name		Threat level	Undefined	Threshold level	Medium
Applies to		Alert version		Show in	None

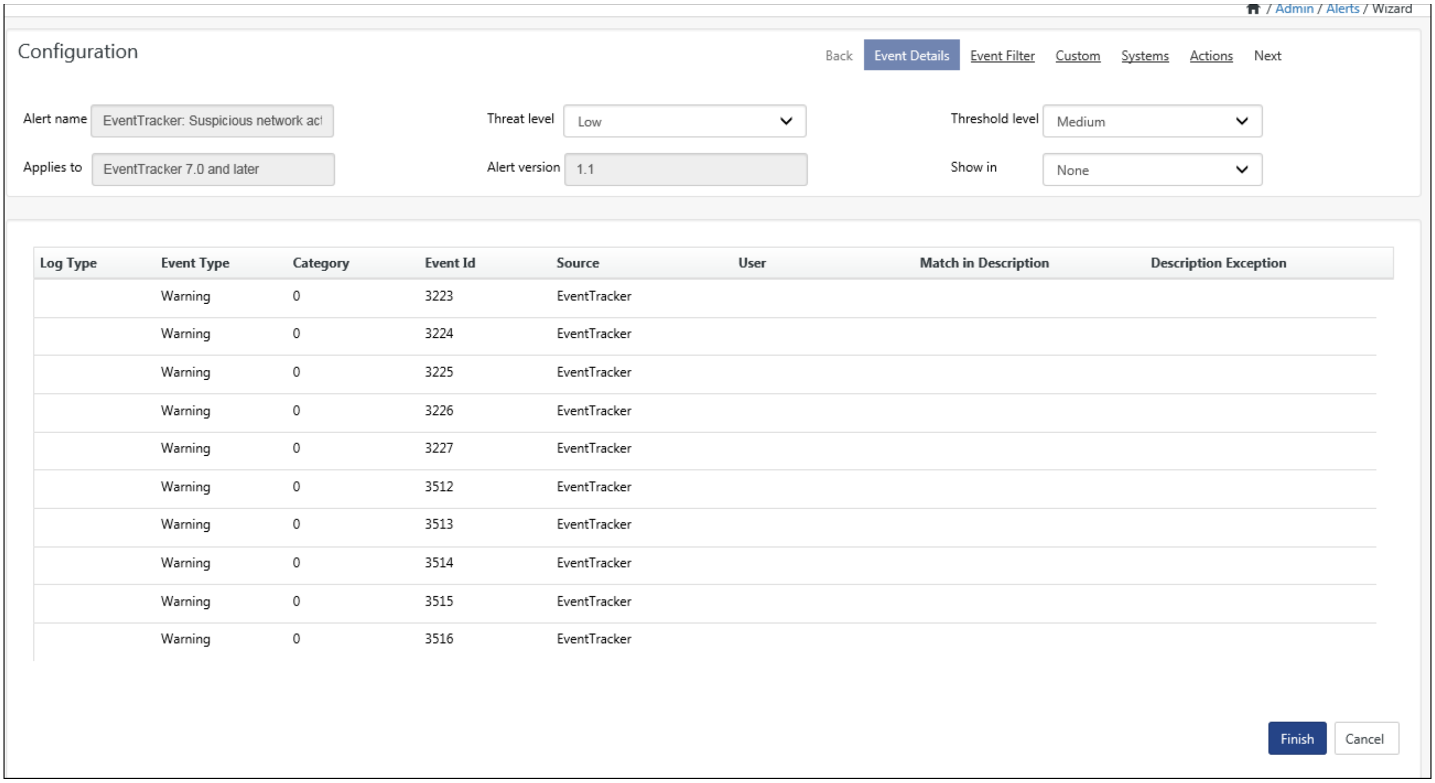
No rule(s) added.

Figure 328

(OR)

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

EventTracker opens the **Alert configuration** page.



Alert name	EventTracker: Suspicious network act	Threat level	Low	Threshold level	Medium
Applies to	EventTracker 7.0 and later	Alert version	1.1	Show in	None

Log Type	Event Type	Category	Event Id	Source	User	Match in Description	Description Exception
	Warning	0	3223	EventTracker			
	Warning	0	3224	EventTracker			
	Warning	0	3225	EventTracker			
	Warning	0	3226	EventTracker			
	Warning	0	3227	EventTracker			
	Warning	0	3512	EventTracker			
	Warning	0	3513	EventTracker			
	Warning	0	3514	EventTracker			
	Warning	0	3515	EventTracker			
	Warning	0	3516	EventTracker			

Figure 329

Fields	Description
Threat level	Select severity of the alert.
Threshold level	Alert notification is sent when the risk is greater or equal to the threshold.
Show in	Select 'Compliance Dashboard' from dropdown to view the selected alert details in the compliance dashboard.
Alert Version	Representation of the version based on alerts, where the default alert version is 1.0.
Applies to	Select the application or server for which the alert has to be generated.

Table 35

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

Example - EventTracker: Suspicious Network Activity.

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

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

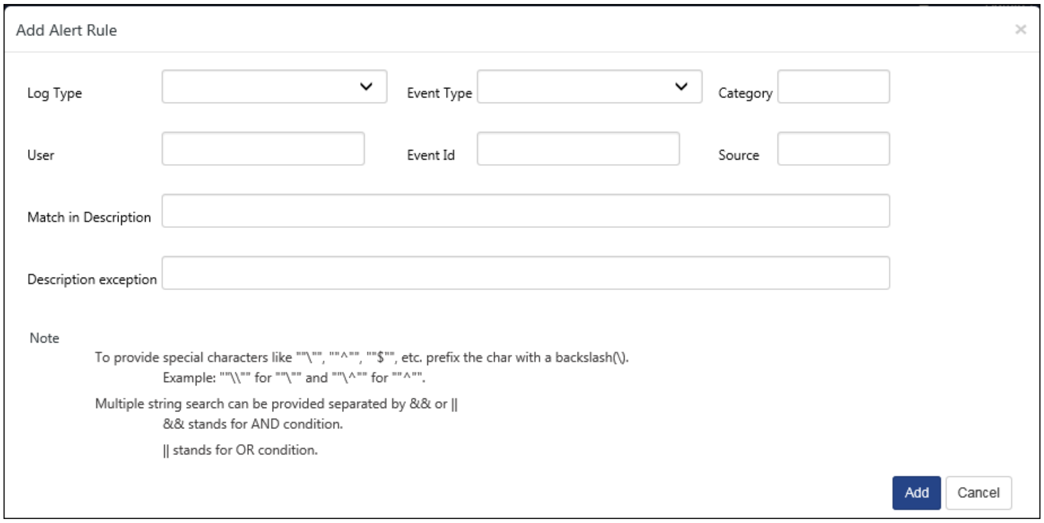
6 To view the alert in compliance dashboard then in '**Show in'** dropdown, select '**Compliance Dashboard**'.

7 To add the version to an alert, select **Alert Version** and enter the version.

8 Add the products for which the alert needs to be generated in the **Applies to** box.

9 Click **Add button** to add event details.

EventTracker opens the **Add Event Rule** dialog box.



Note

To provide special characters like ""\"", ""^"", ""$"", etc. prefix the char with a backslash(\).
Example: ""\\"" for ""\"" and ""\^"" for ""^"".

Multiple string search can be provided separated by && or ||
&& stands for AND condition.
|| stands for OR condition.

Figure 330

🗎 NOTE

User will not have an option to edit the Pre-Defined Alert Rule.

Field	Description
Log Type	It describes the type of log to be monitored.
Event Type	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.
Category	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.
User	Type the name of the user.
Event Id	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.
Source	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, "Elnkii" indicates an EtherLink II driver. Type the source in this field.
Match in Description	Type a sub-string of the description that needs to be matched. EventTracker supports multiple strings separated by the following operands. && stands for AND condition. II stands for OR condition.

	If you type Successful Logon && 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.
Description exception	Type a sub-string of the description that needs to be exempted.

Table 36

Event Type	Description
Error	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.
Warning	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.
Information	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.
Audit Success	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.
Audit Failure	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.
Verbose	A Verbose event is a debugging trace. (Applies only to Vista)
Critical	A critical event is a fatal error or application crash. (Applies only to Vista)

Table 37

10 Enter the required fields, and then click **Add**.

11 Click **Event Filter** hyperlink (OR) click Next .

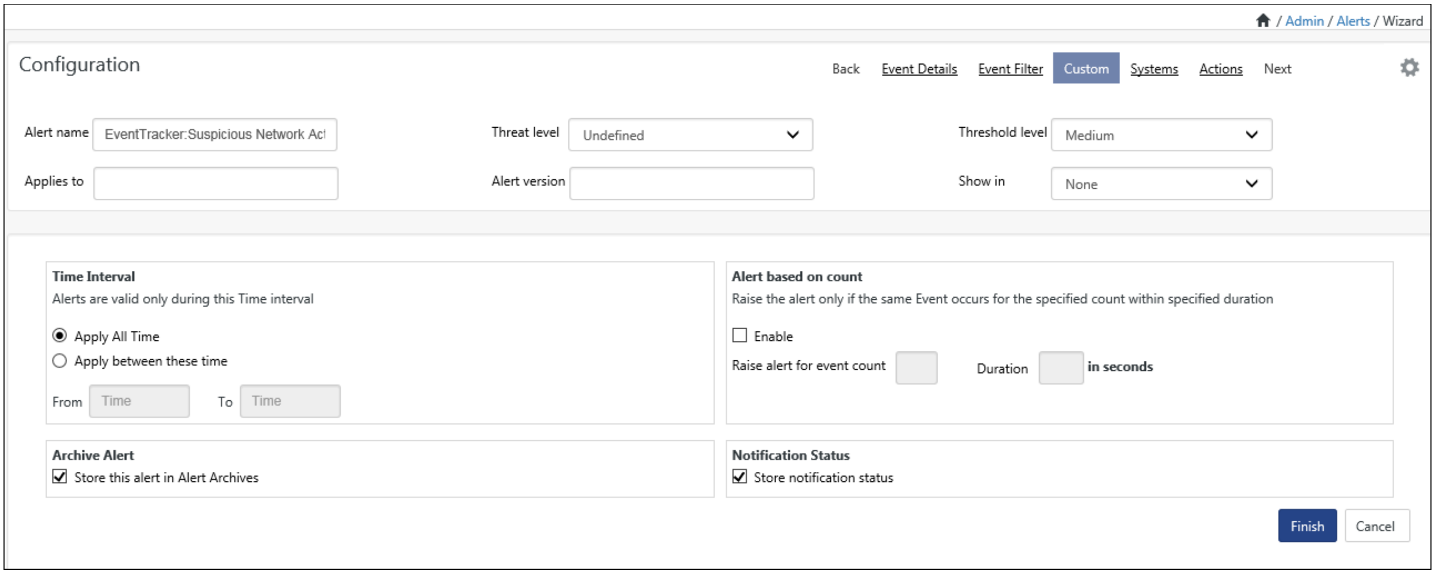
EventTracker opens the **Event Filter** page.

12 Click **Add** to add event details for the event filter.

13 Enter the required fields, and then click **Add**.

14 Click **Custom** hyperlink (OR) click Next .

EventTracker opens the **Custom** page.



Alert name: EventTracker:Suspicious Network Act

Threat level: Undefined

Threshold level: Medium

Applies to:

Alert version:

Show in: None

Time Interval

Alerts are valid only during this Time interval

● Apply All Time

○ Apply between these time

From Time To Time

Alert based on count

Raise the alert only if the same Event occurs for the specified count within specified duration

□ Enable

Raise alert for event count   Duration   in seconds

Archive Alert

☑ Store this alert in Alert Archives

Notification Status

☑ Store notification status

Figure 331

Field	Description
Apply All Time	If selected, alerts actions are executed for events occurred all through the day (24 hours).
Apply between these time	If selected, alerts actions are executed for events occurred during the specified time frame.
Alert based on Count	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.
Archive Alert	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.

Table 332

15 Select **Apply All Time** option.

(OR)

Select the **Apply between this time** option, and then select **From** and **To** time from the calendar control.

16 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.

17 Click **Systems** (OR) click Next .

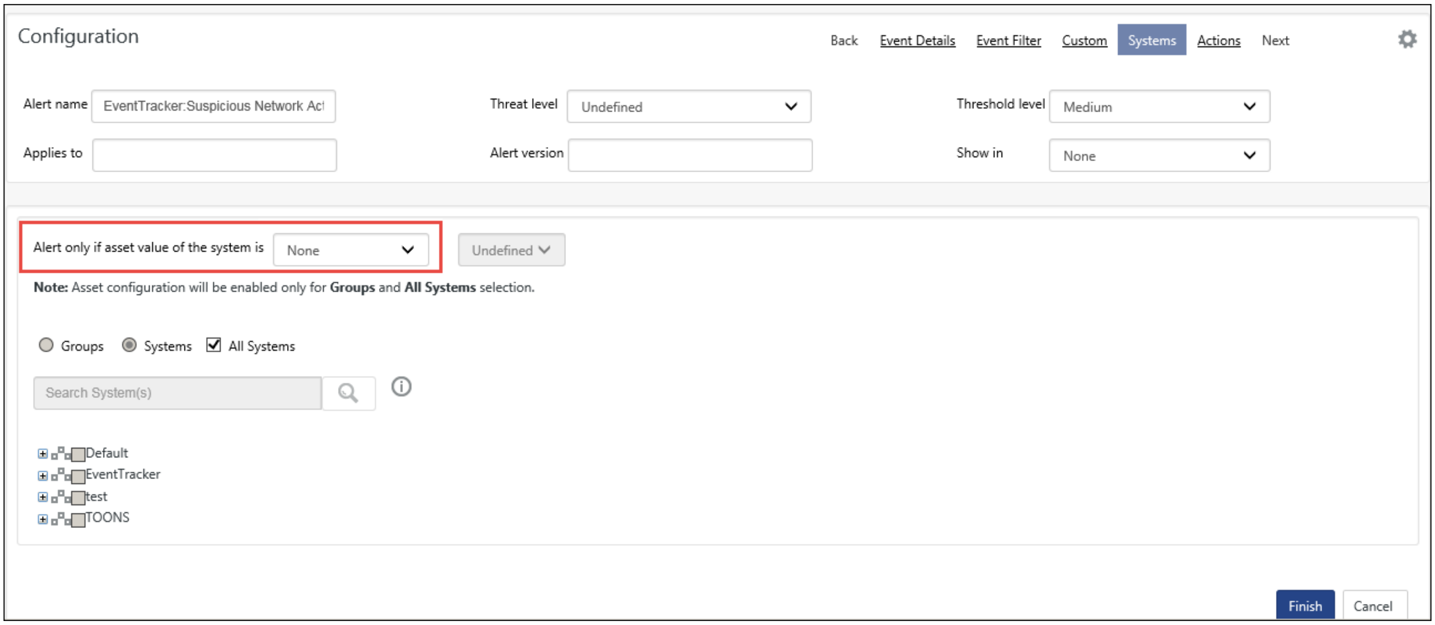
EventTracker opens the **Systems** page.

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

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

🗎 NOTE

We have now provided an interface to configure alert based on the asset value of system.



Configuration

Alert name: EventTracker:Suspicious Network Act

Threat level: Undefined

Threshold level: Medium

Applies to:

Alert version:

Show in: None

Alert only if asset value of the system is: None | Undefined

Note: Asset configuration will be enabled only for **Groups** and **All Systems** selection.

○ Groups ● Systems ☑ All Systems

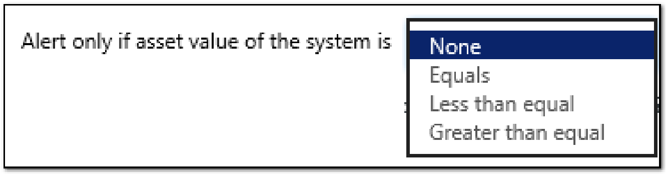
Search System(s)

⊞ Default
⊞ EventTracker
⊞ test
⊞ TOONS

Figure 333

19 The new field "**Alert only if asset value of the system is**" is where the user can select the operator and the asset value from the dropdown list.

20 Select the Operator (Equals/Less than equal/Greater than equal).

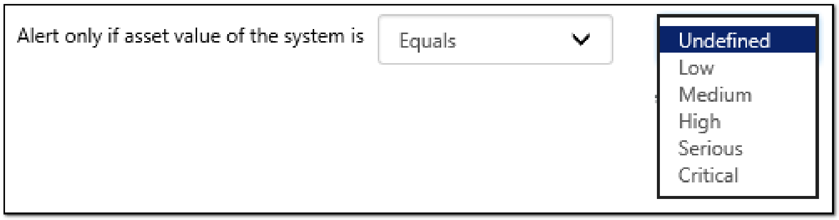


Alert only if asset value of the system is

None
Equals
Less than equal
Greater than equal

Figure 334

21 Select the **Asset Value**.



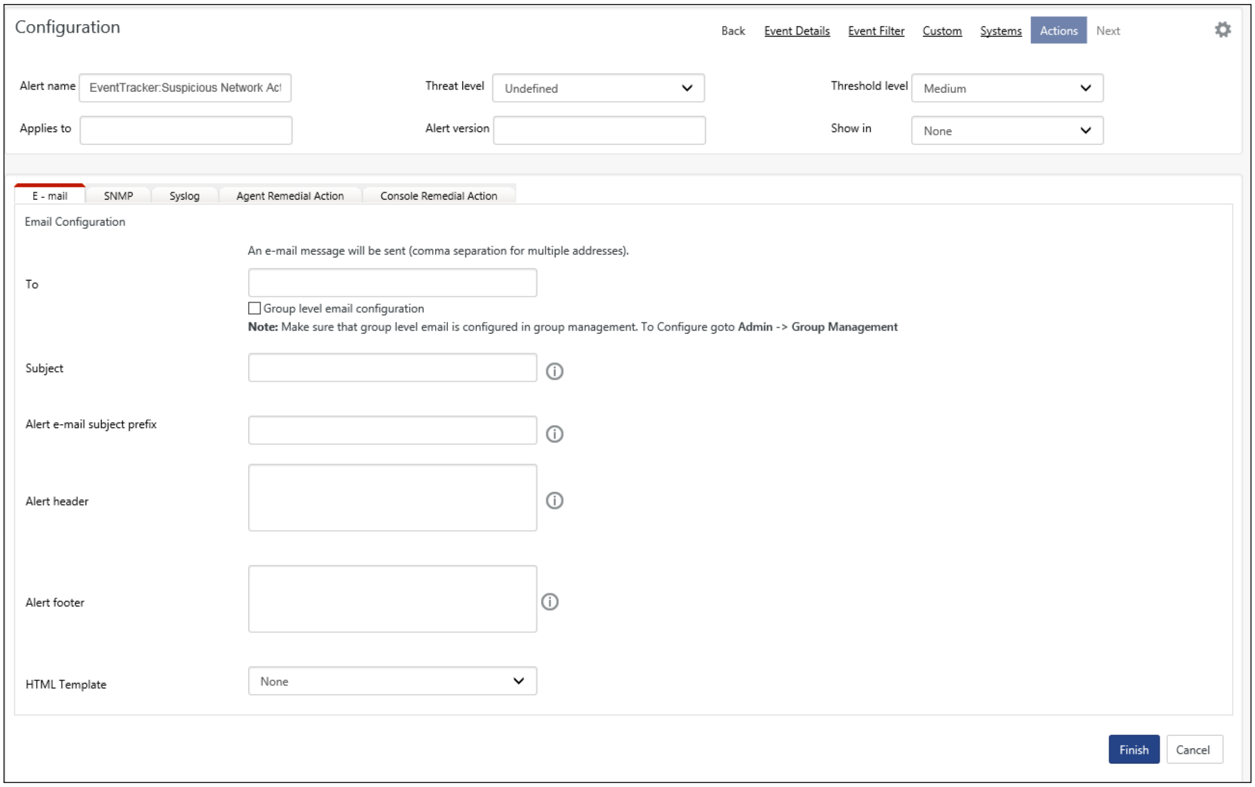
Alert only if asset value of the system is Equals

Undefined
Low
Medium
High
Serious
Critical

Figure 335

22 Click **Actions** hyperlink (OR) click Next .

EventTracker opens the **Actions** page.



Alert name: EventTracker:Suspicious Network Act

Threat level: Undefined

Threshold level: Medium

Applies to:

Alert version:

Show in: None

Email Configuration

An e-mail message will be sent (comma separation for multiple addresses).

To

□ Group level email configuration

Note: Make sure that group level email is configured in group management. To Configure goto **Admin** -> **Group Management**

Subject

Alert e-mail subject prefix

Alert header

Alert footer

HTML Template: None

Figure 336

20 In the e-mail configuration tab, enter the recipient address, subject, alert footer and alert e-mail subject prefix, as per the requirement.

21 Enter multiline header/footer, for configuring an email alert action.

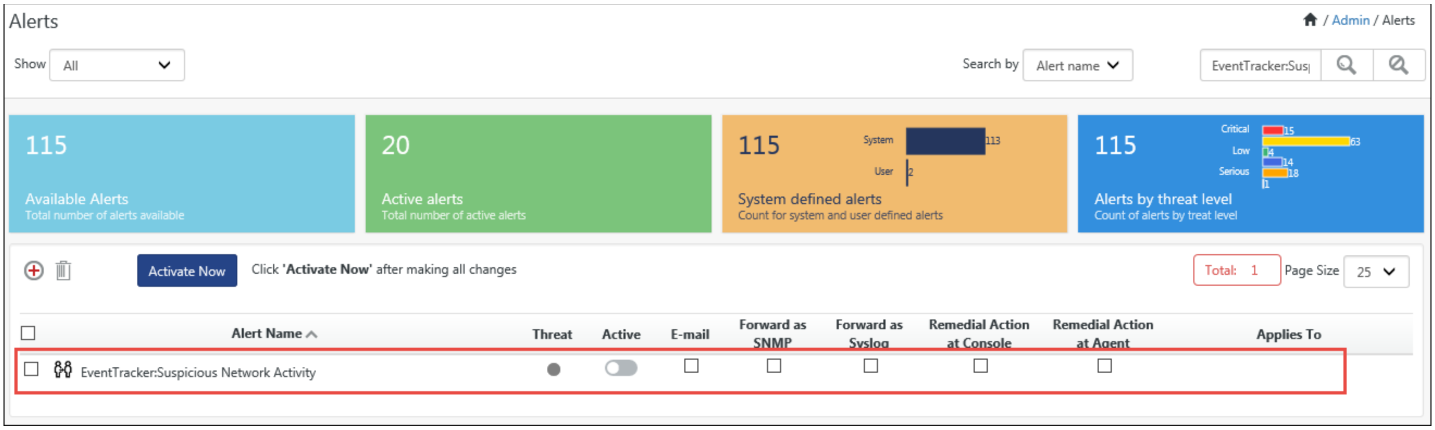
🗎 NOTE

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

22 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).

23 Click **Finish**.

EventTracker adds the newly created alert and opens it on the Alert Management page.



Click **'Activate Now'** after making all changes

☐	Alert Name	Threat	Active	E-mail	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
☐	EventTracker:Suspicious Network Activity	●		☐	☐	☐	☐	☐	

Figure 337

24 To activate the newly added alert, select the checkbox under **Active** column.

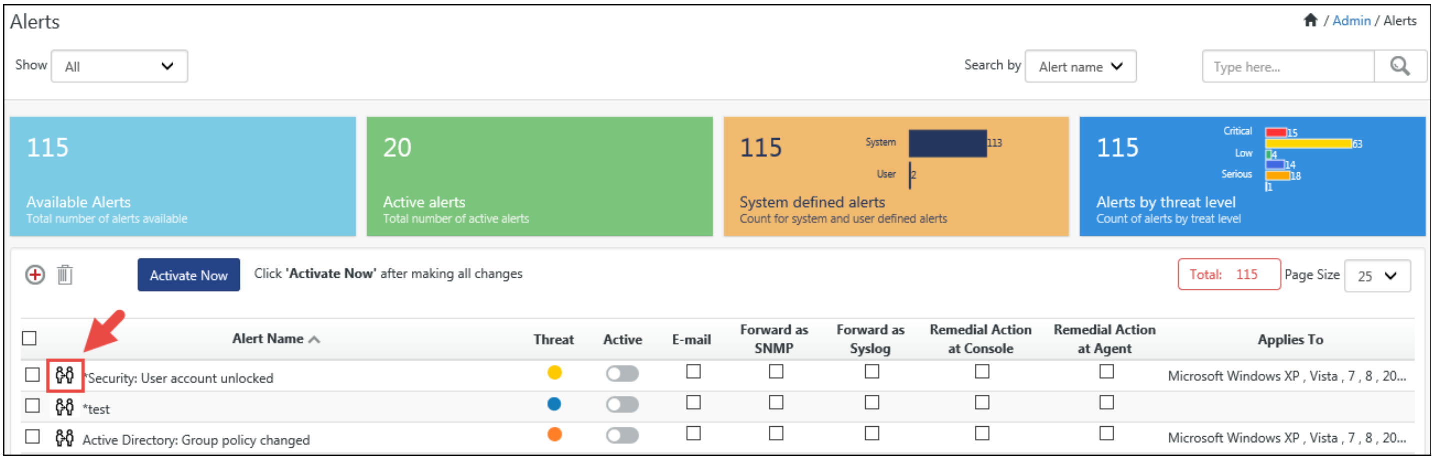
EventTracker opens the success message pop-up window. EventTracker saves the alert configuration.

🗎 NOTE

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

6.4 Copying of Alerts

1. To make a copy of existing alert, select **Copy** ❐ .



Alerts

/ Admin / Alerts

Show All

Search by Alert name

Type here...

115
Available Alerts
Total number of alerts available

20
Active alerts
Total number of active alerts

115
System defined alerts
Count for system and user defined alerts

115
Alerts by threat level
Count of alerts by treat level

Activate Now Click **'Activate Now'** after making all changes

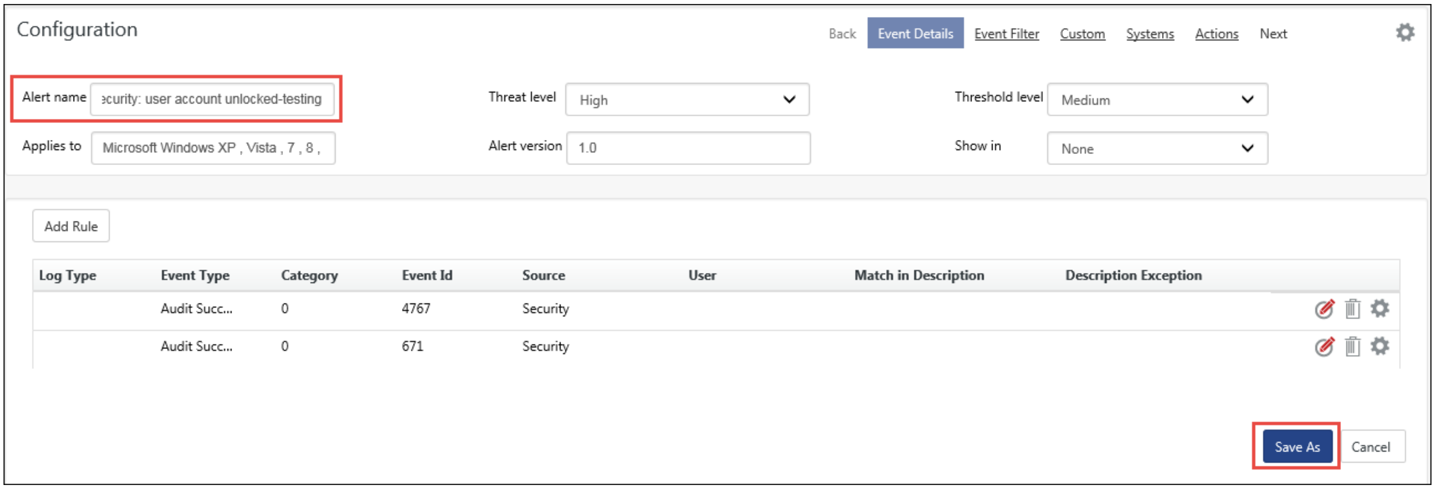
Total: 115 Page Size 25

□		Alert Name	Threat	Active	E-mail	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
□		*Security: User account unlocked	●		□	□	□	□	□	Microsoft Windows XP , Vista , 7 , 8 , 20...
□		*test	●		□	□	□	□	□	
□		Active Directory: Group policy changed	●		□	□	□	□	□	Microsoft Windows XP , Vista , 7 , 8 , 20...

Figure 338

Alert Configuration page opens.

2. Enter **Alert Version: Applies To:** fields.



Configuration

Alert name	ɘcurity: user account unlocked-testing	Threat level	High	Threshold level	Medium
Applies to	Microsoft Windows XP , Vista , 7 , 8 ,	Alert version	1.0	Show in	None

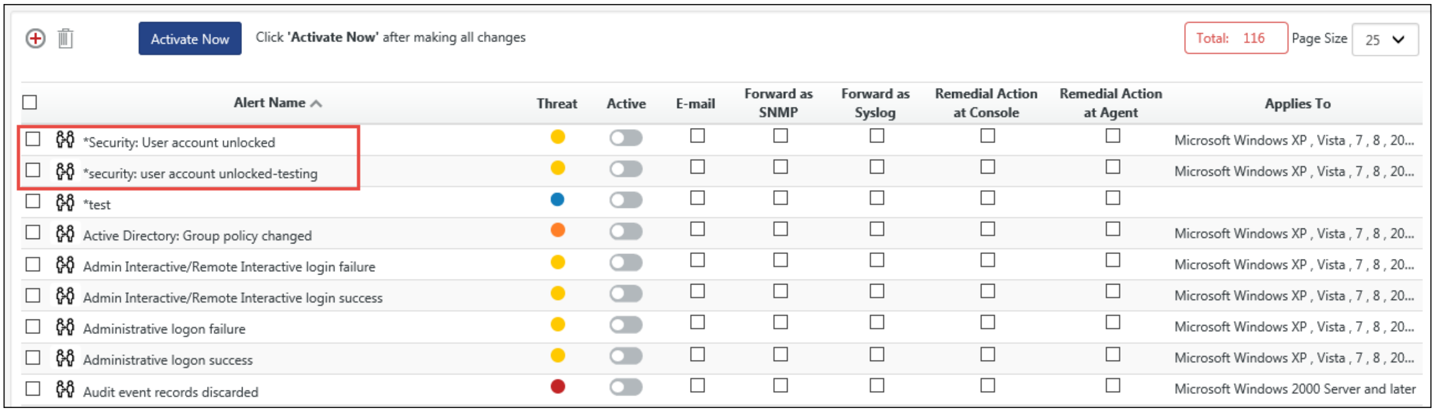
Add Rule

Log Type	Event Type	Category	Event Id	Source	User	Match in Description	Description Exception
	Audit Succ...	0	4767	Security			
	Audit Succ...	0	671	Security			

Figure 339

3. If required, edit/enter rest of the information, and then select **Save As**.

A copy of the existing alert is created.



Activate Now Click **'Activate Now'** after making all changes

Total: 116 Page Size 25

□	Alert Name	Threat	Active	E-mail	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
□	*Security: User account unlocked	🟡	○	□	□	□	□	□	Microsoft Windows XP , Vista , 7 , 8 , 20...
□	*security: user account unlocked-testing	🟡	○	□	□	□	□	□	Microsoft Windows XP , Vista , 7 , 8 , 20...
□	*test	🔵	○	□	□	□	□	□	
□	Active Directory: Group policy changed	🟠	○	□	□	□	□	□	Microsoft Windows XP , Vista , 7 , 8 , 20...
□	Admin Interactive/Remote Interactive login failure	🟡	○	□	□	□	□	□	Microsoft Windows XP , Vista , 7 , 8 , 20...
□	Admin Interactive/Remote Interactive login success	🟡	○	□	□	□	□	□	Microsoft Windows XP , Vista , 7 , 8 , 20...
□	Administrative logon failure	🟡	○	□	□	□	□	□	Microsoft Windows XP , Vista , 7 , 8 , 20...
□	Administrative logon success	🟡	○	□	□	□	□	□	Microsoft Windows XP , Vista , 7 , 8 , 20...
□	Audit event records discarded	🔴	○	□	□	□	□	□	Microsoft Windows 2000 Server and later

Figure 340

Click **Activate Now**.

6.5 Adding Pre-defined Categories as Alerts

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

1) To add pre-defined categories as alerts, click the **Admin**, and then click **Category**.

   EventTracker opens the **Category Management** page.

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

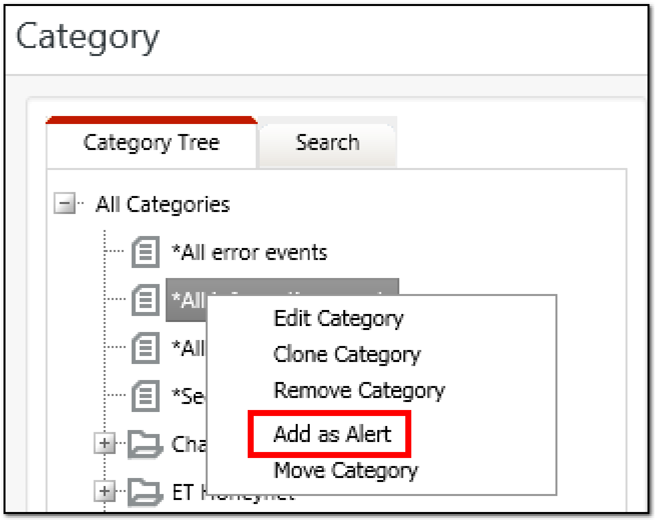
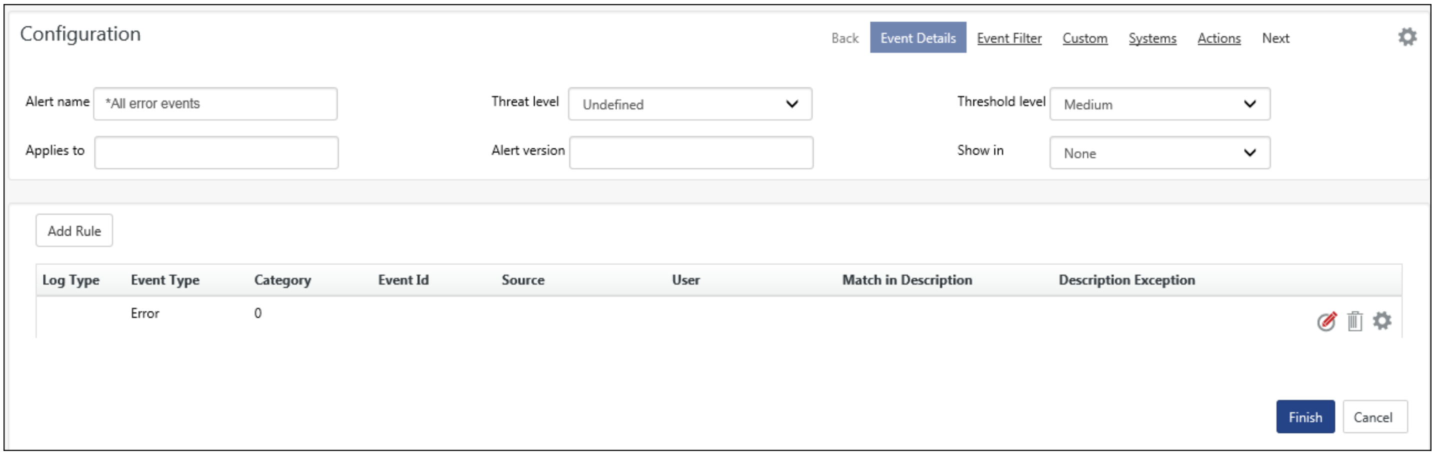


Figure 341

EventTracker opens the **Alert Management** -> **Event Details** page.



Configuration

Alert name: *All error events

Threat level: Undefined

Threshold level: Medium

Applies to:

Alert version:

Show in: None

Log Type	Event Type	Category	Event Id	Source	User	Match in Description	Description Exception
	Error	0					

Figure 342

3) Complete the alert configuration process as described in Add Custom Alerts.

6.6 Deleting Alerts

This option enables you to delete Alerts.

1 On the **Alert Management** page, select the alert to be deleted.

2 Click **Delete**.

6.7 Configuring Alert Actions – Manager Side

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

1 Configure an alert as explained in the Add Custom Alerts.

2 Click an appropriate tab to configure alert actions.

NOTE

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.

6.7.1 Configuring E-mail Alert Action

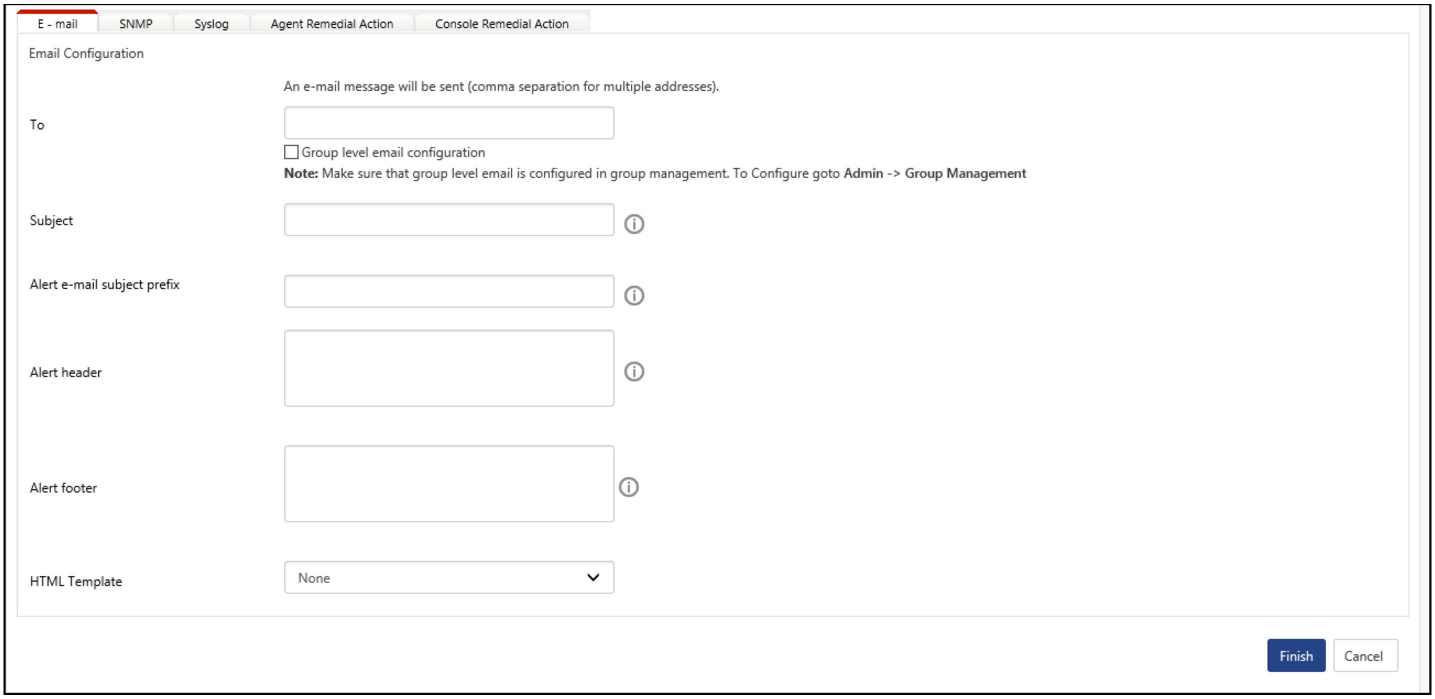
This option enables you to configure an E-mail(s) to send as an alert action.

1 On the **Alert configuration** page, click **Actions** hyperlink, and then click the **E – mail** tab.

(OR)

On the **Alert Management** page, click the checkbox under **E-mail** column.

EventTracker opens the Email dialog box.



Email Configuration

An e-mail message will be sent (comma separation for multiple addresses).

To

□ Group level email configuration

Note: Make sure that group level email is configured in group management. To Configure goto **Admin -> Group Management**

Subject

Alert e-mail subject prefix

Alert header

Alert footer

HTML Template: None

Figure 343

2 Enter required details.

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

(OR)

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

4 On the **Alert Management** page, click the checkbox under **Active** column, and then click **Activate Now** 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.

6.7.2 Forwarding Events as SNMP Traps

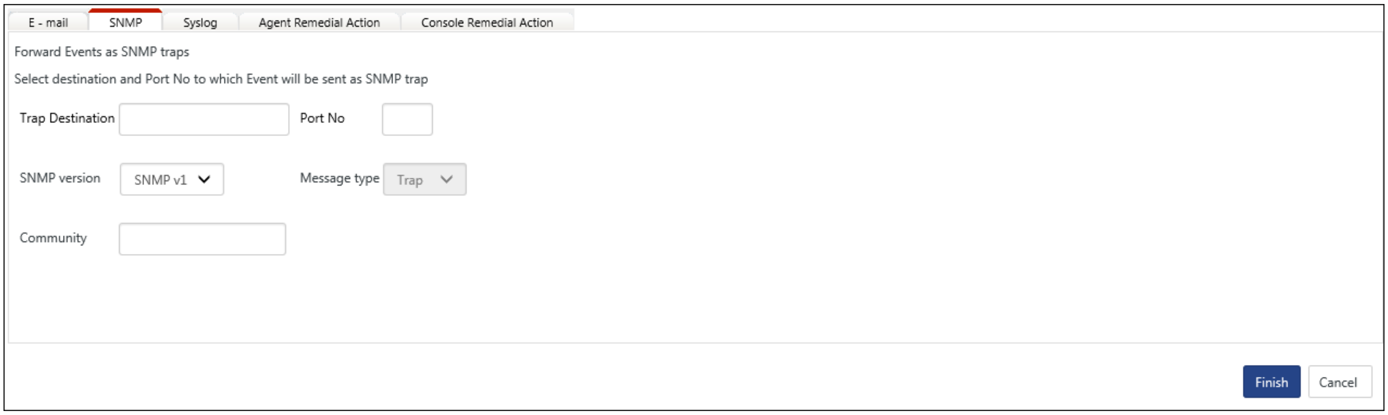
All incoming events are compared with the configured alert. Whenever there is a match between an event and the alert criteria, a copy of the event is forwarded as an SNMP trap to the specified destination.

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 opens the SNMP dialog box.



Forward Events as SNMP traps

Select destination and Port No to which Event will be sent as SNMP trap

Trap Destination

Port No

SNMP version: SNMP v1

Message type: Trap

Community

Figure 344

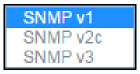
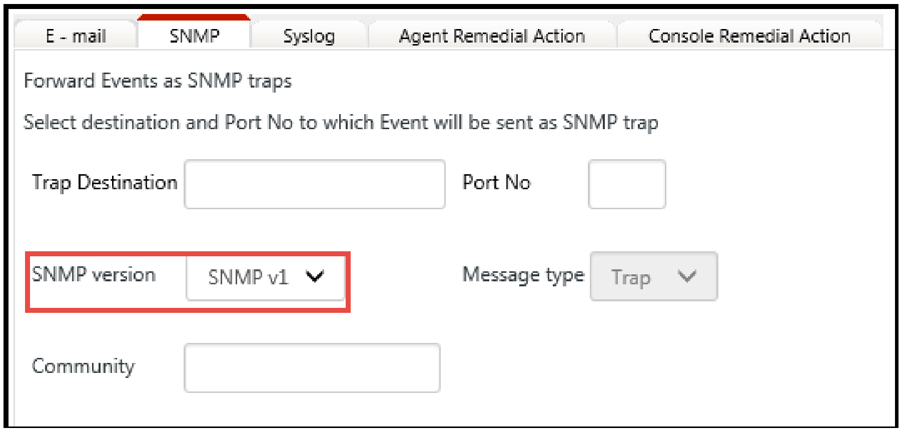
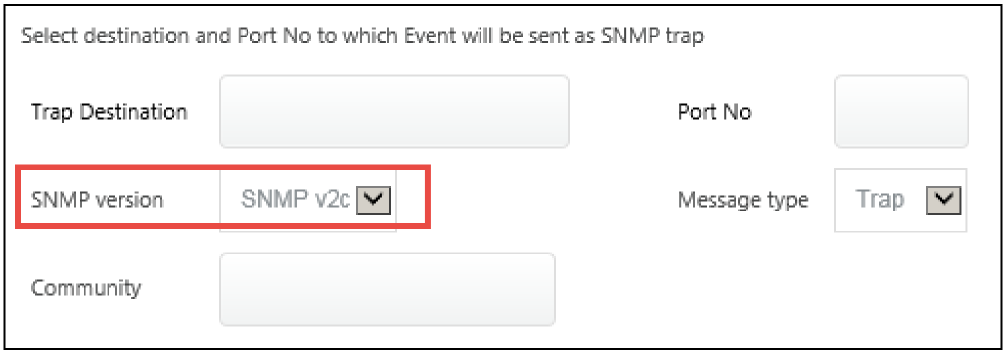
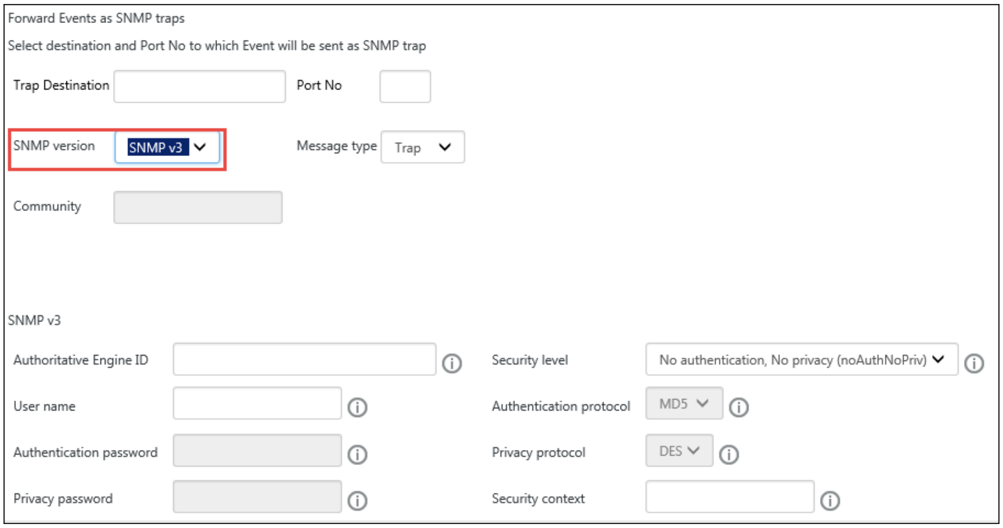
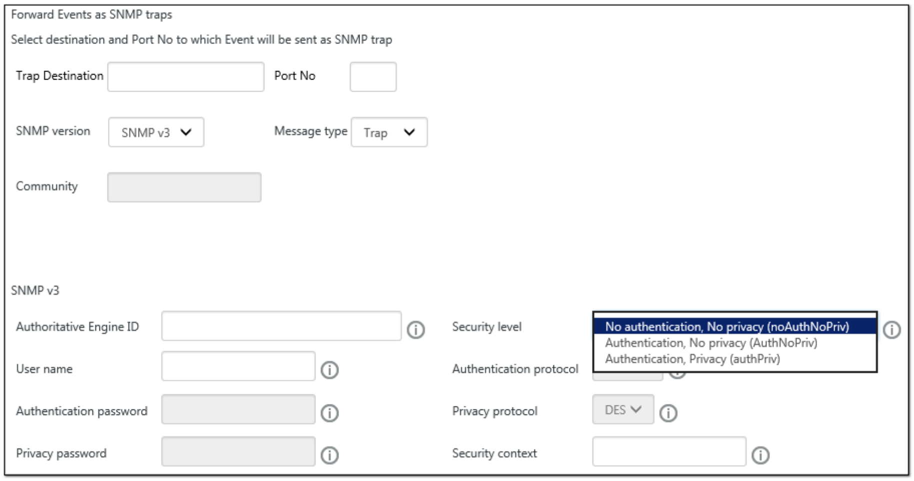
Field	Description
Trap Destination	Type the IP address or host name.
Port No	Type the port number in this field i.e. 162.This field supports numeric data type only.
SNMP version	3 types of SNMP versions used are  SNMP v1 SNMP v2c SNMP v3
Message Type	Trap. Inform – Trap with an acknowledgement
Community	Authentication key for encryption and decryption

Table 39

Field	Description
SNMP v1	 E - mail SNMP Syslog Agent Remedial Action Console Remedial Action Forward Events as SNMP traps Select destination and Port No to which Event will be sent as SNMP trap Trap Destination Port No SNMP version: SNMP v1 Message type: Trap Community
SNMP v2c	 Select destination and Port No to which Event will be sent as SNMP trap Trap Destination Port No SNMP version: SNMP v2c Message type: Trap Community
SNMP v3	By default, No authentication, No privacy is selected.  Forward Events as SNMP traps Select destination and Port No to which Event will be sent as SNMP trap Trap Destination Port No SNMP version: SNMP v3 Message type: Trap Community SNMP v3 Authoritative Engine ID Security level: No authentication, No privacy (noAuthNoPriv) User name Authentication protocol: MD5 Authentication password Privacy protocol: DES Privacy password Security context

Security level	There 3 different security levels been provided No authentication, No privacy (noAuthNoPriv) – Refer picture above. Authentication, No Privacy (AuthNoPriv) - Refer picture below. Authentication and Privacy (authPriv) - Refer picture below.  Forward Events as SNMP traps Select destination and Port No to which Event will be sent as SNMP trap Trap Destination Port No SNMP version: SNMP v3 Message type: Trap Community SNMP v3 Authoritative Engine ID User name Authentication password Privacy password Security level: No authentication, No privacy (noAuthNoPriv) Authentication, No privacy (AuthNoPriv) Authentication, Privacy (authPriv) Authentication protocol Privacy protocol: DES Security context
User name	A string representing the name of the user.
Authentication Protocol	- An indication of whether messages sent on behalf of this user can be authenticated, and if so, the type of authentication protocol which is used. - Two such protocols are defined: MD5 SHA1 The above option is enabled only if the following security levels are selected. Authentication, No Privacy (AuthNoPriv) Authentication and Privacy (authPriv)
Authentication password	If messages sent on behalf of this user can be authenticated, the (private) authentication password for use with the authentication protocol. Note that a user’s authentication key will normally be different at different authoritative SNMP engines. The Authentication password is not accessible via SNMP. The length requirements of the Authentication password are defined by the Authentication Protocol in use.
Privacy Protocol	An indication of whether messages sent on behalf of this user can be protected from disclosure, and if so, the type of privacy protocol which is used. One such protocol is defined in this memo: the CBC-DES Symmetric Encryption Protocol.

Privacy password	If messages sent on behalf of this user can be en/decrypted, the (private) privacy password for use with the privacy protocol. Note that a user's privacy password will normally be different at different authoritative SNMP engines. The Privacy Password is not accessible via SNMP. The length requirements of the Privacy Password are defined by the Privacy Protocol in use.
Security context	A human-readable string representing the user in a format that is Security Model independent. There is a one-to-one relationship between Username and Security Context.

Table 40

2 Type appropriately in the relevant fields.

3 On the **Alert Configuration** page, click **Finish** 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 **Activate Now** to activate the alert action.

🗎 NOTE

The Threat Level and Threshold Level in Event Details page should be Undefined otherwise traps will not be received in Trap Tracker Console. For detail information, refer TrapTracker.

6.7.3 Forwarding events as syslog messages

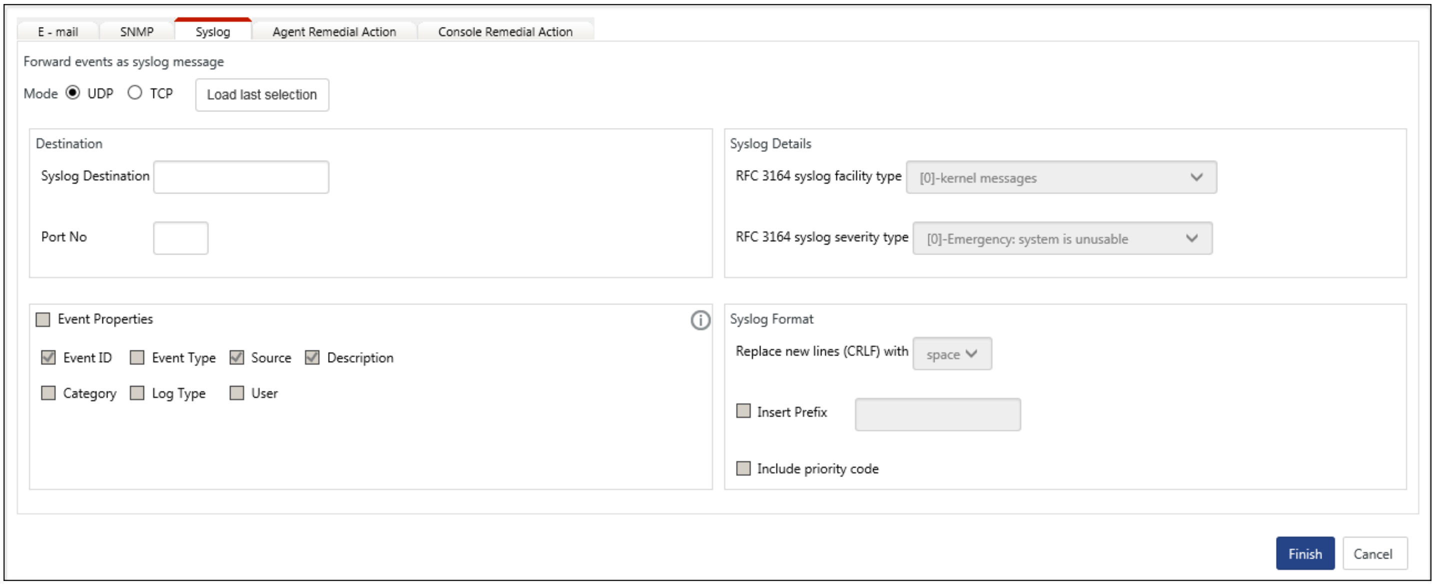
All incoming events are compared with the configured alert. Whenever there is a match between an event and the alert criteria, a copy of the event is forwarded as a syslog message to the specified destination.

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 opens the **syslog** dialog box.



Forward events as syslog message

Mode ● UDP ○ TCP Load last selection

Destination

Syslog Destination

Port No

Syslog Details

RFC 3164 syslog facility type [0]-kernel messages

RFC 3164 syslog severity type [0]-Emergency: system is unusable

□ Event Properties

☑ Event ID □ Event Type ☑ Source ☑ Description

□ Category □ Log Type □ User

Syslog Format

Replace new lines (CRLF) with space

□ Insert Prefix

□ Include priority code

Figure 345

Field	Description
Mode	Select either TCP or UDP as the transport protocol mode.
Load last selection	Click to load the last saved configuration of a syslog message.
Destination	
syslog Destination	Type the IP address or host name.
Port No	Type the port number corresponding to the transport mode selected.
syslog Details	
RFC 3164 syslog facility type	Return facility value from a received and processed syslog message. This is the text representation of the facility.
RFC 3164 syslog severity type	Return severity value from a received and processed syslog message. This is the text representation of the severity.
Event Properties	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.
syslog Format	
Replace new lines (CRLF) with	Replaces the newline characters in the syslog message with tab or space.
Insert prefix	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.
Include priority code	Each syslog message is one line. A message can contain a priority code, marked by a digit enclosed in < > (angle braces) at the beginning of the line. The priority code represents both the Facility and Severity of the message.

Table 41

2 Select/enter appropriately in the relevant fields.

3 Click **OK**.

6.7.4 Executing Remedial Action at EventTracker Manager Console System

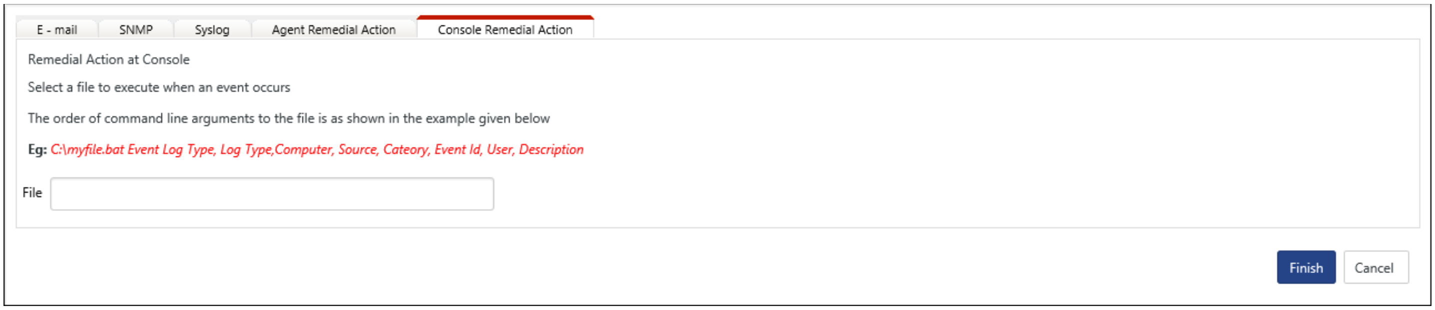
This option enables you to configure custom action to be executed on receipt of an event at the manager system.

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 opens the **Console** dialog box.



Remedial Action at Console

Select a file to execute when an event occurs

The order of command line arguments to the file is as shown in the example given below

Eg: *C:\myfile.bat Event Log Type, Log Type,Computer, Source, Cateory, Event Id, User, Description*

File

Figure 346

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 Save.

6.7.5 Executing 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.

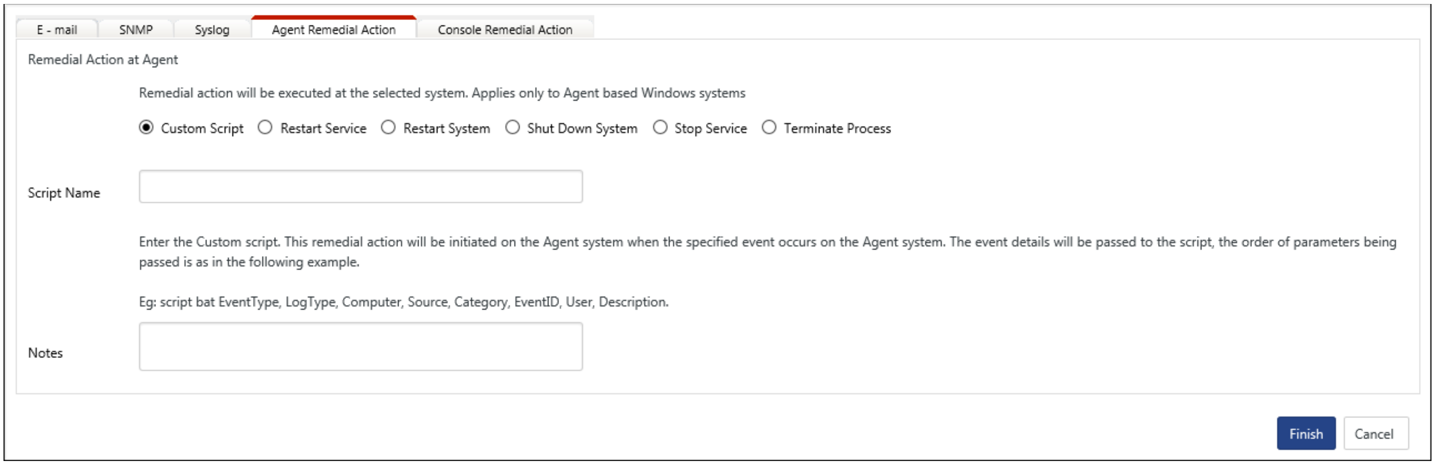
To execute remedial action at the agent system,

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 opens the **Agent** dialog box.



Remedial Action at Agent

Remedial action will be executed at the selected system. Applies only to Agent based Windows systems

● Custom Script ○ Restart Service ○ Restart System ○ Shut Down System ○ Stop Service ○ Terminate Process

Script Name

Enter the Custom script. This remedial action will be initiated on the Agent system when the specified event occurs on the Agent system. The event details will be passed to the script, the order of parameters being passed is as in the following example.

Eg: script bat EventType, LogType, Computer, Source, Category, EventID, User, Description.

Notes

Figure 347

Field	Description
Custom Script	Type the name of the script in Script Name field. **Script files are stored in the default EventTracker Agent installation path typically ...\Program Files\Prism Microsystems\EventTracker\Agent**
Restart Service	Type the name of the service that you want to restart in Service Name field.
Restart System	This option will restart the agent system on the occurrence of the configured EventID.
Shut Down System	This option will shut down the agent system on the occurrence of configured EventID.
Stop Service	Type the name of the service that you want to stop in Service Name field.
Terminate Process	You can configure this action only for events 3217, 3218, 3221, 3223, and 3226.

Table 42

2 Select an appropriate remedial action option.

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

4 Click **Ok**.

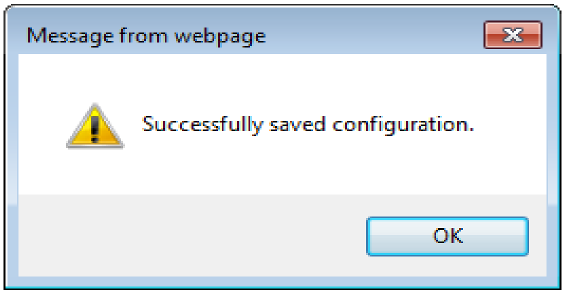
🗎 NOTE

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

6.7.6 Editing Alert Actions

This option enables you to edit the alert actions.

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 **Finish** to save the changes.
5 On the **Alert Management** page, click the checkbox under **Active** column, and then click **Activate Now** to activate the alert action.
A message from webpage opens.



Message from webpage

Successfully saved configuration.

Figure 348

7. Machine Learning Jobs

In this chapter, you will learn how to:

- Manage Machine Learning Jobs
- Add Machine Learning Jobs
- Add custom Jobs in Machine Learning Dashboard

7.1 Manage Machine Learning Jobs

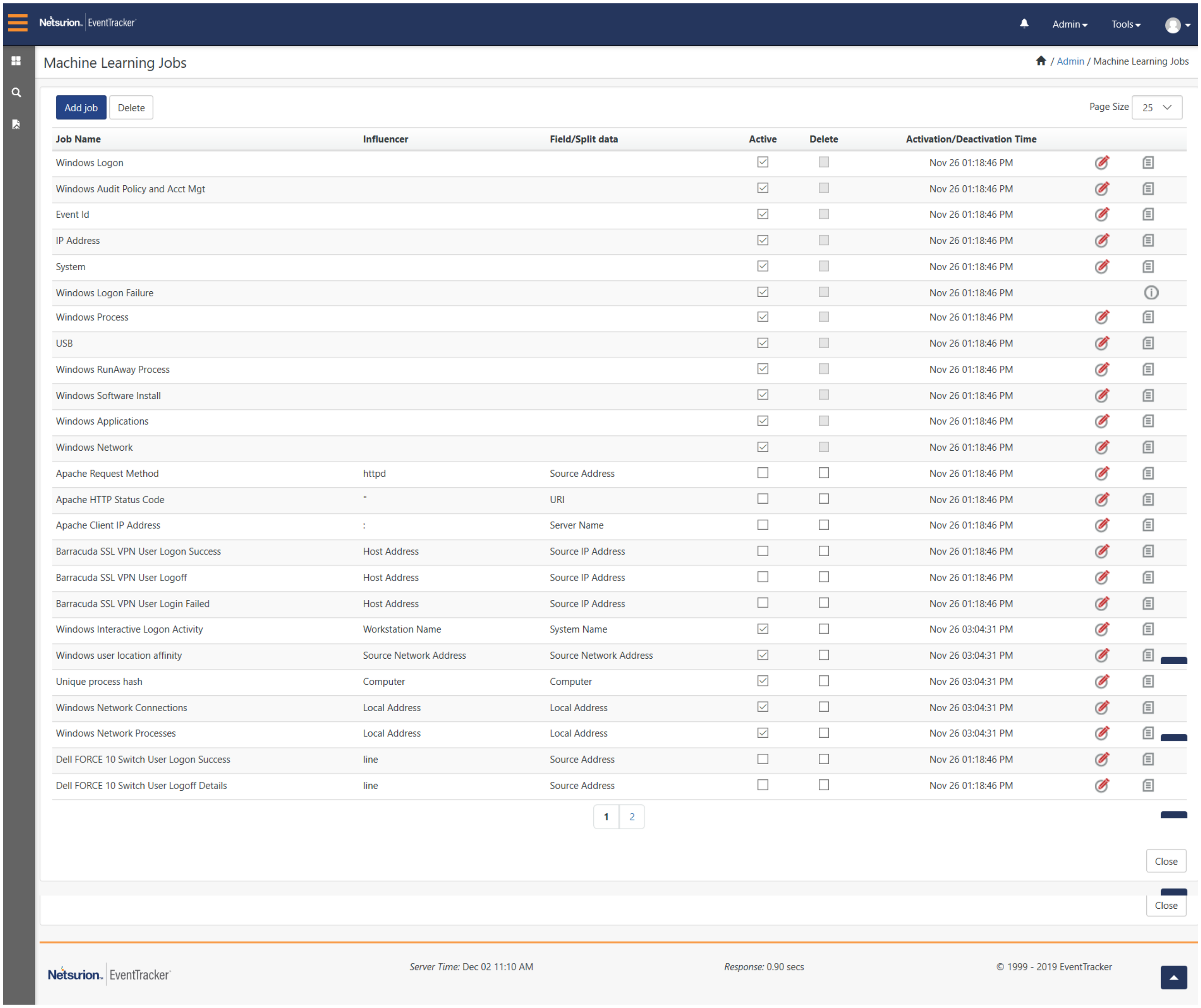
This option helps to set Machine Learning for machine learning activity. You can add these jobs as dashlets under Machine Learning –> **Security** / **Operations**. Correlation Settings is added in Machine Learning to know about the new activities that are occuring in an enterprise. The purpose of the rule is to know the applications that are being used by various users and to be alerted when a new application is detected in the enterprise. The Top 5 activities are displayed for last 1 day except the Logon failure activity which is shown for last 7days.

1 To set **Machine Learning Jobs**, click the **Admin**, and then click **Machine Learning Jobs**.

EventTracker displays the **Machine Learning Jobs** page with pre-defined jobs.

🗎 NOTE

A job is a set of rules based on which new activities and Anomalies are identified in an Environment.



Job Name	Influencer	Field/Split data	Active	Delete	Activation/Deactivation Time
Windows Logon			☑	□	Nov 26 01:18:46 PM
Windows Audit Policy and Acct Mgt			☑	□	Nov 26 01:18:46 PM
Event Id			☑	□	Nov 26 01:18:46 PM
IP Address			☑	□	Nov 26 01:18:46 PM
System			☑	□	Nov 26 01:18:46 PM
Windows Logon Failure			☑	□	Nov 26 01:18:46 PM
Windows Process			☑	□	Nov 26 01:18:46 PM
USB			☑	□	Nov 26 01:18:46 PM
Windows RunAway Process			☑	□	Nov 26 01:18:46 PM
Windows Software Install			☑	□	Nov 26 01:18:46 PM
Windows Applications			☑	□	Nov 26 01:18:46 PM
Windows Network			☑	□	Nov 26 01:18:46 PM
Apache Request Method	httpd	Source Address	□	□	Nov 26 01:18:46 PM
Apache HTTP Status Code	"	URI	□	□	Nov 26 01:18:46 PM
Apache Client IP Address	:	Server Name	□	□	Nov 26 01:18:46 PM
Barracuda SSL VPN User Logon Success	Host Address	Source IP Address	□	□	Nov 26 01:18:46 PM
Barracuda SSL VPN User Logoff	Host Address	Source IP Address	□	□	Nov 26 01:18:46 PM
Barracuda SSL VPN User Login Failed	Host Address	Source IP Address	□	□	Nov 26 01:18:46 PM
Windows Interactive Logon Activity	Workstation Name	System Name	☑	□	Nov 26 03:04:31 PM
Windows user location affinity	Source Network Address	Source Network Address	☑	□	Nov 26 03:04:31 PM
Unique process hash	Computer	Computer	☑	□	Nov 26 03:04:31 PM
Windows Network Connections	Local Address	Local Address	☑	□	Nov 26 03:04:31 PM
Windows Network Processes	Local Address	Local Address	☑	□	Nov 26 03:04:31 PM
Dell FORCE 10 Switch User Logon Success	line	Source Address	□	□	Nov 26 01:18:46 PM
Dell FORCE 10 Switch User Logoff Details	line	Source Address	□	□	Nov 26 01:18:46 PM

Server Time: Dec 02 11:10 AM *Response:* 0.90 secs © 1999 - 2019 EventTracker

Figure 349

Field	Description
Job Name	Name of the Job.
Influencers	Based on this configuration, EventTracker displays the influencer details on the Machine Learning page.
Field/split data	Name of the custom column.
Active	Clear this checkbox to inactivate the Machine Learning Jobs (Dashlet).
Delete	To delete a Job Name
Activation/Deactivation Time	Displays the time of activation or deactivation

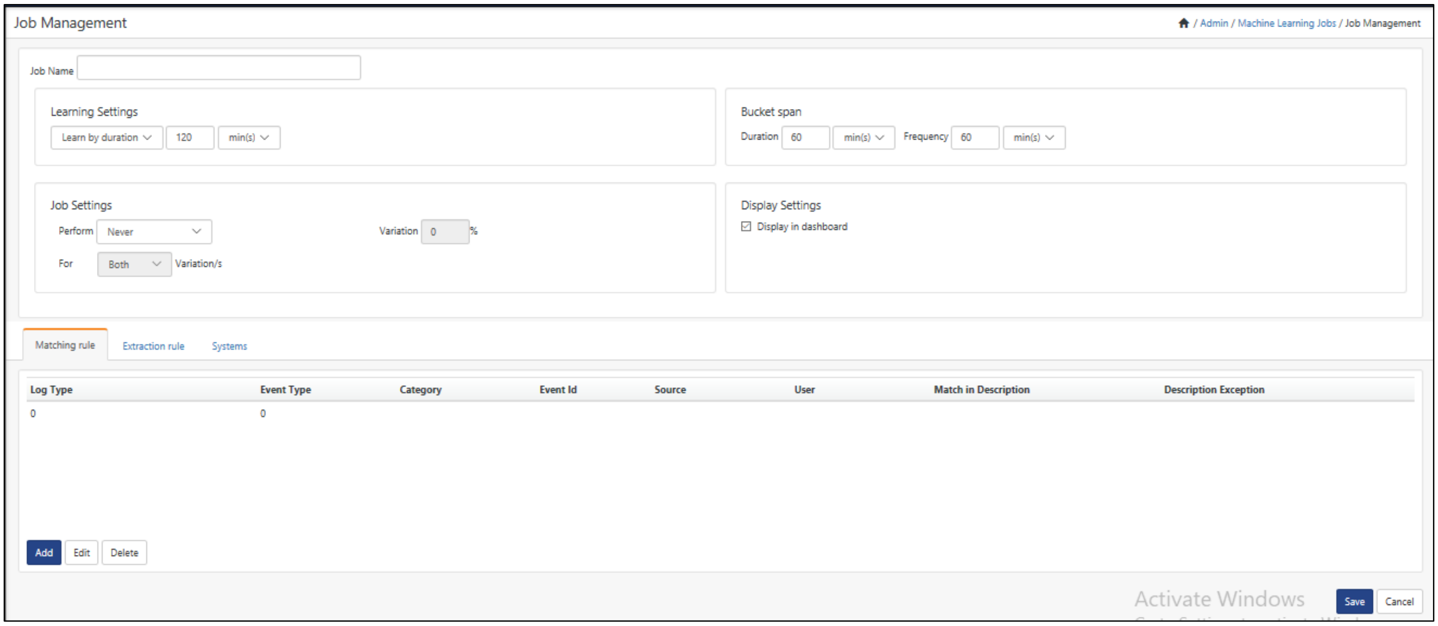
Table 43

7.2 Adding Machine Learning Jobs

This option helps to add Machine Learning Jobs.

i. To add Machine Learning Jobs in **Machine Learning Jobs** page, click **Add Jobs**.

EventTracker displays the **Job Management** page.


Job Management

/ Admin / Machine Learning Jobs / Job Management

Job Name

Learning Settings: Learn by duration 120 min(s)

Bucket span: Duration 60 min(s) Frequency 60 min(s)

Job Settings: Perform Never; Variation 0 %; For Both Variation/s

Display Settings: ☑ Display in dashboard

Log Type	Event Type	Category	Event Id	Source	User	Match in Description	Description Exception
0	0						

Activate Windows

Figure 350

‘Threshold settings’ fields	Description
Learning settings	Learn by duration period (in minutes). The Machine Learning of custom job will be monitored for the set learning period and a threshold value will be benchmarked.
Job Settings	The Job check can be done with With global value/With custom value/Never. **Perform Never**: Job check will not be performed. **With global value**: The Job check will be performed based on the global Machine Learning settings. **With custom value**: The Job check will be performed according to the Job check settings provided in the Machine Learning job.
Bucket Span	The custom job will be evaluated every ‘N’ minute to analyze the activities. The custom rule will be monitored for the duration specified in this field for the respective frequency.
Variation	The variation percentage can be added manually to decide the anomalous activities.

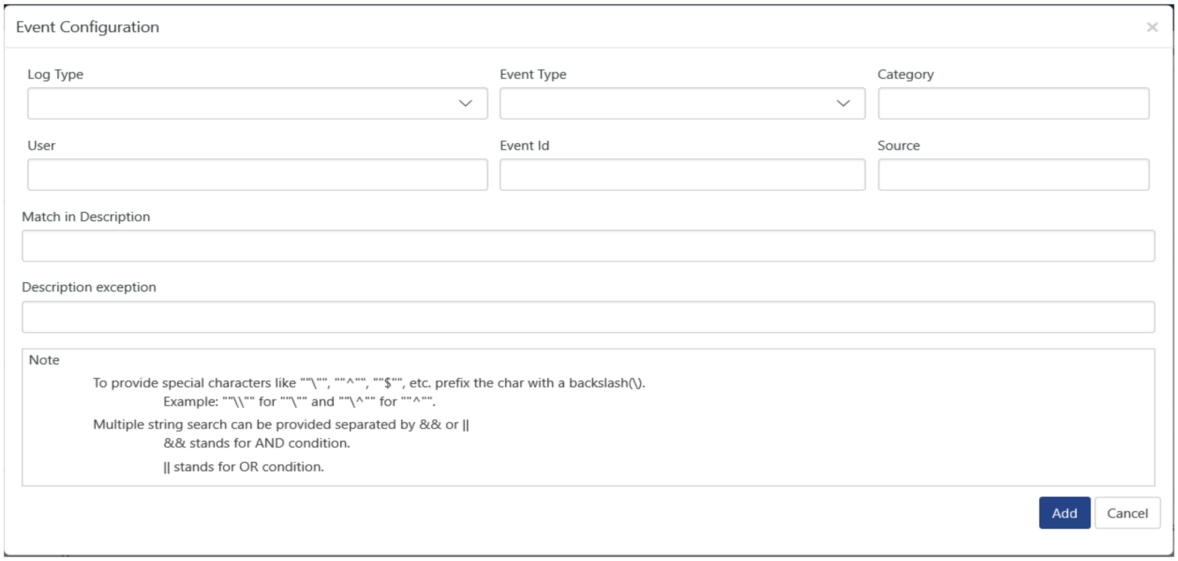
Table 44

2 In the **Matching Rule** field, provide a name for the new Jobs.

Ex: Audit Success.

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

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



Event Configuration ×

Log Type

Event Type

Category

User

Event Id

Source

Match in Description

Description exception

Note

To provide special characters like ""\"", ""^"", ""$"", etc. prefix the char with a backslash(\).
Example: ""\\"" for ""\"" and ""\^"" for ""^"".

Multiple string search can be provided separated by && or ||
&& stands for AND condition.
|| stands for OR condition.

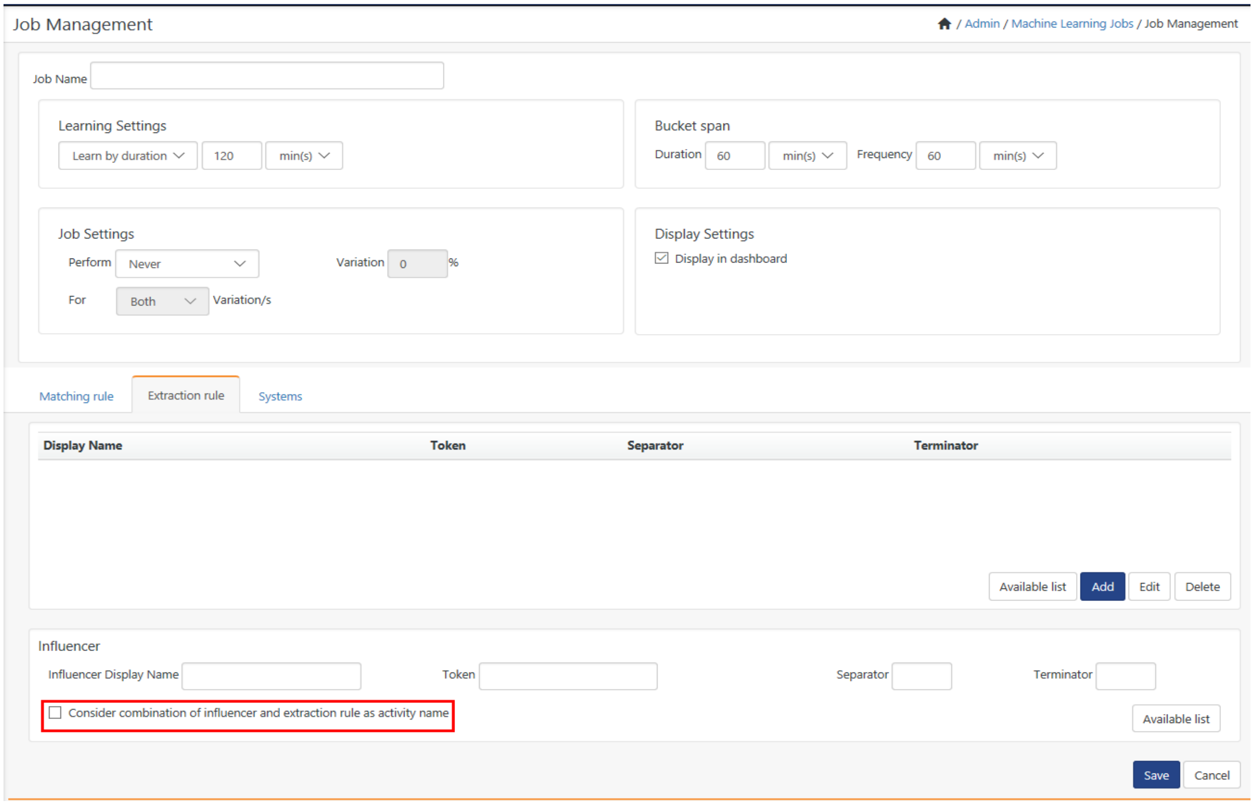
Add Cancel

Figure 351

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

The newly created event rule gets listed on **Matching Rule** tab.

5 Click the **Extraction Rule** tab.



Job Management

/ Admin / Machine Learning Jobs / Job Management

Job Name

Learning Settings

Learn by duration 120 min(s)

Bucket span

Duration 60 min(s) Frequency 60 min(s)

Job Settings

Perform Never Variation 0 %

For Both Variation/s

Display Settings

☑ Display in dashboard

Matching rule | Extraction rule | Systems

Display Name	Token	Separator	Terminator

Available list Add Edit Delete

Influencer

Influencer Display Name Token Separator Terminator

☐ Consider combination of influencer and extraction rule as activity name

Available list

Save Cancel

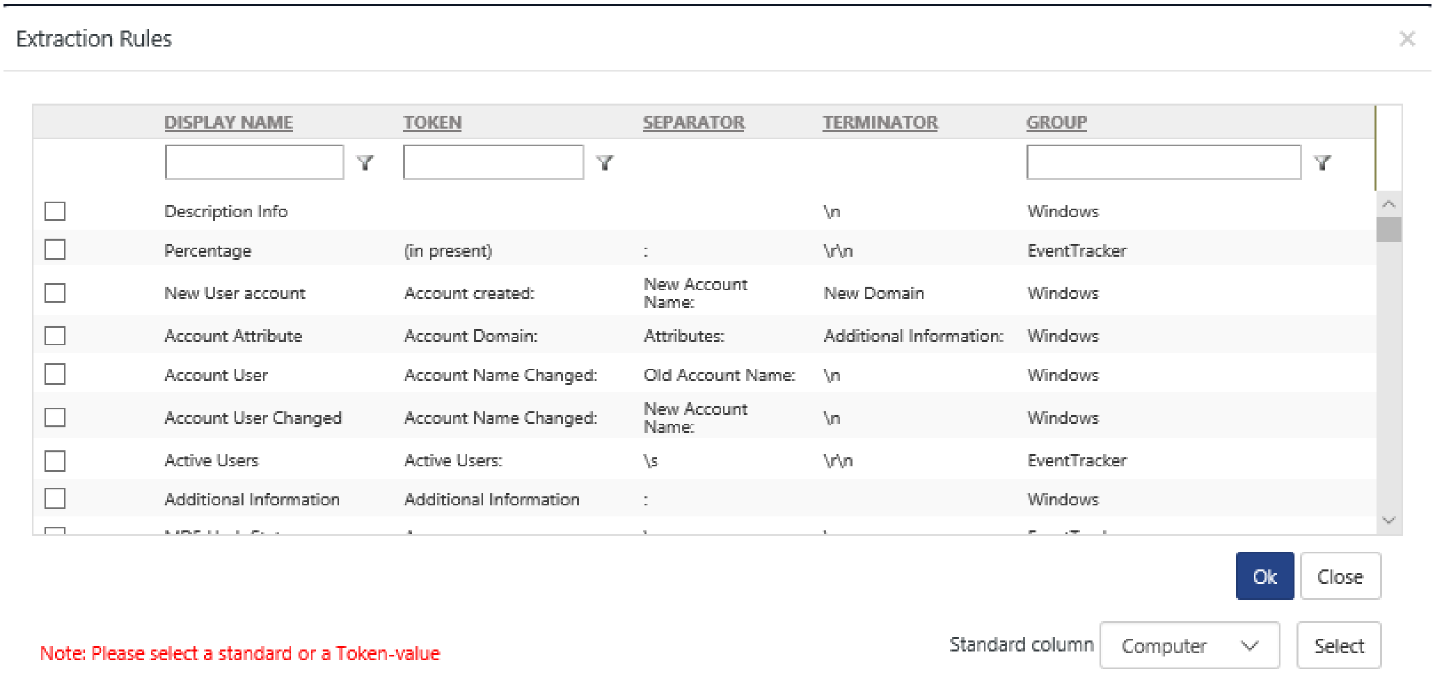
Figure 352

NOTE

You can select processing rule from a custom list or you can configure it on your own. You can also consider the combination of break-up column and processed column as activity name by selecting the check box as highlighted in the figure above.

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

Available list – It is a pre-defined rule set.


Extraction Rules

	DISPLAY NAME	TOKEN	SEPARATOR	TERMINATOR	GROUP
□	Description Info			\n	Windows
□	Percentage	(in present)	:	\r\n	EventTracker
□	New User account	Account created:	New Account Name:	New Domain	Windows
□	Account Attribute	Account Domain:	Attributes:	Additional Information:	Windows
□	Account User	Account Name Changed:	Old Account Name:	\n	Windows
□	Account User Changed	Account Name Changed:	New Account Name:	\n	Windows
□	Active Users	Active Users:	\s	\r\n	EventTracker
□	Additional Information	Additional Information	:		Windows

Note: Please select a standard or a Token-value

Standard column: Computer

Figure 353

a. Select the checkbox to add a **Token-value** as Extraction rule, and then click the **OK** button.

These Token-values are extracted from '**Event Description'**.

(OR)

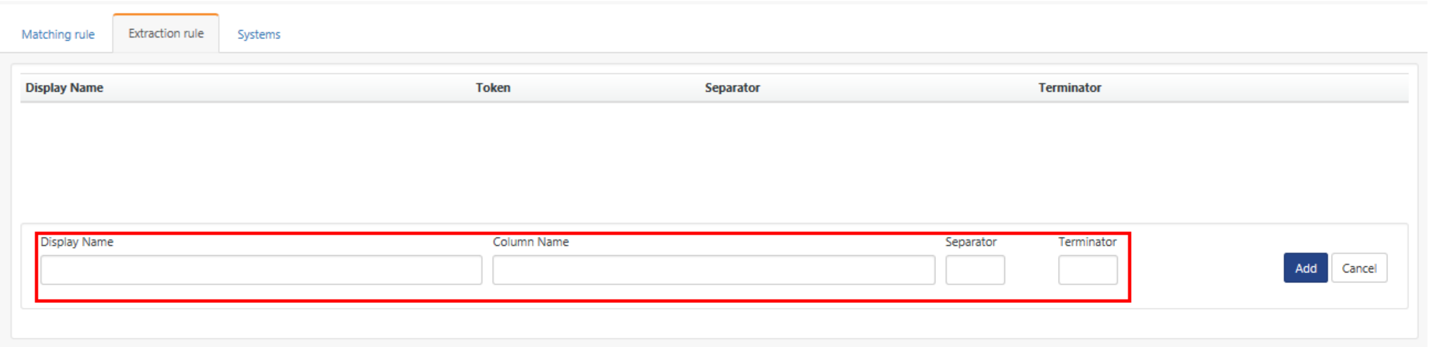
Select an appropriate option from the **Standard column** drop-down list.

These column names are extracted from '**Event Properties'**.

EventTracker adds the Extraction rule.

7 Click **Add**.

EventTracker displays the required fields for you to enter.



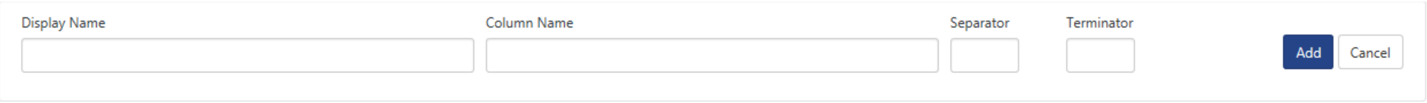
Display Name	Token	Separator	Terminator

Display Name | Column Name | Separator | Terminator

Figure 354

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

8 Add **Influencer** column details.

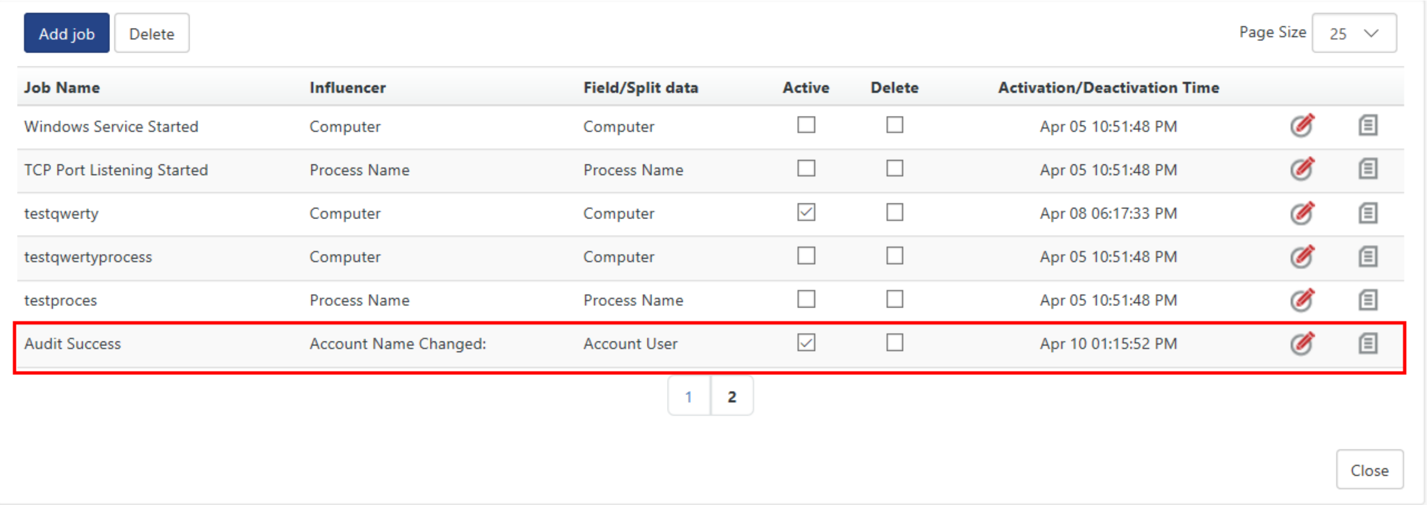


Display Name | Column Name | Separator | Terminator

Figure 355

These fields are mandatory. Click **Save**.

EventTracker displays the **Machine Learning Jobs** page with newly added job(s).



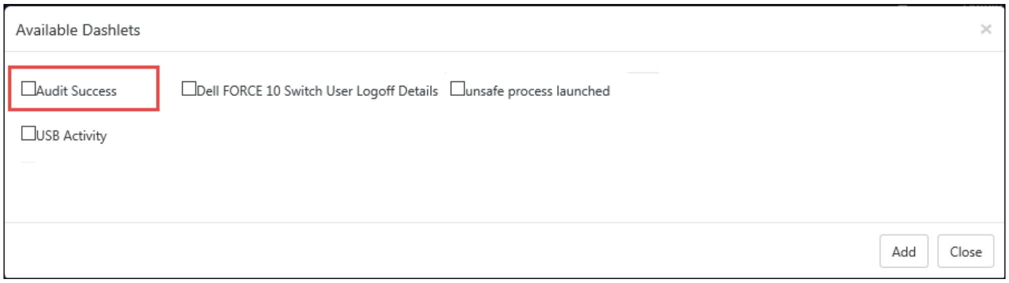
Job Name	Influencer	Field/Split data	Active	Delete	Activation/Deactivation Time
Windows Service Started	Computer	Computer	☐	☐	Apr 05 10:51:48 PM
TCP Port Listening Started	Process Name	Process Name	☐	☐	Apr 05 10:51:48 PM
testqwerty	Computer	Computer	☑	☐	Apr 08 06:17:33 PM
testqwertyprocess	Computer	Computer	☐	☐	Apr 05 10:51:48 PM
testproces	Process Name	Process Name	☐	☐	Apr 05 10:51:48 PM
Audit Success	Account Name Changed:	Account User	☑	☐	Apr 10 01:15:52 PM

Figure 356

7.2.1 Adding custom Machine Learning Jobs in Machine Learning Dashboard

1. Click **Machine Learning;** select the **Customize** option from the drop-down list.

   Available Dashlets dialog box displays the newly added Machine Learning Jobs as a dashlet.



Available Dashlets

□Audit Success □Dell FORCE 10 Switch User Logoff Details □unsafe process launched

□USB Activity

Figure 357

2. Check the newly created Machine Learning Jobs option, and then click **Add**.

   EventTracker displays the dashlet on the **Machine Learning** dashboard.

3. Click a donut on the chart or a legend to view non-admin user activity details.

   EventTracker displays the "**Model Explorer**" page.

8. Machine Learning Settings

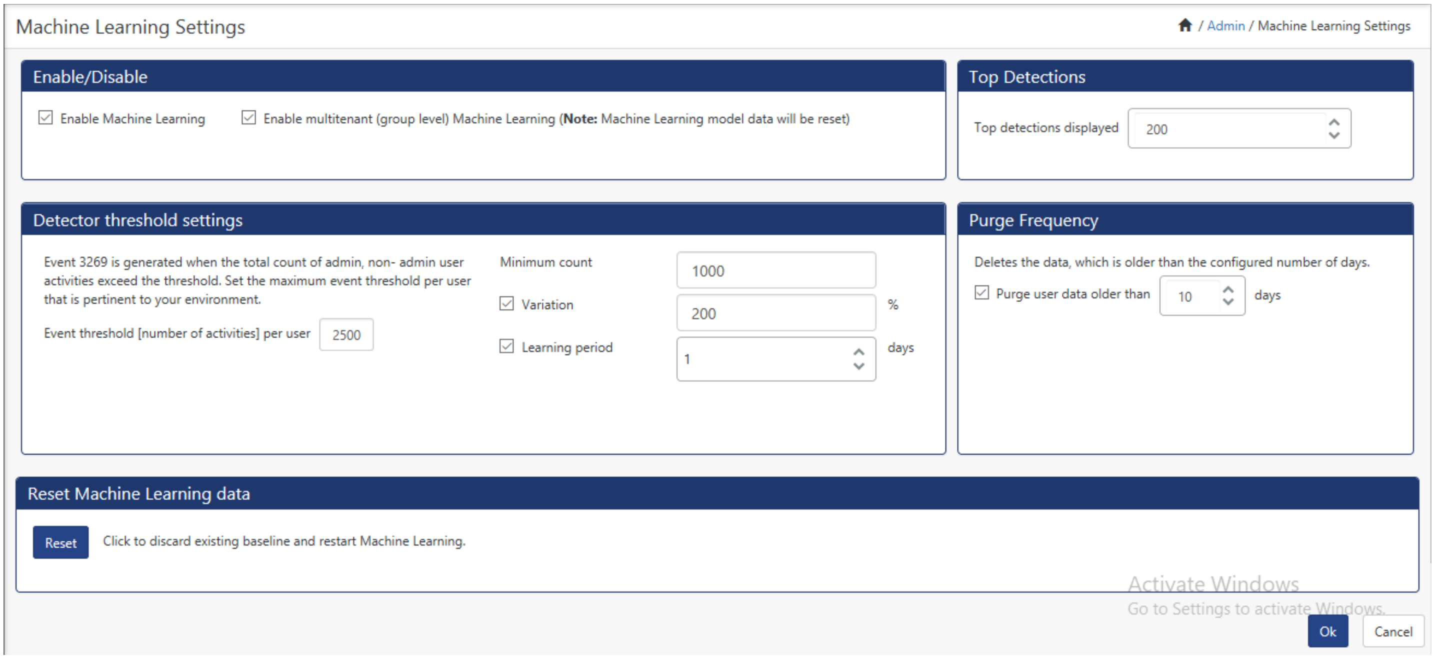
In this chapter, you will learn about:

- Configuring Machine Learning Settings

8.1 Machine Learning Settings

1. This option helps you configure Machine Learning Activity monitoring parameters.
2. Click the **Admin**, and then select **Machine Learning Settings**.

   EventTracker displays the **Machine Learning Settings** page.



Machine Learning Settings

/ Admin / Machine Learning Settings

Enable/Disable

☑ Enable Machine Learning ☑ Enable multitenant (group level) Machine Learning (**Note:** Machine Learning model data will be reset)

Top Detections

Top detections displayed: 200

Detector threshold settings

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.

Event threshold [number of activities] per user: 2500

Minimum count: 1000

☑ Variation: 200 %

☑ Learning period: 1 days

Purge Frequency

Deletes the data, which is older than the configured number of days.

☑ Purge user data older than 10 days

Reset Machine Learning data

Reset — Click to discard existing baseline and restart Machine Learning.

Activate Windows
Go to Settings to activate Windows.

Ok Cancel

Figure 358

Field	Description
Enable/Disable	
Enable Machine Learning	This parameter is used for backward compatibility. Any time any user crosses 2500 (default) activities - EventTracker will generate an event. This is only for user and admin activity (IP, process, alerts and event-ids are excluded)
Detector threshold	
Detector Threshold settings [number of activities] per user	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.
Purge Frequency	
Purge user data older than	EventTracker purges the Machine Learning activity data older than the configured number of days.
Top Detection	
Top detections displayed	Only the selected number of activities will be displayed on the left hand side pane of the 'Model Explorer page.
Group Level	
Enable multitenant	It will monitor Machine Learning and can be set at different group level.
Reset Machine Learning Data	
Reset	Reset the existing baseline of Machine learning and start a new learning of the data. It deletes all the previous Machine Learning related data and not the customized jobs.

Table 45

9. Casebook Configuration

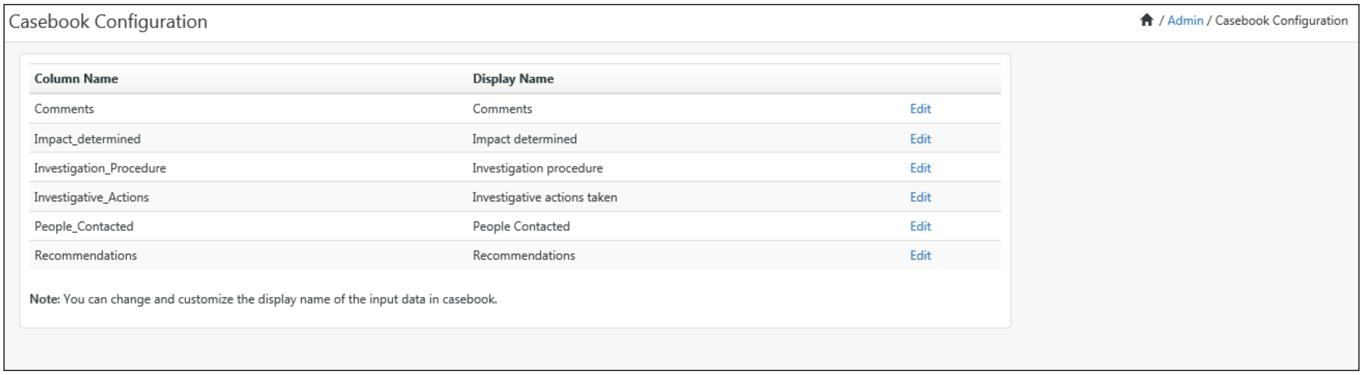
In this chapter, you will learn how to use:

- Casebook Configuration

9.1 Using Casebook Configuration

Casebook Configuration allows a user to change and customize the display name of the input data in Casebook.

1. Logon to EventTracker.
2. Select the **Admin** menu and then click **Casebook Configuration** from the drop-down list.
   Casebook Configuration window opens.



Casebook Configuration

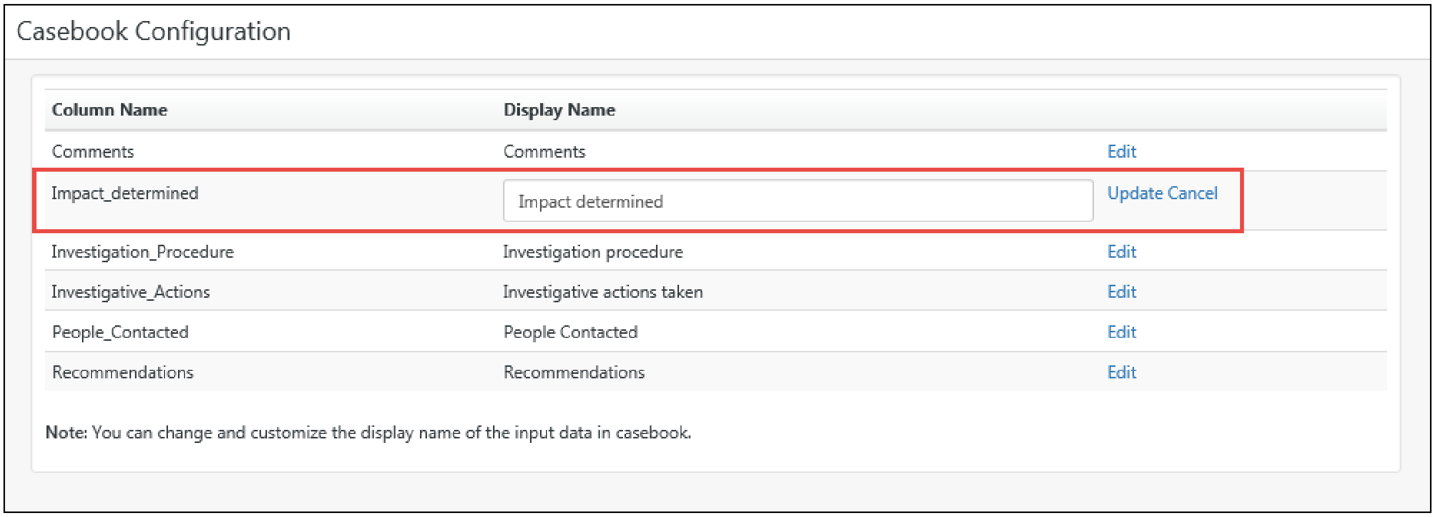
/ Admin / Casebook Configuration

Column Name	Display Name	
Comments	Comments	Edit
Impact_determined	Impact determined	Edit
Investigation_Procedure	Investigation procedure	Edit
Investigative_Actions	Investigative actions taken	Edit
People_Contacted	People Contacted	Edit
Recommendations	Recommendations	Edit

Note: You can change and customize the display name of the input data in casebook.

Figure 359

3. Click **Edit** ✎.



Casebook Configuration

Column Name	Display Name	
Comments	Comments	Edit
Impact_determined	Impact determined	Update Cancel
Investigation_Procedure	Investigation procedure	Edit
Investigative_Actions	Investigative actions taken	Edit
People_Contacted	People Contacted	Edit
Recommendations	Recommendations	Edit

Note: You can change and customize the display name of the input data in casebook.

Figure 360

4. Enter the new **Column Name, Display Name** and then click **Update**.
   The display name is changed accordingly in the Casebook.

NOTE

Only the respective logged in user can enter display name and the updated display name will be shown while adding new Casebook.

10. Category

In this chapter, you will learn about

- Category Management
- Add Categories as alerts
- Move Categories

10.1 Managing Category Groups

A set of relevant Categories can be organized under a Group.

10.1.1 Creating 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**, and then click **Category**.

2 Right-click **All Categories** or any other Category group.

EventTracker opens the shortcut menu.

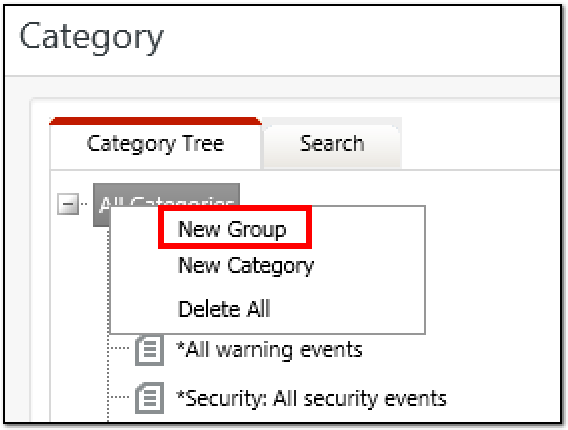


Figure 361

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.

Field	Description
Parent Node	Name of the parent group under which EventTracker adds the newly created group as a sub-group.
Enter Group name	Type the name of the group.

Table 46

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 opens the newly added Category group under the selected parent group.

10.1.2 Modifying Category Groups

This option enables you to modify a Category group.

1 Right-click the group that you want to modify, and then select **Edit Group**.

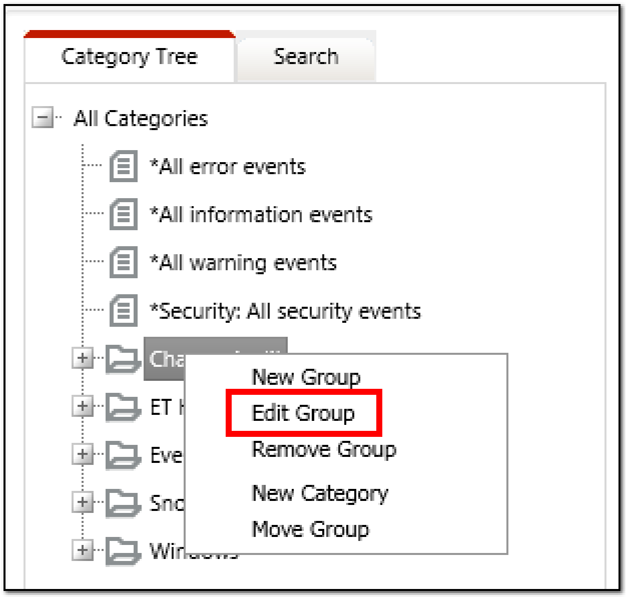


Figure 362

EventTracker opens the **Edit Group** page on the right pane.

2 Type appropriate group name in the **Enter Group Name** field.

3 Click **OK**.

🗎 NOTE

You cannot edit the name of the Parent Node.

10.1.3 Deleting Category Groups

This option enables you to remove a **Category Group**.

1 Right-click the group that you want to delete, and then select **Remove Group**.

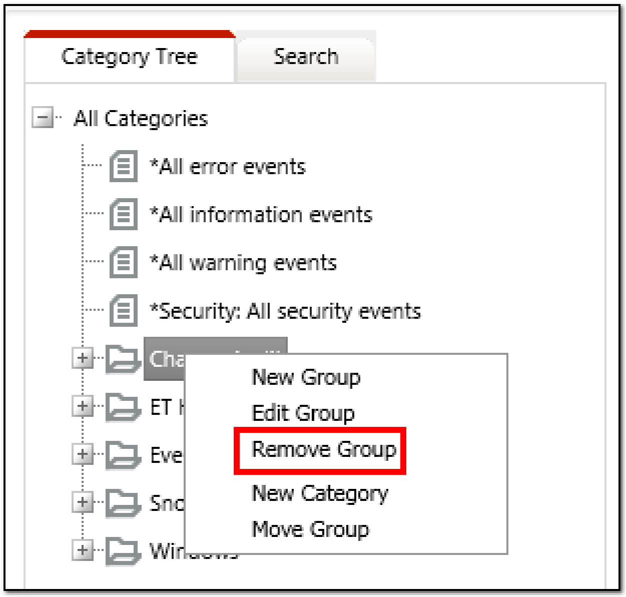


Figure 363

EventTracker opens the Confirmation message box.

2 Click **OK** to remove or **Cancel** to abort.

10.1.4 Modifying Category

This option enables you to modify a **Category group**.

1. Right-click the category that you want to modify, and then select **Edit Category**.

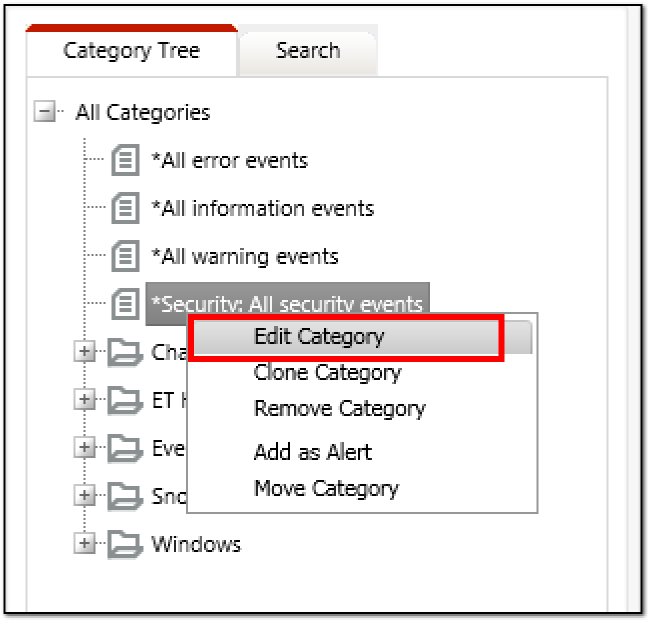
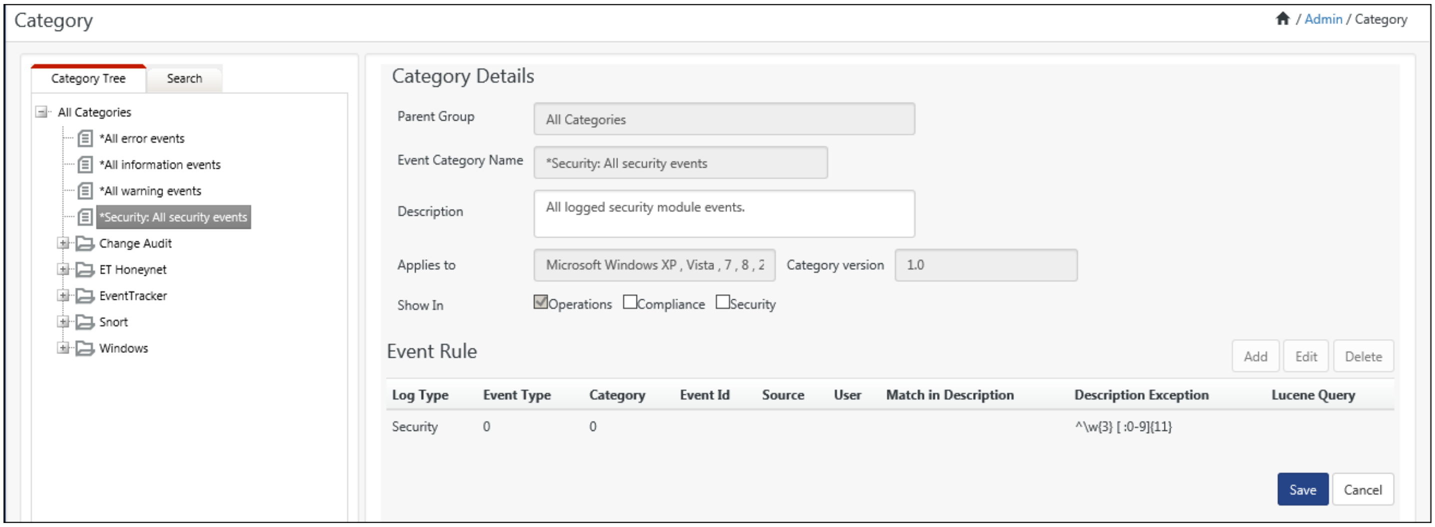


Figure 364

Category Details pane opens. Only the few options are editable.



Category Details

Parent Group: All Categories

Event Category Name: *Security: All security events

Description: All logged security module events.

Applies to: Microsoft Windows XP , Vista , 7 , 8 , 2 Category version: 1.0

Show In: ☑Operations □Compliance □Security

Event Rule

Log Type	Event Type	Category	Event Id	Source	User	Match in Description	Description Exception	Lucene Query
Security	0	0					^\w{3} [:0-9]{11}	

Figure 365

2. If required, enter the **Description:**
3. If required, select **Compliance** and **Security** options, and then select **Save**.

🗎 NOTE

You cannot edit the name of the Parent Node.

10.2 Cloning category

This feature is used to make a copy of the existing category.

1. Right-click a category and then select **Clone Category**.

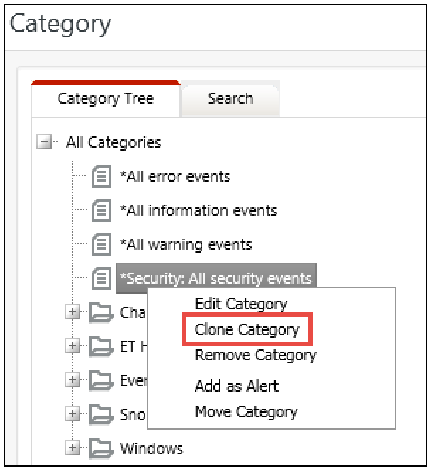
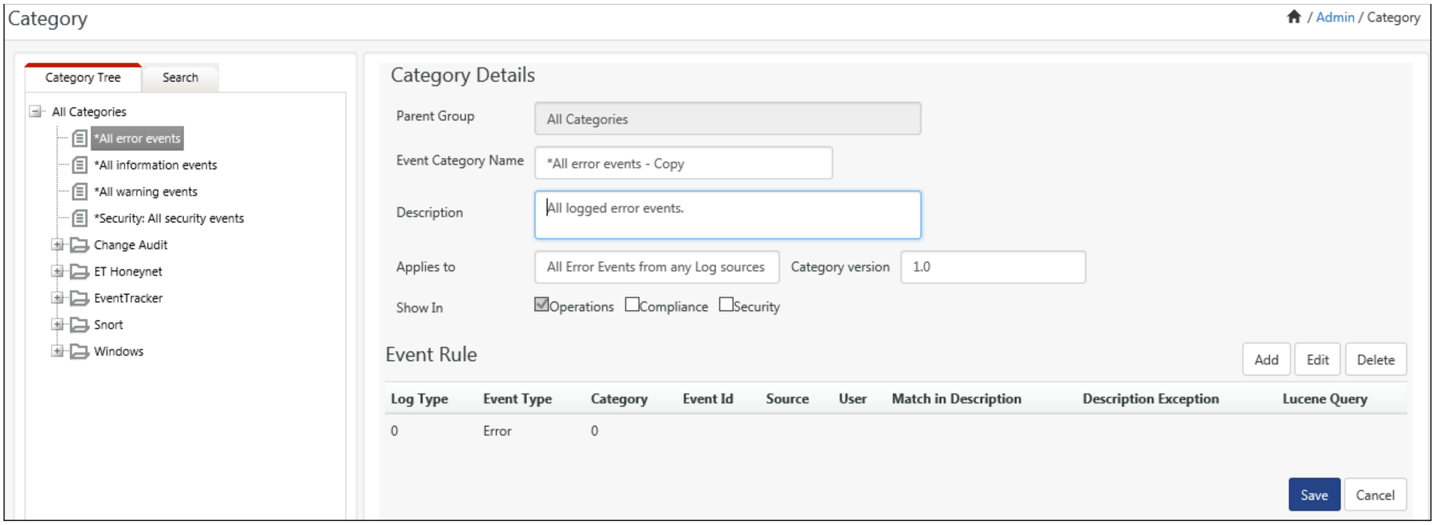


Figure 366

Category Details pane opens.



Category

/ Admin / Category

Category Tree | Search

- All Categories
  - *All error events
  - *All information events
  - *All warning events
  - *Security: All security events
  - Change Audit
  - ET Honeynet
  - EventTracker
  - Snort
  - Windows

Category Details

Parent Group	All Categories		
Event Category Name	*All error events - Copy		
Description	All logged error events.		
Applies to	All Error Events from any Log sources	Category version	1.0
Show In	☑Operations ☐Compliance ☐Security		

Event Rule

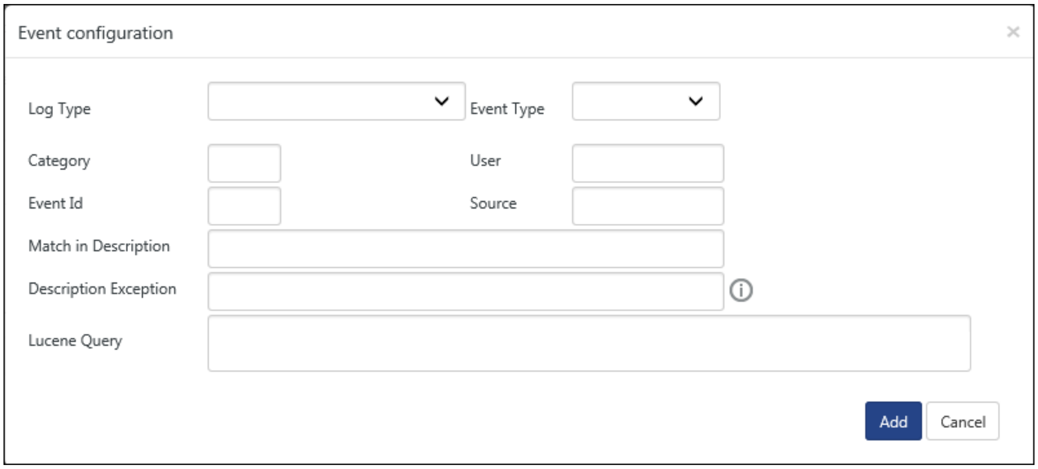
Add | Edit | Delete

Log Type	Event Type	Category	Event Id	Source	User	Match in Description	Description Exception	Lucene Query
0	Error	0						

Save | Cancel

Figure 367

2. To add a new event rule or edit a rule, click **Add** or **Edit**.



Event configuration ×

Log Type		Event Type	
Category		User	
Event Id		Source	
Match in Description			
Description Exception			
Lucene Query			

Add | Cancel

Figure 368

3. Click **Save**.

10.2.1 Removing Category Groups

This option enables you to remove a Category Group.

1 Right-click the group that you want to delete.

EventTracker opens the shortcut menu.

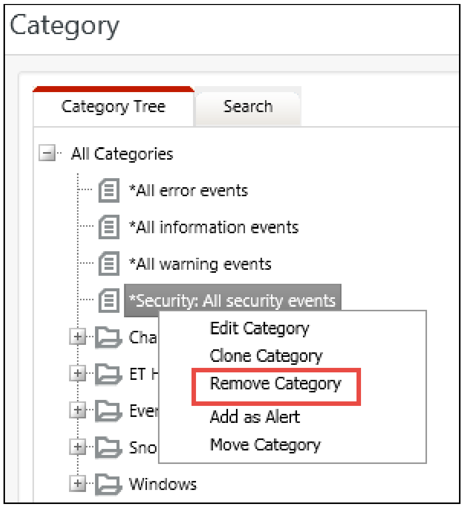


Figure 369

2 From the shortcut menu, click **Remove Group**.

EventTracker opens the Confirmation message box.

3 Click **OK** to remove or **Cancel** to abort.

10.3 Managing 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.

10.3.1 Creating 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 opens the shortcut menu.

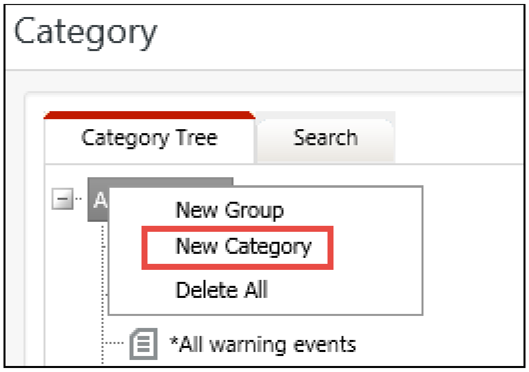
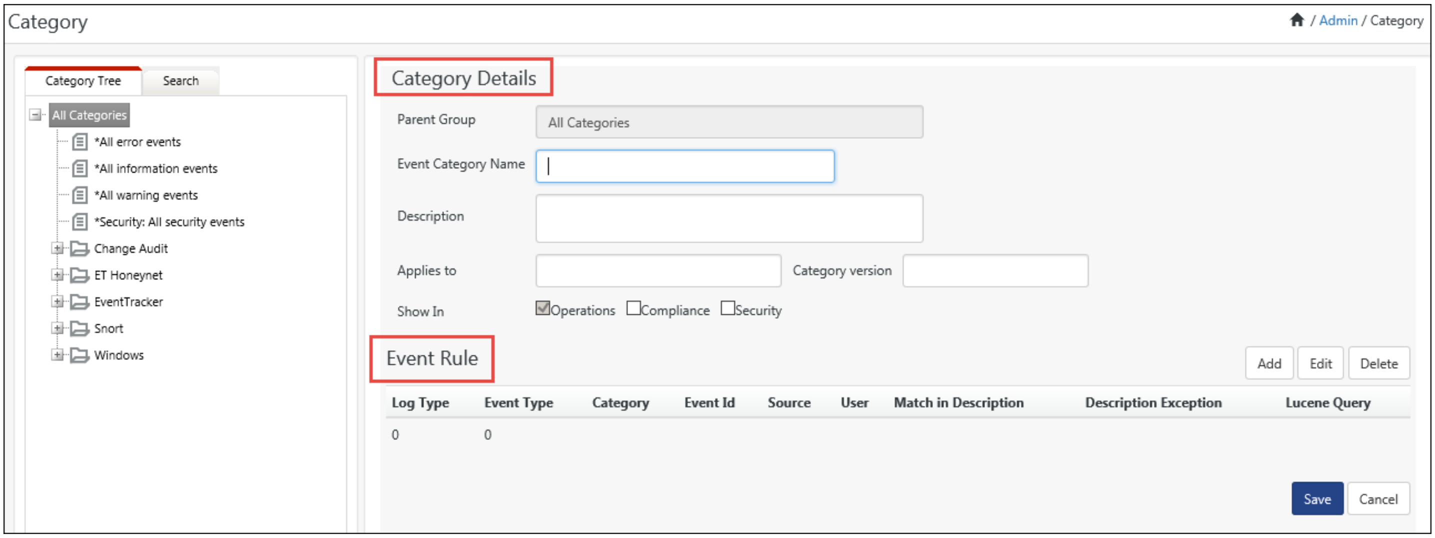


Figure 370

2. From the shortcut menu, click **New Category**.

   EventTracker opens the **Category Details** page on the right pane.



Category Details

Parent Group: All Categories

Event Category Name:

Description:

Applies to: Category version:

Show In: ☑ Operations ☐ Compliance ☐ Security

Event Rule

Log Type	Event Type	Category	Event Id	Source	User	Match in Description	Description Exception	Lucene Query
0	0							

Figure 371

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.
Applies to	Type the name of the application or server for which the category is created
Category Version	Type the version of the category.

Table 47

3. Enter appropriate data in relevant fields.
4. Click **Add** to add **Event Rule**.

   EventTracker opens the Event Configuration pop-up window.

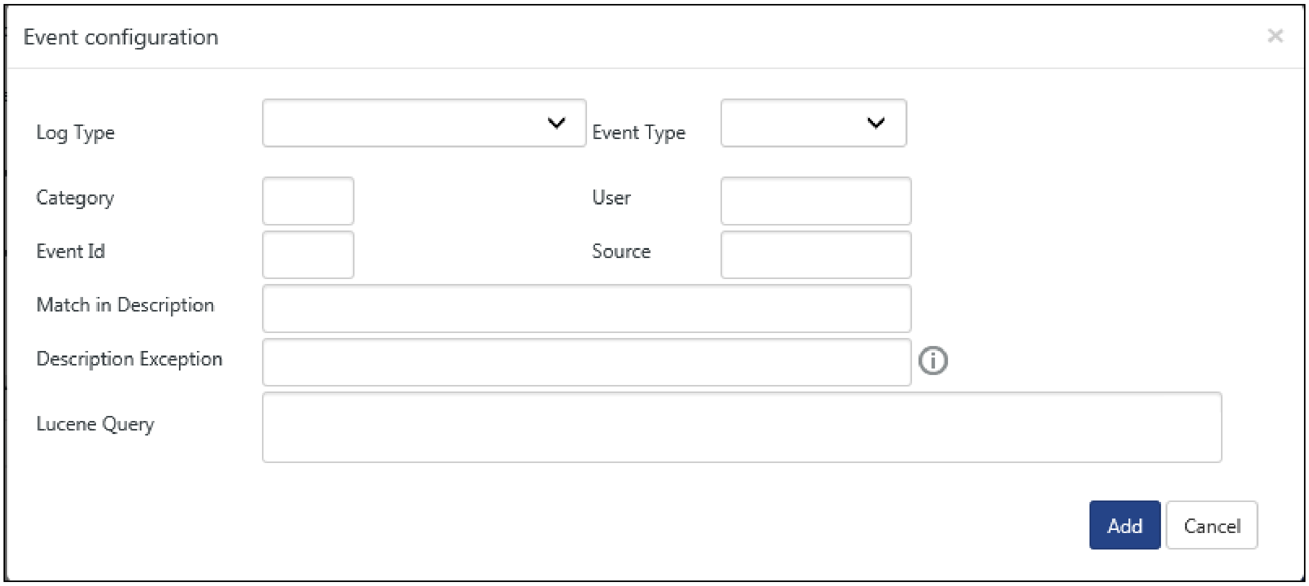


Figure 372

Field	Description
Event Rule	
Event Type	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.
Category	Type the category number in this field. This field supports numeric data type only.
Log Type	This field describes the options are System, Security, Application, DNS Server, File Replication, and Directory Service.
Event ID	Type the event ID number in this field. This field supports numeric data type only.
Source	Type the source in this field.
User	Type the user name in this field.
Match in Event Description	Type a sub-string of the description that needs to be matched.
More information	Type the additional information about the event category in this field.

Table 48

🗎 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**.

10.3.2 Modifying Categories

This option helps you modify Categories.

1. To modify categories, right-click the Category to modify, and then select Edit Category.

   EventTracker opens the shortcut menu.

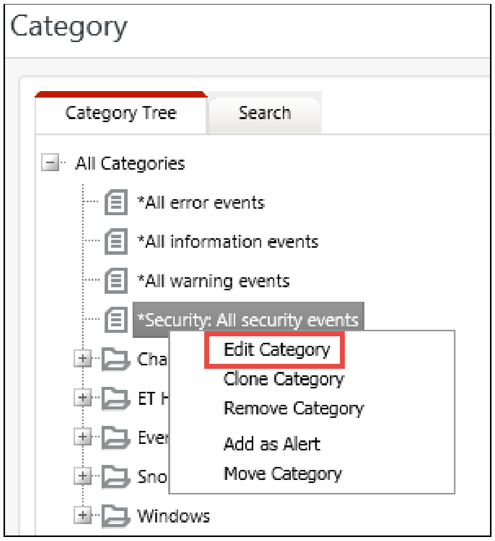


Figure 373

2. From the shortcut menu, click **Edit Category**.

   EventTracker opens the **Category Details** page on the right pane.
3. To edit event details, select an event and then click **Edit**.

   EventTracker opens the **Event Configuration** pop-up window.
4. Enter appropriate data and then click **Save**.

🗎 NOTE

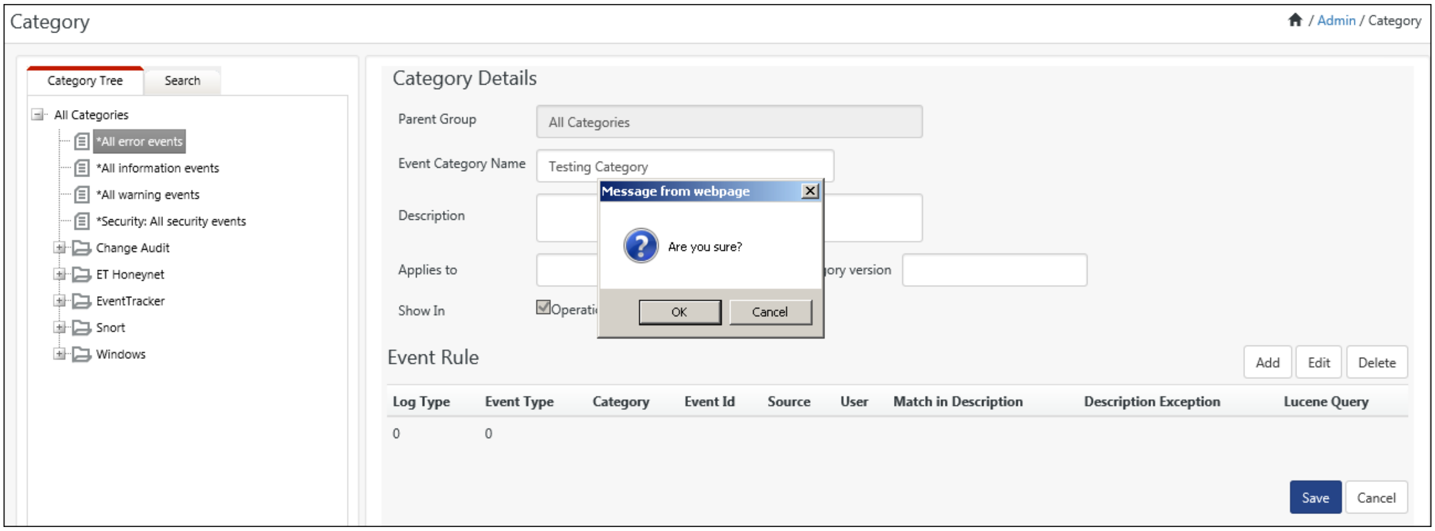
You can edit only the custom created categories. The pre-defined categories cannot be edited.

10.3.3 Removing Categories

This option enables you to delete a Category.

1. Right-click the Category to remove, and then select **Remove category**.

   Message from webpage opens.



Parent Group: All Categories

Event Category Name: Testing Category

Show In: ☑ Operati

Message from webpage

Are you sure?

Log Type	Event Type	Category	Event Id	Source	User	Match in Description	Description Exception	Lucene Query
0	0							

Figure 374

2. Click **OK**.

   EventTracker deletes the selected Category.

10.3.4 Deleting Event Rules

This option helps you delete Event Rules.

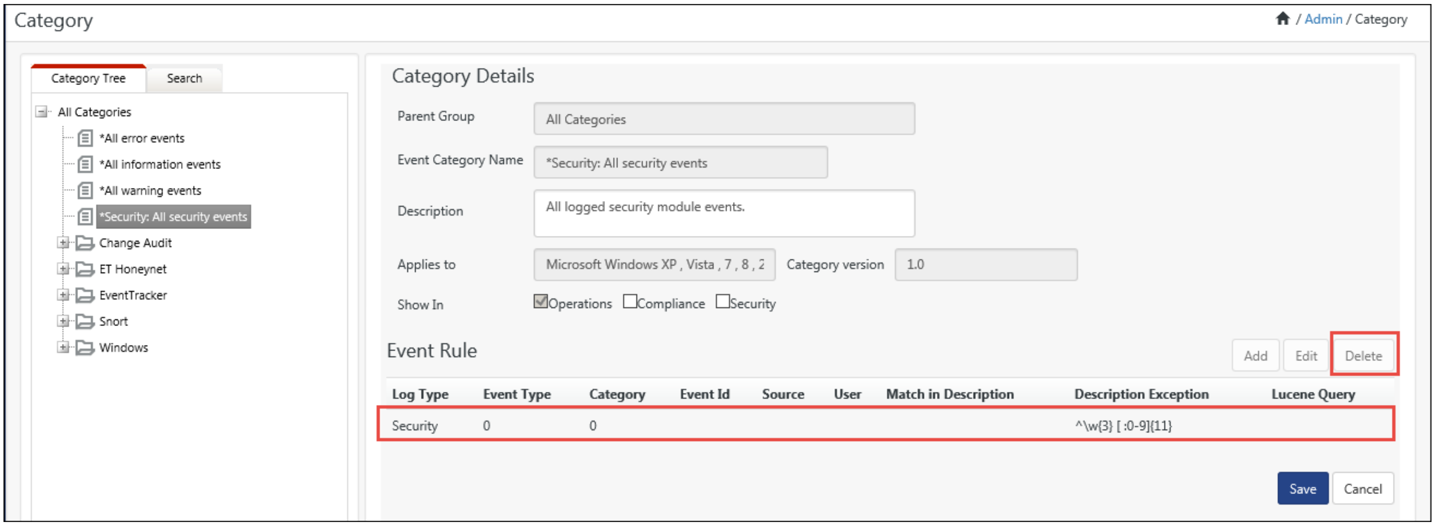
1. Right-click the Category that you want to edit.

   EventTracker opens the shortcut menu.

2. From the shortcut menu, click **Edit Category**.

   EventTracker opens the **Category Details** page.

3. Select the **Event Rule** that you want to delete.



Category Details

Parent Group: All Categories

Event Category Name: *Security: All security events

Description: All logged security module events.

Applies to: Microsoft Windows XP , Vista , 7 , 8 , 2 Category version: 1.0

Show In: ☑Operations □Compliance □Security

Event Rule

Log Type	Event Type	Category	Event Id	Source	User	Match in Description	Description Exception	Lucene Query
Security	0	0					^\w{3} [:0-9]{11}	

Figure 375

4. Click **Delete**.

   EventTracker opens the Confirmation message box.

5. Click **OK**.

   EventTracker deletes the selected event rule.

6. Click **Save** on the **Category Details** page.

10.4 Adding Categories as Alerts

This option enables you to add Categories as Alerts.

1. To add a category as an alert, right-click a category, and then select **Add as Alert**.

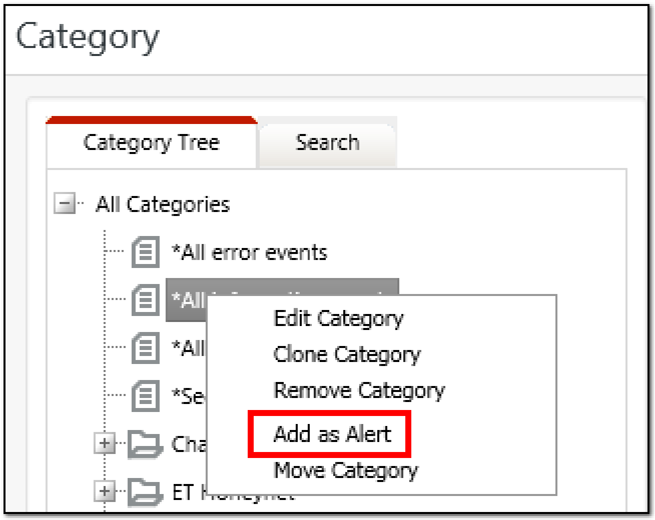
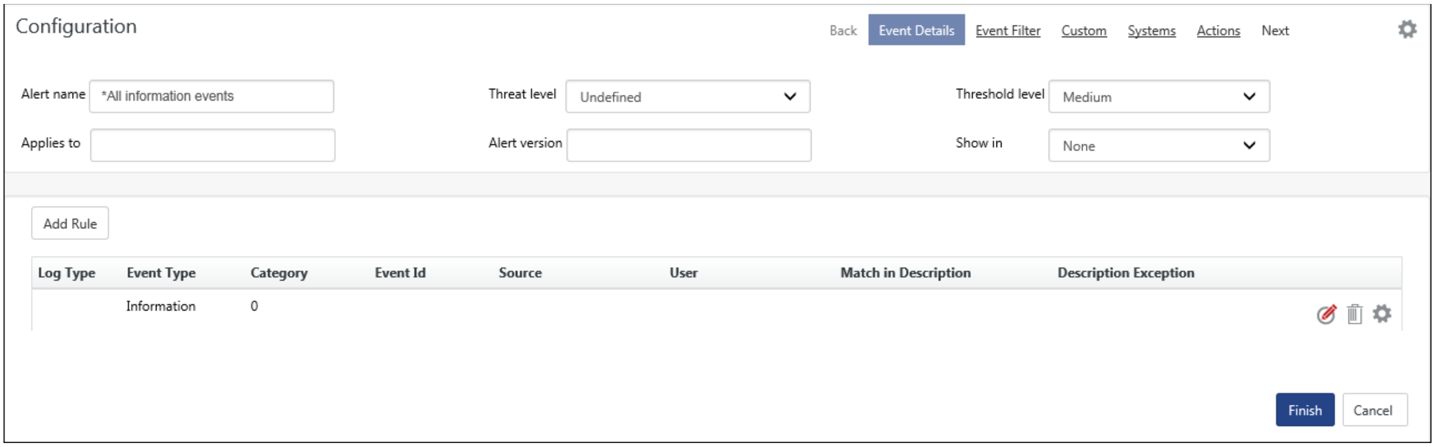


Figure 376

Alert Configuration window opens.

2. Enter **Alert Version:**, **Applies To:** fields.

   For more details regarding How to Configure an Alert, please refer Alerts.



Alert name: *All information events

Threat level: Undefined

Threshold level: Medium

Applies to:

Alert version:

Show in: None

Log Type	Event Type	Category	Event Id	Source	User	Match in Description	Description Exception
	Information	0					

Figure 377

3. Select/Enter the required fields, and then select **Finish**.

   For more details, please refer Add Custom Alerts.

10.5 Moving Category

This option helps you to move categories.

1. To move a category, right-click the category and then select **Move category**.

   EventTracker opens the shortcut menu.

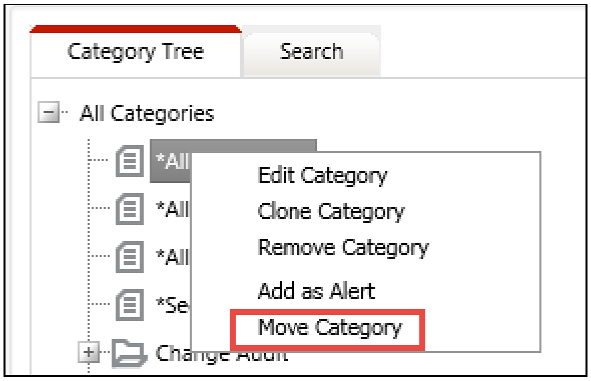
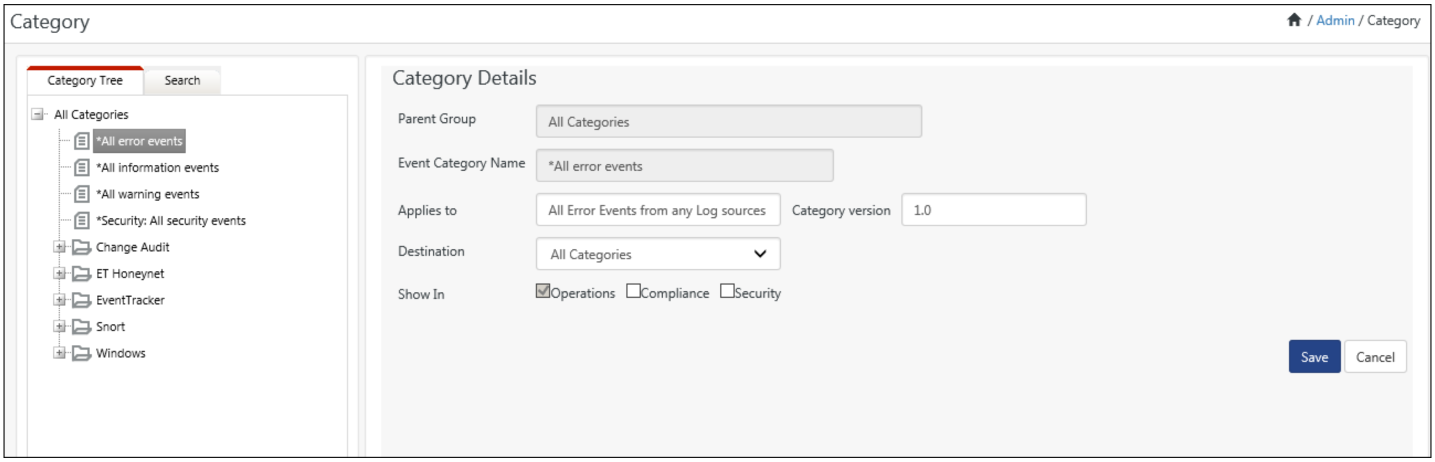


Figure 378

Category Details window opens.



Category Details

Parent Group: All Categories

Event Category Name: *All error events

Applies to: All Error Events from any Log sources

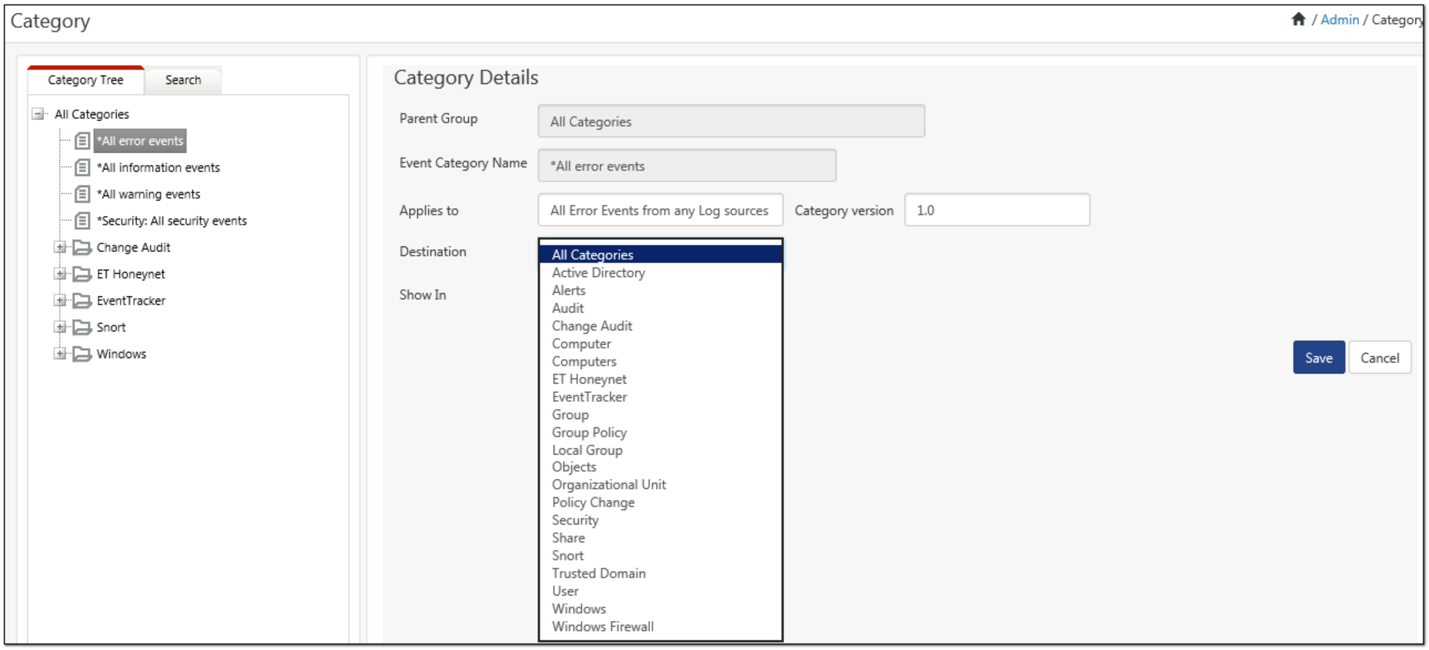
Category version: 1.0

Destination: All Categories

Show In: ☑Operations ☐Compliance ☐Security

Figure 379

1. Select **Destination**, and then select **Show In:** any options.



Category Details

Parent Group: All Categories

Event Category Name: *All error events

Applies to: All Error Events from any Log sources

Category version: 1.0

Destination:

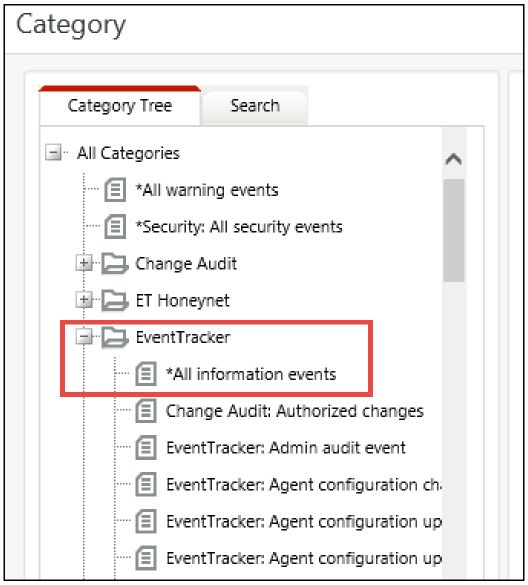
- All Categories
- Active Directory
- Alerts
- Audit
- Change Audit
- Computer
- Computers
- ET Honeynet
- EventTracker
- Group
- Group Policy
- Local Group
- Objects
- Organizational Unit
- Policy Change
- Security
- Share
- Snort
- Trusted Domain
- User
- Windows
- Windows Firewall

Show In

Figure 380

2. Select **Save**.

The category '*All information events' has been moved from its current location.



Category

Category Tree
Search
All Categories
*All warning events
*Security: All security events
Change Audit
ET Honeynet
EventTracker
*All information events
Change Audit: Authorized changes
EventTracker: Admin audit event
EventTracker: Agent configuration ch
EventTracker: Agent configuration up
EventTracker: Agent configuration up

Figure 381

11. Collection Point and Collection Master

In this chapter, you will learn about:

- Collection Point
- View Collection Point Configuration
- Add Collection Masters
- Edit Collection Master Settings in Collection Point
- Delete Collection Master Settings
- Collection Master
- View and edit Collection Point Details in Collection Master
- Configure Collection Master listening port
- Delete CAB Files
- Delete Collection Point Details

11.1 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. EventTracker 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.

11.1.1 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.

11.2 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.

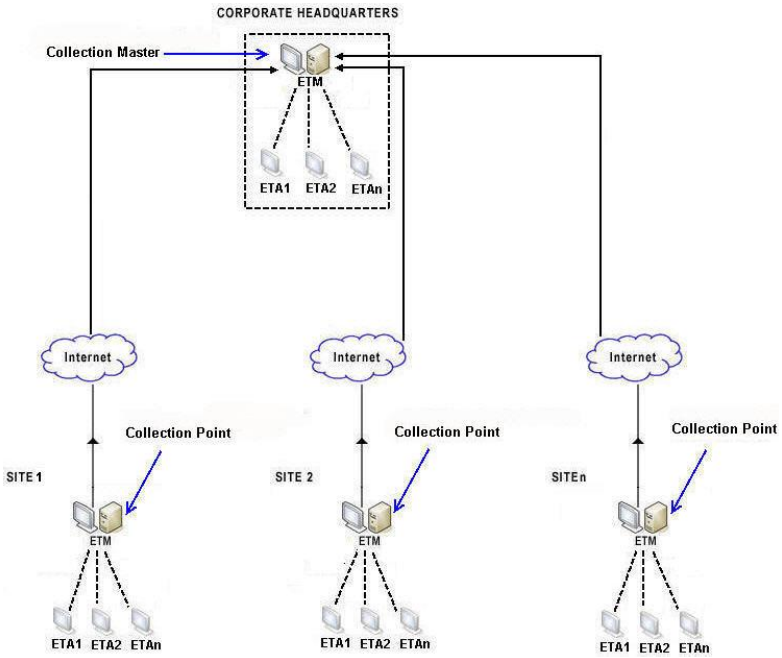


Figure 382

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.

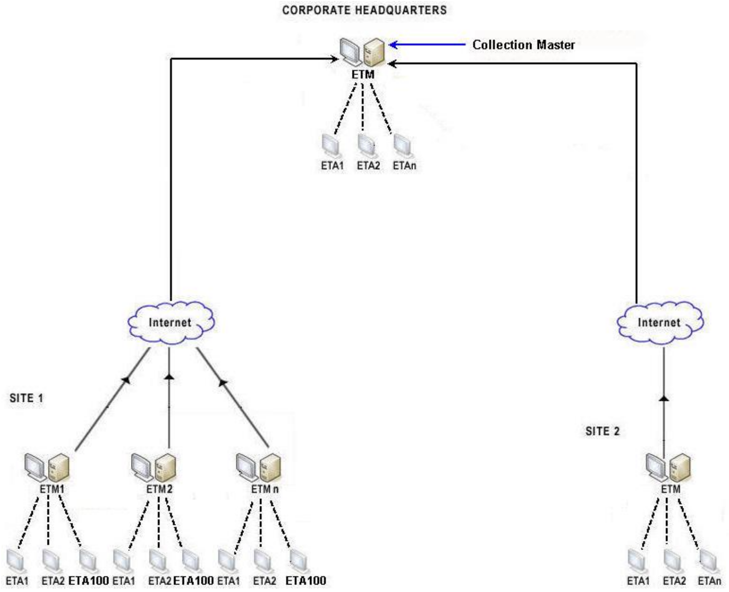


Figure 383

Scenario 3:

The scenario above corroborates the statement that one Collection Point (client) could be configured to report up to five Collection Masters (servers).

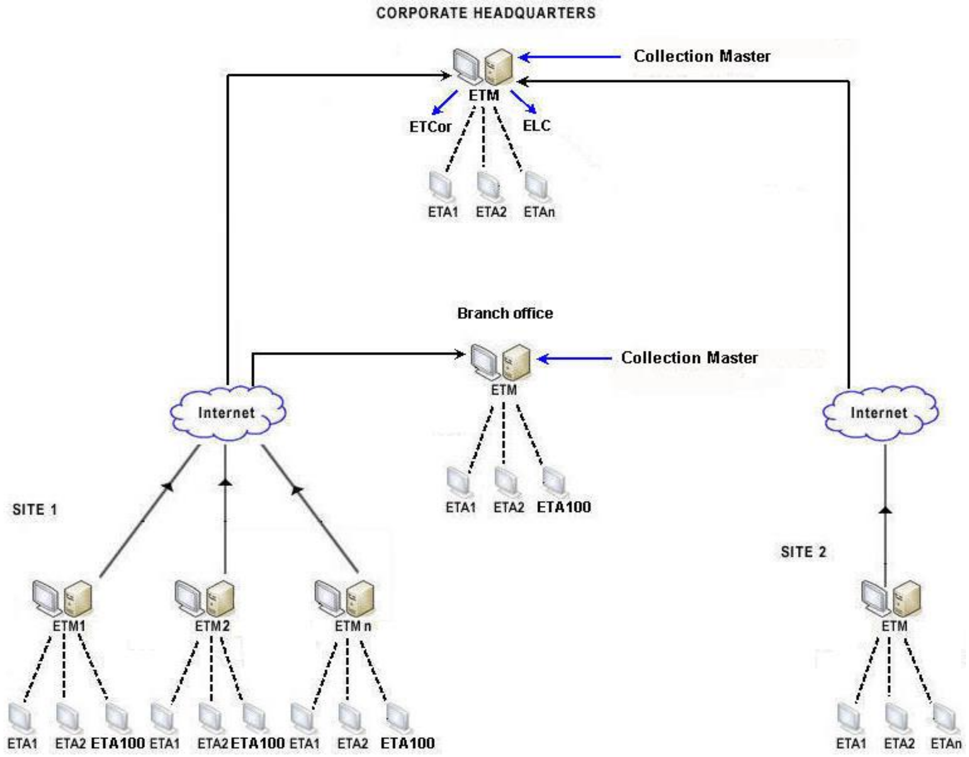


Figure 384

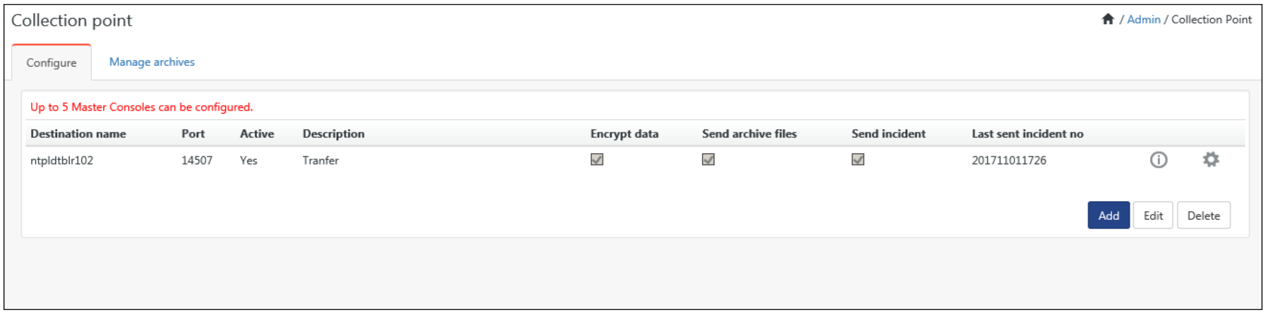
11.3 Viewing Collection Point Configuration

If CP is not sending Reports, behavior, Event-O-Meter or behavior data, the respective CP site will not be shown under the respective features of CM. You can now send Reports, Behavior, Sparse matrix, Event-O-Meter events to Collection Point.

1 To view Collection Point configuration, log on to EventTracker.

2 Click **Admin**, and then click the **Collection Point**.

EventTracker opens the Collection Point page.



Collection point

🏠 / Admin / Collection Point

Up to 5 Master Consoles can be configured.

Destination name	Port	Active	Description	Encrypt data	Send archive files	Send incident	Last sent incident no		
ntpldtblr102	14507	Yes	Tranfer	☑	☑	☑	201711011726	ⓘ	⚙

Figure 385

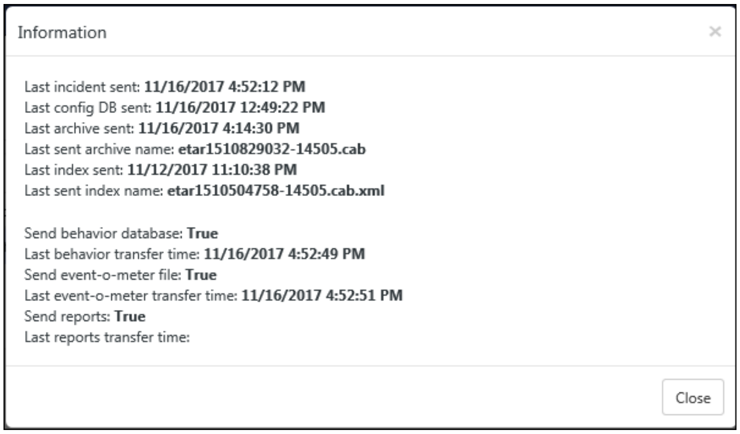
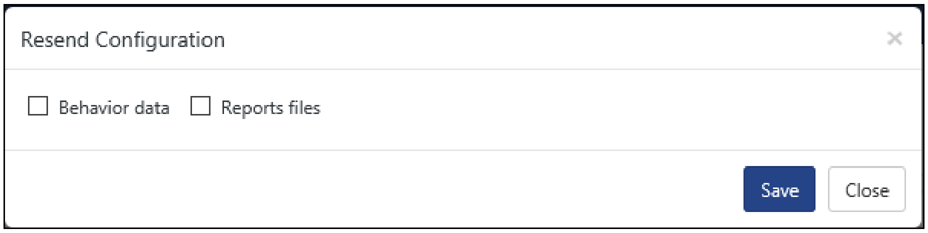
Click	To
Add	Add new Collection master(s)/ manager(s).
Edit	Edit Collection master(s)/ manager(s) configuration settings.
Delete	Delete Collection master(s)/ manager(s) configuration settings.
Information	Click ⓘ icon. Detailed regarding the Last sent incident, archives, db, index time displays.  Information Last incident sent: **11/16/2017 4:52:12 PM** Last config DB sent: **11/16/2017 12:49:22 PM** Last archive sent: **11/16/2017 4:14:30 PM** Last sent archive name: **etar1510829032-14505.cab** Last index sent: **11/12/2017 11:10:38 PM** Last sent index name: **etar1510504758-14505.cab.xml** Send behavior database: **True** Last behavior transfer time: **11/16/2017 4:52:49 PM** Send event-o-meter file: **True** Last event-o-meter transfer time: **11/16/2017 4:52:51 PM** Send reports: **True** Last reports transfer time:
Resend Configuration	Click ⚙ icon to retain the Behavior/Reports that were mistakenly deleted in the Collection Master. It will resend the data.  Resend Configuration ☐ Behavior data ☐ Reports files

Table 49

11.4 Adding Collection Masters

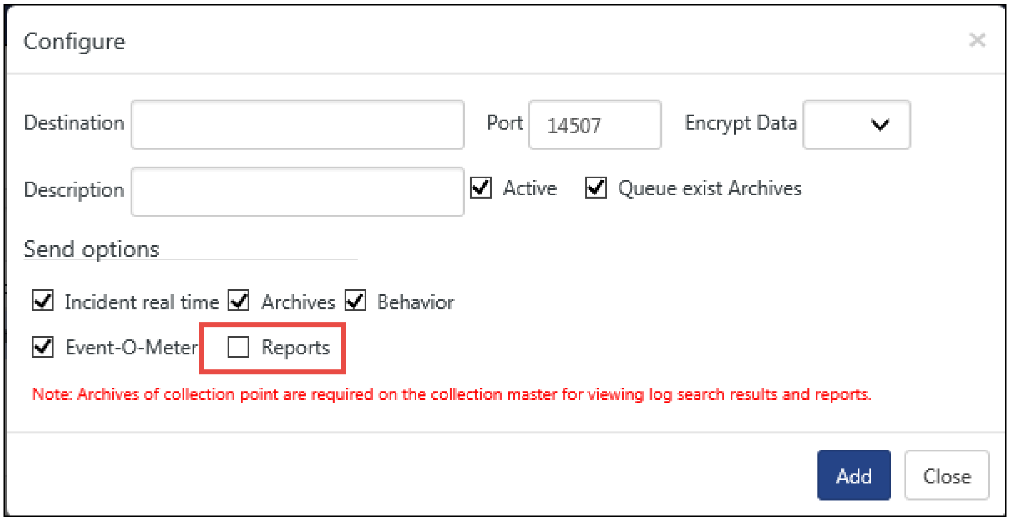
Every Collection Point can be configured to send CAB files simultaneously up to 5 Collection Masters. The Collection Master may exist in the same domain or in the trusted domain. Collection Points can be configured to send both cab files and incidents.

You can now send Reports, Behavior, Sparse matrix, Event-O-Meter events to Collection Master.

The user who is sysadmin in SQL should only change the archive path on a CM machine. Since ET admin user will not have rights to CP site data base and changing the archive path will fail.

1 To configure Collection Master, click the **Configure** tab if not selected.

2 Click **Add**.



Configure

Destination

Port 14507

Encrypt Data

Description

☑ Active ☑ Queue exist Archives

Send options

☑ Incident real time ☑ Archives ☑ Behavior

☑ Event-O-Meter □ Reports

Note: Archives of collection point are required on the collection master for viewing log search results and reports.

Figure 368

NOTE

To send CP generated reports to CM, click the checkbox Reports option as highlighted in the figure above. By default, the Reports checkbox will be disabled.

Field	Description
Configure- Configured Collection Master(s) details are displayed on this page.	
Destination	Type the name / IP address of the Collection Master.
Port	Default port is 14507. You can modify the port number. Port numbers should be same on both the Collection Master and Collection Point.
Encrypt Data	Select an appropriate option to encrypt data.
Active	By default, EventTracker selects this checkbox to activate the Collection Master. Hence the incidents and archives will be sent accordingly. **NOTE**: Collection Point will not send CAB files to the Collection Master(s) if that is Inactive.
Description	Type short description about the Collection Master.
Queue exist CABs	By default, EventTracker selects the Queue exist CABs checkbox and queues all existing CAB files. Clear this checkbox to queue only new CAB files.
Send incident real time	To forward real time incidents, enable this option.
Send Archives	To forward archive files, enable this option.
Send Reports	To forward reports to Collection Master, enable this option.

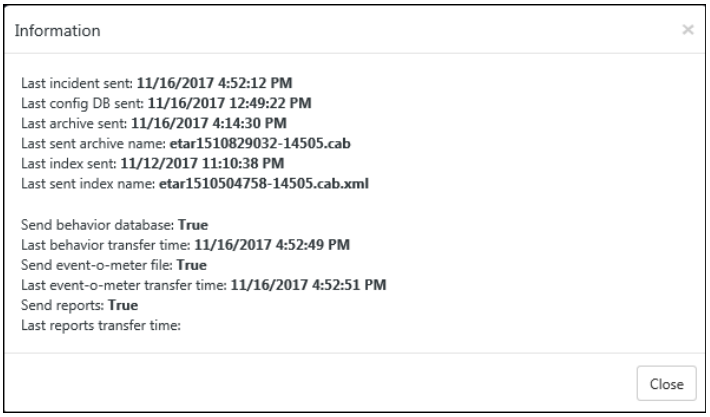
Information ⓘ	The Collection Point displays detailed information regarding last incident / archive / index sent, date and time.It also includes the CAB and XML file name. You can now send Behavior, Sparse matrix, Event-O-Meter events to Collection Point.  Information × Last incident sent: **11/16/2017 4:52:12 PM** Last config DB sent: **11/16/2017 12:49:22 PM** Last archive sent: **11/16/2017 4:14:30 PM** Last sent archive name: **etar1510829032-14505.cab** Last index sent: **11/12/2017 11:10:38 PM** Last sent index name: **etar1510504758-14505.cab.xml** Send behavior database: **True** Last behavior transfer time: **11/16/2017 4:52:49 PM** Send event-o-meter file: **True** Last event-o-meter transfer time: **11/16/2017 4:52:51 PM** Send reports: **True** Last reports transfer time: Close

Table 50

🗎 NOTE

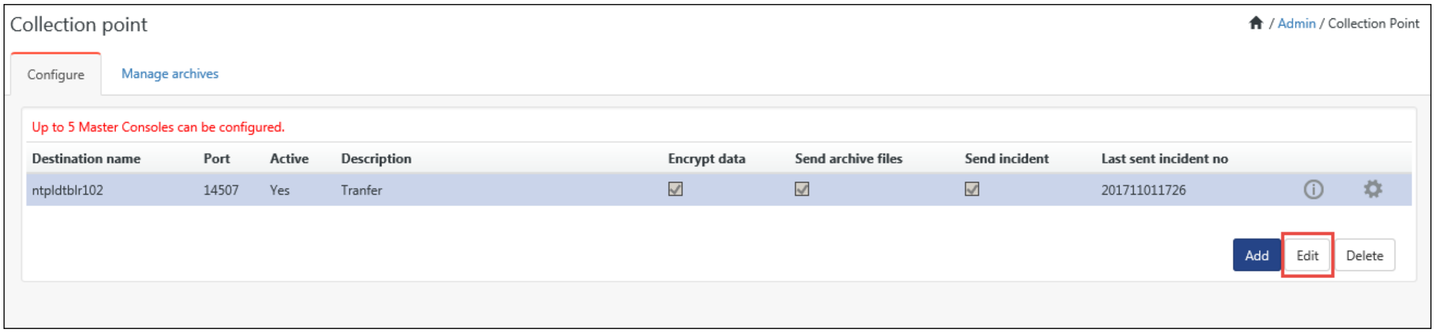
You cannot configure more than 5 Collection Masters.

3 Enter/select appropriate data in the relevant fields and then click **Save**.

11.5 Editing Collection Master Settings in Collection Point

1 To edit Collection Master settings, click **Configure** tab if not selected.

2 Select the Collection Master, and then click **Edit**.



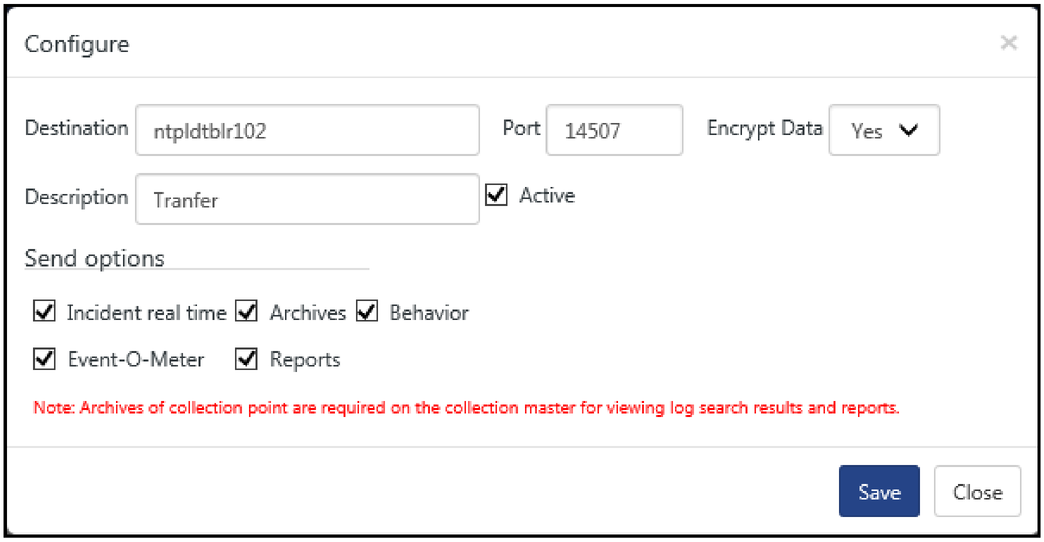
Collection point

Up to 5 Master Consoles can be configured.

Destination name	Port	Active	Description	Encrypt data	Send archive files	Send incident	Last sent incident no		
ntpldtblr102	14507	Yes	Tranfer	☑	☑	☑	201711011726	ⓘ	⚙

Figure 387

3 Enter/select appropriate changes in the relevant fields, and then click **Save**.



Configure

Destination: ntpldtblr102 Port: 14507 Encrypt Data: Yes

Description: Tranfer ☑ Active

Send options

☑ Incident real time ☑ Archives ☑ Behavior

☑ Event-O-Meter ☑ Reports

Note: Archives of collection point are required on the collection master for viewing log search results and reports.

Figure 388

🗎 NOTE

The updated Collection Point name will be shown in all places of EventTracker i.e. reports system tree, EventVault explorer system tree and Incidents Dashboard -> All Sites.

11.6 Deleting Collection Master Settings

1 Click the **Configure** tab if not selected.

2 Select the Collection Master and then click **Delete**.

EventTracker opens the confirmation pop-up window.

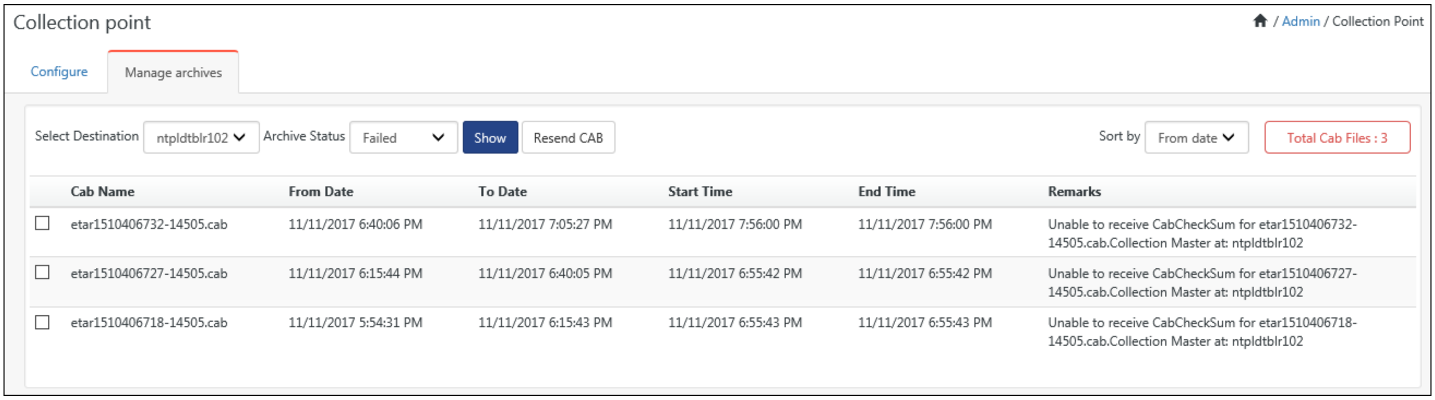
3 Click **Ok**.

EventTracker deletes the selected Collection Master Configuration settings

11.7 Managing Archives

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 archive files, click the **Manage archives** tab.



	Cab Name	From Date	To Date	Start Time	End Time	Remarks
□	etar1510406732-14505.cab	11/11/2017 6:40:06 PM	11/11/2017 7:05:27 PM	11/11/2017 7:56:00 PM	11/11/2017 7:56:00 PM	Unable to receive CabCheckSum for etar1510406732-14505.cab.Collection Master at: ntpldtblr102
□	etar1510406727-14505.cab	11/11/2017 6:15:44 PM	11/11/2017 6:40:05 PM	11/11/2017 6:55:42 PM	11/11/2017 6:55:42 PM	Unable to receive CabCheckSum for etar1510406727-14505.cab.Collection Master at: ntpldtblr102
□	etar1510406718-14505.cab	11/11/2017 5:54:31 PM	11/11/2017 6:15:43 PM	11/11/2017 6:55:43 PM	11/11/2017 6:55:43 PM	Unable to receive CabCheckSum for etar1510406718-14505.cab.Collection Master at: ntpldtblr102

Figure 389

Field	Description
Select Destination	Select Destination from the drop-down list. All configured Collection Masters are listed in this drop-down list.
Archive Status	Available options are Success, Failed, Not Sent, In Progress and Queued. Select the status of the archive files from this drop-down list and then click Show.
Resend CAB	If you wish to resend the CAB files again, click Resend CAB button.
Sort By	Sort the CAB files based on From date / To date / CAB name.

Table 51

11.8 Resending CAB Files

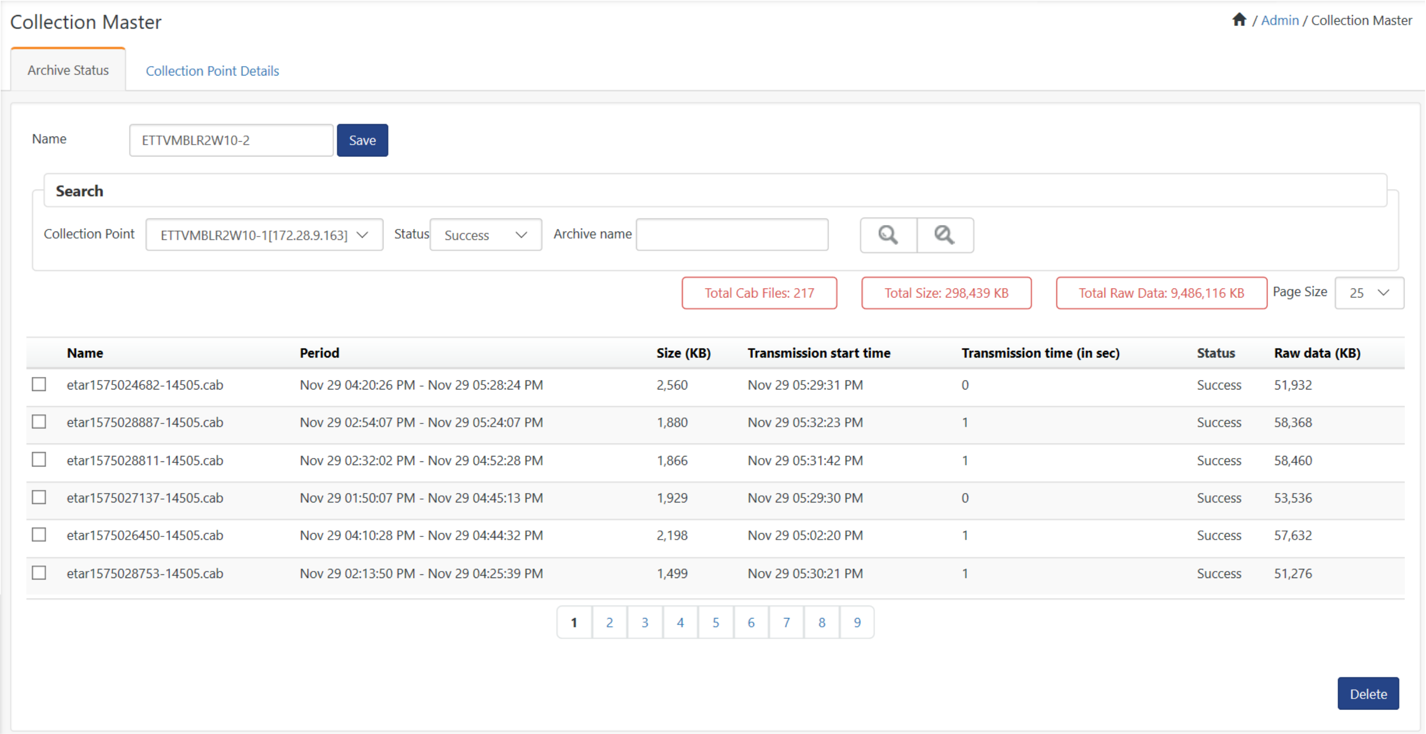
1. Select the Collection Master from the **Select Destination** drop-down list.
2. Select the status from the **Select CAB Status** drop-down list.
3. Select the required CAB files, and then select **Resend CAB**.

   Collection Point resends the CAB file(s) to the destination(s).

11.9 Collection Master

This option helps you to view Collection Master Console.

1. To access Collection Master, log on to EventTracker.
2. Click the **Admin**, and then click **Collection Master**.
   EventTracker opens the Collection Point Master page.



Name: ETTVMBLR2W10-2 Save

Search

Collection Point: ETTVMBLR2W10-1[172.28.9.163] Status: Success Archive name:

Total Cab Files: 217 Total Size: 298,439 KB Total Raw Data: 9,486,116 KB Page Size: 25

	Name	Period	Size (KB)	Transmission start time	Transmission time (in sec)	Status	Raw data (KB)
□	etar1575024682-14505.cab	Nov 29 04:20:26 PM - Nov 29 05:28:24 PM	2,560	Nov 29 05:29:31 PM	0	Success	51,932
□	etar1575028887-14505.cab	Nov 29 02:54:07 PM - Nov 29 05:24:07 PM	1,880	Nov 29 05:32:23 PM	1	Success	58,368
□	etar1575028811-14505.cab	Nov 29 02:32:02 PM - Nov 29 04:52:28 PM	1,866	Nov 29 05:31:42 PM	1	Success	58,460
□	etar1575027137-14505.cab	Nov 29 01:50:07 PM - Nov 29 04:45:13 PM	1,929	Nov 29 05:29:30 PM	0	Success	53,536
□	etar1575026450-14505.cab	Nov 29 04:10:28 PM - Nov 29 04:44:32 PM	2,198	Nov 29 05:02:20 PM	1	Success	57,632
□	etar1575028753-14505.cab	Nov 29 02:13:50 PM - Nov 29 04:25:39 PM	1,499	Nov 29 05:30:21 PM	1	Success	51,276

Figure 390

'Archives Status' tab is selected by default.

Field	Description
Name	Name of the CAB file.
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.
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.
Archive name	To search for a particular archive, enter name of the archive and then click Search 🔍. To clear the search criteria, click Clear Search 🔍.

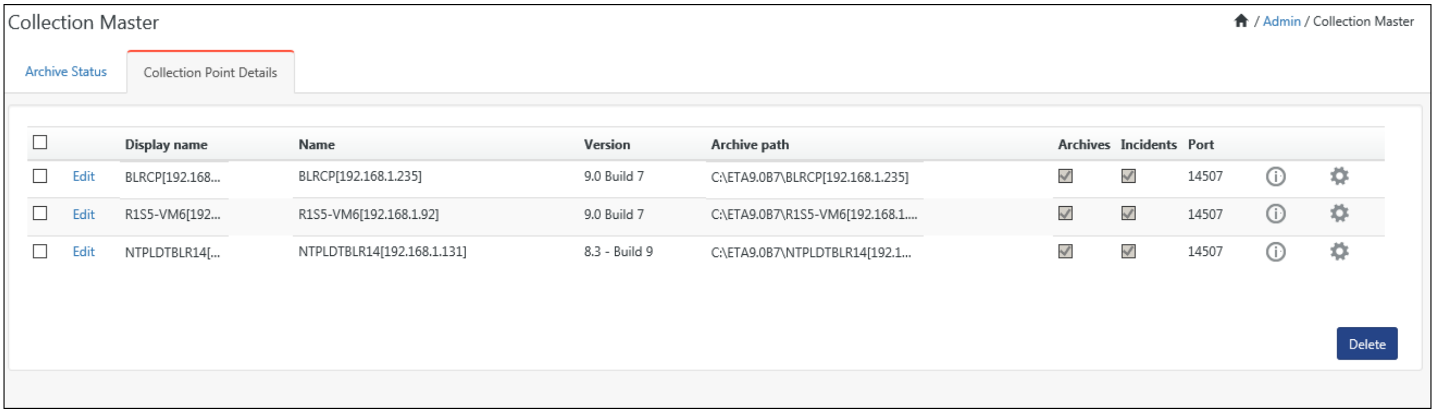
Table 52

11.10 Viewing and Editing Collection Point Details in Collection Master

This option helps you view details of the Collection Points that are forwarding CAB files to the Collection Master.

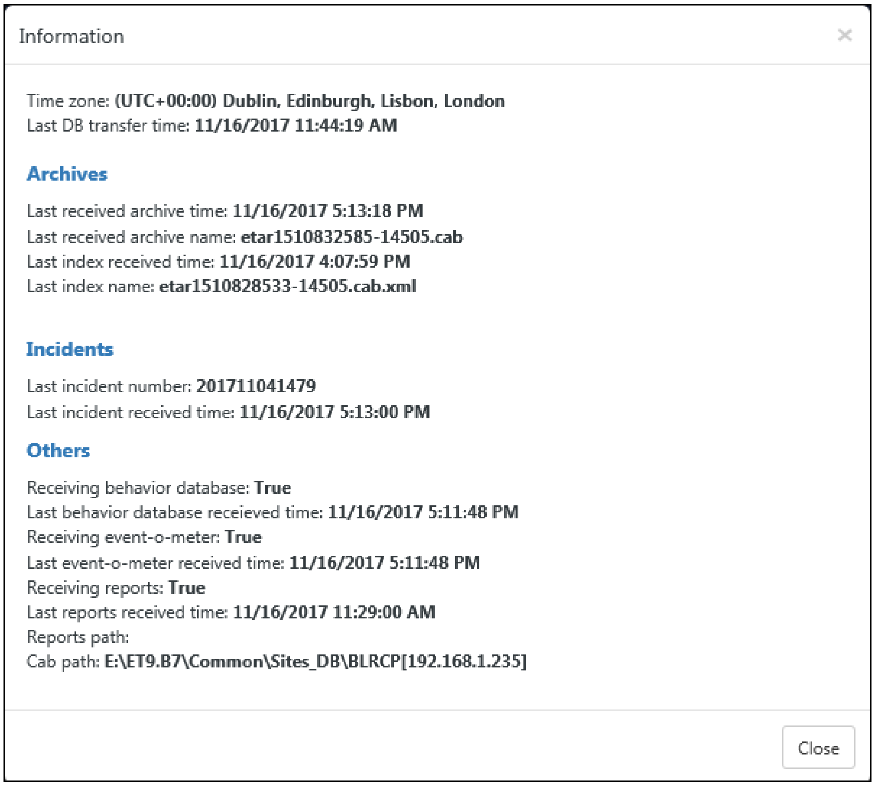
- To view Collection Point data, click the **Collection Point Details** tab.

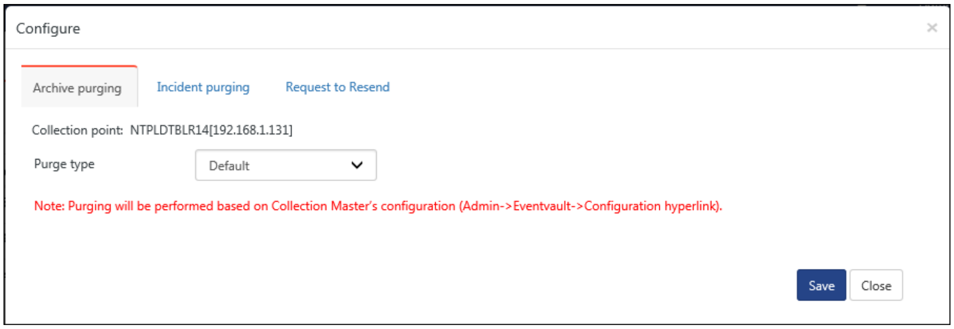
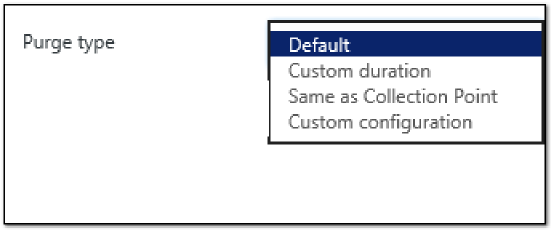
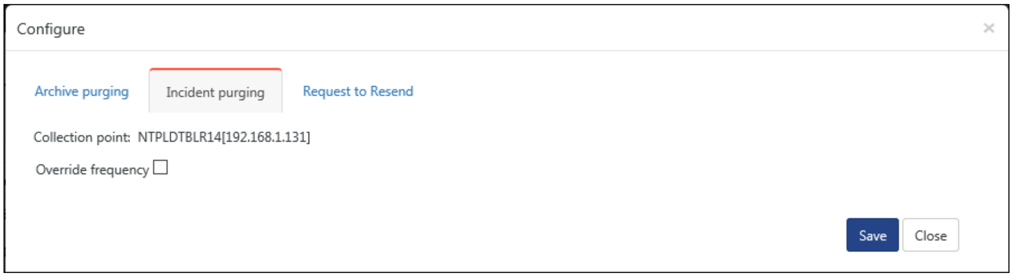
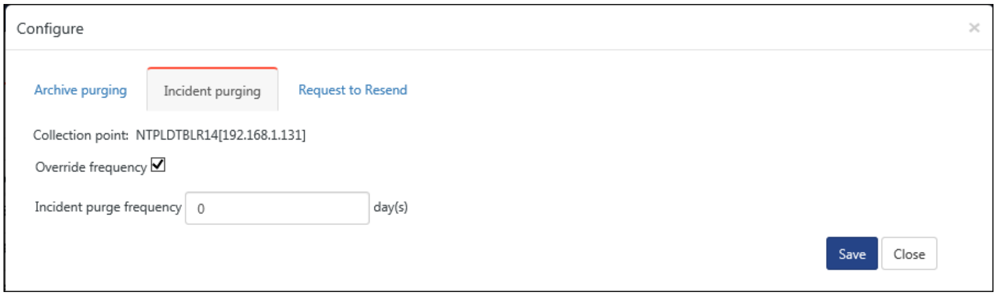
  EventTracker opens the Collection Point Details page.



□		Display name	Name	Version	Archive path	Archives	Incidents	Port		
□	Edit	BLRCP[192.168...	BLRCP[192.168.1.235]	9.0 Build 7	C:\ETA9.0B7\BLRCP[192.168.1.235]	☑	☑	14507	ⓘ	⚙
□	Edit	R1S5-VM6[192...	R1S5-VM6[192.168.1.92]	9.0 Build 7	C:\ETA9.0B7\R1S5-VM6[192.168.1....	☑	☑	14507	ⓘ	⚙
□	Edit	NTPLDTBLR14[...	NTPLDTBLR14[192.168.1.131]	8.3 - Build 9	C:\ETA9.0B7\NTPLDTBLR14[192.1...	☑	☑	14507	ⓘ	⚙

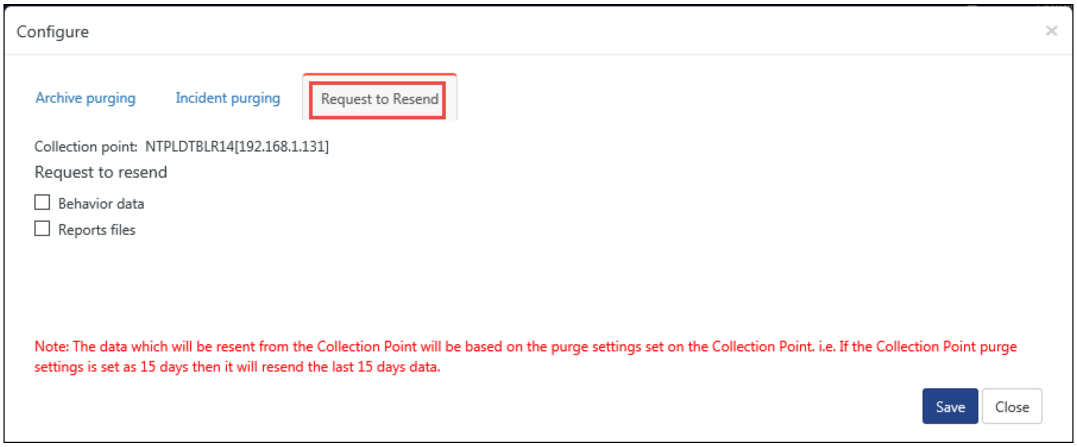
Figure 391

Field	Description
Display name	Name of the Collection Point.
Port Number	Default port is 14507. You can modify the port number. Port numbers should be same on both the Collection Master and Collection Point.
Collection Point Name	Displays the name of the Collection Points that are reporting to the Collection Master.
Version Info	Displays the version of the Collection Points.
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\NEWYORK[191.155.1.100]
Receiving Archives	This option is checked if the archives are successfully received.
Receiving Incidents	This option is checked if the incidents are successfully received.
Information ⓘ icon	Displays detailed information regarding Archives and Incidents. Refer the picture below.  Information × Time zone: **(UTC+00:00) Dublin, Edinburgh, Lisbon, London** Last DB transfer time: **11/16/2017 11:44:19 AM** **Archives** Last received archive time: **11/16/2017 5:13:18 PM** Last received archive name: **etar1510832585-14505.cab** Last index received time: **11/16/2017 4:07:59 PM** Last index name: **etar1510828533-14505.cab.xml** **Incidents** Last incident number: **201711041479** Last incident received time: **11/16/2017 5:13:00 PM** **Others** Receiving behavior database: **True** Last behavior database receieved time: **11/16/2017 5:11:48 PM** Receiving event-o-meter: **True** Last event-o-meter received time: **11/16/2017 5:11:48 PM** Receiving reports: **True** Last reports received time: **11/16/2017 11:29:00 AM** Reports path: Cab path: **E:\ET9.B7\Common\Sites_DB\BLRCP[192.168.1.235]** Close

Settings ⚙ icon	Purging of archive files and incidents sent from Collection Point to Collection Master have been implemented.  Configure × Archive purging Incident purging Request to Resend Collection point: NTPLDTBLR14[192.168.1.131] Purge type: Default Note: Purging will be performed based on Collection Master's configuration (Admin->Eventvault->Configuration hyperlink). Save Close a) Select **Archive purging** tab, and then select **Purge type:** drop down.  Purge type Default Custom duration Same as Collection Point Custom configuration b) Select **Default/Custom Duration/Same as Collection Point/Custom Configuration**, and then click **Save**.  Configure × Archive purging Incident purging Request to Resend Collection point: NTPLDTBLR14[192.168.1.131] Override frequency □ Save Close c) Select **Incident purging** tab, and then select **Override frequency**.  Configure × Archive purging Incident purging Request to Resend Collection point: NTPLDTBLR14[192.168.1.131] Override frequency ☑ Incident purge frequency: 0 day(s) Save Close

d) Enter **Incident purge frequency** in number of **day(s)**, and then click **Save**.

e) Select **Request to Resend** tab.



Configure

Collection point: NTPLDTBLR14[192.168.1.131]

Request to resend

☐ Behavior data

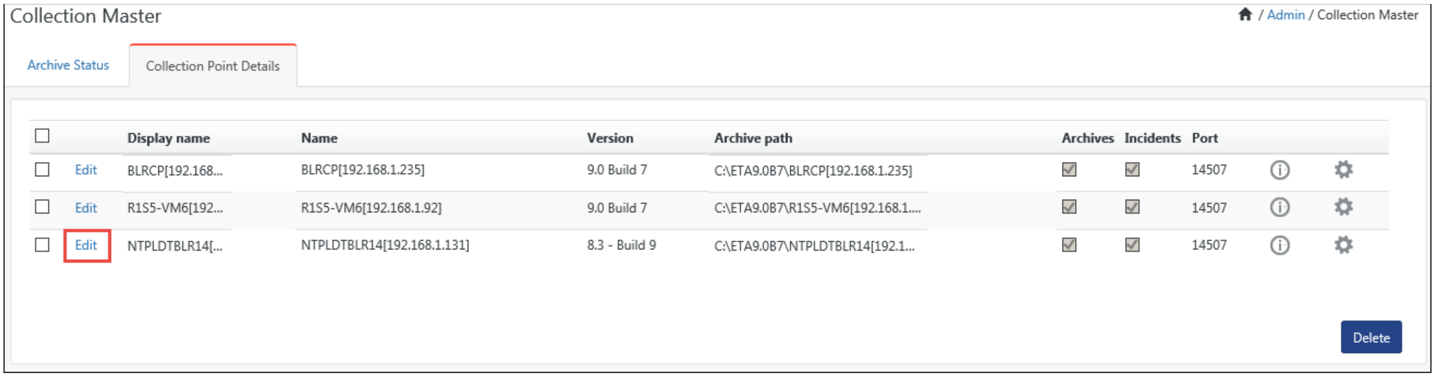
☐ Reports files

Note: The data which will be resent from the Collection Point will be based on the purge settings set on the Collection Point. i.e. If the Collection Point purge settings is set as 15 days then it will resend the last 15 days data.

Select the **Behavior data/Reports Files** to retain the Behavior/Reports that were mistakenly deleted. It will resend the data.

Table 53

- To edit Collection Point details, click **Edit** hyperlink.
- Enter a unique display name and then click **Update**.



Collection Master

☐		Display name	Name	Version	Archive path	Archives	Incidents	Port		
☐	Edit	BLRCP[192.168...	BLRCP[192.168.1.235]	9.0 Build 7	C:\ETA9.0B7\BLRCP[192.168.1.235]	☑	☑	14507	ⓘ	⚙
☐	Edit	R1S5-VM6[192...	R1S5-VM6[192.168.1.92]	9.0 Build 7	C:\ETA9.0B7\R1S5-VM6[192.168.1....	☑	☑	14507	ⓘ	⚙
☐	Edit	NTPLDTBLR14[...	NTPLDTBLR14[192.168.1.131]	8.3 - Build 9	C:\ETA9.0B7\NTPLDTBLR14[192.1...	☑	☑	14507	ⓘ	⚙

Figure 392

🗎 NOTE

The updated Collection Master name will be shown in all places of EventTracker i.e. reports system tree, EventVault explorer system tree and Incidents Dashboard -> All Sites.

11.11 Configuring 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. If you want to configure a new port other than the default one, you can update it by going to the **Admin> Manager > Collection Master Port** for successful communication between the Collection Points and Collection Master.

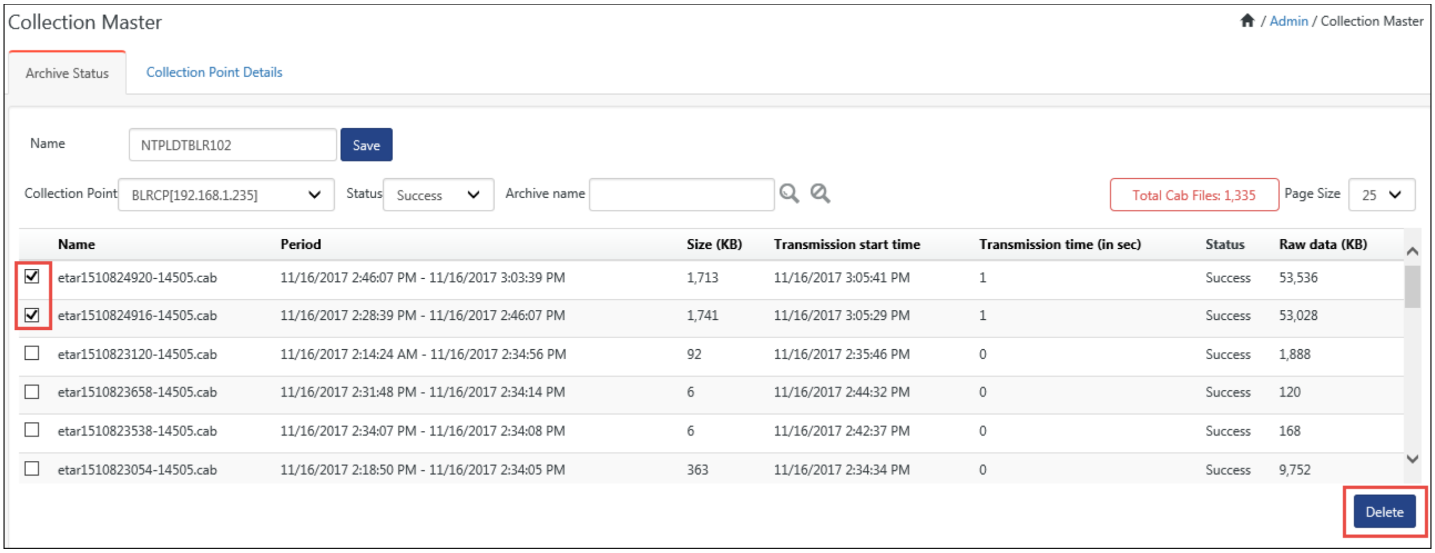
1 To configure Collection Master listening port, click the **Archive Status** tab.

2 In **Collection Master** pane, type the **Name:** and **Port No:**, and then click **Save**.

11.12 Deleting CAB Files

1 To delete CAB files, click the **Archive Status** tab.

2 Select the checkbox against the CAB files, and then click **Delete**.



Name NTPLDTBLR102 Save

Collection Point BLRCP[192.168.1.235] Status Success Archive name

	Name	Period	Size (KB)	Transmission start time	Transmission time (in sec)	Status	Raw data (KB)
☑	etar1510824920-14505.cab	11/16/2017 2:46:07 PM - 11/16/2017 3:03:39 PM	1,713	11/16/2017 3:05:41 PM	1	Success	53,536
☑	etar1510824916-14505.cab	11/16/2017 2:28:39 PM - 11/16/2017 2:46:07 PM	1,741	11/16/2017 3:05:29 PM	1	Success	53,028
□	etar1510823120-14505.cab	11/16/2017 2:14:24 AM - 11/16/2017 2:34:56 PM	92	11/16/2017 2:35:46 PM	0	Success	1,888
□	etar1510823658-14505.cab	11/16/2017 2:31:48 PM - 11/16/2017 2:34:14 PM	6	11/16/2017 2:44:32 PM	0	Success	120
□	etar1510823538-14505.cab	11/16/2017 2:34:07 PM - 11/16/2017 2:34:08 PM	6	11/16/2017 2:42:37 PM	0	Success	168
□	etar1510823054-14505.cab	11/16/2017 2:18:50 PM - 11/16/2017 2:34:05 PM	363	11/16/2017 2:34:34 PM	0	Success	9,752

Figure 393

11.13 Deleting Collection Point Details

1 To delete Collection Point data, click the **Collection Point Details** tab.

2 Select the Collection Point, and then click **Delete.**

NOTE

When you delete details of a Collection Point, EventTracker will also delete their respective CAB files. Deleting a CP will delete both cab files and incidents. To delete all CP’s, you can also select the checkbox on the title bar, and then click Delete.

12. Admin Diagnostics

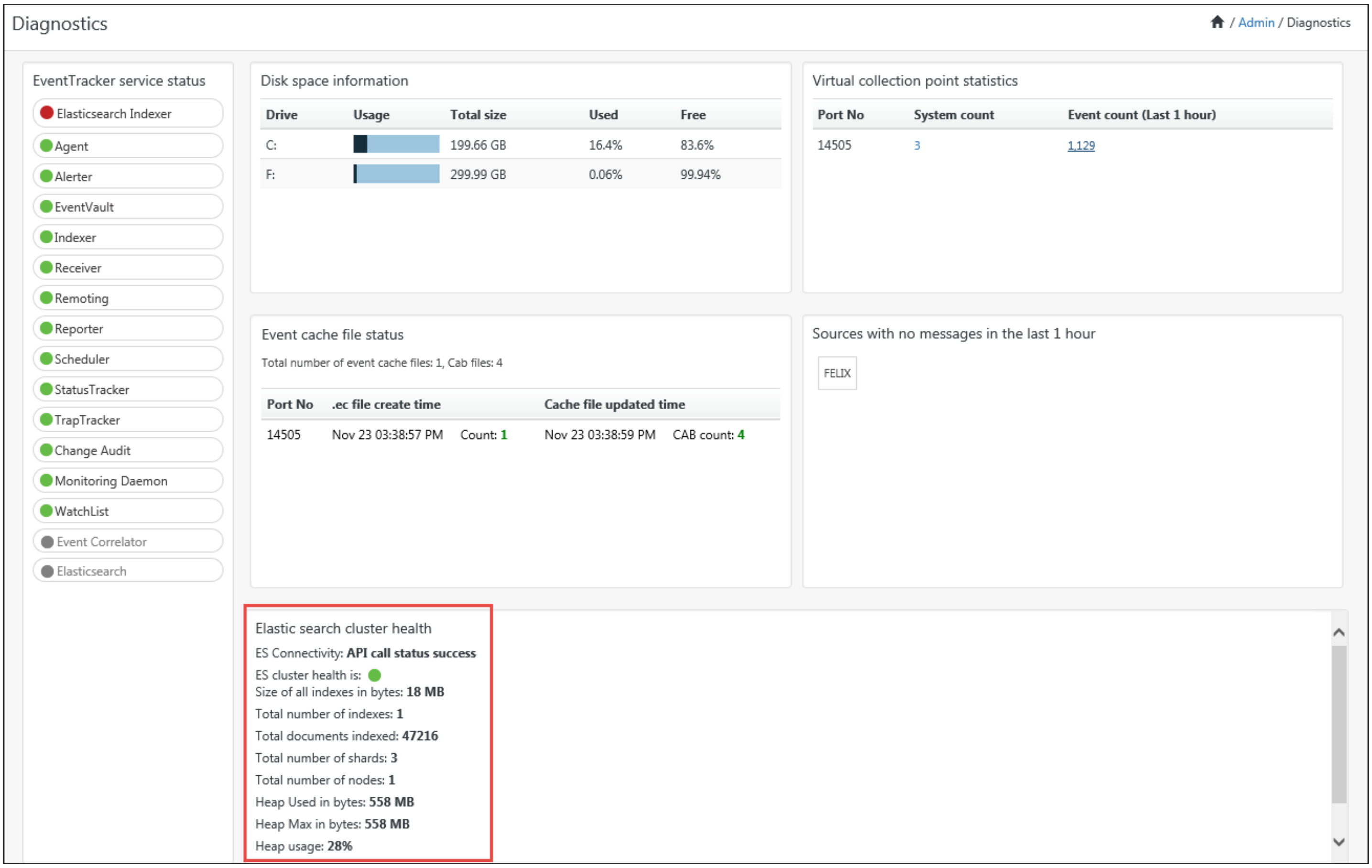
In this chapter, you will learn:

- Diagnostics

12.1 Diagnostics

Diagnostics data includes Service Status, Drive Usage, Virtual Collection Point statistics, and event cache file status.

EventTracker opens the EventTracker **Diagnostics** page.



Diagnostics

/ Admin / Diagnostics

EventTracker service status

- ● Elasticsearch Indexer
- ● Agent
- ● Alerter
- ● EventVault
- ● Indexer
- ● Receiver
- ● Remoting
- ● Reporter
- ● Scheduler
- ● StatusTracker
- ● TrapTracker
- ● Change Audit
- ● Monitoring Daemon
- ● WatchList
- ● Event Correlator
- ● Elasticsearch

Disk space information

Drive	Usage	Total size	Used	Free
C:		199.66 GB	16.4%	83.6%
F:		299.99 GB	0.06%	99.94%

Virtual collection point statistics

Port No	System count	Event count (Last 1 hour)
14505	3	1,129

Event cache file status

Total number of event cache files: 1, Cab files: 4

Port No	.ec file create time		Cache file updated time	
14505	Nov 23 03:38:57 PM	Count: 1	Nov 23 03:38:59 PM	CAB count: 4

Sources with no messages in the last 1 hour

FELIX

Elastic search cluster health

ES Connectivity: **API call status success**

ES cluster health is: ●

Size of all indexes in bytes: **18 MB**

Total number of indexes: **1**

Total documents indexed: **47216**

Total number of shards: **3**

Total number of nodes: **1**

Heap Used in bytes: **558 MB**

Heap Max in bytes: **558 MB**

Heap usage: **28%**

Figure 394

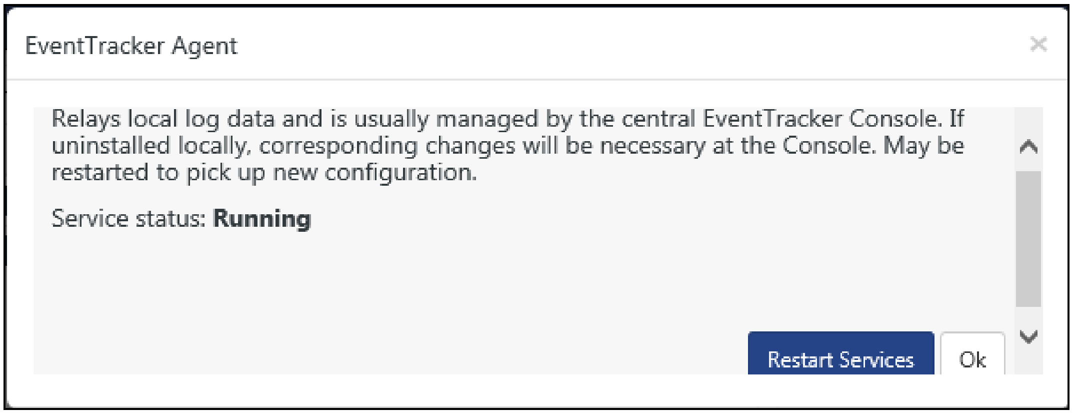
Elastic search related health information will be shown in diagnostics dashboard as highlighted in the figure above.

Icon	Represents
EventTracker service status	
🔴	Service stopped.
🟢	Service is running.
●	Service not installed.

Table 54

Move the mouse pointer over the service, EventTracker displays the status in a tooltip.

5 Click the name of the service, EventTracker opens the description of the service in a pop-up window. (Example: Agent).



EventTracker Agent

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.

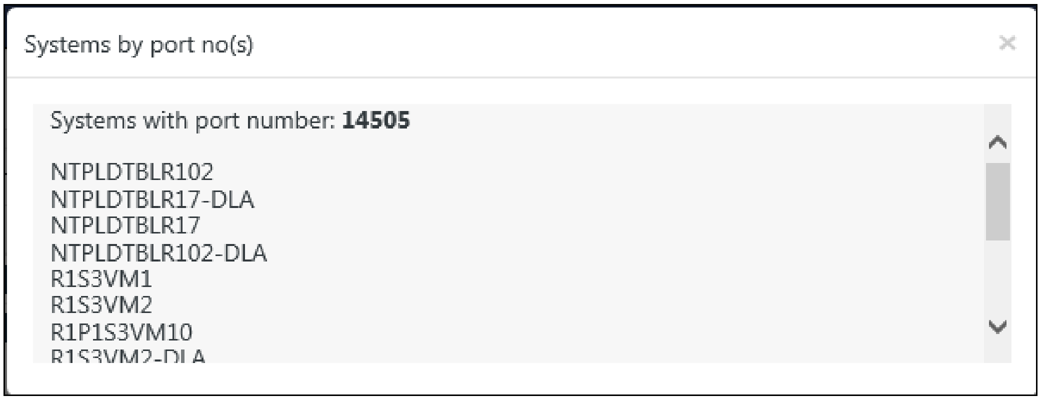
Service status: **Running**

Figure 395

6 Click on the **Restart Services** button to restart the service or click **Start Services** 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 port.

EventTracker displays the name of the systems in a pop-up window.



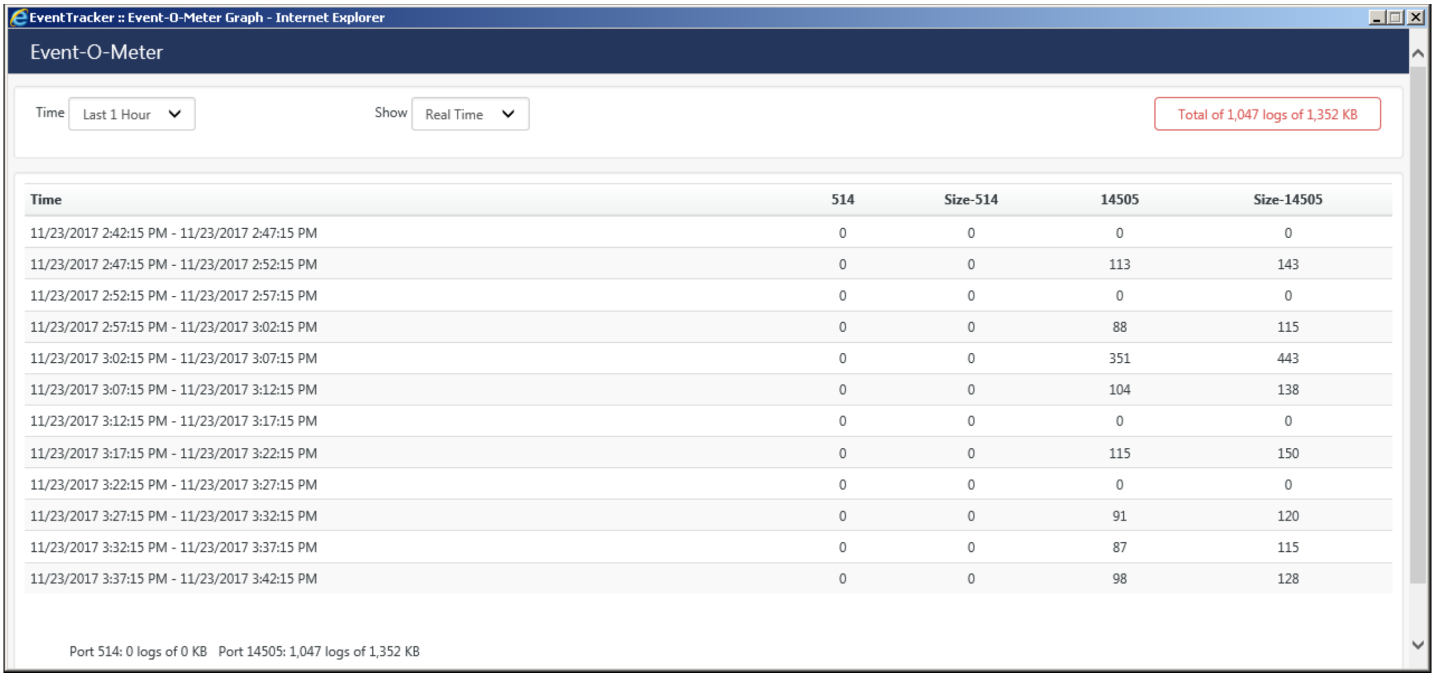
Systems by port no(s)

Systems with port number: **14505**

NTPLDTBLR102
NTPLDTBLR17-DLA
NTPLDTBLR17
NTPLDTBLR102-DLA
R1S3VM1
R1S3VM2
R1P1S3VM10
R1S3VM2-DLA

Figure 396

8 Click on the **Event Count** to get the Event-O-Meter dashboard opens.



EventTracker :: Event-O-Meter Graph - Internet Explorer

Event-O-Meter

Time: Last 1 Hour   Show: Real Time   Total of 1,047 logs of 1,352 KB

Time	514	Size-514	14505	Size-14505
11/23/2017 2:42:15 PM - 11/23/2017 2:47:15 PM	0	0	0	0
11/23/2017 2:47:15 PM - 11/23/2017 2:52:15 PM	0	0	113	143
11/23/2017 2:52:15 PM - 11/23/2017 2:57:15 PM	0	0	0	0
11/23/2017 2:57:15 PM - 11/23/2017 3:02:15 PM	0	0	88	115
11/23/2017 3:02:15 PM - 11/23/2017 3:07:15 PM	0	0	351	443
11/23/2017 3:07:15 PM - 11/23/2017 3:12:15 PM	0	0	104	138
11/23/2017 3:12:15 PM - 11/23/2017 3:17:15 PM	0	0	0	0
11/23/2017 3:17:15 PM - 11/23/2017 3:22:15 PM	0	0	115	150
11/23/2017 3:22:15 PM - 11/23/2017 3:27:15 PM	0	0	0	0
11/23/2017 3:27:15 PM - 11/23/2017 3:32:15 PM	0	0	91	120
11/23/2017 3:32:15 PM - 11/23/2017 3:37:15 PM	0	0	87	115
11/23/2017 3:37:15 PM - 11/23/2017 3:42:15 PM	0	0	98	128

Port 514: 0 logs of 0 KB   Port 14505: 1,047 logs of 1,352 KB

Figure 397

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.

13. Event Filters

In this chapter, you will learn how to:

- Configuring Event Filters
- Configuring Event Filters with exception

13.1 Filtering 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.

13.2 Event Filter (Global/Receiver/Archiver filter)

EventTracker now adds the option to configure filters for Global, Archiver and Receiver in **Admin -> Event Filters**.

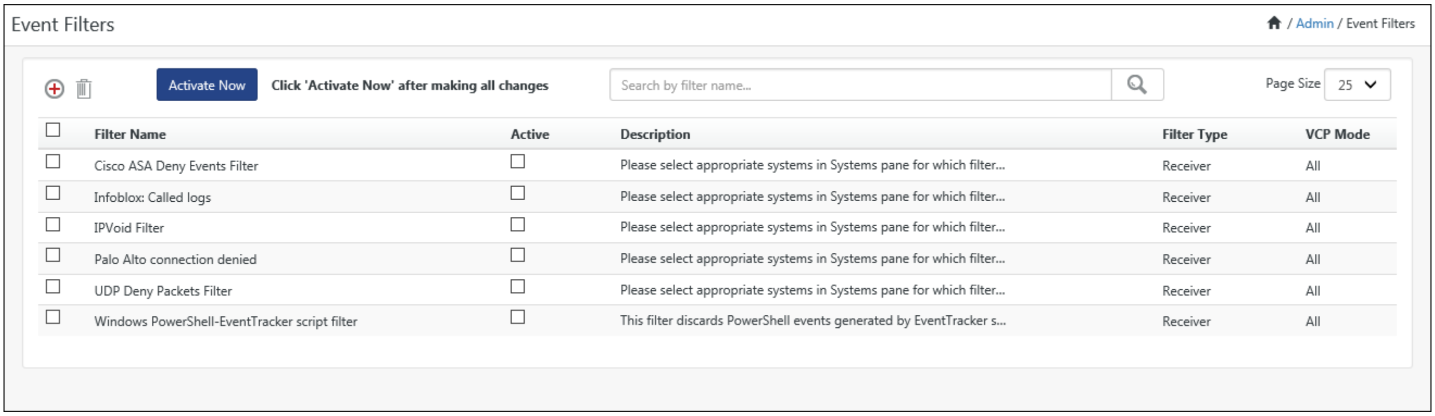
How it will benefit the user?

- All the configured filter events will now be dropped, which in turn will minimize the archive database storage.
- The user can now filter both real time and offline events using the filter types:
  - **Global**
  - **Archive**
- The feature will also filter out the real time events after alerting has been performed **(Selecting Archive** as **Filter type).**
- The user will also be able to configure a filter by selecting specific systems/ groups and specific VCP ports.

How it Works?

Configuring Event Filters

1. Click the **Admin** and select **Event filters** option.



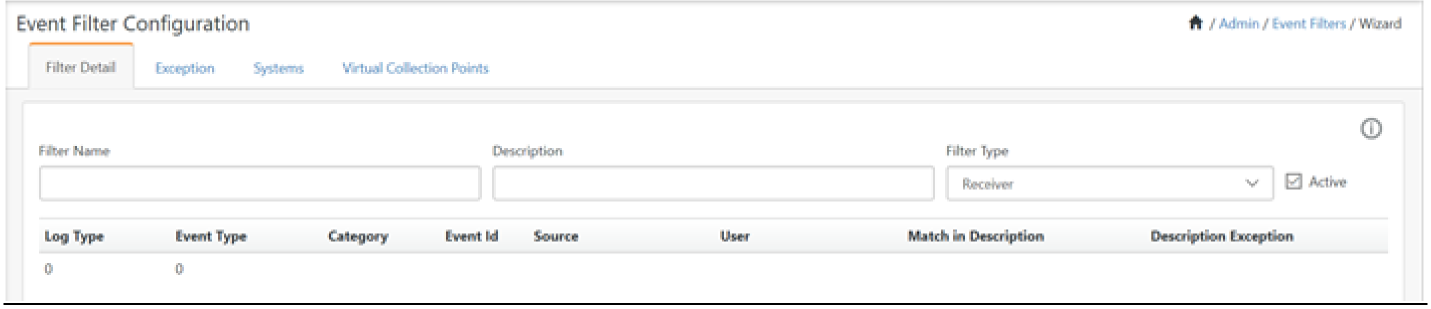
Event Filters

🏠 / Admin / Event Filters

□	Filter Name	Active	Description	Filter Type	VCP Mode
□	Cisco ASA Deny Events Filter	□	Please select appropriate systems in Systems pane for which filter...	Receiver	All
□	Infoblox: Called logs	□	Please select appropriate systems in Systems pane for which filter...	Receiver	All
□	IPVoid Filter	□	Please select appropriate systems in Systems pane for which filter...	Receiver	All
□	Palo Alto connection denied	□	Please select appropriate systems in Systems pane for which filter...	Receiver	All
□	UDP Deny Packets Filter	□	Please select appropriate systems in Systems pane for which filter...	Receiver	All
□	Windows PowerShell-EventTracker script filter	□	This filter discards PowerShell events generated by EventTracker s...	Receiver	All

Figure 398

2. Click Add new ⊕ .
   EventTracker open the Event Filter configuration page.



Event Filter Configuration

🏠 / Admin / Event Filters / Wizard

Filter Name

Description

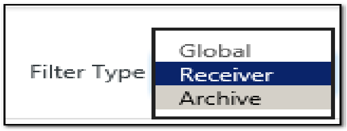
Filter Type: Receiver

☑ Active

Log Type	Event Type	Category	Event Id	Source	User	Match in Description	Description Exception
0	0						

Figure 399

3. Enter the name of the filter in the **Filter Name** field and a brief description in the Description field. Example: **All error Events with Event ID**
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 the **Filter Type** field, select **Global**/**Receiver**/**Archive** from the drop-down list. By default, it will select “**Receiver**”.



Filter Type

Global
Receiver
Archive

Figure 400

6. Click **Information** ⓘ to know more about the filter type options.
7. In Event Filter Configuration page, click **Add**.
8. In Add Event dialog box, enter appropriate data in the relevant fields.

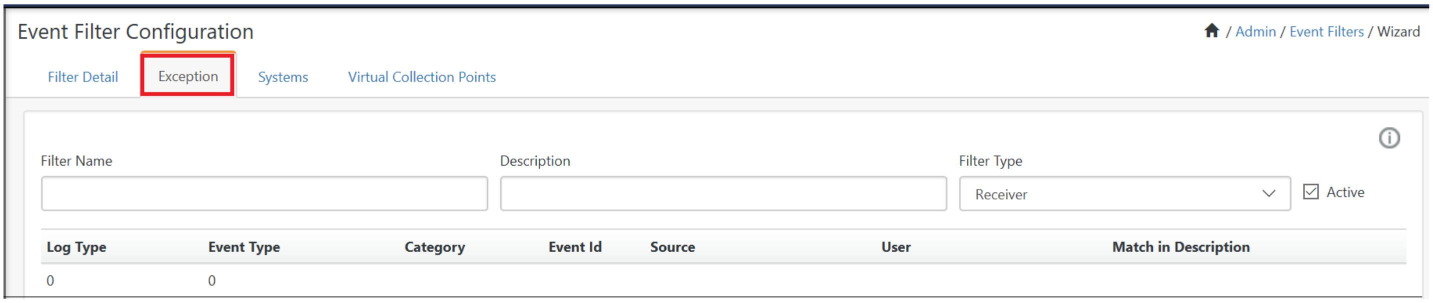
🗎 NOTE

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.

9. After adding relevant data, click **Add**.

   EventTracker opens the '**Event Filter Configuration'** page with newly added filter details.

10. Click the **Exception** tab.



Event Filter Configuration

Filter Name:
Description:
Filter Type: Receiver
☑ Active

Log Type	Event Type	Category	Event Id	Source	User	Match in Description
0	0					

Figure 401

11. Click **Add** to add exception criteria.
12. Enter/select appropriately in the relevant fields, and then click **Add**.

🗎 NOTE

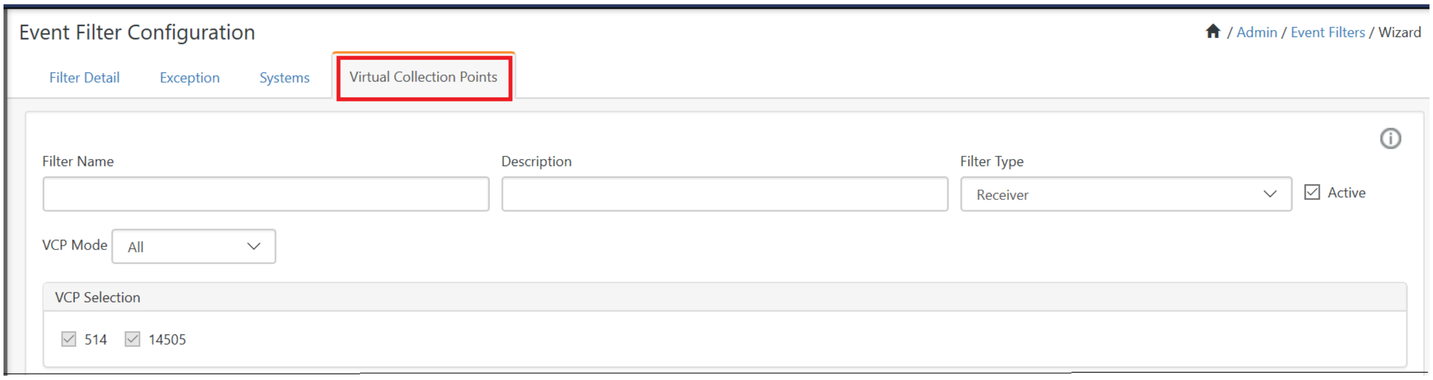
For example, if you wish to filter out all events of Event Type- Information but interested in monitoring a event for example – Event ID 3223. Then in this case, all events of 'Information' event type will be ignored except the event id 3223.

13. Click the **Systems** tab.

    All Systems option is selected by default, which means the filter is applied to all the monitored systems.

14. Select required system groups / systems to apply the filter.

15. Click the **Virtual Collection Points** tab.



Event Filter Configuration

/ Admin / Event Filters / Wizard

Filter Detail | Exception | Systems | Virtual Collection Points

Filter Name

Description

Filter Type: Receiver

☑ Active

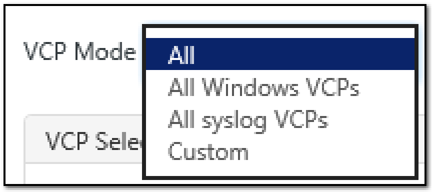
VCP Mode: All

VCP Selection

☑ 514 ☑ 14505

Figure 402

16. In the **VCP Mode** field, select any option from the dropdown list.

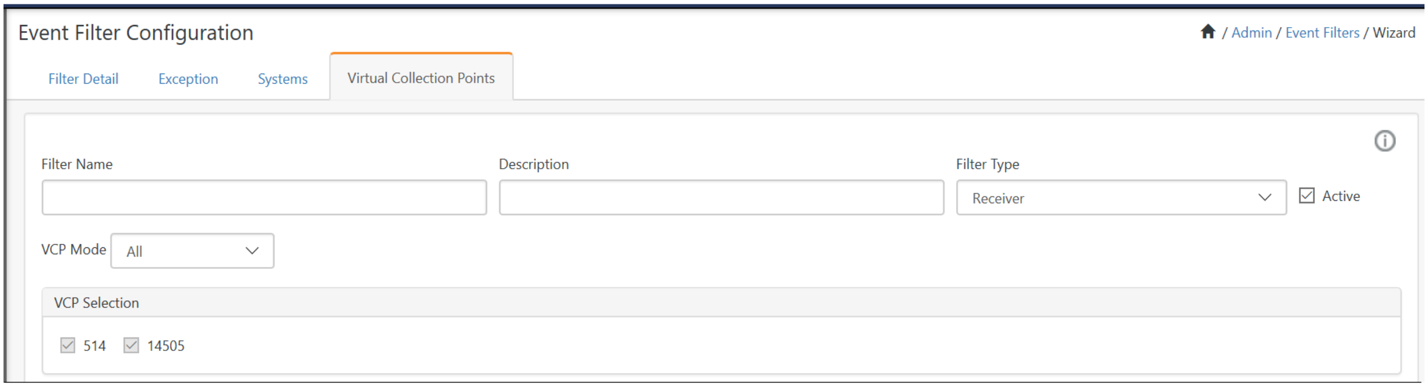


VCP Mode

Figure 403

NOTE: By default, "**All**" option is selected. On selecting "**Custom**" the user will be allowed to select one or more VCPs from a list of available/configured VCPs.

- VCP Mode: "**All**" will consider both the windows and syslog VCPs for filtering.



Event Filter Configuration

/ Admin / Event Filters / Wizard

Filter Detail | Exception | Systems | Virtual Collection Points

Filter Name

Description

Filter Type: Receiver

☑ Active

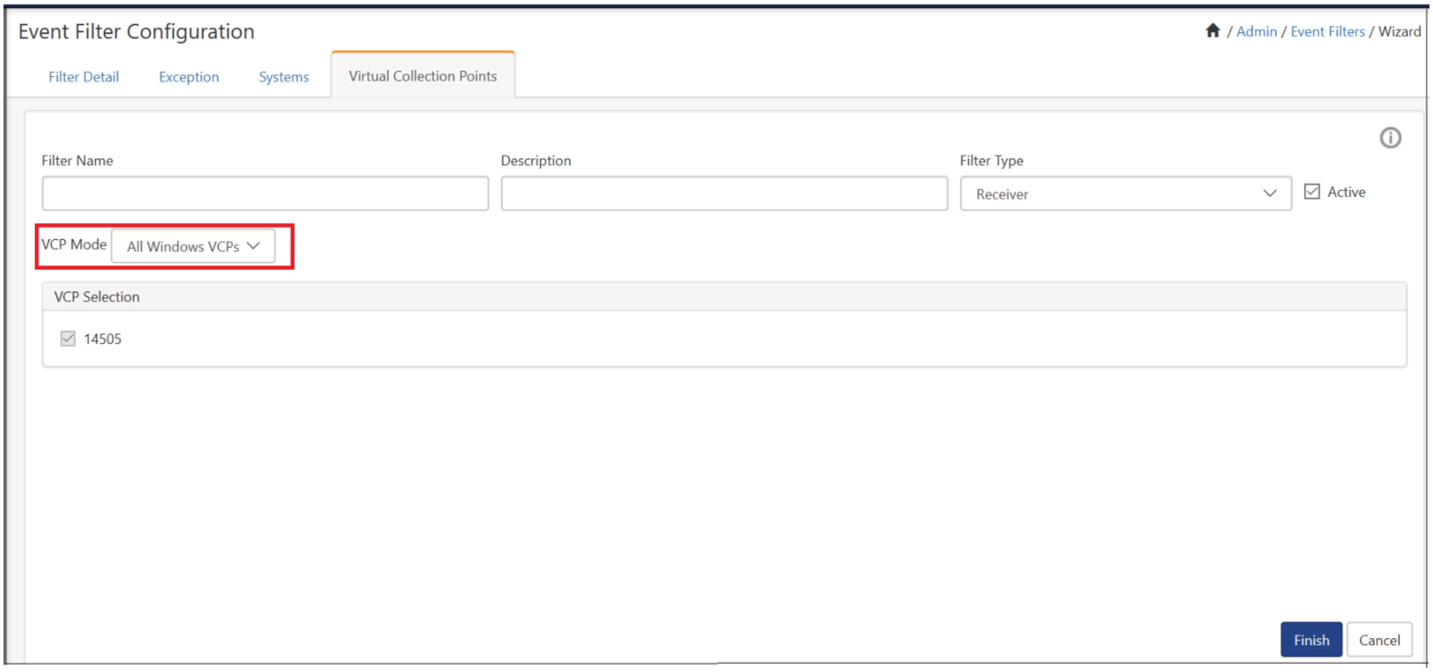
VCP Mode: All

VCP Selection

☑ 514 ☑ 14505

Figure 404

- VCP Mode: "**All Windows VCPs**" will consider only the windows related VCPs for filtering.



Event Filter Configuration

Filter Name:

Description:

Filter Type: Receiver

☑ Active

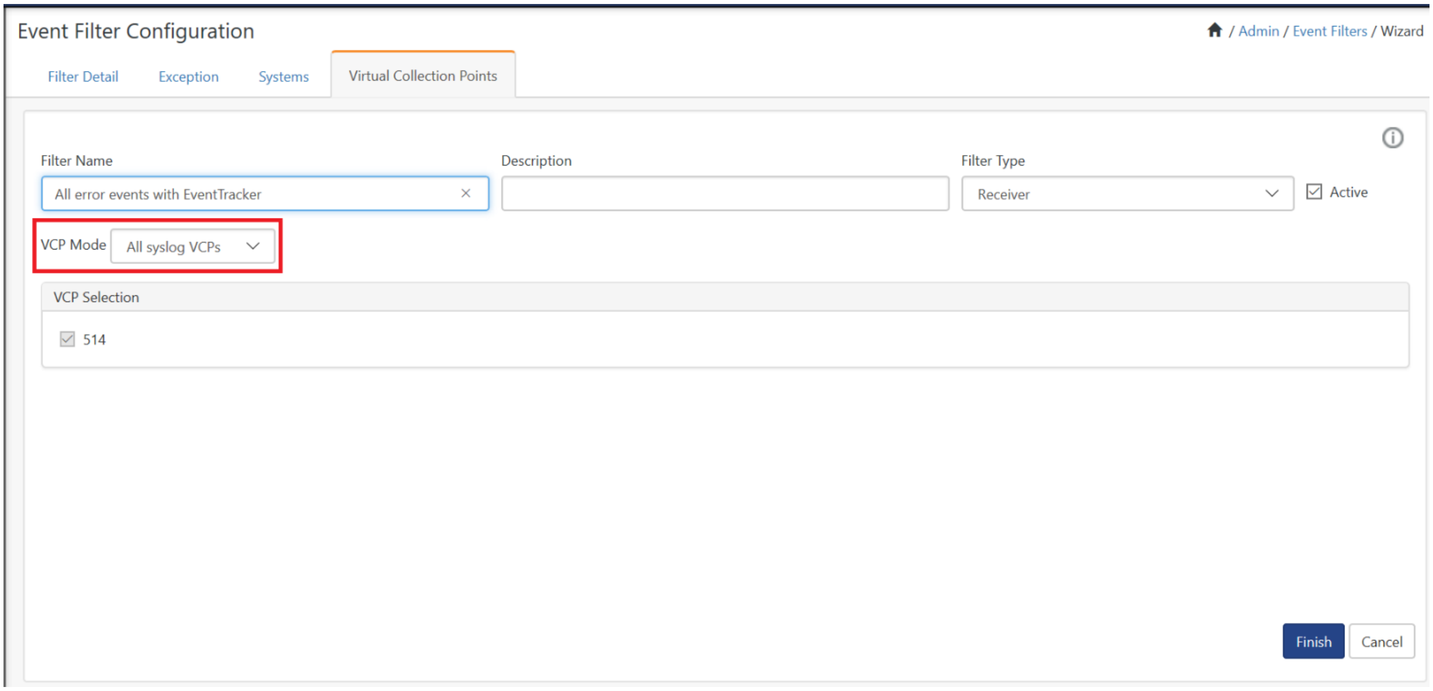
VCP Mode: All Windows VCPs

VCP Selection

☑ 14505

Figure 405

- VCP Mode: “**All syslog VCPs**” will consider all the syslog related VCPs for filtering.



Event Filter Configuration

Filter Name: All error events with EventTracker

Description:

Filter Type: Receiver

☑ Active

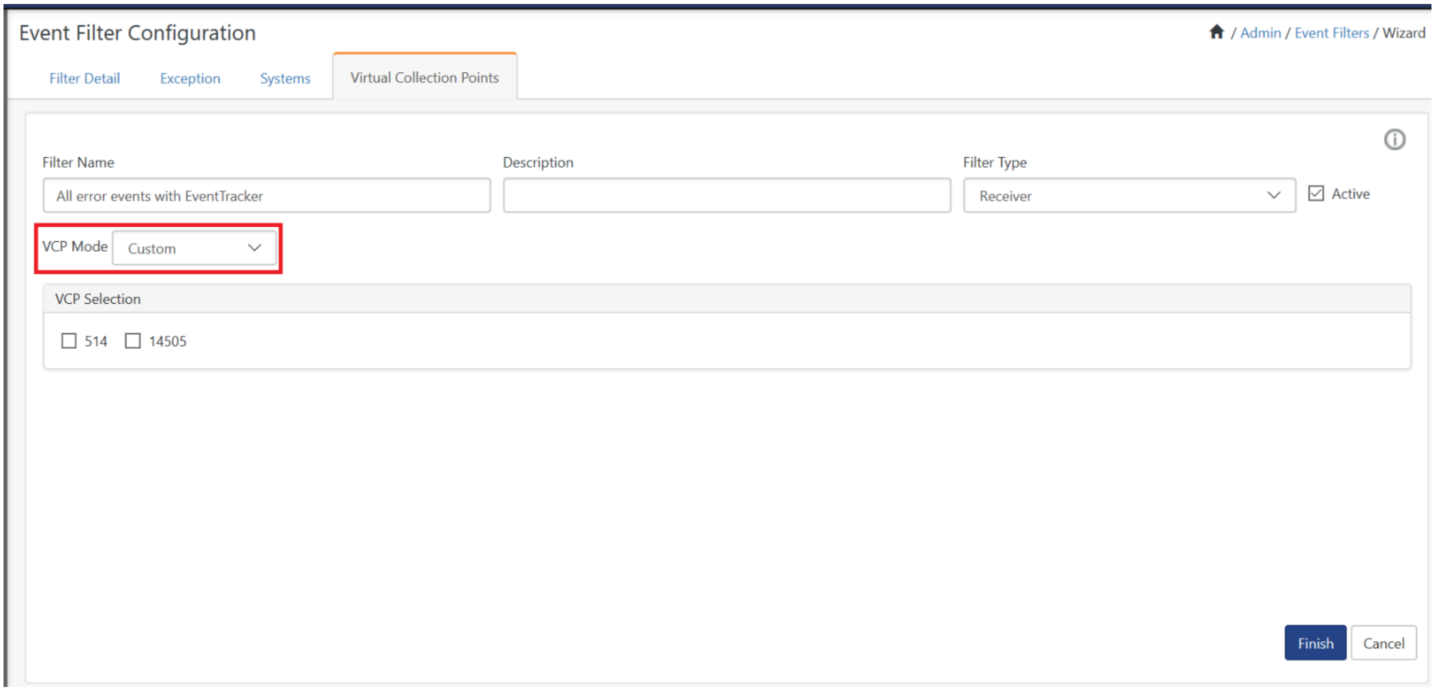
VCP Mode: All syslog VCPs

VCP Selection

☑ 514

Figure 406

- VCP Mode: “**Custom** “will list all the configured VCPs and based on the user selection, ports will be considered for filtering.



Event Filter Configuration

/ Admin / Event Filters / Wizard

Filter Name: All error events with EventTracker

Description:

Filter Type: Receiver

☑ Active

VCP Mode: Custom

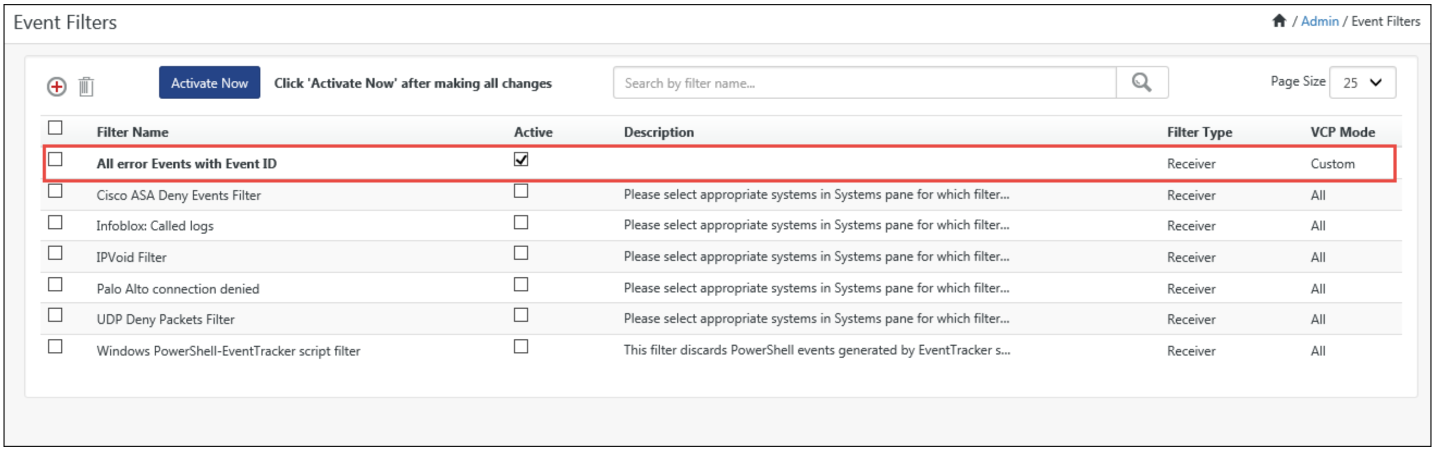
VCP Selection

☐ 514 ☐ 14505

Figure 407

17. Click **Finish** to save the changes.

    The Filter name will get listed in the Event filter page.



Event Filters

/ Admin / Event Filters

☐	Filter Name	Active	Description	Filter Type	VCP Mode
☐	All error Events with Event ID	☑		Receiver	Custom
☐	Cisco ASA Deny Events Filter	☐	Please select appropriate systems in Systems pane for which filter...	Receiver	All
☐	Infoblox: Called logs	☐	Please select appropriate systems in Systems pane for which filter...	Receiver	All
☐	IPVoid Filter	☐	Please select appropriate systems in Systems pane for which filter...	Receiver	All
☐	Palo Alto connection denied	☐	Please select appropriate systems in Systems pane for which filter...	Receiver	All
☐	UDP Deny Packets Filter	☐	Please select appropriate systems in Systems pane for which filter...	Receiver	All
☐	Windows PowerShell-EventTracker script filter	☐	This filter discards PowerShell events generated by EventTracker s...	Receiver	All

Figure 408

- Now, click "**Activate now**" to activate the event filter.

13.2.1 Understanding 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 **Delete**.

EventTracker opens the confirmation message box.

3 Click **OK** to remove the filter details.

EventTracker removes the filter details.

4 Click the **Exception** tab.

The filter exception you have set earlier remains unaltered.

5 Select the exception rule to be deleted, and then click **Delete**.

EventTracker opens 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.

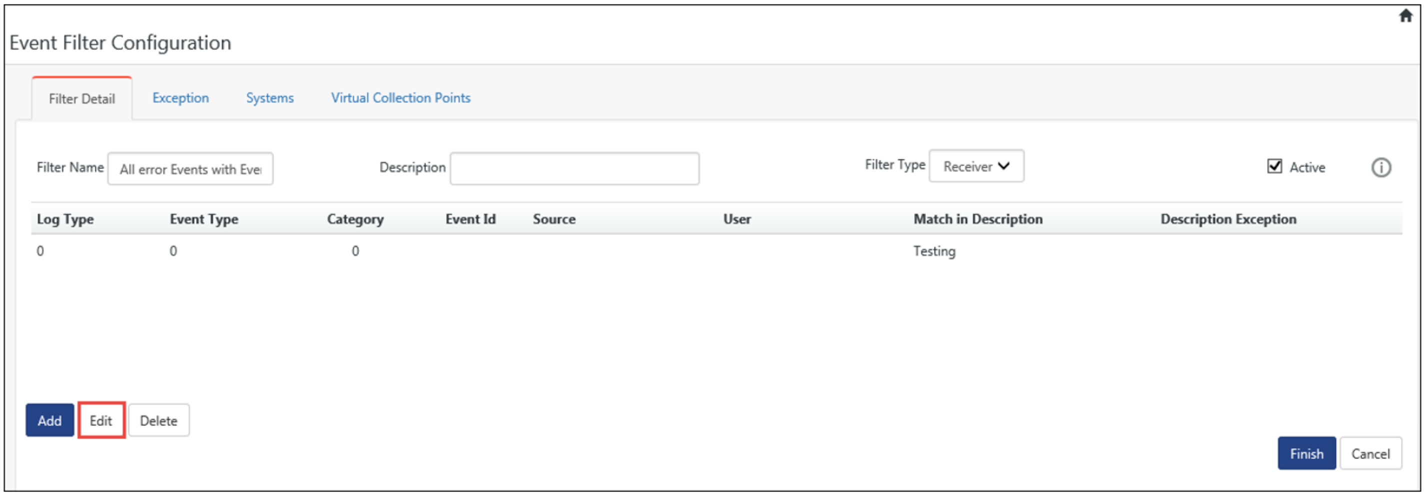
Filter	Exception	Result
Y	N	EventTracker filters all events from the view.
N	Y	EventTracker allows all events.
Y	Y	EventTracker allows events with exception.
N	N	EventTracker allows all events.

Table 55

13.3 Viewing and Editing Alert Details

For viewing and editing filter details,

1. Go to **Admin**
2. Click the **Event Filters** option from the menu.
3. Click on the filter you want to view and edit.
4. Click **Edit** to modify the filter configuration.



Event Filter Configuration

Filter Name: All error Events with Eve
Description:
Filter Type: Receiver
☑ Active

Log Type	Event Type	Category	Event Id	Source	User	Match in Description	Description Exception
0	0	0				Testing	

Figure 409

5. Click **Finish**, once you complete viewing and editing the filter.

14. EventVault

In this chapter, you will learn how to use:

- EventVault Manager
- Verifying Archive Files
- Exporting Archive Files

14.1 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.

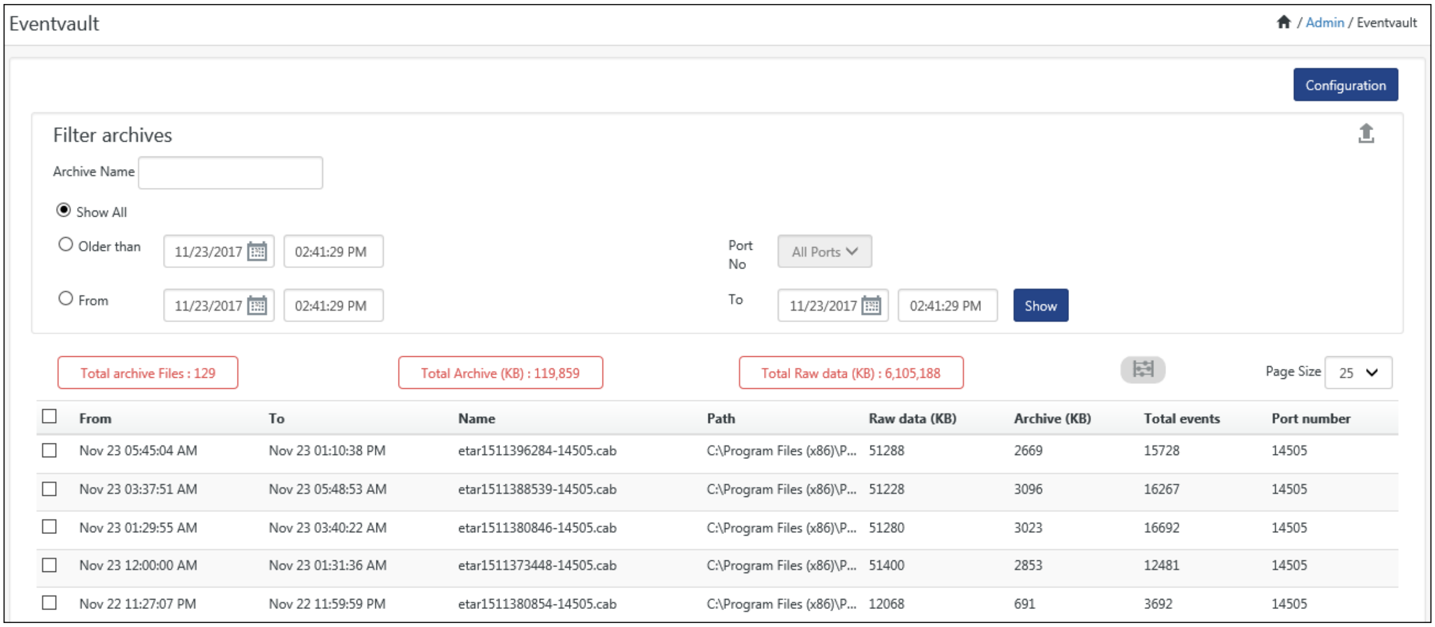
In most enterprise networks with multiple critical servers and workstations, the event log data can become huge and unmanageable. Those event data may not be immediately required once the initial analysis is completed. At the same time, they cannot be completely discarded, as they will be required for 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.

14.1.1 Starting EventVault Manager

1. Click the **Admin**, and then select **EventVault**.

   EventTracker opens the **EventVault Manager** screen.



Archive Name

● Show All

○ Older than 11/23/2017 02:41:29 PM Port No All Ports

○ From 11/23/2017 02:41:29 PM To 11/23/2017 02:41:29 PM

Total archive Files : 129

Total Archive (KB) : 119,859

Total Raw data (KB) : 6,105,188

Page Size 25

□	From	To	Name	Path	Raw data (KB)	Archive (KB)	Total events	Port number
□	Nov 23 05:45:04 AM	Nov 23 01:10:38 PM	etar1511396284-14505.cab	C:\Program Files (x86)\P...	51288	2669	15728	14505
□	Nov 23 03:37:51 AM	Nov 23 05:48:53 AM	etar1511388539-14505.cab	C:\Program Files (x86)\P...	51228	3096	16267	14505
□	Nov 23 01:29:55 AM	Nov 23 03:40:22 AM	etar1511380846-14505.cab	C:\Program Files (x86)\P...	51280	3023	16692	14505
□	Nov 23 12:00:00 AM	Nov 23 01:31:36 AM	etar1511373448-14505.cab	C:\Program Files (x86)\P...	51400	2853	12481	14505
□	Nov 22 11:27:07 PM	Nov 22 11:59:59 PM	etar1511380854-14505.cab	C:\Program Files (x86)\P...	12068	691	3692	14505

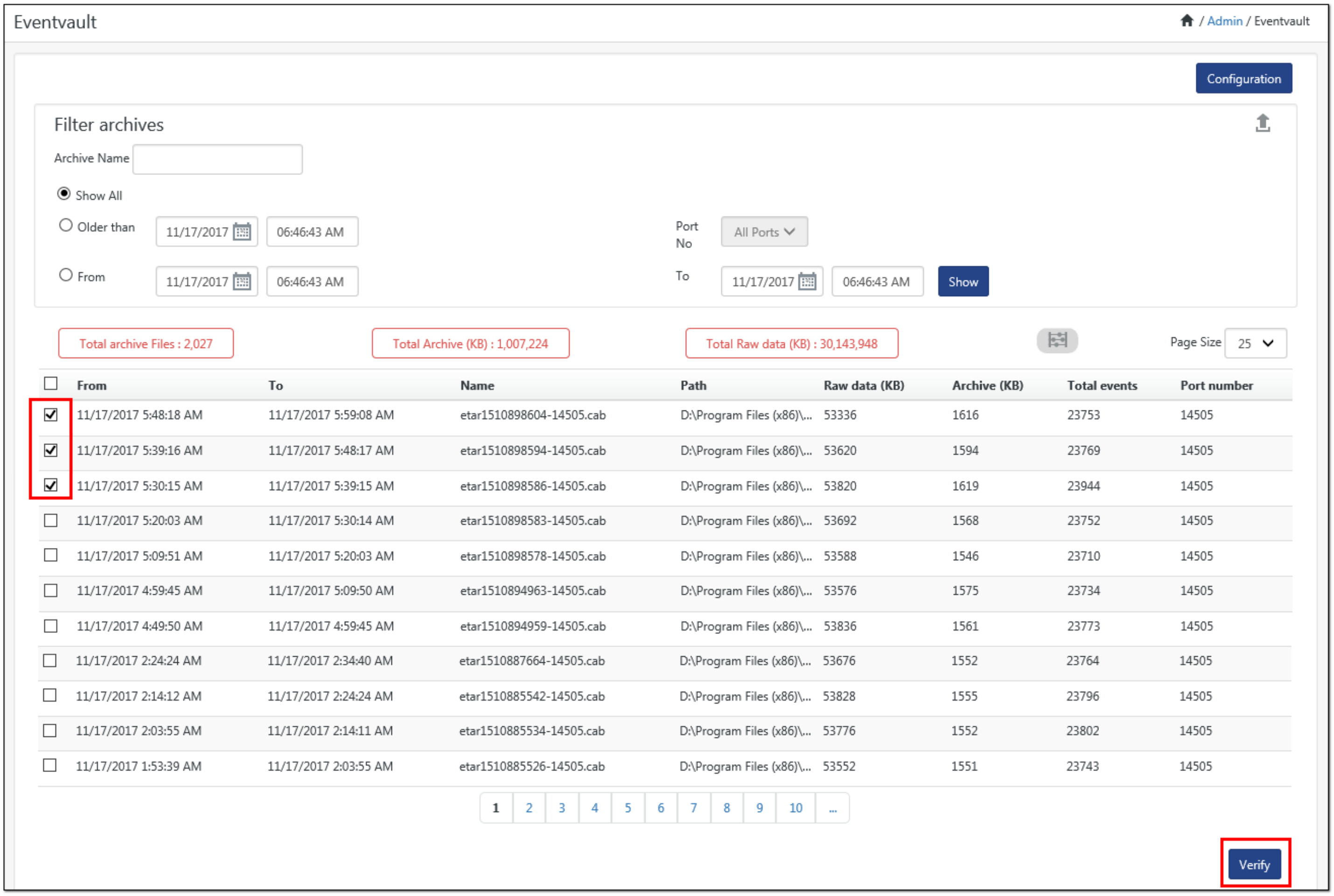
Figure 410

Click	To
Configuration	Configure EventVault Manager to archive the events from EventTracker database.
Verify	Verify the integrity of selected EventBoxes.
Show	View the CAB files for a specific period.
From	Date & Time of the first event stored in the CAB file.
To	Date & Time of the last event stored in the CAB file.
Archive Name	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
Path	Path of the folder where the archives are stored typically, EventTracker install path\ port number \ year \ month.
Size (KB)	Size of the CAB file in KB.
Total Events	Total number of events accommodated in the CAB file.
Port Number	Port number through which the EventTracker Receiver service received events.
Raw data	Display size of that particular raw data available.
Archives	Display size of that particular archive.

Table 56

14.2 Verifying Archive File(s)

1. To verify the archive files, select any Archive file option and then click **Verify**.



Eventvault

Filter archives

Archive Name

● Show All

○ Older than 11/17/2017 06:46:43 AM

Port No All Ports

○ From 11/17/2017 06:46:43 AM

To 11/17/2017 06:46:43 AM

Total archive Files : 2,027

Total Archive (KB) : 1,007,224

Total Raw data (KB) : 30,143,948

Page Size 25

□	From	To	Name	Path	Raw data (KB)	Archive (KB)	Total events	Port number
☑	11/17/2017 5:48:18 AM	11/17/2017 5:59:08 AM	etar1510898604-14505.cab	D:\Program Files (x86)\...	53336	1616	23753	14505
☑	11/17/2017 5:39:16 AM	11/17/2017 5:48:17 AM	etar1510898594-14505.cab	D:\Program Files (x86)\...	53620	1594	23769	14505
☑	11/17/2017 5:30:15 AM	11/17/2017 5:39:15 AM	etar1510898586-14505.cab	D:\Program Files (x86)\...	53820	1619	23944	14505
□	11/17/2017 5:20:03 AM	11/17/2017 5:30:14 AM	etar1510898583-14505.cab	D:\Program Files (x86)\...	53692	1568	23752	14505
□	11/17/2017 5:09:51 AM	11/17/2017 5:20:03 AM	etar1510898578-14505.cab	D:\Program Files (x86)\...	53588	1546	23710	14505
□	11/17/2017 4:59:45 AM	11/17/2017 5:09:50 AM	etar1510894963-14505.cab	D:\Program Files (x86)\...	53576	1575	23734	14505
□	11/17/2017 4:49:50 AM	11/17/2017 4:59:45 AM	etar1510894959-14505.cab	D:\Program Files (x86)\...	53836	1561	23773	14505
□	11/17/2017 2:24:24 AM	11/17/2017 2:34:40 AM	etar1510887664-14505.cab	D:\Program Files (x86)\...	53676	1552	23764	14505
□	11/17/2017 2:14:12 AM	11/17/2017 2:24:24 AM	etar1510885542-14505.cab	D:\Program Files (x86)\...	53828	1555	23796	14505
□	11/17/2017 2:03:55 AM	11/17/2017 2:14:11 AM	etar1510885534-14505.cab	D:\Program Files (x86)\...	53776	1552	23802	14505
□	11/17/2017 1:53:39 AM	11/17/2017 2:03:55 AM	etar1510885526-14505.cab	D:\Program Files (x86)\...	53552	1551	23743	14505

Figure 411

The data is downloaded in a text file.

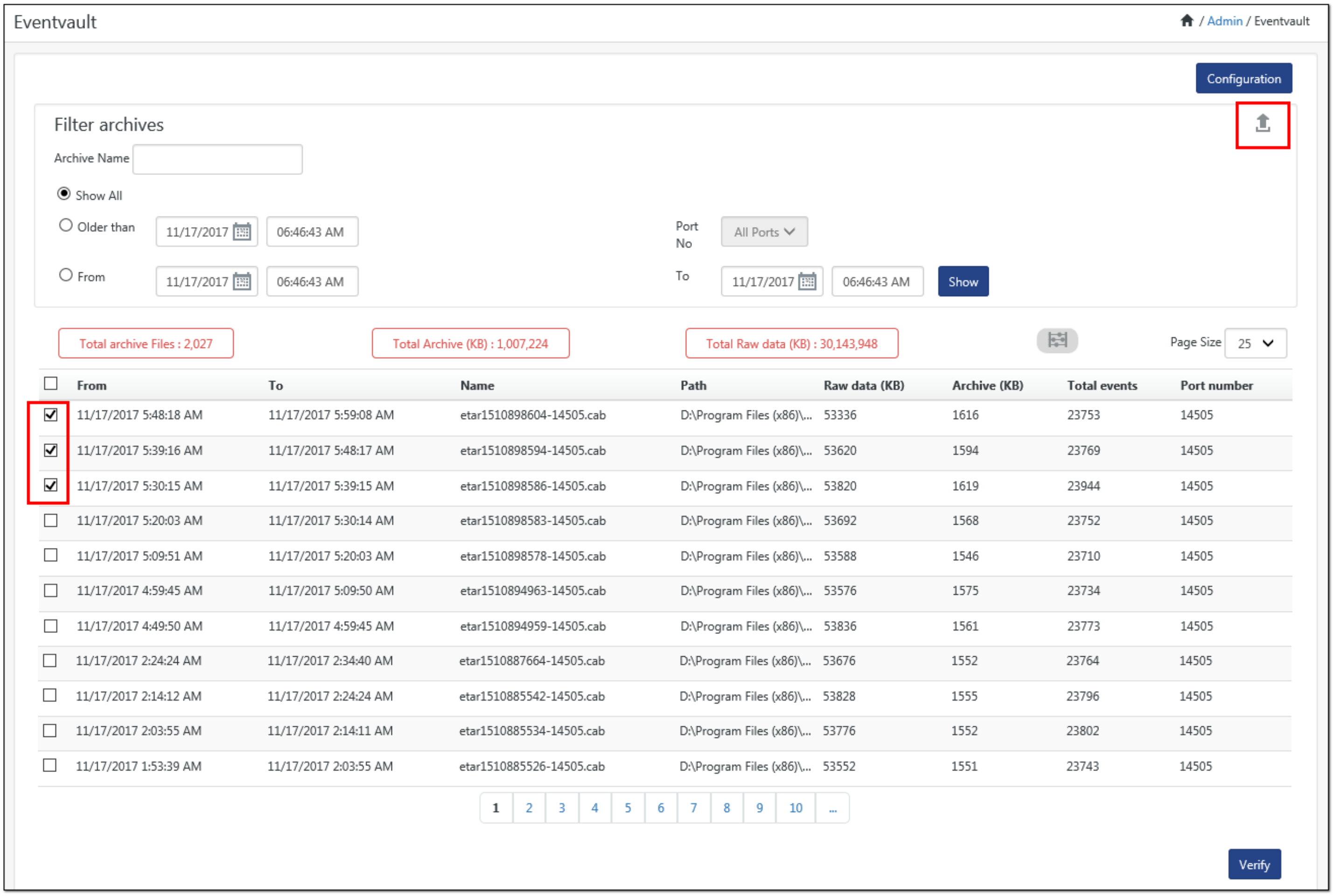
2. Click **Open** to view the result.

   (OR)

3. Save the file in local drive and then click **Open** to view result.

14.3 Exporting Archive File(s)

1. To export the archive files, select any Archive file, and then click **Export icon** .



Filter archives

Archive Name

● Show All

○ Older than 11/17/2017 06:46:43 AM

Port No All Ports

○ From 11/17/2017 06:46:43 AM To 11/17/2017 06:46:43 AM

Total archive Files : 2,027

Total Archive (KB) : 1,007,224

Total Raw data (KB) : 30,143,948

Page Size 25

□	From	To	Name	Path	Raw data (KB)	Archive (KB)	Total events	Port number
☑	11/17/2017 5:48:18 AM	11/17/2017 5:59:08 AM	etar1510898604-14505.cab	D:\Program Files (x86)\...	53336	1616	23753	14505
☑	11/17/2017 5:39:16 AM	11/17/2017 5:48:17 AM	etar1510898594-14505.cab	D:\Program Files (x86)\...	53620	1594	23769	14505
☑	11/17/2017 5:30:15 AM	11/17/2017 5:39:15 AM	etar1510898586-14505.cab	D:\Program Files (x86)\...	53820	1619	23944	14505
□	11/17/2017 5:20:03 AM	11/17/2017 5:30:14 AM	etar1510898583-14505.cab	D:\Program Files (x86)\...	53692	1568	23752	14505
□	11/17/2017 5:09:51 AM	11/17/2017 5:20:03 AM	etar1510898578-14505.cab	D:\Program Files (x86)\...	53588	1546	23710	14505
□	11/17/2017 4:59:45 AM	11/17/2017 5:09:50 AM	etar1510894963-14505.cab	D:\Program Files (x86)\...	53576	1575	23734	14505
□	11/17/2017 4:49:50 AM	11/17/2017 4:59:45 AM	etar1510894959-14505.cab	D:\Program Files (x86)\...	53836	1561	23773	14505
□	11/17/2017 2:24:24 AM	11/17/2017 2:34:40 AM	etar1510887664-14505.cab	D:\Program Files (x86)\...	53676	1552	23764	14505
□	11/17/2017 2:14:12 AM	11/17/2017 2:24:24 AM	etar1510885542-14505.cab	D:\Program Files (x86)\...	53828	1555	23796	14505
□	11/17/2017 2:03:55 AM	11/17/2017 2:14:11 AM	etar1510885534-14505.cab	D:\Program Files (x86)\...	53776	1552	23802	14505
□	11/17/2017 1:53:39 AM	11/17/2017 2:03:55 AM	etar1510885526-14505.cab	D:\Program Files (x86)\...	53552	1551	23743	14505

Figure 412

The data will be exported in an excel file.

2. Click **Open** to view the result.

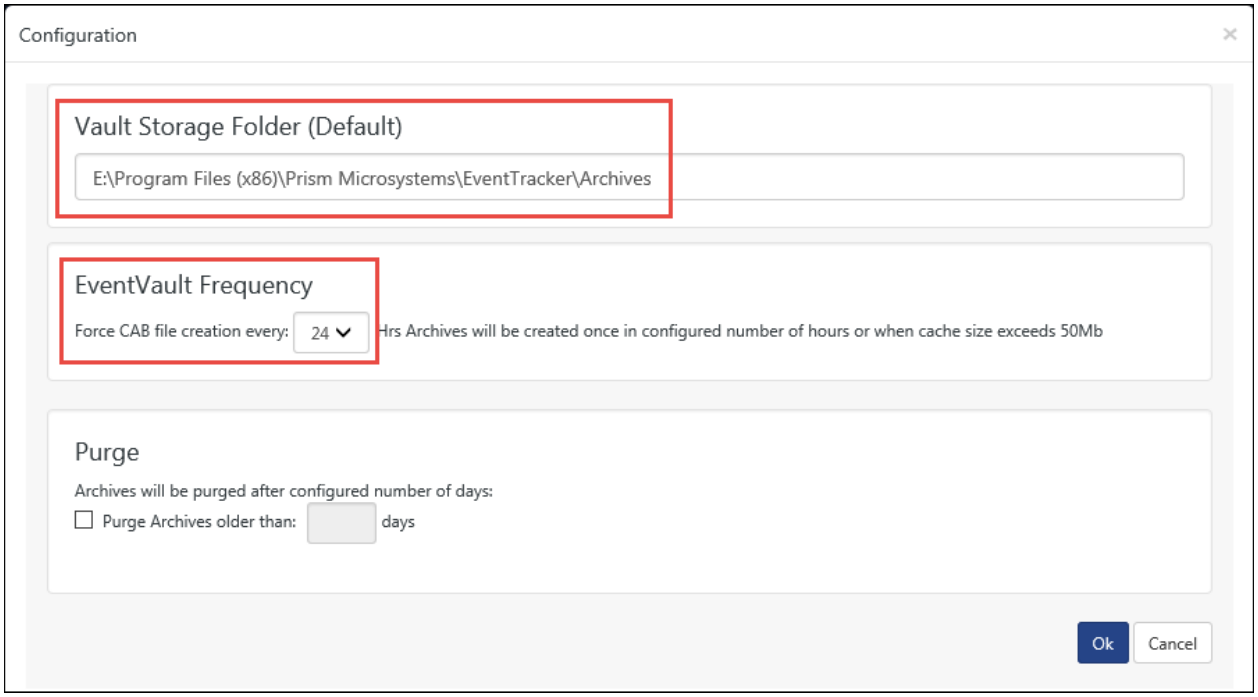
   (OR)

3. Save the file in local drive and then click **Open** to view result.

14.4 Configuring EventVault Manager

1. Click the **Configuration** hyperlink to configure **EventVault Manager**.

   Configuration window opens.



Configuration

Vault Storage Folder (Default)

E:\Program Files (x86)\Prism Microsystems\EventTracker\Archives

EventVault Frequency

Force CAB file creation every: 24 Hrs Archives will be created once in configured number of hours or when cache size exceeds 50Mb

Purge

Archives will be purged after configured number of days:

□ Purge Archives older than: days

Figure 413

2. Enter relevant data and click **Ok**.

   For detail information refer chapter Control Panel -> EventVault.

15. FAQ Tile Configuration

In this chapter, you will learn how to use:

- Configure FAQ Tiles

15.1 Configuring FAQ Tiles

In v9.3, the user can configure FAQ tiles which will be displayed in modules like Home, Alerts and Systems.

To configure FAQ tile,

- Click the icon ⚙.
  The FAQ tile configuration window gets displayed.

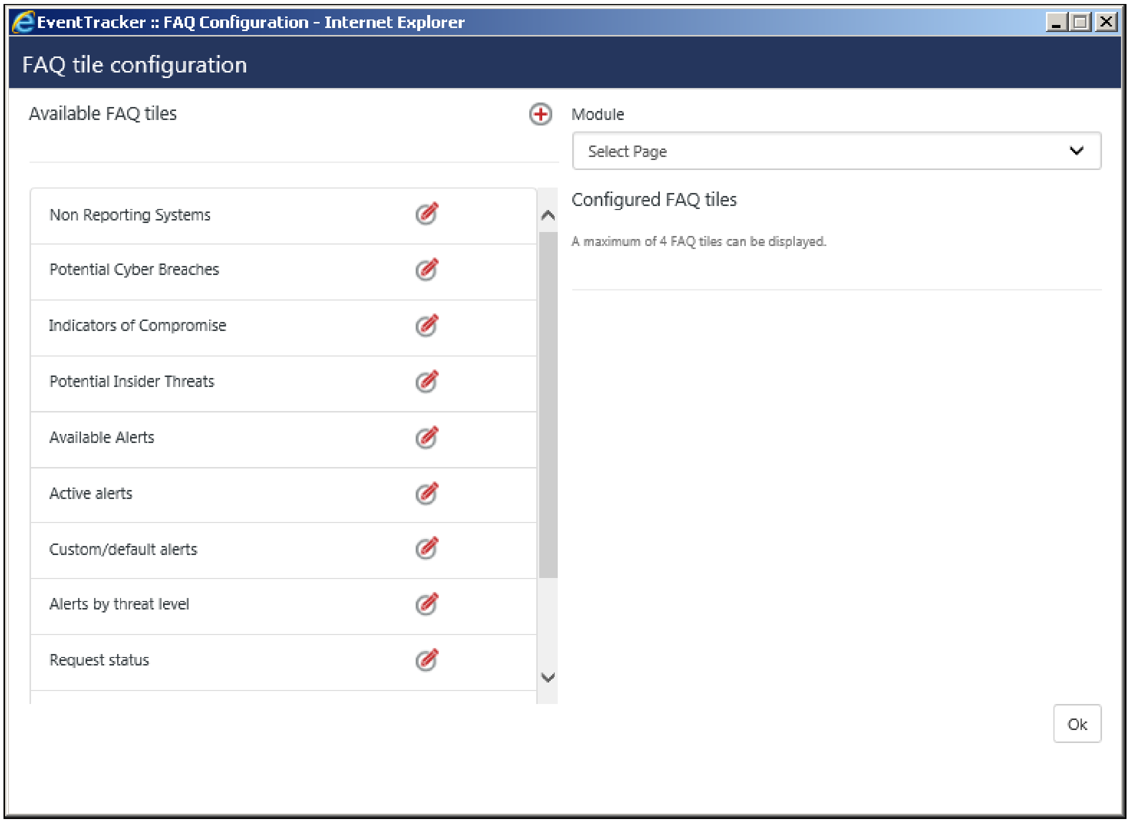


Figure 414

- In the right pane, the user can select from the modules, where they want to display the tiles.

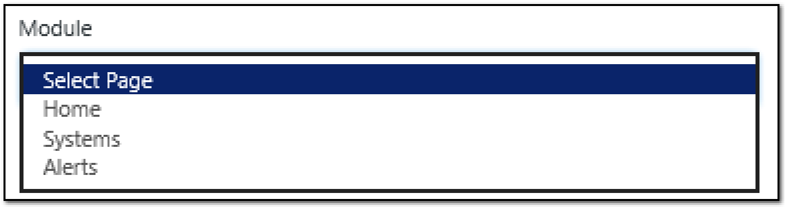
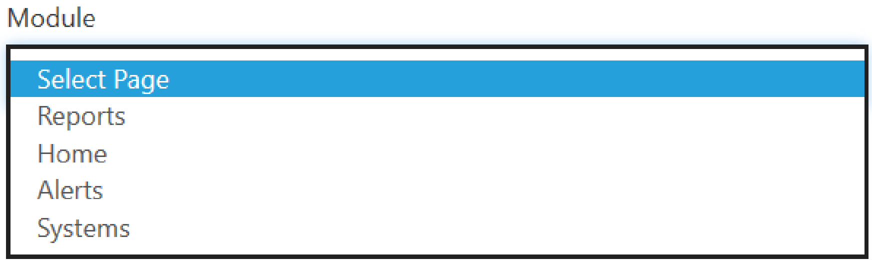


Figure 415

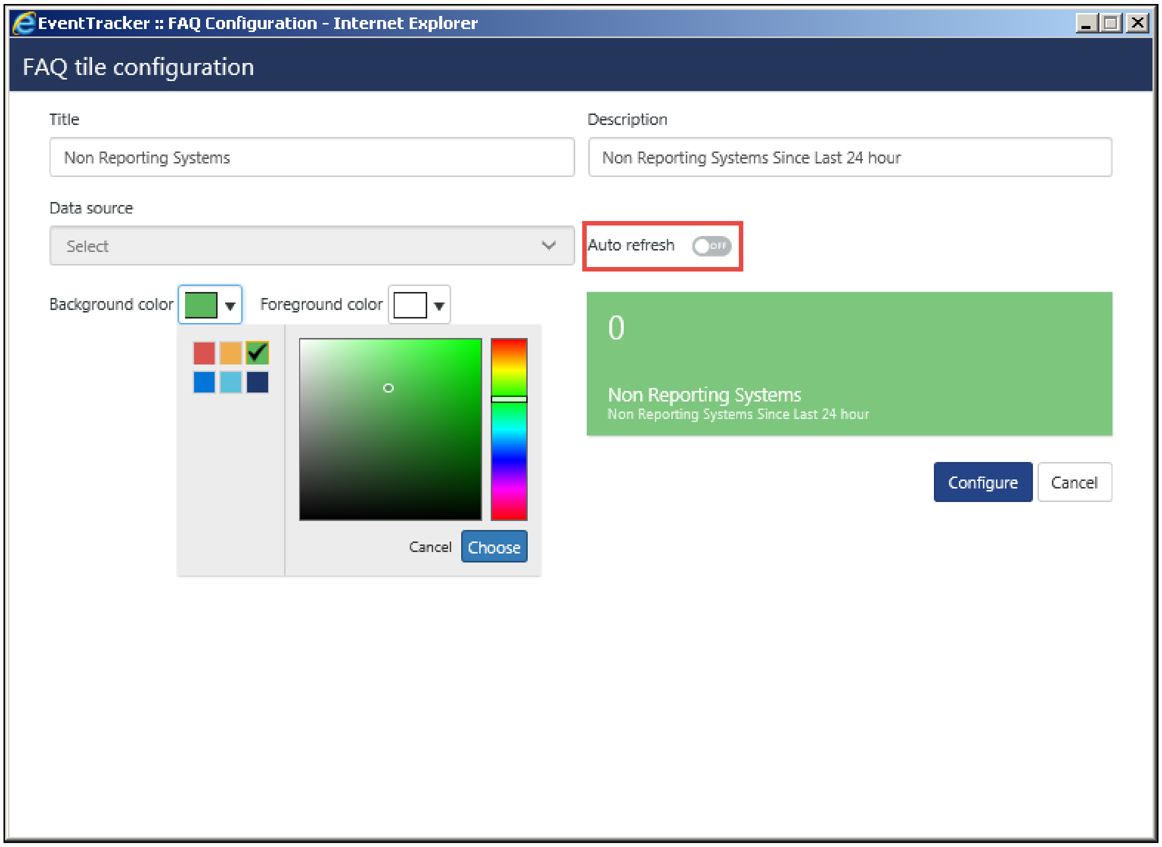


Module

- Select Page
- Reports
- Home
- Alerts
- Systems

Figure 416

- The left pane displays the available list of FAQ tiles.
- Click the Edit icon ✎ to make changes in any tile.
- The user can change the Title and Description.
- The user can also modify the background color, the foreground color and can even turn on the "Auto-refresh".



EventTracker :: FAQ Configuration - Internet Explorer

FAQ tile configuration

Title: Non Reporting Systems

Description: Non Reporting Systems Since Last 24 hour

Data source: Select

Auto refresh: OFF

Background color: 🟩

Foreground color: □

Figure 417

- To add the configured FAQ tiles to the respective modules, select the module and click **Add** 🔗 to map it to the respective module.
- To remove a mapped tile, use the icon 🔗.

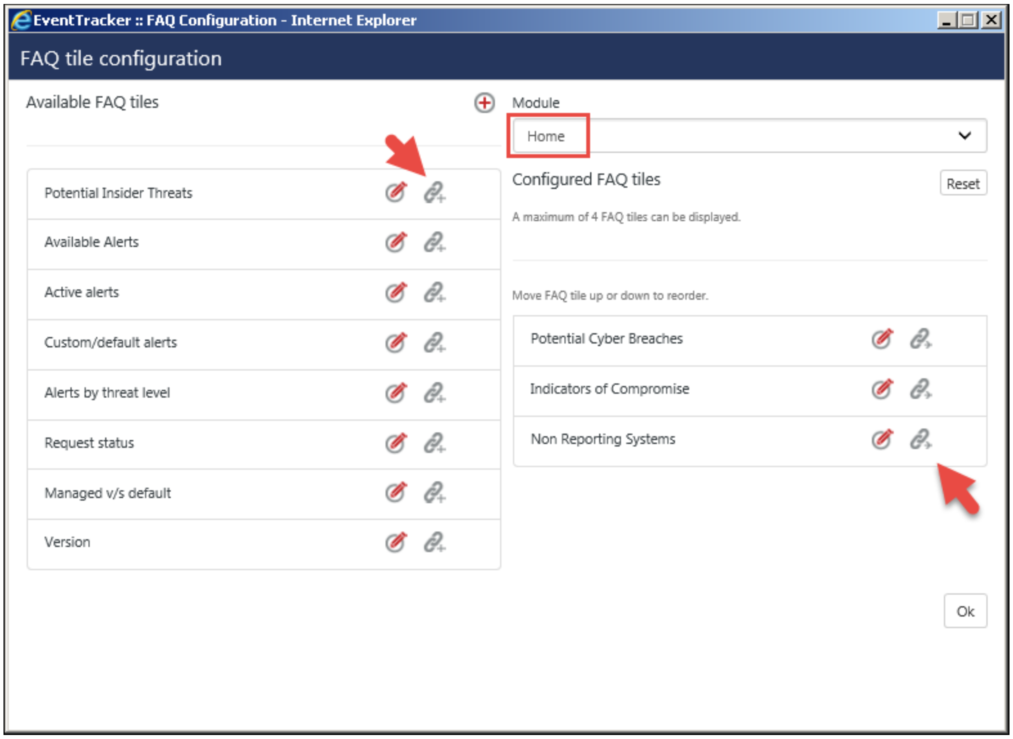


Figure 418

- After mapping the FAQ tiles, click **OK**.

  It opens in the Home Dashboard.

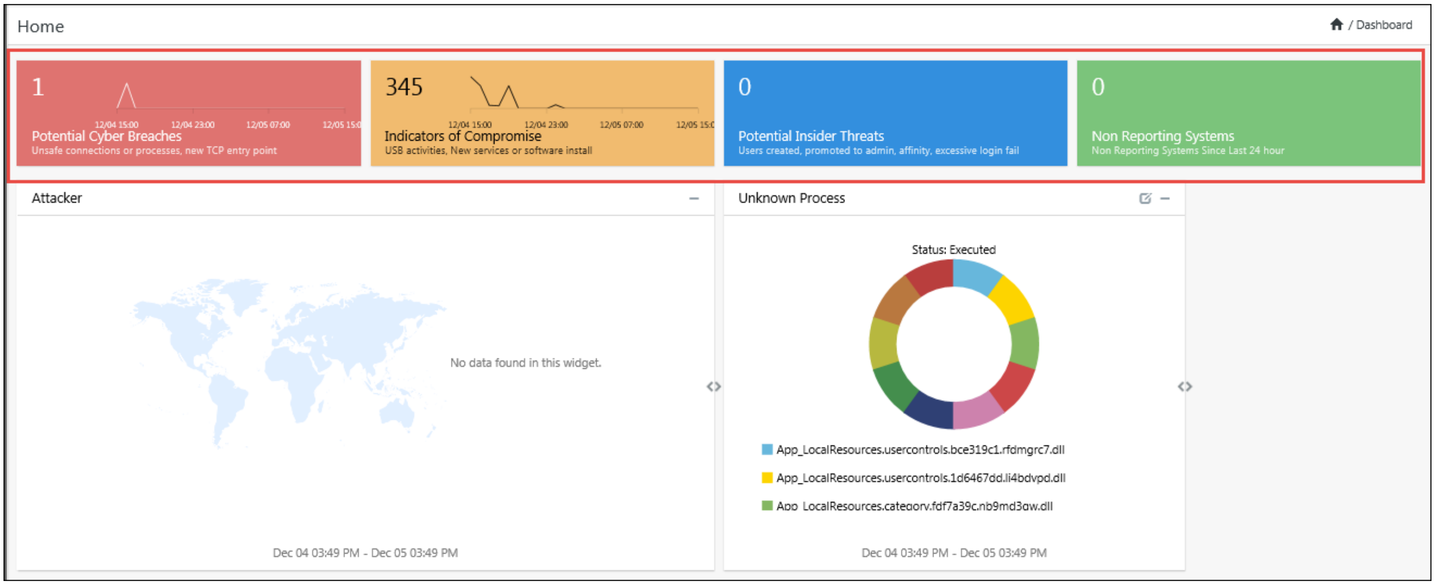

Home
/ Dashboard
1
12/04 15:00
12/04 23:00
12/05 07:00
12/05 15:0
Potential Cyber Breaches
Unsafe connections or processes, new TCP entry point
345
12/04 15:00
12/04 23:00
12/05 07:00
12/05 15:0
Indicators of Compromise
USB activities, New services or software install
0
Potential Insider Threats
Users created, promoted to admin, affinity, excessive login fail
0
Non Reporting Systems
Non Reporting Systems Since Last 24 hour
Attacker
No data found in this widget.
Dec 04 03:49 PM - Dec 05 03:49 PM
Unknown Process
Status: Executed
App_LocalResources.usercontrols.bce319c1.rfdmgrc7.dll
App_LocalResources.usercontrols.1d6467dd.li4bdvpd.dll
App_LocalResources.category.fdf7a39c.nb9md3gw.dll
Dec 04 03:49 PM - Dec 05 03:49 PM

Figure 419

15.1.1 Permalink

User(s) can use this option to provide Useful links like Solution brief link, Compliance mapping document, PCI DSS requirement link etc. which is useful for reference.

15.1.1.1 Configuring a permalink in FAQ tile configuration

In v9.3, the user can configure FAQ tiles which will be displayed in modules like Home, Alerts, Reports and Systems.

To configure FAQ tile,

- Click the FAQ configuration option in Admin dropdown.
  The FAQ tile configuration window gets displayed.

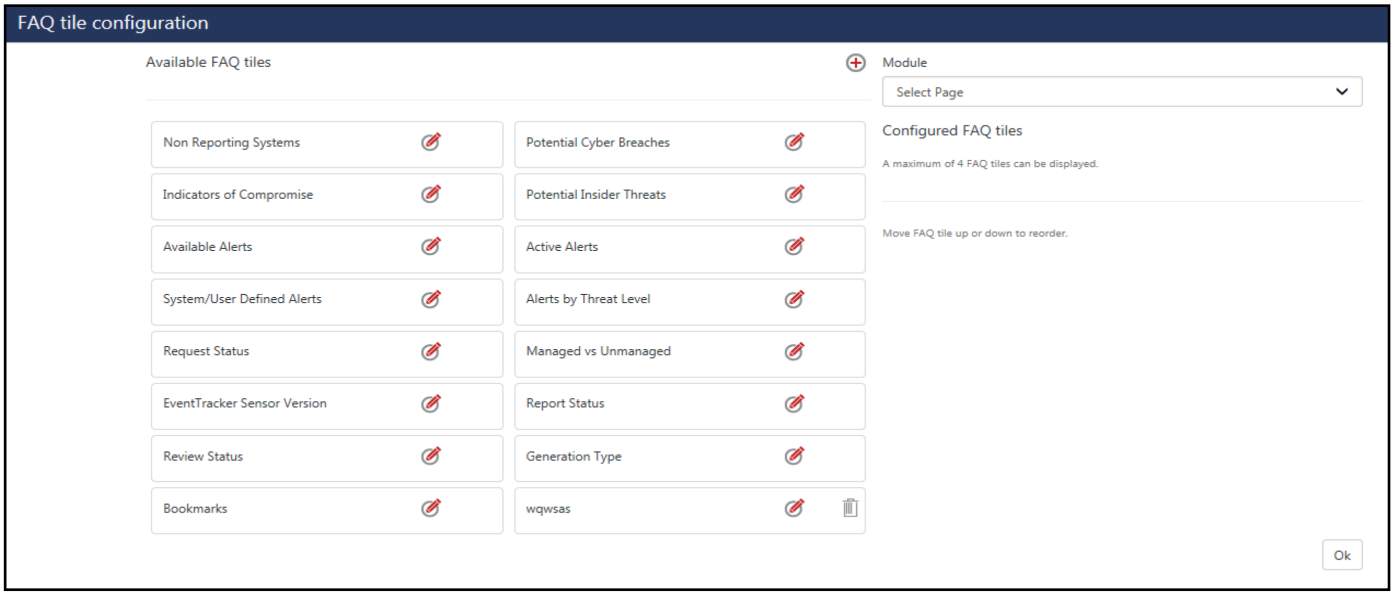


Figure 420

- In the right pane, the user can select from the modules, where they want to display the tiles.

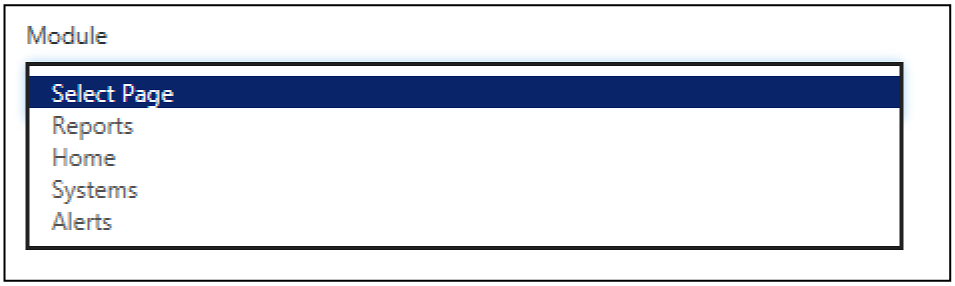
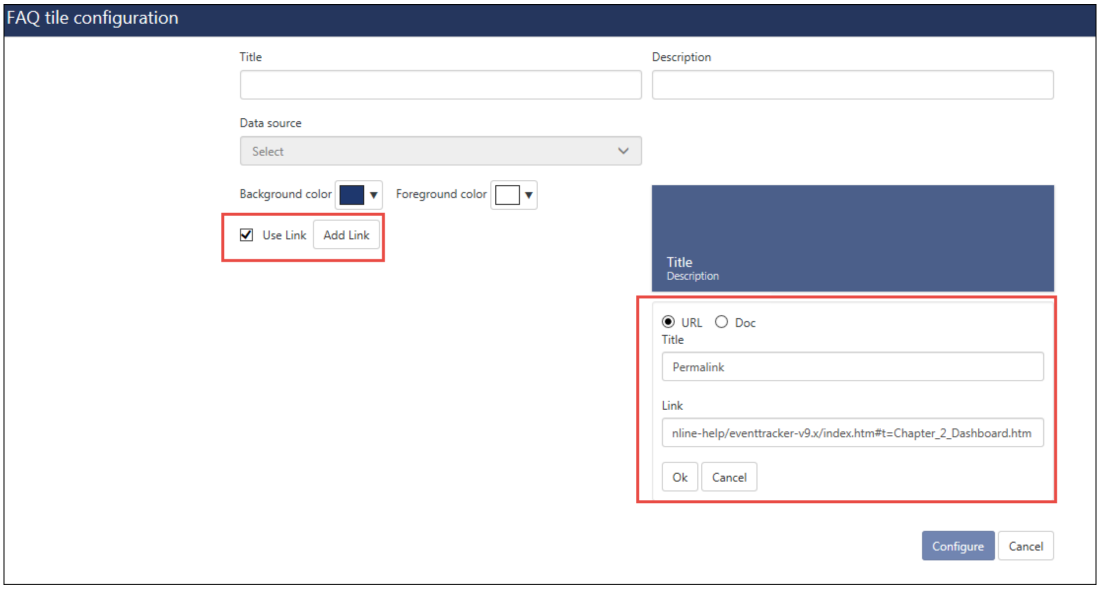


Figure 421

- The left pane displays the available list of FAQ tiles.

To add a link to a FAQ Tile, click the add icon and check **Use Link** option.

- Click the Add Link button to add URL or Documents, as per requirement.



FAQ tile configuration

Title

Description

Data source

Select

Background color ▾ Foreground color ▾

☑ Use Link Add Link

● URL ○ Doc

Title

Permalink

Link

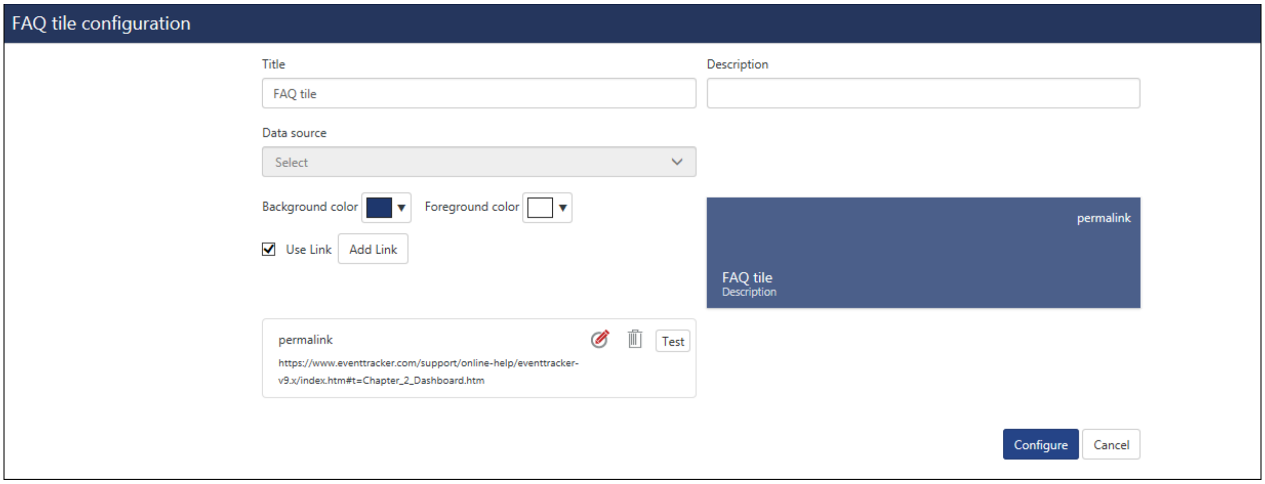
nline-help/eventtracker-v9.x/index.htm#t=Chapter_2_Dashboard.htm

Ok Cancel

Configure Cancel

Figure 422

- Give a suitable title and click OK. It will be listed in the left pane.
- And then click the **Configure** button.



FAQ tile configuration

Title

FAQ tile

Description

Data source

Select

Background color ▾ Foreground color ▾

☑ Use Link Add Link

permalink

https://www.eventtracker.com/support/online-help/eventtracker-v9.x/index.htm#t=Chapter_2_Dashboard.htm

Test

Configure Cancel

Figure 423

In the same way, the user can also add documents and configure a FAQ tile, as per needs.

NOTE:

1. The supported document extensions are (.txt,.pdf,.doc,.docx,.rtf,.xlsx,.xls).
2. The maximum size of the document is 2MB.

16. Group Management

In this chapter, you will learn about:

- Group Management

16.1 Group Management

Group management allows the admin to Configure Alert action email based on system group. There will be cases where each client will be belonging to each group. In such cases, when an alert is triggered in any customer place, the action item (email) is sent to a Super admin. So, it becomes difficult to differentiate from which customer the incident happened. Group management helps in solving these hassles.

Navigate to **Admin** and then select **Group Management**.

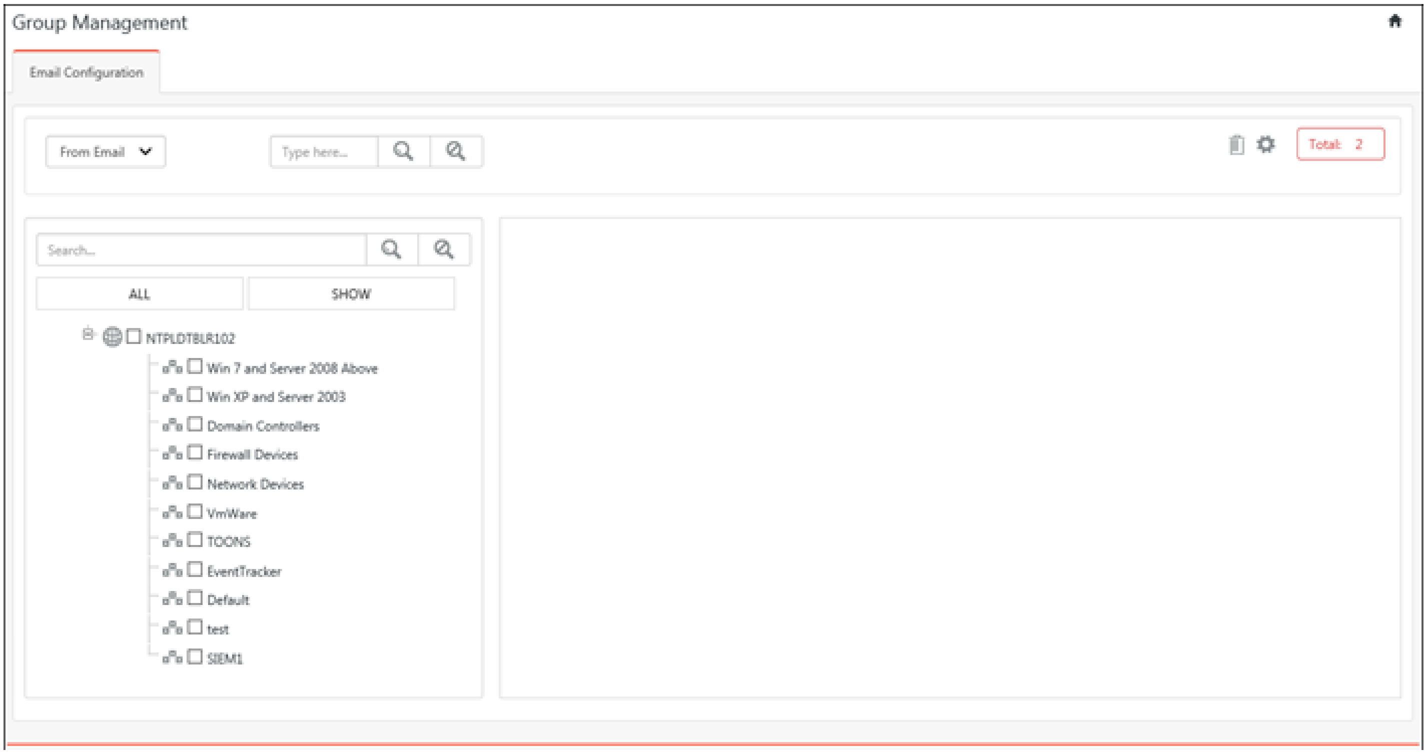
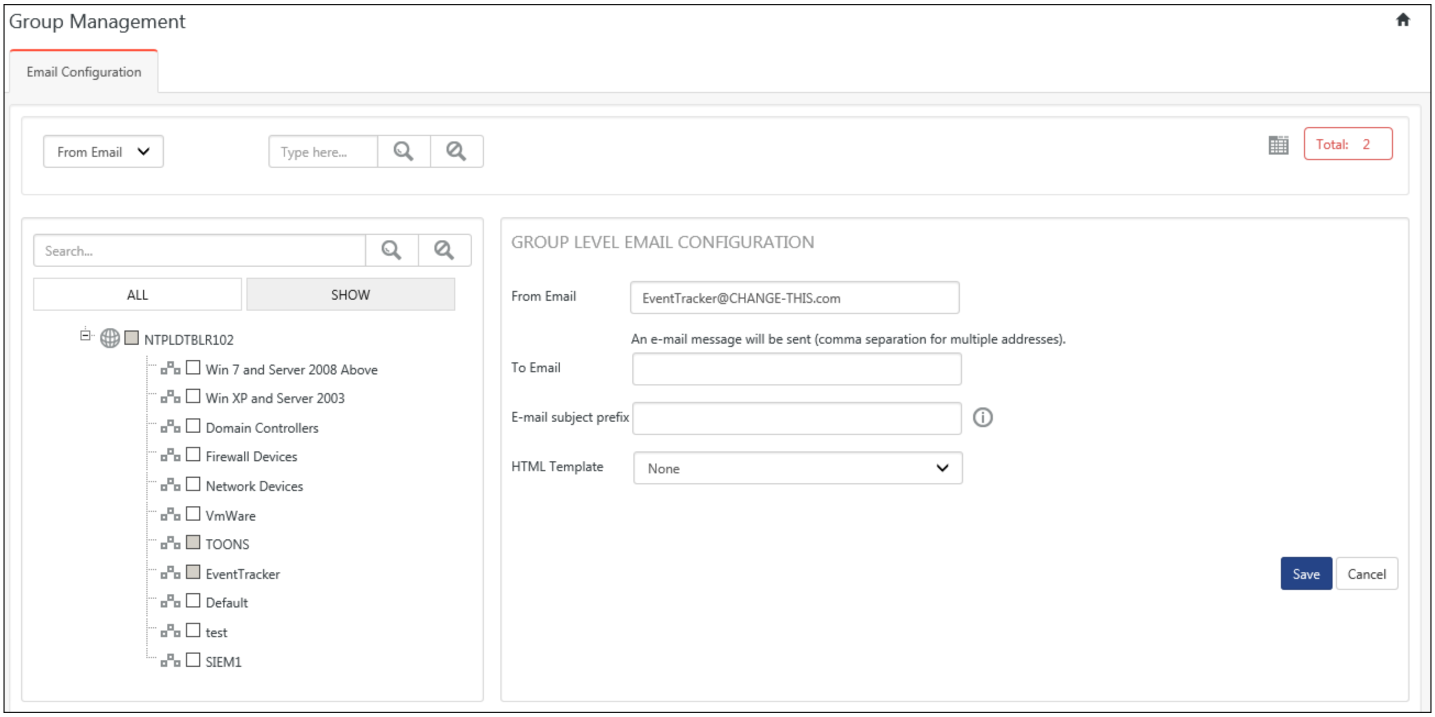


Figure 424

- To configure e-mail, click the icon ⚙.

The e-mail configuration page opens.



GROUP LEVEL EMAIL CONFIGURATION

From Email: EventTracker@CHANGE-THIS.com

An e-mail message will be sent (comma separation for multiple addresses).

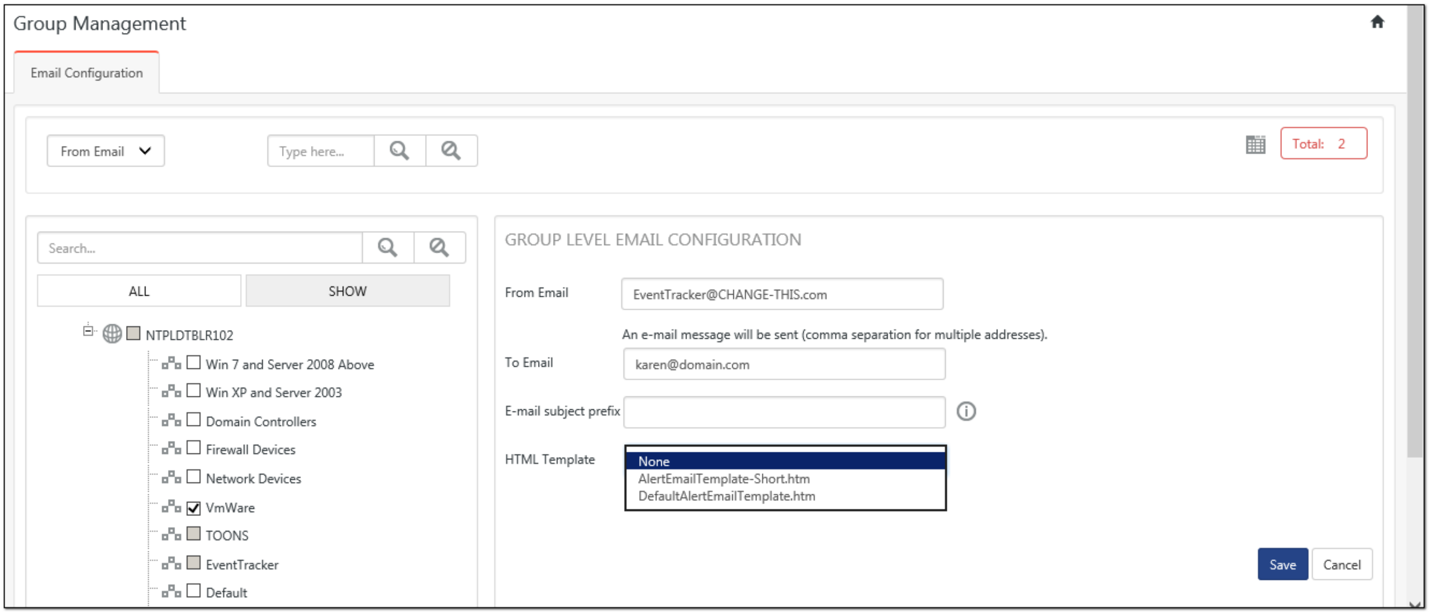
To Email:

E-mail subject prefix:

HTML Template: None

Figure 425

- Select the **Group** from the left tree pane.
- Enter the details in the respective fields.
- Select the HTML template and then click **Save**.



GROUP LEVEL EMAIL CONFIGURATION

From Email: EventTracker@CHANGE-THIS.com

An e-mail message will be sent (comma separation for multiple addresses).

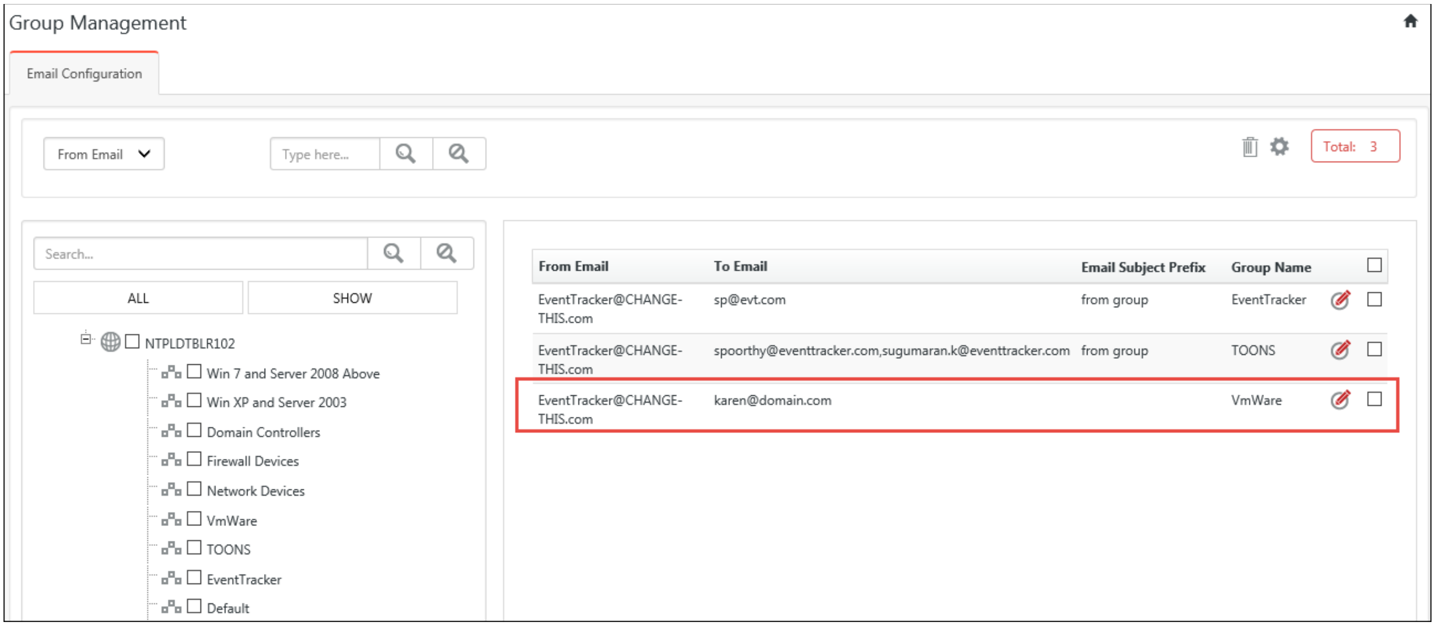
To Email: karen@domain.com

E-mail subject prefix:

HTML Template:
None
AlertEmailTemplate-Short.htm
DefaultAlertEmailTemplate.htm

Figure 426

The e-mail configuration gets added.



From Email	To Email	Email Subject Prefix	Group Name	□
EventTracker@CHANGE-THIS.com	sp@evt.com	from group	EventTracker	□
EventTracker@CHANGE-THIS.com	spoorthy@eventtracker.com,sugumaran.k@eventtracker.com	from group	TOONS	□
EventTracker@CHANGE-THIS.com	karen@domain.com		VmWare	□

Figure 427

17. IP Lookup Configuration

In this chapter, you will learn about:

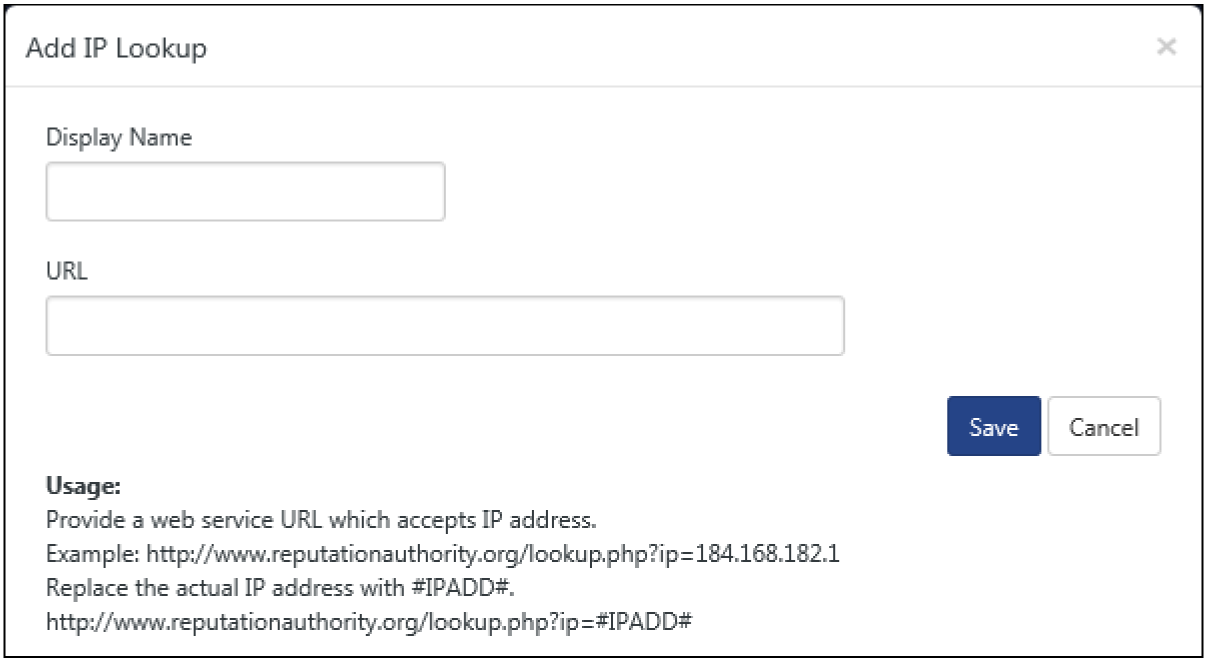
- Add IP Lookup

17.1 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.

17.1.1 Adding IP Lookup

1. Go to **Admin.**
2. Select the **IP Lookup Configuration.**
3. Click **Add New**.



Usage:
Provide a web service URL which accepts IP address.
Example: http://www.reputationauthority.org/lookup.php?ip=184.168.182.1
Replace the actual IP address with #IPADD#.
http://www.reputationauthority.org/lookup.php?ip=#IPADD#

Figure 428

EventTracker:: Add IP Lookup window opens.

4) Enter the **Display Name:** in the box.
Users can give any relevant name in display name field.
5) 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.
6) Click **Save**.
7) In **Behavior** menu, select **Security** dropdown.
8) Select any **IP address Activity**, and then click **Go**.
The respective IP address is displayed as configured in Add IP Lookup configuration.

18. Knowledge objects

In this chapter, you will learn how to use:

- Knowledge objects

18.1 Knowledge Objects and Interesting tokens

In every area of IT systems and devices generate plethora of data. Turning this data in to informative and actionable is the key. Data is heterogeneous, complex and contain wealth valuable information. Message generated by various application/devices has varying degree of message signature. Message may be well formatted or verbose plain English sentence. Knowledge Object will perform extraction of information in log search which and is known as" *Interesting Tokens".*

Knowledge Object is collection of 'Event Rules' and 'Expressions' under these rules. Important key definitions are as below

Event Rule:

'Event Rule' can be defined by assigning at least one Standard property [Log Type, Event Source, Event ID and Event Type] and specifying expression in description [both Inclusion and Exclusion]. Description can be specified either by Regular Expression or text. Following are some constraints while creating rule:

- Specify at least one of the Properties and Description pattern to recognize uniquely.
- May contain more than one 'Event Rule' per 'Knowledge Object'.
- There should not be any ambiguity in constraint which could match to more than one 'Knowledge Object'

Message Signature:

Message signature is part of 'Event Rule' and is a distinct pattern to identify message. In EventTracker logs are stored in database with certain degree of normalization and schema. A log can be divided in to two sections i.e. 'Properties' and 'Description'. Together these can be part of the signature. Message signature can contain matching or exception message pattern and may also contain any of the event properties.

Event rules and Ambiguity:

Each Knowledge Object constitutes of 'Event Rule' and 'Expressions' for extracting valuable information. One of the most important factors about 'Event Rule' definition is that there should not be any ambiguity in identifying 'Knowledge Object'. To achieve this, every 'Event Rule' must be unique and should not resolve to more than one 'Knowledge Object'. In case a log matches more than one Knowledge Object, weightage-based algorithm will decide the 'Knowledge Object' that has to be applied to the target log and will extract interesting tokens accordingly.

Expressions:

Expressions are defined under each rule. 'Expression' is used to extract atomic information from the message. One rule can have zero or more expressions. If no expressions are specified, search engine will try to match with well-known signature and extract information.
Message signature recognition can be helpful in extracting 'Key' and 'Value' pairs from the message if any.

Some signature will have definitive Key-Value Pair (KVP) pattern where it is sufficient just to provide **Key** and **Value** delimiter for e.g. in windows messages KVPs are recognized by ':' (colon) and '\r\n' (new line). In many cases this KVP may be found with various **Key** and **Value** delimiter. But sometimes it is not possible to define any KVP because the message is in plain verbose English. In these cases, there will not be any key to specify value. Generally, messages can be identified having:

- Well-defined KVP with single Key and Value delimiter
- Well-defined KVP with multiple Key and Value delimiter.
- Messages with well-known information pattern (IP, URL, filenames, dates etc.) but missing KVP
- Verbose plain English sentence where neither KVP nor well-known information pattern exists.

Based on above observations 'Expression' can be of following type

- Key Value delimiter
- Regular expression (Requires virtual column name depending on Regular Expression)
- Column delimiter (Requires virtual column name)
- Between 2 constant string (Requires virtual column name)

Knowledge Objects consists of 2 panes namely action pane and editor pane.

Action Pane: This pane will have list of all available Source types and can be viewed and edited by clicking one of the Source types

Editor pane: This is the pane where are CRUD operations, Validations and Verification of constraint and Expressions can be carried out.

18.2 Group Knowledge Objects

User can now categorize the knowledge objects by creating customized groups and adding Knowledge Objects to the group, as per requirement.

1. Login to EventTracker.
2. Click the **Admin** menu, and then click **Knowledge Objects**.
   Knowledge Objects page opens.

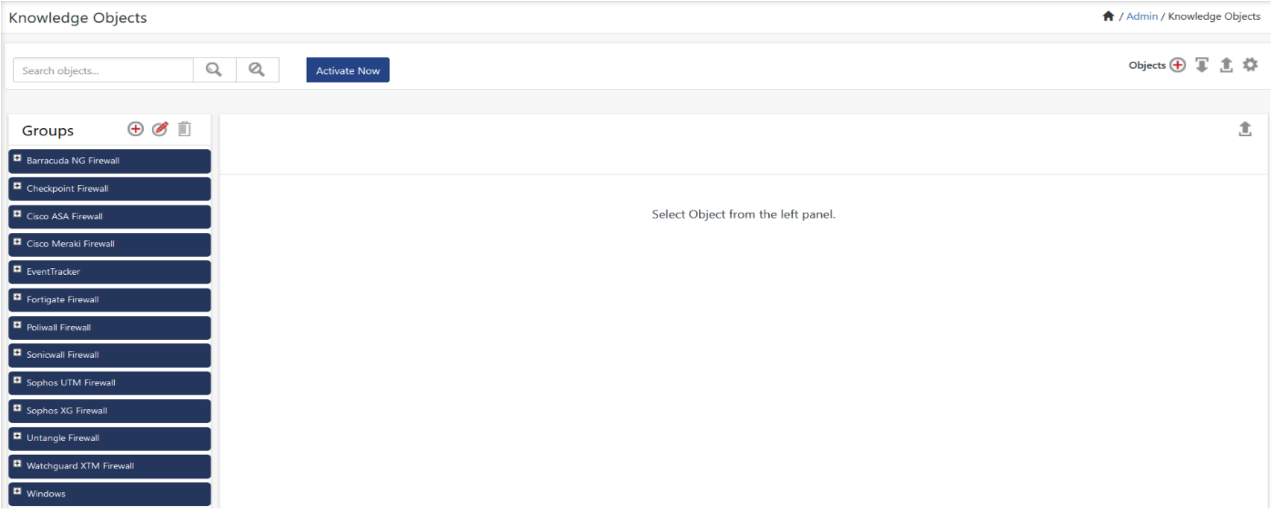


Figure 429

The Knowledge Objects is listed.

3. To add a group, click ⊕ icon in the GROUP pane.
   Add Group window opens.

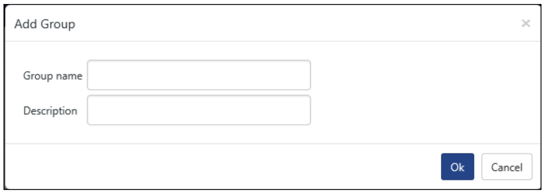


Figure 430

4. Enter the **Group name: and Description.**

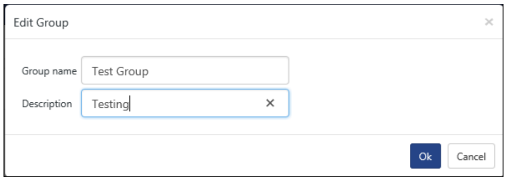
   NOTE:

   - The Group name is unique.

   To activate the group and adding Knowledge Objects to it, make the required changes using Edit feature and it is explained below.

   a. Click ✎ icon in the GROUPS pane for editing the group.

      Edit group window opens.



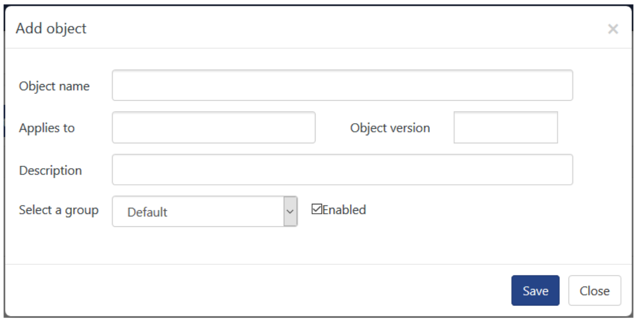
Group name: Test Group

Description: Testing

Figure 431

18.2.1 Adding Knowledge Objects to a Group

1. To add an object to a group, click Objects ⊕ icon in the right-hand corner. Add object window opens.



Add object

Object name

Applies to

Object version

Description

Select a group: Default

☑Enabled

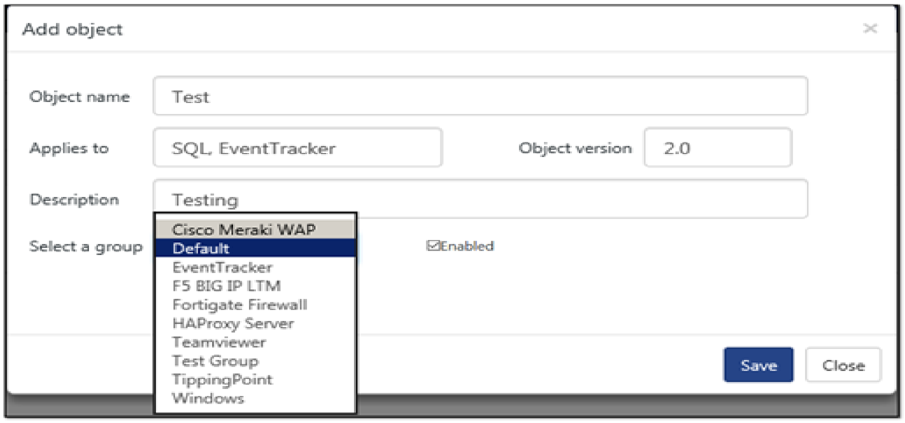
Figure 432

2. Enter the **Object name: Applies to:, Object version:, Description.**

   NOTE:

   The Object name is unique.

3. Select the group from the dropdown box, where you wish to add the object.
4. Click **Enabled** option.



Add object

Object name: Test

Applies to: SQL, EventTracker

Object version: 2.0

Description: Testing

Select a group:

- Cisco Meraki WAP
- Default
- EventTracker
- F5 BIG IP LTM
- Fortigate Firewall
- HAProxy Server
- Teamviewer
- Test Group
- TippingPoint
- Windows

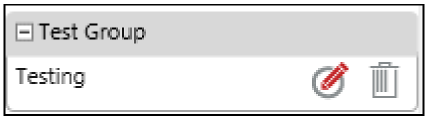
☑Enabled

Figure 433

5. Click **Save**.

   NOTE:

   The object added to the group can be edited and can also be enabled or disabled.



⊟ Test Group

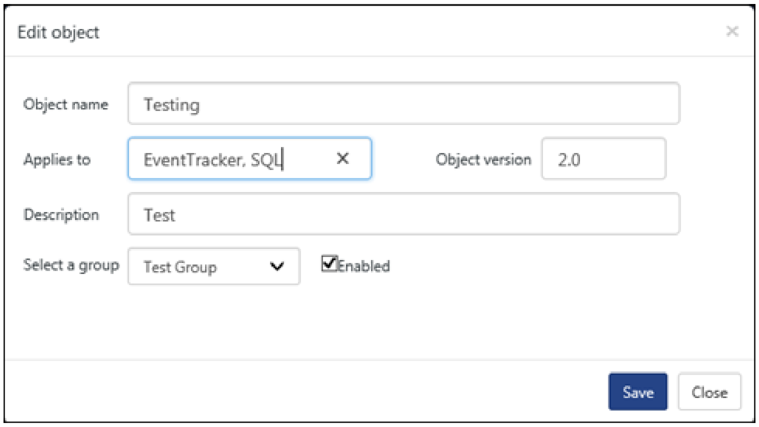
Testing

Figure 434

To activate this data in the Knowledge Object, make the required changes using Edit feature and it is explained below.

b. Click icon for editing the Object.

Edit object window opens.



Edit object

Object name: Testing

Applies to: EventTracker, SQL

Object version: 2.0

Description: Test

Select a group: Test Group

☑ Enabled

Figure 435

c. Select **Enabled** option, and if required make the necessary changes.

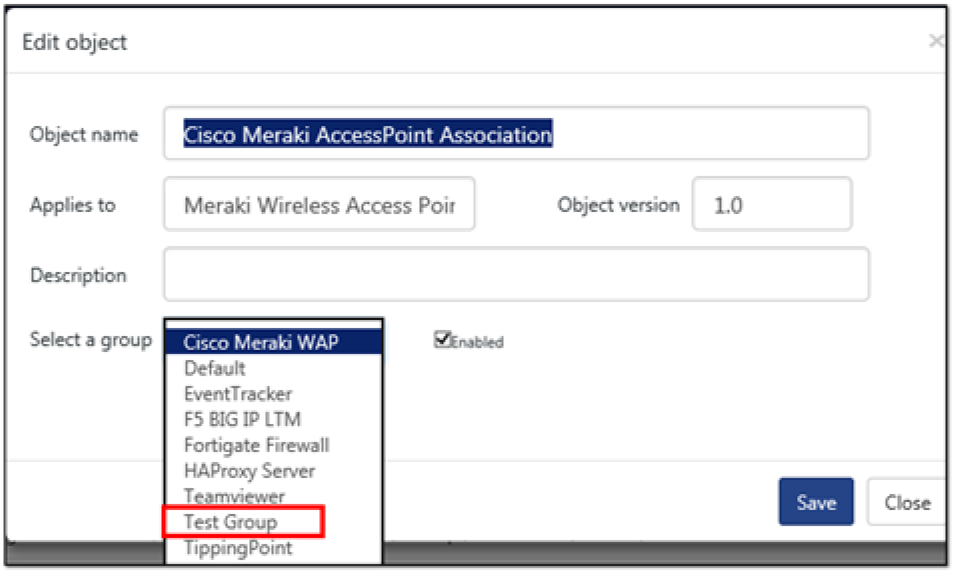
d. Click **Save**.

To add Default Knowledge Objects to the Custom Group,

1. Expand the Group.
2. Select the Knowledge Object and click **Edit** icon.
   For Example: **Cisco Meraki AccessPoint Association**

Edit Object window opens.

3. Select the custom group.
   Here we selected “**Test Group**”.



Object name: Cisco Meraki AccessPoint Association

Applies to: Meraki Wireless Access Poir

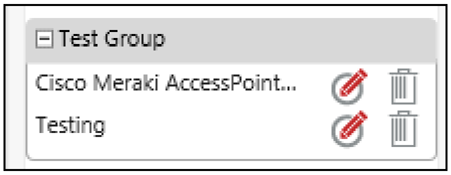
Object version: 1.0

Select a group: Cisco Meraki WAP, Default, EventTracker, F5 BIG IP LTM, Fortigate Firewall, HAProxy Server, Teamviewer, Test Group, TippingPoint

Figure 436

4. Click **Save**.

   The Object gets added to the group.



⊟ Test Group

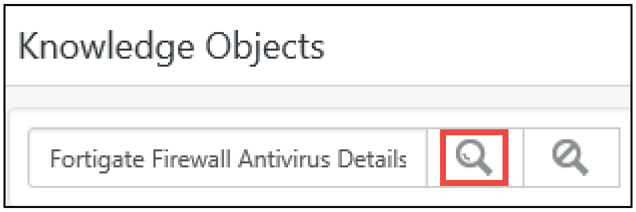
Cisco Meraki AccessPoint...

Testing

Figure 437

18.2.2 Searching Objects

The user will now be able to search a Knowledge Object by typing the name of the object in the search box and click **search** icon 🔍.



Knowledge Objects

Fortigate Firewall Antivirus Details

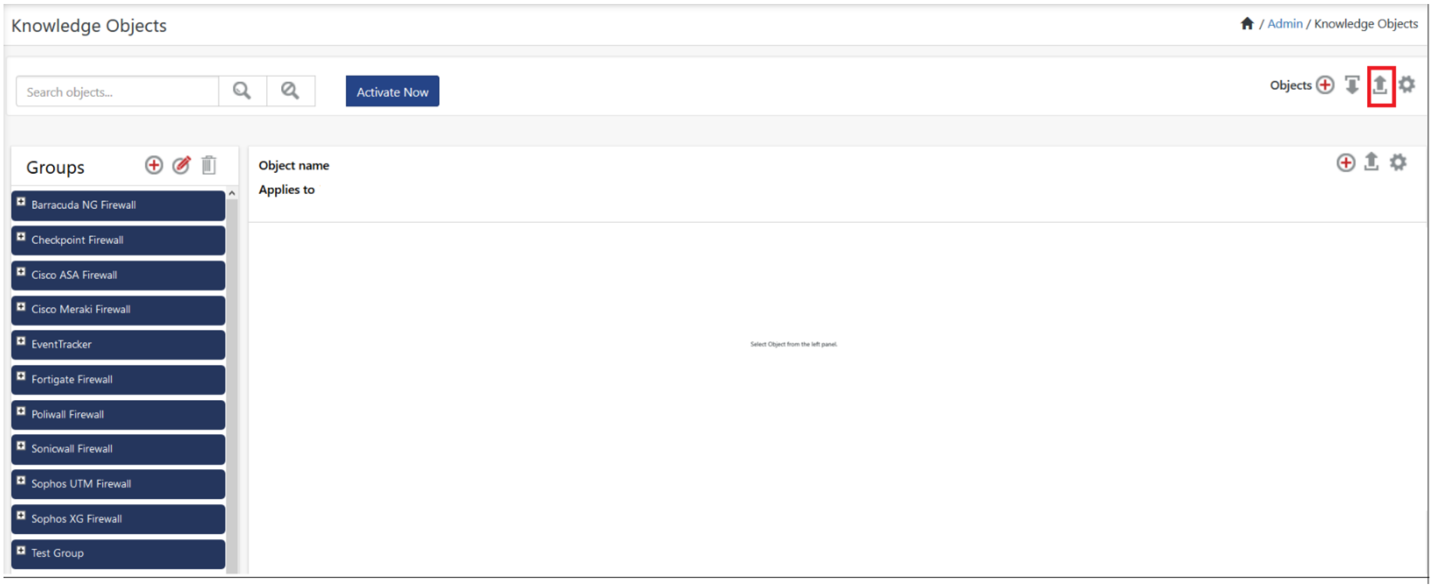
Figure 438

18.3 Exporting Object

Objects are available to import or export in a JSON format, file with extension .etko.

For Exporting Objects,

- Click on the **Admin> Knowledge Objects.**
- Expand the respective group and select the Knowledge object you want to export and click Export .



Knowledge Objects

/ Admin / Knowledge Objects

Search objects...

Activate Now

Objects

Groups

- Barracuda NG Firewall
- Checkpoint Firewall
- Cisco ASA Firewall
- Cisco Meraki Firewall
- EventTracker
- Fortigate Firewall
- Poliwall Firewall
- Sonicwall Firewall
- Sophos UTM Firewall
- Sophos XG Firewall
- Test Group

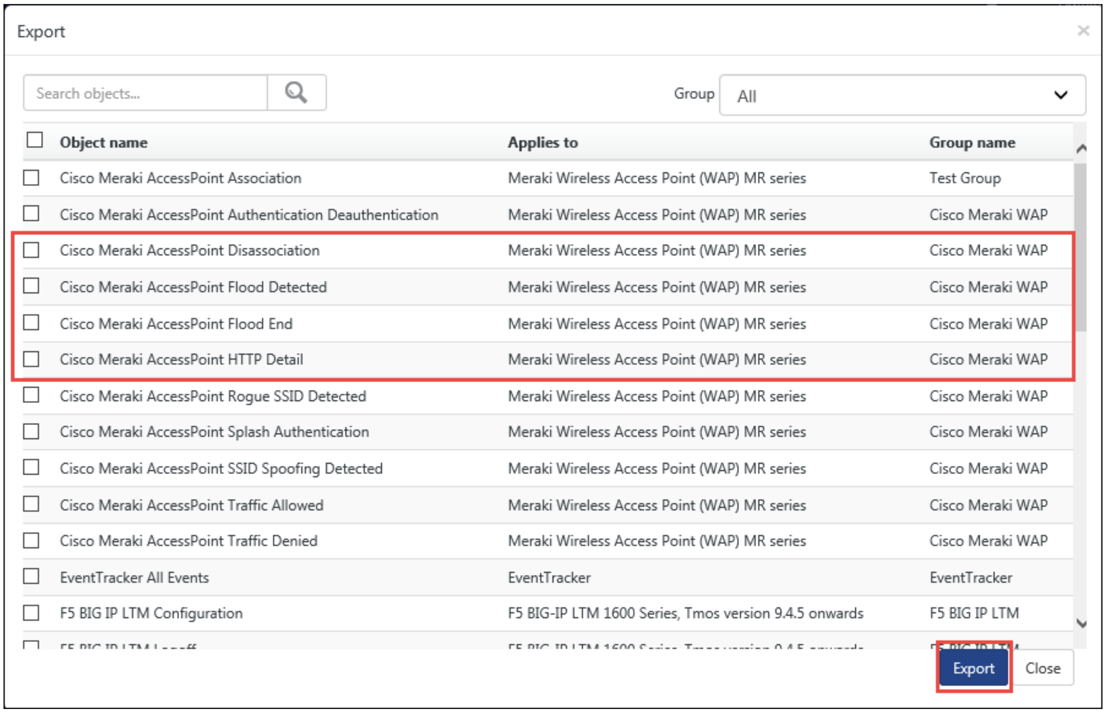
Object name

Applies to

Select Object from the left panel.

Figure 439

- EventTracker: Knowledge Object Import/Export page opens.



Export

Search objects...

Group: All

□ Object name	Applies to	Group name
□ Cisco Meraki AccessPoint Association	Meraki Wireless Access Point (WAP) MR series	Test Group
□ Cisco Meraki AccessPoint Authentication Deauthentication	Meraki Wireless Access Point (WAP) MR series	Cisco Meraki WAP
□ Cisco Meraki AccessPoint Disassociation	Meraki Wireless Access Point (WAP) MR series	Cisco Meraki WAP
□ Cisco Meraki AccessPoint Flood Detected	Meraki Wireless Access Point (WAP) MR series	Cisco Meraki WAP
□ Cisco Meraki AccessPoint Flood End	Meraki Wireless Access Point (WAP) MR series	Cisco Meraki WAP
□ Cisco Meraki AccessPoint HTTP Detail	Meraki Wireless Access Point (WAP) MR series	Cisco Meraki WAP
□ Cisco Meraki AccessPoint Rogue SSID Detected	Meraki Wireless Access Point (WAP) MR series	Cisco Meraki WAP
□ Cisco Meraki AccessPoint Splash Authentication	Meraki Wireless Access Point (WAP) MR series	Cisco Meraki WAP
□ Cisco Meraki AccessPoint SSID Spoofing Detected	Meraki Wireless Access Point (WAP) MR series	Cisco Meraki WAP
□ Cisco Meraki AccessPoint Traffic Allowed	Meraki Wireless Access Point (WAP) MR series	Cisco Meraki WAP
□ Cisco Meraki AccessPoint Traffic Denied	Meraki Wireless Access Point (WAP) MR series	Cisco Meraki WAP
□ EventTracker All Events	EventTracker	EventTracker
□ F5 BIG IP LTM Configuration	F5 BIG-IP LTM 1600 Series, Tmos version 9.4.5 onwards	F5 BIG IP LTM
□ F5 BIG IP LTM Logoff	F5 BIG-IP LTM 1600 Series, Tmos version 9.4.5 onwards	F5 BIG IP LTM

Figure 440

- Select the object by clicking on the check box and click **Export**.

18.4 Importing Objects

1. To import objects, click **Import** .
   Import window opens.

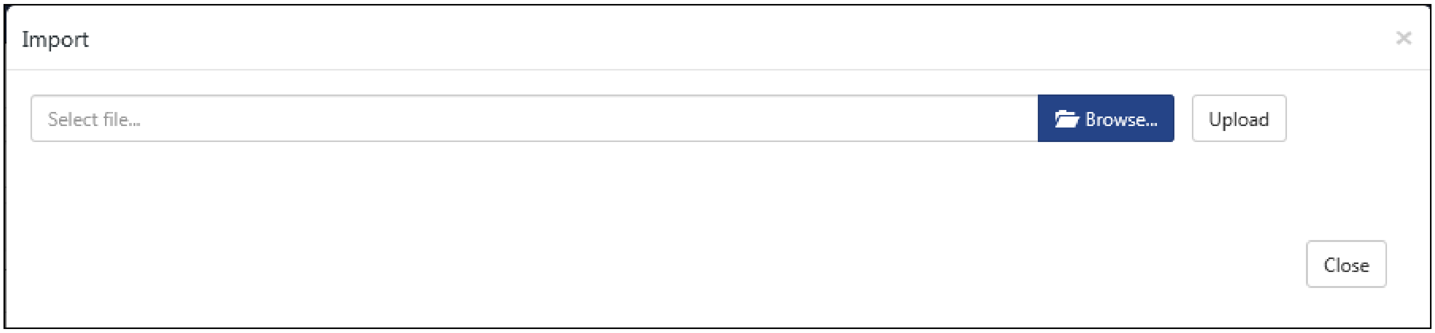
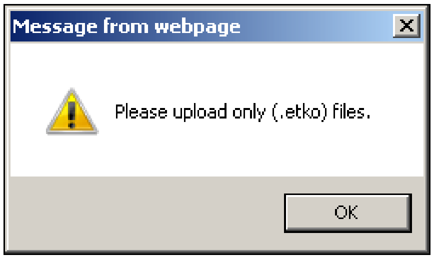


Figure 441

2. Click **Browse**, and then select the location of the file.

NOTE:

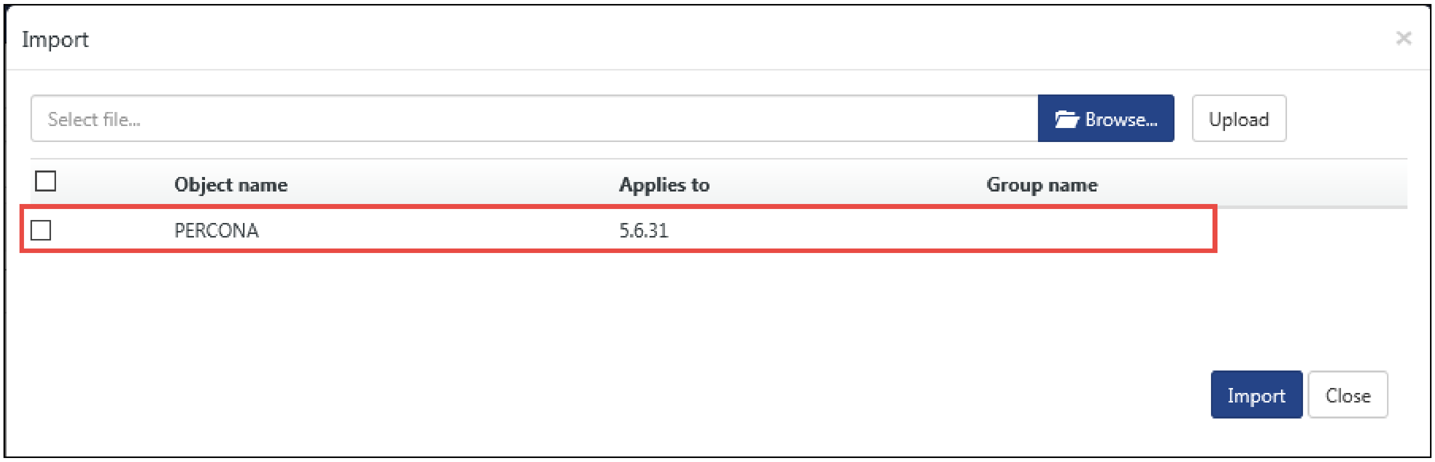
- The file to be uploaded should be in '.etko' format only otherwise an error message is displayed as shown below.



Please upload only (.etko) files.

Figure 442

3. Click **Upload**.

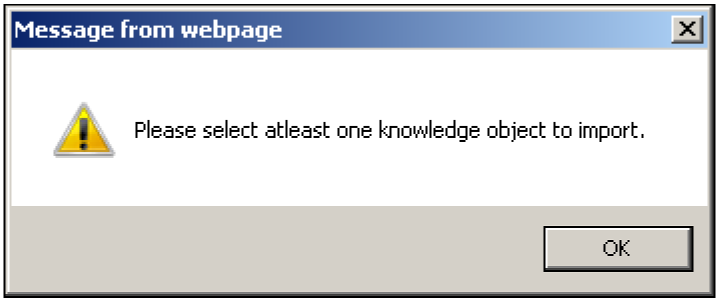


□	Object name	Applies to	Group name
□	PERCONA	5.6.31	

Figure 443

4. Select the **Object name** option.

NOTE: If the Object name is not selected an error message opens. Click **OK**.



Please select atleast one knowledge object to import.

Figure 444

5. Click **Merge/Overwrite**.

18.5 Editing Knowledge Objects

This option allows to activate/deactivate the default Knowledge Objects that have been provided. It is not possible to edit other details of default Knowledge Object. The user defined/created Knowledge Objects can be edited/updated.

1. To edit the Knowledge Object, click **Edit** .

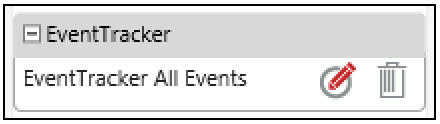
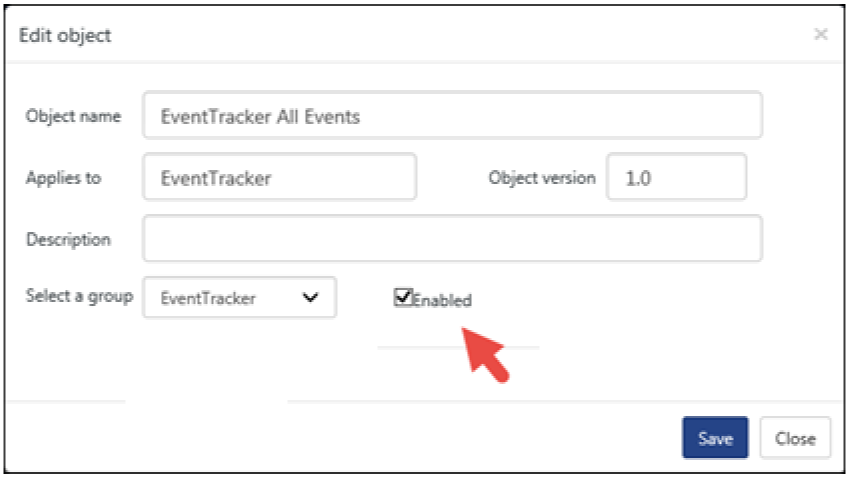


Figure 445

Edit object window opens.

2. To disable the Knowledge Object, select the **Enabled** option and then click **Save**.



Edit object

Object name: EventTracker All Events

Applies to: EventTracker

Object version: 1.0

Description:

Select a group: EventTracker

☑ Enabled

Figure 446

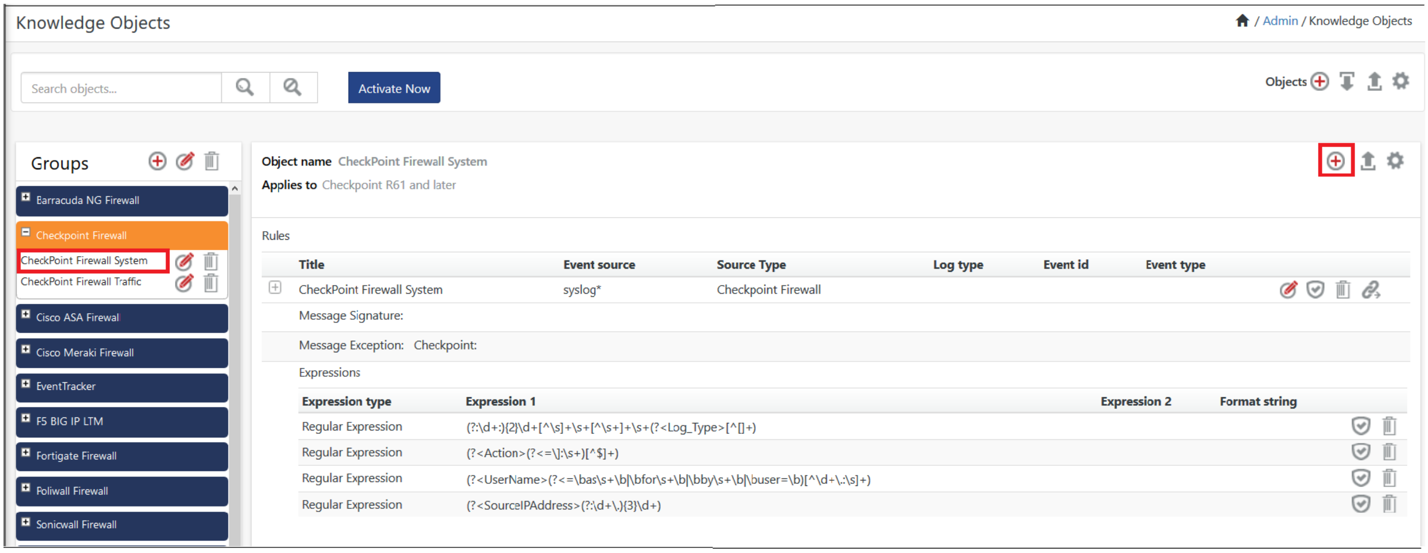
🗎 NOTE

However, you don’t have an option to edit and remove the Pre-Defined Knowledge Objects

18.6 Adding Rule to existing Knowledge Objects

1. Expand an existing Knowledge Object group and select the object.

   Ex: **CheckPoint Firewall System**



Knowledge Objects

Object name CheckPoint Firewall System

Applies to Checkpoint R61 and later

Rules

Title	Event source	Source Type	Log type	Event id	Event type
CheckPoint Firewall System	syslog*	Checkpoint Firewall			

Message Signature:

Message Exception: Checkpoint:

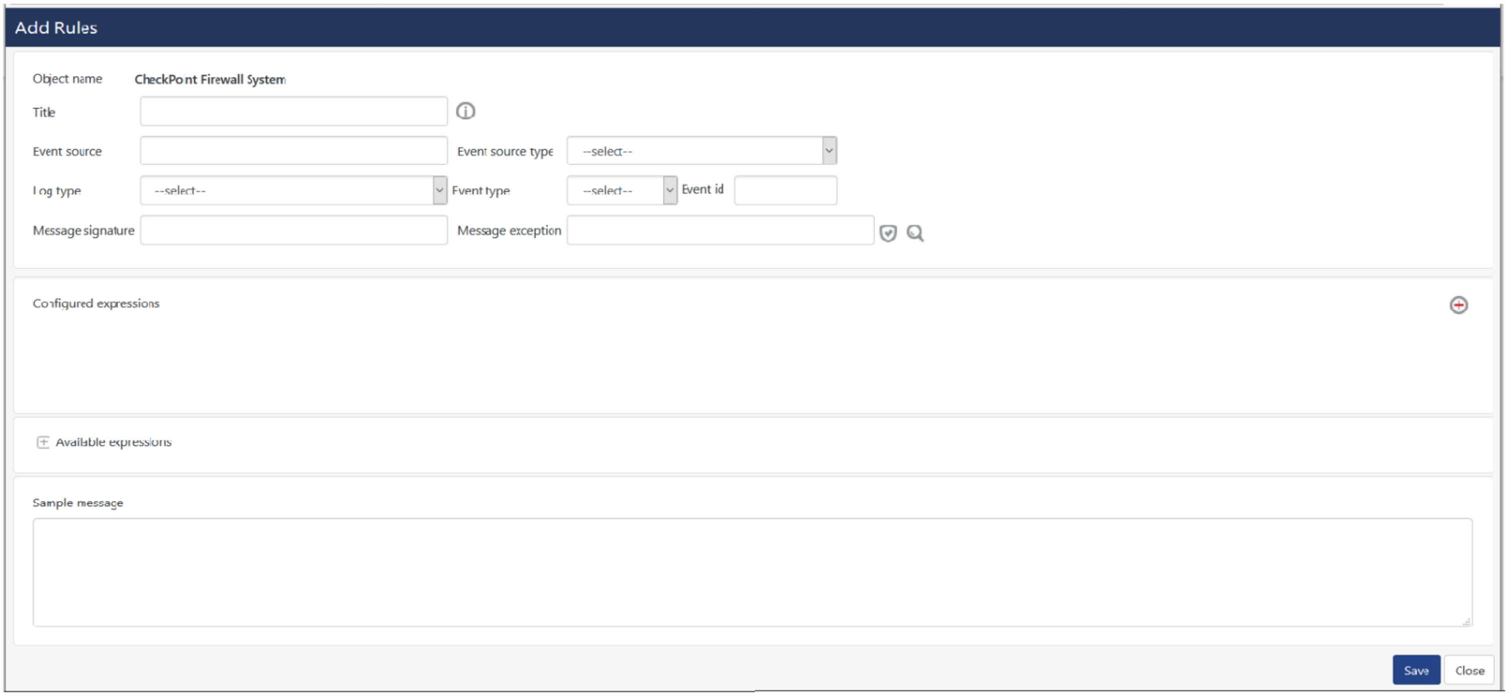
Expressions

Expression type	Expression 1	Expression 2	Format string
Regular Expression	(?:\d+:){2}\d+[^\s]+\s+[^\s+]+\s+(?<Log_Type>[^[]+)		
Regular Expression	(?<Action>(?<=\]:\s+)[^$]+)		
Regular Expression	(?<UserName>(?<=\bas\s+\b|\bfor\s+\b|\bby\s+\b|\buser=\b)[^\d+\.:\s]+)		
Regular Expression	(?<SourceIPAddress>(?:\d+\.){3}\d+)		

Figure 447

2. Click **Add Rule** ⊕.

   EventTracker Add Rules page opens.



Add Rules

Object name CheckPoint Firewall System

Title

Event source

Event source type --select--

Log type --select--

Event type --select--

Event id

Message signature

Message exception

Configured expressions

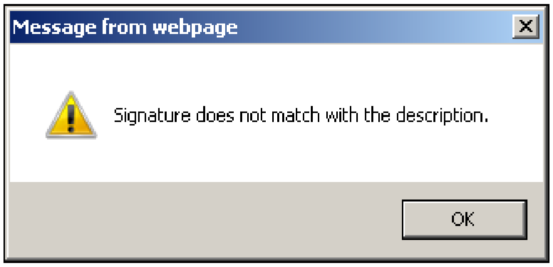
Available expressions

Sample message

Figure 448

3. Enter **Title, Log type, Event type, Event source, Event id, Message signature, Event source type, Message exception, Sample message**.

4. To verify message signature and exception, click **Verify signature & exception** ✓ .



Message from webpage

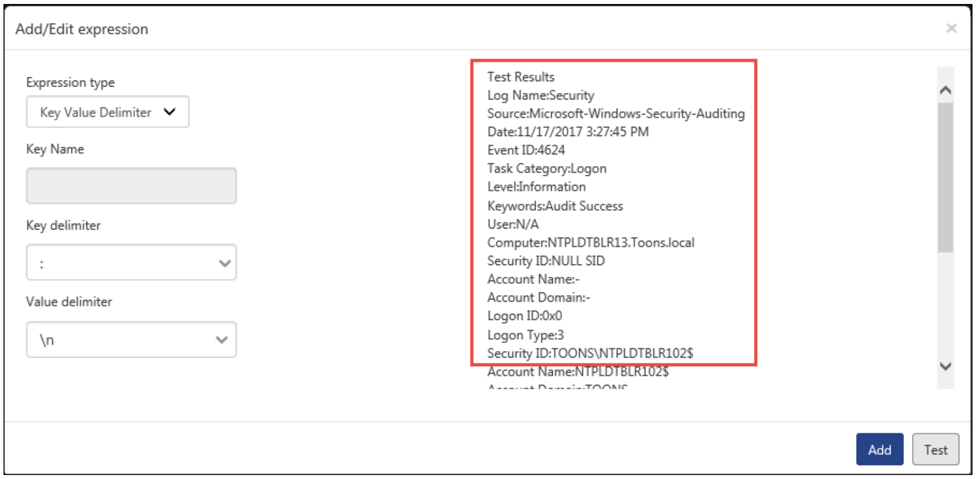
Signature does not match with the description.

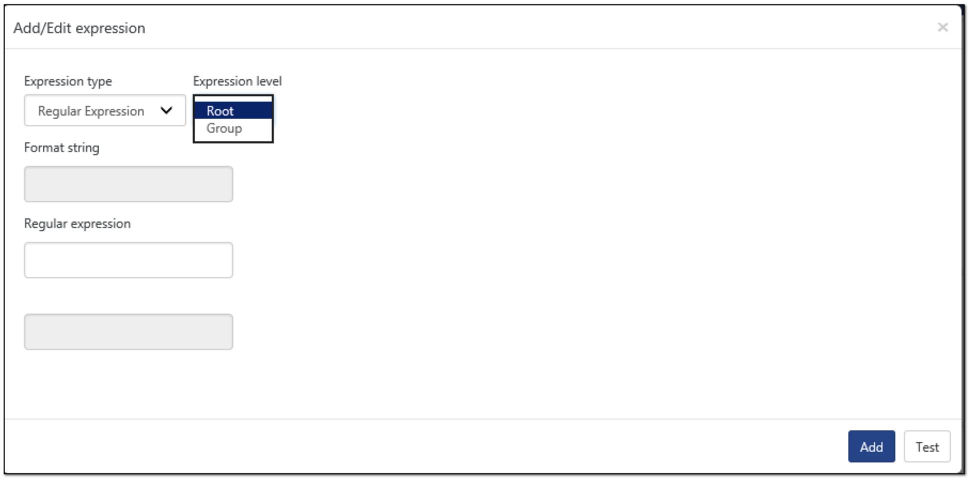
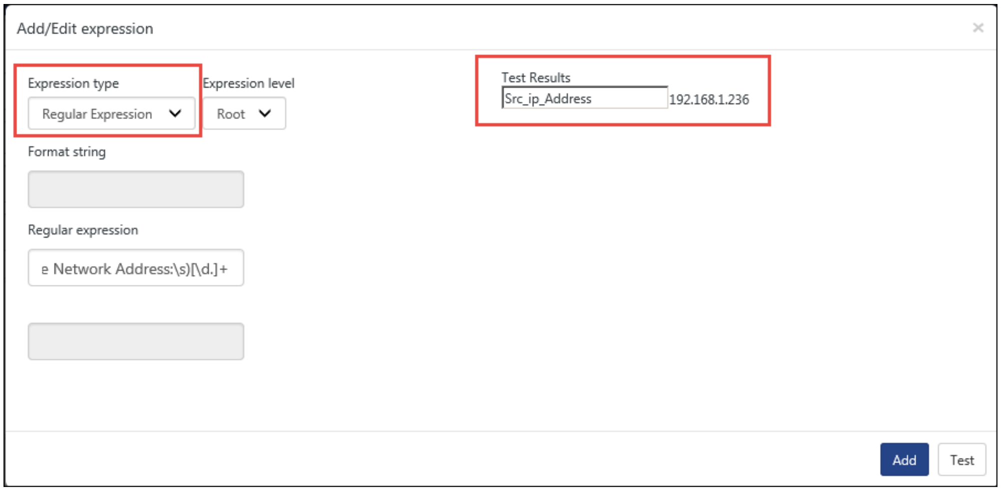
Figure 449

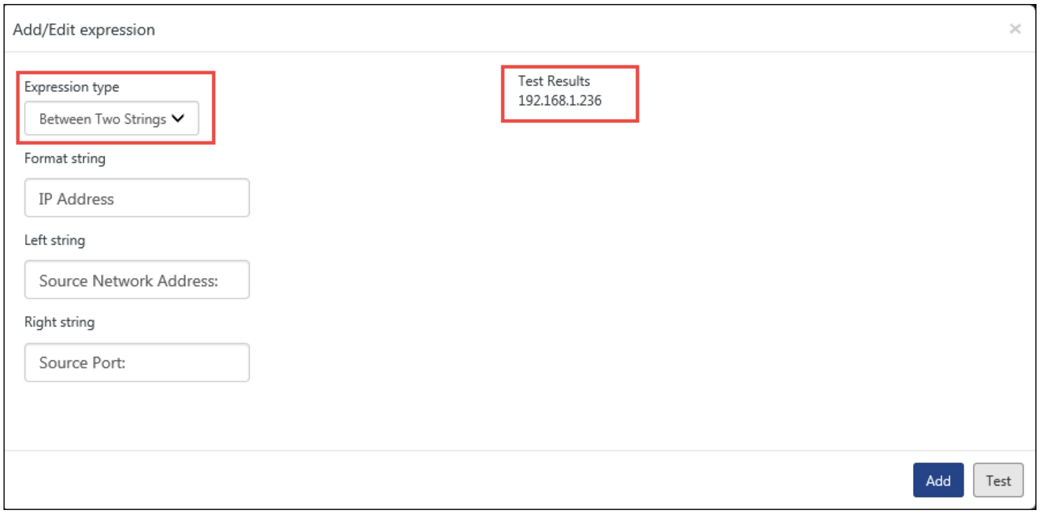
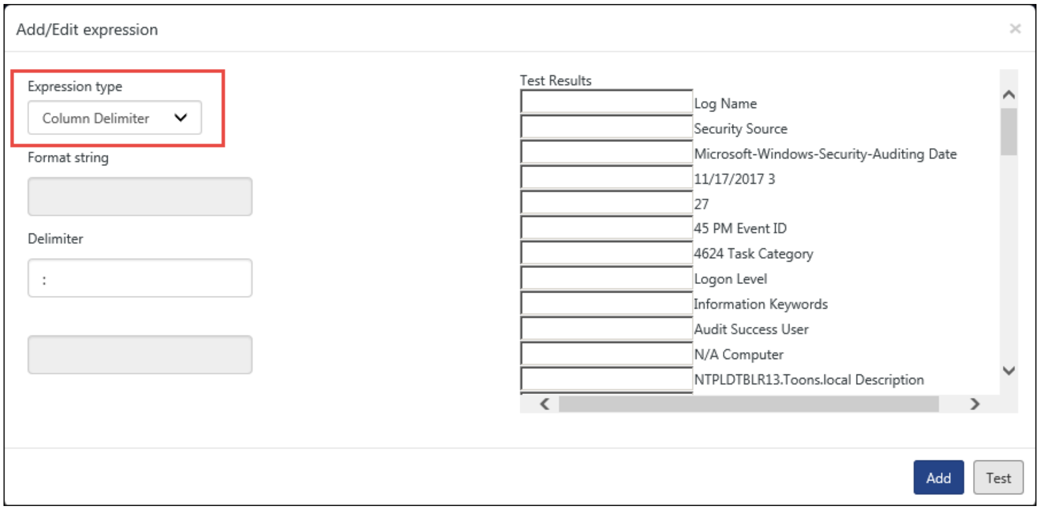
5. To perform a log search, click **Log search** 🔍 .

6. To add a regular expression, click **Add new expression** ⊕.

   NOTE: Without Sample message, you cannot add expression type.

Expression type	Description
Key Value Delimiter	Enter **Key delimiter** and **Value delimiter**. Click **Add**. To test the key value delimiter, click **Test**. Examples of Key Value delimiter is colon (:), hyphen (-), space (/s), newline (\n) etc.  Add/Edit expression Expression type: Key Value Delimiter Key Name: Key delimiter: : Value delimiter: \n Test Results Log Name:Security Source:Microsoft-Windows-Security-Auditing Date:11/17/2017 3:27:45 PM Event ID:4624 Task Category:Logon Level:Information Keywords:Audit Success User:N/A Computer:NTPLDTBLR13.Toons.local Security ID:NULL SID Account Name:- Account Domain:- Logon ID:0x0 Logon Type:3 Security ID:TOONS\NTPLDTBLR102$ Account Name:NTPLDTBLR102$ Account Domain:TOONS

Regular Expression	Enter a **Regular expression**, select **Expression level** and then click **Add**.  Add/Edit expression Expression type: Regular Expression Expression level: Root Group Format string Regular expression If ‘**Expression level**’ is selected as ‘**Root’,** then entire regular expression is considered to extract the values. If **Expression level** is selected as **Group**, then the regular expression is split into smaller groups for extraction. If **Format string** has not been provided. To test the Regular Expression, click **Test**.  Add/Edit expression Expression type: Regular Expression Expression level: Root Format string Regular expression: e Network Address:\s)[\d.]+ Test Results Src_ip_Address 192.168.1.236

Between Two Strings	Enter **Format String, Left String, Right String**. If required to test the expression, click **Test**. Click **Add**. For example:  Add/Edit expression Expression type: Between Two Strings Format string: IP Address Left string: Source Network Address: Right string: Source Port: Test Results 192.168.1.236
Column Delimiter	Enter column **Delimiter** and then click **Add**. To test the column delimiter, click **Test**. For example:  Add/Edit expression Expression type: Column Delimiter Format string: Delimiter: : Test Results Log Name Security Source Microsoft-Windows-Security-Auditing Date 11/17/2017 3 27 45 PM Event ID 4624 Task Category Logon Level Information Keywords Audit Success User N/A Computer NTPLDTBLR13.Toons.local Description

18.7 Deleting Knowledge Objects

The predefined Knowledge Objects cannot be deleted. The Knowledge Object created by the user can be deleted by him/her only.

1. To delete a knowledge object, click **Delete** 🗑.

Test

Figure 450

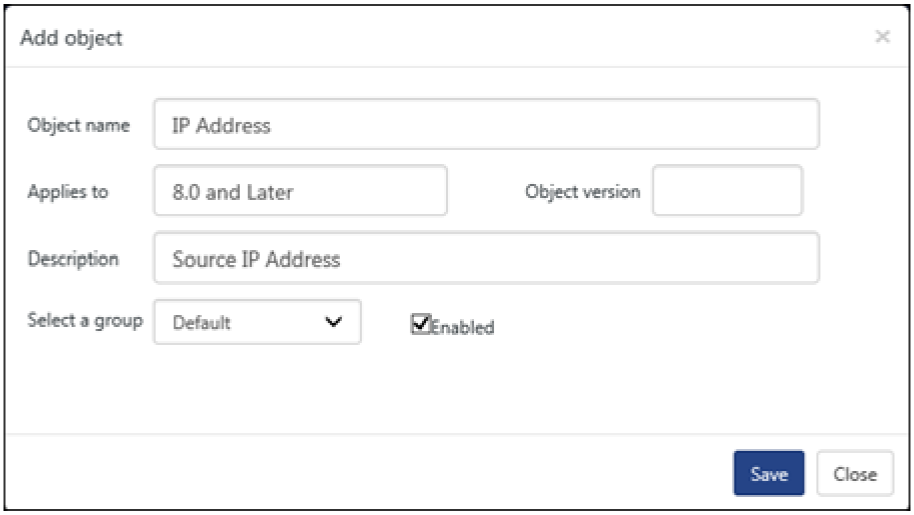
Message from webpage opens.

2. Select **OK**.

18.7.1 Example to create Knowledge Object

Let us consider an example to add IP Address as a Knowledge Object.

1. Click **Add Object** icon.
2. Enter the relevant data; click **Enabled** option to activate the Knowledge Object.
3. Click **Save**.



Add object

Object name: IP Address

Applies to: 8.0 and Later

Object version:

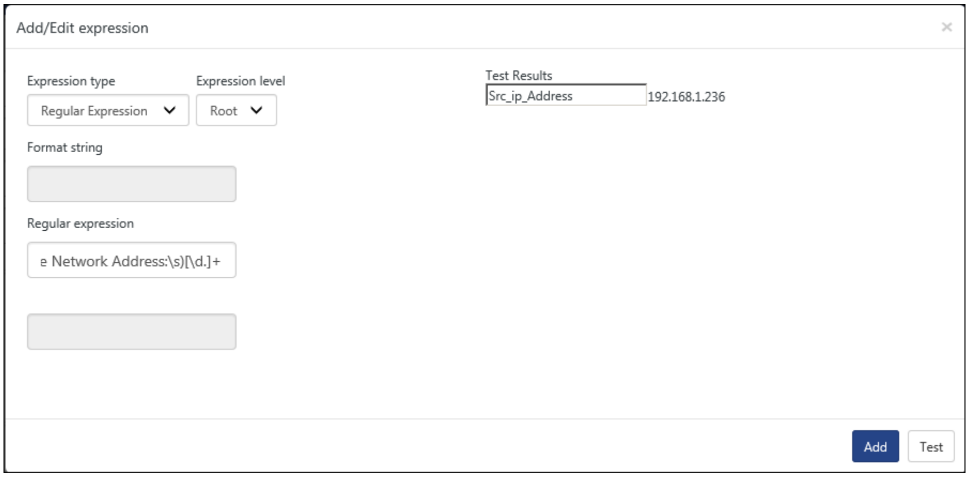
Description: Source IP Address

Select a group: Default

☑ Enabled

Figure 451

4. Click **Add Rule** ⊕.
5. Enter **Title, Event source, Message signature, Event source type and Sample Message**.
   If **Log type, Event type, Event id, Message exception** is known, then enter the information.
6. Click **Add new expression** ⊕.
   Add/Edit expression window opens.
7. Select **Expression type** and **Expression level** as required.
   In our example, we are selecting Regular Expression as Remote Address:\s[\d.]+. Enter the **Regular Expression**, and then click **Test**.
   Test results opens.



Add/Edit expression

Expression type: Regular Expression

Expression level: Root

Format string

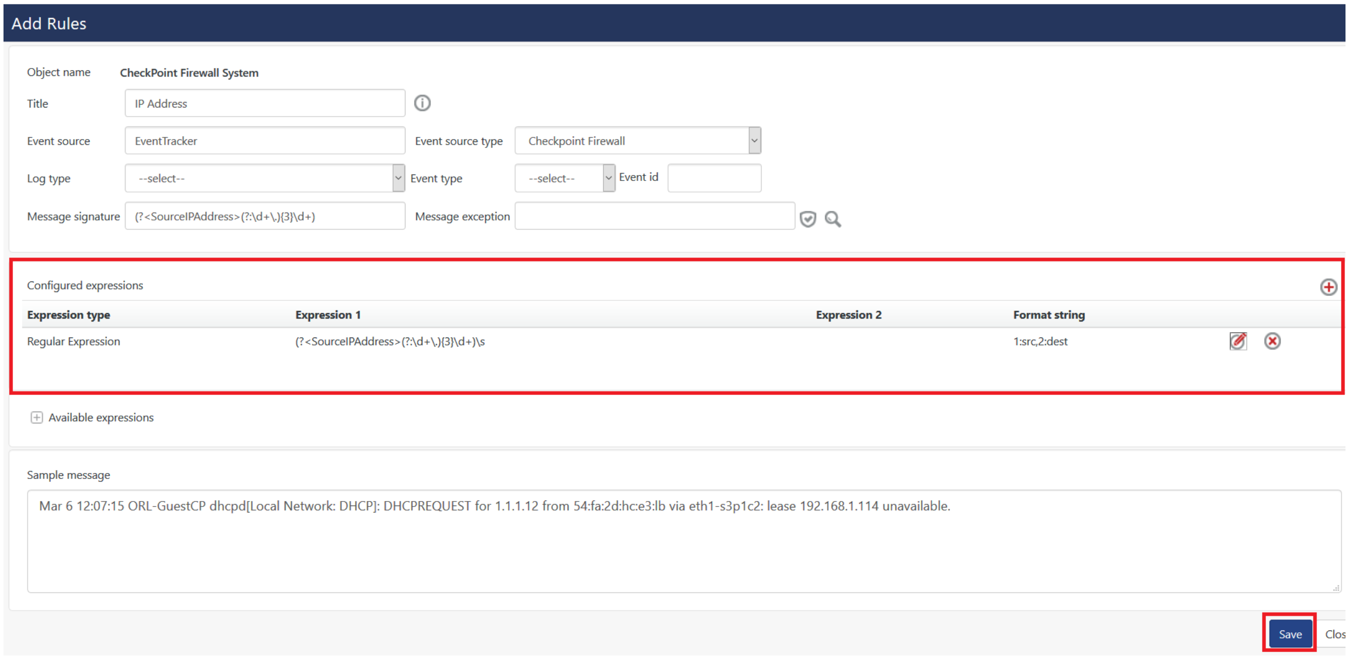
Regular expression: e Network Address:\s)[\d.]+

Test Results

Src_ip_Address	192.168.1.236

Figure 452

8. Enter a name for **Test Results** box as it is the Format String.
9. Click **Add**.



Add Rules

Object name: CheckPoint Firewall System

Title: IP Address

Event source: EventTracker

Event source type: Checkpoint Firewall

Log type: --select--

Event type: --select--

Event id

Message signature: (?<SourceIPAddress>(?:\d+\.){3}\d+)

Message exception

Configured expressions

Expression type	Expression 1	Expression 2	Format string
Regular Expression	(?<SourceIPAddress>(?:\d+\.){3}\d+)\s		1:src,2:dest

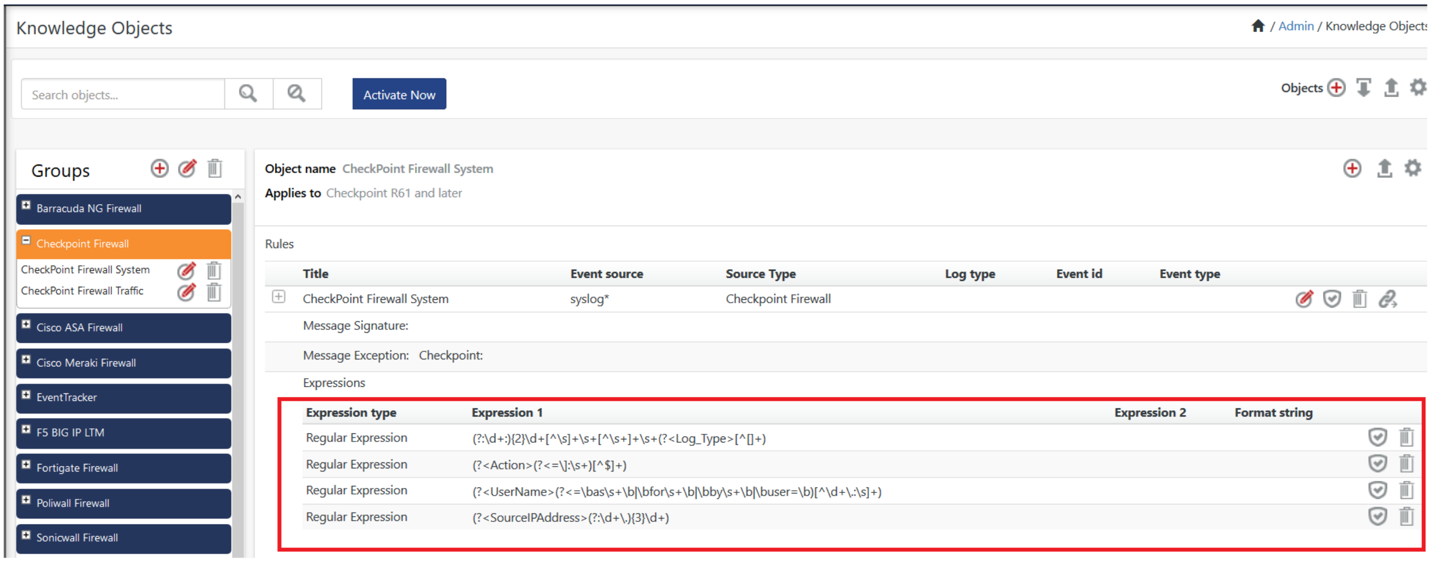
Available expressions

Sample message

Mar 6 12:07:15 ORL-GuestCP dhcpd[Local Network: DHCP]: DHCPREQUEST for 1.1.1.12 from 54:fa:2d:hc:e3:lb via eth1-s3p1c2: lease 192.168.1.114 unavailable.

Figure 453

10. To edit the configured expression, click **Edit** ✎.
11. To delete the configured expression, click **Remove** ☒.
12. Click **Save**.



Object name CheckPoint Firewall System

Applies to Checkpoint R61 and later

Rules

Title	Event source	Source Type	Log type	Event id	Event type
CheckPoint Firewall System	syslog*	Checkpoint Firewall			

Message Signature:

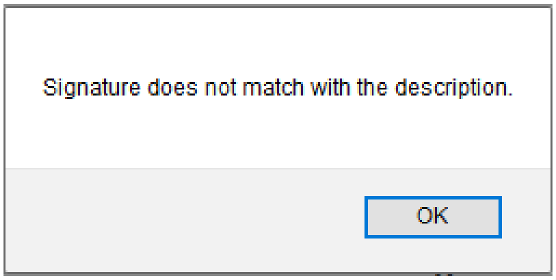
Message Exception: Checkpoint:

Expressions

Expression type	Expression 1	Expression 2	Format string
Regular Expression	(?:\d+:){2}\d+[^\s]+\s+[^\s+]+\s+(?<Log_Type>[^[]+)		
Regular Expression	(?<Action>(?<=\]:\s+)[^$]+)		
Regular Expression	(?<UserName>(?<=\bas\s+\b|\bfor\s+\b|\bby\s+\b|\buser=\b)[^\d+\.:\s]+)		
Regular Expression	(?<SourceIPAddress>(?:\d+\.){3}\d+)		

Figure 454

13. In **Rules** pane, click **Verify Signature** ✓ .

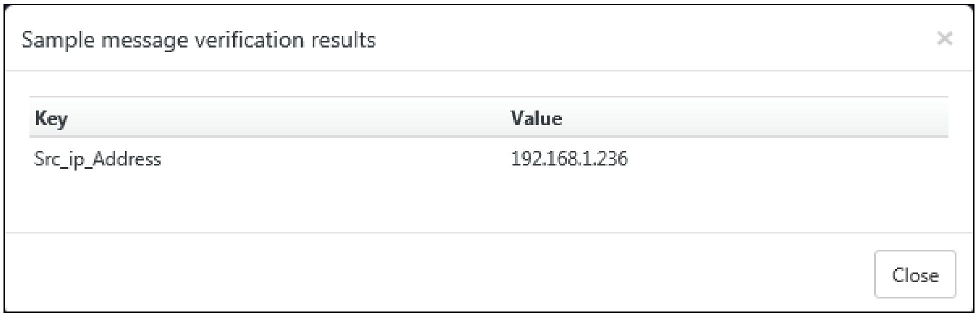


Signature does not match with the description.

Figure 455

14. In **Expressions** pane, click **Verify Signature** ✓ .

Sample message verification results opens.



Sample message verification results

Key	Value
Src_ip_Address	192.168.1.236

Figure 456

18.8 Conditional Tag Configuration for Knowledge Objects Search

EventTracker v9.3 introduces optimized Knowledge Objects search and improved mapping capabilities to speed search performance.

Conditional tagging helps to users to perform efficient log search across all log sources.

With EventTracker v9.3, the user can now use Configured Conditional tags to identify the values which they are looking in log search result from across all the log sources (Knowledge Objects -KOs).

The below Knowledge Objects have the updated conditional tag configuration.

- Barracuda NG Firewall
- Checkpoint Firewall
- Cisco ASA Firewall
- Cisco Meraki Firewall
- EventTracker
- Fortigate Firewall
- Poliwall Firewall
- Sonicwall Firewall
- Sophos UTM Firewall
- Sophos XG Firewall
- Untangle Firewall
- Watchguard XTM Firewall
- Windows

Accessing the Conditional Tag Configuration

1. Log into EventTracker, go to Admin and select knowledge objects.

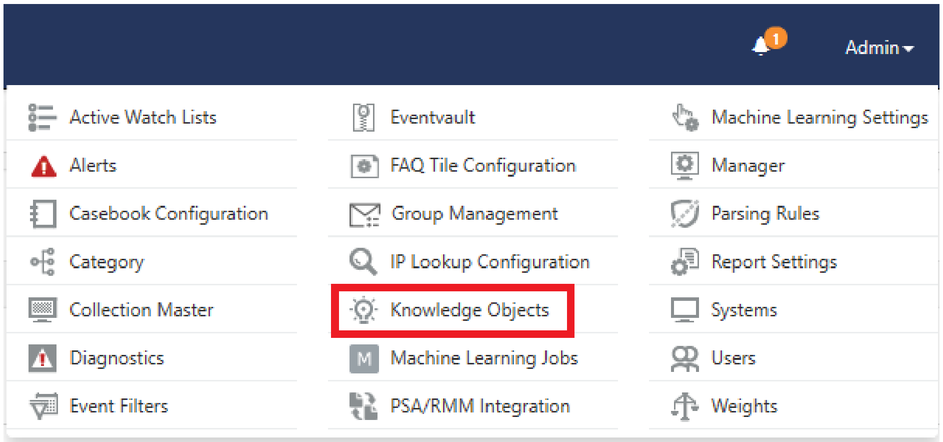
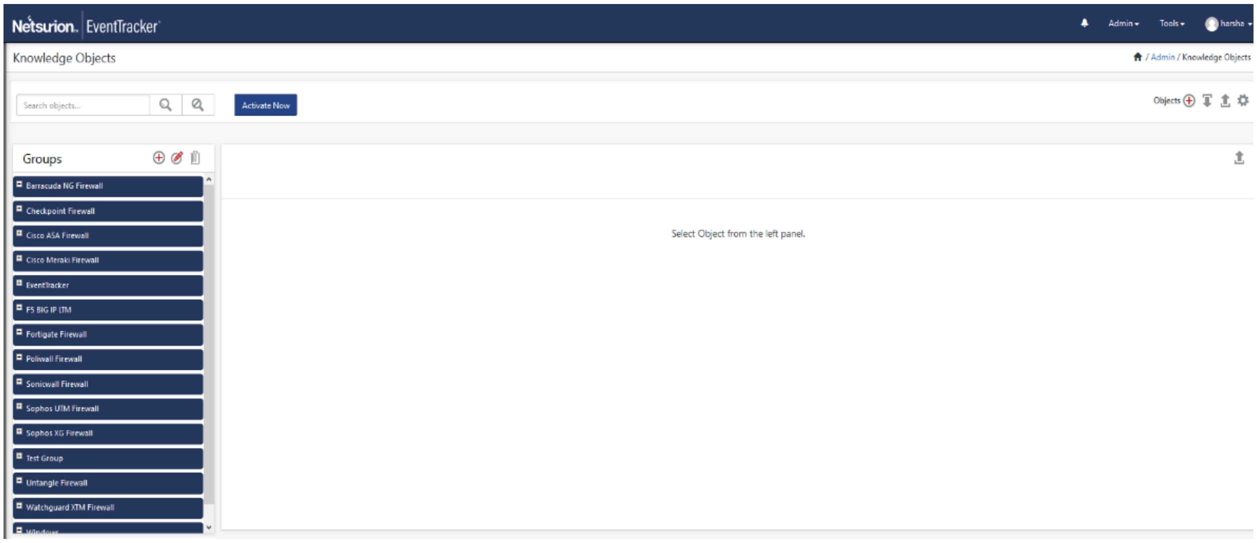


Figure 457

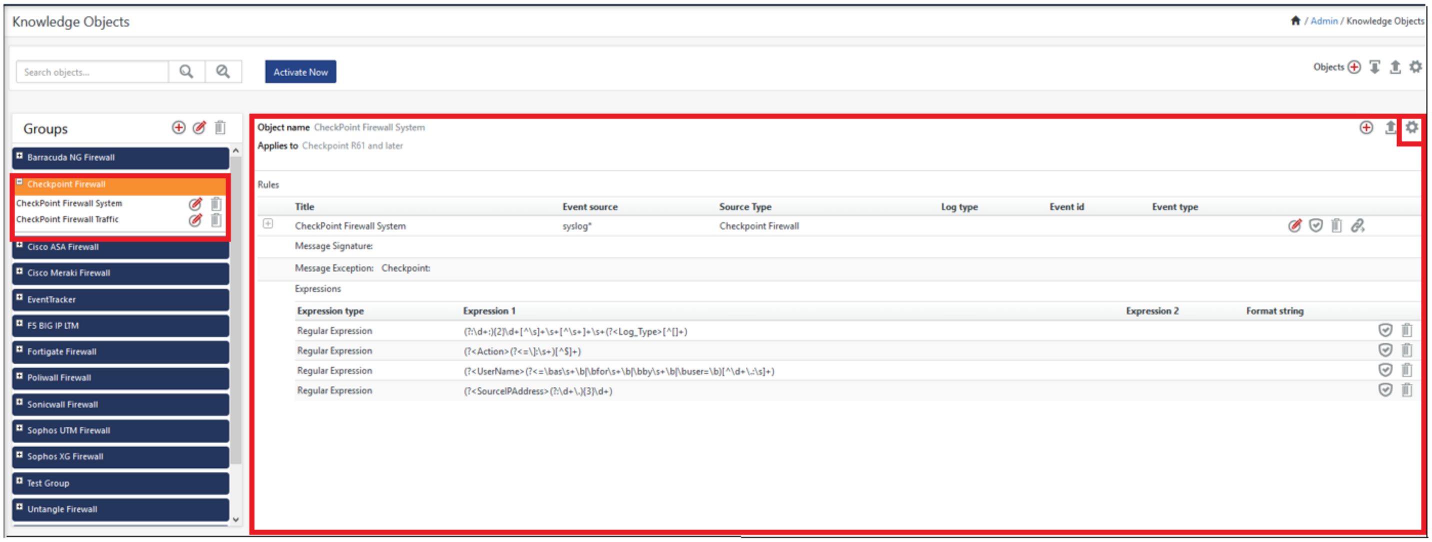
Knowledge objects page opens.



Select Object from the left panel.

Figure 458

2. Click on **Groups** to expand, here **Checkpoint Firewall** is taken as an example, and then click on the object **CheckPoint Firewall System**.
   CheckPoint Firewall System pane is displayed on the right side.
3. Click on the CIM Mapping icon ⚙, located at the right top corner of the right pane.



Object name CheckPoint Firewall System
Applies to Checkpoint R61 and later

Rules

Title	Event source	Source Type	Log type	Event id	Event type
CheckPoint Firewall System	syslog*	Checkpoint Firewall			

Message Signature:

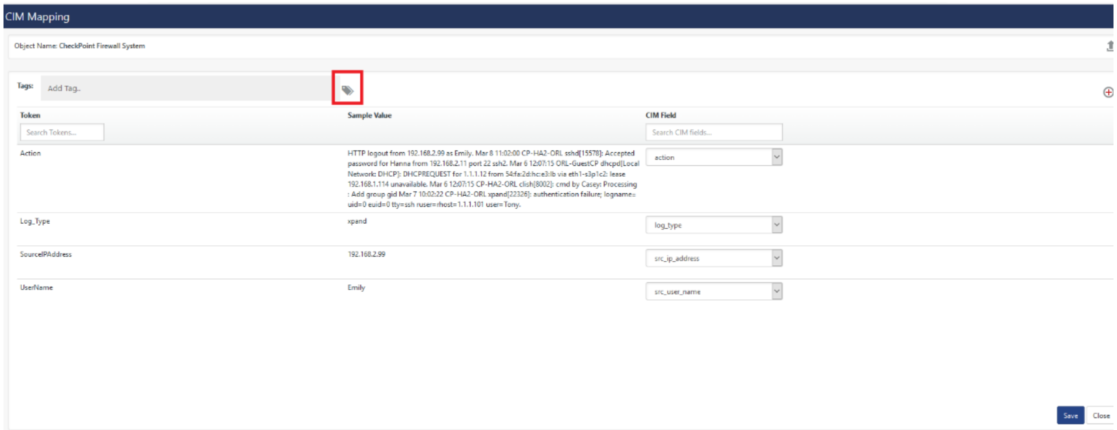
Message Exception: Checkpoint:

Expressions

Expression type	Expression 1	Expression 2	Format string
Regular Expression	(?:\d+:){2}\d+[^\s]+\s+[^\s+]+\s+(?<Log_Type>[^[]+)		
Regular Expression	(?<Action>(?<=\]:\s+)[^$]+)		
Regular Expression	(?<UserName>(?<=\bas\s+\b|\bfor\s+\b|\bby\s+\b|\buser=\b)[^\d+\.:\s]+)		
Regular Expression	(?<SourceIPAddress>(?:\d+\.){3}\d+)		

Figure 459

CIM Mapping page opens.



CIM Mapping

Object Name: CheckPoint Firewall System

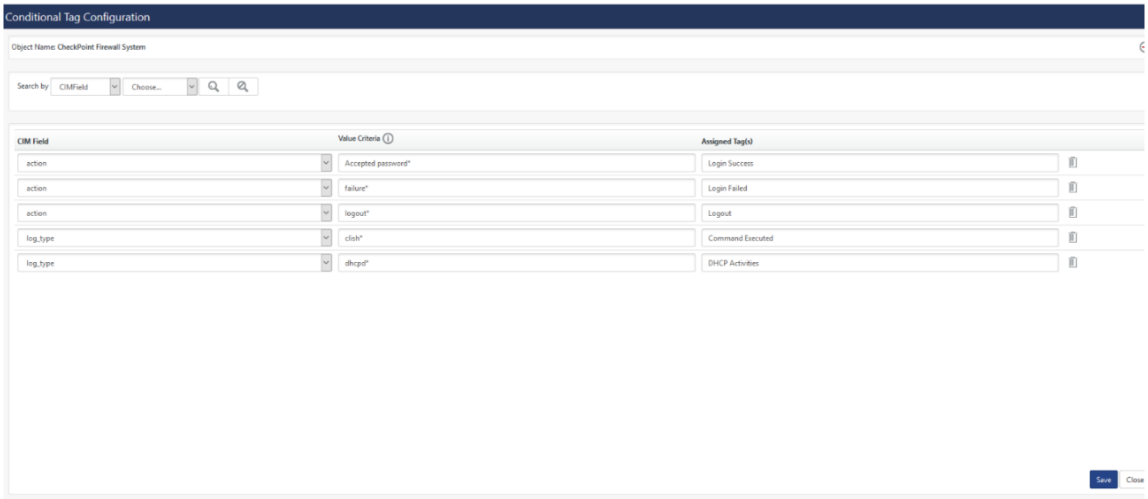
Tags: Add Tag..

Token	Sample Value	CIM Field
Action	HTTP logout from 192.168.2.99 as Emily. Mar 8 11:02:00 CP-HA2-ORL sshd[15578]: Accepted password for Hanna from 192.168.2.11 port 22 ssh2. Mar 6 12:07:15 ORL-GuestCP dhcpd[Local Network: DHCP]: DHCPREQUEST for 1.1.1.12 from 54:fa:2d:hc:e3:lb via eth1-s3p1c2: lease 192.168.1.114 unavailable. Mar 6 12:07:15 CP-HA2-ORL clish[8002]: cmd by Casey: Processing : Add group gid Mar 7 10:02:22 CP-HA2-ORL xpand[22326]: authentication failure; logname= uid=0 euid=0 tty=ssh ruser=rhost=1.1.1.101 user=Tony.	action
Log_Type	xpand	log_type
SourceIPAddress	192.168.2.99	src_ip_address
UserName	Emily	src_user_name

Figure 460

4. Click on the Configure Conditional Tag(s) icon.

5. Conditional Tag Configuration page opens.



Conditional Tag Configuration

Object Name: CheckPoint Firewall System

Search by CIMField Choose...

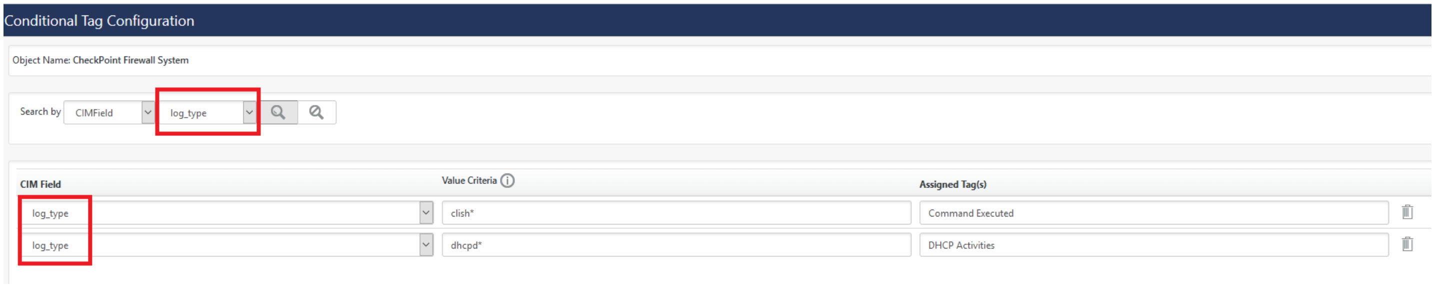
CIM Field	Value Criteria	Assigned Tag(s)
action	Accepted password*	Login Success
action	failure*	Login Failed
action	logout*	Logout
log_type	clish*	Command Executed
log_type	dhcpd*	DHCP Activities

Figure 461

You can search by CIM Field and value criteria. Accordingly, the results appear.

CIM Fields available in knowledge objects are shown.

1. In the **Search by** field, let us choose **CIM Field** and choose the **log_type** and then click **search**.
2. All the **CIM Fields** related to **log_type** results appear.


Conditional Tag Configuration

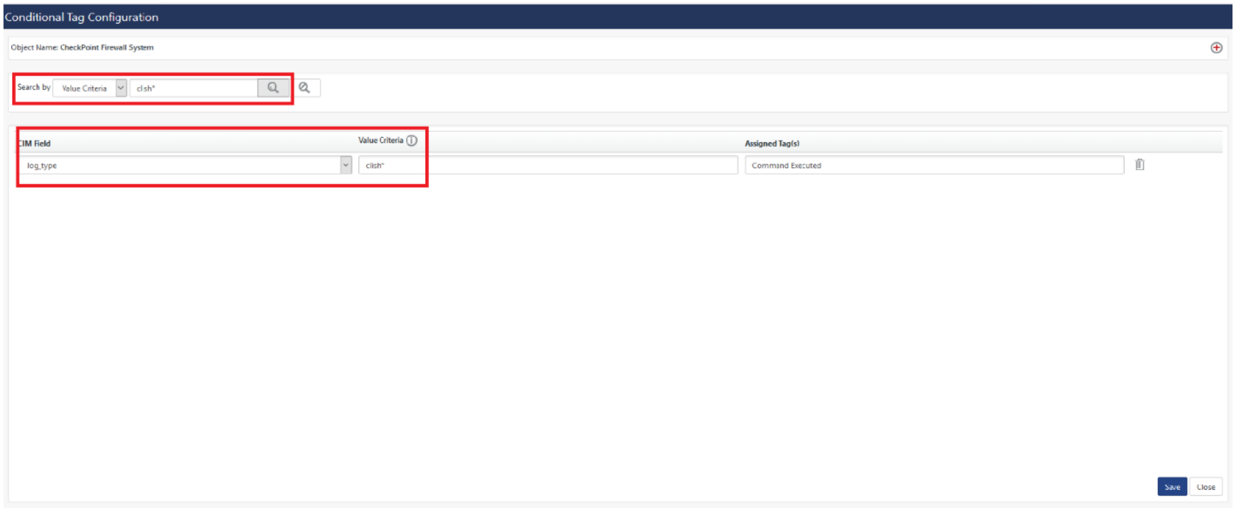
Object Name: CheckPoint Firewall System

Search by CIMField log_type

CIM Field	Value Criteria	Assigned Tag(s)
log_type	clish*	Command Executed
log_type	dhcpd*	DHCP Activities

Figure 462

3. Choose **Value Criteria** in the **Search by** and type in the value criteria **clish*.**
4. The results with **CIM Field** log_type and value criteria **clish* is** opens**.**


Conditional Tag Configuration

Object Name: CheckPoint Firewall System

Search by Value Criteria clish*

CIM Field	Value Criteria	Assigned Tag(s)
log_type	clish*	Command Executed

Figure 463

19. Manager

In this chapter, you will learn how to use:

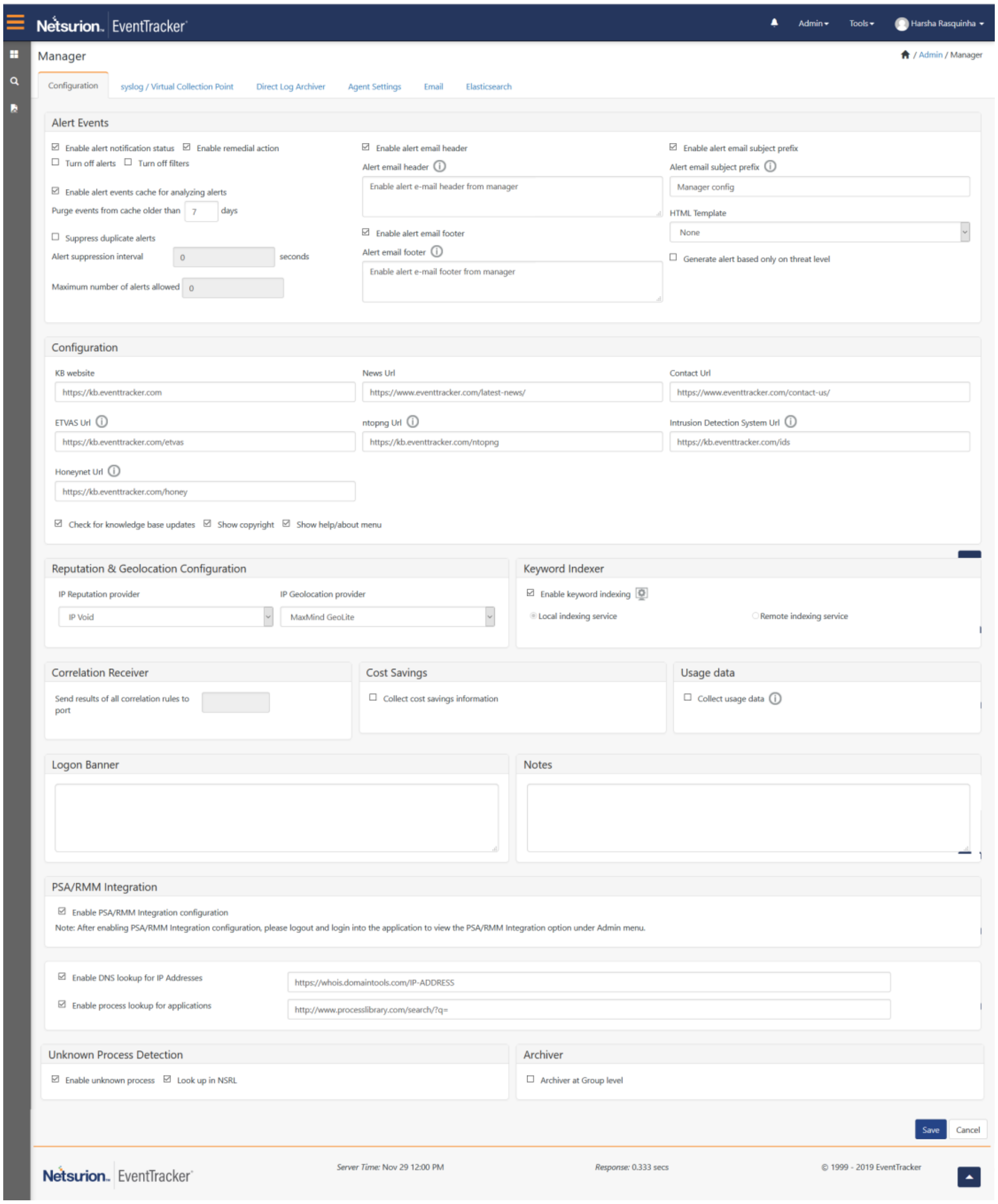
- Configure Alert Events
- Syslog/Virtual Collection Point
- Direct Log Archiver
- Agent Settings
- E-mail Configuration
- Collection Master Ports
- Elasticsearch

19.1 Configuring - Alert Events

19.1.1 Enabling Alert Notification

This option helps you track success/failure alert notification status.

1. To enable alert notification, click the **Admin**, and then click **Manager**.
2. Click **Configuration** tab, if not selected.



Alert Events

☑ Enable alert notification status ☑ Enable remedial action
☐ Turn off alerts ☐ Turn off filters
☑ Enable alert events cache for analyzing alerts
Purge events from cache older than 7 days
☐ Suppress duplicate alerts
Alert suppression interval 0 seconds
Maximum number of alerts allowed 0

☑ Enable alert email header
Alert email header: Enable alert e-mail header from manager
☑ Enable alert email footer
Alert email footer: Enable alert e-mail footer from manager

☑ Enable alert email subject prefix
Alert email subject prefix: Manager config
HTML Template: None
☐ Generate alert based only on threat level

Configuration

KB website: https://kb.eventtracker.com
News Url: https://www.eventtracker.com/latest-news/
Contact Url: https://www.eventtracker.com/contact-us/
ETVAS Url: https://kb.eventtracker.com/etvas
ntopng Url: https://kb.eventtracker.com/ntopng
Intrusion Detection System Url: https://kb.eventtracker.com/ids
Honeynet Url: https://kb.eventtracker.com/honey
☑ Check for knowledge base updates ☑ Show copyright ☑ Show help/about menu

Reputation & Geolocation Configuration

IP Reputation provider: IP Void
IP Geolocation provider: MaxMind GeoLite

Keyword Indexer

☑ Enable keyword indexing
● Local indexing service ○ Remote indexing service

Correlation Receiver

Send results of all correlation rules to port

Cost Savings

☐ Collect cost savings information

Usage data

☐ Collect usage data

Logon Banner

Notes

PSA/RMM Integration

☑ Enable PSA/RMM Integration configuration
Note: After enabling PSA/RMM Integration configuration, please logout and login into the application to view the PSA/RMM Integration option under Admin menu.

☑ Enable DNS lookup for IP Addresses: https://whois.domaintools.com/IP-ADDRESS
☑ Enable process lookup for applications: http://www.processlibrary.com/search/?q=

Unknown Process Detection

☑ Enable unknown process ☑ Look up in NSRL

Archiver

☐ Archiver at Group level

Server Time: Nov 29 12:00 PM
Response: 0.333 secs
© 1999 - 2019 EventTracker

Figure 464

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**.

19.1.2 Purging 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.

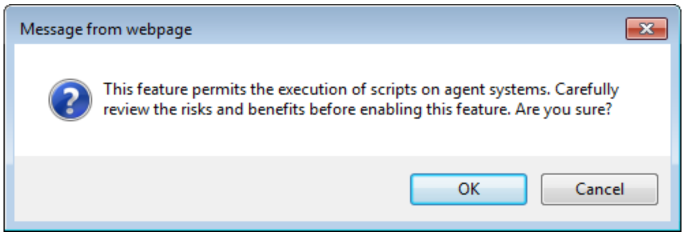
1) To purge alert events cache, in **Manager Configuration** page, click the **Configuration** tab.
2) Select the **Enable Alert Events Cache for Analyzing Alerts** checkbox, if not selected by default.
3) EventTracker enable **Purge events from cache older than – days** field, if not selected by default.
4) Type the duration in **Purge events from cache older than – days** field.
5) Click **Save**.

19.1.3 Enabling 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 opens the Caution dialog box.



Message from webpage

This feature permits the execution of scripts on agent systems. Carefully review the risks and benefits before enabling this feature. Are you sure?

Figure 465

3) Click **OK**, and then click **Save**.

19.1.4 Suppressing 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.

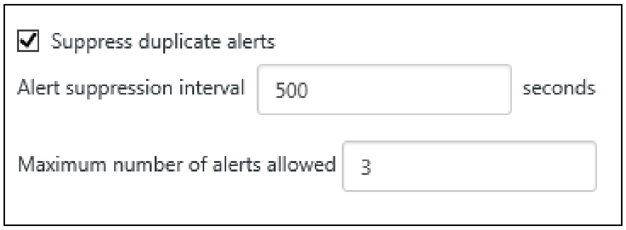
In case the multiple instances of an event with a configured alert are received in a short period of time then many alerts will be generated, this could confuse the user.

'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.



☑ Suppress duplicate alerts

Alert suppression interval: 500 seconds

Maximum number of alerts allowed: 3

Figure 466

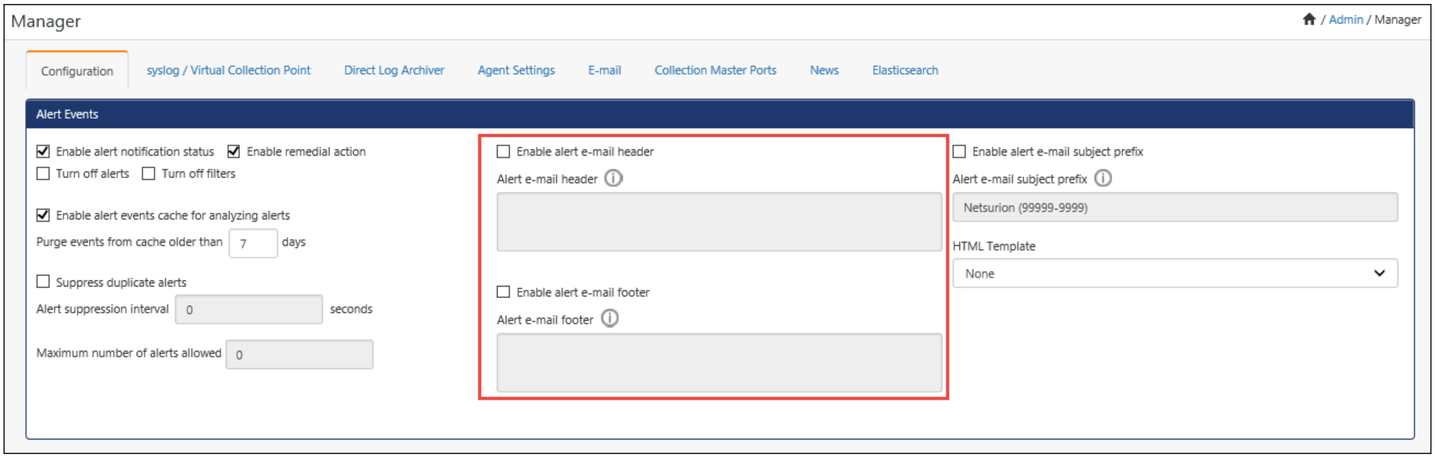
EventTracker enables the **Alert suppression interval** and **Maximum number of alerts allowed** fields.

3) Enter appropriate data and then click **Save**.

19.1.5 Enabling 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 custom email footer also for the 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.



Manager

Home / Admin / Manager

Alert Events

☑ Enable alert notification status ☑ Enable remedial action

□ Turn off alerts □ Turn off filters

☑ Enable alert events cache for analyzing alerts

Purge events from cache older than 7 days

□ Suppress duplicate alerts

Alert suppression interval 0 seconds

Maximum number of alerts allowed 0

□ Enable alert e-mail header

Alert e-mail header

□ Enable alert e-mail footer

Alert e-mail footer

□ Enable alert e-mail subject prefix

Alert e-mail subject prefix: Netsurion (99999-9999)

HTML Template: None

Figure 467

3) To add the **Alert Header/Footer**, check the options and add the header/footer in the respective fields and then click **Save**.

19.1.6 Configuring 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.
3) Click **Save**.

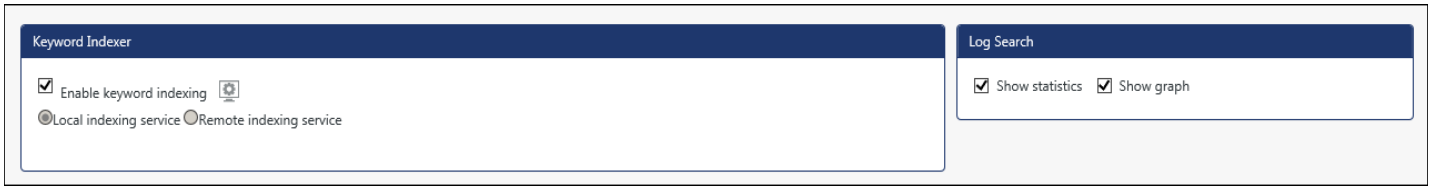
NOTE

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 Event Correlator.

19.1.7 Configuring 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.



Keyword Indexer

☑ Enable keyword indexing

● Local indexing service ○ Remote indexing service

Log Search

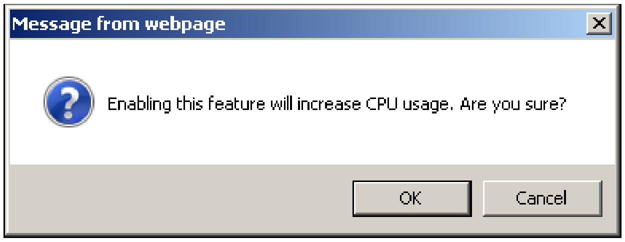
☑ Show statistics ☑ Show graph

Figure 468

NOTE

If the user(s) disable the Sparse matrix indexing option, it will not create the sparse matrix files for indexing.

EventTracker opens caution dialog box.

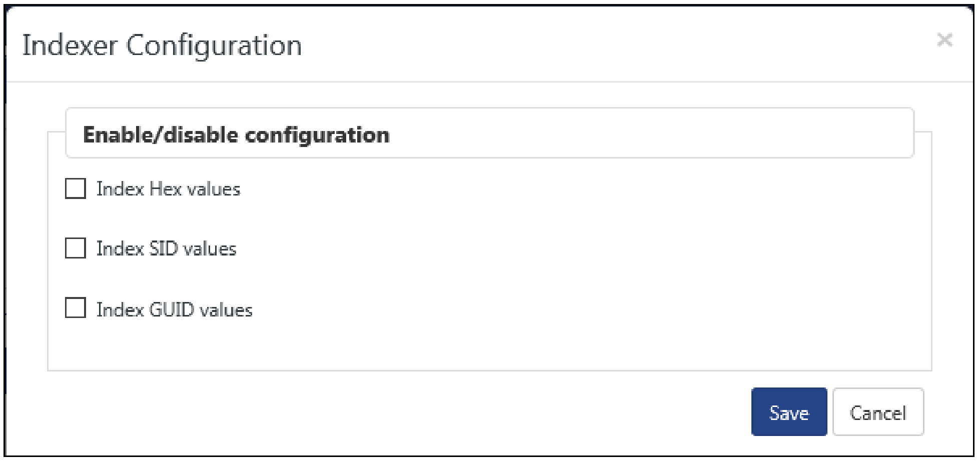


Message from webpage

Enabling this feature will increase CPU usage. Are you sure?

Figure 469

3) Click **Settings** to make changes in Indexer Configuration.
The Indexer Configuration window opens.



Indexer Configuration

Enable/disable configuration

□ Index Hex values

□ Index SID values

□ Index GUID values

Figure 470

4) Select required option and click **Save**.

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.
- Clear the Enable Keyword Indexing checkbox if the ‘Keyword Indexer’ hogs the system resources.

Field	Description
Local Indexing service	Keyword indexing process is carried out on the local machine. You are not allowed to change this option.
Remote Indexing service	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.
Show statistic	Show/hide the statistics in the log search page. Clear the Show statistic checkbox to view only graphs in the log search page.
Show graph	Show/hide the graphs in the log search page. Clear the Show graph checkbox to view only statistics in the log search page.

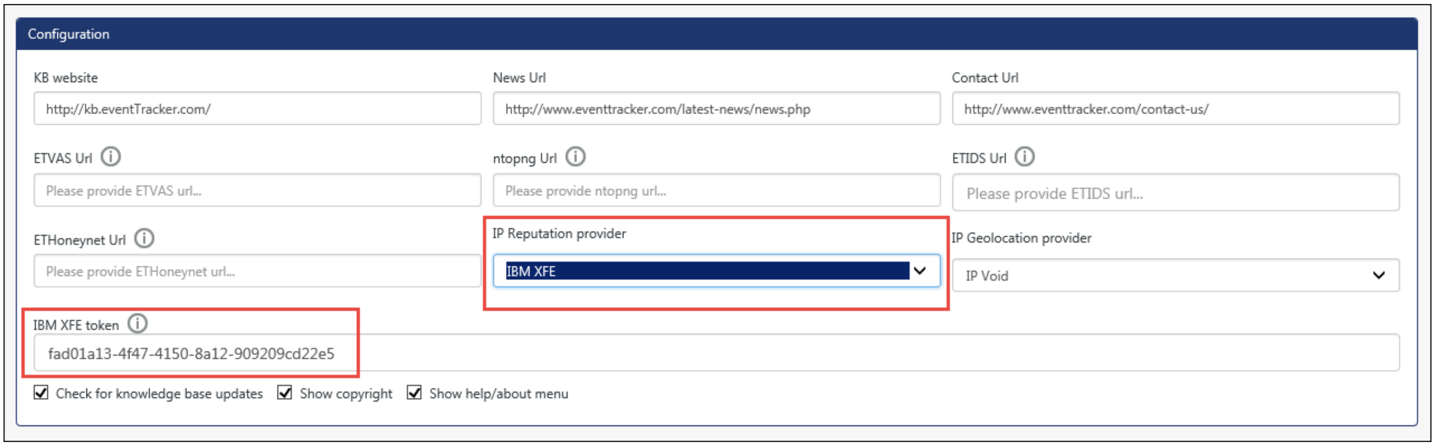
Table 57

> 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.

19.1.8 Configuration pane

This option enables you to configure 'EventTracker Knowledge Base' Web site.

1) In **Configuration** pane, select/enter required data.
   Also, news URL/contact URL/ETVAS URL/ntopng URL/ETIDS URL is configurable.
   The user will also be able to configure ETHoneynet URL.



Configuration

KB website: http://kb.eventTracker.com/
News Url: http://www.eventtracker.com/latest-news/news.php
Contact Url: http://www.eventtracker.com/contact-us/
ETVAS Url: Please provide ETVAS url...
ntopng Url: Please provide ntopng url...
ETIDS Url: Please provide ETIDS url...
ETHoneynet Url: Please provide ETHoneynet url...
IP Reputation provider: IBM XFE
IP Geolocation provider: IP Void
IBM XFE token: fad01a13-4f47-4150-8a12-909209cd22e5

☑ Check for knowledge base updates ☑ Show copyright ☑ Show help/about menu

Figure 471

1) Select the **IP Reputation Provider** from the drop-down option (**IP Void/IBM XFE/Borderware**).

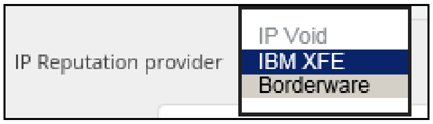


Figure 472

🗎 NOTE

The IBM XFE token field will be available only if the user selects service provider: IBM XFE. Click the ⓘ icon to know the detailed process of obtaining the token for IBM XFE.

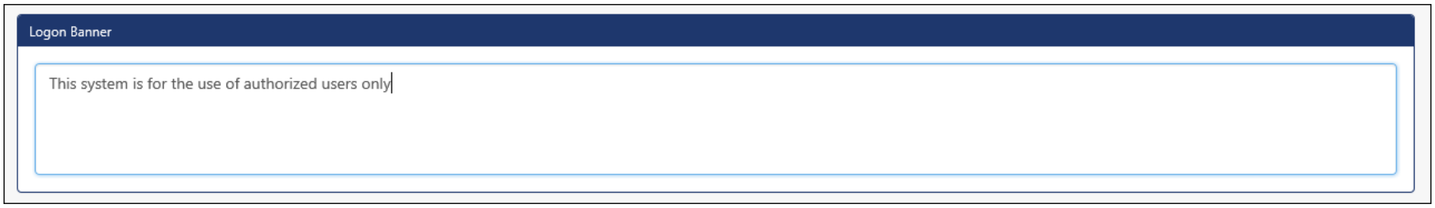
2) Select the **IP Geolocation Provider** from the drop-down option (**IP Void**/**MaxMind GeoLite**).

   Option has been provided to enter “Check for knowledge base updates”, “Show Copyright”, “Show help/about menu”.

4) Click **Save**.

19.1.9 Configuring 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’.


Logon Banner

This system is for the use of authorized users only

Figure 473

1 To configure custom logon message, in **Manager Configuration** page, click **Configuration** tab.

2 Type the warning or custom message in the **Logon Banner** field, and then click **Save**.

19.1.10 Configuring 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**.

19.1.11 Configuring Usage data

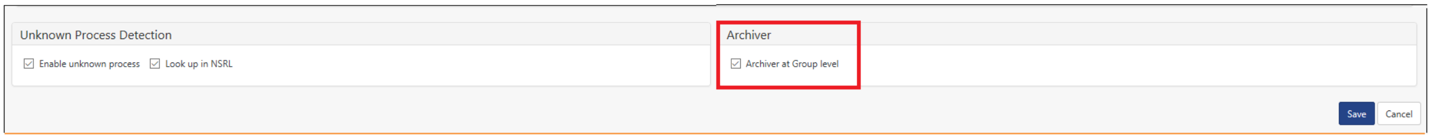
This option is used to update license usage details in EventTracker License Server.

1 In **Manager Configuration** page, click the **Configuration** tab, if not selected.
2 Check the **Collect Usage data** option, and then click **Save**.

19.1.12 Group based Archiving

By enabling “Archiver at Group Level”,

- Data for the respective group is stored in the dedicated file (in the form of cab) with group name suffix added.
- Log search will be faster when user does group level search instead of site level search.
- Report generation is faster when user configures group level report instead of site level report.



Unknown Process Detection

☑ Enable unknown process ☑ Look up in NSRL

Archiver

☑ Archiver at Group level

Figure 474

19.2 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.

1 In **Manager Configuration** page to enable syslog receiver, click **syslog / Virtual Collection Point** tab.
2 Select the **Enable syslog receiver** checkbox, if not selected by default, and then click **Save**.

19.2.1 Monitoring 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 12.19.15.15, add the following detail to the syslog.conf file. *.err @12.19.15.15

🗎 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.

19.2.2 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 several 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.

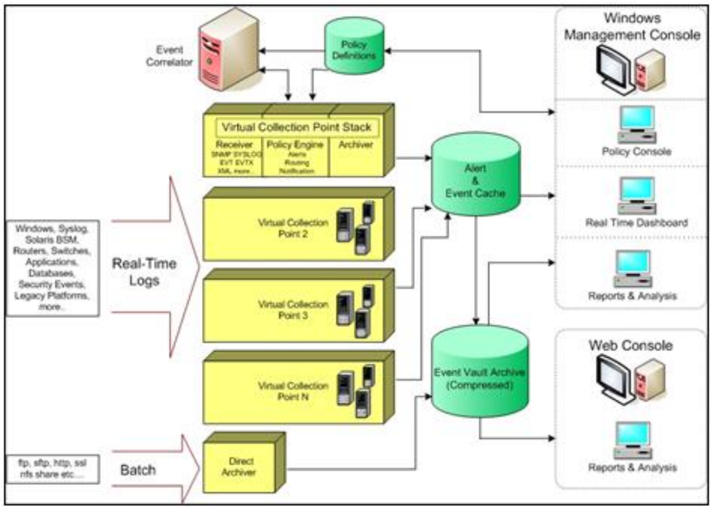

Event Correlator
Policy Definitions
Windows Management Console
Virtual Collection Point Stack
Receiver
SNMP SYSLOG
EVT EVTX
XML, more...
Policy Engine
Alerts
Routing
Notification
Archiver
Alert & Event Cache
Policy Console
Real Time Dashboard
Windows, Syslog, Solaris BSM, Routers, Switches, Applications, Databases, Security Events, Legacy Platforms, more..
Real-Time Logs
Virtual Collection Point 2
Virtual Collection Point 3
Virtual Collection Point N
Reports & Analysis
Web Console
Event Vault Archive (Compressed)
Reports & Analysis
ftp, sftp, http, ssl nfs share etc...
Batch
Direct Archiver

Figure 475

19.2.3 Configuring 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 whereas from the UI (Admin -> Manager) still there is a limit of 20 VCP's (10 Windows & 10 SYSLOG). Depending upon the system capacity (Disk, RAM, CPU, etc.,) any number of VCP's can be created. Please contact eventtracker-support@netsurion.com to increase the limit.

ET Modules	Suggested Trap Ports
You need to add the ports that you are using to the Firewall exceptions list.	
EventTracker Receiver (Incoming)	14505 default port. 14515, 14525, 14535, 14545, 14555, 14565, 14575, 14585, 14595 514 (UDP/TCP) for syslogs.

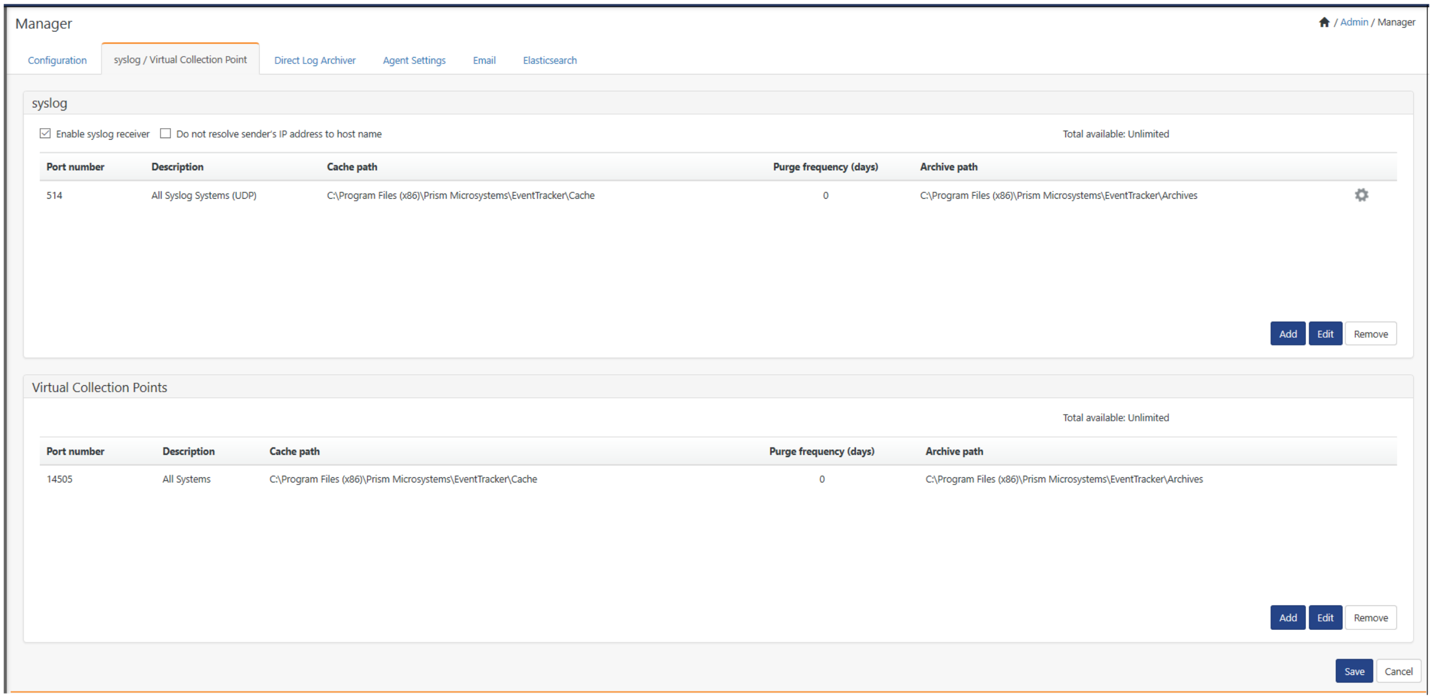
Table 58

For more information, refer https://www.netsurion.com/Corporate/media/Corporate/Files/support-docs/Feature-Guide-Virtual-Collection-Point.pdf

19.2.4 Virtual Collection Points for syslogs

This option helps you configure EventTracker receiver to listen on different ports.

1 Click **syslog / Virtual Collection Point** tab.



Manager

/ Admin / Manager

syslog

☑ Enable syslog receiver ☐ Do not resolve sender's IP address to host name

Total available: Unlimited

Port number	Description	Cache path	Purge frequency (days)	Archive path
514	All Syslog Systems (UDP)	C:\Program Files (x86)\Prism Microsystems\EventTracker\Cache	0	C:\Program Files (x86)\Prism Microsystems\EventTracker\Archives

Virtual Collection Points

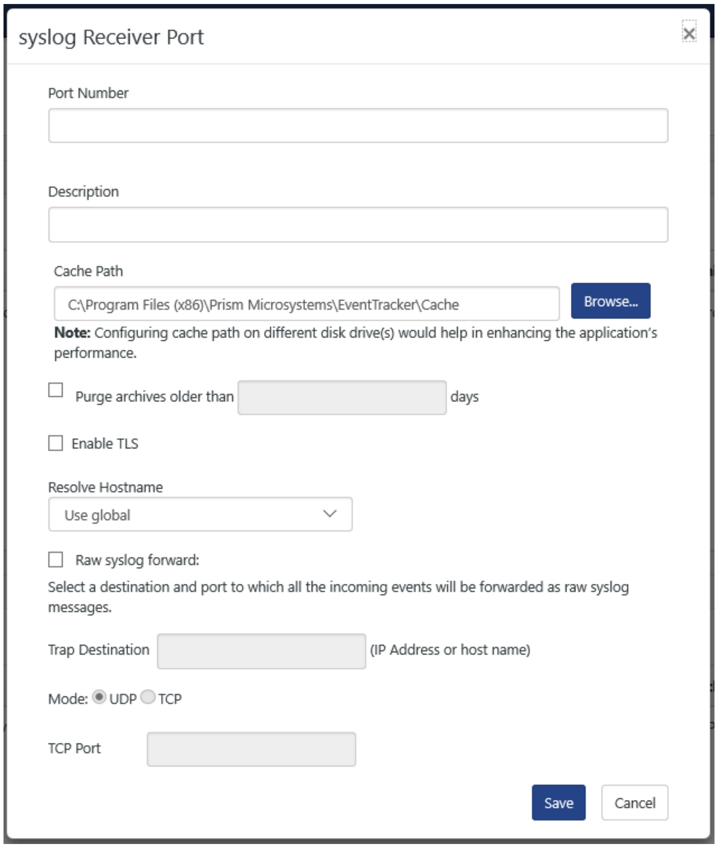
Total available: Unlimited

Port number	Description	Cache path	Purge frequency (days)	Archive path
14505	All Systems	C:\Program Files (x86)\Prism Microsystems\EventTracker\Cache	0	C:\Program Files (x86)\Prism Microsystems\EventTracker\Archives

Figure 476

2 Check **Enable syslog receiver** option if not checked by default, and then click **Add**.

EventTracker opens the **Syslog Receiver Port** dialog box.



syslog Receiver Port

Port Number

Description

Cache Path

C:\Program Files (x86)\Prism Microsystems\EventTracker\Cache

Note: Configuring cache path on different disk drive(s) would help in enhancing the application's performance.

□ Purge archives older than days

□ Enable TLS

Resolve Hostname

Use global

□ Raw syslog forward:

Select a destination and port to which all the incoming events will be forwarded as raw syslog messages.

Trap Destination (IP Address or host name)

Mode: ● UDP ○ TCP

TCP Port

Figure 477

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/ browse the path to save the cache files.

This is not mandatory but changing the location would result in enhancing application's performance.

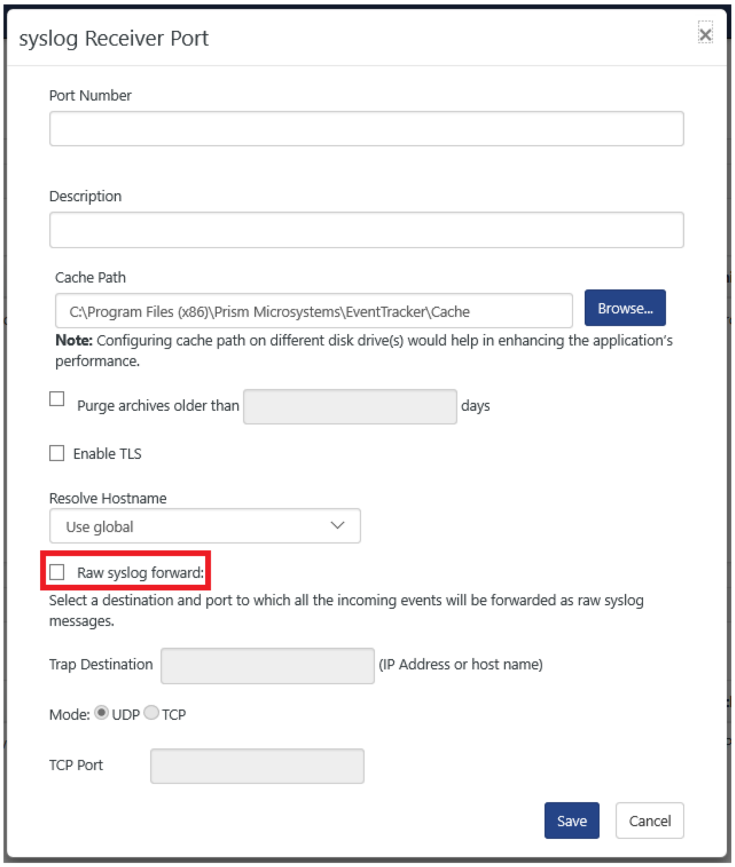
5. Click the check box **Purge archives older than** and enter the number of days for which you want to get the data deleted.

6. Click **Save**.

19.2.5 Forwarding 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.



syslog Receiver Port

Port Number

Description

Cache Path

C:\Program Files (x86)\Prism Microsystems\EventTracker\Cache

Note: Configuring cache path on different disk drive(s) would help in enhancing the application's performance.

□ Purge archives older than days

□ Enable TLS

Resolve Hostname

Use global

□ Raw syslog forward:

Select a destination and port to which all the incoming events will be forwarded as raw syslog messages.

Trap Destination (IP Address or host name)

Mode: ● UDP ○ TCP

TCP Port

Figure 478

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**.

19.2.6 Virtual Collection Points for Windows Events

EventTracker Receiver can be configured to listen on 10 ports for Windows Events.

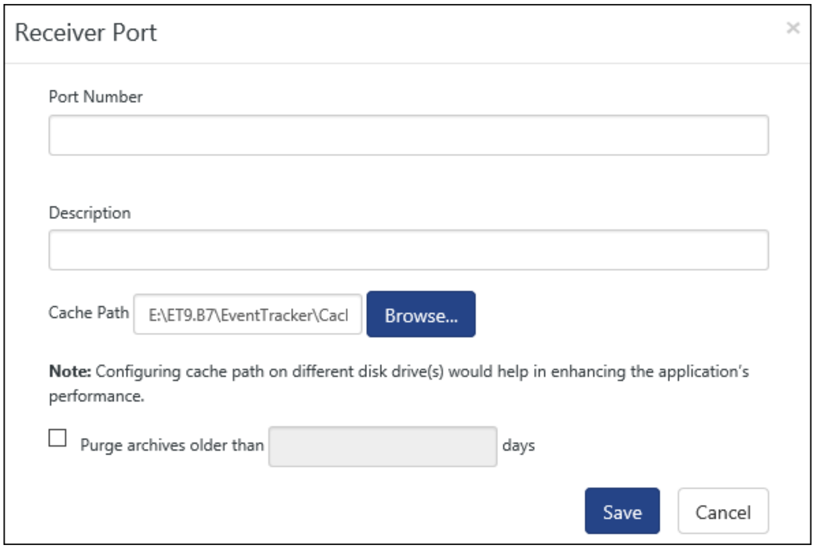
Example Scenario

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:

19.2.7 Computer: Sys1 – Configure Ports

1 In **syslog / Virtual Collection Point** tab, click **Add** button under **Virtual Collection Points** pane.

EventTracker opens the **Receiver Port** dialog box.



Receiver Port

Port Number

Description

Cache Path E:\ET9.B7\EventTracker\Cacl

Note: Configuring cache path on different disk drive(s) would help in enhancing the application's performance.

□ Purge archives older than days

Figure 479

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 Select **Purge archives older than** option and enter the number of **days** to purge the data.

5 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
You need to add these ports to the Firewall exceptions list	
EventTracker Receiver (Incoming)	14505, 14515, 14525

Table 59

19.2.8 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.

19.2.9 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**.

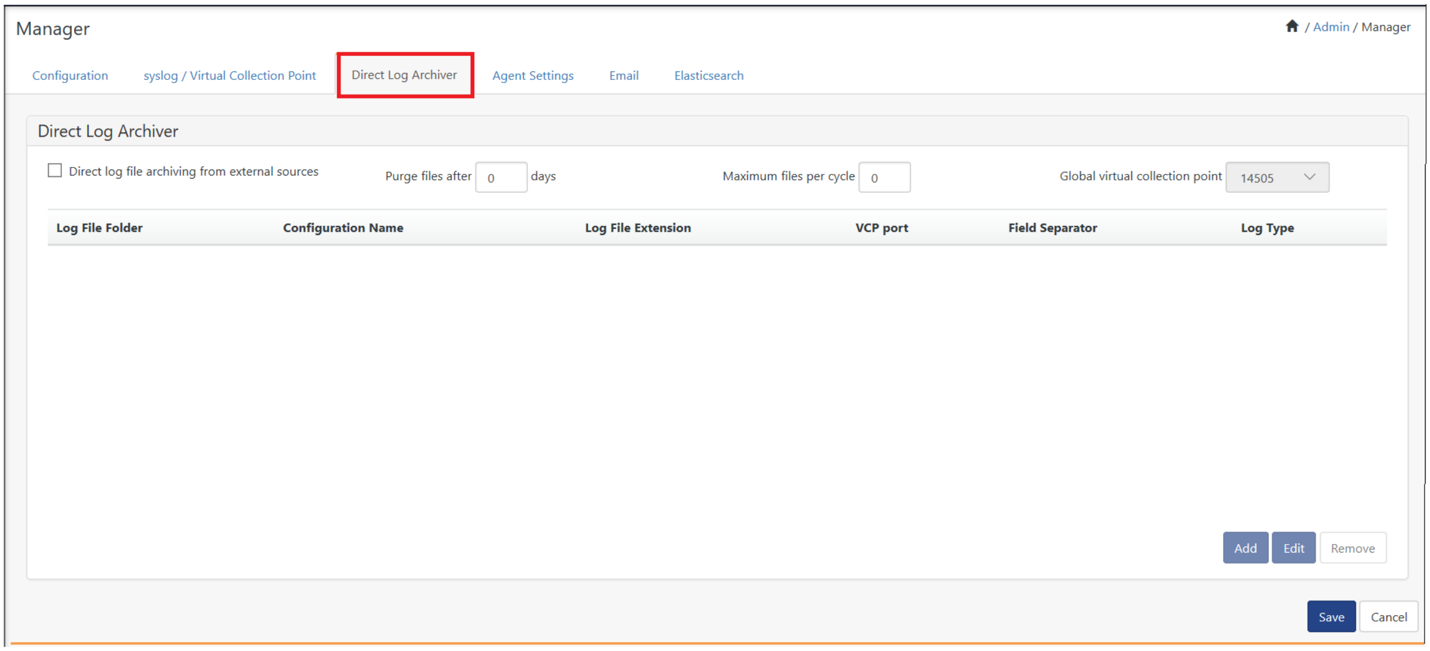
   EventTracker overwrites etaconfig.ini file with new settings.

19.3 Direct Log Archiver

19.3.1 Configuring Direct Log File Archiver

This option helps to 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** tab.



Direct Log Archiver

□ Direct log file archiving from external sources

Purge files after 0 days

Maximum files per cycle 0

Global virtual collection point 14505

Log File Folder	Configuration Name	Log File Extension	VCP port	Field Separator	Log Type

Figure 480

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 To process maximum of 'N' files of each configuration in one cycle, enter the number in the option **Maximum file per cycle.**

6 Select a port from the **Global virtual collection point** drop-down list.

7 Assign an exclusive port that is not associated with any collection groups.

8 Click **Save**.

For more information about Direct Log Archiver (DLA), refer https://www.netsurion.com/Corporate/media/Corporate/Files/Support-Docs/Feature-Guide-Direct-Log-Archiver-(DLA)-v8.pdf

The user can now configure a DLA configuration by using different VCP port selection and the log parser will now pick all the configurations to parse at the same time as per the port selected.

For more Information, Refer: https://www.netsurion.com/Corporate/media/Corporate/Files/Support-Docs/Enhancement-in-Direct-Log-Archiver-to-specify-different-VCP-port-for-each-configuration.pdf

19.3.1.1 Adding archive log file from external sources

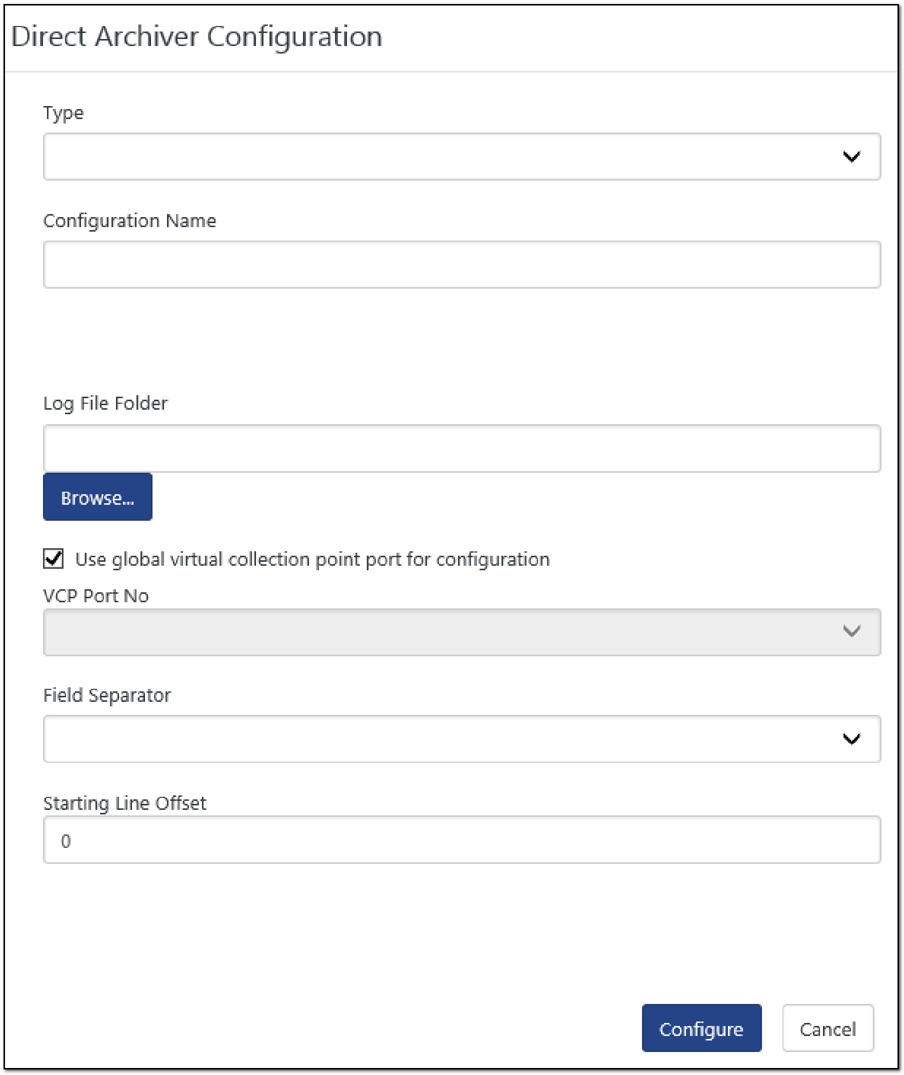
DLA now supports multiline log parsing.

1. Select the **Admin** menu, and then select **Manager**.

   Configuration tab opens by default.

2. Select **Direct Log Archiver** tab.
3. Select the **Direct log file archiving from external sources** option, and then click **Add**.

   Direct Archiver Configuration window opens.



Direct Archiver Configuration

Type

Configuration Name

Log File Folder

☑ Use global virtual collection point port for configuration

VCP Port No

Field Separator

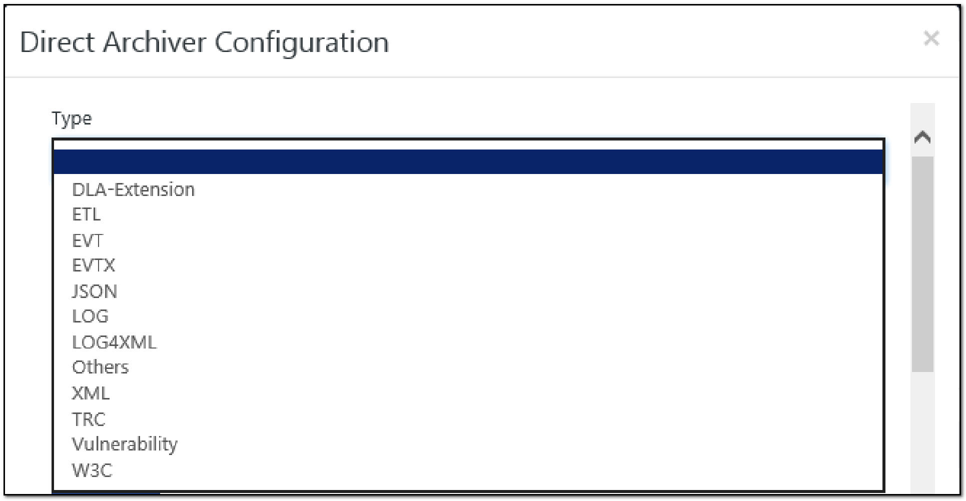
Starting Line Offset: 0

Figure 481

4. Select the **Type, Configuration Name, Log File Folder, Field Separator,** and **Starting Line Offset**.
5. In the **Type** field, select the file type from the dropdown list.

   A new feature Starting Line offset has been added. This feature is used to skip N number lines in a log file. To ignore irrelevant information in a log file you can specify a number to skip those lines. This feature will be available only for the **Type**: Others/Logs/W3C.

   A field separator can be Tab, Space, etc.



Direct Archiver Configuration

Type

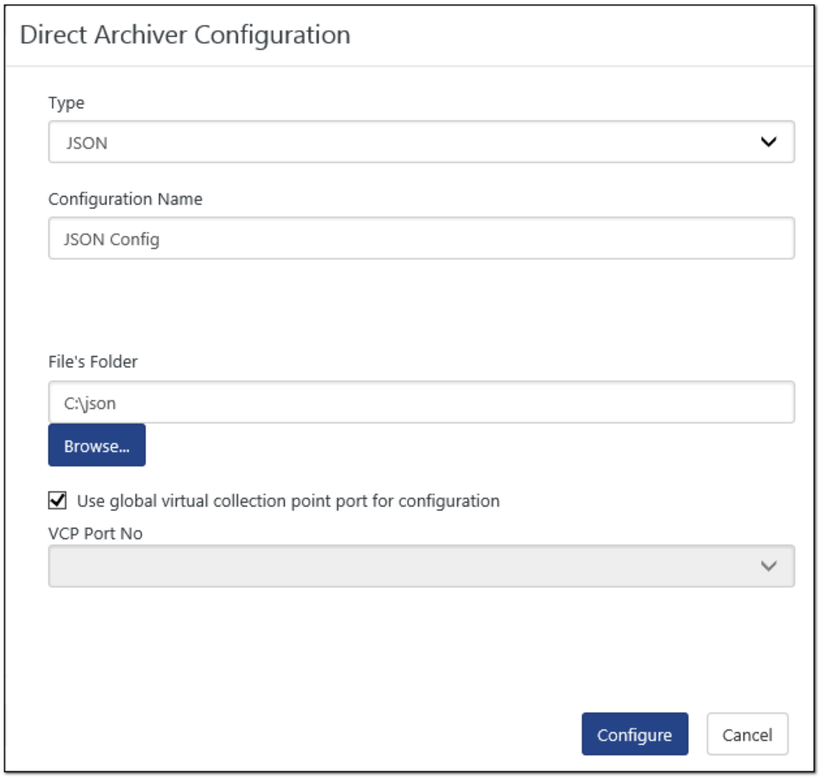
- DLA-Extension
- ETL
- EVT
- EVTX
- JSON
- LOG
- LOG4XML
- Others
- XML
- TRC
- Vulnerability
- W3C

Figure 482

EventTracker now also supports “**XML**” and “**LOG4XML**” along with **JSON** file type and **ETL** file type.

19.3.1.2 Supporting for JSON log files

1. In the Log file configuration window, select the **Type** as **JSON**.



Direct Archiver Configuration

Type: JSON

Configuration Name: JSON Config

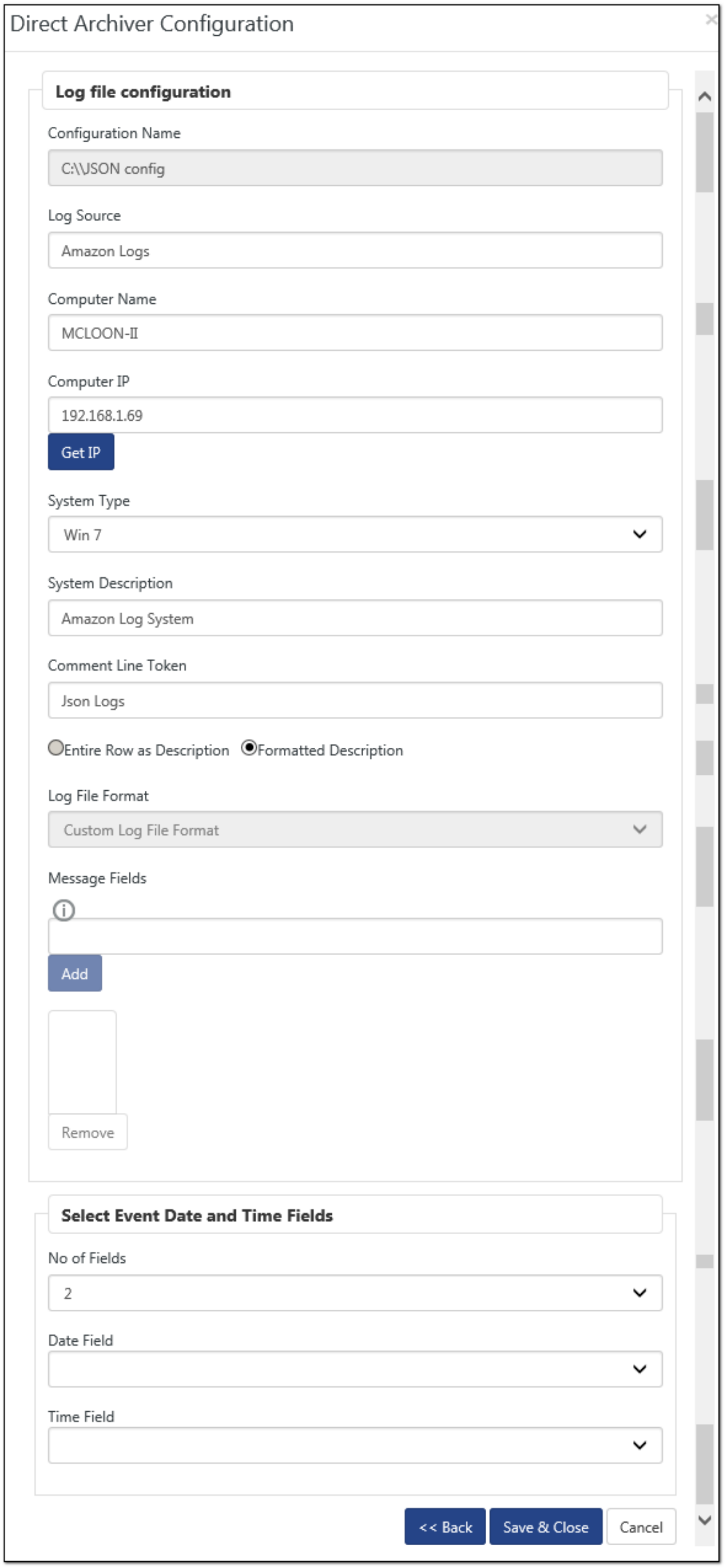
File's Folder: C:\json

☑ Use global virtual collection point port for configuration

VCP Port No

Figure 483

2. Enter required information, and then click **Configure**.



Direct Archiver Configuration

Log file configuration

Configuration Name: C:\\JSON config

Log Source: Amazon Logs

Computer Name: MCLOON-II

Computer IP: 192.168.1.69

System Type: Win 7

System Description: Amazon Log System

Comment Line Token: Json Logs

○ Entire Row as Description ● Formatted Description

Log File Format: Custom Log File Format

Message Fields

Select Event Date and Time Fields

No of Fields: 2

Date Field:

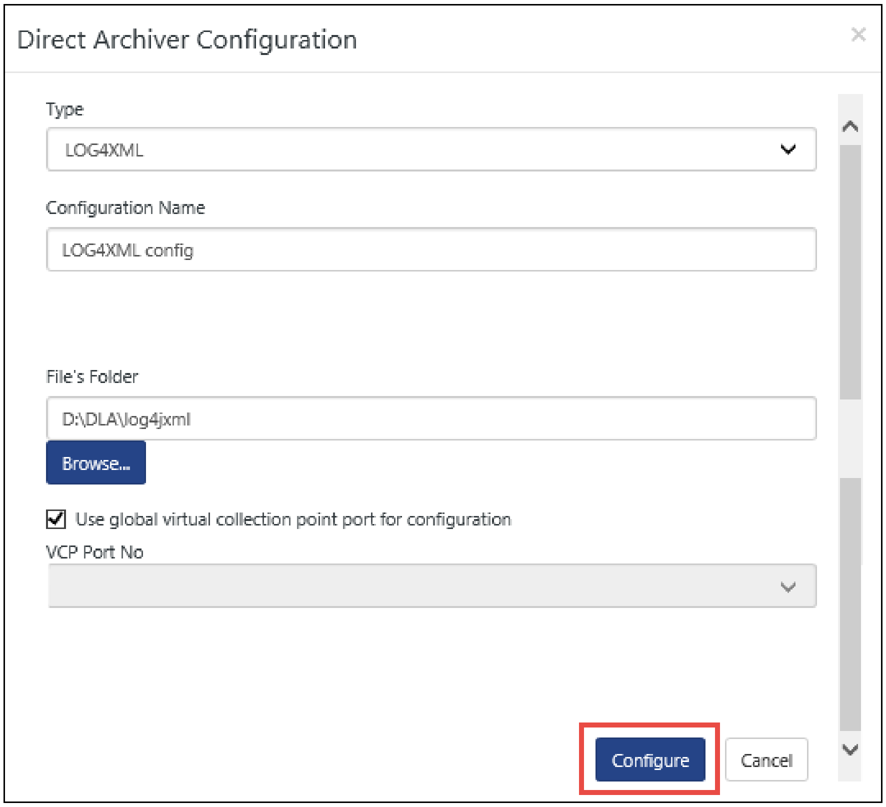
Time Field:

Figure 484

3. Click **Save & Close**.

19.3.1.3 Supporting for LOG4XML files

1. In the Log file configuration window, select the **Type** as **LOG4XML**.



Direct Archiver Configuration

Type: LOG4XML

Configuration Name: LOG4XML config

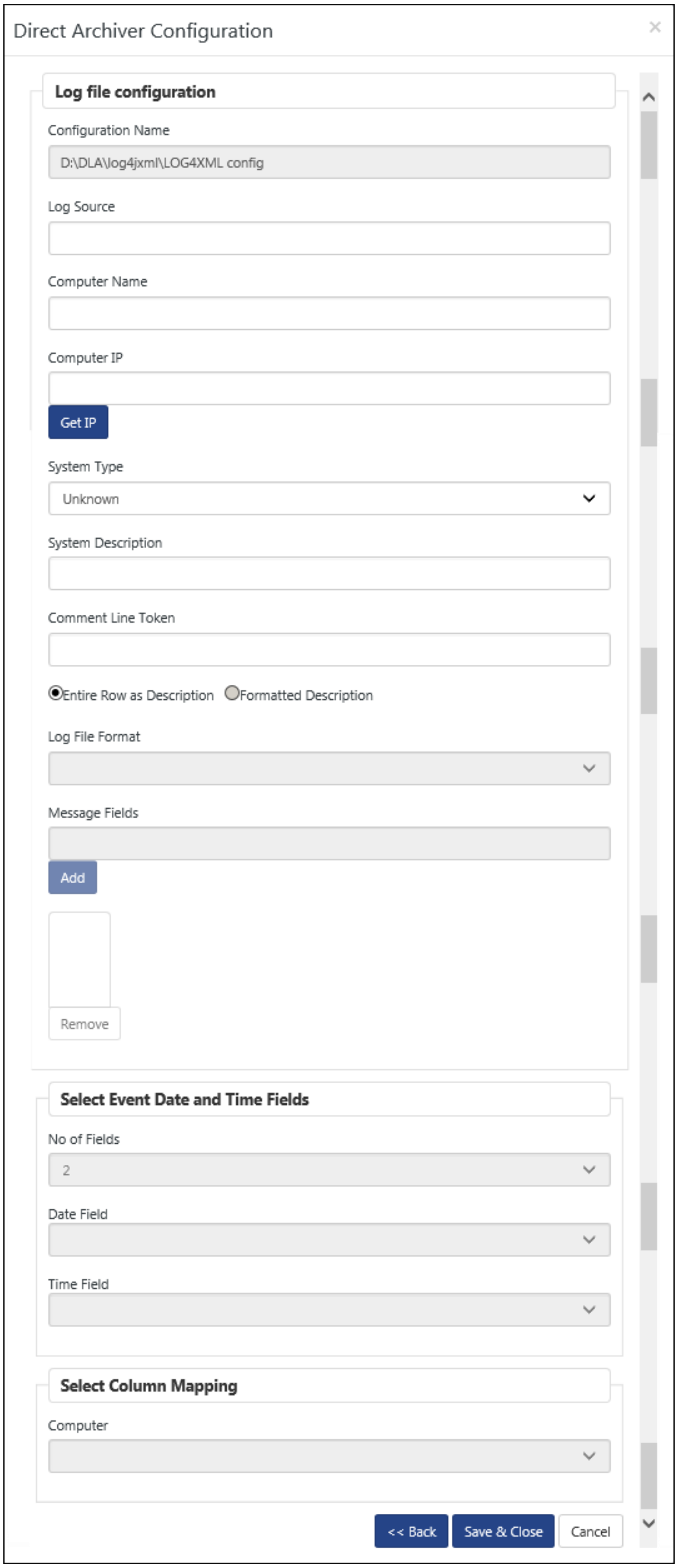
File's Folder: D:\DLA\log4jxml

☑ Use global virtual collection point port for configuration

VCP Port No

Figure 485

2. Enter the configuration name, browse the file, and then click **Configure**.
   The configuration window opens.



Direct Archiver Configuration

Log file configuration

Configuration Name: D:\DLA\log4jxml\LOG4XML config

Log Source

Computer Name

Computer IP

System Type: Unknown

System Description

Comment Line Token

● Entire Row as Description ○ Formatted Description

Log File Format

Message Fields

Select Event Date and Time Fields

No of Fields: 2

Date Field

Time Field

Select Column Mapping

Computer

Figure 486

3. Enter the required field and click **Save & Close**.

19.4 Agent Settings

19.4.1 Configuring 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 **Browse** to navigate and select a folder.

5 Click **Save**.

19.5 Configuring 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 reports published.

1 Select **Admin** drop down, and then select **Manager**.

2 In the **Manager Configuration** page, click the **E-Mail configuration** tab.

Field	Description
SMTP Server	Type the name or IP address of your enterprise mail server.
Port	Type a valid SMTP server port number.
From E-mail id	Type a valid sender e-mail address.
To E-mail id	Type a valid recipient e-mail address.
Email attachment maximum size	Type the maximum size of attachment file in terms of MB. The default size will be 5 MB.
Enable authentication	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.
Test E-mail	Click to check whether you have provided valid data. EventTracker displays the confirmation message box. Click OK to continue. EventTracker displays "success" message if the configuration is correct and "failed" message if the configuration is not correct.

Table 60

3 Provide the details in required fields, and then click **Save**.

19.5.1 Managing Email Accounts

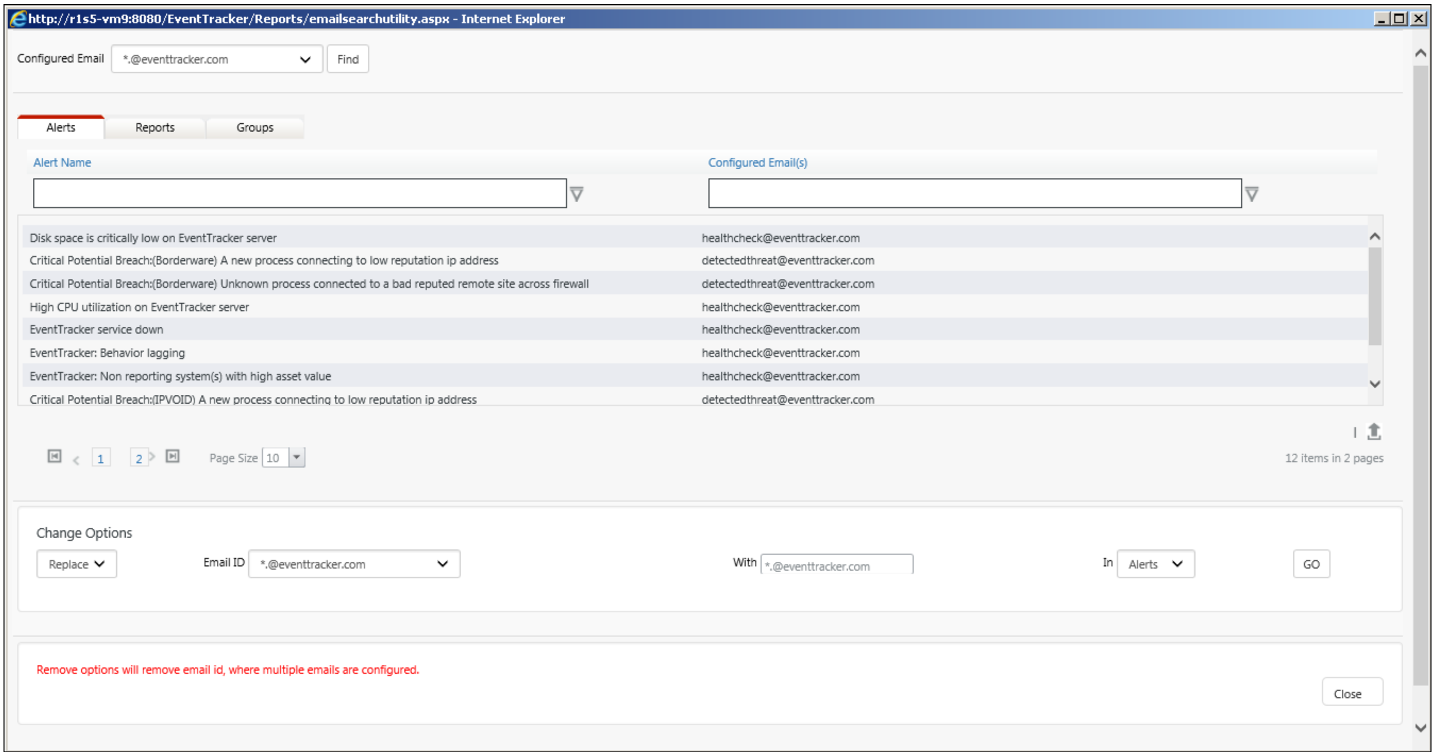
All the Email Ids configured in alerts, reports, and flex reports can be managed from this Email search utility. The Email Ids can be replaced with a new Email Id or removed if it is no more in use or invalid address.

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 **Save**.

3 Click the **Manage email** hyperlink.

EventTracker opens **Email search utility** window.


http://r1s5-vm9:8080/EventTracker/Reports/emailsearchutility.aspx - Internet Explorer

Configured Email: *.@eventtracker.com | Find

Alerts | Reports | Groups

Alert Name	Configured Email(s)
Disk space is critically low on EventTracker server	healthcheck@eventtracker.com
Critical Potential Breach:(Borderware) A new process connecting to low reputation ip address	detectedthreat@eventtracker.com
Critical Potential Breach:(Borderware) Unknown process connected to a bad reputed remote site across firewall	detectedthreat@eventtracker.com
High CPU utilization on EventTracker server	healthcheck@eventtracker.com
EventTracker service down	healthcheck@eventtracker.com
EventTracker: Behavior lagging	healthcheck@eventtracker.com
EventTracker: Non reporting system(s) with high asset value	healthcheck@eventtracker.com
Critical Potential Breach:(IPVOID) A new process connecting to low reputation ip address	detectedthreat@eventtracker.com

Page Size 10 — 12 items in 2 pages

Change Options

Replace | Email ID: *.@eventtracker.com | With: *.@eventtracker.com | In: Alerts | GO

Remove options will remove email id, where multiple emails are configured.

Figure 487

Field	Description
Configured Email	The list of all configured email Ids.
Alerts	The list of alerts configured with the selected email Id.
Reports	The list of reports configured with the selected email Id.
Export alerts to excel / Export reports to excel	Click to export the alerts or reports along with the configured email Id.
Change Option	Remove or replace the configured email Id.

Table 61

4 From **Configured Email** dropdown, select the required email Id, and then click **Find**.

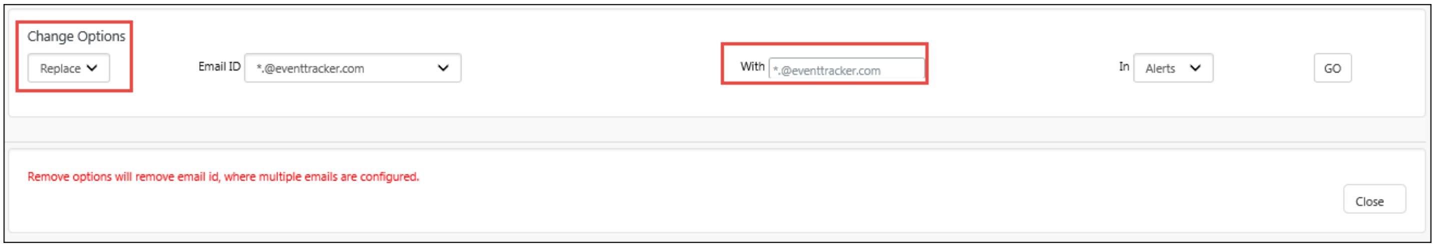
The alert(s) and report(s) configured with the email Id will be displayed under **Alerts** and **Reports** tab, respectively.

19.5.2 Replacing Email Id

1 Click the **Manage email** hyperlink.

EventTracker opens 'E-mail search utility' window.

2 In the **Change Options** pane, select **Replace** from the dropdown, if not selected.



Change Options: Replace

Email ID: *.@eventtracker.com

With: *.@eventtracker.com

In: Alerts

Remove options will remove email id, where multiple emails are configured.

Figure 488

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**.

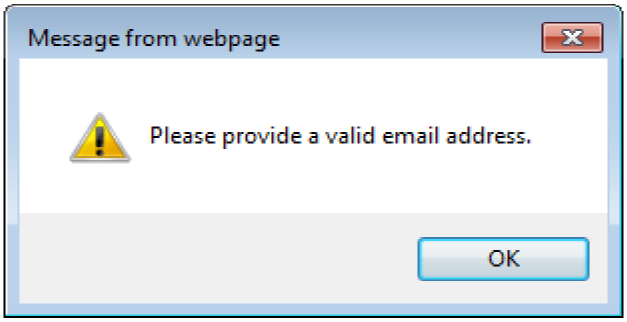
6 Click **Go**.

EventTracker opens confirmation message box.

7 Click **OK**.

EventTracker opens success message box.

If any special character or wrong Email Id is provided, then EventTracker opens the error message.



Please provide a valid email address.

Figure 489

8 Click **OK** in the success message box.

9 To verify the replacement, click the **Configured Email** dropdown, select the replaced Email address, and then click **Find**.

EventTracker opens the alerts or reports configured with the selected Email Id.

19.5.3 Removing Email ID

1 Click the **Manage email** hyperlink.

EventTracker opens ‘E-mail search utility’ window.

2 In the **Change Options** pane, select **Remove** from the dropdown.

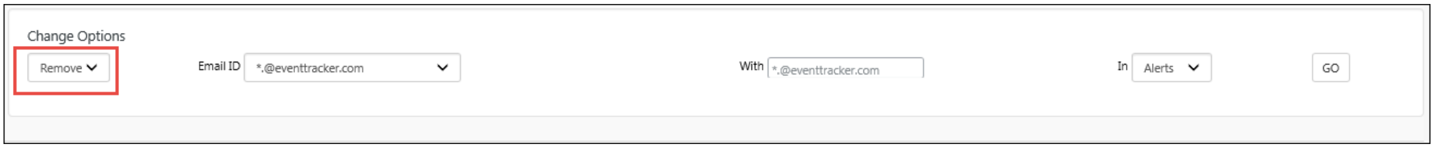


Figure 490

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**.

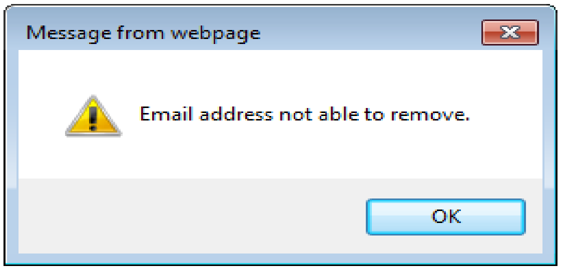
5 Click **Go**.

EventTracker opens confirmation message box.

6 Click **OK**.

EventTracker opens 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.


Message from webpage

Email address not able to remove.

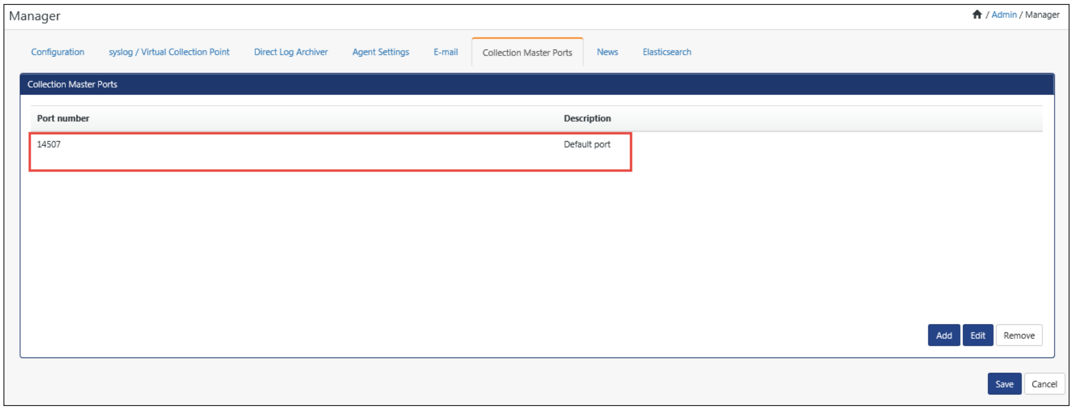
Figure 491

7 Click **OK** in the success message box.

19.6 Collection Master Ports

The Collection Master Ports can be configured in Manager.

1. Click the **Admin** menu, click **Manager**, and then click **Collection Master Ports**.



Port number	Description
14507	Default port

Figure 492

2. Click **Add**.

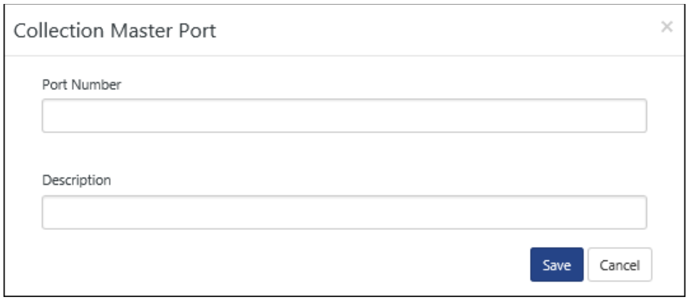
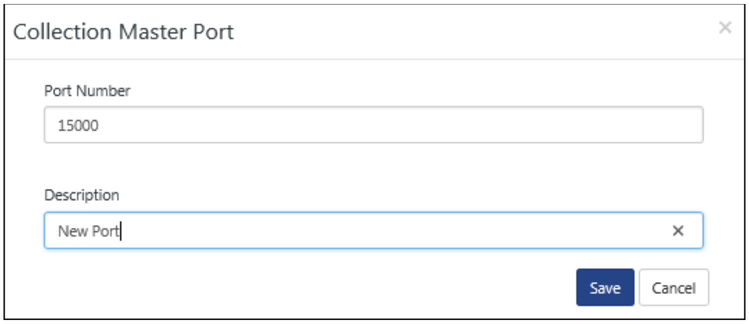


Figure 493

3. Enter the **Port Number:**, **Description:**, and then click **Save**.



Port Number: 15000

Description: New Port

Figure 494

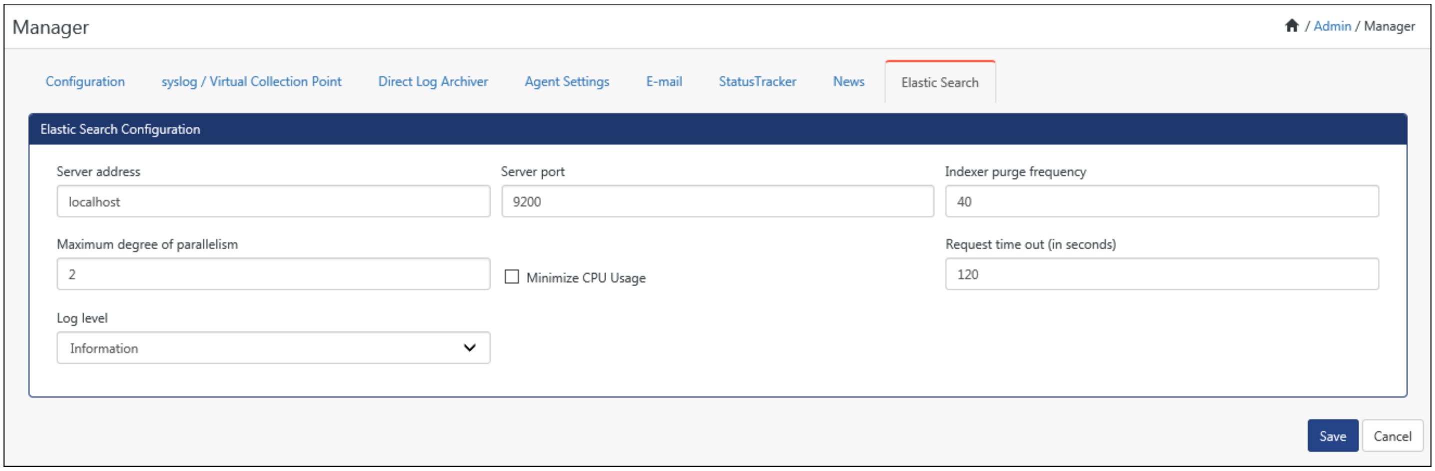
4. To edit the **Collection Master Port**s, click **Edit**.
5. To remove the **Collection Master Ports**, click **Remove**.

NOTE

This Collection Master Port option is available on the Console Type: Collection Master

19.7 Elastic Search

In this tab, we can make configuration changes for the Elastic Search.



Elastic Search Configuration

Server address: localhost

Server port: 9200

Indexer purge frequency: 40

Maximum degree of parallelism: 2

□ Minimize CPU Usage

Request time out (in seconds): 120

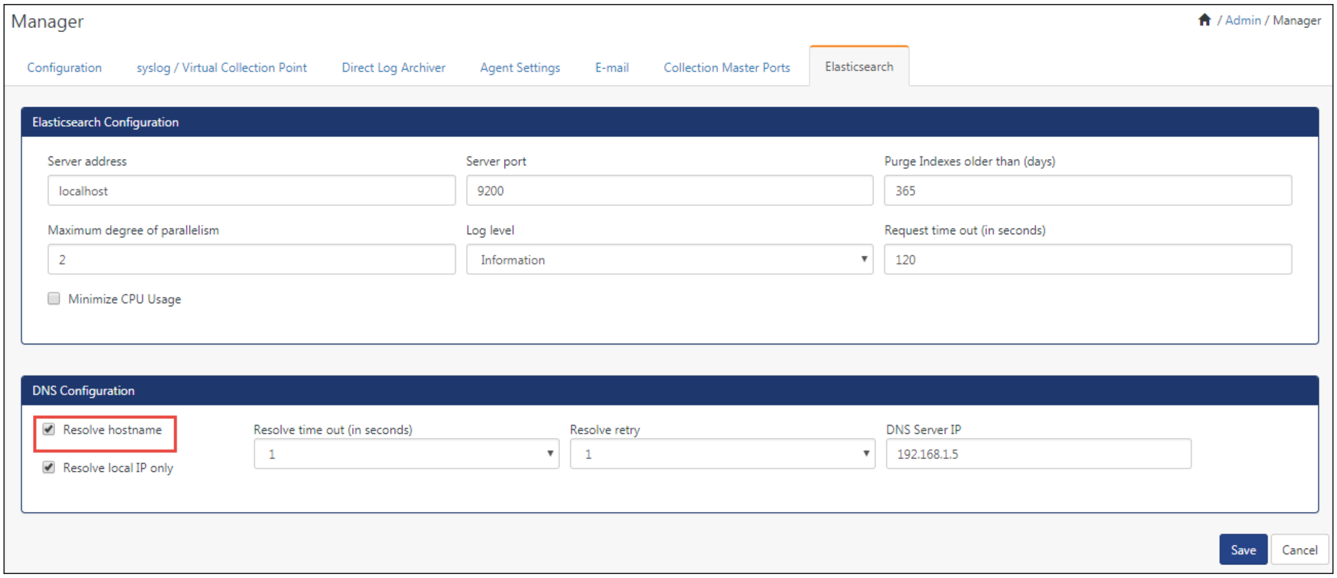
Log level: Information

Figure 495

- Enter the server address, port, purge frequency, degree of parallelism and even select the log level from the dropdown list.
- The user can also check the **Minimize CPU usage** option, if required.
- After making the configuration changes, click **Save**.

19.7.1 Resolving Hostname through Elasticsearch

By default, the “**Resolve Hostname**” option will be disabled. In this case, the hostname for the IP addresses will not be resolved (Local or Public IP). User can enable this option by navigating to Admin--> Manager--> Elasticsearch tab, under DNS configuration.



Elasticsearch Configuration

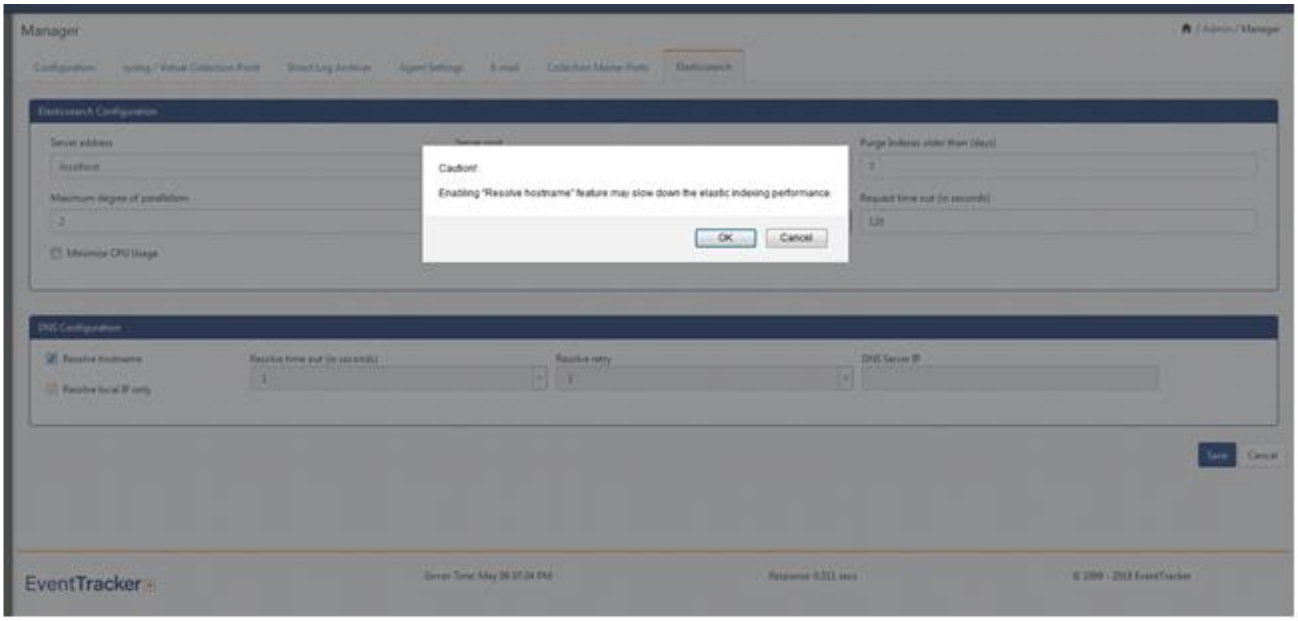
Server address: localhost
Server port: 9200
Purge Indexes older than (days): 365
Maximum degree of parallelism: 2
Log level: Information
Request time out (in seconds): 120
☐ Minimize CPU Usage

DNS Configuration

☑ Resolve hostname
☑ Resolve local IP only
Resolve time out (in seconds): 1
Resolve retry: 1
DNS Server IP: 192.168.1.5

Figure 496

On enabling Resolved hostname option, the alert message appears.



Caution!

Enabling "Resolve hostname" feature may slow down the elastic indexing performance.

Figure 497

After enabling this option Resolved hostname the DNS server IP address will be fetched automatically. By default, it is set to Resolve local IP only.

The user can also provide the DNS Server IP manually.

Whenever a local IP address is identified in **src_ip_address** or **dest_ip_address** during elastic index, Elasticsearch service will resolves the hostname for IP address and puts the same hostname in the associated CIM fields, i.e. **src_host_name** or **dest_host_name** respectively.

When the “**Resolve local IP only**” option is unchecked, then Elasticsearch will resolve both Public and Local IP addresses.

20. Parsing Rules

In this chapter, you will learn how to:

- Parsing Rule
- Components of Parsing Rules
- Add Token Value Groups
- Template
- Generate Flex Report

20.1 About Parsing Rules

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 rules** helps to manipulate data and generate comprehensible reports.

20.1.1 The Need for adding Parsing Rules 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 are used by an administrator to decipher syslog messages.

20.1.2 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.

20.1.3 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.

20.2 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.

20.3 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.

20.3.1 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#)

20.3.2 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.

20.3.3 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

20.3.4 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

20.3.5 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

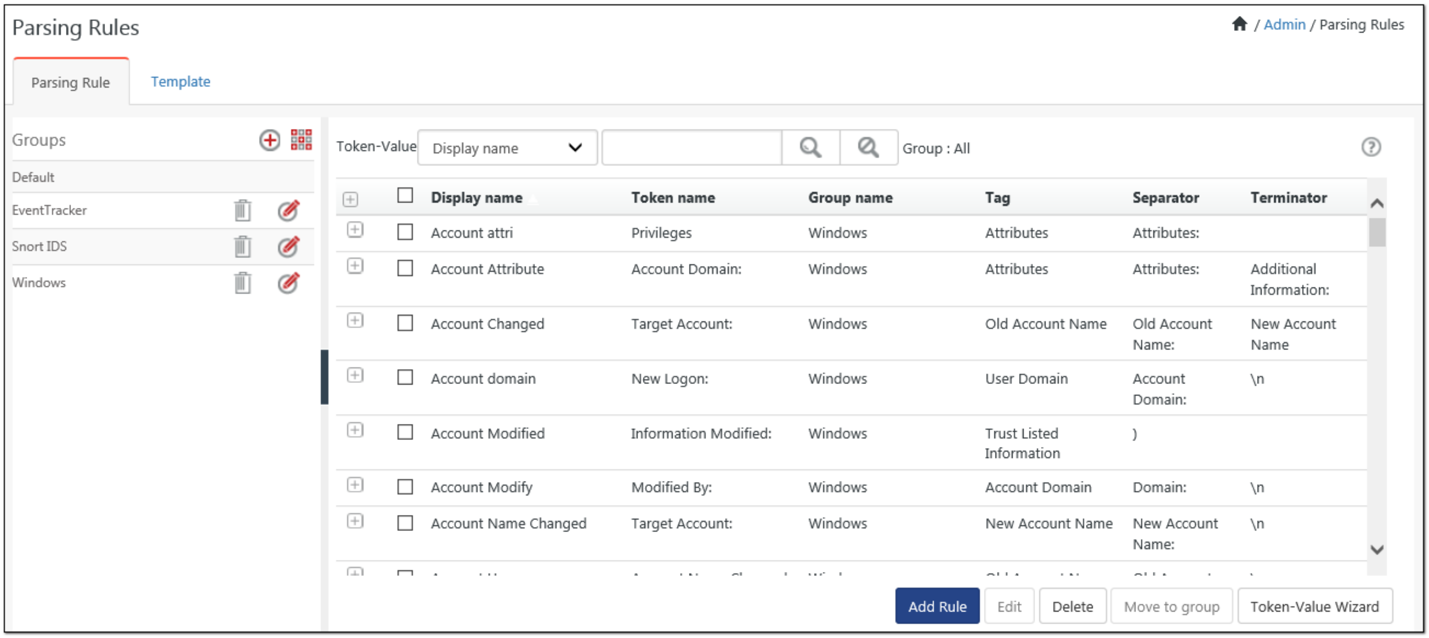
Thus, parsing rule offers flexibility to customize:

- Data selection
- Sort sequences

20.4 Viewing Parsing Rules

1 To view Parsing Rules, select the **Admin** drop down, and then select **Parsing Rules**.

The default Token-Value groups display. EventTracker provides predefined parsing rules.



Display name	Token name	Group name	Tag	Separator	Terminator
Account attri	Privileges	Windows	Attributes	Attributes:	
Account Attribute	Account Domain:	Windows	Attributes	Attributes:	Additional Information:
Account Changed	Target Account:	Windows	Old Account Name	Old Account Name:	New Account Name
Account domain	New Logon:	Windows	User Domain	Account Domain:	\n
Account Modified	Information Modified:	Windows	Trust Listed Information	)	
Account Modify	Modified By:	Windows	Account Domain	Domain:	\n
Account Name Changed	Target Account:	Windows	New Account Name	New Account Name:	\n

Figure 498

2 To search based on token values, click **Token-Value** drop down, and select the required option.

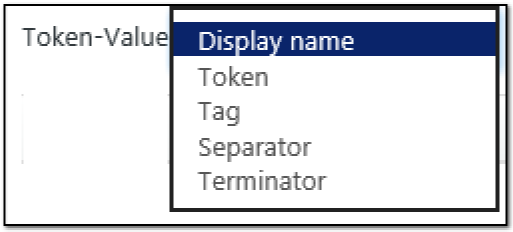
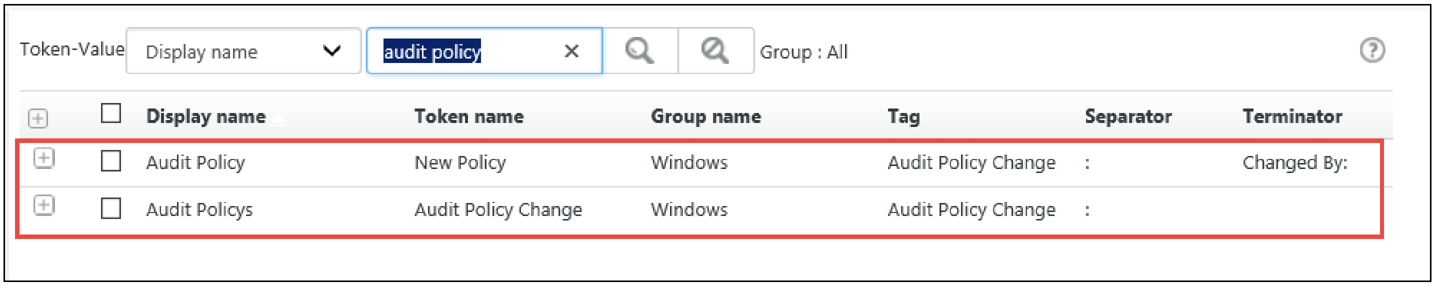


Figure 499

3 Enter the search criteria in the Search box and then click **Search** .

Ex: To search for Token Value 'audit policy', enter the word 'audit policy' in the search box, and then click the search icon. The respective information is displayed.



Display name	Token name	Group name	Tag	Separator	Terminator
Audit Policy	New Policy	Windows	Audit Policy Change	:	Changed By:
Audit Policys	Audit Policy Change	Windows	Audit Policy Change	:	

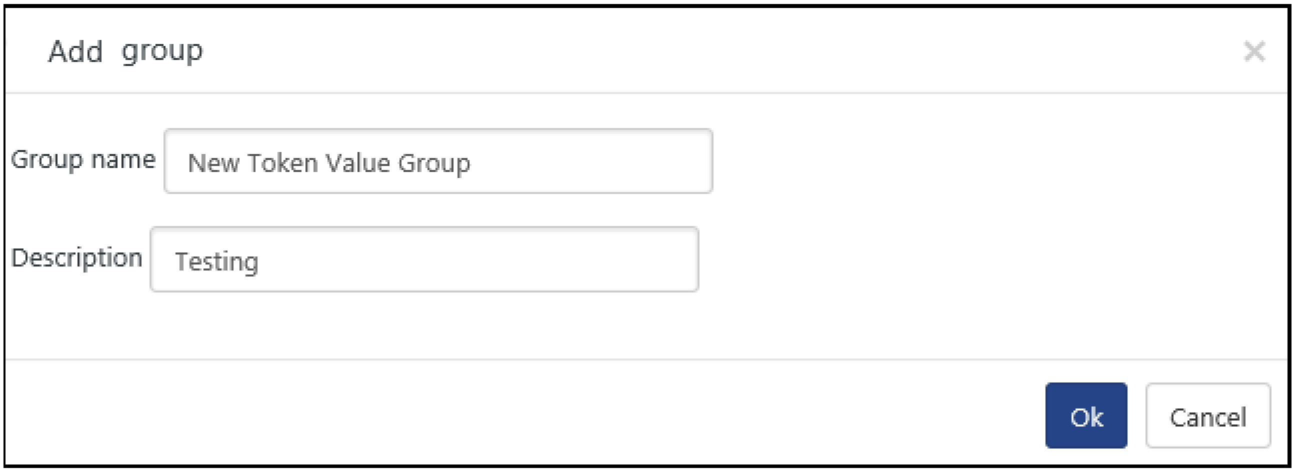
Figure 500

4 To clear the search criteria, select **Clear all** .

20.5 Adding Token Value Groups

The default Token-Value Groups are available in the Token Value pane.

1 To add a new group, click the icon ⊕.
2 Enter the relevant group name, description and then click **OK**.



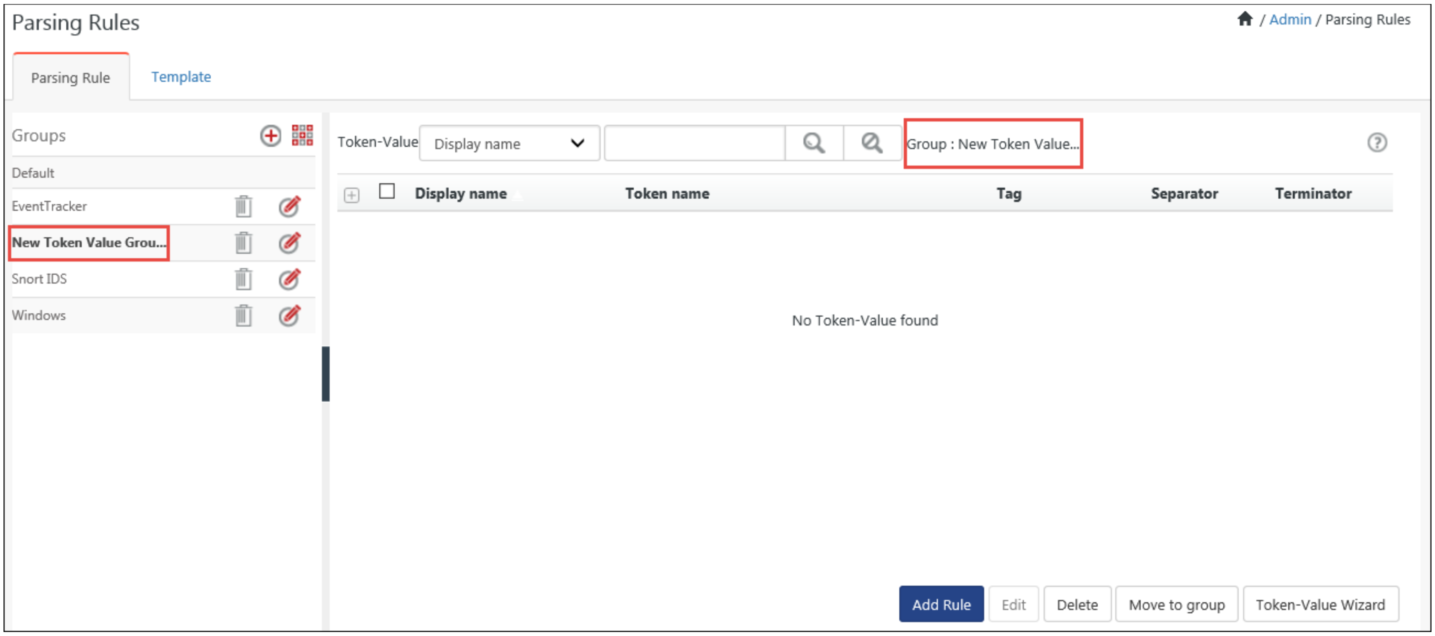
Add group

Group name: New Token Value Group

Description: Testing

Figure 501

A new token value group is created.



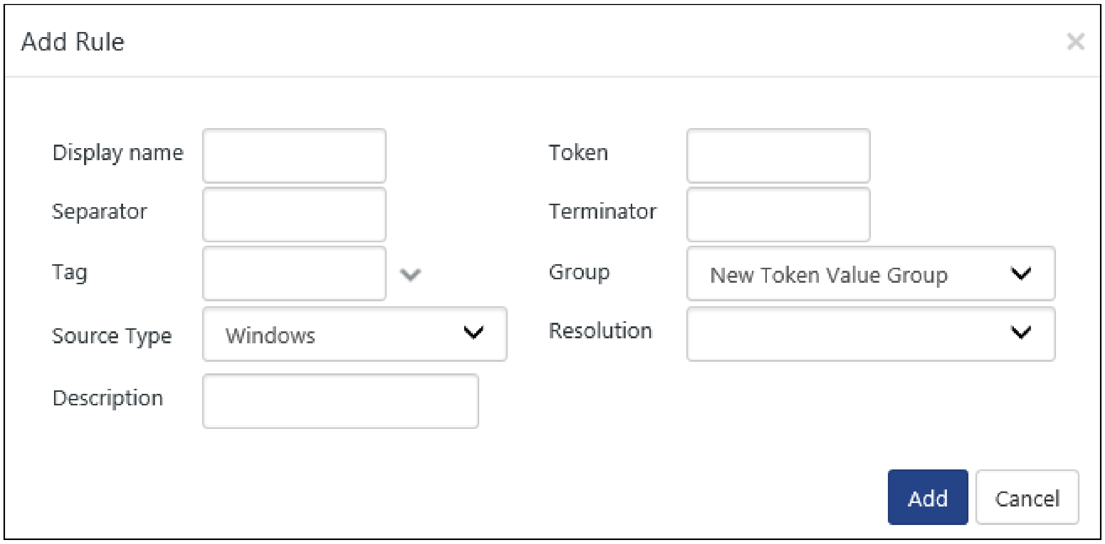
Parsing Rules

No Token-Value found

Figure 502

20.5.1 Adding Rule

1 To add a new rule, click **Add Rule**.



Add Rule

Display name

Separator

Tag

Source Type: Windows

Description

Token

Terminator

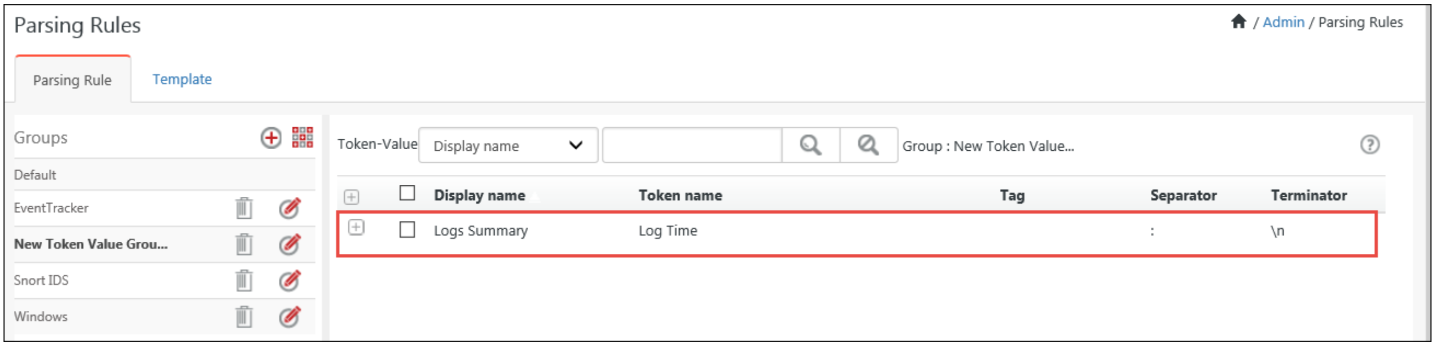
Group: New Token Value Group

Resolution

Figure 503

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.



Parsing Rules

Display name	Token name	Tag	Separator	Terminator
Logs Summary	Log Time		:	\n

Figure 504

🗎 NOTE

There can be more than one Token-Value with the same Display name but one of the tokens, separator or terminator should be different/unique.

Ex: The Display name is the same in the screenshot given below but the separator is different.

3 To edit the token value, click **Edit**, make the required changes and then click **Save**.

NOTE

You can edit only one Token-Value at a time.

4 To delete the token value, click **Delete**.

5 To the token value to another group, click **Move to group.**

NOTE

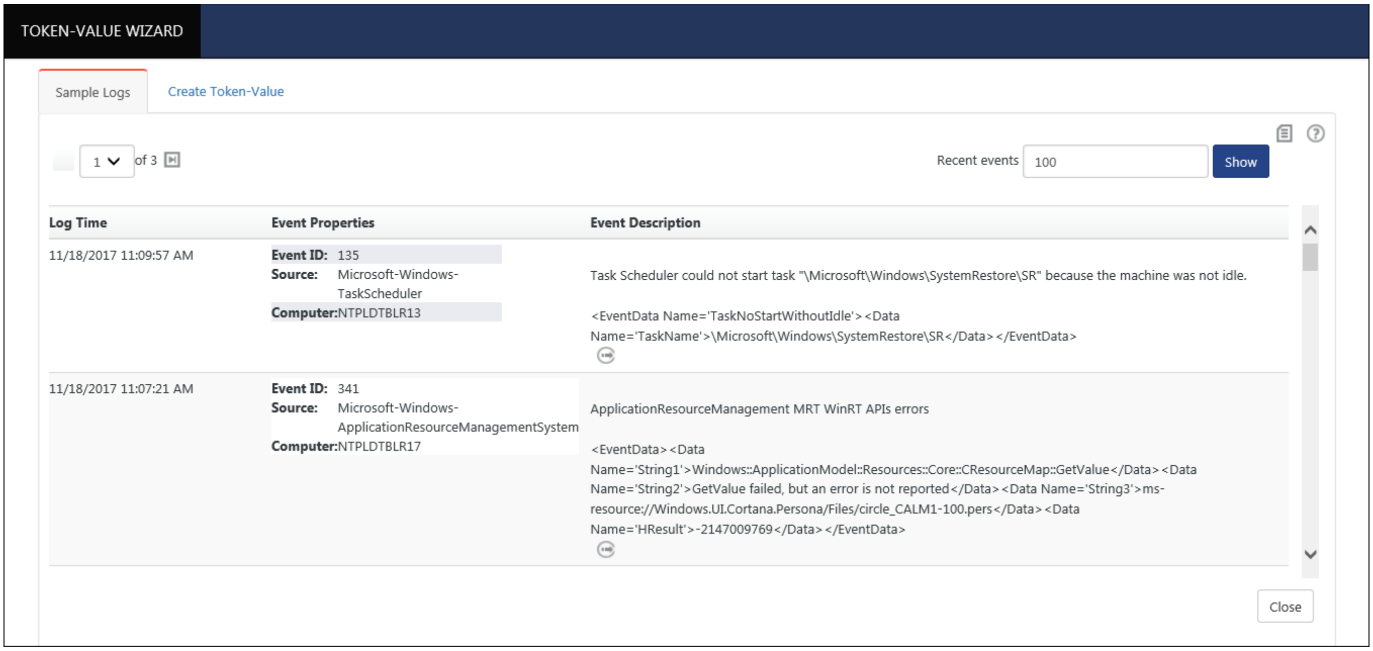
You can move to another group if there are other Token-Value groups existing apart from the Selected one.

20.5.2 Token Value Wizard

1 To view **Token Value Wizard**, select the **Admin**, select **Parsing Rules**.
The default **Token-Value** groups opens.

2 Select **Token Value Wizard**.

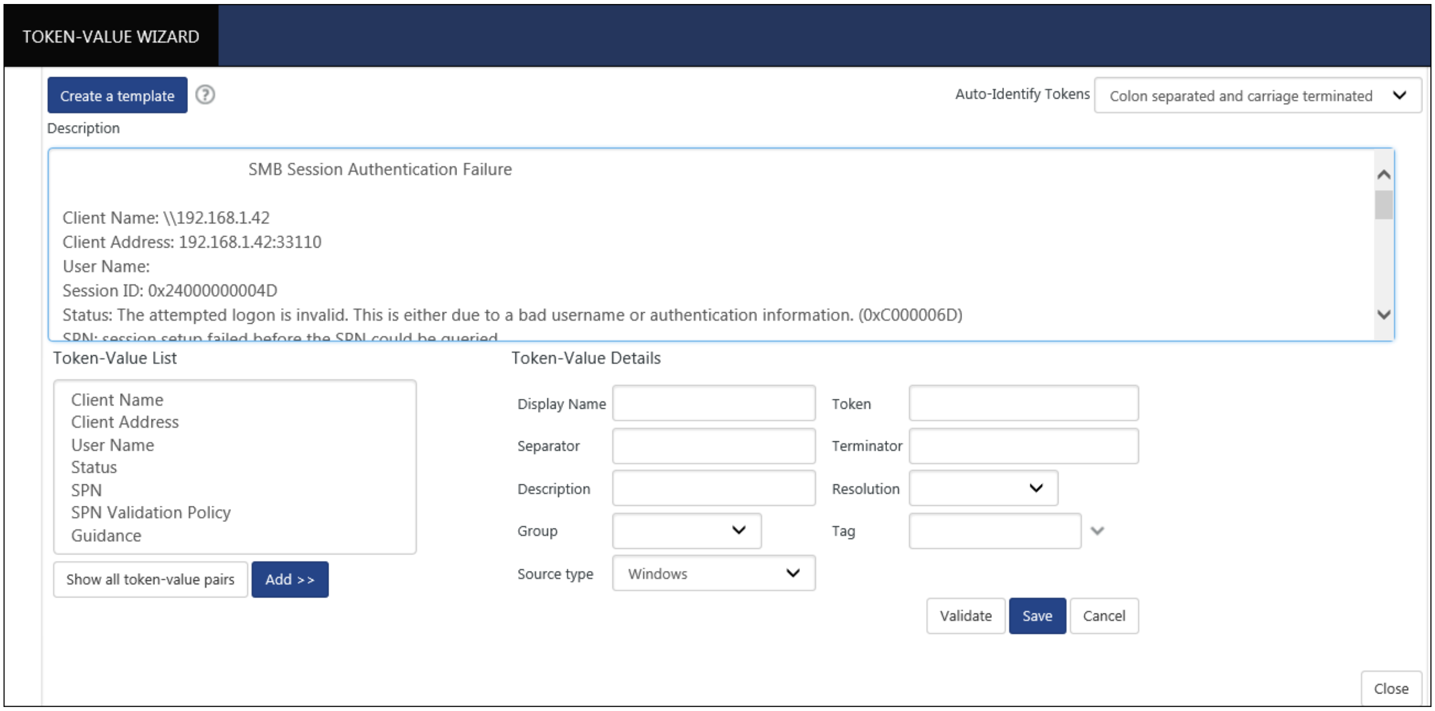
The Token-Value Wizard displays Sample Logs window.



Log Time	Event Properties	Event Description
11/18/2017 11:09:57 AM	**Event ID:** 135 **Source:** Microsoft-Windows-TaskScheduler **Computer:**NTPLDTBLR13	Task Scheduler could not start task "\Microsoft\Windows\SystemRestore\SR" because the machine was not idle. <EventData Name='TaskNoStartWithoutIdle'><Data Name='TaskName'>\Microsoft\Windows\SystemRestore\SR</Data></EventData>
11/18/2017 11:07:21 AM	**Event ID:** 341 **Source:** Microsoft-Windows-ApplicationResourceManagementSystem **Computer:**NTPLDTBLR17	ApplicationResourceManagement MRT WinRT APIs errors <EventData><Data Name='String1'>Windows::ApplicationModel::Resources::Core::CResourceMap::GetValue</Data><Data Name='String2'>GetValue failed, but an error is not reported</Data><Data Name='String3'>ms-resource://Windows.UI.Cortana.Persona/Files/circle_CALM1-100.pers</Data><Data Name='HResult'>-2147009769</Data></EventData>

Figure 505

3 Click any one of the **Extract Token Value Pairs** icon.
Create Token-Value tab open with additional data.



Auto-Identify Tokens: Colon separated and carriage terminated

SMB Session Authentication Failure

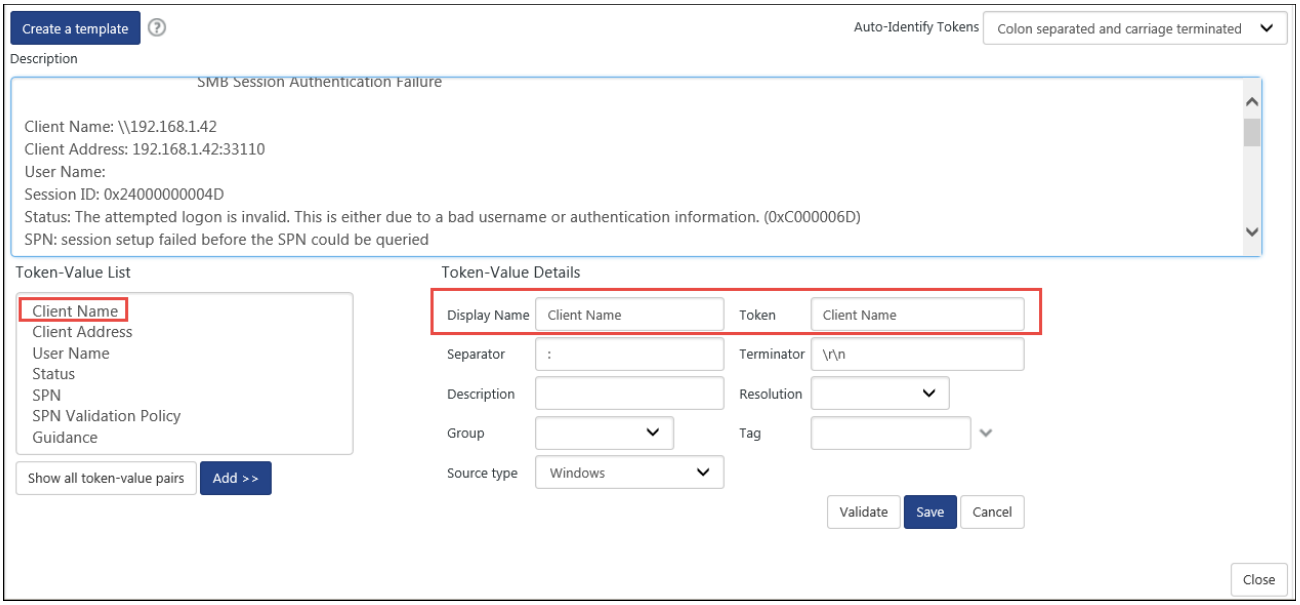
Client Name: \\192.168.1.42
Client Address: 192.168.1.42:33110
User Name:
Session ID: 0x24000000004D
Status: The attempted logon is invalid. This is either due to a bad username or authentication information. (0xC000006D)
SPN: session setup failed before the SPN could be queried

Token-Value List:
Client Name
Client Address
User Name
Status
SPN
SPN Validation Policy
Guidance

Source type: Windows

Figure 506

4 Select a **Token Value List** and then click **Add >>**.
Ex: Select **Client Name** in Token Value List and then click **Add**.



Auto-Identify Tokens: Colon separated and carriage terminated

SMB Session Authentication Failure

Client Name: \\192.168.1.42
Client Address: 192.168.1.42:33110
User Name:
Session ID: 0x24000000004D
Status: The attempted logon is invalid. This is either due to a bad username or authentication information. (0xC000006D)
SPN: session setup failed before the SPN could be queried

Token-Value List:
Client Name
Client Address
User Name
Status
SPN
SPN Validation Policy
Guidance

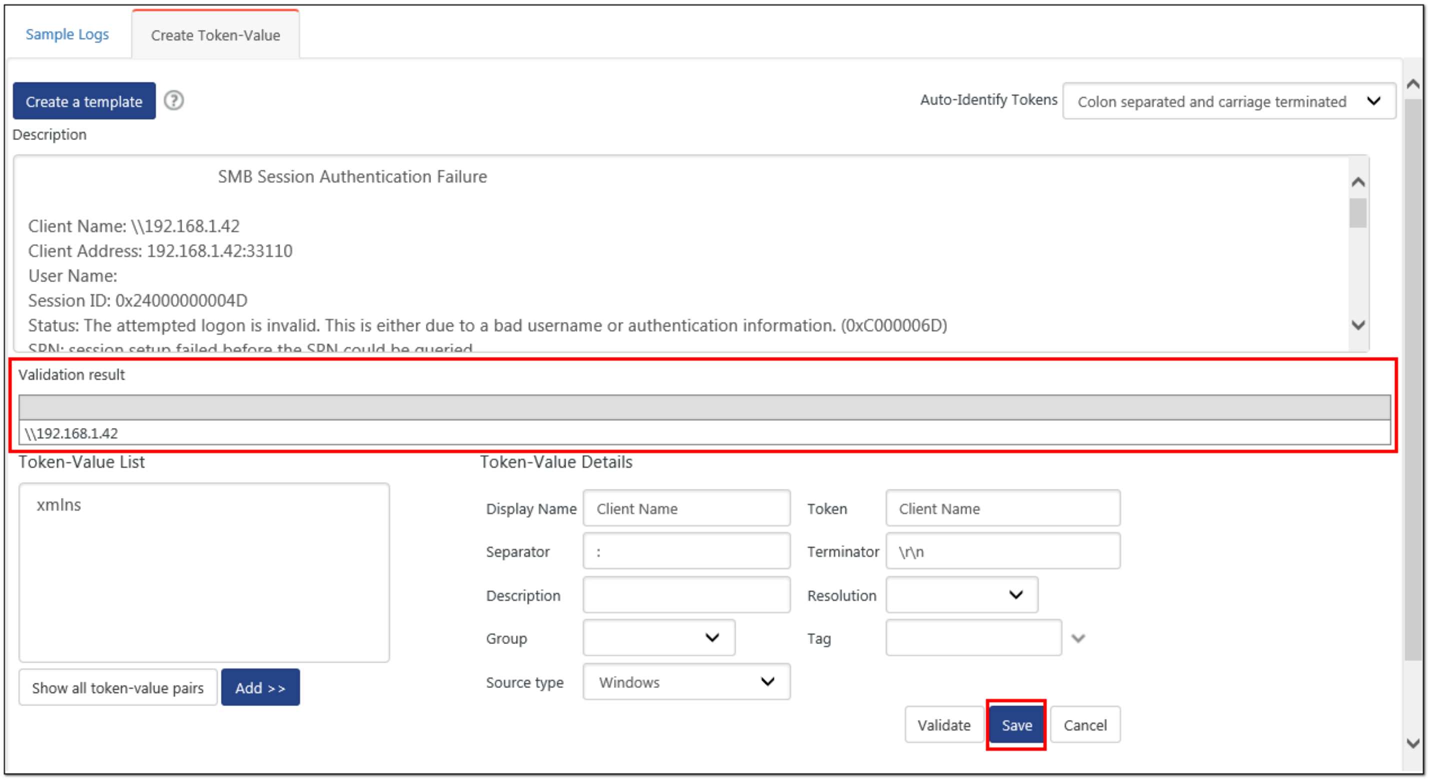
Display Name: Client Name
Token: Client Name
Separator: :
Terminator: \r\n
Source type: Windows

Figure 507

Token-Value Details appears.

You can make the changes in the default values displayed.

5 Click **Validate,** and then click **Save.**



Auto-Identify Tokens: Colon separated and carriage terminated

Description

```
SMB Session Authentication Failure

Client Name: \\192.168.1.42
Client Address: 192.168.1.42:33110
User Name:
Session ID: 0x24000000004D
Status: The attempted logon is invalid. This is either due to a bad username or authentication information. (0xC000006D)
SPN: session setup failed before the SPN could be queried
```

Validation result

\\192.168.1.42

Token-Value List

xmlns

Token-Value Details

Display Name	Client Name	Token	Client Name
Separator	:	Terminator	\r\n
Description		Resolution	
Group		Tag	
Source type	Windows		

Figure 508

20.5.3 Using Default Template

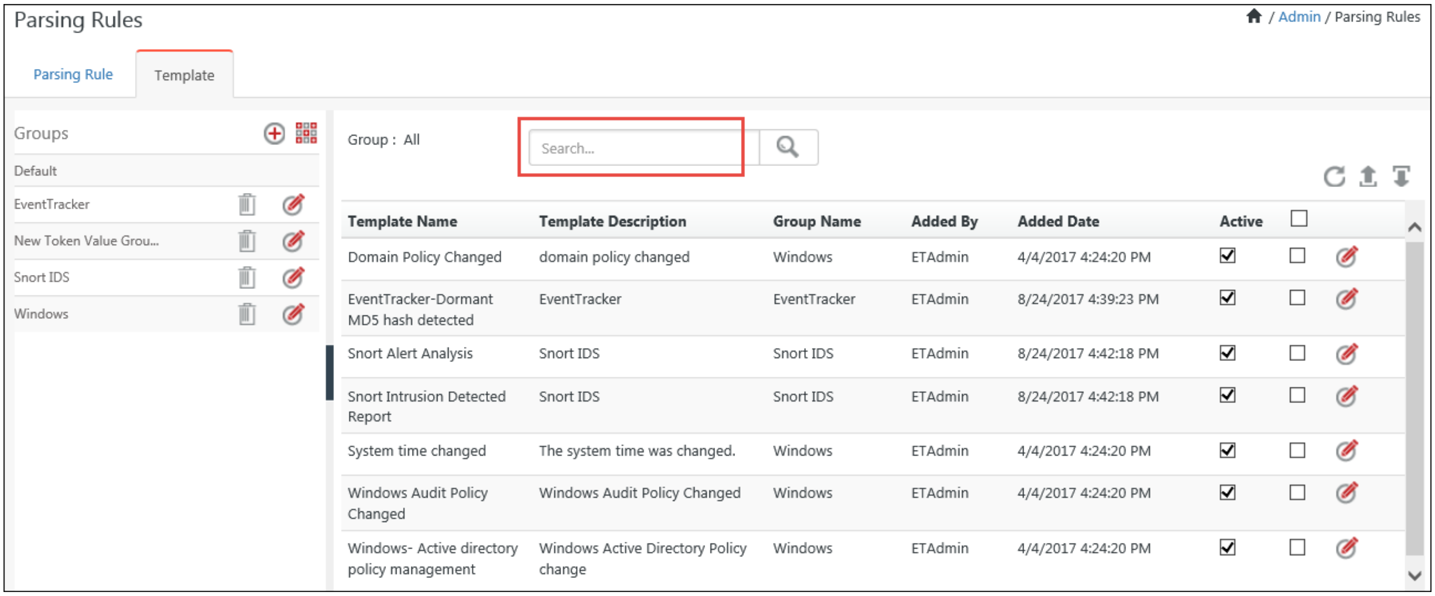
1 Select the **Admin**, and then select **Parsing Rules**.

The default Token-Value groups display. EventTracker provides predefined parsing rules.

2 Select the **Template** tab.

The Template group opens in the left pane and the Templates opens in the right pane.

3 To Search a group name, enter the name in the **Search** box and click search 🔍 .



Groups:
- Default
- EventTracker
- New Token Value Grou...
- Snort IDS
- Windows

Group : All

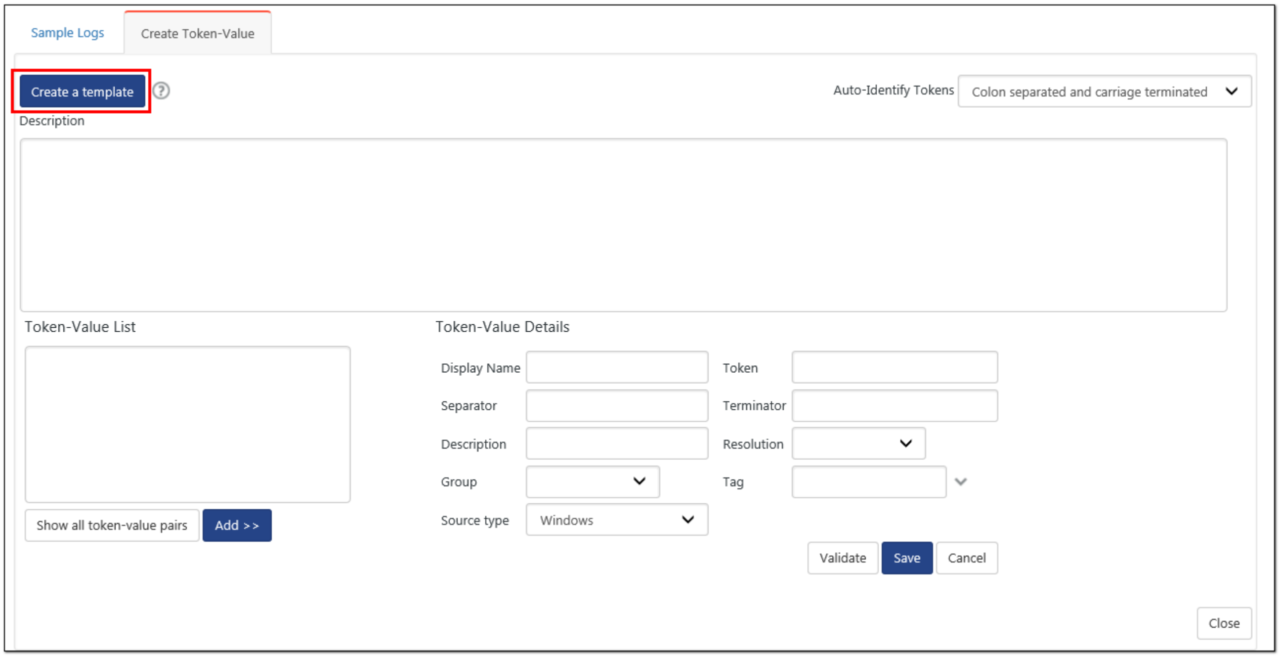
Template Name	Template Description	Group Name	Added By	Added Date	Active	☐	
Domain Policy Changed	domain policy changed	Windows	ETAdmin	4/4/2017 4:24:20 PM	☑	☐	✎
EventTracker-Dormant MD5 hash detected	EventTracker	EventTracker	ETAdmin	8/24/2017 4:39:23 PM	☑	☐	✎
Snort Alert Analysis	Snort IDS	Snort IDS	ETAdmin	8/24/2017 4:42:18 PM	☑	☐	✎
Snort Intrusion Detected Report	Snort IDS	Snort IDS	ETAdmin	8/24/2017 4:42:18 PM	☑	☐	✎
System time changed	The system time was changed.	Windows	ETAdmin	4/4/2017 4:24:20 PM	☑	☐	✎
Windows Audit Policy Changed	Windows Audit Policy Changed	Windows	ETAdmin	4/4/2017 4:24:20 PM	☑	☐	✎
Windows- Active directory policy management	Windows Active Directory Policy change	Windows	ETAdmin	4/4/2017 4:24:20 PM	☑	☐	✎

Figure 509

4 To export or import configuration, use **Export** ⭱ or **Import** ⭳ .

20.5.4 Creating a new template

1. In Token-Value Wizard, click **Create Token Value** tab,
2. Add description and click on **Create a Template.**

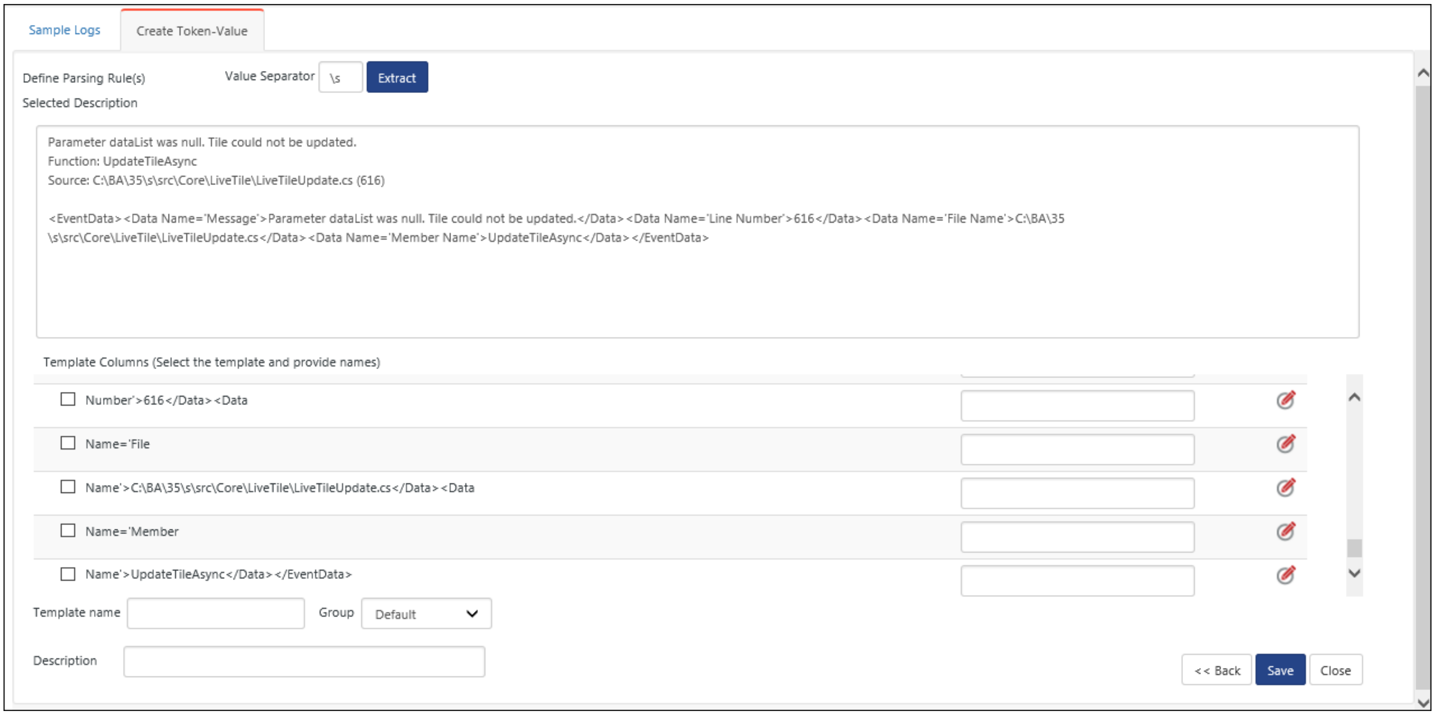


Auto-Identify Tokens: Colon separated and carriage terminated

Source type: Windows

Figure 510

The below page opens:



Define Parsing Rule(s)   Value Separator \s   Extract

Selected Description

```
Parameter dataList was null. Tile could not be updated.
Function: UpdateTileAsync
Source: C:\BA\35\s\src\Core\LiveTile\LiveTileUpdate.cs (616)

<EventData><Data Name='Message'>Parameter dataList was null. Tile could not be updated.</Data><Data Name='Line Number'>616</Data><Data Name='File Name'>C:\BA\35
\s\src\Core\LiveTile\LiveTileUpdate.cs</Data><Data Name='Member Name'>UpdateTileAsync</Data></EventData>
```

Template Columns (Select the template and provide names)

□ Number'>616</Data><Data

□ Name='File

□ Name'>C:\BA\35\s\src\Core\LiveTile\LiveTileUpdate.cs</Data><Data

□ Name='Member

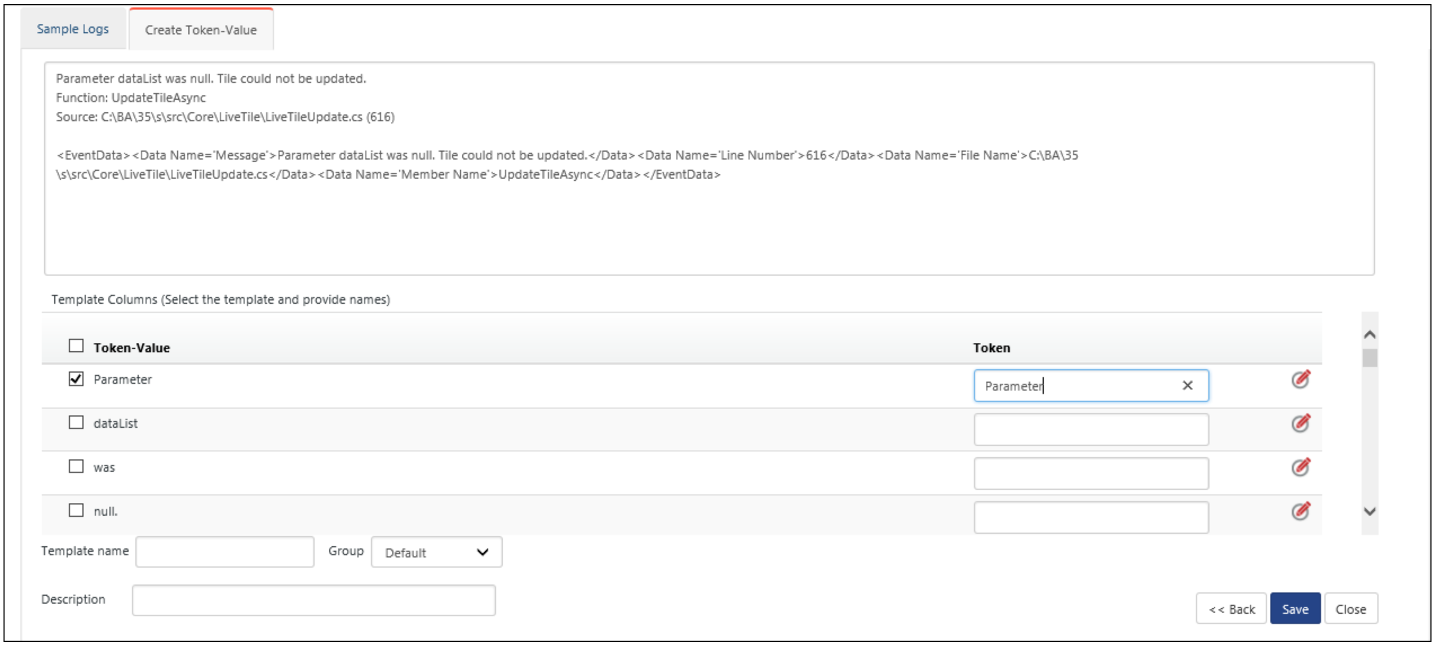
□ Name'>UpdateTileAsync</Data></EventData>

Template name   Group Default

Description

Figure 511

3. Enter the required changes in **Token Value** option and **Token**.
4. Enter a **Template name**.



```
Parameter dataList was null. Tile could not be updated.
Function: UpdateTileAsync
Source: C:\BA\35\s\src\Core\LiveTile\LiveTileUpdate.cs (616)

<EventData><Data Name='Message'>Parameter dataList was null. Tile could not be updated.</Data><Data Name='Line Number'>616</Data><Data Name='File Name'>C:\BA\35
\s\src\Core\LiveTile\LiveTileUpdate.cs</Data><Data Name='Member Name'>UpdateTileAsync</Data></EventData>
```

Template Columns (Select the template and provide names)

□ Token-Value	Token
☑ Parameter	Parameter
□ dataList	
□ was	
□ null.	

Template name   Group Default

Description

Figure 512

5. To filter the values further click the ✎ icon.
   EventTracker: Defined Template window opens.

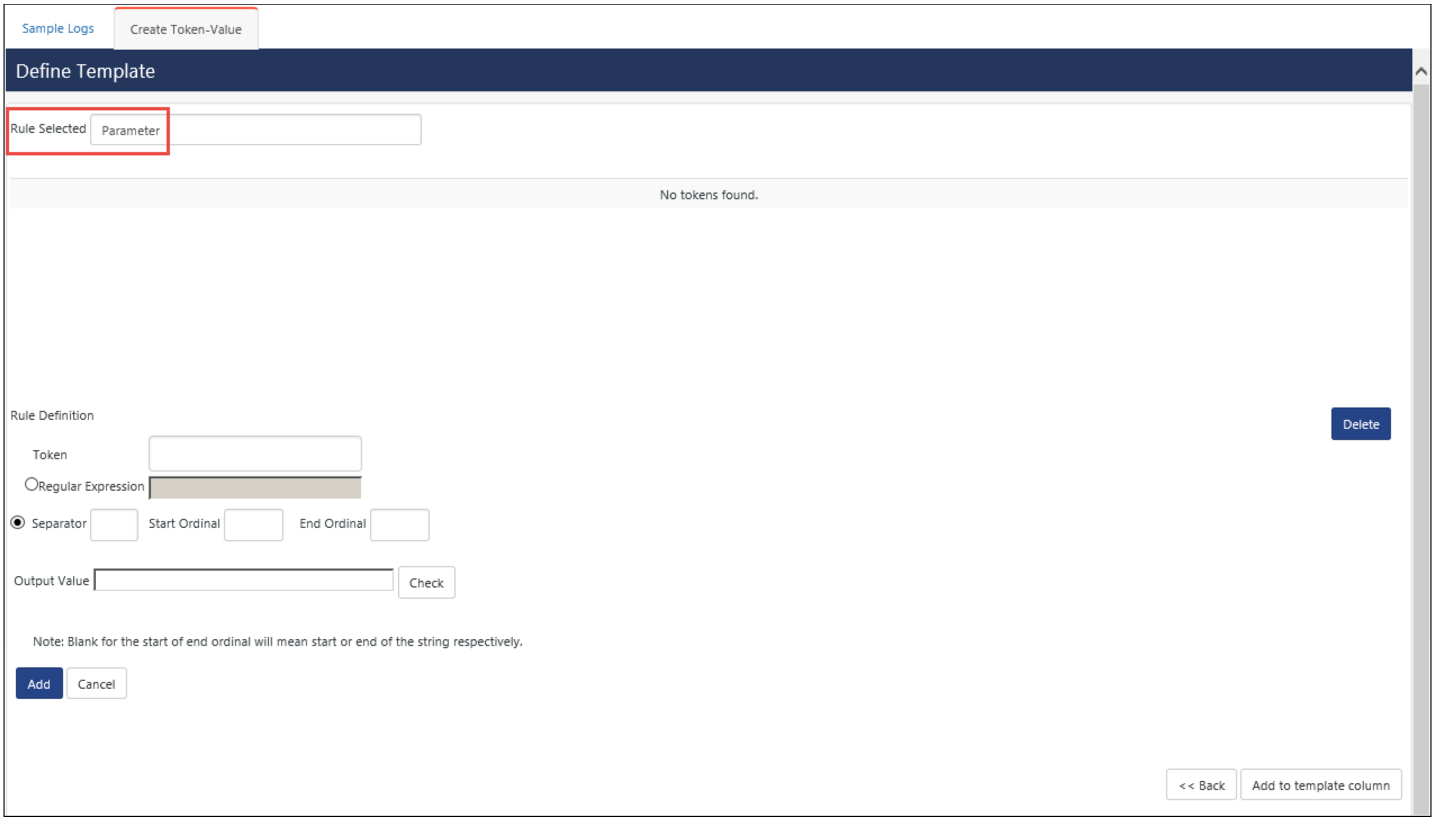
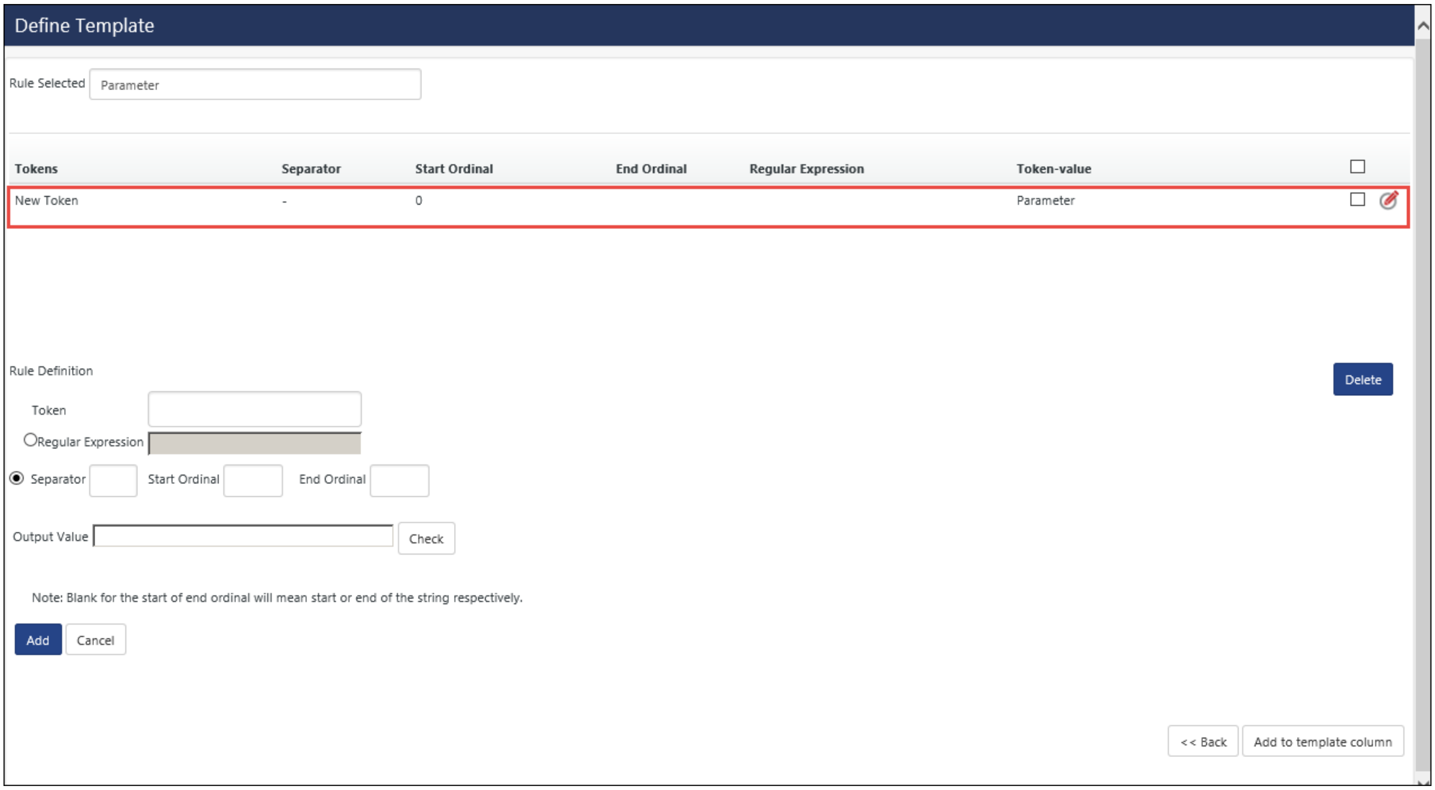


Figure 513

6. Enter the relevant data and then click **Add**.
   Ex: Enter a token name (i.e. New Token), Output value (i.e. Parameter).
   You can select Regular Expression or Separator. A regular expression is used to find a pattern.
   - Select a separator as '-'. It can be space, equal '=' symbol etc.
   - Select the ordinal values (i.e. Numeric) to further separate the rules.



Rule Selected: Parameter

Tokens	Separator	Start Ordinal	End Ordinal	Regular Expression	Token-value	□
New Token	-	0			Parameter	□

Token

○Regular Expression

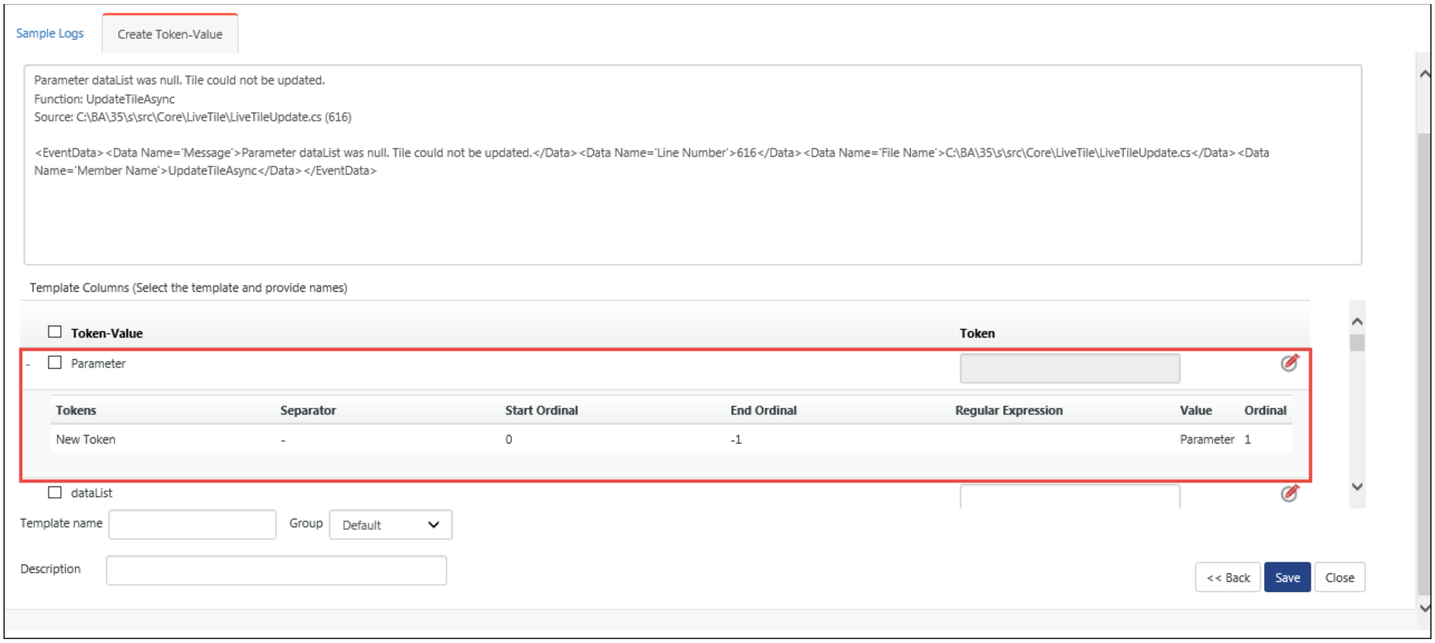
● Separator Start Ordinal End Ordinal

Output Value

Note: Blank for the start of end ordinal will mean start or end of the string respectively.

Figure 514

7. Click **Add to template column**.



```
Parameter dataList was null. Tile could not be updated.
Function: UpdateTileAsync
Source: C:\BA\35\s\src\Core\LiveTile\LiveTileUpdate.cs (616)

<EventData><Data Name='Message'>Parameter dataList was null. Tile could not be updated.</Data><Data Name='Line Number'>616</Data><Data Name='File Name'>C:\BA\35\s\src\Core\LiveTile\LiveTileUpdate.cs</Data><Data
Name='Member Name'>UpdateTileAsync</Data></EventData>
```

Template Columns (Select the template and provide names)

□ Token-Value	Token
□ Parameter	
□ dataList	

Tokens	Separator	Start Ordinal	End Ordinal	Regular Expression	Value	Ordinal
New Token	-	0	-1		Parameter	1

Template name

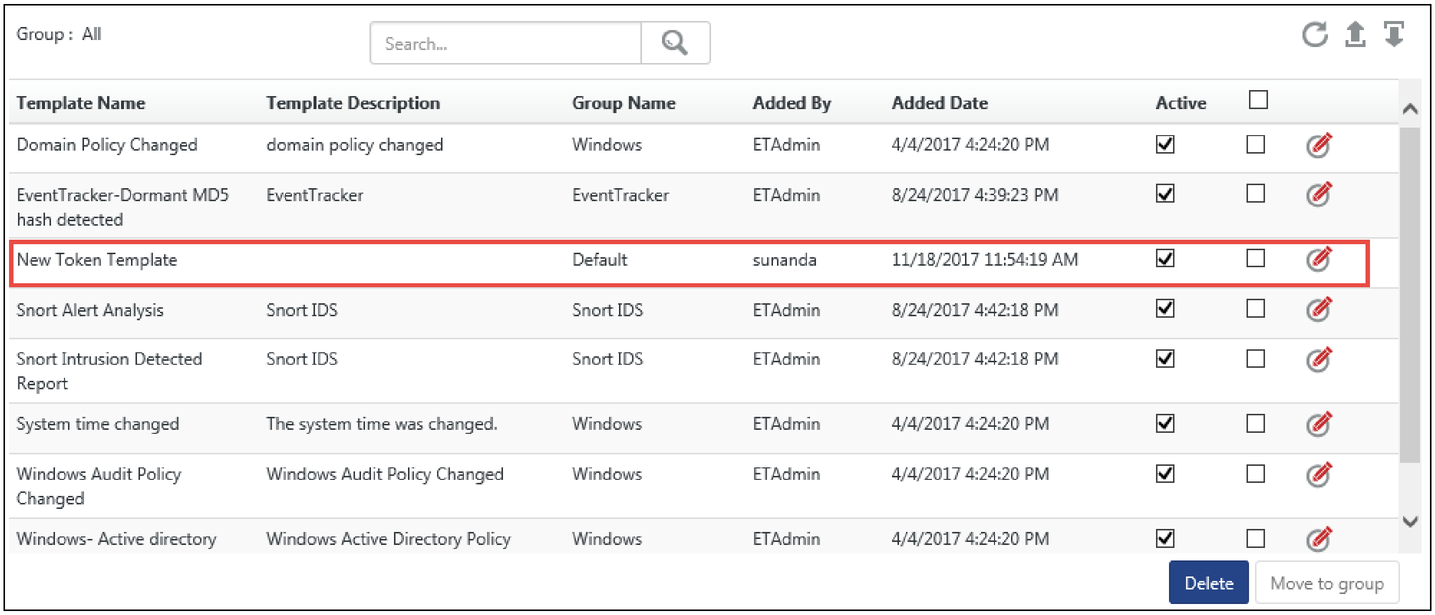
Group: Default

Description

Figure 515

8. Click **Save**.

Now, In Define Parsing Rule(s) window, the created new template opens in **Template** tab.



Template Name	Template Description	Group Name	Added By	Added Date	Active	□
Domain Policy Changed	domain policy changed	Windows	ETAdmin	4/4/2017 4:24:20 PM	☑	□
EventTracker-Dormant MD5 hash detected	EventTracker	EventTracker	ETAdmin	8/24/2017 4:39:23 PM	☑	□
New Token Template		Default	sunanda	11/18/2017 11:54:19 AM	☑	□
Snort Alert Analysis	Snort IDS	Snort IDS	ETAdmin	8/24/2017 4:42:18 PM	☑	□
Snort Intrusion Detected Report	Snort IDS	Snort IDS	ETAdmin	8/24/2017 4:42:18 PM	☑	□
System time changed	The system time was changed.	Windows	ETAdmin	4/4/2017 4:24:20 PM	☑	□
Windows Audit Policy Changed	Windows Audit Policy Changed	Windows	ETAdmin	4/4/2017 4:24:20 PM	☑	□
Windows- Active directory	Windows Active Directory Policy	Windows	ETAdmin	4/4/2017 4:24:20 PM	☑	□

Figure 516

20.6 Generating a Flex Reports

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

2 Click **New** 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. 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 opens 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>>.**

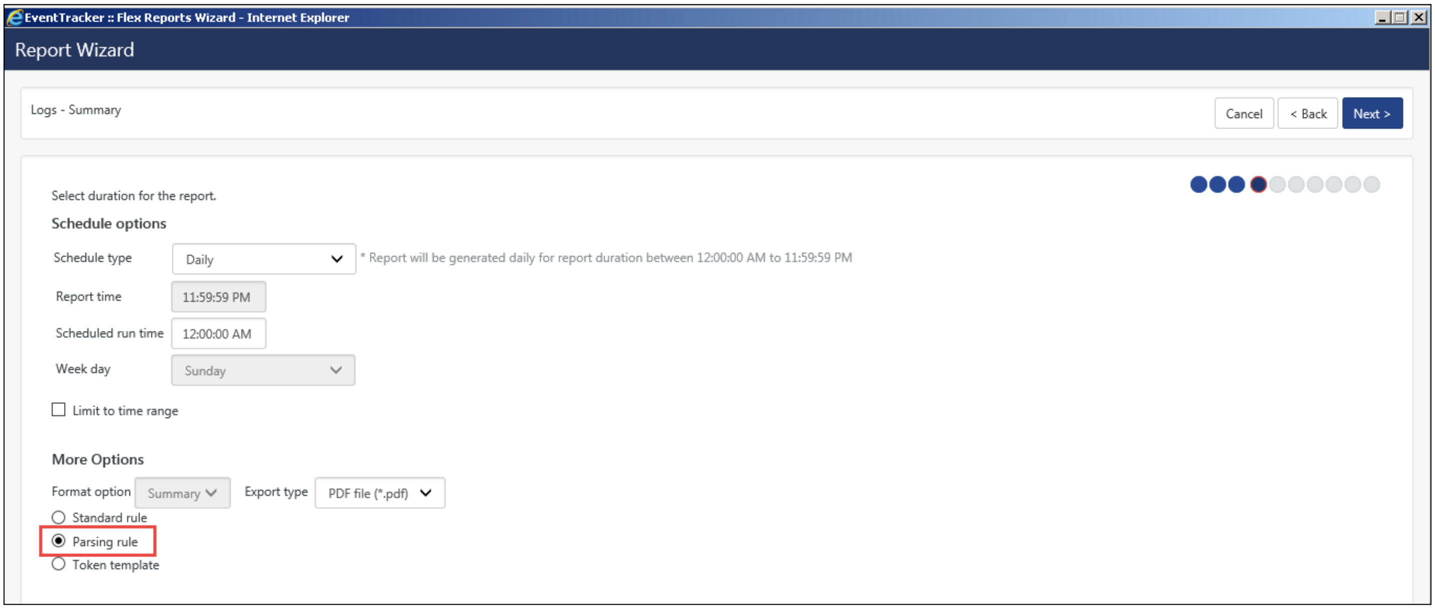
8 Select the required **Interval** and **Limit to time Range option.**

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

Select duration for the report.

Schedule options

Schedule type: Daily

* Report will be generated daily for report duration between 12:00:00 AM to 11:59:59 PM

Report time: 11:59:59 PM

Scheduled run time: 12:00:00 AM

Week day: Sunday

□ Limit to time range

More Options

Format option: Summary

Export type: PDF file (*.pdf)

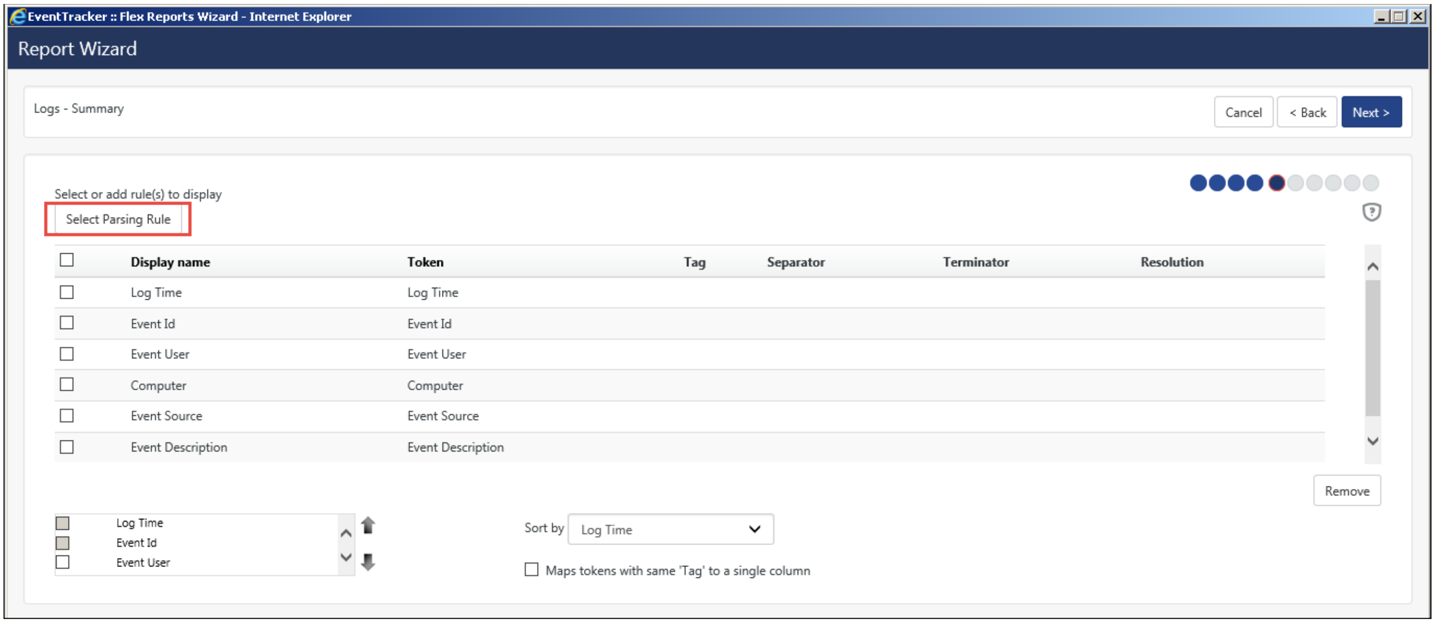
○ Standard rule

● Parsing rule

○ Token template

Figure 517

Logs Summary opens to select the parsing rule.



Logs - Summary

Select or add rule(s) to display

□	Display name	Token	Tag	Separator	Terminator	Resolution
□	Log Time	Log Time				
□	Event Id	Event Id				
□	Event User	Event User				
□	Computer	Computer				
□	Event Source	Event Source				
□	Event Description	Event Description				

□ Log Time

□ Event Id

□ Event User

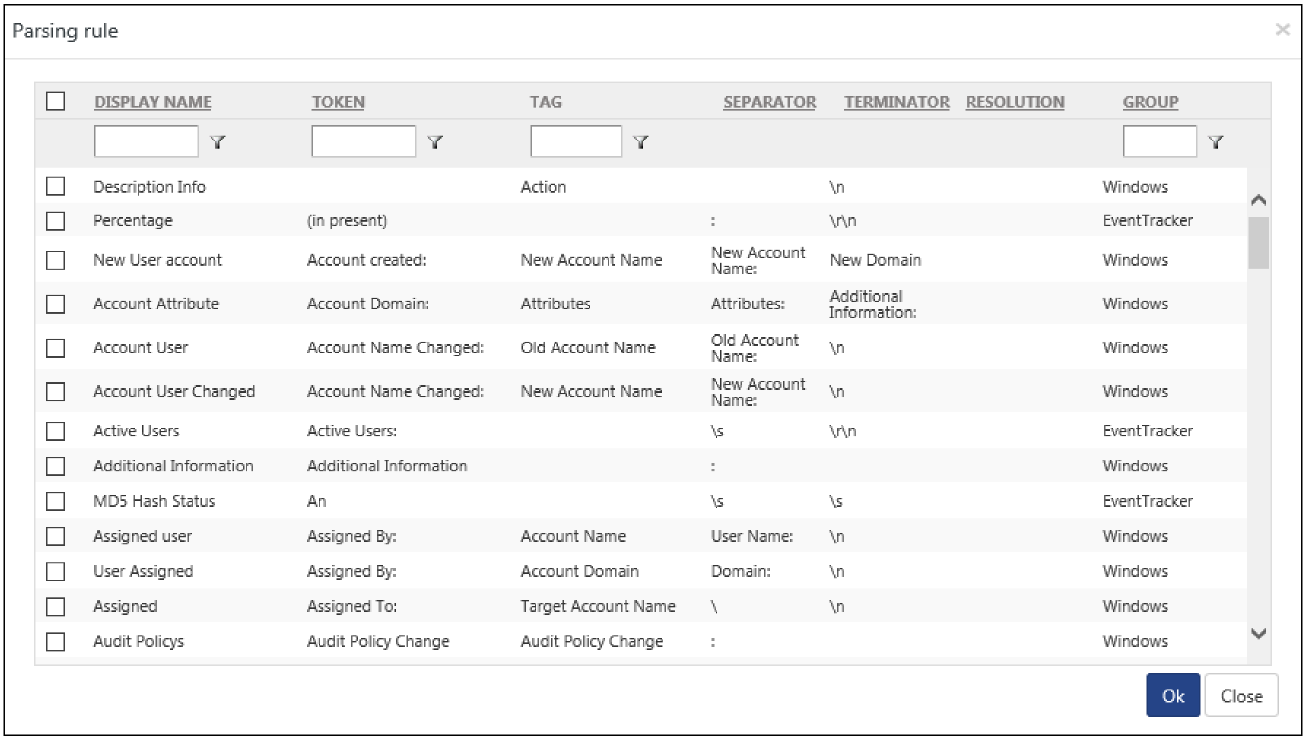
Sort by: Log Time

□ Maps tokens with same 'Tag' to a single column

Figure 518

b. Click **Select Parsing Rule** hyperlink.

Search Parsing Rule window opens.



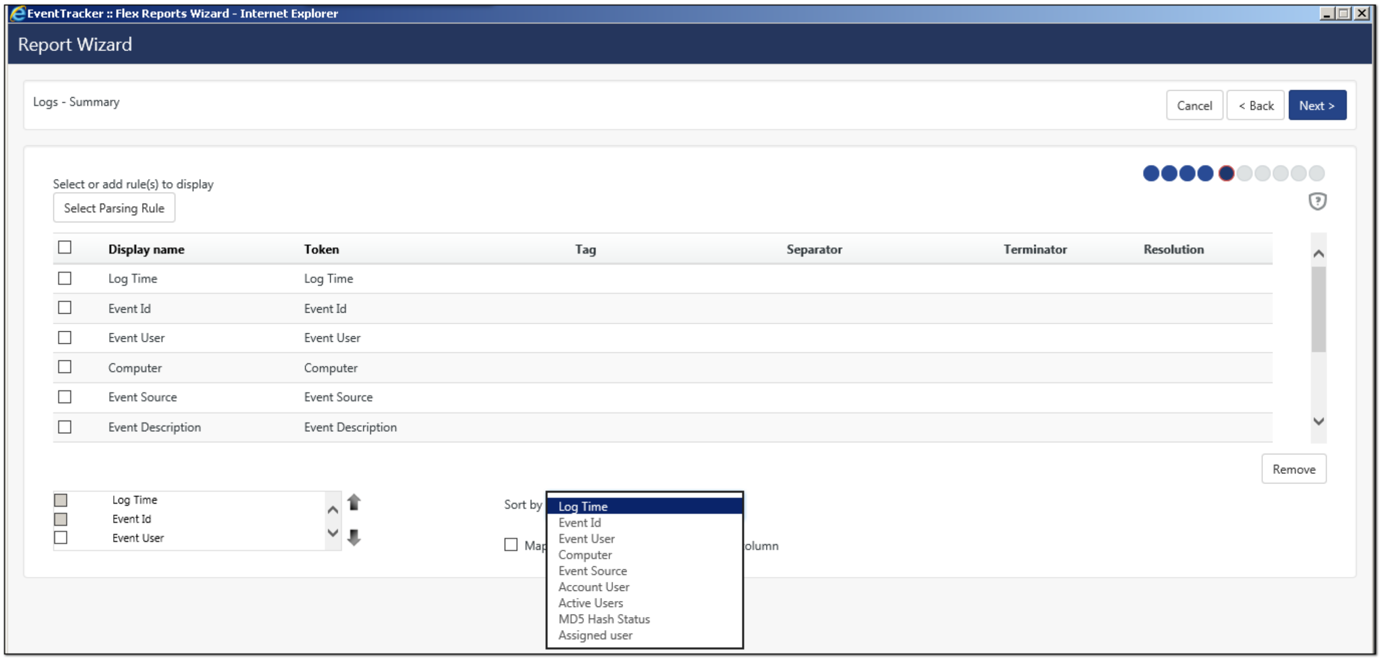
Parsing rule

☐	DISPLAY NAME	TOKEN	TAG	SEPARATOR	TERMINATOR	RESOLUTION	GROUP
☐	Description Info		Action		\n		Windows
☐	Percentage	(in present)		:	\r\n		EventTracker
☐	New User account	Account created:	New Account Name	New Account Name:	New Domain		Windows
☐	Account Attribute	Account Domain:	Attributes	Attributes:	Additional Information:		Windows
☐	Account User	Account Name Changed:	Old Account Name	Old Account Name:	\n		Windows
☐	Account User Changed	Account Name Changed:	New Account Name	New Account Name:	\n		Windows
☐	Active Users	Active Users:		\s	\r\n		EventTracker
☐	Additional Information	Additional Information		:			Windows
☐	MD5 Hash Status	An		\s	\s		EventTracker
☐	Assigned user	Assigned By:	Account Name	User Name:	\n		Windows
☐	User Assigned	Assigned By:	Account Domain	Domain:	\n		Windows
☐	Assigned	Assigned To:	Target Account Name	\	\n		Windows
☐	Audit Policys	Audit Policy Change	Audit Policy Change	:			Windows

Figure 519

c. Select the required options and then click **OK**.

Logs Summary (i.e. Step 5) displays.



EventTracker :: Flex Reports Wizard - Internet Explorer

Report Wizard

Logs - Summary

Select or add rule(s) to display

☐	Display name	Token	Tag	Separator	Terminator	Resolution
☐	Log Time	Log Time				
☐	Event Id	Event Id				
☐	Event User	Event User				
☐	Computer	Computer				
☐	Event Source	Event Source				
☐	Event Description	Event Description				

☐ Log Time
☐ Event Id
☐ Event User

Sort by Log Time

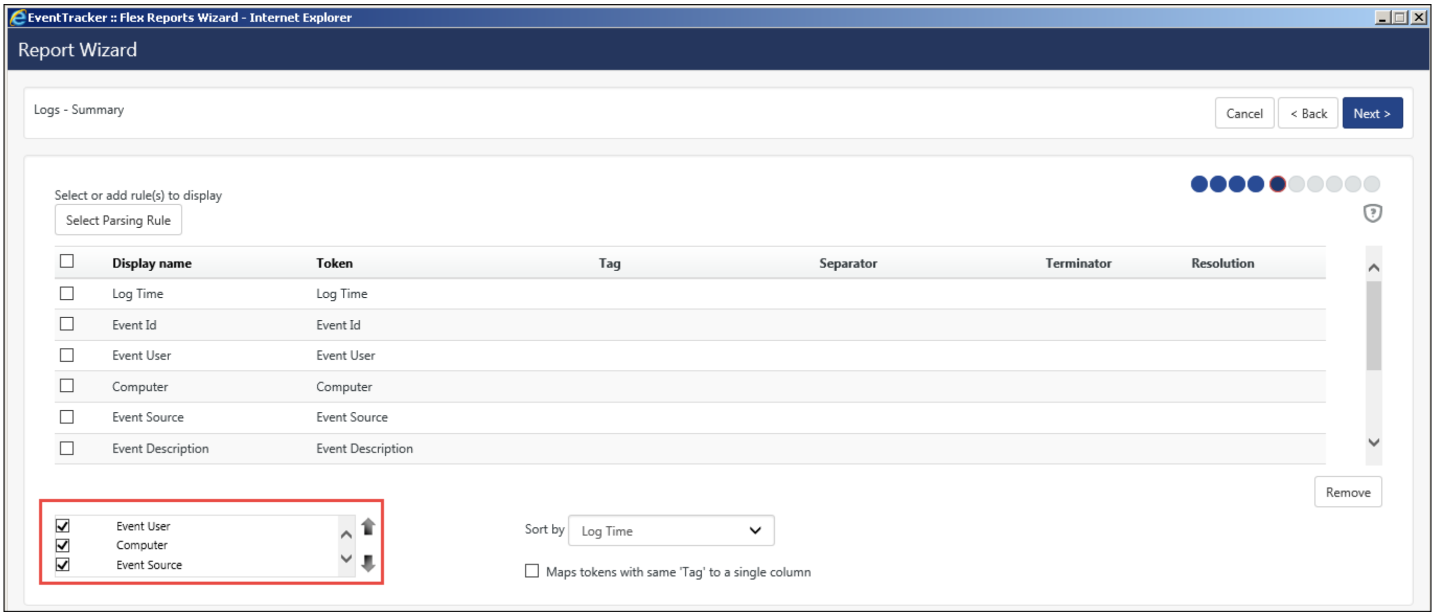
☐ Map[...]olumn

Figure 520

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)
f. If you select **Token Template**, click **Next>>.**
g. Select a template. (i.e. enter the template name which you had earlier configured in Parsing Rules – Token Value Wizard)

h. Select/Enter the required options and then click **Next>>.**


EventTracker :: Flex Reports Wizard - Internet Explorer
Report Wizard
Logs - Summary
Cancel
< Back
Next >
Select or add rule(s) to display
Select Parsing Rule
Remove

☐	Display name	Token	Tag	Separator	Terminator	Resolution
☐	Log Time	Log Time				
☐	Event Id	Event Id				
☐	Event User	Event User				
☐	Computer	Computer				
☐	Event Source	Event Source				
☐	Event Description	Event Description				

☑ Event User
☑ Computer
☑ Event Source

Sort by Log Time

☐ Maps tokens with same 'Tag' to a single column

Figure 521

----

11 Click **Next>>**.
12 Enter the appropriate **Refine** and **Filter** details.
13 Click **Next>>**.
14 Enter the relevant **Title**, **Header**, **Footer**, and **Description** data.
15 Click **Next>>**.
   Review cost details and configure the publishing options window opens.

NOTE

Publishing options are disabled because On Demand (foreground processing) has been selected.

16 Click **Next>>**.
   The last step of **Completing Report Configuration Wizard** opens.
17 Select **Generate Report.**

21. Reports Settings

In this chapter, you will learn how to:

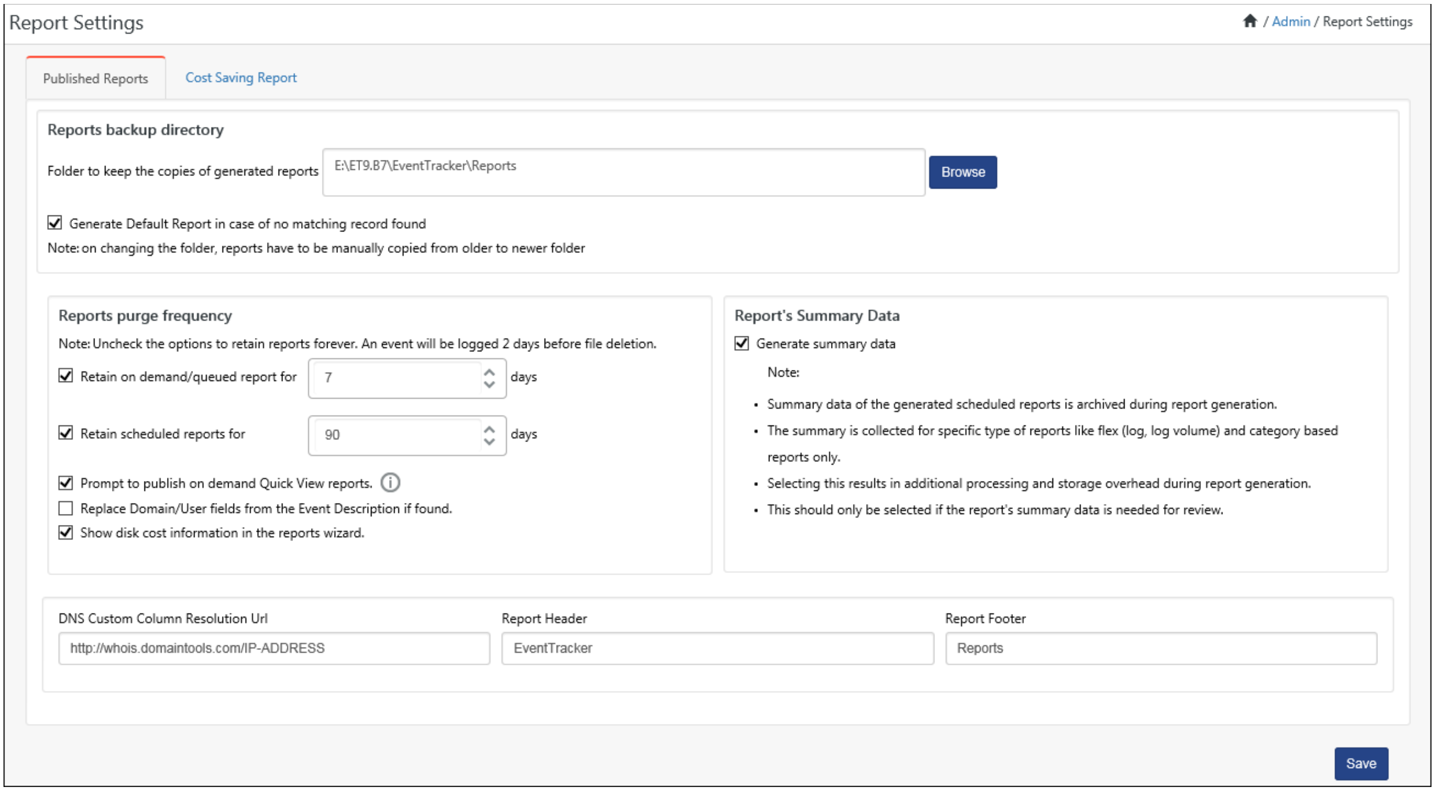
- Configure Published Reports
- Configure Cost Saving Report

21.1 Configuring Published Reports

This option helps to configure published reports settings.

1 Click the **Admin**, and then click **Report Settings**.

EventTracker opens the **Published Reports** tab.



Report Settings

Reports backup directory

Folder to keep the copies of generated reports: E:\ET9.B7\EventTracker\Reports

☑ Generate Default Report in case of no matching record found

Note: on changing the folder, reports have to be manually copied from older to newer folder

Reports purge frequency

Note: Uncheck the options to retain reports forever. An event will be logged 2 days before file deletion.

☑ Retain on demand/queued report for 7 days

☑ Retain scheduled reports for 90 days

☑ Prompt to publish on demand Quick View reports.

☐ Replace Domain/User fields from the Event Description if found.

☑ Show disk cost information in the reports wizard.

Report's Summary Data

☑ Generate summary data

Note:

- Summary data of the generated scheduled reports is archived during report generation.
- The summary is collected for specific type of reports like flex (log, log volume) and category based reports only.
- Selecting this results in additional processing and storage overhead during report generation.
- This should only be selected if the report's summary data is needed for review.

DNS Custom Column Resolution Url: http://whois.domaintools.com/IP-ADDRESS

Report Header: EventTracker

Report Footer: Reports

Figure 522

Field	Description
Reports backup directory	Folder to keep copies of generated reports. By default, EventTracker saves the reports in ...\Program Files\Prism Microsystems\EventTracker\Reports folder. You can select a different folder as you wish. On changing the folder, manually copy the reports from old to new folder
Generate Default Report in case of no matching record found	If checked, EventTracker will generate a PDF with the message "No Matching Record Found," if there are no matching records found for the Queued or Scheduled reports. The PDF will be generated irrespective of the report format type.
Reports purge frequency	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 -> EventTracker -> EventTracker: Published reports cleanup Category. 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.
Report's Summary Data	If checked, EventTracker will create summary data of the generated scheduled report during report generation. The summary is collected for specific type of reports like flex (log, log volume) and category based reports only.
Prompt to publish on demand Quick View repots	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.
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.

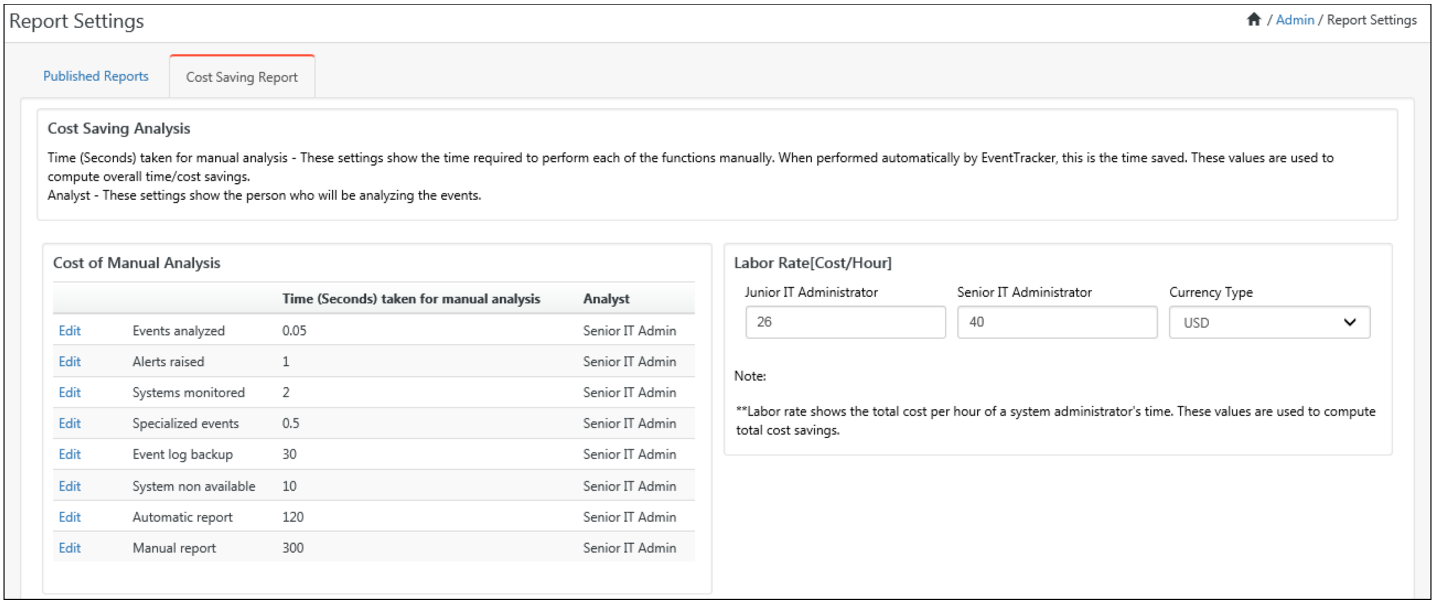
Table 62

Event Id	Description
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.

Table 63

21.2 Configuring Cost Saving Report Settings

1 Click the **Cost Saving Analysis** tab.



Cost Saving Analysis

Time (Seconds) taken for manual analysis - These settings show the time required to perform each of the functions manually. When performed automatically by EventTracker, this is the time saved. These values are used to compute overall time/cost savings.
Analyst - These settings show the person who will be analyzing the events.

Cost of Manual Analysis

		Time (Seconds) taken for manual analysis	Analyst
Edit	Events analyzed	0.05	Senior IT Admin
Edit	Alerts raised	1	Senior IT Admin
Edit	Systems monitored	2	Senior IT Admin
Edit	Specialized events	0.5	Senior IT Admin
Edit	Event log backup	30	Senior IT Admin
Edit	System non available	10	Senior IT Admin
Edit	Automatic report	120	Senior IT Admin
Edit	Manual report	300	Senior IT Admin

Labor Rate[Cost/Hour]

Junior IT Administrator: 26
Senior IT Administrator: 40
Currency Type: USD

Note:

**Labor rate shows the total cost per hour of a system administrator's time. These values are used to compute total cost savings.

Figure 523

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.

🗎 NOTE

Before generating any cost saving analysis, please ensure that the Collect cost savings information checkbox is enabled in Admin menu -> Manager -> Configuration (Cost Saving Report).

22. Manage System Groups

In this chapter, you will learn how to:

- Auto Discover System Groups
- Add Computers Manually
- Add Logical System Group
- Manage Asset Value
- Delete Systems
- Systems Report

22.1 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.

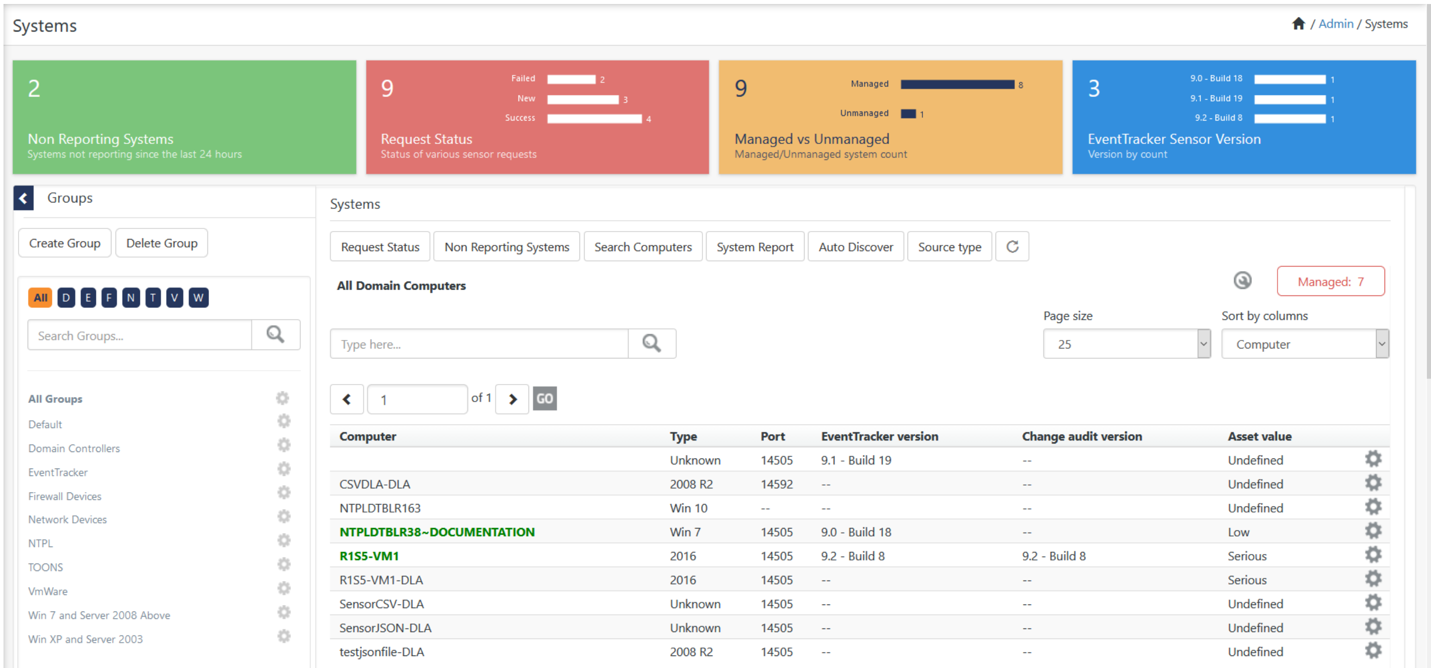
Systems manager helps you to:

- 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

22.1.1 Starting System Manager

1. Click the **Admin**, and then select **Systems**.

   EventTracker opens **Systems Manager** screen.



Computer	Type	Port	EventTracker version	Change audit version	Asset value
	Unknown	14505	9.1 - Build 19	--	Undefined
CSVDLA-DLA	2008 R2	14592	--	--	Undefined
NTPLDTBLR163	Win 10	--	--	--	Undefined
NTPLDTBLR38~DOCUMENTATION	Win 7	14505	9.0 - Build 18	--	Low
R1S5-VM1	2016	14505	9.2 - Build 8	9.2 - Build 8	Serious
R1S5-VM1-DLA	2016	14505	--	--	Serious
SensorCSV-DLA	Unknown	14505	--	--	Undefined
SensorJSON-DLA	Unknown	14505	--	--	Undefined
testjsonfile-DLA	2008 R2	14505	--	--	Undefined

Figure 524

Field	Description
Computer	Name of the computer or name of the DLA / NetFlow instance.
Type	Operating system installed on the computer.
EventTracker Port	Port through which the EventTracker Windows agent and the EventTracker manager communicates.
EventTracker Version	Displays EventTracker version and build number.
Change Audit Version	Displays Change Audit version and build number.
Asset Value	Asset value indicates how important or critical the computer is.

Table 64

Click	To
Create Group	Create logical system groups.
Delete Group	Delete logical system groups.
Interface Manager	Modify Netflow interface details.
Request Status	Checks install / upgrade / uninstall status of EventTracker Windows agent / Change Audit agent. Also, to check status of computer search.
Non Reporting Systems	Search a list of systems which have not reported any events to the EventTracker manager in a specific duration of time.
Search Computers	Manually add enterprise domains and computers.
System Report	Generate status report of managed and unmanaged computers.
Auto Discover	Automatically discover enterprise domains and computers.
Source type	

Table 65

22.2 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.

22.2.1 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**, and then click **Systems**.

2 Click **Auto Discover** at the upper-right corner.

System manager opens the confirmation message.

3 Click **Ok**.
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.

22.2.2 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.

22.3 Adding Computers Manually

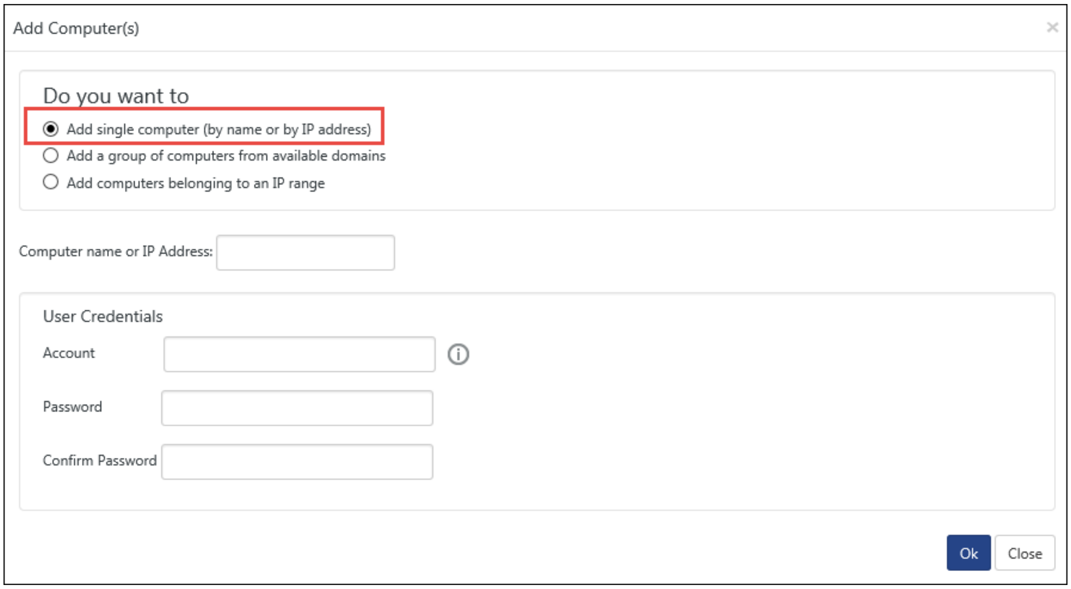
In 'Auto discover' mode, the 'System' manager automatically discovers domains and computers when you keep adding them in your enterprise. All you need to do is to refresh the System manager. However, in 'Manual' mode, you have to add them explicitly.

22.3.1 Adding a Single Computer

This option enables you to add a computer.

1 Click the **Admin** dropdown, and then click **Systems**.
EventTracker open the **Systems** manager page.

2 Click **Search Computers** button.
System Manager opens the **Add Computer(s)** pop-up window.



Add Computer(s)

Do you want to

● Add single computer (by name or by IP address)

○ Add a group of computers from available domains

○ Add computers belonging to an IP range

Computer name or IP Address:

User Credentials

Account

Password

Confirm Password

Figure 525

3 Select the **Add a single computer (by name or by IP address)** option, if not selected.

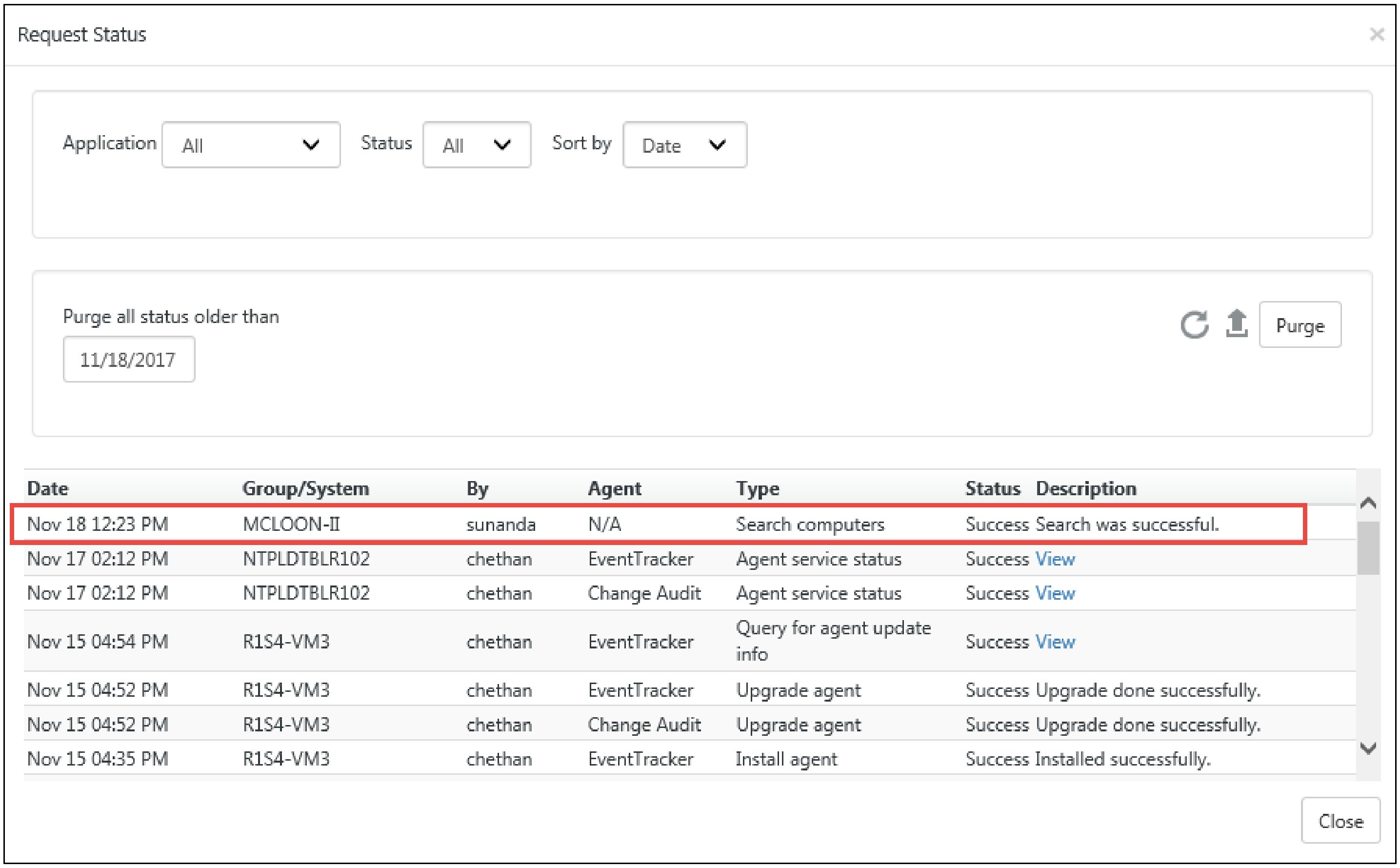
4 Type the name of the computer in the **Enter computer name or IP Address** field.

5 Provide valid **User Credentials**, and then click **Ok**.

System manager opens the message box.

6 Click **OK**, and then click ↻ icon to refresh the **Systems** manager.

7 Click **Request Status** to view the status.



Request Status

Application All | Status All | Sort by Date

Purge all status older than 11/18/2017

Date	Group/System	By	Agent	Type	Status	Description
Nov 18 12:23 PM	MCLOON-II	sunanda	N/A	Search computers	Success	Search was successful.
Nov 17 02:12 PM	NTPLDTBLR102	chethan	EventTracker	Agent service status	Success	View
Nov 17 02:12 PM	NTPLDTBLR102	chethan	Change Audit	Agent service status	Success	View
Nov 15 04:54 PM	R1S4-VM3	chethan	EventTracker	Query for agent update info	Success	View
Nov 15 04:52 PM	R1S4-VM3	chethan	EventTracker	Upgrade agent	Success	Upgrade done successfully.
Nov 15 04:52 PM	R1S4-VM3	chethan	Change Audit	Upgrade agent	Success	Upgrade done successfully.
Nov 15 04:35 PM	R1S4-VM3	chethan	EventTracker	Install agent	Success	Installed successfully.

Figure 526

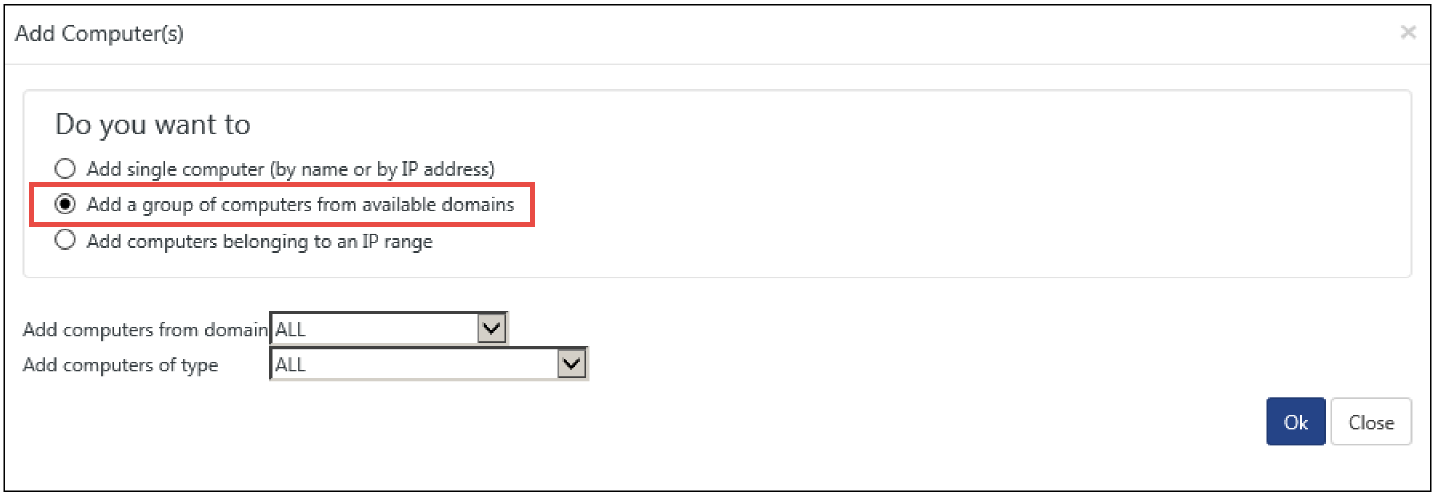
22.3.2 Adding a Group of Computers

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.



Add Computer(s)

Do you want to

○ Add single computer (by name or by IP address)

● Add a group of computers from available domains

○ Add computers belonging to an IP range

Add computers from domain: ALL

Add computers of type: ALL

Figure 527

Field	Description
Add computers from domain	This drop-down list lists the available domains. Select a domain from where you want to add computers.
Add computers of type	Select a system type from the drop-down list.

Table 66

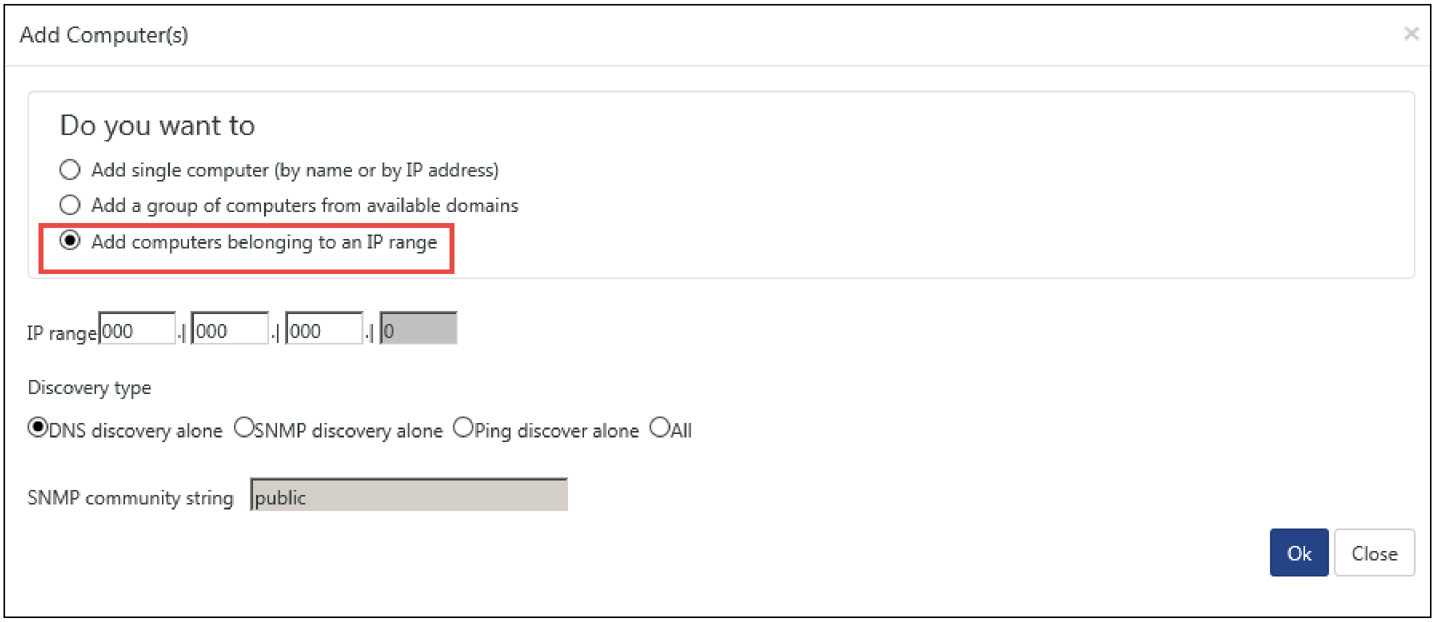
2 Select appropriate options, and then click **OK**.
A **Message from webpage** window opens.

3 Click the ↻ icon to refresh the **Systems** manager to view Request Status.

22.3.3 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.



Add Computer(s)

Do you want to

○ Add single computer (by name or by IP address)

○ Add a group of computers from available domains

● Add computers belonging to an IP range

IP range 000 .| 000 .| 000 .| 0

Discovery type

● DNS discovery alone ○ SNMP discovery alone ○ Ping discover alone ○ All

SNMP community string public

Figure 528

Field	Description
IP range	Type the IP address range to be added.
DNS discovery alone	The specified IP range will be discovered using DNS method.
SNMP discovery alone	The specified IP range will be discovered using SNMP method.
Ping discover alone	The specified IP range will be discovered using Ping method.
All	The specified IP range will be discovered using DNS /SNMP/Ping method.
SNMP community string	A password which is necessary to read/write SNMP data.

Table 67

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.

22.4 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.

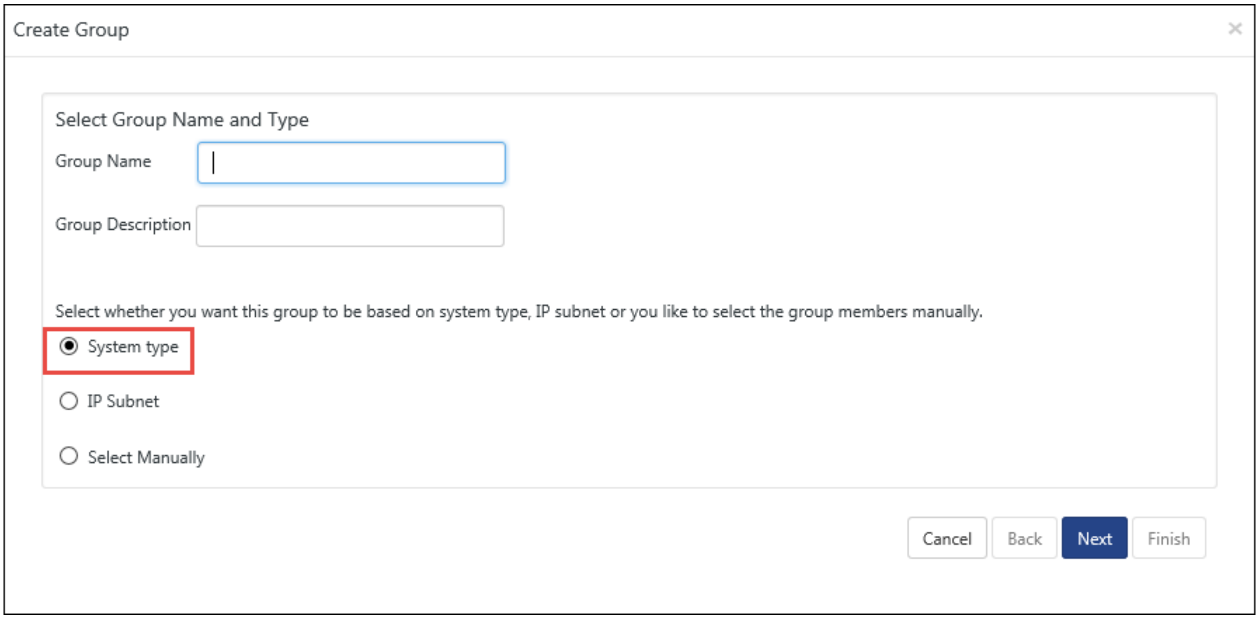
22.4.1 Creating a New Logical Group – System Type

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 **Create Group**.

System manager opens the **Create Group** dialog box window.



Create Group

Select Group Name and Type

Group Name

Group Description

Select whether you want this group to be based on system type, IP subnet or you like to select the group members manually.

● System type

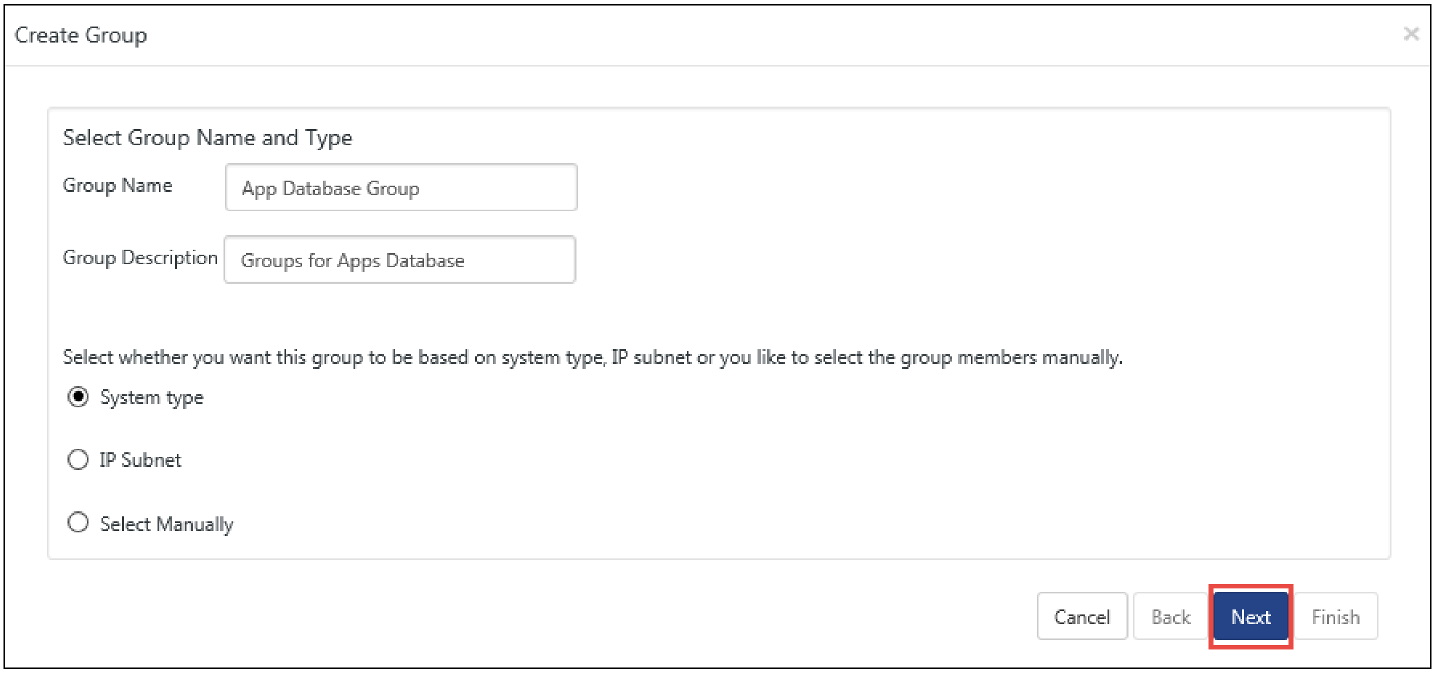
○ IP Subnet

○ Select Manually

Figure 529

Field	Description
Group Name	Type the group name in this field. The group name should be unique.
Group Description	Type the group description in this field.
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.

Table 68


Create Group

Select Group Name and Type

Group Name: App Database Group

Group Description: Groups for Apps Database

Select whether you want this group to be based on system type, IP subnet or you like to select the group members manually.

● System type

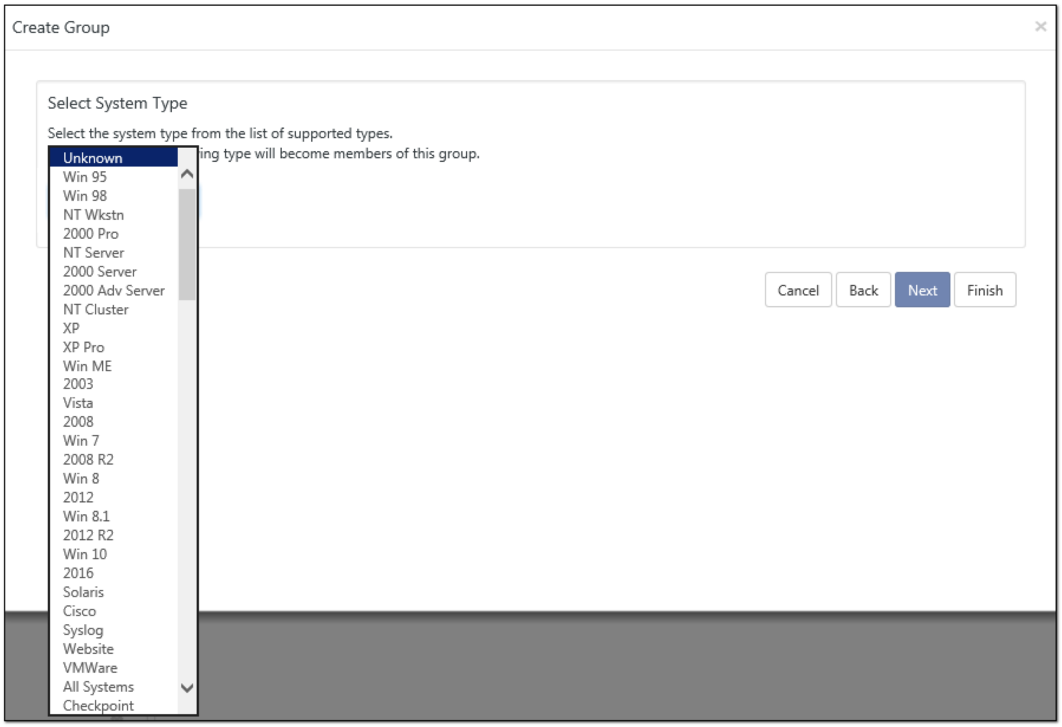
○ IP Subnet

○ Select Manually

Figure 530

3 Enter appropriate data in relevant fields, and then click **Next**.

If you select the **System Type** option, **System** Manager opens the **Create Group** dialog box with the option to select O/S type.


Create Group

Select System Type

Select the system type from the list of supported types.

ing type will become members of this group.

Unknown
Win 95
Win 98
NT Wkstn
2000 Pro
NT Server
2000 Server
2000 Adv Server
NT Cluster
XP
XP Pro
Win ME
2003
Vista
2008
Win 7
2008 R2
Win 8
2012
Win 8.1
2012 R2
Win 10
2016
Solaris
Cisco
Syslog
Website
VMWare
All Systems
Checkpoint

Figure 531

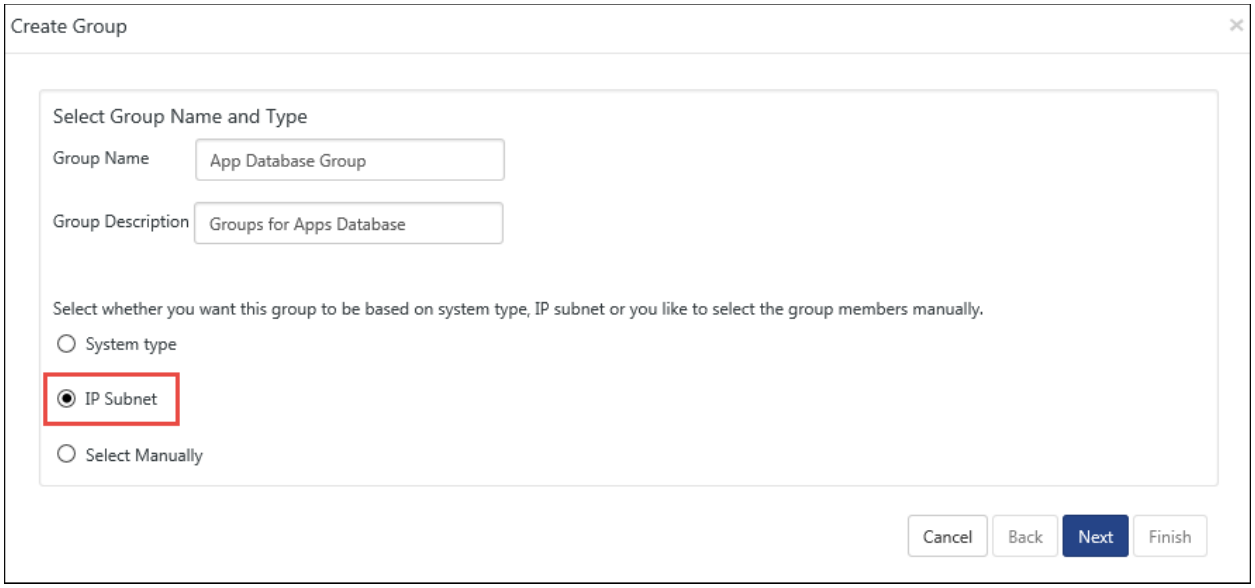
4 Select the system type from the **Select System Type** drop-down list and then click **Finish**.

System Manager creates and populates the newly created system group with the systems that have O/S type selected.

22.4.2 Creating 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.


Create Group

Select Group Name and Type

Group Name: App Database Group

Group Description: Groups for Apps Database

Select whether you want this group to be based on system type, IP subnet or you like to select the group members manually.

○ System type

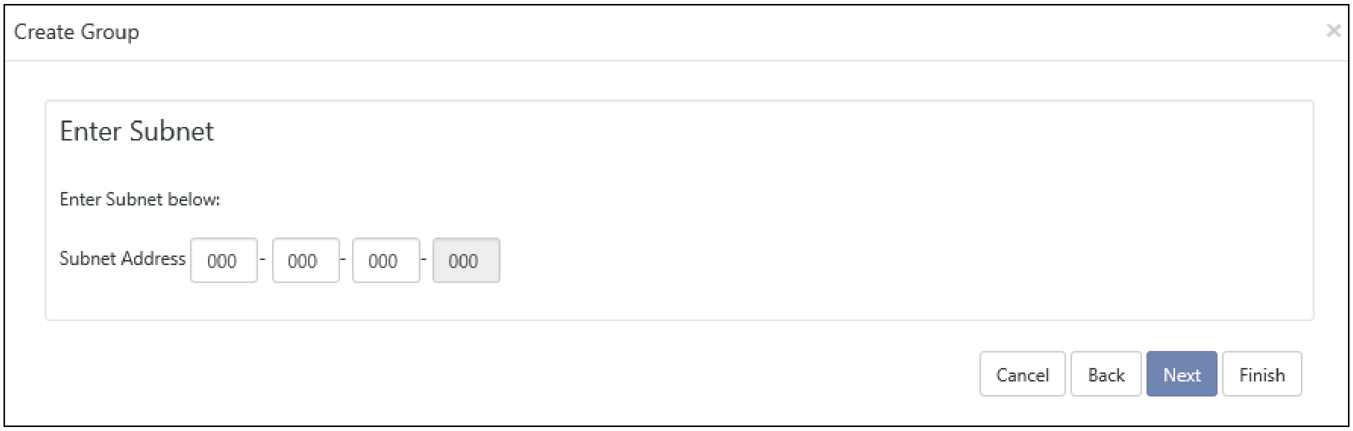
● IP Subnet

○ Select Manually

Figure 532

2 Click **Next**.

System Manager opens the **Enter Subnet** pane.


Create Group

Enter Subnet

Enter Subnet below:

Subnet Address 000 - 000 - 000 - 000

Figure 533

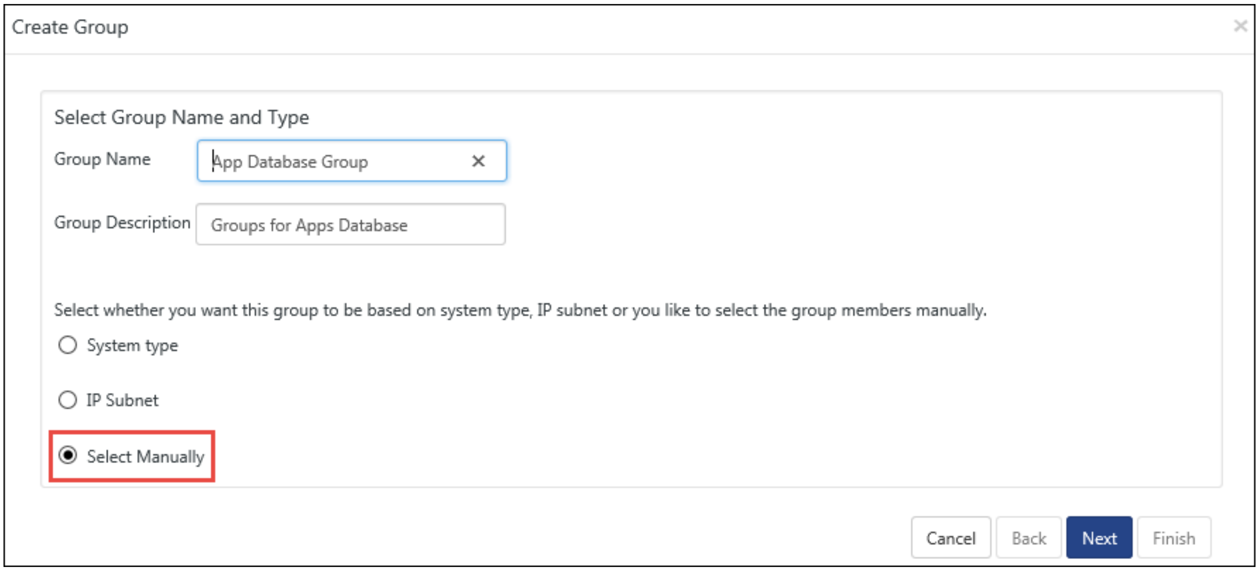
3 Type the **Subnet Address**, and then click **Finish**.

System Manager creates and populates the newly created system group with the systems from the IP subnet selected.

22.4.3 Creating 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

Select Group Name and Type

Group Name: App Database Group

Group Description: Groups for Apps Database

Select whether you want this group to be based on system type, IP subnet or you like to select the group members manually.

○ System type

○ IP Subnet

● Select Manually

Figure 534

2. Click **Next**.

System Manager opens the Create Group pop-up window with the option to select managed and unmanaged systems.

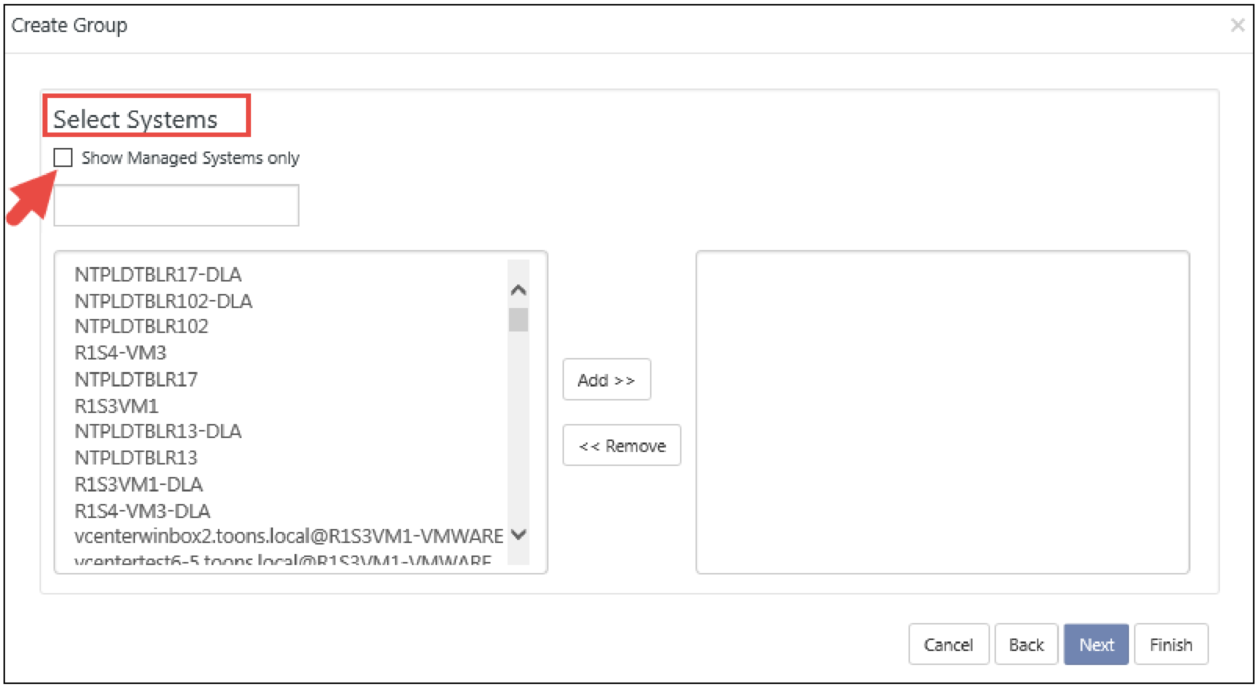


Figure 535

Field	Description
Description	Type the system-related information in this field.
Group Members	Select the computer that you want to remove from the group. Click <<Remove.
Available Systems	Select the computer that you want to add to the group. Click Add>>. The selected computer is added to the list of Group Members.
Port	Select the port number from the dropdown list.

Table 69

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 click **Add>>** button.
5. Click **Finish**.

   System Manager creates and populates the newly created system group with the systems selected.

22.4.4 Modifying a Group

Through 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.
System Manager opens the shortcut menu.

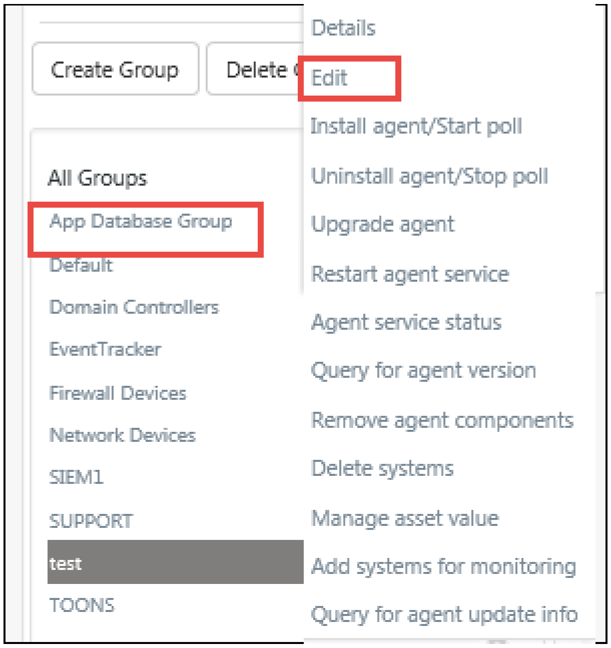
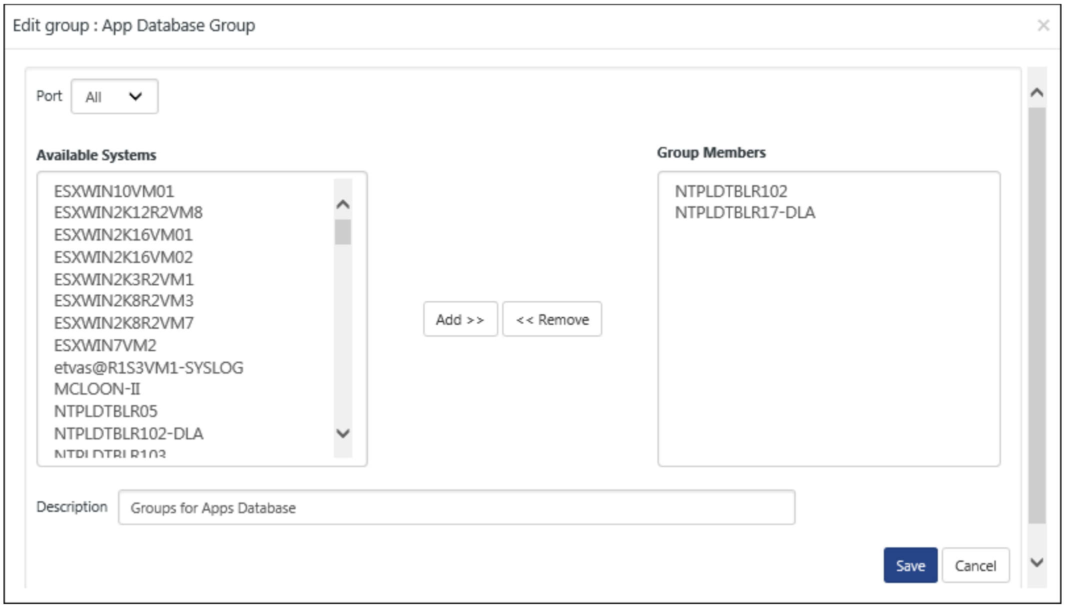


Figure 536

2 From the shortcut menu, choose **Edit**.
System Manager opens the details of the group with the available systems list.



Edit group : App Database Group

Port All

Available Systems

ESXWIN10VM01
ESXWIN2K12R2VM8
ESXWIN2K16VM01
ESXWIN2K16VM02
ESXWIN2K3R2VM1
ESXWIN2K8R2VM3
ESXWIN2K8R2VM7
ESXWIN7VM2
etvas@R1S3VM1-SYSLOG
MCLOON-II
NTPLDTBLR05
NTPLDTBLR102-DLA
NTPLDTBLR103

Group Members

NTPLDTBLR102
NTPLDTBLR17-DLA

Description Groups for Apps Database

Figure 537

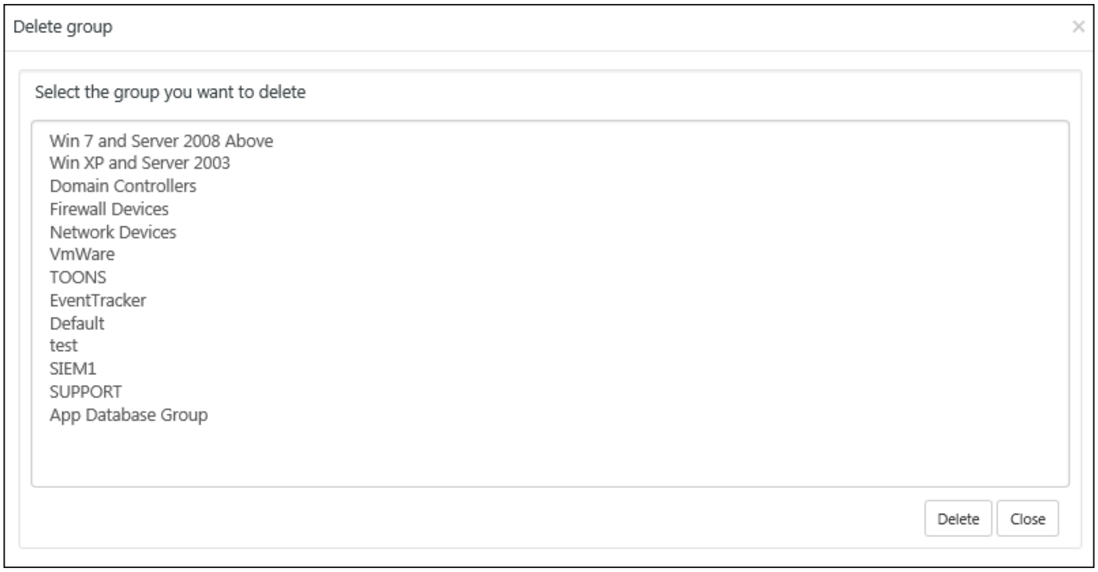
3 Select the available systems, select **Add>>** or **<<Remove**, and then click **Save**.

22.4.5 Deleting a Group

This option enables you to delete an existing Group.

1. Click **Delete Group**.
   System Manager opens the confirmation message box.

1 Click **OK**.
   System Manager opens the list of system groups.



Delete group

Select the group you want to delete

Win 7 and Server 2008 Above
Win XP and Server 2003
Domain Controllers
Firewall Devices
Network Devices
VmWare
TOONS
EventTracker
Default
test
SIEM1
SUPPORT
App Database Group

Figure 538

2 Select a group and then click **Delete**.

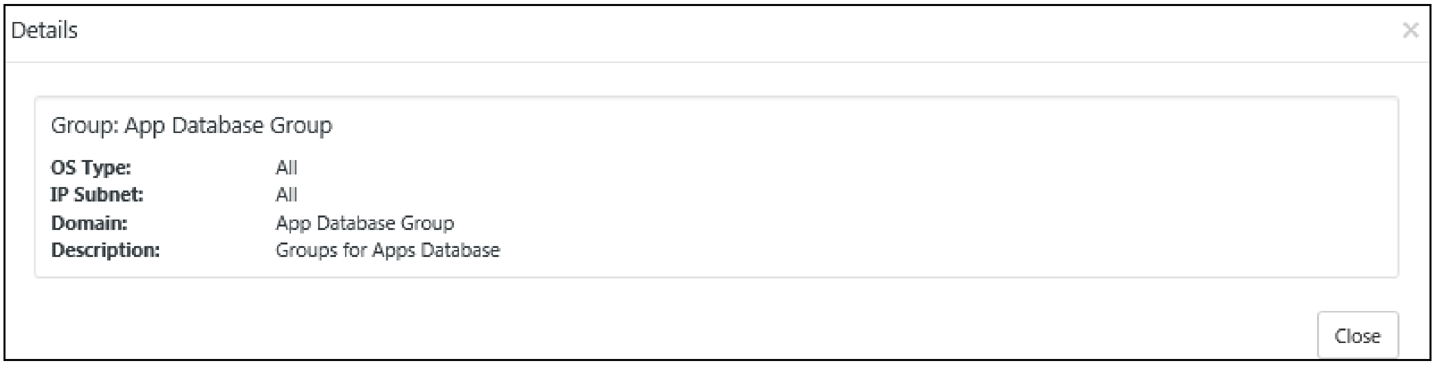
22.5 Viewing System Details

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** menu, select **Systems**.
2. To view **system group details**, in **Groups** pane, right-click a system group.
   System Manager opens the shortcut menu.
   From the shortcut menu, choose **Details**.
   System Manager opens 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 opens the shortcut menu.
   From the shortcut menu, choose Details.

System Manager opens the system Details window.



Details

Group: App Database Group

OS Type: All
IP Subnet: All
Domain: App Database Group
Description: Groups for Apps Database

Figure 539

22.6 Restarting 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, click the ⚙ icon corresponding to the managed system.

System Manager opens the shortcut menu.

4 From the shortcut menu, choose **Restart agent service**.

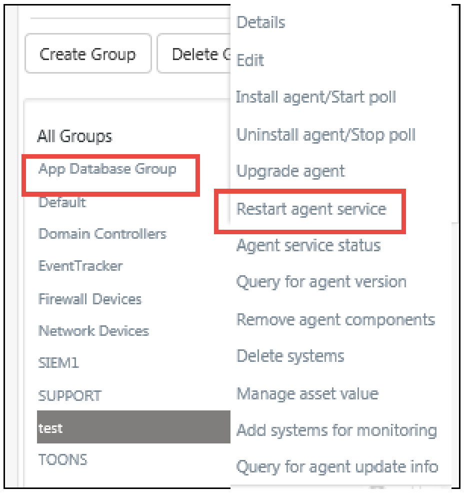
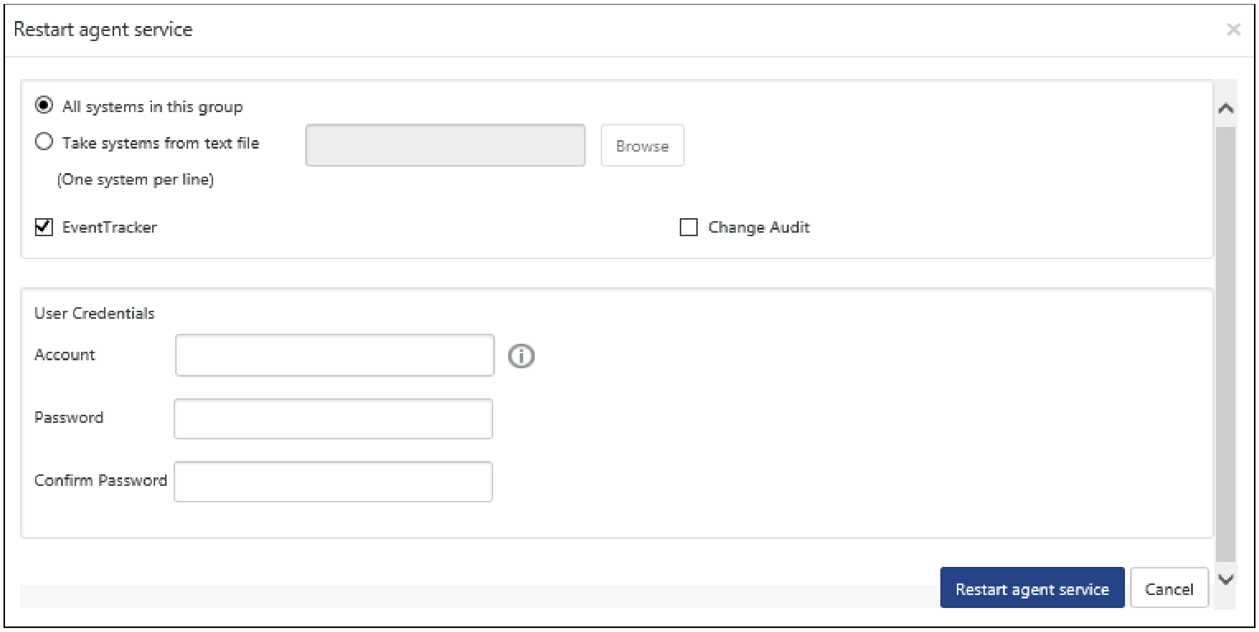


Figure 540

System Manager opens the Restart agent service window.



Restart agent service

● All systems in this group

○ Take systems from text file

(One system per line)

☑ EventTracker

□ Change Audit

User Credentials

Account:

Password:

Confirm Password:

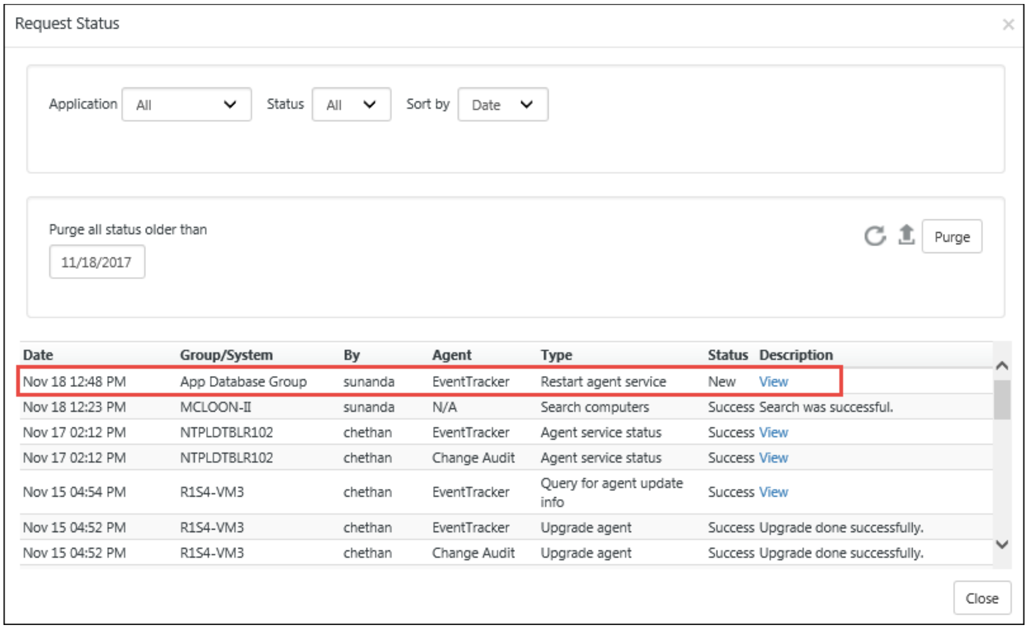
Figure 541

5 Enter valid user credentials and then click **Restart agent service**.

System Manager opens the status of the action.

6 To view the status, click the **Request Status** button.

System Manager opens the Request Status window.



Request Status

Application: All

Status: All

Sort by: Date

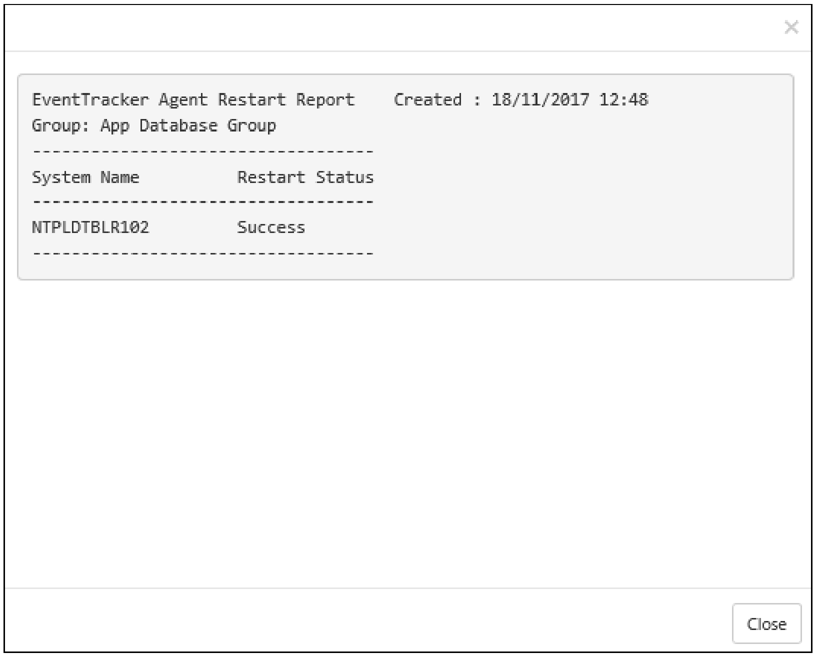
Purge all status older than: 11/18/2017

Date	Group/System	By	Agent	Type	Status	Description
Nov 18 12:48 PM	App Database Group	sunanda	EventTracker	Restart agent service	New	View
Nov 18 12:23 PM	MCLOON-II	sunanda	N/A	Search computers	Success	Search was successful.
Nov 17 02:12 PM	NTPLDTBLR102	chethan	EventTracker	Agent service status	Success	View
Nov 17 02:12 PM	NTPLDTBLR102	chethan	Change Audit	Agent service status	Success	View
Nov 15 04:54 PM	R1S4-VM3	chethan	EventTracker	Query for agent update info	Success	View
Nov 15 04:52 PM	R1S4-VM3	chethan	EventTracker	Upgrade agent	Success	Upgrade done successfully.
Nov 15 04:52 PM	R1S4-VM3	chethan	Change Audit	Upgrade agent	Success	Upgrade done successfully.

Figure 542

7 Click the **View** link in the Description column.

System Manager opens the status of the remote agent.



```
EventTracker Agent Restart Report    Created : 18/11/2017 12:48
Group: App Database Group
----------------------------------
System Name          Restart Status
----------------------------------
NTPLDTBLR102         Success
----------------------------------
```

Figure 543

22.7 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 opens the Agent service status window.

4 Enter valid user credentials and then click **Agent service status**.

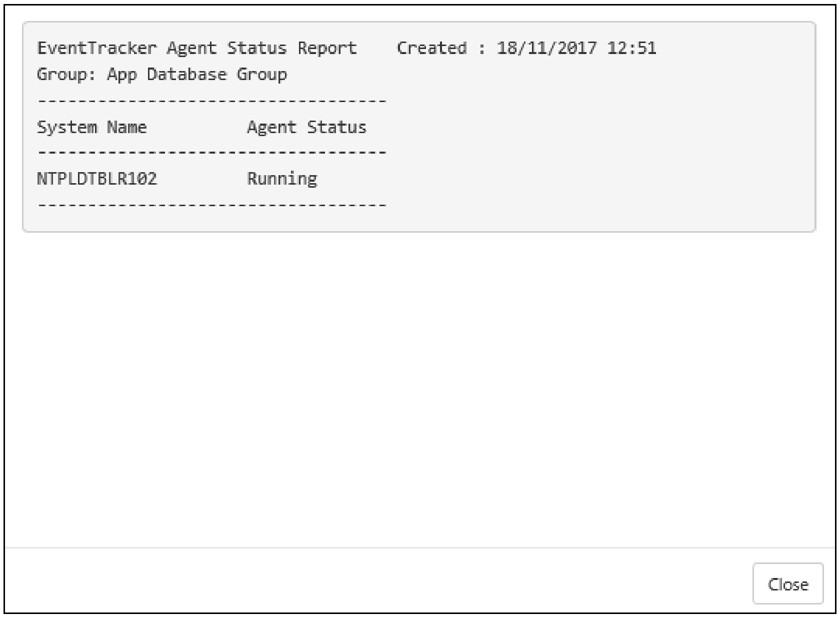
System Manager opens the status of the action.

5 To view the status, click **Request Status**.

System Manager opens the System Status window.

6 Click the **View** link in the Description column.

System Manager opens the status of the remote agent.



```
EventTracker Agent Status Report    Created : 18/11/2017 12:51
Group: App Database Group
----------------------------------
System Name          Agent Status
----------------------------------
NTPLDTBLR102         Running
----------------------------------
```

Figure 544

22.8 Query Agent Version option

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 opens the Query for Agent version window.

4. Type valid user credentials and then click **Query for Agent version**.

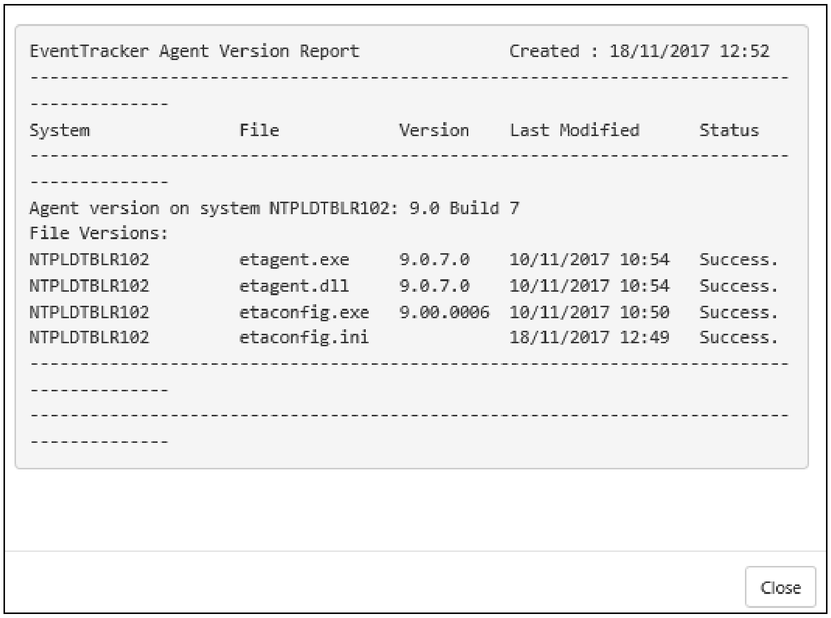
   System Manager opens the status of the action.

5. As advised on the pop-up window, click the **Request Status** button.

   System Manager opens the System Status window.

6. Click the **View** link in the Description column.

   System Manager opens the version of the remote agent.



```
EventTracker Agent Version Report                 Created : 18/11/2017 12:52
-----------------------------------------------------------------------------
-------------
System               File            Version     Last Modified      Status
-----------------------------------------------------------------------------
-------------
Agent version on system NTPLDTBLR102: 9.0 Build 7
File Versions:
NTPLDTBLR102         etagent.exe     9.0.7.0     10/11/2017 10:54   Success.
NTPLDTBLR102         etagent.dll     9.0.7.0     10/11/2017 10:54   Success.
NTPLDTBLR102         etaconfig.exe   9.00.0006   10/11/2017 10:50   Success.
NTPLDTBLR102         etaconfig.ini               18/11/2017 12:49   Success.
-----------------------------------------------------------------------------
-------------
-----------------------------------------------------------------------------
-------------
```

Figure 545

22.9 Query for Agent Update Info

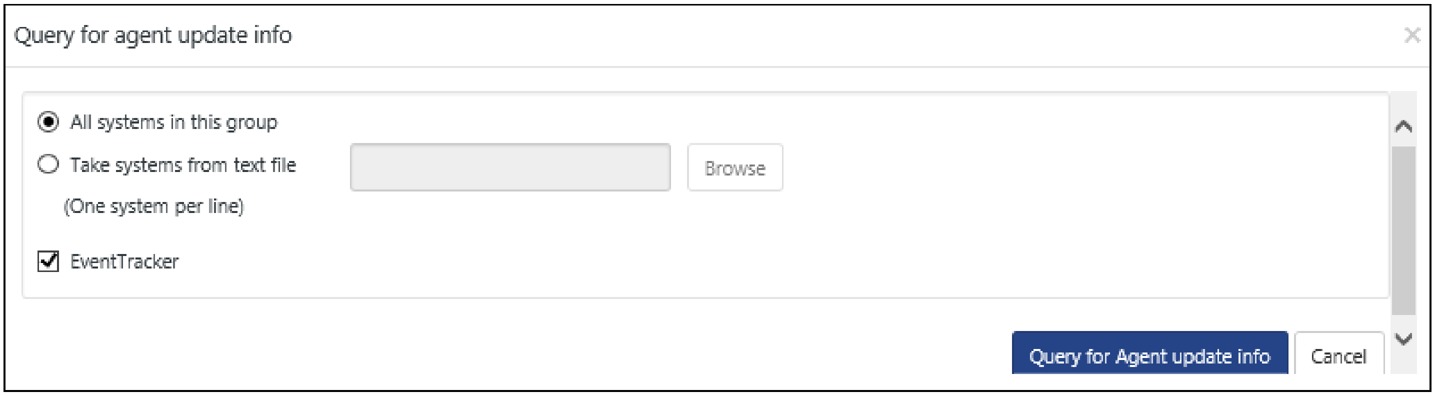
This option helps you query EventTracker Windows Agent update info.

1 To query agent update info, click **Admin** drop-down menu, select **Systems**.

2 To query **Agent Update Info** in a group, right-click a system group. From the shortcut menu, choose **Query for agent Update Info**.

3 To query **Agent Update Info** in a managed system, move the mouse pointer over a managed system. From the shortcut menu, choose **Query for agent update info**.

System Manager opens the Query for Agent Update Info window.



Query for agent update info

● All systems in this group

○ Take systems from text file

(One system per line)

☑ EventTracker

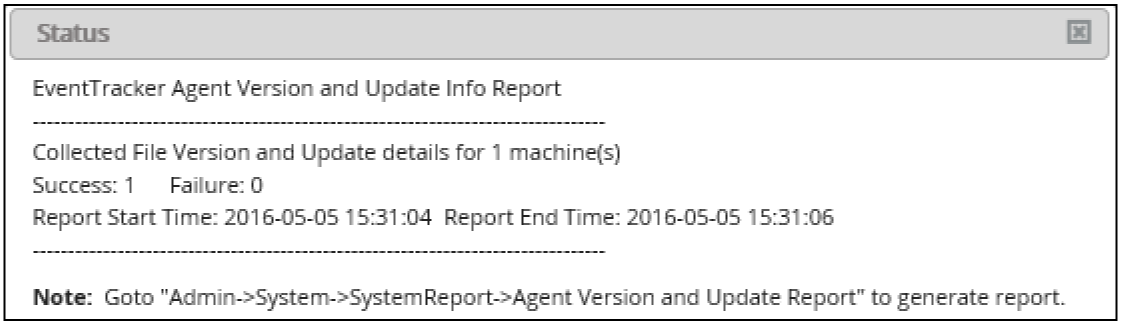
Figure 546

4 Click **Query for Agent Update Info**.

5 As advised on the pop-up window, click **Request Status**.

System Manager opens the System Status window.

6 Click the **View** link in the Description column.
Check the report in **Admin->System->System Report->Agent Version and Update Report**" to generate report.



Status

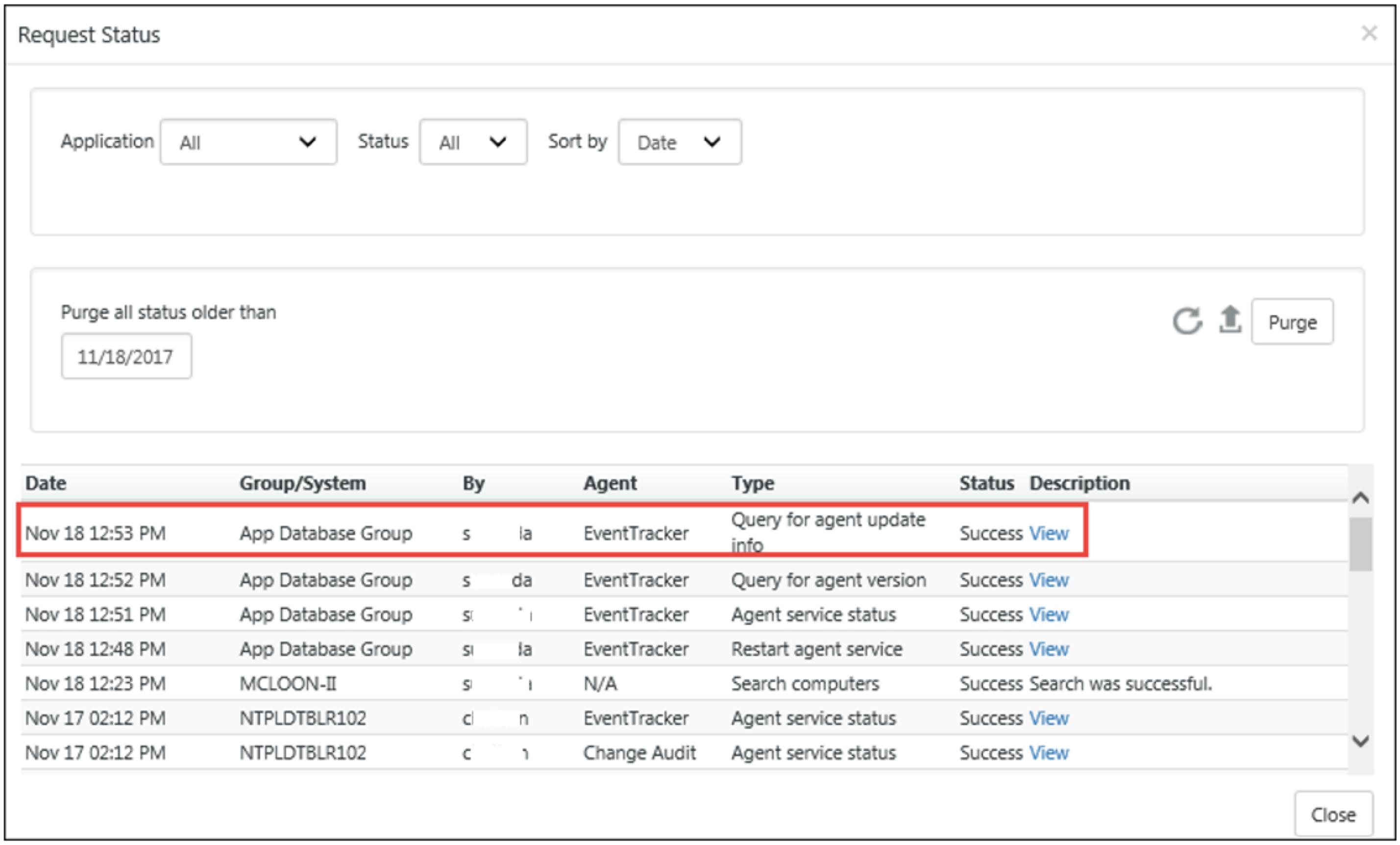
EventTracker Agent Version and Update Info Report

Collected File Version and Update details for 1 machine(s)
Success: 1 Failure: 0
Report Start Time: 2016-05-05 15:31:04 Report End Time: 2016-05-05 15:31:06

Note: Goto "Admin->System->SystemReport->Agent Version and Update Report" to generate report.

Figure 547

NOTE: Incase an older version agent is reporting, the Request Status will display as “success”.



Request Status

Application: All | Status: All | Sort by: Date

Purge all status older than: 11/18/2017

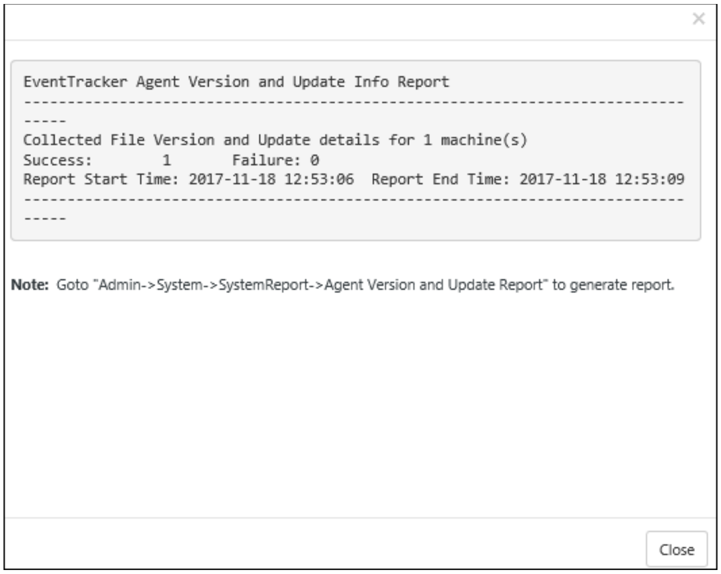
Purge

Date	Group/System	By	Agent	Type	Status	Description
Nov 18 12:53 PM	App Database Group	[redacted]	EventTracker	Query for agent update info	Success	View
Nov 18 12:52 PM	App Database Group	[redacted]	EventTracker	Query for agent version	Success	View
Nov 18 12:51 PM	App Database Group	[redacted]	EventTracker	Agent service status	Success	View
Nov 18 12:48 PM	App Database Group	[redacted]	EventTracker	Restart agent service	Success	View
Nov 18 12:23 PM	MCLOON-II	[redacted]	N/A	Search computers	Success	Search was successful.
Nov 17 02:12 PM	NTPLDTBLR102	[redacted]	EventTracker	Agent service status	Success	View
Nov 17 02:12 PM	NTPLDTBLR102	[redacted]	Change Audit	Agent service status	Success	View

Close

Figure 548

To generate the report, go to **Admin->System->System Report->Agent Version and Update Report**.



```
EventTracker Agent Version and Update Info Report
-----------------------------------------------------------------------------
-----
Collected File Version and Update details for 1 machine(s)
Success:        1       Failure: 0
Report Start Time: 2017-11-18 12:53:06  Report End Time: 2017-11-18 12:53:09
-----------------------------------------------------------------------------
-----
```

Note: Goto "Admin->System->SystemReport->Agent Version and Update Report" to generate report.

Figure 549

- In System type, select the appropriate system to generate report.

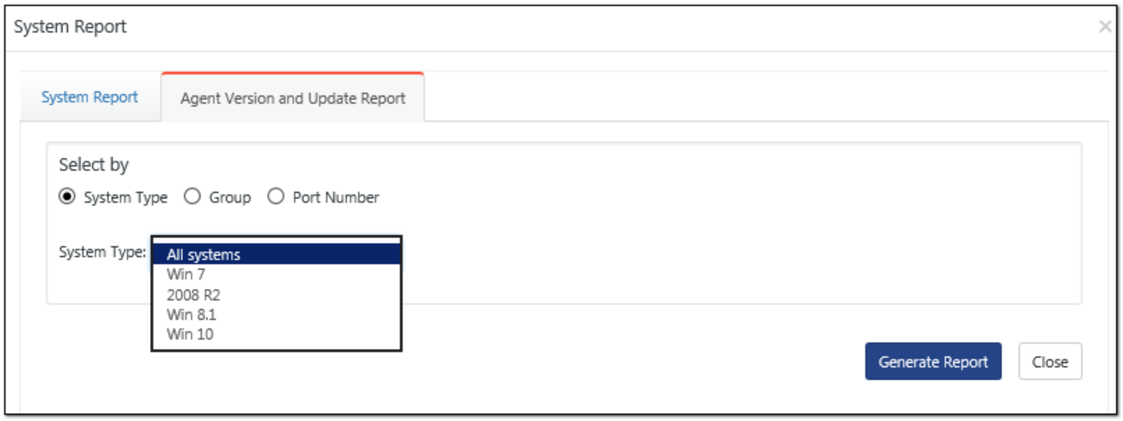
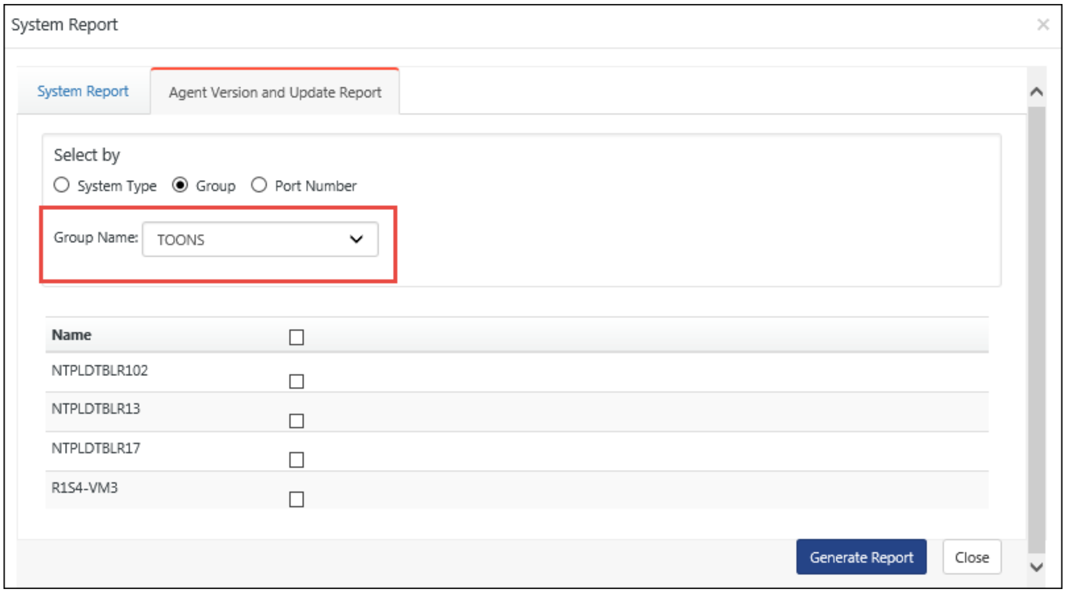


Figure 550

- In group, select the appropriate group along with the systems.



System Report

System Report | Agent Version and Update Report

Select by

○ System Type ● Group ○ Port Number

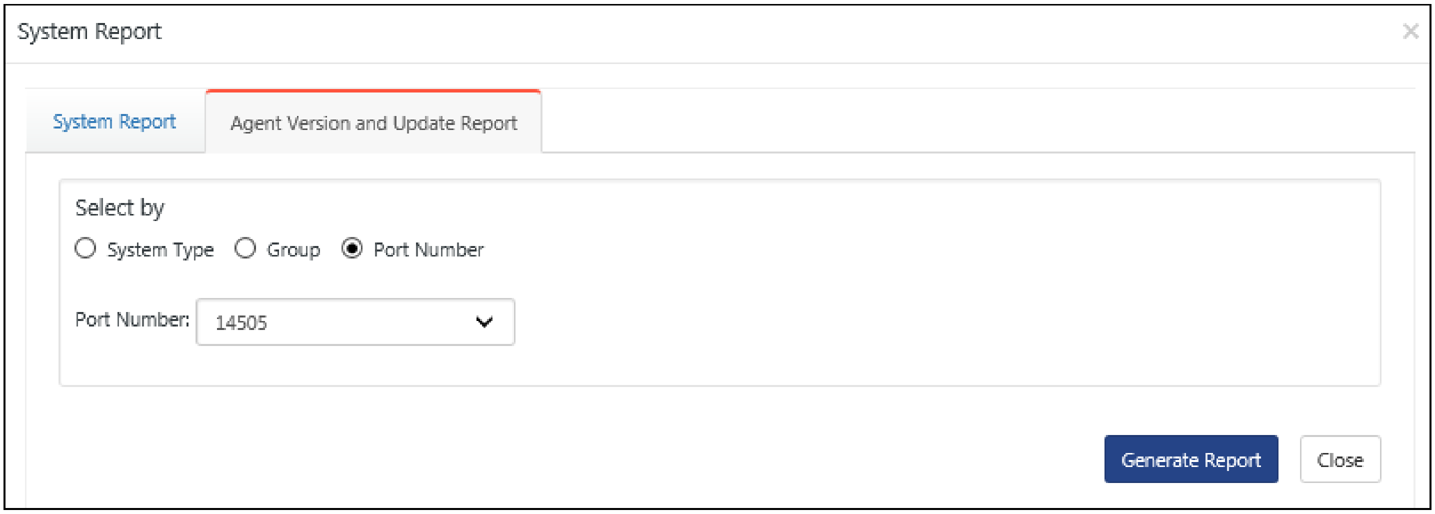
Group Name: TOONS

Name	□
NTPLDTBLR102	□
NTPLDTBLR13	□
NTPLDTBLR17	□
R1S4-VM3	□

Figure 551

- Reports can also be generated by selecting Port numbers.

NOTE: Only Windows ports are supported.



System Report

System Report | Agent Version and Update Report

Select by

○ System Type ○ Group ● Port Number

Port Number: 14505

Figure 552

22.10 Managing 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 opens the shortcut menu.

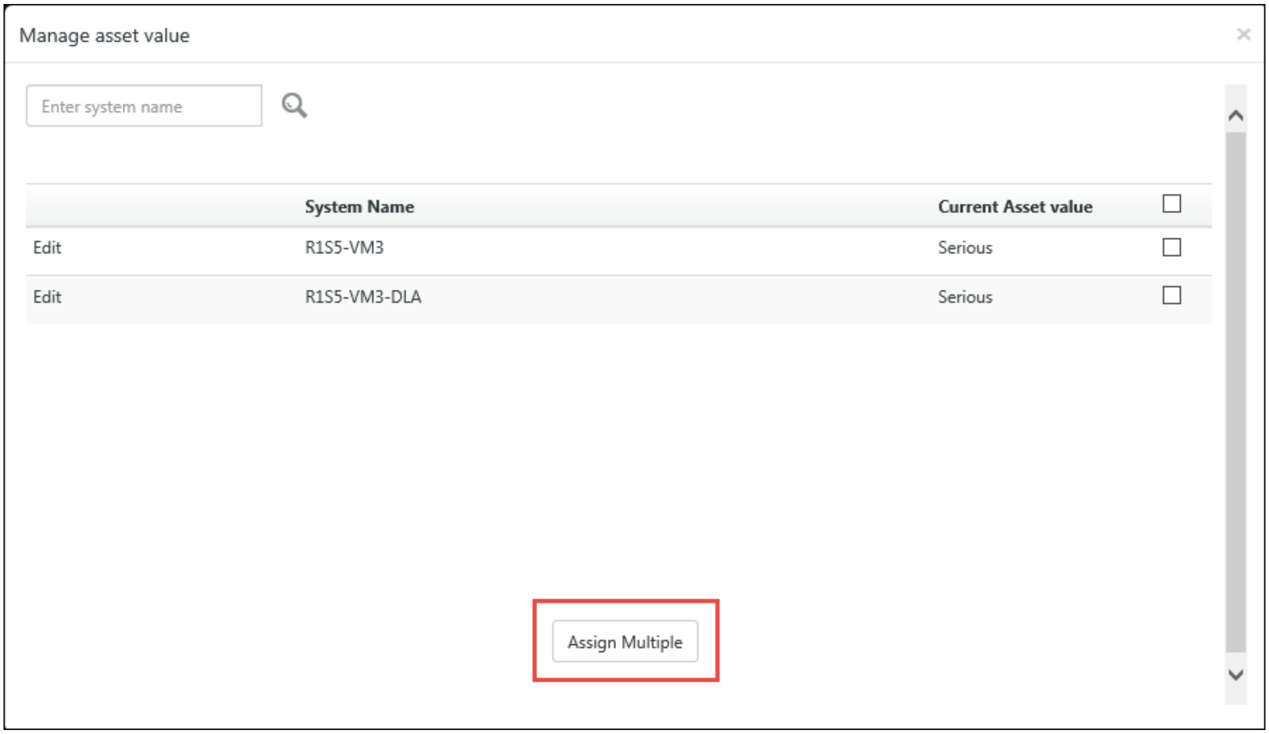
2 From the shortcut menu, choose **Manage Asset value**.
System Manager opens the Manage Asset Value pop-up window.

3 Select the value from the **Asset value** drop-down list, and then click **Save**.

22.10.1 Setting 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.

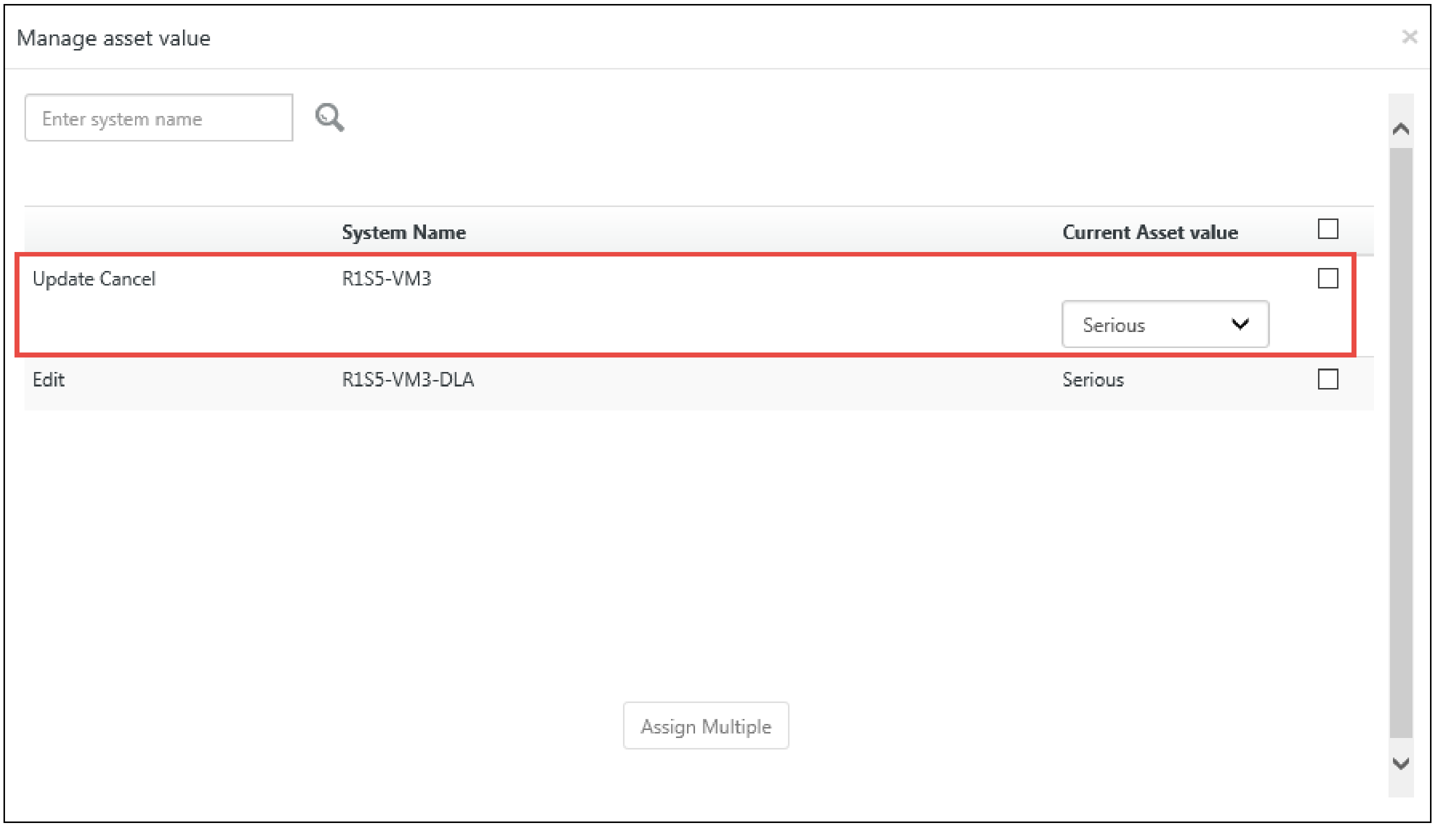
2 From the shortcut menu, choose **Manage Asset Value**.
System Manager opens the Manage Asset Value pop-up window.



	System Name	Current Asset value	□
Edit	R1S5-VM3	Serious	□
Edit	R1S5-VM3-DLA	Serious	□

Figure 553

3 Select **Edit** to change the current asset value of the system.



Manage asset value

	System Name	Current Asset value	□
Update Cancel	R1S5-VM3	Serious	□
Edit	R1S5-VM3-DLA	Serious	□

Figure 554

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 systems, and then click **Assign multiple**.

EventTracker opens Assign Asset Value pop-up window.

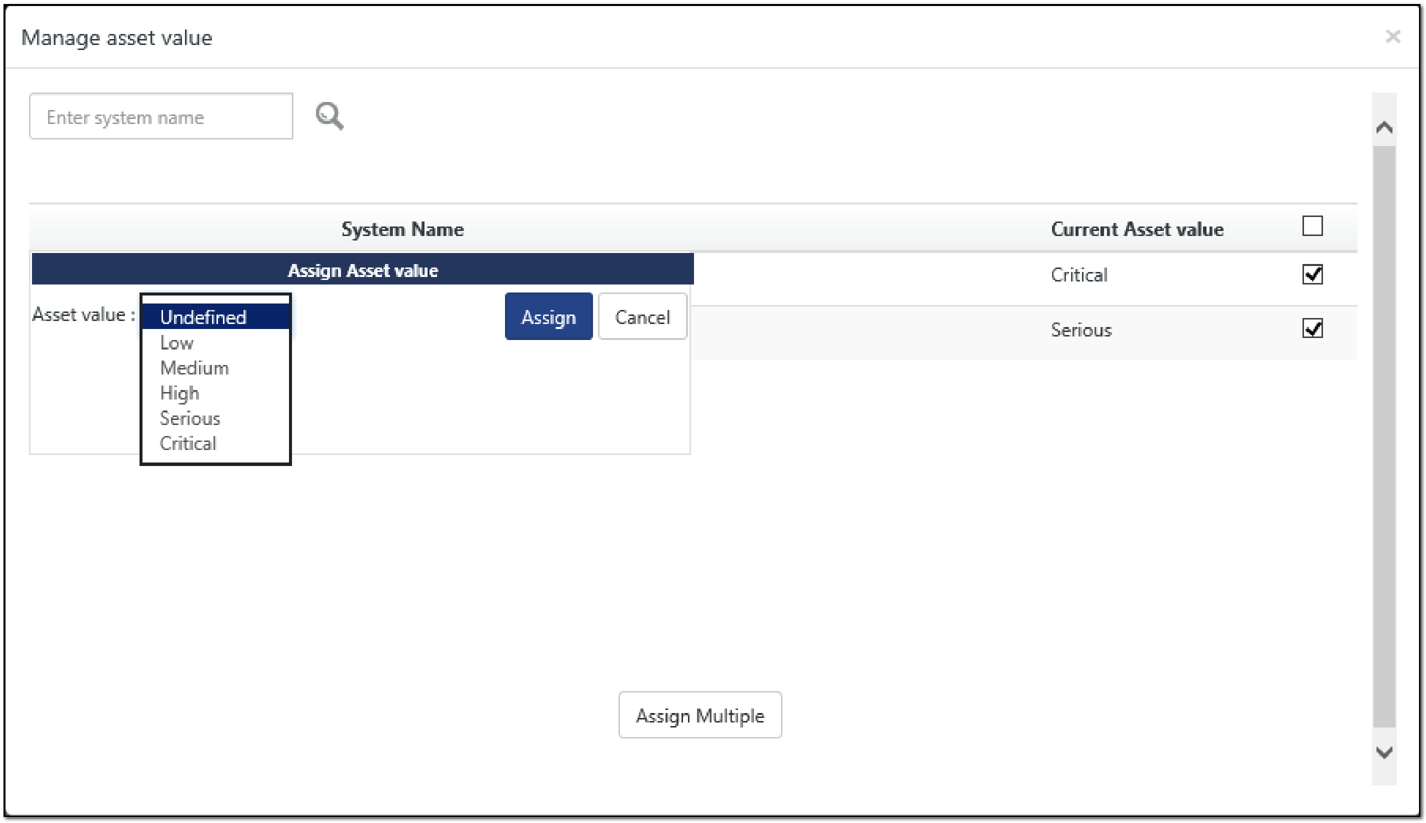


Figure 555

6 Select the value from the **Asset value** drop-down list, and then click **Assign**.

22.11 Deleting Systems

This option helps to remove unmanaged systems.

1 Right-click the system group from where you want to remove the systems.

System Manager opens the shortcut menu.

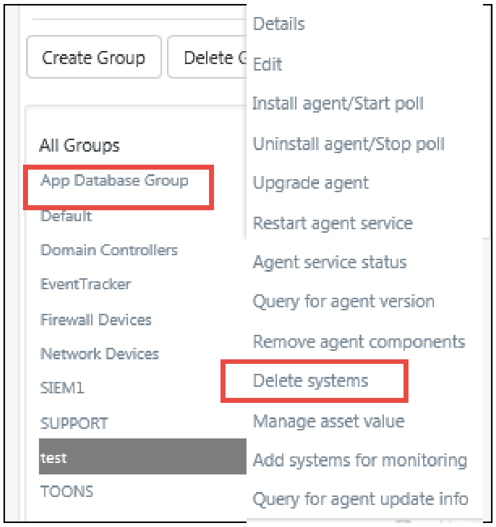


Figure 556

2 From the shortcut menu, click **Delete systems**.

System Manager opens the Delete systems window.

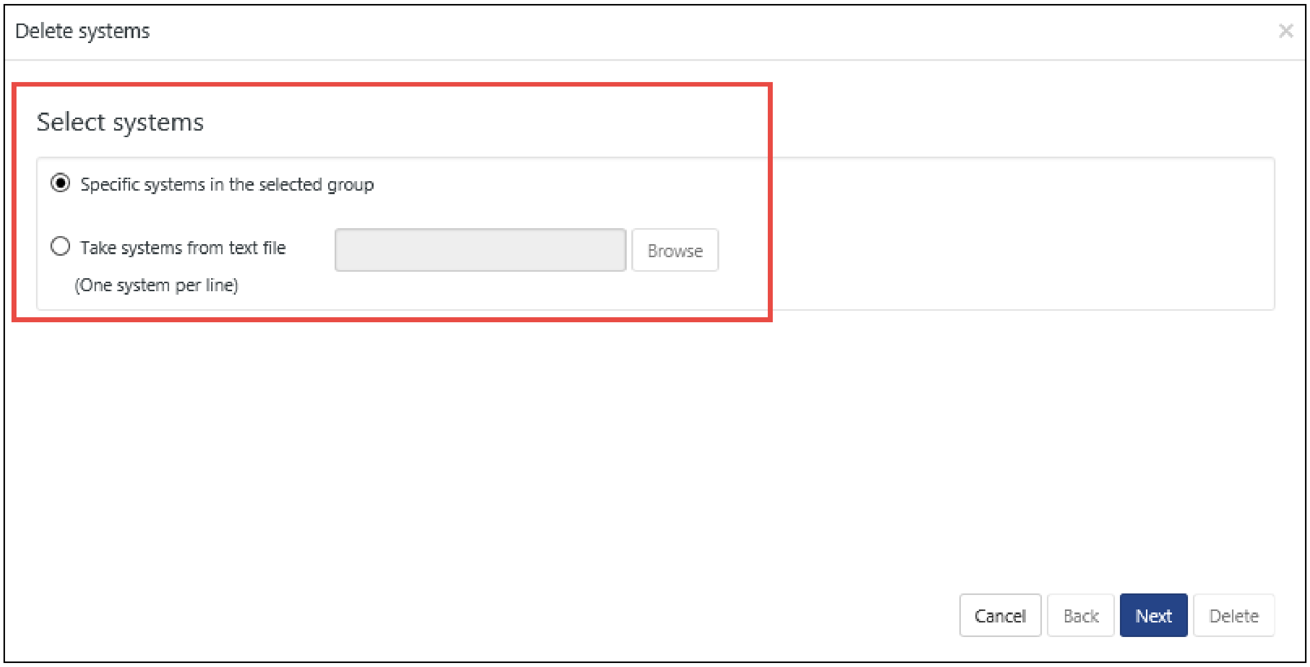


Figure 557

3 Select the required option and then click **Next>>.**

4 Select the system, and then click **Delete**.

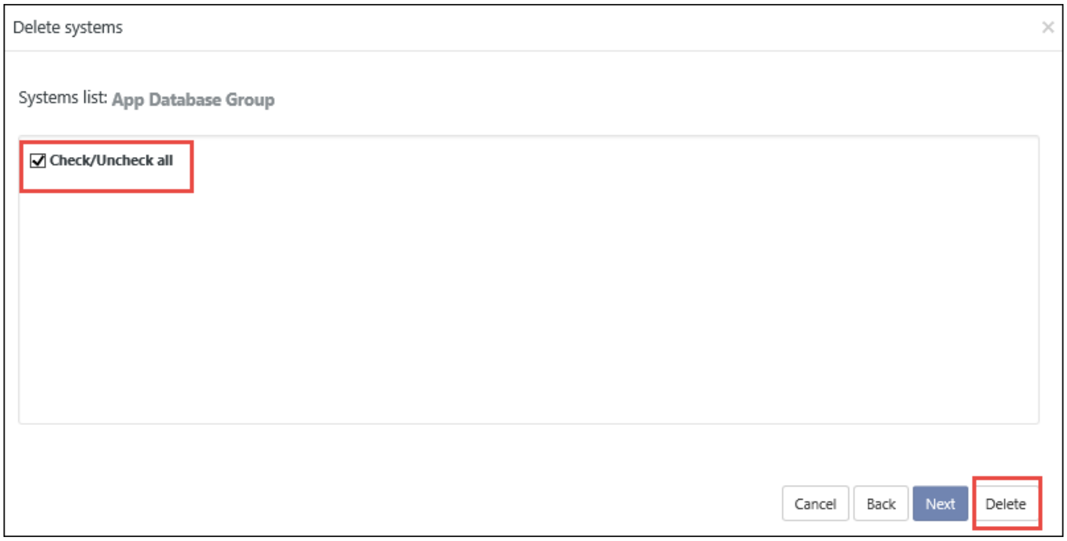


Figure 558

Click the **Check/Uncheck all** checkbox to select all the systems, and then click **Delete** button.

System Manager opens the confirmation message box.

5 Click **OK** to confirm

System Manager removes the system.

22.12 Search Systems option

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 **Go**.

EventTracker opens the search result.

2 Click **Show All** to view all systems.

22.13 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.

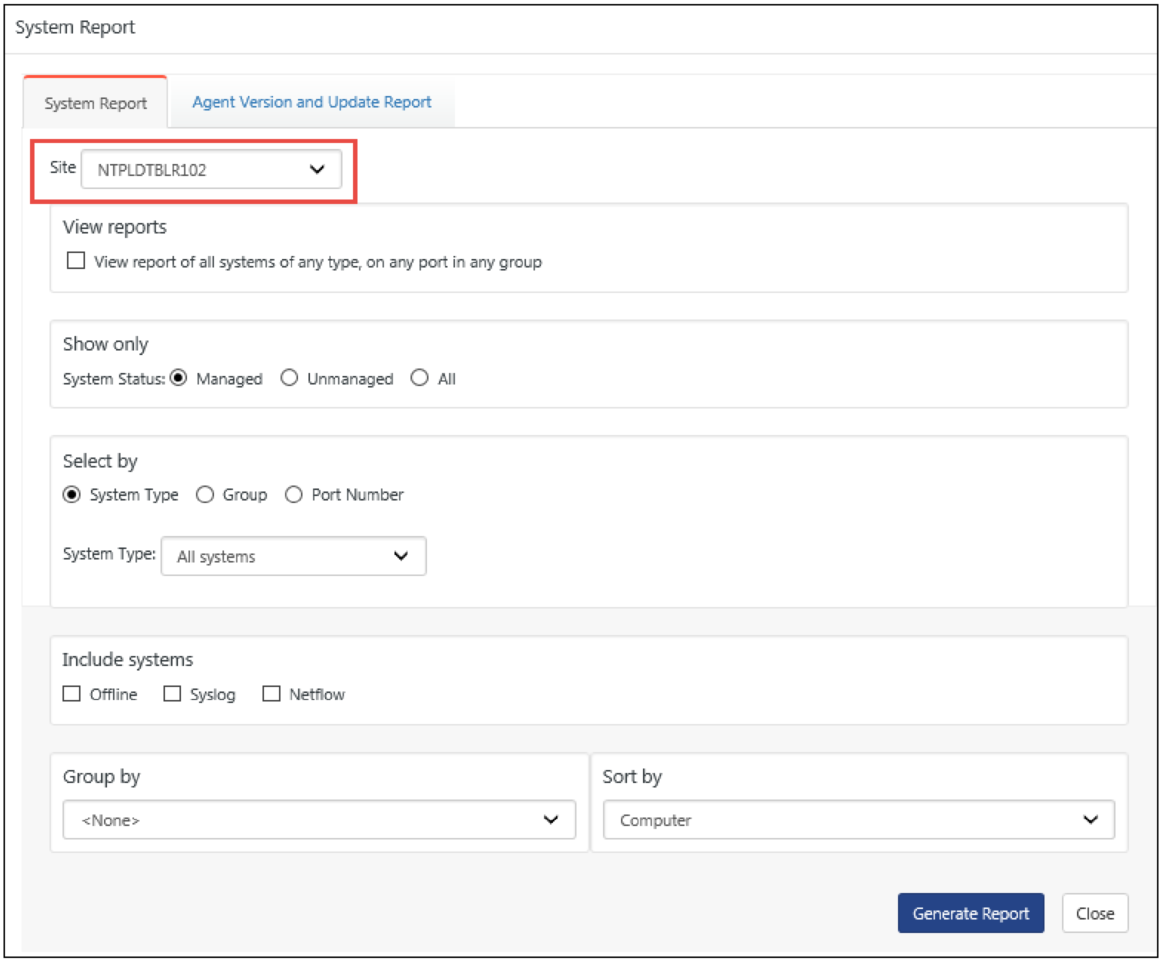
- If you select **Name**, EventTracker opens the system names in alphabetical order.
- If you select **Asset value**, EventTracker opens the system names by priority starting from High.
- If you select **Port**, EventTracker opens the system names with the port number (in descending order) on the top of the list.
- If you select **Status**, EventTracker opens the system names by priority starting from Low.

22.14 Systems Report

This option allows you to generate report of the Collection Point systems which are reporting to the Collection Master. User needs to select the CP site from the site drop down to generate the system report.

1. In Systems Manager, click the **Systems Report** button to generate a report of the systems.

   System Report page opens.



System Report

System Report | Agent Version and Update Report

Site: NTPLDTBLR102

View reports
☐ View report of all systems of any type, on any port in any group

Show only
System Status: ● Managed ○ Unmanaged ○ All

Select by
● System Type ○ Group ○ Port Number

System Type: All systems

Include systems
☐ Offline ☐ Syslog ☐ Netflow

Group by: <None>

Sort by: Computer

Figure 559

2. Select the required options, and then select **Generate Report**.

22.15 Configuring Agent-less collection via System Manager (limited features)

In cases where it is not possible or desirable to install the EventTracker Windows Agent, EventTracker can be configured to subscribe/poll the event log of remote computers over the network to collect new event log entries.

Pros

No agent to deploy – Simpler product deployment. There is lesser effort during planning, deployment and upgrade.

Cons

- Increased network load – Depending on the selected polling cycle or level of event generation, network load is greater.
- Greater dependency, more critical points of failure – The Console becomes critical since it is polling target machines. Network choke points can impact performance.
- Limited to operation within a domain – The Console and target machine must be in the same domain so that domain privileges are preserved.
- Performance monitoring – This feature is not available.
- Application monitoring – This feature is not available.
- Software install/removal monitoring – This feature is not available.
- Service monitoring – This feature is not available.
- Monitoring external log files – This feature is not available.
- Host based intrusion detection – This feature is not available.
- Non-domain topologies not supported – This feature is only available when the Console and target machine are in the same Windows domain.

22.15.1 Adding Systems for Agent-less monitoring

This option enables you to add systems from where you want to collect events periodically. The resource (CPU/memory/disk) usage, log file monitoring, and other agent required features are disabled, in the agent-less monitoring systems. Additionally, the service account of the local agent should have administrative privileges on all the systems that are added for collecting events.

NOTE: Make sure that the Remote Event Log Management is added in the filter exception list in Windows Firewall, or else it will not connect to the target system.

22.15.2 Adding systems for Agent-less monitoring

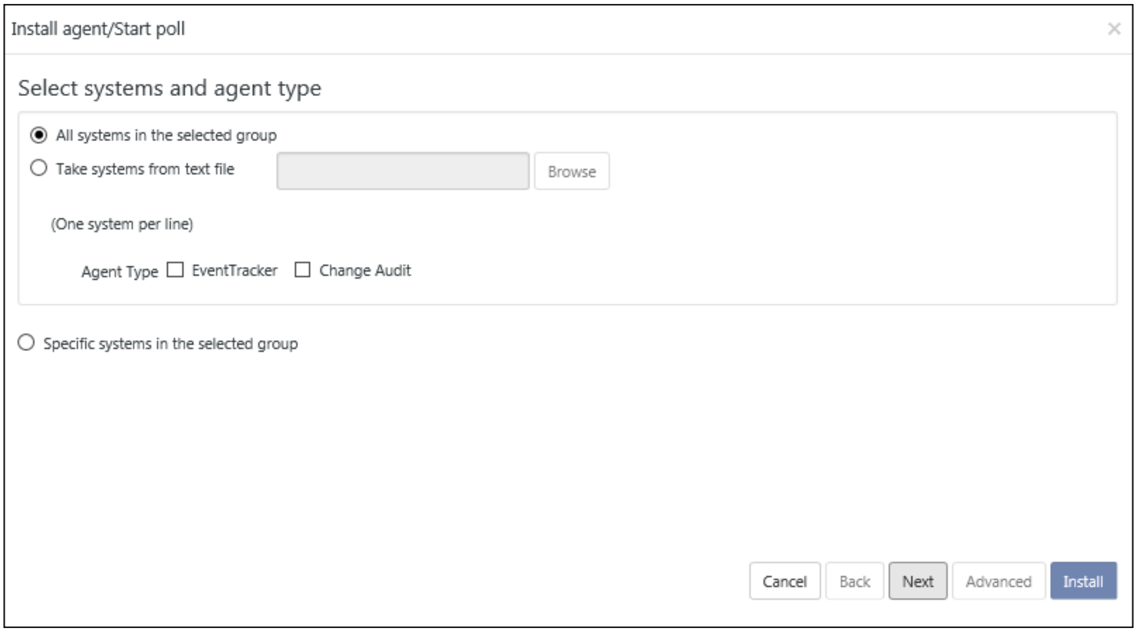
In the **System** manager page, move the mouse pointer over the system where you wish to install the agent.

a) Click the dropdown icon ⚙.

EventTracker opens the drop-down list.

b) Click **Install agent/ Start poll**.

EventTracker opens the **Install Agent/Start poll** dialog box.



Install agent/Start poll

Select systems and agent type

● All systems in the selected group

○ Take systems from text file

(One system per line)

Agent Type □ EventTracker □ Change Audit

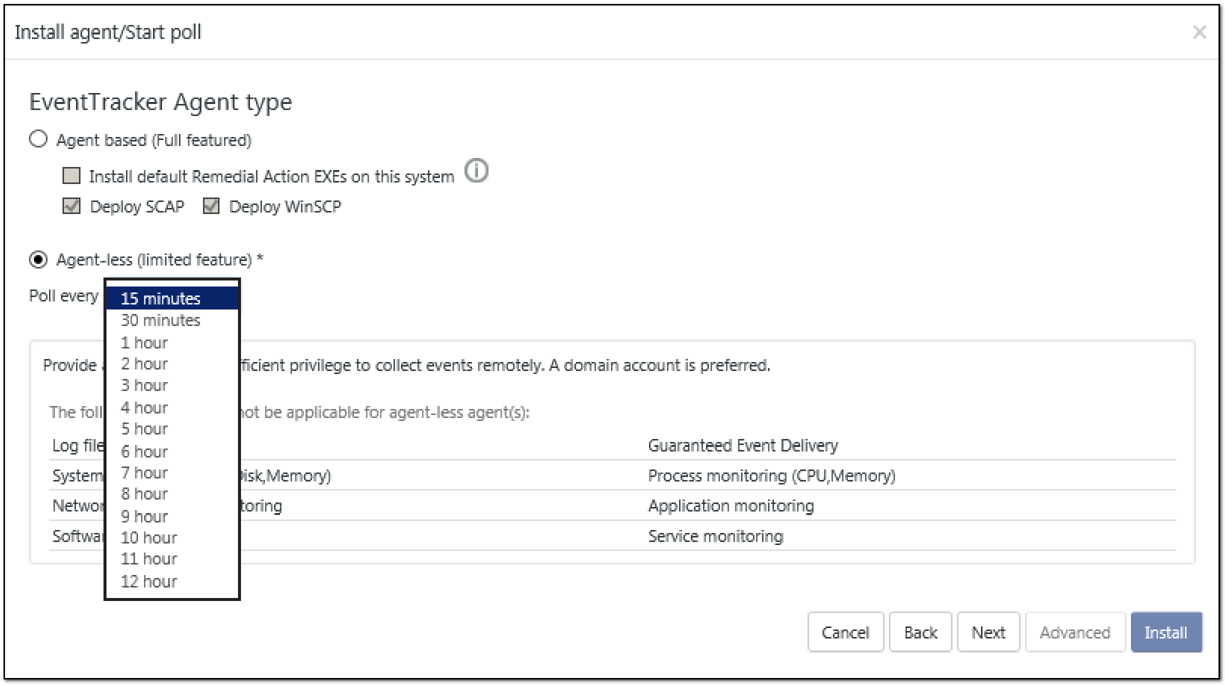
○ Specific systems in the selected group

Figure 560

- Check the **EventTracker** option to install EventTracker agent (Agent-less).
- Check the **Change Audit** option to install Change Audit agent (Only for agent based option)

c) Click **Next**.

d) Select **EventTracker Agent Type i.e. Agent-less (limited feature)*** option.



Install agent/Start poll

EventTracker Agent type

○ Agent based (Full featured)

□ Install default Remedial Action EXEs on this system ⓘ

☑ Deploy SCAP ☑ Deploy WinSCP

● Agent-less (limited feature) *

Poll every 15 minutes

Provide ficient privilege to collect events remotely. A domain account is preferred.

The foll ot be applicable for agent-less agent(s):

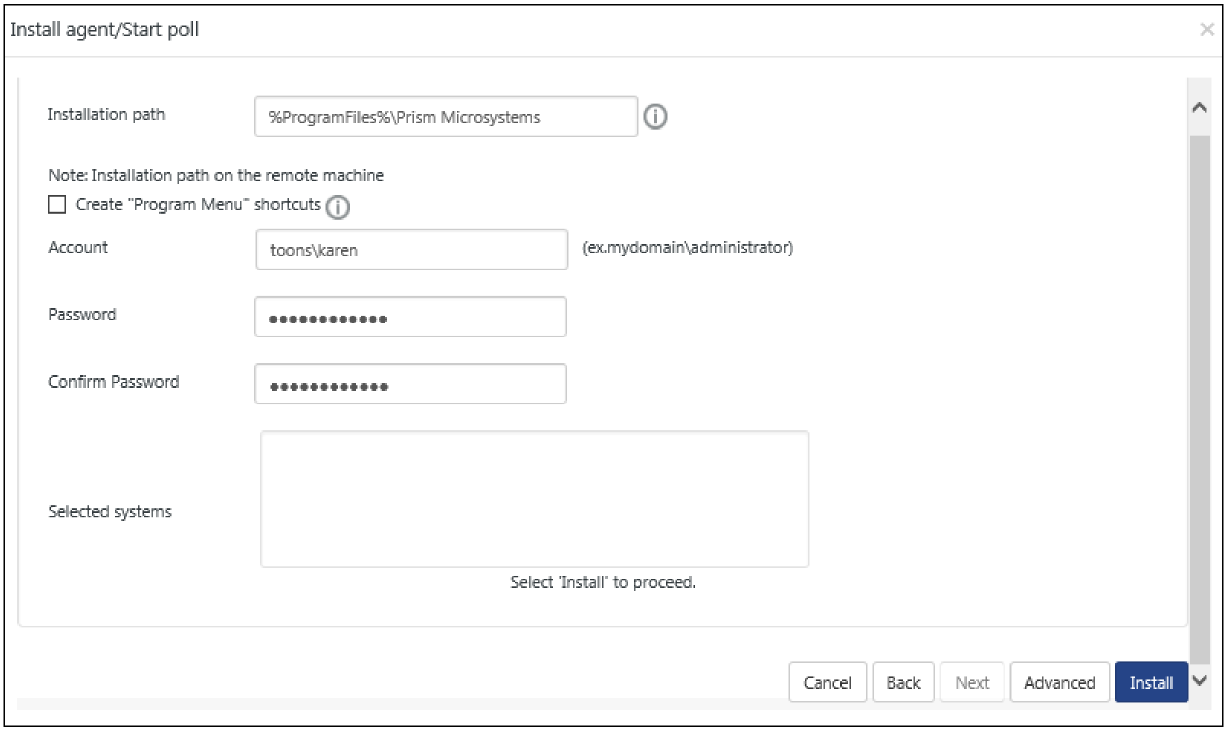
Log file	Guaranteed Event Delivery
System isk,Memory)	Process monitoring (CPU,Memory)
Networ toring	Application monitoring
Softwa	Service monitoring

Figure 561

Agent less (limited feature)	
Select this option to add the system with limited EventTracker Agent features.	In the Agent-less type, the following features are not available: • Log file Monitoring • System Monitoring • Network Connection Monitoring • Software Install / Uninstall • Guaranteed Event Delivery • Process Monitoring • Application Monitoring • Service Monitoring
Poll Every	By default, the frequency is set to 15 min to receive events from the remote agent system. **NOTE**: The poll frequency is applicable for windows 2003 and below and not for Vistas and above.

e) Click **Next**.

EventTracker opens the Install agent/Start poll dialog box with default client installation path on the remote computer.



Install agent/Start poll

Installation path: %ProgramFiles%\Prism Microsystems

Note: Installation path on the remote machine

□ Create "Program Menu" shortcuts

Account: toons\karen (ex.mydomain\administrator)

Password: ●●●●●●●●●●●●●

Confirm Password: ●●●●●●●●●●●●●

Selected systems

Select 'Install' to proceed.

Figure 652

Field	Description
Polling frequency	**Poll Every** Select the time frequency for which you want to get the events.
Domain Admin account	Type valid username and password in Account, Password and Confirm Password fields respectively.
Selected Systems	This field displays the selected system list.

f) Click **Install**.

The agent is installed on the selected machine with the default ‘etaconfig.ini’ configuration.

(OR)

1. To set a more specific configuration, click **Advanced**.

   The **Default** option is selected by default to apply manager side ‘Agent configuration’ settings (etaconfig.ini).

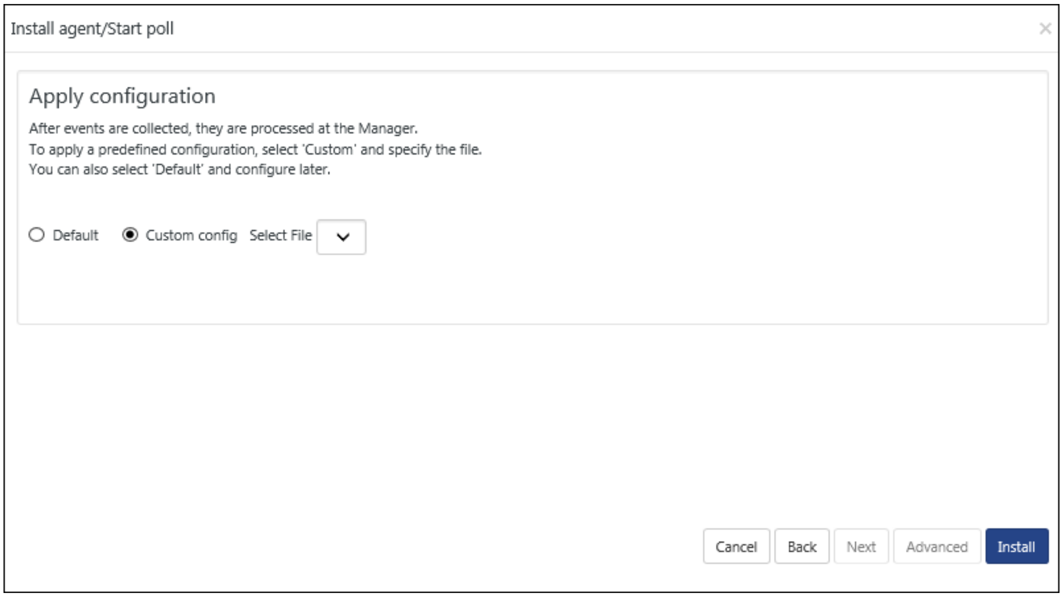
2. Select **Default** or **Custom config** option to select a custom configuration file as per the requirement.

   The custom configuration will provide you the templates which you have created in Agent configuration and two more predefined templates.

You can select the template of your choice.

etaconfig_Servers.ini: This predefined template contains the ideal server configurations which can be applied to the selected agent system.

etaconfig_Workstations.ini: This predefined template contains the ideal workstation configurations which can be applied to the selected agent system. This option disables the 'Offline event sending' option.


Install agent/Start poll

Apply configuration

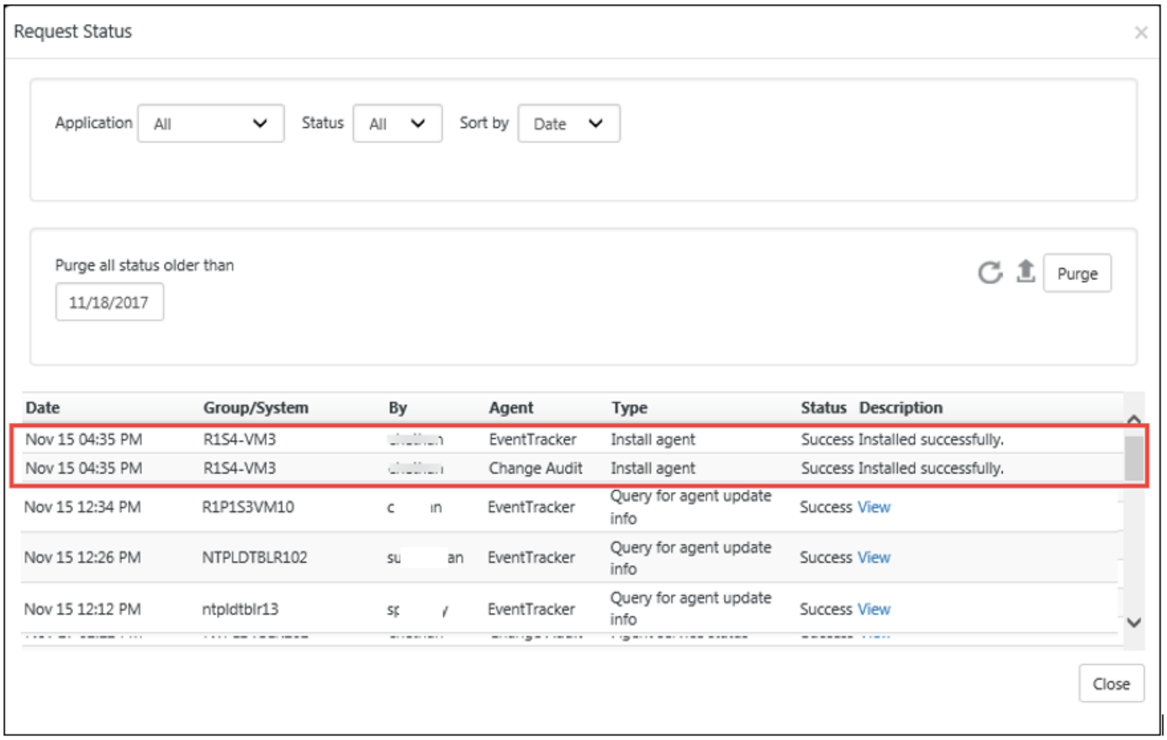
After events are collected, they are processed at the Manager.
To apply a predefined configuration, select 'Custom' and specify the file.
You can also select 'Default' and configure later.

○ Default ● Custom config Select File

Figure 563

g) Select the configuration file from the **File** dropdown, and then click **Install**.
EventTracker opens the pop-up window with appropriate message.

h) Click **OK.**
EventTracker opens Request Status screen.



Request Status

Application: All | Status: All | Sort by: Date

Purge all status older than: 11/18/2017

Date	Group/System	By	Agent	Type	Status	Description
Nov 15 04:35 PM	R1S4-VM3	[redacted]	EventTracker	Install agent	Success	Installed successfully.
Nov 15 04:35 PM	R1S4-VM3	[redacted]	Change Audit	Install agent	Success	Installed successfully.
Nov 15 12:34 PM	R1P1S3VM10	[redacted]	EventTracker	Query for agent update info	Success	View
Nov 15 12:26 PM	NTPLDTBLR102	[redacted]	EventTracker	Query for agent update info	Success	View
Nov 15 12:12 PM	ntpldtblr13	[redacted]	EventTracker	Query for agent update info	Success	View

Figure 564

Select	To
Application	Sort the **Request Status** results by the application installed. Available options are EventTracker & Change Audit.
Status	Sort the **Request Status** results by status of the application installed. Available options are All, New, Success, and Failed.
Sort by	Sort the **Request Status** results by **Date** application was installed /on which **System** it is installed / **Type** of activity performed/ **Status** of the application.
Purge all status older than	Remove the older Request Status details from the list.
Export	Export the 'System Status' into **Excel** format

i) Click **Refresh** ↻ to view the current status.
(OR)
Reopen the **Request Status** dialog box to see the updated status.

j) Click **Close.**

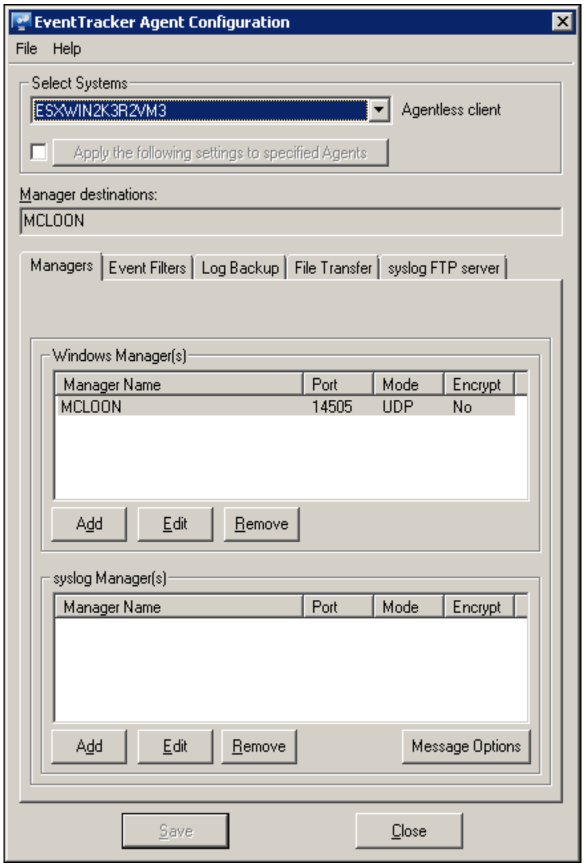
k) Refresh the **System** manager.

Now,

1. Open **EventTracker Control Panel**.

2. Double-Click on **EventTracker Agent Configuration**.

   Only limited feature tabs are available as shown in the figure below:



Select Systems: ESXWIN2K3R2VM3

Manager destinations: MCLOON

Manager Name	Port	Mode	Encrypt
MCLOON	14505	UDP	No

Figure 565

Go to **EventTracker Web,**

1. Click the **Admin** drop-down list at the upper-right corner.
2. Click the **Windows Agent Config**.
3. Click **Search system** to select the system.

NOTE: For **Agent-less (limited feature)*** option, all the above-mentioned feature tabs is displayed but only limited feature will be available.

22.16 Source type mapping to systems

Systems can be mapped to “Source Type” which will improve the Elasticsearch indexer performance.

Elasticsearch indexer performance will improve only when the optimized KO’s are used, and the respective system is mapped to the Source Type

To know the list of optimized KO’s, click here.

1. Log into EventTracker, click Admin and then choose Systems.

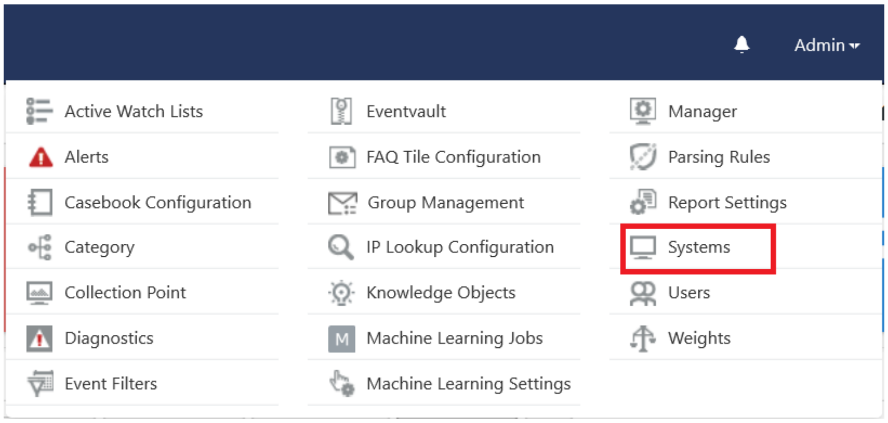
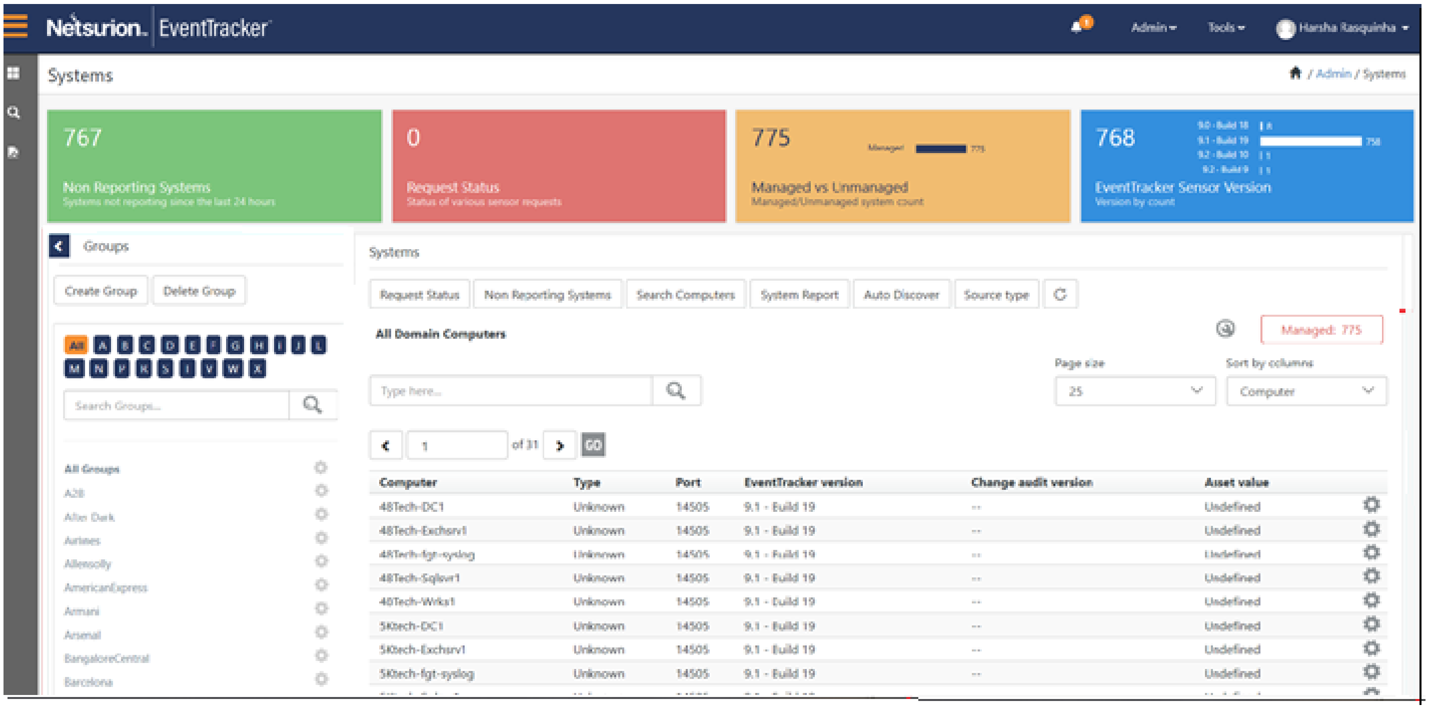


Figure 567

2. The Systems page opens.

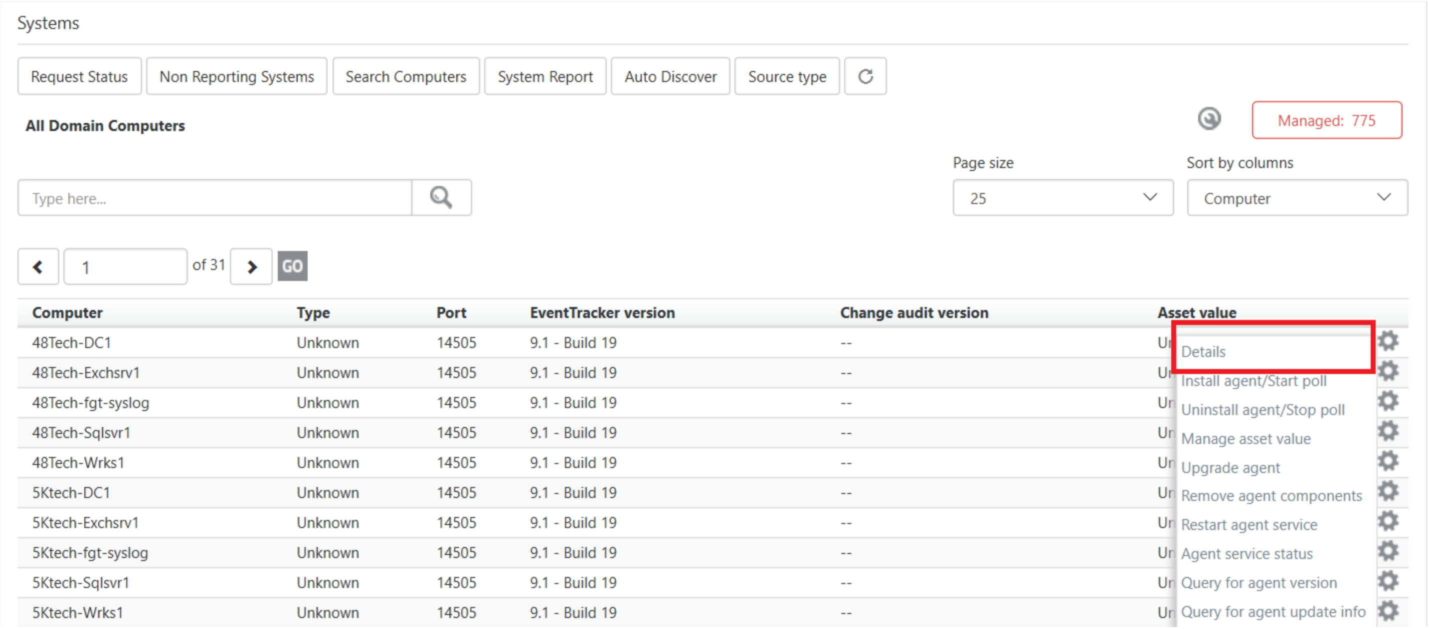


Computer	Type	Port	EventTracker version	Change audit version	Asset value
48Tech-DC1	Unknown	14505	9.1 - Build 19	--	Undefined
48Tech-Exchsrv1	Unknown	14505	9.1 - Build 19	--	Undefined
48Tech-fgt-syslog	Unknown	14505	9.1 - Build 19	--	Undefined
48Tech-Sqlsvr1	Unknown	14505	9.1 - Build 19	--	Undefined
40Tech-Wrks1	Unknown	14505	9.1 - Build 19	--	Undefined
5Ktech-DC1	Unknown	14505	9.1 - Build 19	--	Undefined
5Ktech-Exchsrv1	Unknown	14505	9.1 - Build 19	--	Undefined
5Ktech-fgt-syslog	Unknown	14505	9.1 - Build 19	--	Undefined

Figure 568

22.16.1 Mapping the individual System to the "Source Type"

In the below available list of the systems choose any system and then click the Gear ⚙ icon, choose Details.



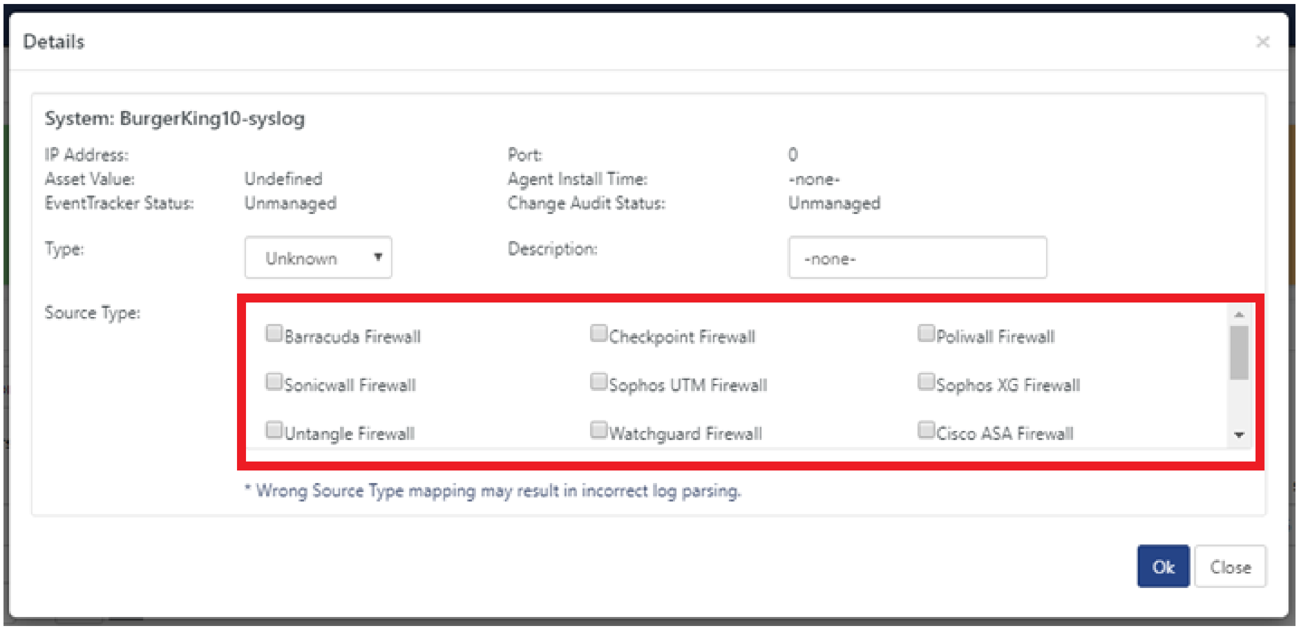
All Domain Computers

Page size: 25 — Sort by columns: Computer — 1 of 31

Computer	Type	Port	EventTracker version	Change audit version	Asset value
48Tech-DC1	Unknown	14505	9.1 - Build 19	--	Ur
48Tech-Exchsrv1	Unknown	14505	9.1 - Build 19	--	Ur
48Tech-fgt-syslog	Unknown	14505	9.1 - Build 19	--	Ur
48Tech-Sqlsvr1	Unknown	14505	9.1 - Build 19	--	Ur
48Tech-Wrks1	Unknown	14505	9.1 - Build 19	--	Ur
5Ktech-DC1	Unknown	14505	9.1 - Build 19	--	Ur
5Ktech-Exchsrv1	Unknown	14505	9.1 - Build 19	--	Ur
5Ktech-fgt-syslog	Unknown	14505	9.1 - Build 19	--	Ur
5Ktech-Sqlsvr1	Unknown	14505	9.1 - Build 19	--	Ur
5Ktech-Wrks1	Unknown	14505	9.1 - Build 19	--	Ur

Figure 569

The Details window opens, select the required source type from the list for the system and then click **OK**.



System: BurgerKing10-syslog

IP Address:		Port:	0
Asset Value:	Undefined	Agent Install Time:	-none-
EventTracker Status:	Unmanaged	Change Audit Status:	Unmanaged
Type:	Unknown	Description:	-none-

Source Type:

□Barracuda Firewall □Checkpoint Firewall □Poliwall Firewall
□Sonicwall Firewall □Sophos UTM Firewall □Sophos XG Firewall
□Untangle Firewall □Watchguard Firewall □Cisco ASA Firewall

* Wrong Source Type mapping may result in incorrect log parsing.

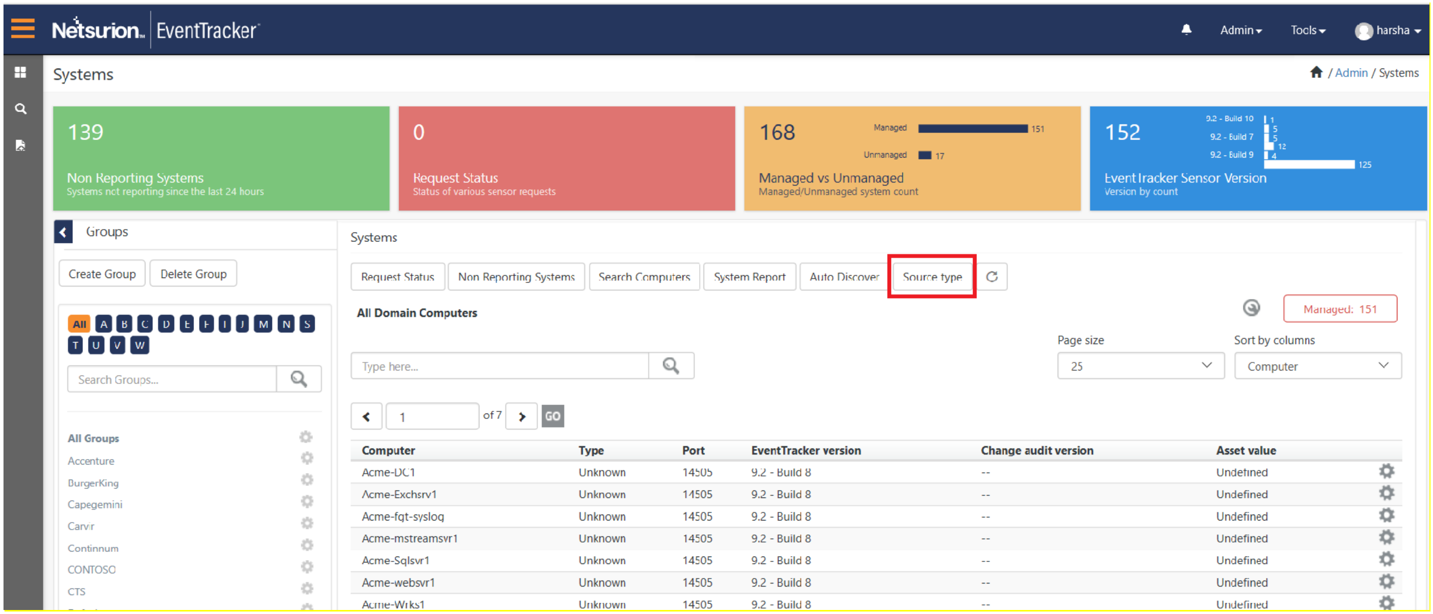
Figure 570

Similarly, to unassign from the System.

Uncheck the required source type from the list for the system and then click **OK**.

22.16.2 Mapping the Group to the “Source Type”

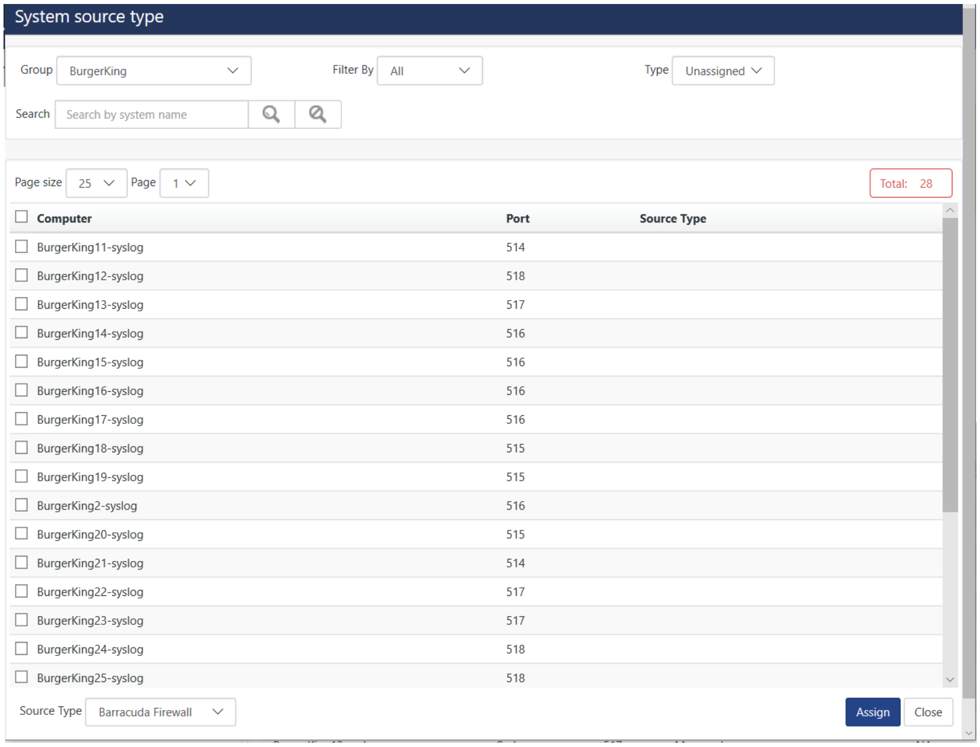
1. Click on the **Source type tab.**



Computer	Type	Port	EventTracker version	Change audit version	Asset value
Acme-DC1	Unknown	14505	9.2 - Build 8	--	Undefined
Acme-Exchsrv1	Unknown	14505	9.2 - Build 8	--	Undefined
Acme-fqt-syslog	Unknown	14505	9.2 - Build 8	--	Undefined
Acme-mstreamsvr1	Unknown	14505	9.2 - Build 8	--	Undefined
Acme-Sqlsvr1	Unknown	14505	9.2 - Build 8	--	Undefined
Acme-websvr1	Unknown	14505	9.2 - Build 8	--	Undefined
Acme-Wrks1	Unknown	14505	9.2 - Build 8	--	Undefined

Figure 571

2. The **System source type** window opens.



Group: BurgerKing Filter By: All Type: Unassigned

□ Computer	Port	Source Type
□ BurgerKing11-syslog	514	
□ BurgerKing12-syslog	518	
□ BurgerKing13-syslog	517	
□ BurgerKing14-syslog	516	
□ BurgerKing15-syslog	516	
□ BurgerKing16-syslog	516	
□ BurgerKing17-syslog	516	
□ BurgerKing18-syslog	515	
□ BurgerKing19-syslog	515	
□ BurgerKing2-syslog	516	
□ BurgerKing20-syslog	515	
□ BurgerKing21-syslog	514	
□ BurgerKing22-syslog	517	
□ BurgerKing23-syslog	517	
□ BurgerKing24-syslog	518	
□ BurgerKing25-syslog	518	

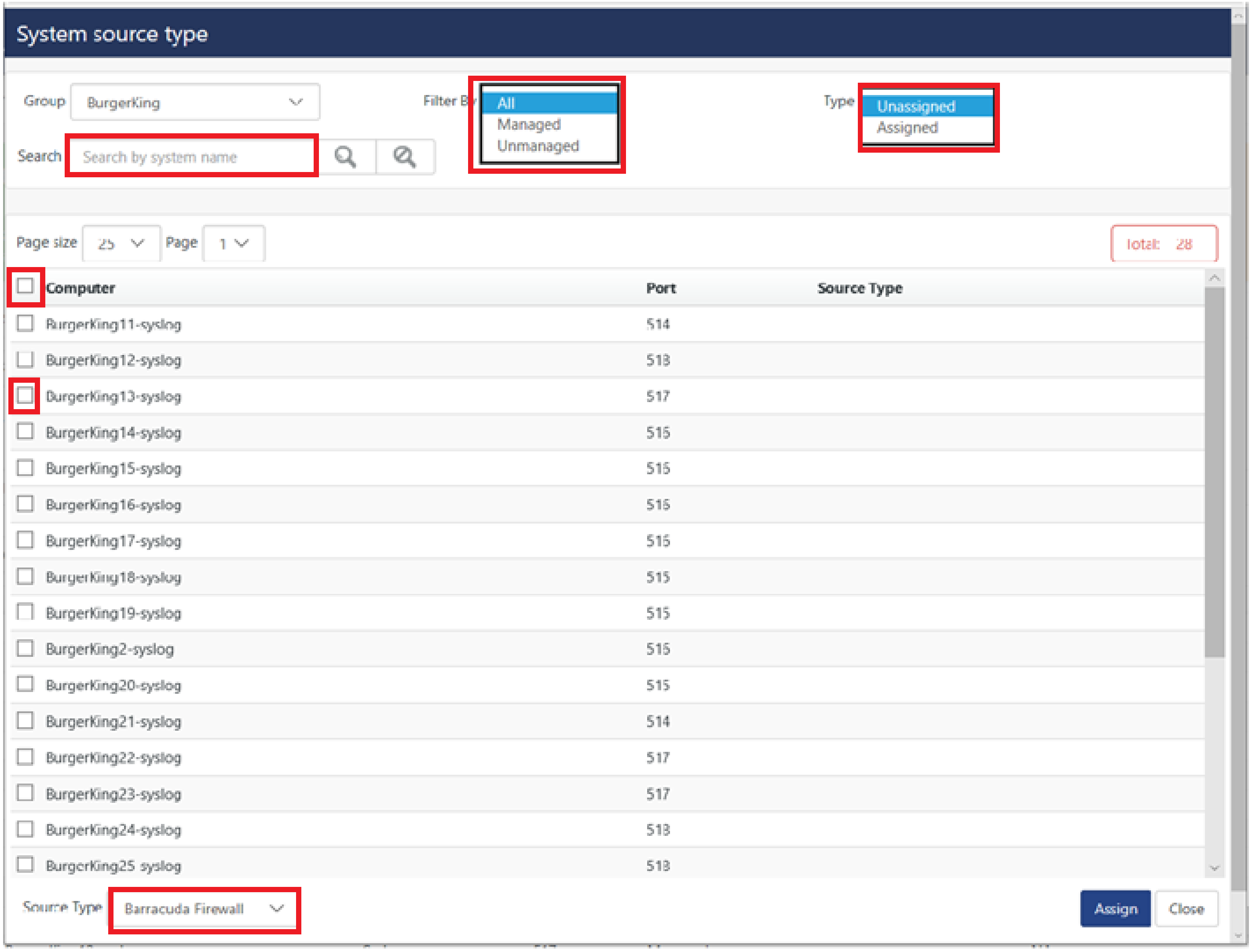
Source Type: Barracuda Firewall

Figure 572

3. You can filter the groups based on **Type** and **Filter By**.
   You can also search the systems by typing in the search bar.

   To assign the source type to the group.

4. Choose the group you want to assign the source type to and Select **unassigned** option in the **Type** dropdown.
   All the unassigned systems appear.



System source type

Group: BurgerKing

Search: Search by system name

Filter By: All / Managed / Unmanaged

Type: Unassigned / Assigned

Page size: 25 Page: 1 Total: 28

□ Computer	Port	Source Type
□ BurgerKing11-syslog	514	
□ BurgerKing12-syslog	513	
□ BurgerKing13-syslog	517	
□ BurgerKing14-syslog	515	
□ BurgerKing15-syslog	515	
□ BurgerKing16-syslog	515	
□ BurgerKing17-syslog	515	
□ BurgerKing18-syslog	515	
□ BurgerKing19-syslog	515	
□ BurgerKing2-syslog	515	
□ BurgerKing20-syslog	515	
□ BurgerKing21-syslog	514	
□ BurgerKing22-syslog	517	
□ BurgerKing23-syslog	517	
□ BurgerKing24-syslog	513	
□ BurgerKing25-syslog	513	

Source Type: Barracuda Firewall

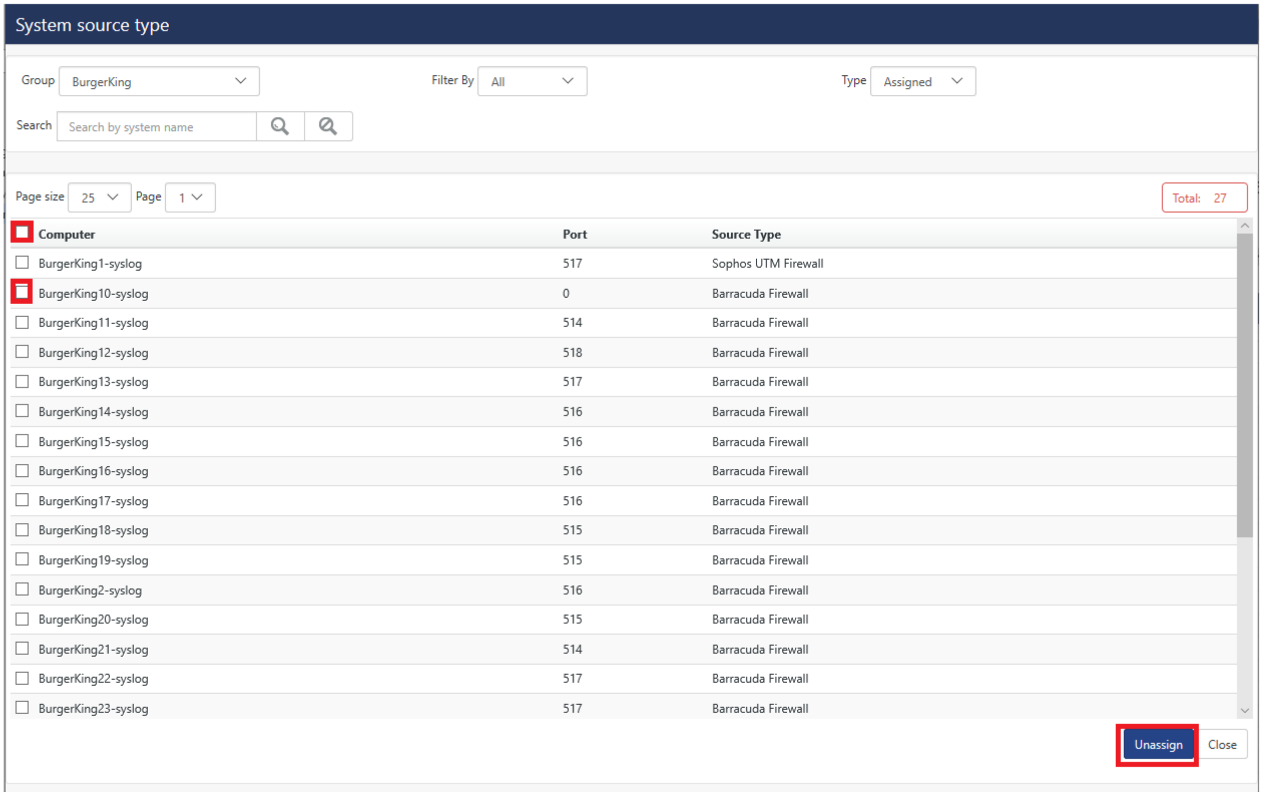
Figure 573

5. Choose the required source type by clicking on the **Source Type** dropdown at the bottom.
   Select the check box next to the computer to select all the computers in that group and click **Assign**.
   You may also uncheck the check box next to the systems to unassign the system.

6. The source type is assigned to all the selected systems of the group.

Similarly, to unassign the Group.

1. Choose the **Group** you want to unassign the source type to.
2. Select **Assigned option** in the **Type** drop down.
3. All the assigned systems appear.
4. Click **Unassign** to unassign source type to all the selected system of the group.
   Select the check box next to the computer to select all the computers in that group and click Unassign.
   You may also uncheck the check box next to the systems to unassign the system.
5. The source type is unassigned to all the selected systems of the group.



System source type

Group: BurgerKing
Filter By: All
Type: Assigned
Search: Search by system name

Page size: 25 Page: 1 Total: 27

□	Computer	Port	Source Type
□	BurgerKing1-syslog	517	Sophos UTM Firewall
□	BurgerKing10-syslog	0	Barracuda Firewall
□	BurgerKing11-syslog	514	Barracuda Firewall
□	BurgerKing12-syslog	518	Barracuda Firewall
□	BurgerKing13-syslog	517	Barracuda Firewall
□	BurgerKing14-syslog	516	Barracuda Firewall
□	BurgerKing15-syslog	516	Barracuda Firewall
□	BurgerKing16-syslog	516	Barracuda Firewall
□	BurgerKing17-syslog	516	Barracuda Firewall
□	BurgerKing18-syslog	515	Barracuda Firewall
□	BurgerKing19-syslog	515	Barracuda Firewall
□	BurgerKing2-syslog	516	Barracuda Firewall
□	BurgerKing20-syslog	515	Barracuda Firewall
□	BurgerKing21-syslog	514	Barracuda Firewall
□	BurgerKing22-syslog	517	Barracuda Firewall
□	BurgerKing23-syslog	517	Barracuda Firewall

Figure 574

23. Manage Users

In this chapter, you will learn to:

- Elevate normal user as an EventTracker Administrator or Read Only Administrator
- Logo Customization

23.1 EventTracker Roles, Permissions & Privileges

23.1.1 Roles

Role can be defined in terms of the authorization and obligation policies for a 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.

23.1.2 Privileges

Privileges are the rights granted to roles to access EventTracker modules.

23.1.3 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

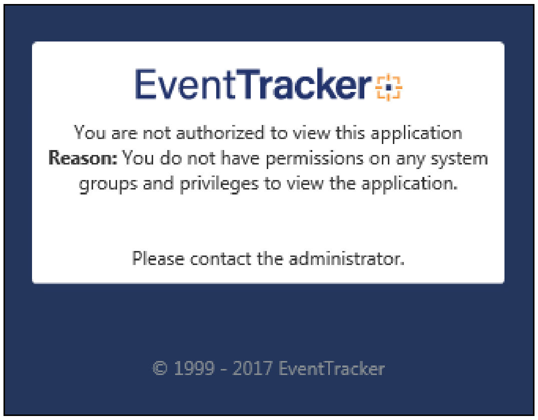
A non-Admin user

- Cannot access the EventTracker Web Control Panel
- Is restricted to the access of only those modules for which he/she is having permissions and privileges granted

For Example: If the non-admin user is granted permission for a group, he/she will only have access to the systems within that group. The user will be able to view the data pertaining to that group in various places such as Dashboards, Incidents, Search, Reports, etc.

If a non-admin user is granted privileges for modules such as Search, Reports and Incidents, then the user will be able to make use of only those modules.

Even if the user is a member of EventTracker User Group, EventTracker denies access if the user is not explicitly granted permissions and privileges.



EventTracker

You are not authorized to view this application
Reason: You do not have permissions on any system groups and privileges to view the application.

Please contact the administrator.

© 1999 - 2017 EventTracker

Figure 575

23.2 Managed Service Provider feature

The User Interface for the feature" **User Management**" has been revamped. A new feature "**Managed Service provider (MSP) in User management**", while enabling Database Authentication.

The MSP feature provided in the update will serve the sole purpose of managing subscription related activities such as managing user accounts and monthly usage details of services provided by EventTracker per client.

23.2.1 How it Works?

The MSP feature will be available only when the user enables the Database Authentication in EventTracker Configuration.

MSP Admin will be responsible in managing and handling users at Customers' environment (by adding/removing/changing password).

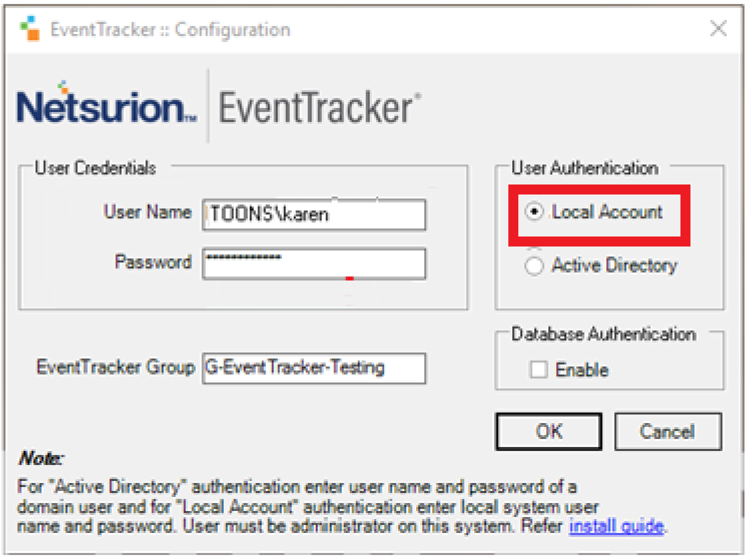
EventTracker Console might also run on Local or Active Directory authentication, based on selection made in EventTracker Configuration.

****IMPORTANT**: MSP feature will be available only for Database Authentication.

23.2.2 EventTracker with Local Account Authentication only/ Active Directory Authentication only

NOTE: Depending on the User Authentication selected, the database will be fetched in the User Management page.

For Local account authentication,



EventTracker :: Configuration

User Credentials

User Name: TOONS\karen

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

EventTracker Group: G-Event Tracker-Testing

User Authentication

● Local Account

○ Active Directory

Database Authentication

□ Enable

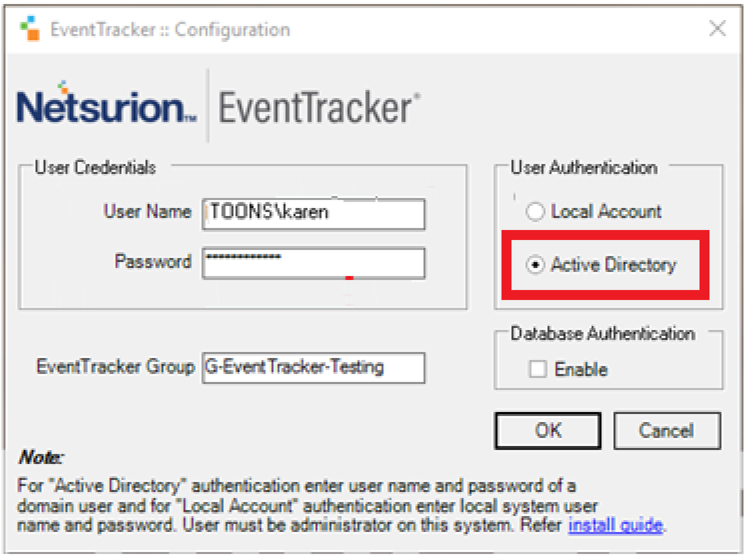
Note:

For "Active Directory" authentication enter user name and password of a domain user and for "Local Account" authentication enter local system user name and password. User must be administrator on this system. Refer install guide.

Figure 576

(Local Account)

For Active Directory authentication,



EventTracker :: Configuration

User Credentials

User Name: TOONS\karen

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

EventTracker Group: G-Event Tracker-Testing

User Authentication

○ Local Account

● Active Directory

Database Authentication

□ Enable

Note:

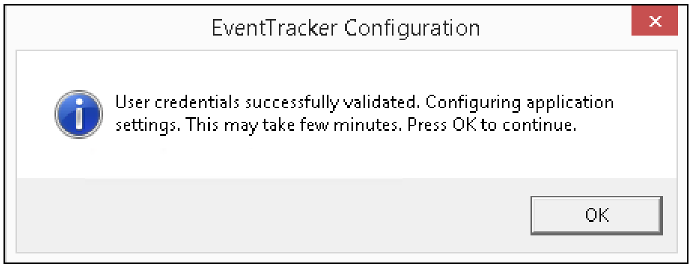
For "Active Directory" authentication enter user name and password of a domain user and for "Local Account" authentication enter local system user name and password. User must be administrator on this system. Refer install guide.

Figure 577

(Active Directory)

1. Enter the credentials in the “**EventTracker Configuration**” window selecting **Active Directory** and click **OK**.

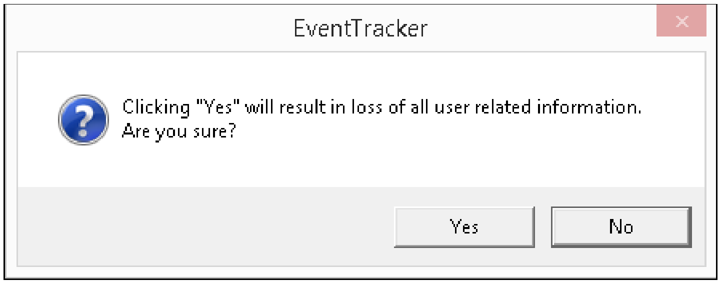
- It will display the below message.



User credentials successfully validated. Configuring application settings. This may take few minutes. Press OK to continue.

Figure 578

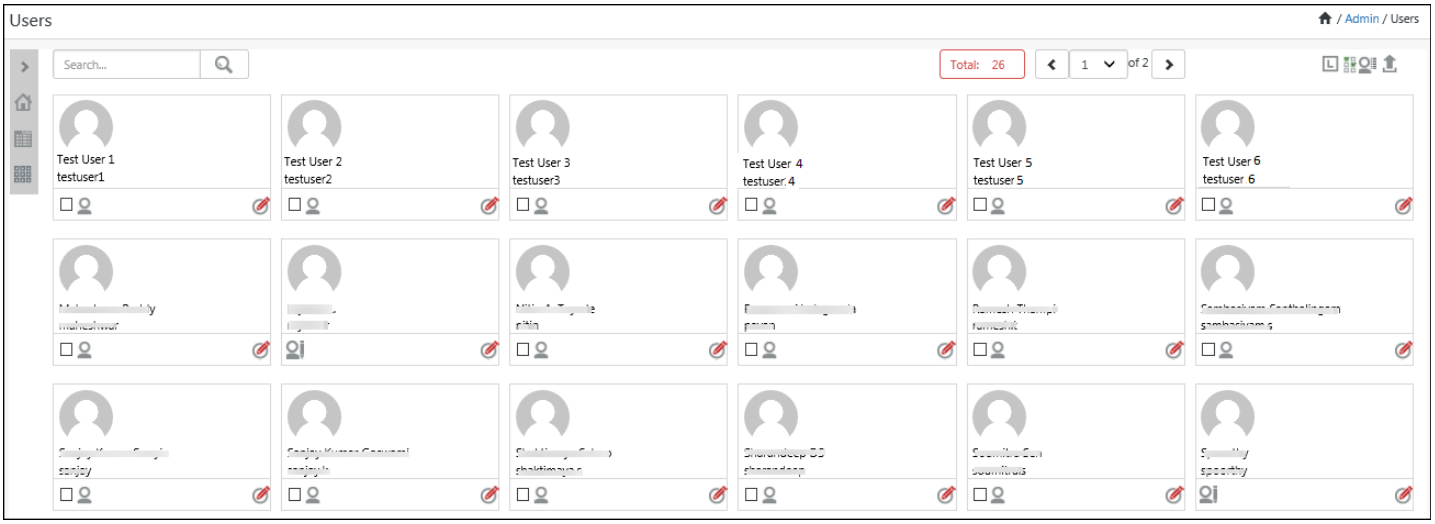
****IMPORTANT**: If the user toggles between **Database Authentication** being **Enabled/Disabled**, you will get the following warning message.



Clicking "Yes" will result in loss of all user related information. Are you sure?

Figure 579

2. The user can click "**Yes**" and proceed.
3. Now login to **EventTracker Web** and navigate to **Admin->Users.**



Test User 1
testuser1

Test User 2
testuser2

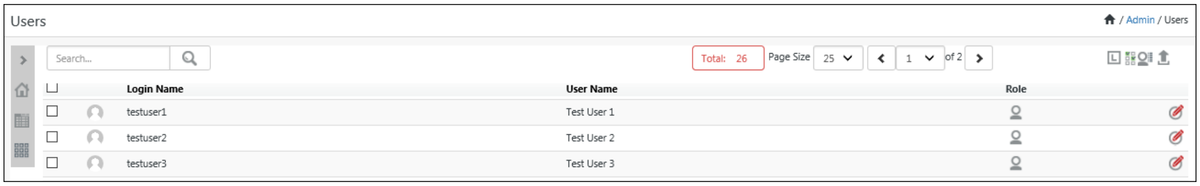
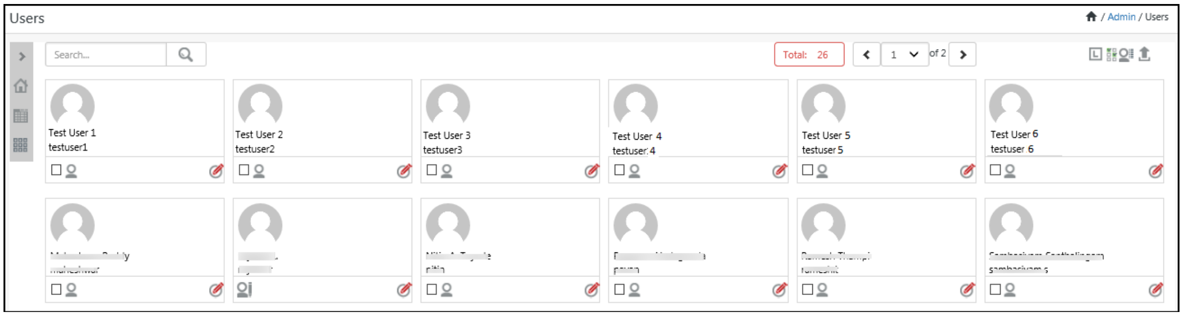
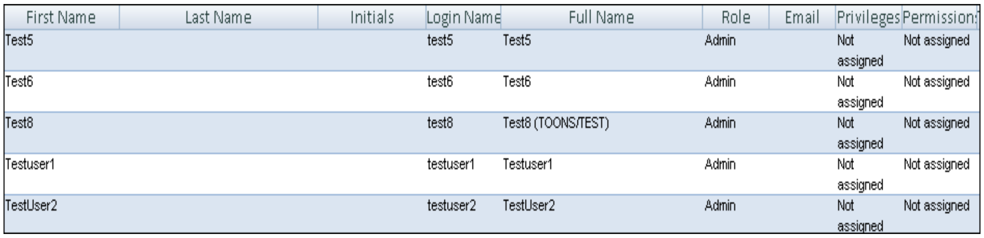
Test User 3
testuser3

Test User 4
testuser 4

Test User 5
testuser 5

Test User 6
testuser 6

Figure 580

<table>
<tr><th>Click</th><th>To</th></tr>
<tr><td>🏠</td><td>View the Home page for the respective view format selected (Tabular or Tile).</td></tr>
<tr><td>▦</td><td>Tabular view of users.

Users
/ Admin / Users
Search... Total: 26 Page Size 25 1 of 2
<table>
<tr><th>□</th><th></th><th>Login Name</th><th>User Name</th><th>Role</th><th></th></tr>
<tr><td>□</td><td></td><td>testuser1</td><td>Test User 1</td><td></td><td></td></tr>
<tr><td>□</td><td></td><td>testuser2</td><td>Test User 2</td><td></td><td></td></tr>
<tr><td>□</td><td></td><td>testuser3</td><td>Test User 3</td><td></td><td></td></tr>
</table></td></tr>
<tr><td>▦</td><td>Tile view of users.

Users
/ Admin / Users
Search... Total: 26 1 of 2
Test User 1 testuser1
Test User 2 testuser2
Test User 3 testuser3
Test User 4 testuser 4
Test User 5 testuser 5
Test User 6 testuser 6
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]</td></tr>
<tr><td></td><td>To export the user details in an excel format.

<table>
<tr><th>First Name</th><th>Last Name</th><th>Initials</th><th>Login Name</th><th>Full Name</th><th>Role</th><th>Email</th><th>Privileges</th><th>Permission!</th></tr>
<tr><td>Test5</td><td></td><td></td><td>test5</td><td>Test5</td><td>Admin</td><td></td><td>Not assigned</td><td>Not assigned</td></tr>
<tr><td>Test6</td><td></td><td></td><td>test6</td><td>Test6</td><td>Admin</td><td></td><td>Not assigned</td><td>Not assigned</td></tr>
<tr><td>Test8</td><td></td><td></td><td>test8</td><td>Test8 (TOONS/TEST)</td><td>Admin</td><td></td><td>Not assigned</td><td>Not assigned</td></tr>
<tr><td>Testuser1</td><td></td><td></td><td>testuser1</td><td>Testuser1</td><td>Admin</td><td></td><td>Not assigned</td><td>Not assigned</td></tr>
<tr><td>TestUser2</td><td></td><td></td><td>testuser2</td><td>TestUser2</td><td>Admin</td><td></td><td>Not assigned</td><td>Not assigned</td></tr>
</table></td></tr>
</table>

In the User Management page, click **Expand** ‹ to view the sites and the groups under it.

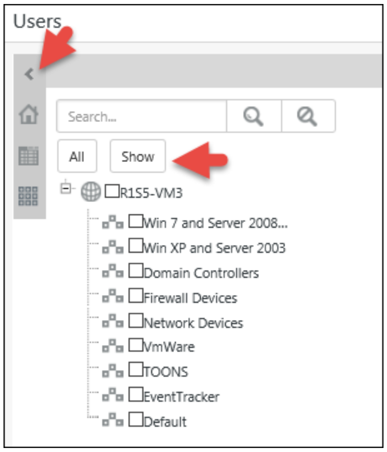


Figure 581

- Select the Site(s) or group(s) and click **Show** option. It shows all the user(s) who are given permission to those respective group(s) or Site(s).

23.2.3 Assigning Permission to users

If a user is granted permission for a group, you will only have access to the systems within that group. The user will be able to view the data pertaining to that group in various places such as Dashboards, Incidents, Search, Reports, etc.

1. To assign permission to a user, select the user.

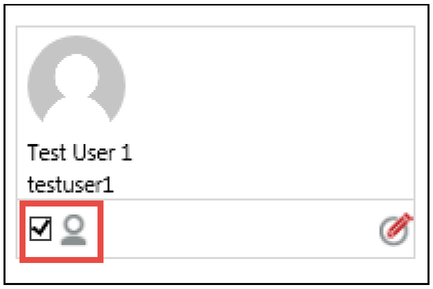


Figure 582

2. Click the assign permission icon ▦.
   It opens the below message.

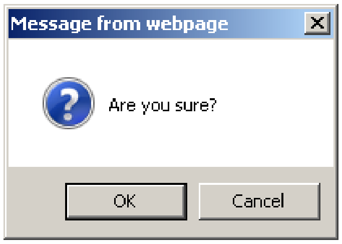
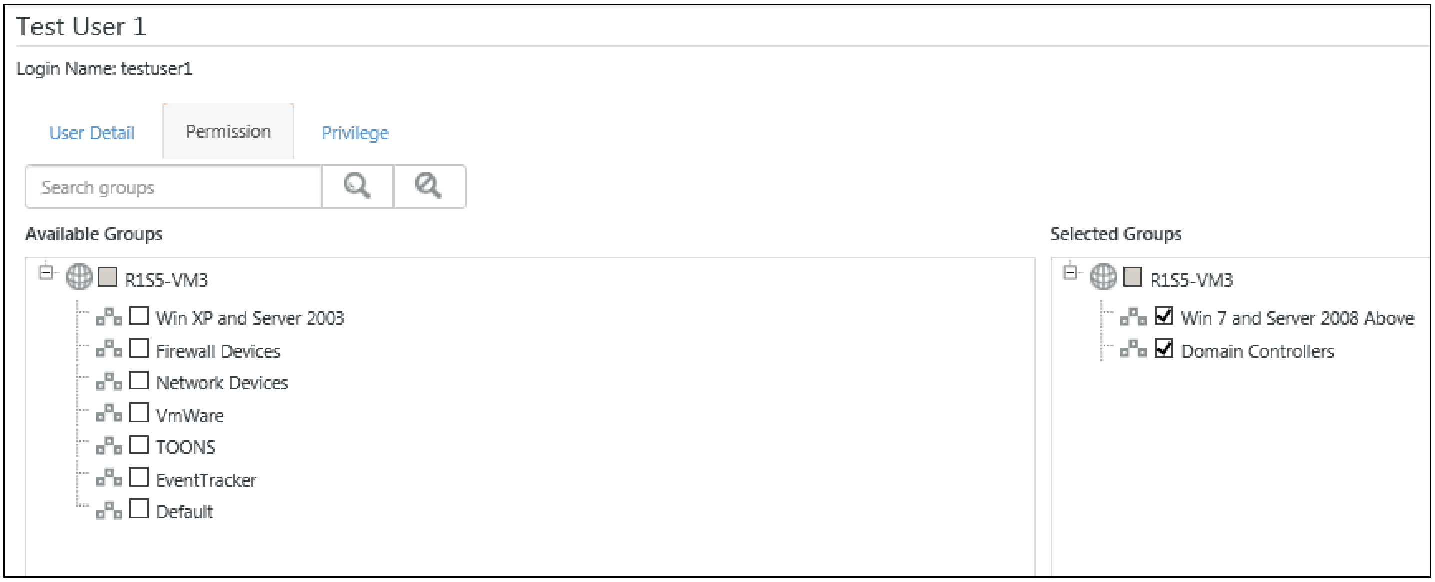


Figure 583

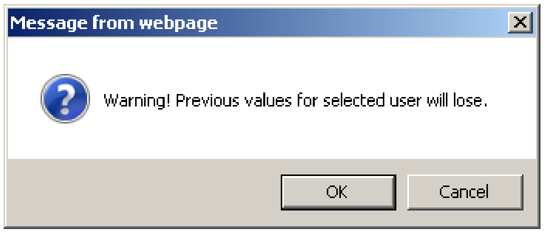
3. Click **OK**.
4. Select the groups which will get listed and displayed in the right pane.


Test User 1

Login Name: testuser1

Figure 584

5. Click **Save**.
   It will display a warning message.


Message from webpage

Warning! Previous values for selected user will lose.

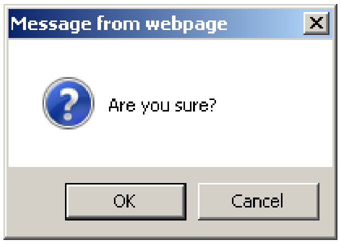
Figure 585

6. Click **OK**.

23.2.4 Assigning Privilege to users

If a user is granted privileges for modules such as Search, Reports and Incidents, then the user will be able to make use of only those modules.

1. Select the user and click Assign privilege 👤 .
   The following message opens.

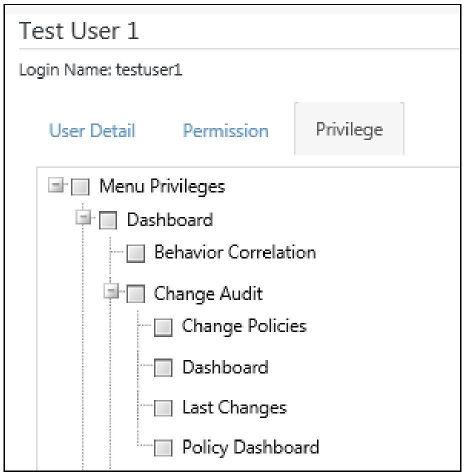


Message from webpage

Are you sure?

Figure 586

2. Click **OK**.
3. Select the modules and click **Save**.



Test User 1

Login Name: testuser1

- □ Menu Privileges
  - □ Dashboard
    - □ Behavior Correlation
    - □ Change Audit
      - □ Change Policies
      - □ Dashboard
      - □ Last Changes
      - □ Policy Dashboard

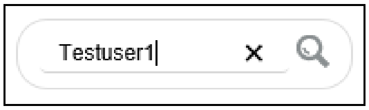
Figure 587

23.2.5 Promoting a User as an Administrator or Read Only Administrator

Some customers or administrators may wish to restrict permissions of other users/administrators by giving read only permissions to other users/administrators. We have the option for read only admin(s) in which they will have the permission to only view data and reports. They cannot edit or modify them. All the modules in which there is an option to create, add, save, modify, and delete have been provided will be disabled.

To promote a User as an Administrator or Read Only Administrator-

1. Search the user by entering the name in the search box and click **Search** 🔍 .



Testuser1

Figure 588

2. To modify permissions of the user, click the respective edit ✎ icon.

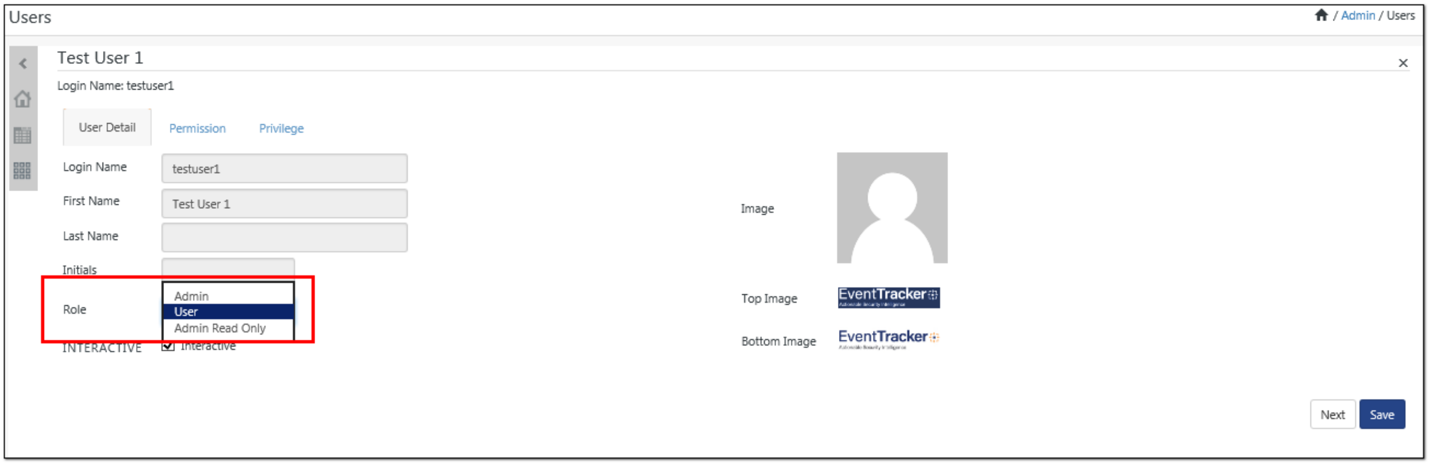
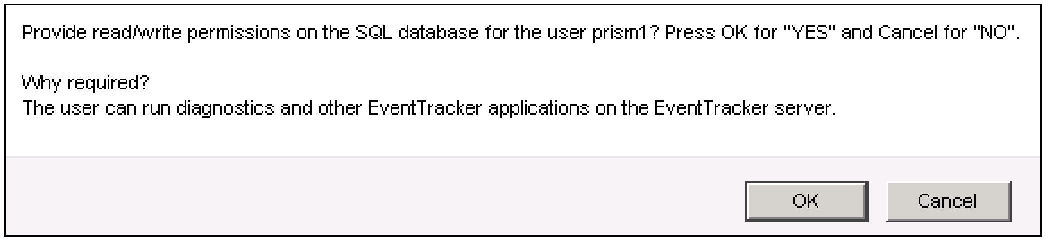


Figure 589

3. The user can give either **Admin/Admin Read Only** permission for that respective user.
4. After **Saving** the following message opens.


Provide read/write permissions on the SQL database for the user prism1? Press OK for "YES" and Cancel for "NO".

Why required?
The user can run diagnostics and other EventTracker applications on the EventTracker server.

Figure 590

(Applies to Admin only)

5. Click **OK**.

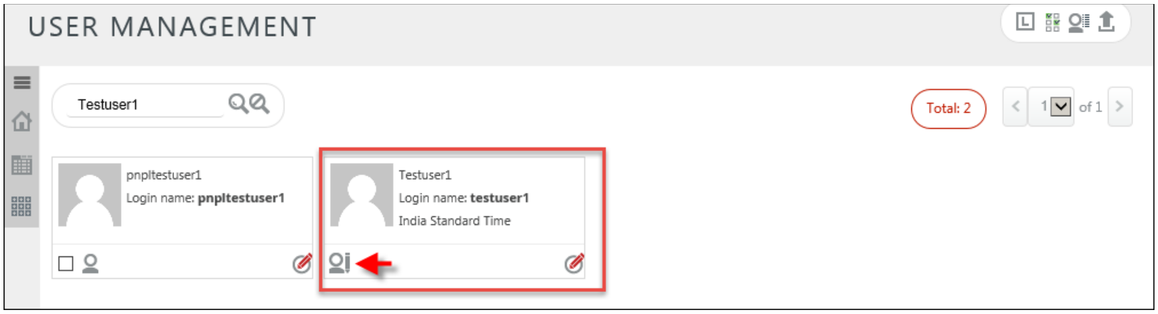
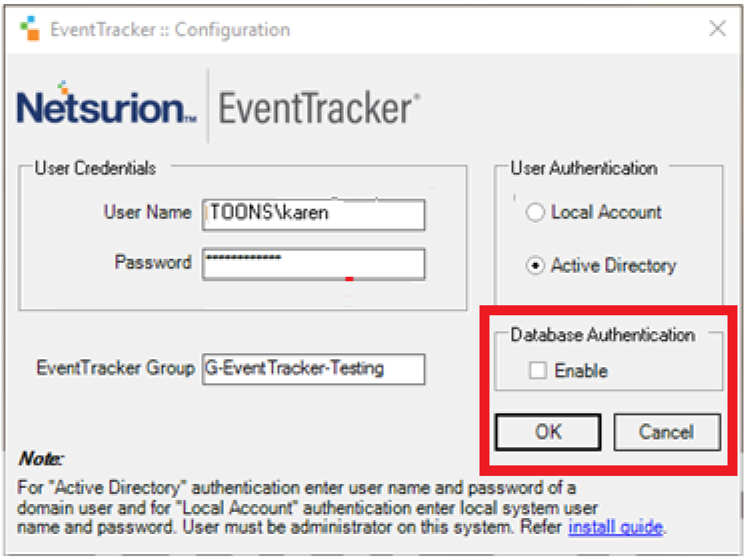


Figure 591

NOTE: The icon signifies that administrator permissions have been assigned and the icon signifies that read only administrator permissions have been assigned.

23.3 EventTracker with Active Directory and Database Authentication

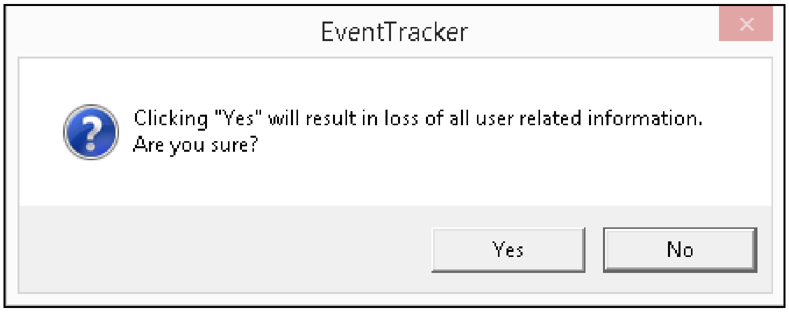
a) For Active Directory authentication with database enabled, in EventTracker Configuration window, enter the user credentials and check the option “**Enable**” under Database authentication.



Note:
For "Active Directory" authentication enter user name and password of a domain user and for "Local Account" authentication enter local system user name and password. User must be administrator on this system. Refer install guide.

Figure 592

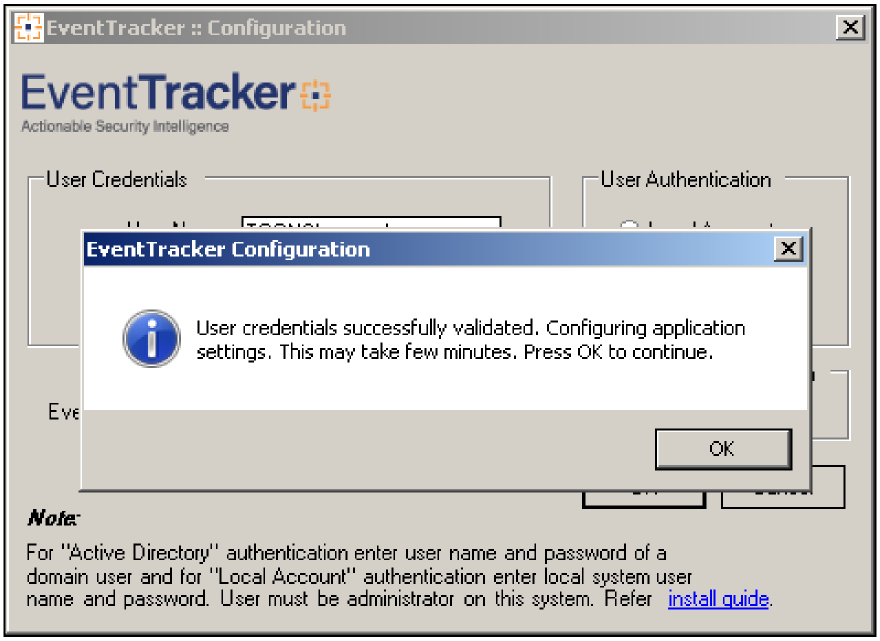
b) Once you click **OK**, the following message appears.



Clicking "Yes" will result in loss of all user related information. Are you sure?

Figure 593

c) Click **Yes** and proceed.


EventTracker :: Configuration
EventTracker
Actionable Security Intelligence
User Credentials
User Authentication
Eve
EventTracker Configuration
OK

User credentials successfully validated. Configuring application settings. This may take few minutes. Press OK to continue.

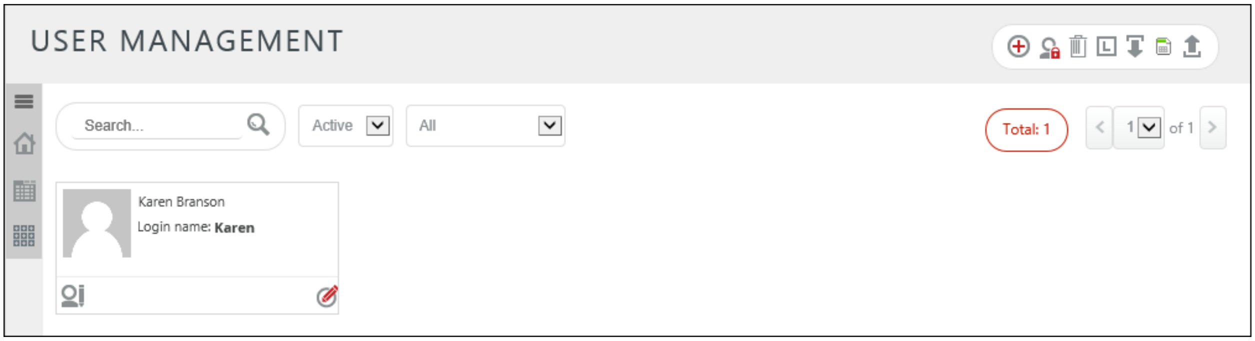
Note:

For "Active Directory" authentication enter user name and password of a domain user and for "Local Account" authentication enter local system user name and password. User must be administrator on this system. Refer install guide.

Figure 594

d) Click **OK.**

6. Now login to **EventTracker Web** and navigate to **Admin->Users.**



Karen Branson
Login name: **Karen**

Figure 595

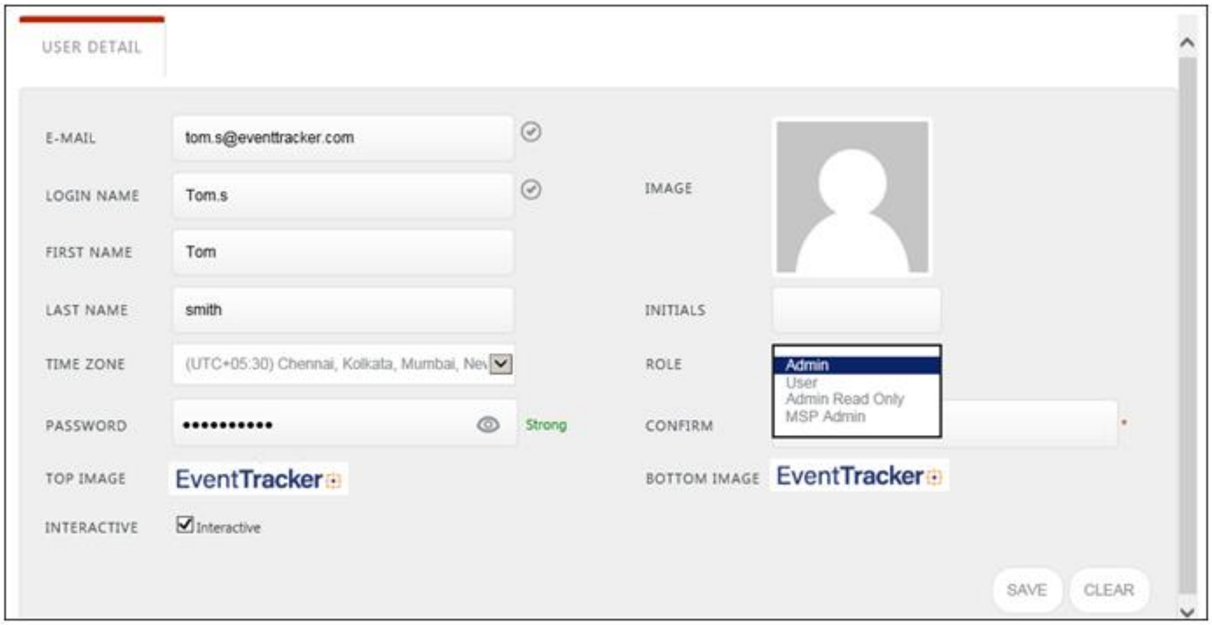
Click	To
⊕	Add a user
🔒	Inactivate a user
🗑	Delete a user
⬇	Import the user details to excel.
▦	Download the excel template.

Figure 596

23.3.1 Adding an Admin User

The admin user will have the permission to assign role of other **Admin(s)**, **MSP Admin(s)**, **Users** and **Admin Read Only.**

- Click **Add a user** ⊕ and enter the user details as shown in the figure below.

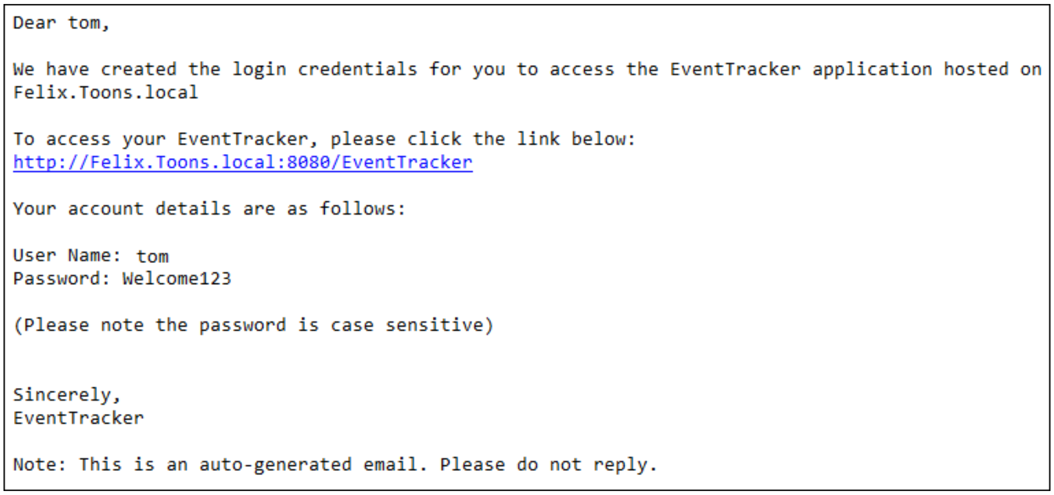


USER DETAIL

E-MAIL	tom.s@eventtracker.com
LOGIN NAME	Tom.s
FIRST NAME	Tom
LAST NAME	smith
TIME ZONE	(UTC+05:30) Chennai, Kolkata, Mumbai, Ne\
PASSWORD	••••••••••• Strong
TOP IMAGE	EventTracker
INTERACTIVE	☑ Interactive
IMAGE	
INITIALS	
ROLE	Admin User Admin Read Only MSP Admin
CONFIRM	
BOTTOM IMAGE	EventTracker

Figure 597

- After entering the user details, click **Save**.
  The created user will receive an e-mail id with "**Login Details**" message.



```
Dear tom,

We have created the login credentials for you to access the EventTracker application hosted on
Felix.Toons.local

To access your EventTracker, please click the link below:
http://Felix.Toons.local:8080/EventTracker

Your account details are as follows:

User Name:  tom
Password: Welcome123

(Please note the password is case sensitive)


Sincerely,
EventTracker

Note: This is an auto-generated email. Please do not reply.
```

Figure 598

7. The user needs to click the URL provided in the e-mail and enter the credentials in the login page.

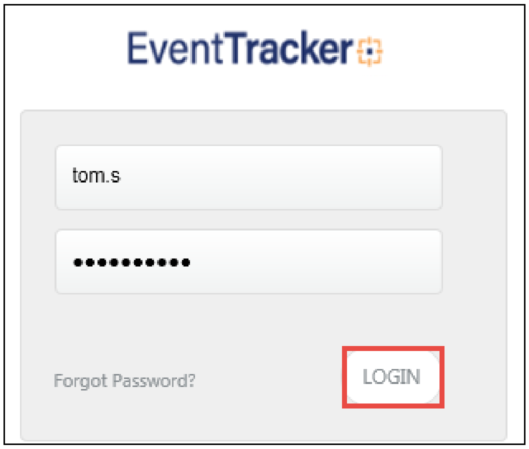
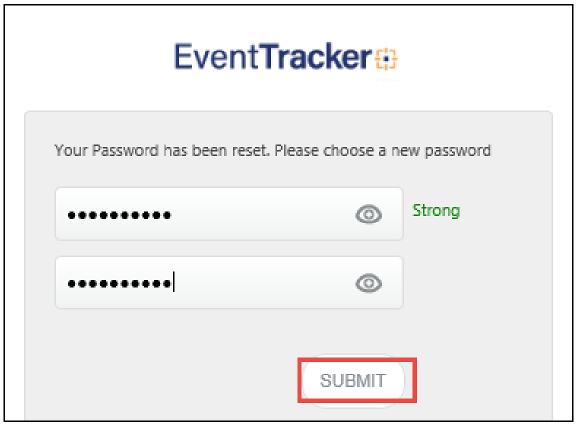


Figure 599

8. Click **LOGIN.**
   The reset password page opens.



Your Password has been reset. Please choose a new password

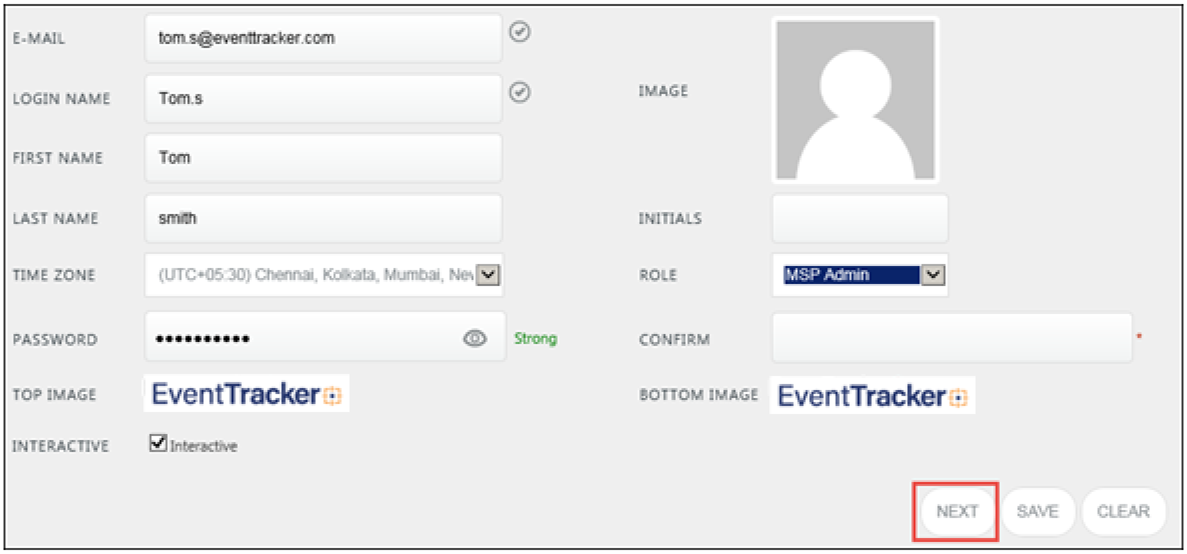
Figure 600

9. Enter your user-friendly password and click **SUBMIT**.
   The main page for the user opens. Hover over the profile name and select " **View profile**" option for the profile details.

23.3.2 Adding an MSP Admin(s) User

NOTE: For assigning role as (**MSP Admin**), the admin user will have options to add permissions.

For example: If the admin user assigns "**Tom**", the role of an MSP admin, you will have the option of navigating to the **Next ->**tab. This is shown in the figure below:

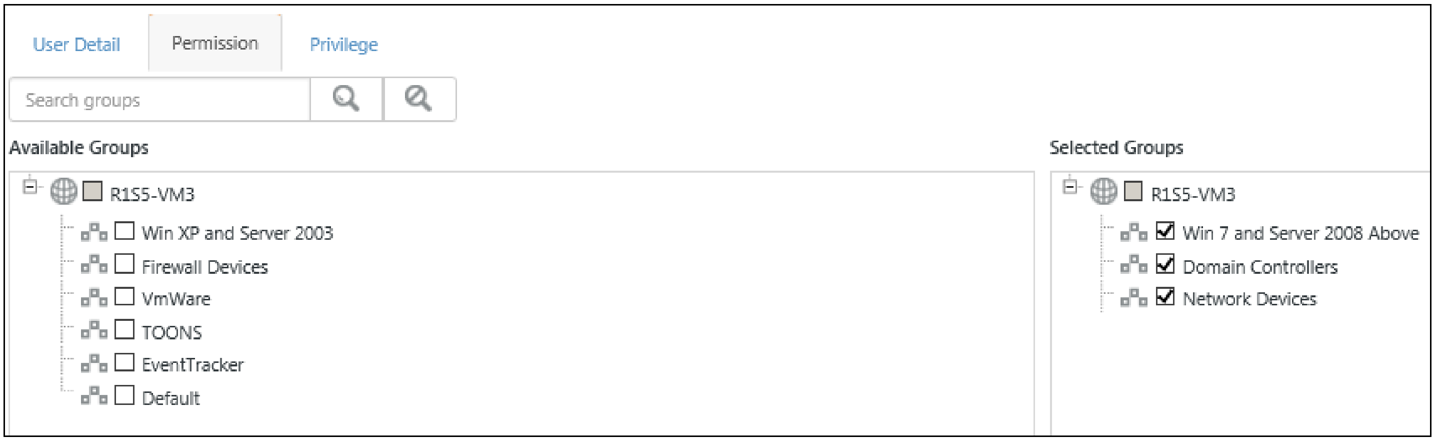


E-MAIL: tom.s@eventtracker.com
LOGIN NAME: Tom.s
FIRST NAME: Tom
LAST NAME: smith
TIME ZONE: (UTC+05:30) Chennai, Kolkata, Mumbai, Nev
PASSWORD: •••••••••• Strong
INTERACTIVE: ☑ Interactive
INITIALS:
ROLE: MSP Admin
CONFIRM:

Figure 601

Assign permission to selected Groups from the sites available and then click **Save**.

- The selected groups open in the right pane.



User Detail | Permission | Privilege

Search groups

Available Groups

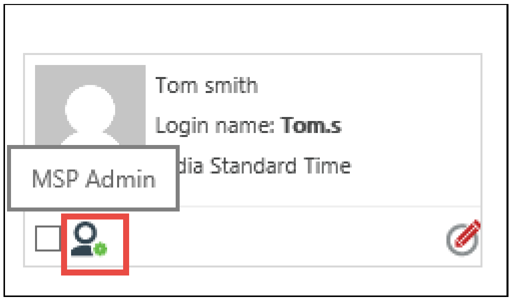
- ☐ R1S5-VM3
  - ☐ Win XP and Server 2003
  - ☐ Firewall Devices
  - ☐ VmWare
  - ☐ TOONS
  - ☐ EventTracker
  - ☐ Default

Selected Groups

- ☐ R1S5-VM3
  - ☑ Win 7 and Server 2008 Above
  - ☑ Domain Controllers
  - ☑ Network Devices

Figure 601

10. The 👤 icon signifies that MSP Admin permissions have been assigned.



Tom smith

Login name: **Tom.s**

dia Standard Time

MSP Admin

☐

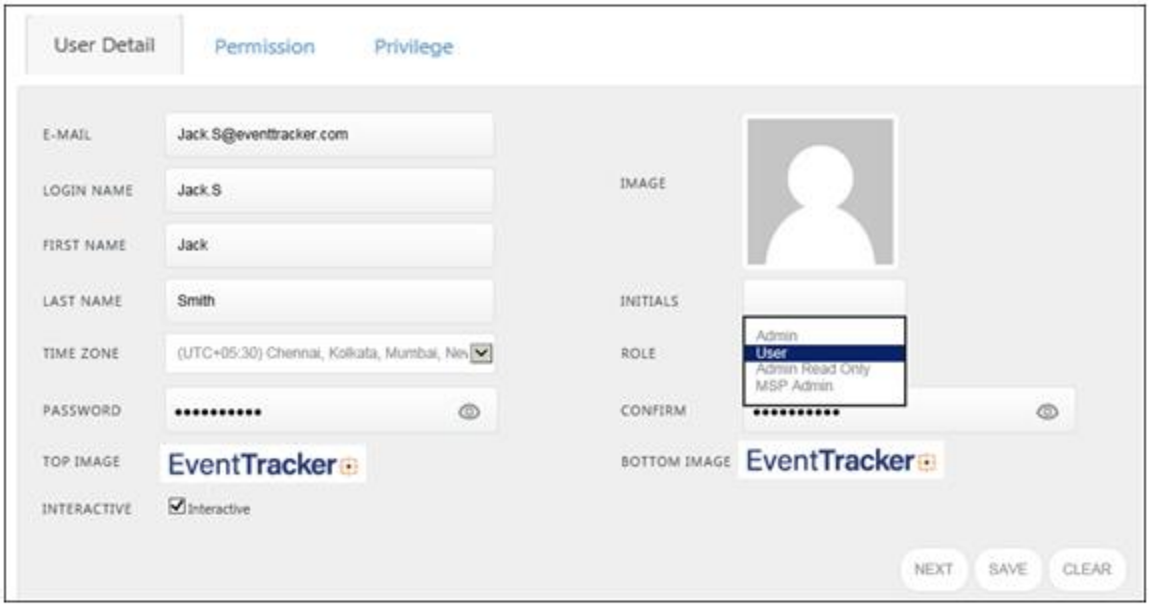
Figure 602

11. The created MSP Admin user will receive an e-mail id with “**Login Details**” message. The user needs to click the URL, enter the credentials and login to EventTracker.

23.3.3 Adding a User(s)

NOTE: For assigning “**User**” roles, the admin user/MSP Admin will have both the options to add permissions and privileges to the user(s).

1. In the User details Page, in the **Role** field, select **User** from the dropdown options.
2. Click **Next**.



E-MAIL: Jack.S@eventtracker.com

LOGIN NAME: Jack.S

FIRST NAME: Jack

LAST NAME: Smith

TIME ZONE: (UTC+05:30) Chennai, Kolkata, Mumbai, Nev

PASSWORD: •••••••••••

TOP IMAGE: EventTracker

INTERACTIVE: ☑ Interactive

IMAGE

INITIALS

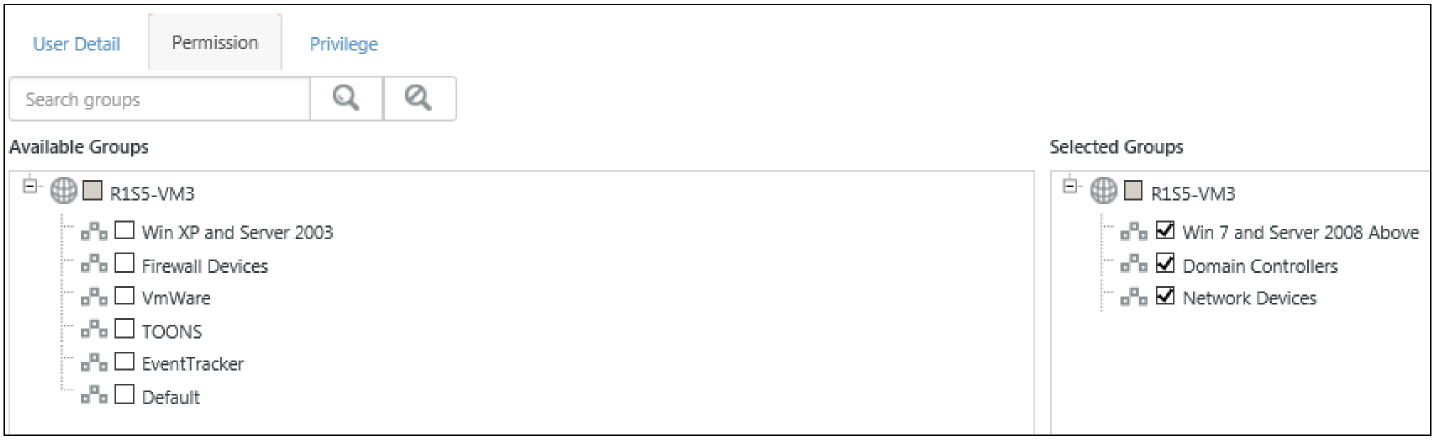
ROLE: Admin / User / Admin Read Only / MSP Admin (User selected)

CONFIRM: •••••••••••

BOTTOM IMAGE: EventTracker

Figure 603

3. Assign permission to selected groups from the site and click **Next**.



Available Groups

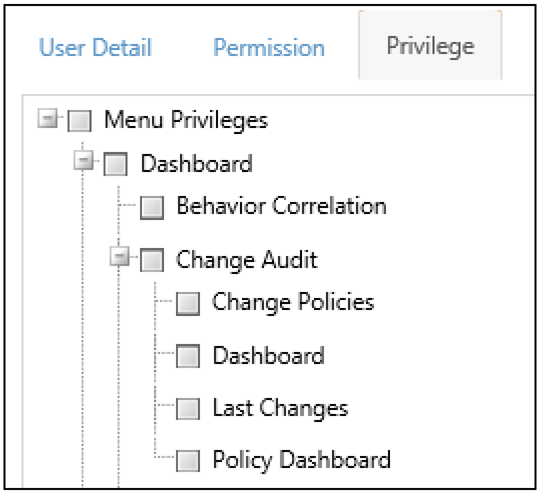
- □ R1S5-VM3
  - □ Win XP and Server 2003
  - □ Firewall Devices
  - □ VmWare
  - □ TOONS
  - □ EventTracker
  - □ Default

Selected Groups

- □ R1S5-VM3
  - ☑ Win 7 and Server 2008 Above
  - ☑ Domain Controllers
  - ☑ Network Devices

Figure 604

Assign the selected modules which they can make use of and then **Save** the changes.



- □ Menu Privileges
  - □ Dashboard
    - □ Behavior Correlation
    - □ Change Audit
      - □ Change Policies
      - □ Dashboard
      - □ Last Changes
      - □ Policy Dashboard

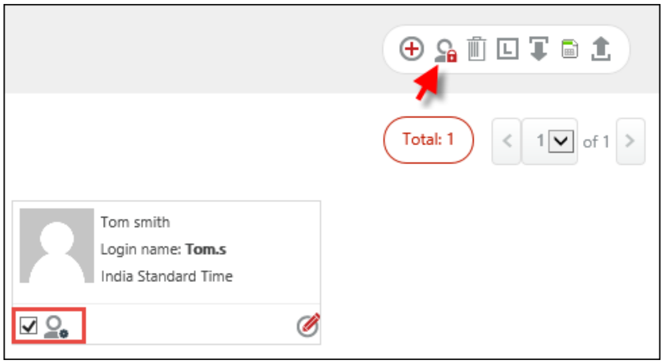
Figure 605

4. The created user will receive an e-mail id with “**Login Details**” message. The user needs to click the URL, enter the credentials and login to EventTracker.

23.4 Activating/Inactivating Users

To deactivate a user account,

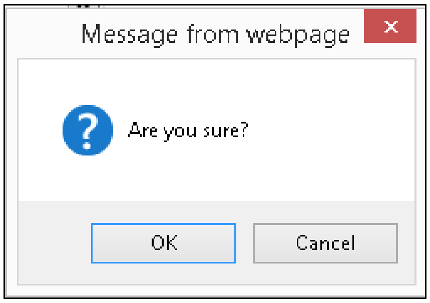
1. Select the respective user and then click **Inactivate user** in the right-hand side corner of the page.



Tom smith
Login name: **Tom.s**
India Standard Time

Figure 606

A confirmation message appears.



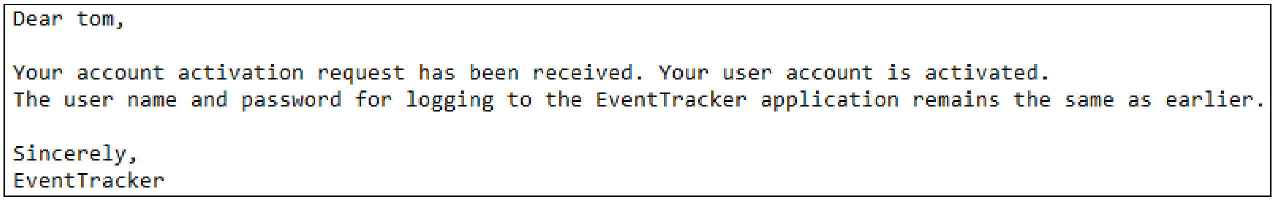
Message from webpage

Are you sure?

Figure 607

2. Click “**OK**”.
3. Similarly, to activate a user, select the respective inactive user(s), and click **activate user** . It opens the confirmation message. Click **OK**.

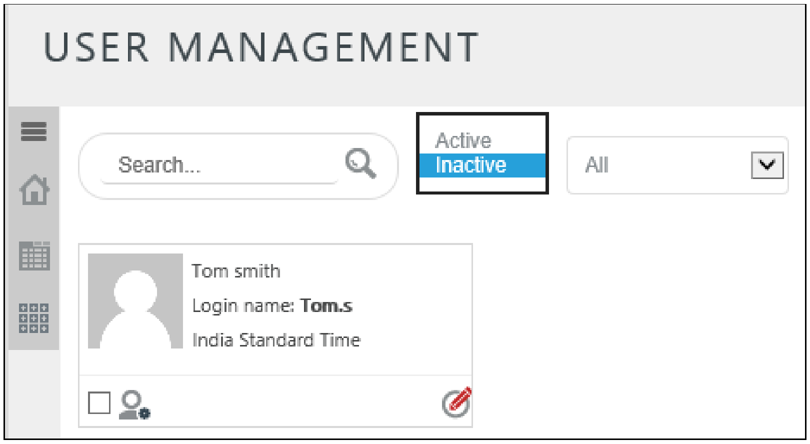
Once the user(s) gets activated, an auto-generated e-mail is received by the respective user(s). The figure is shown below:



```
Dear tom,

Your account activation request has been received. Your user account is activated.
The user name and password for logging to the EventTracker application remains the same as earlier.

Sincerely,
EventTracker
```

Figure 608

4. To view the active/ Inactive users, select the preferred option from the dropdown box.



USER MANAGEMENT

Tom smith

Login name: **Tom.s**

India Standard Time

Figure 609

5. Similarly, for viewing the user(s) based on their respective roles, use the dropdown option.

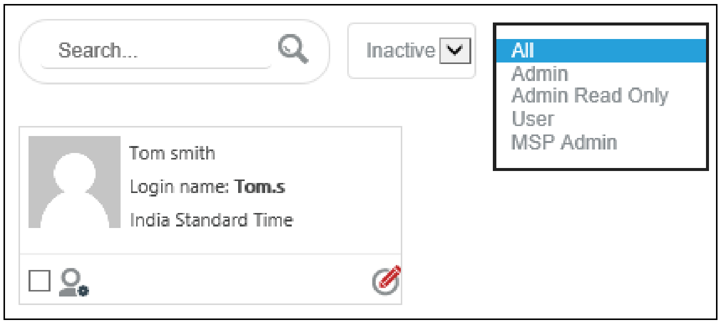


Figure 610

23.5 Forgot Password option

If the created **Admin(s)/MSP Admin(s)/User(s)** fail to remember the password, you can follow the below steps:

1. Login to **EventTracker** web.
2. In the login page, click **Forgot Password.**

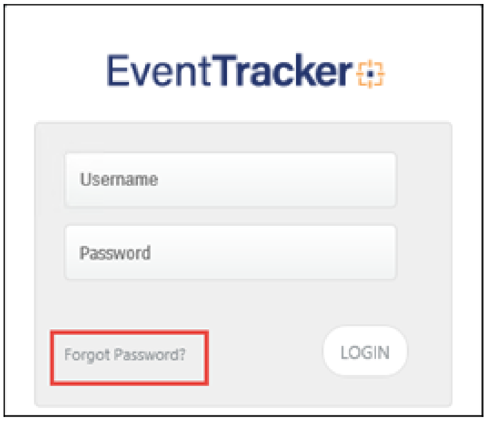
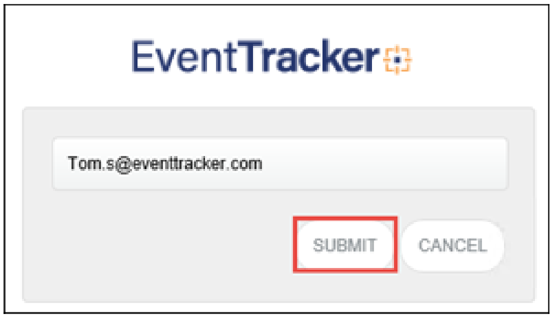


Figure 611

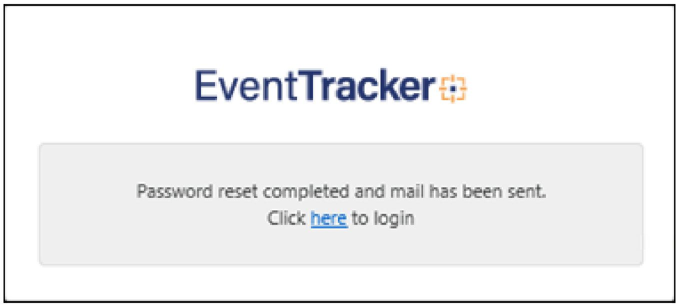
3. It will prompt you to enter your e-mail id. Provide the e-mail id and click **Submit**.



Tom.s@eventtracker.com

Figure 612

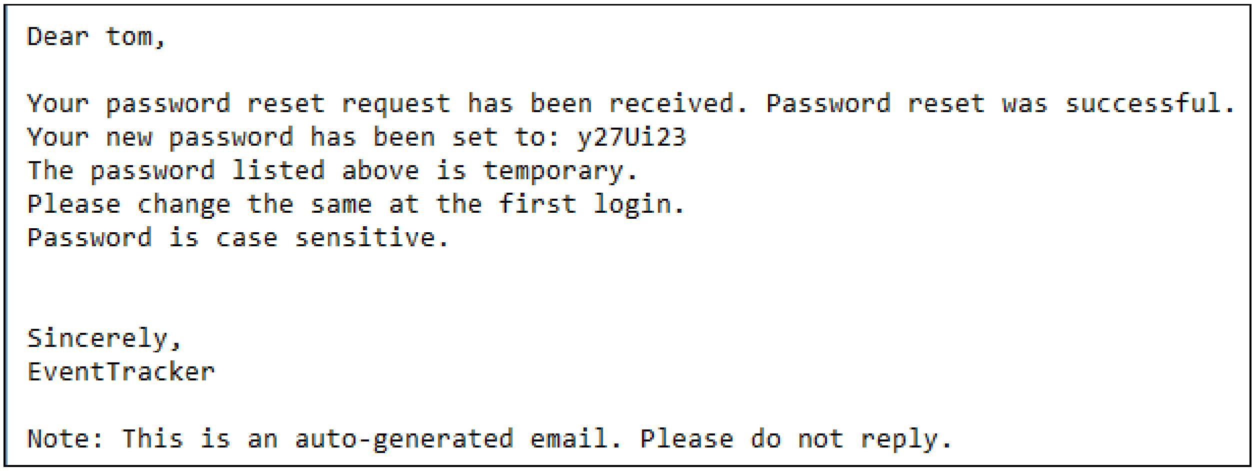
It opens the below message.



Password reset completed and mail has been sent.
Click here to login

Figure 613

4. It will send a "**Password Reset Confirmation**" e-mail to your mentioned e-mail id.



```
Dear tom,

Your password reset request has been received. Password reset was successful.
Your new password has been set to: y27Ui23
The password listed above is temporary.
Please change the same at the first login.
Password is case sensitive.


Sincerely,
EventTracker

Note: This is an auto-generated email. Please do not reply.
```

Figure 614

5. Use the new password sent via e-mail and click **Login**.

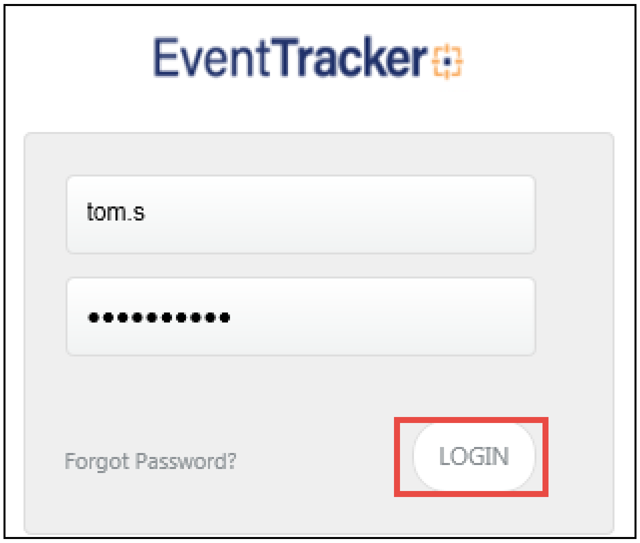
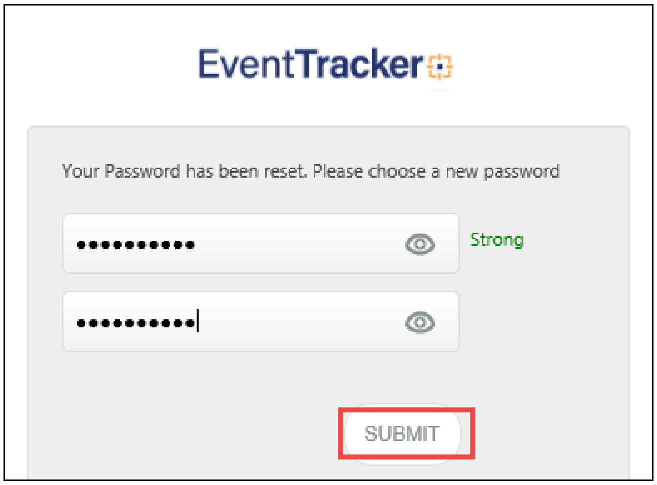


Figure 615

It opens “redirect to the Password reset page.”

6. Reset the password in to a user-friendly one and click **SUBMIT**.



Your Password has been reset. Please choose a new password

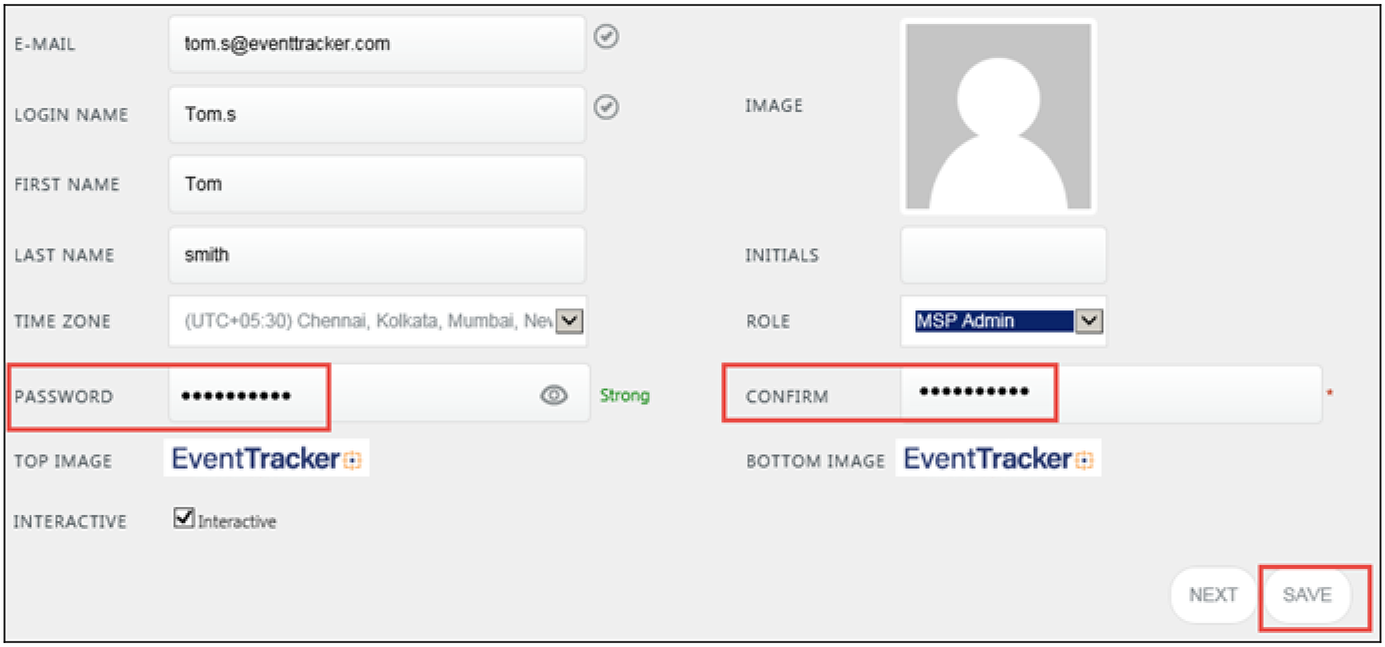
Figure 616

The user can successfully login to the EventTracker application.

23.6 Changing Password

If the MSP Admin(s) or User(s) wishes to change their password, follow the below mentioned steps:

- Login to **EventTracker** web using the existing password and click on **View Profile** from the dropdown list
- In the profile page, change the password and click **Save**.

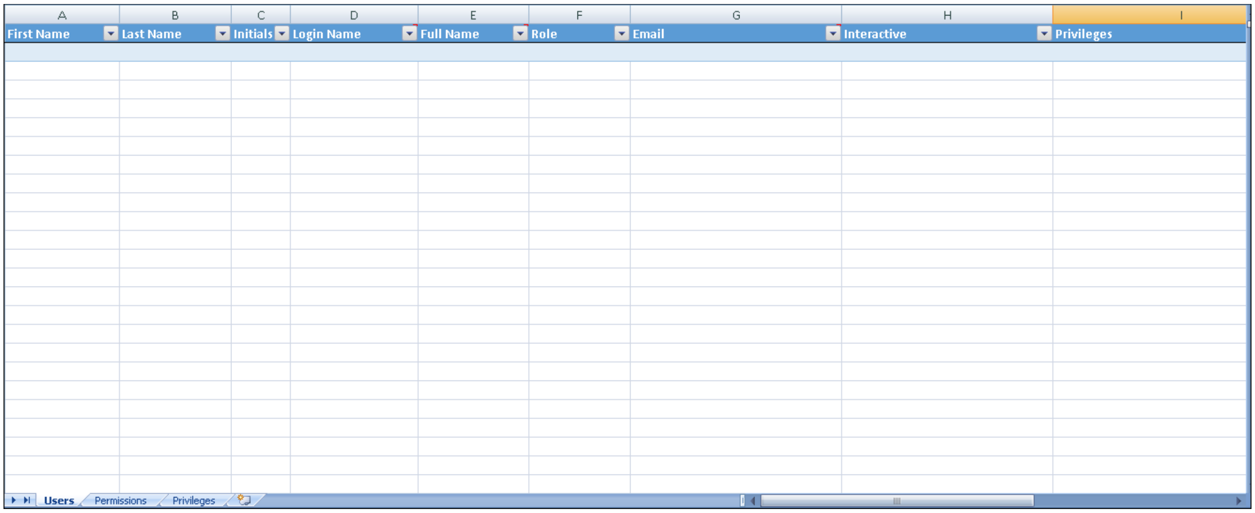


E-MAIL	tom.s@eventtracker.com	IMAGE	
LOGIN NAME	Tom.s		
FIRST NAME	Tom		
LAST NAME	smith	INITIALS	
TIME ZONE	(UTC+05:30) Chennai, Kolkata, Mumbai, Nev	ROLE	MSP Admin
PASSWORD	••••••••••• Strong	CONFIRM	•••••••••••
TOP IMAGE	EventTracker	BOTTOM IMAGE	EventTracker
INTERACTIVE	☑ Interactive		

Figure 617

23.7 Downloading Excel Template

Templates can be downloaded in the excel format using the icon , where the user can manually enter the user details in the respective columns provided. The user can also mention the permissions and privileges in the respective columns, by copying the required permissions and privileges from the respective sheets, provided in the template. The excel report prepared using the downloaded template can be further imported In excel format using the **Import** icon .

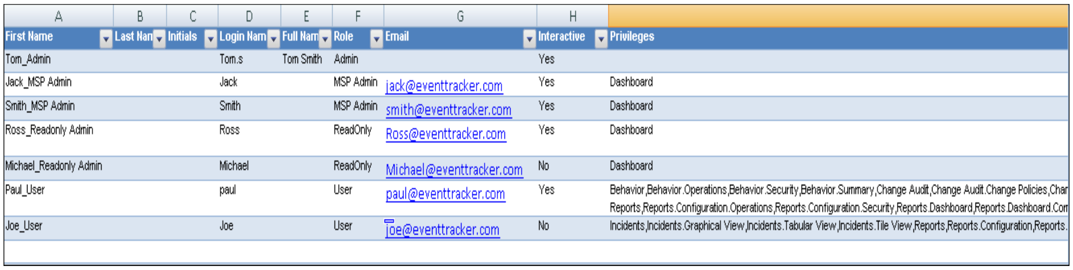


First Name	Last Name	Initials	Login Name	Full Name	Role	Email	Interactive	Privileges

Figure 618

23.8 Exporting to excel

To export the user roles in the excel format, click **Export** ⭱. The excel report gets exported with the user details.



First Name	Last Nam	Initials	Login Nam	Full Nam	Role	Email	Interactive	Privileges
Tom_Admin			Tom.s	Tom Smith	Admin		Yes	
Jack_MSP Admin			Jack		MSP Admin	jack@eventtracker.com	Yes	Dashboard
Smith_MSP Admin			Smith		MSP Admin	smith@eventtracker.com	Yes	Dashboard
Ross_Readonly Admin			Ross		ReadOnly	Ross@eventtracker.com	Yes	Dashboard
Michael_Readonly Admin			Michael		ReadOnly	Michael@eventtracker.com	No	Dashboard
Paul_User			paul		User	paul@eventtracker.com	Yes	Behavior,Behavior.Operations,Behavior.Security,Behavior.Summary,Change Audit,Change Audit.Change Policies,Char Reports,Reports.Configuration.Operations,Reports.Configuration.Security,Reports.Dashboard,Reports.Dashboard.Con
Joe_User			Joe		User	joe@eventtracker.com	No	Incidents,Incidents.Graphical View,Incidents.Tabular View,Incidents.Tile View,Reports,Reports.Configuration,Reports.

Figure 619

23.9 FAQs

1. **What are the types and roles of the User(s)?**

- **EventTracker Admin** (will be able to access all the available modules): Can create/assign user(s), MSP Admin(s) and Admin(s).

- **MSP Admin** (will be able to manage only its users): The MSP admin can perform CRUD operation for his/her MSP Users.

- **User(s)** (will not be able to access Admin modules): The users can only access modules to which he/she has been given permissions and privileges.

2. **If user re-runs the EventTracker configuration, what will be the existing database?**

   If user toggles (Enable/Disable), the Database authentication and runs the EventTracker configuration, then user data will be lost. Only the admin who runs the configuration, his/her data will be retained.

   When user re-runs the configuration, without toggling the Database authentication, then the user data will not be affected.

3. **Can the user change his details? Ex: E-mail, Password?**

   User can change his First name, Last name, Initials and Password. But the User cannot change his E-mail id, Username and the Role assigned.

4. **Can the user deploy Agent on other system who has logged in using database authentication?**

No. Agent deployment is possible only for Active Directory Users.

5. **Does the Database authenticated user need any folder or SQL server permission?**

   No. The user does not require any special permission.

6. **Who can set the logo customization image?**

   The ET Admin and MSP Admin can change their respective user’s logo. The User(s) is allowed to change his/her own logo.

7. **Is there any limit for MSP Admin to add users?**

   No.

8. **What if user forgets the password?**

   Forget password link is provided during login, user will receive the mail regarding it.

9. **What does Import of user mean?**

   Importing user with privilege and permission but we should assign it from the template.

10. **Who can remove MSP Admin?**

    EventTracker Admin and MSP Admin.

11. **Can MSP Admin remove another MSP Admin?**

    Yes, if both MSP Admin(s) have the common group permission.

12. **If MSP has been removed (or disabled) what about the users under that MSP?**

    The user(s) will be active and can access EventTracker.

13. **Can ETAdmin change the role of a MSP Admin to user or other?**

    Yes.

14. **Can ETAdmin change the Permission of MSP?**

    Yes.

15. **Can the MSP Admin and Admin change the password of user?**

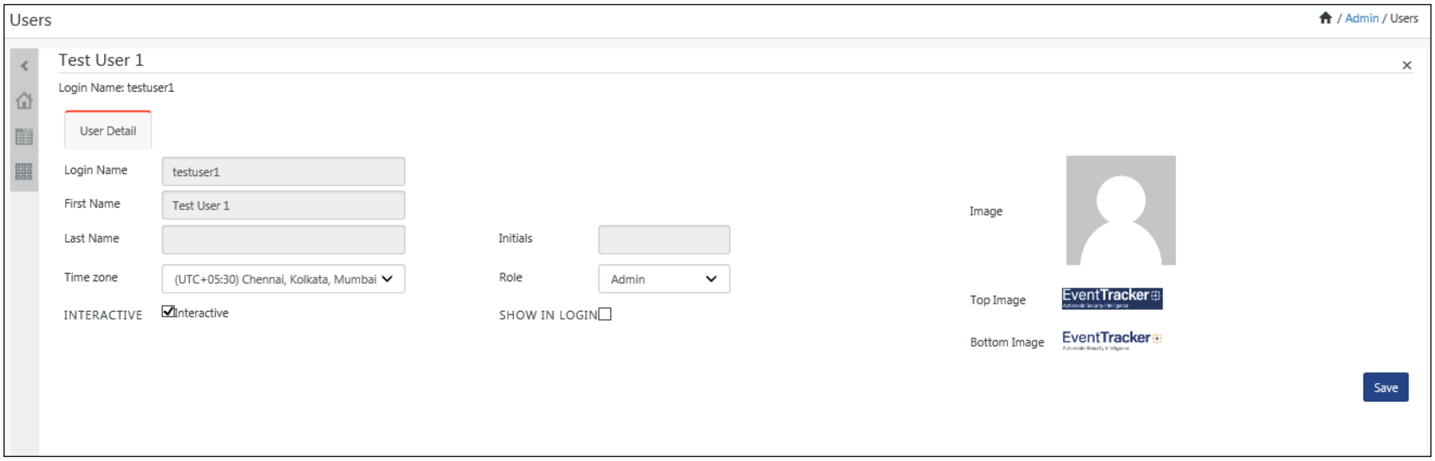
    No. Only the user can change his/her password from the user profile.

23.10 Logo Customization

We have provided an option to customize EventTracker logo based on user. You can add your company logo or any appropriate logo in EventTracker based on requirement.

> NOTE
>
> - The top left and bottom left images inside the EventTracker application should be per user setting.
> - If no image is assigned to a user then default EventTracker logo displays.
> - A library of images can be maintained by the user to be used for assigning logo.
> - The image mapping is available only to the admin user.
> - User can also delete an image uploaded to the library.

1. To customize EventTracker logo and other details, click **Edit** .



Users

/ Admin / Users

Test User 1

Login Name: testuser1

User Detail

Login Name: testuser1

First Name: Test User 1

Last Name:

Initials:

Time zone: (UTC+05:30) Chennai, Kolkata, Mumbai

Role: Admin

INTERACTIVE ☑Interactive

SHOW IN LOGIN□

Image

Top Image: EventTracker

Bottom Image: EventTracker

Figure 620

2. Click on the image and browse the customized logo.

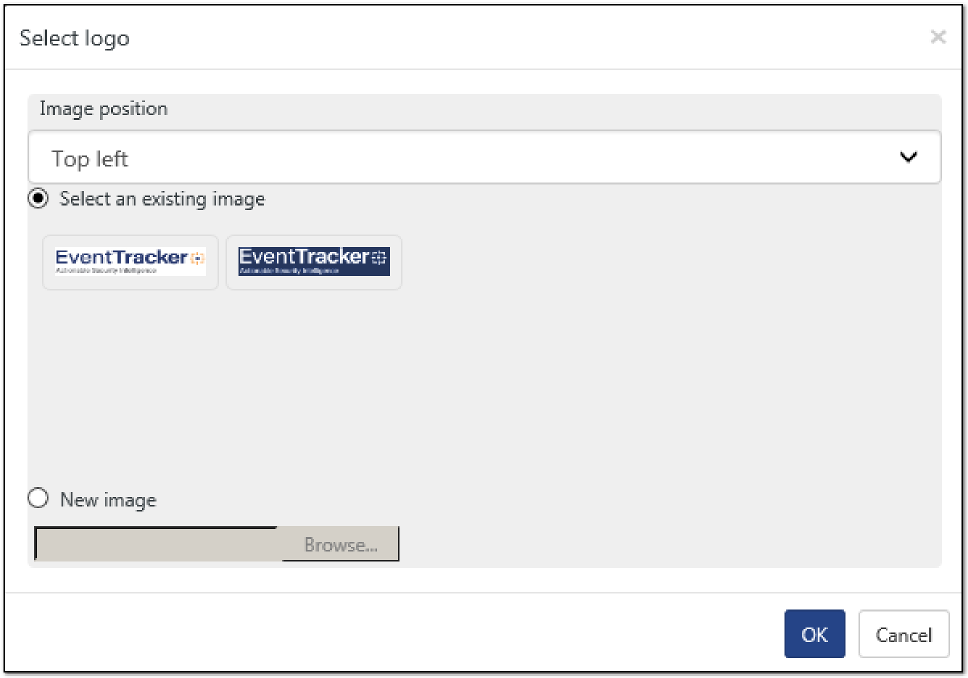

Select logo

Image position

Top left

● Select an existing image

○ New image

Figure 621

3. Select **Image position:** i.e. **Top Image** or **Bottom Image** or **Both**.
   If Both are selected, then the image/logo will be replaced in bottom and top position.
4. **Select an existing image** or **New image** option.
   In our example we will select a new image.
5. Click **Browse**.
6. Select an image present in local drive or network drive having a resolution of 106 x 30 px.
   The allowed image file formats are gif, jpeg, jpg and png.
7. Click **Save**.
   The respective logo displays.

23.10.1 Deleting logo

1. To delete the customized logo, select the logo icon L at the right-hand corner.
   Select logo window opens.
2. To delete, select the required logo.

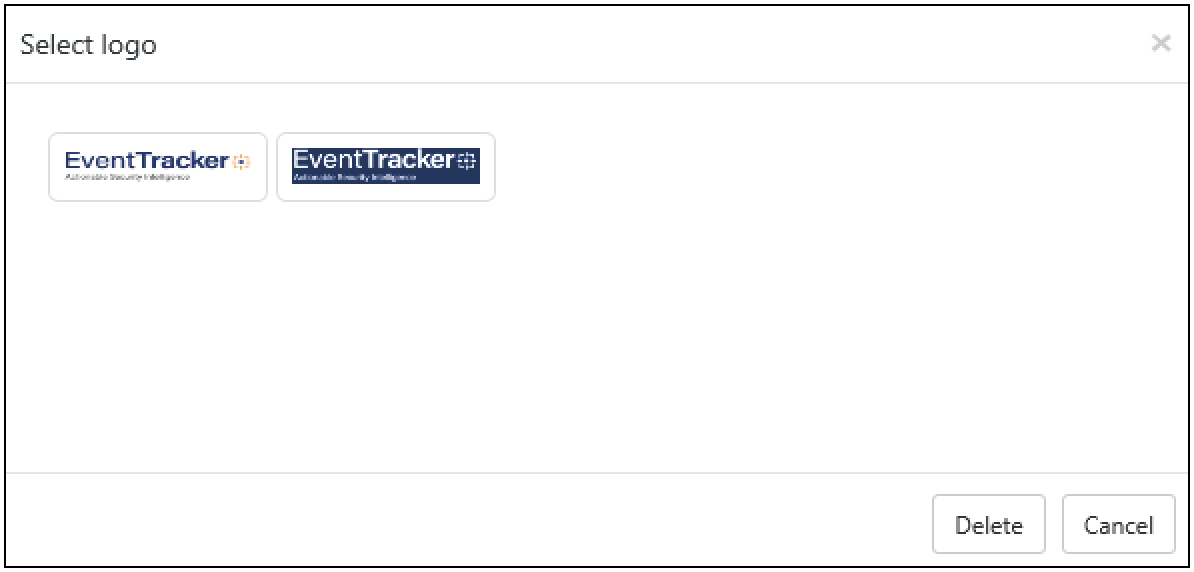


Figure 622

3. Select **Delete**.
   A message to confirm the deletion of logo opens.
4. Click **OK**.

23.11 Export icon

- To export data to excel, click **Export**.
  You can view the data in an excel file.

24. Tag Weights

In this chapter, you will learn how to:

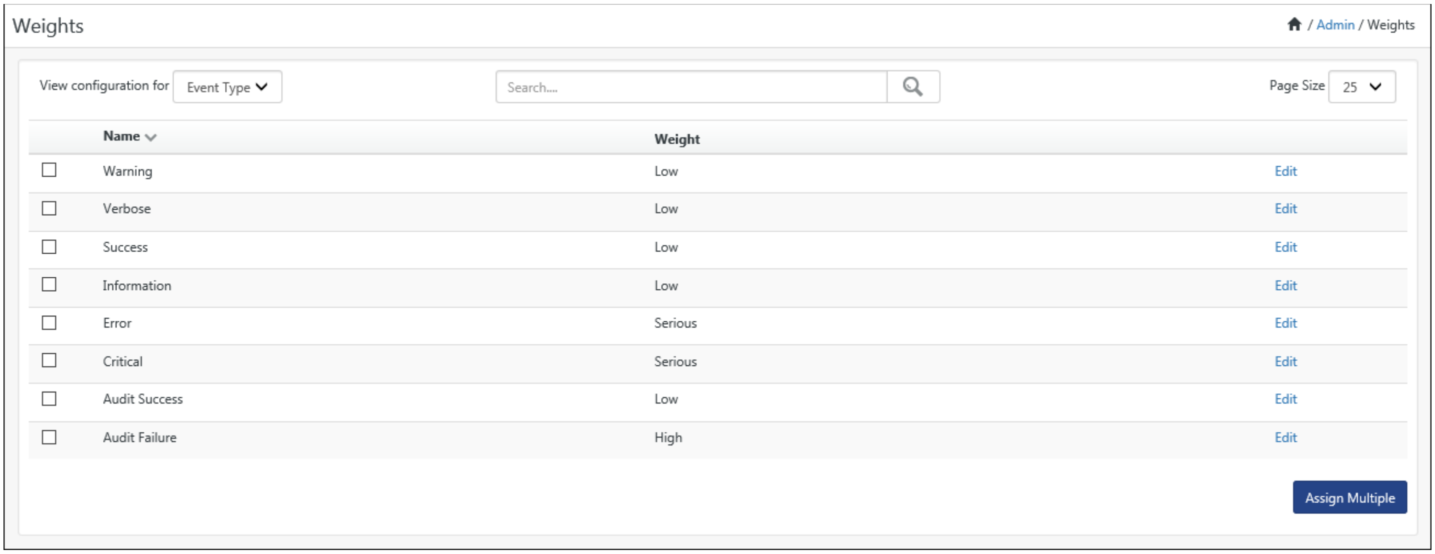
- Assigning Weights to Tags
- Adding Keywords as Tags

24.1 Assigning Weights to Tags

This option helps to assign weights to tags.

1 Log on to EventTracker. Click the **Admin**, and then click **Weights**.

EventTracker opens the **Weights** page.



Weights

🏠 / Admin / Weights

View configuration for: Event Type

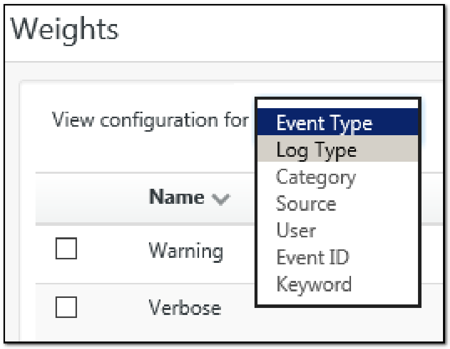
Search....

Page Size: 25

	Name	Weight	
□	Warning	Low	Edit
□	Verbose	Low	Edit
□	Success	Low	Edit
□	Information	Low	Edit
□	Error	Serious	Edit
□	Critical	Serious	Edit
□	Audit Success	Low	Edit
□	Audit Failure	High	Edit

Figure 623

2 Select an option from the **View configuration for** drop-down list.



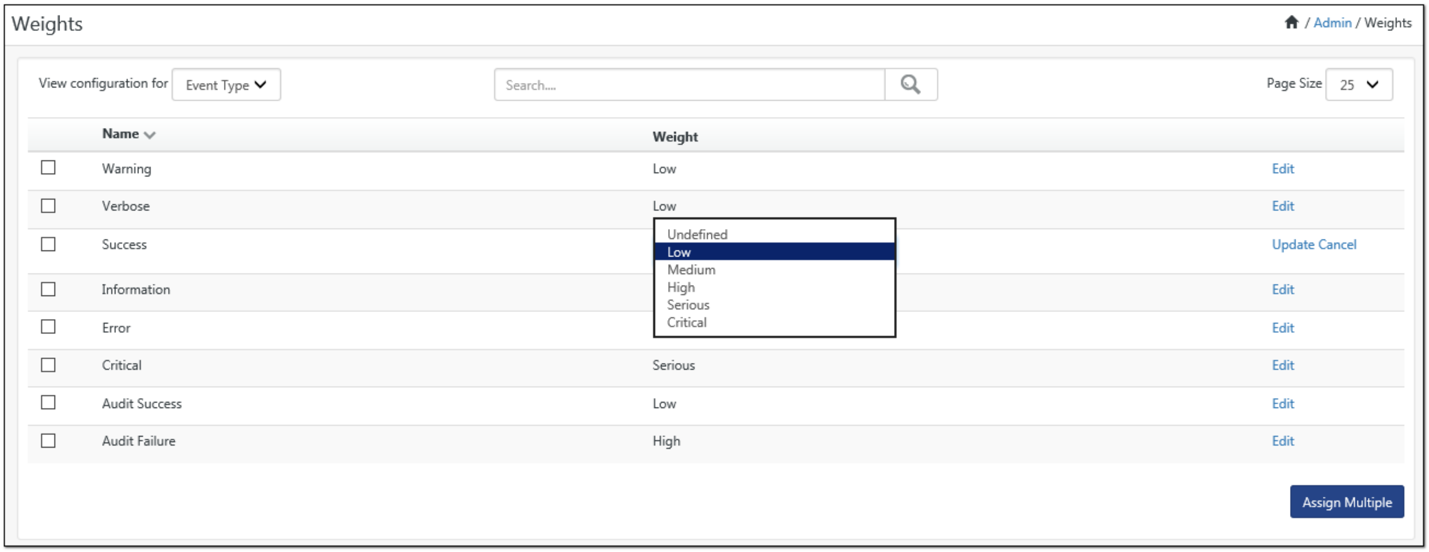
Weights

View configuration for

Figure 624

EventTracker opens the Weight configuration page with corresponding details.

3 Click **Edit** against the tag you wish to reassign the Weight.



Weights

/ Admin / Weights

View configuration for Event Type

Page Size 25

	Name	Weight	
□	Warning	Low	Edit
□	Verbose	Low	Edit
□	Success	Undefined Low Medium High Serious Critical	Update Cancel
□	Information		Edit
□	Error		Edit
□	Critical	Serious	Edit
□	Audit Success	Low	Edit
□	Audit Failure	High	Edit

Figure 625

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.

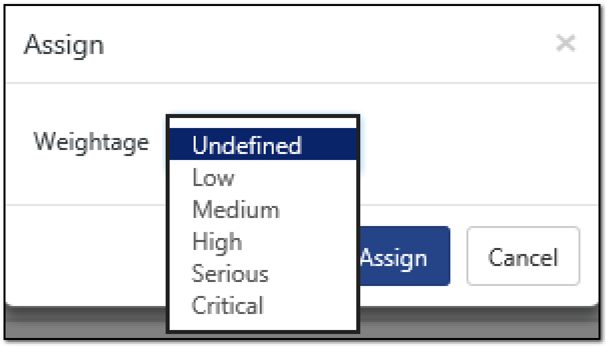
24.1.1 Assigning Weights to Multiple Tags

This option helps you assign weights to multiple tags.

1 Select the checkbox against the tags you want to assign weights and then click **Assign Multiple**.

EventTracker opens the **Assign** window.

2 Select the required option from the **Weightage** drop-down list and then click **Assign**.



Assign

Weightage: Undefined

Figure 626

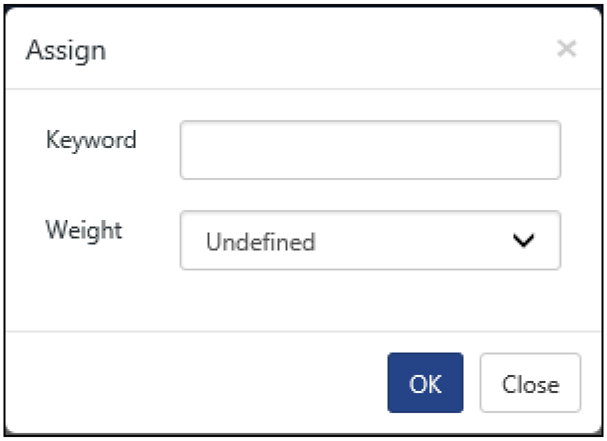
EventTracker assigns weights to the selected tags.

24.1.2 Adding 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 opens the **Add Keyword Weight pop-up** window.



Assign

Keyword:

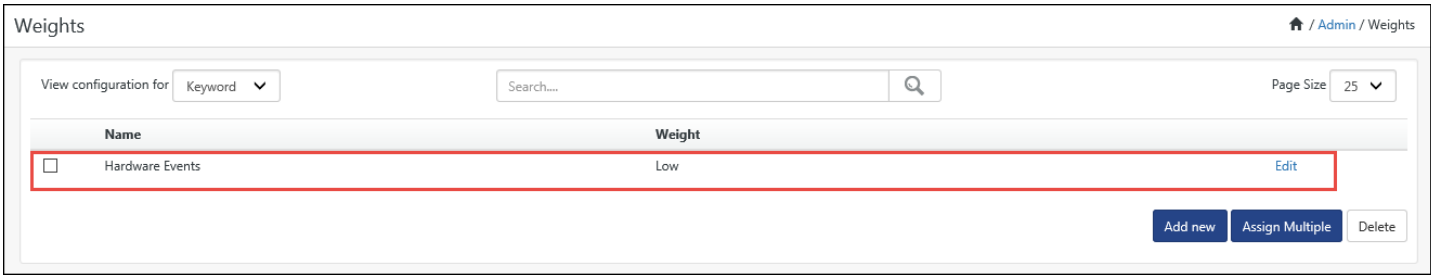
Weight: Undefined

Figure 627

2 Type keyword in the **Keyword** field.

Example: Hardware Events

3 Select an option from the **Weight** drop-down list, and then click **OK**.



Weights

View configuration for: Keyword

Page Size: 25

	Name	Weight	
□	Hardware Events	Low	Edit

Figure 628

25. Casebook

In this chapter, you will learn about:

- Usage of Casebook
- Creating new Casebook
- Adding to existing Casebook

25.1 About Casebook

Casebook is an electronic book in which users can add entries from Incidents, Reports, Change Audit, and prepare notes directly. A user can also auto date/sign entries.

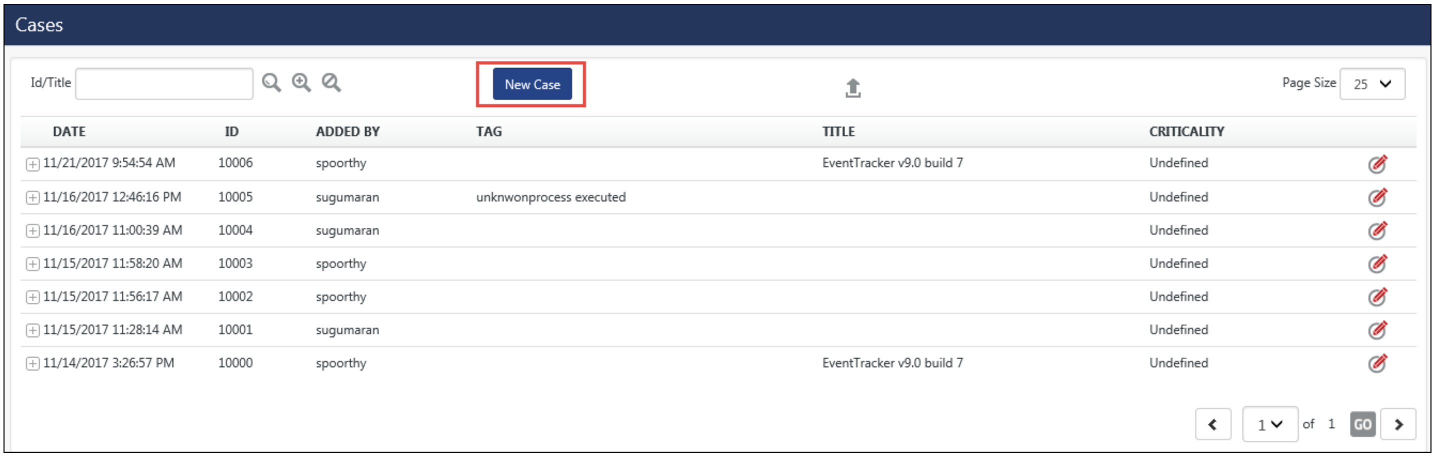
When doing quarterly review, we can take report to remind ourselves of the 'victories'. When we do log review of alerts and reports, we sometimes come across a low disk condition, an application crash, a SQL injection attempt etc. In order to notify users, a casebook is provided so that when a necessary incident/alert occurs, necessary precaution can be taken care of.

NOTE

The required license has to be purchased in order to use the Casebook feature.

25.2 Usage of Casebook

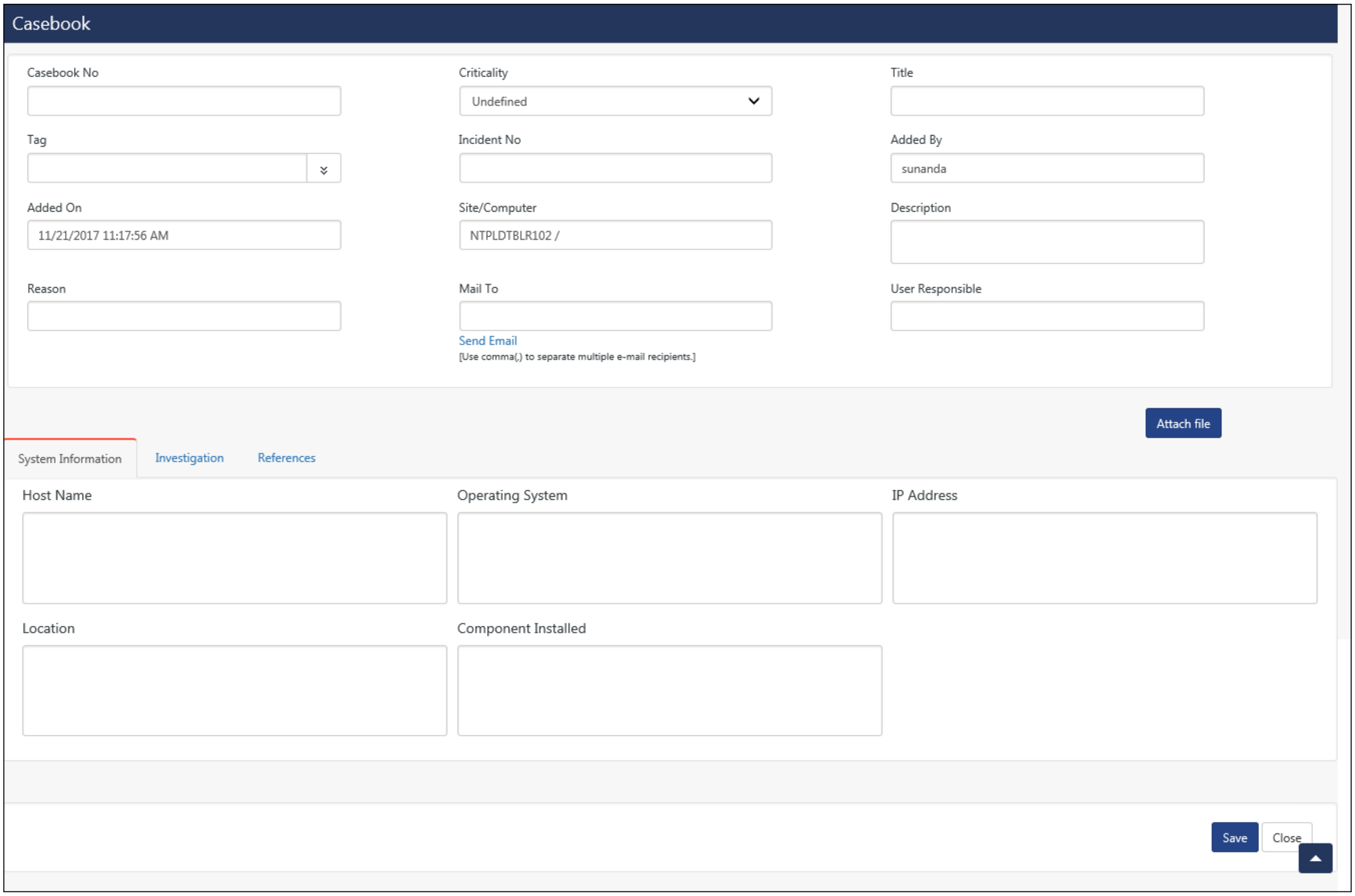
1. Log on to **EventTracker**.
2. Select the **Tools** drop-down, and then select **Casebook**.
   The Casebook displays only added entries.



DATE	ID	ADDED BY	TAG	TITLE	CRITICALITY
11/21/2017 9:54:54 AM	10006	spoorthy		EventTracker v9.0 build 7	Undefined
11/16/2017 12:46:16 PM	10005	sugumaran	unknwonprocess executed		Undefined
11/16/2017 11:00:39 AM	10004	sugumaran			Undefined
11/15/2017 11:58:20 AM	10003	spoorthy			Undefined
11/15/2017 11:56:17 AM	10002	spoorthy			Undefined
11/15/2017 11:28:14 AM	10001	sugumaran			Undefined
11/14/2017 3:26:57 PM	10000	spoorthy		EventTracker v9.0 build 7	Undefined

Figure 629

3. To add a new Casebook, click **New Case**.
   Casebook window opens.



Casebook

Casebook No:

Criticality: Undefined

Title:

Tag:

Incident No:

Added By: sunanda

Added On: 11/21/2017 11:17:56 AM

Site/Computer: NTPLDTBLR102 /

Description:

Reason:

Mail To:

Send Email

[Use comma(,) to separate multiple e-mail recipients.]

User Responsible:

Figure 630

4. Enter **Title** of the alert/report.
5. Select **Tag** from the drop-down.
6. Select priority level from **Criticality** drop-down.
7. Enter the valid Email address in **Mail to** 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.
12. To add a file, click **Attach file** link.

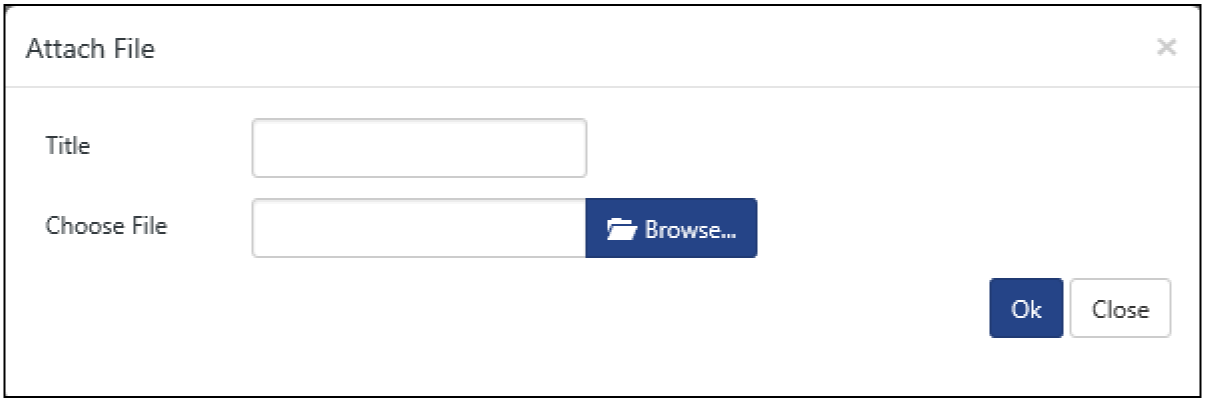
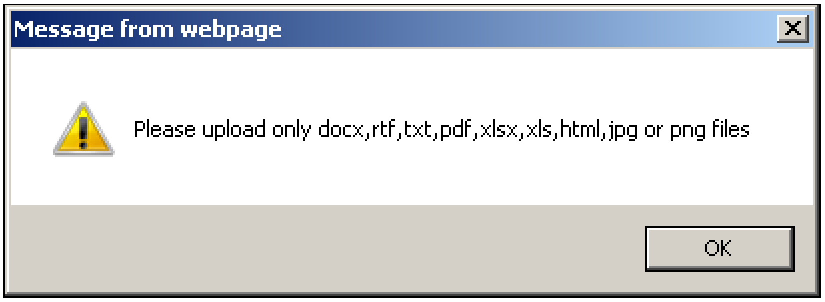


Figure 631

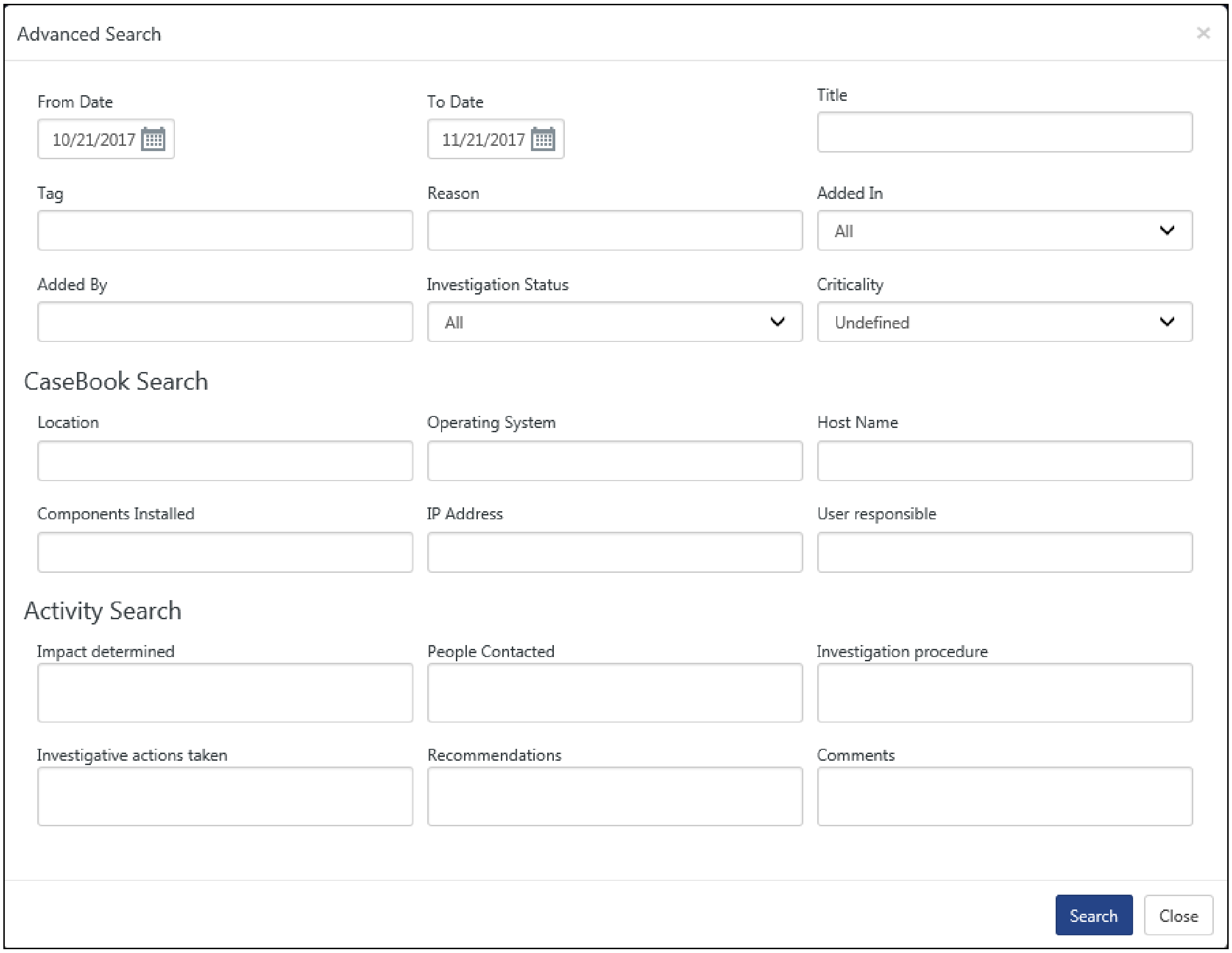
You can attach only Text, Word, Excel, PDF, RTF, HTML, JPEG, PNG files otherwise an error message opens.



Please upload only docx,rtf,txt,pdf,xlsx,xls,html,jpg or png files

Figure 632

13. Enter the required and mandatory information and then click **Save**.
14. To search Casebook information, click **Advanced Search** 🔍 .



Advanced Search

From Date 10/21/2017	To Date 11/21/2017	Title
Tag	Reason	Added In All
Added By	Investigation Status All	Criticality Undefined

CaseBook Search

Location	Operating System	Host Name
Components Installed	IP Address	User responsible

Activity Search

Impact determined	People Contacted	Investigation procedure
Investigative actions taken	Recommendations	Comments

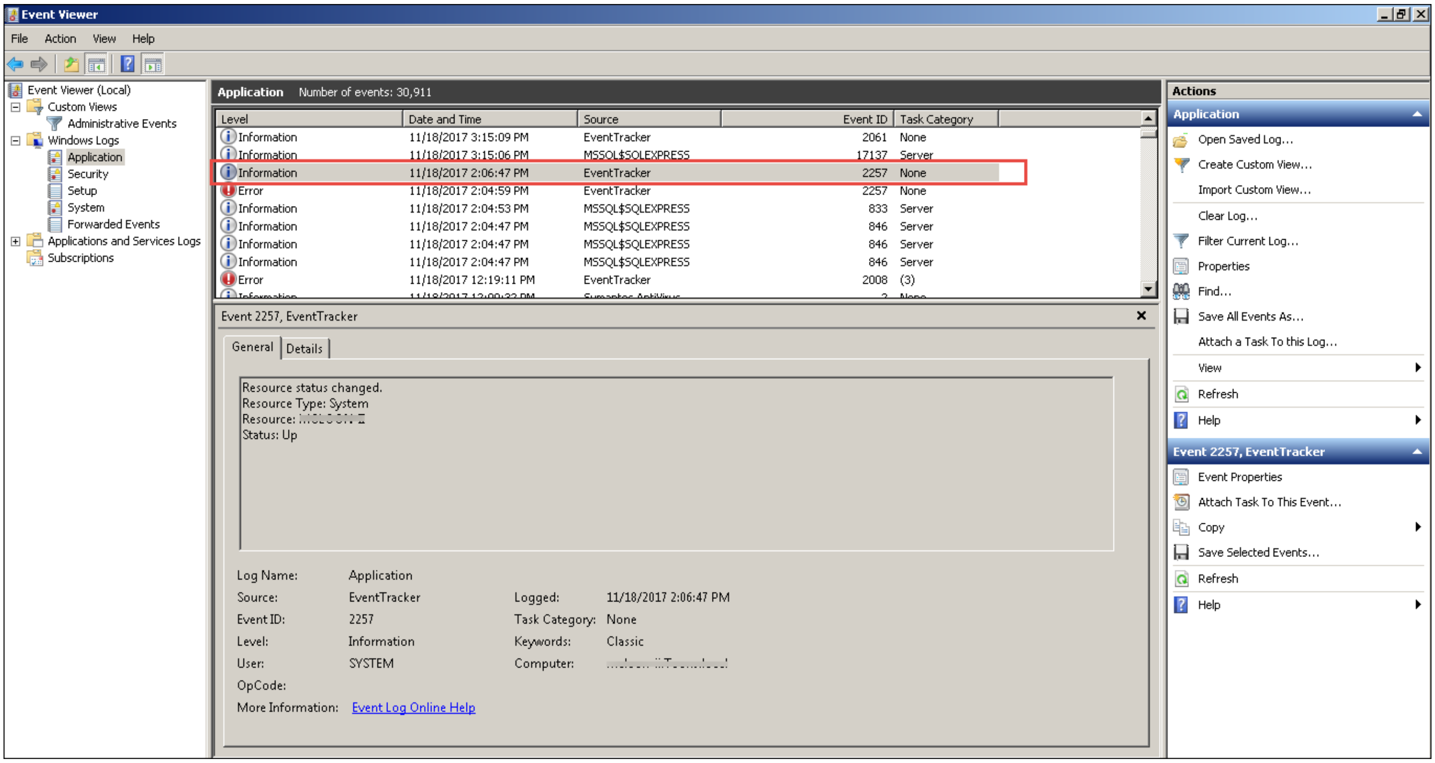
Figure 633

15. Enter the relevant search information, and then click **Search**.

NOTE

- A user has to add investigation information since it is mandatory.
- System Information provides information about a system.
- For a Casebook entry, there can be N number of activities.
- A user who adds the Casebook, only can edit Casebook 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 Casebook shows only added Casebook entry details and how to search the available Casebook entries.
- After adding the casebook, the user can edit Casebook completely where as other users can add only investigation details. Other users don’t have permission to delete an uploaded file and the references.

- If you want to view the actions that are recorded in Casebook such as an email has been sent or an added comment or references, you can go to the Windows Event Viewer and monitor the details as shown in the figure below.



Application Number of events: 30,911

Level	Date and Time	Source	Event ID	Task Category
Information	11/18/2017 3:15:09 PM	EventTracker	2061	None
Information	11/18/2017 3:15:06 PM	MSSQL$SQLEXPRESS	17137	Server
Information	11/18/2017 2:06:47 PM	EventTracker	2257	None
Error	11/18/2017 2:04:59 PM	EventTracker	2257	None
Information	11/18/2017 2:04:53 PM	MSSQL$SQLEXPRESS	833	Server
Information	11/18/2017 2:04:47 PM	MSSQL$SQLEXPRESS	846	Server
Information	11/18/2017 2:04:47 PM	MSSQL$SQLEXPRESS	846	Server
Information	11/18/2017 2:04:47 PM	MSSQL$SQLEXPRESS	846	Server
Error	11/18/2017 12:19:11 PM	EventTracker	2008	(3)
Information	11/18/2017 12:00:32 PM	Symantec AntiVirus	2	None

Event 2257, EventTracker

General | Details

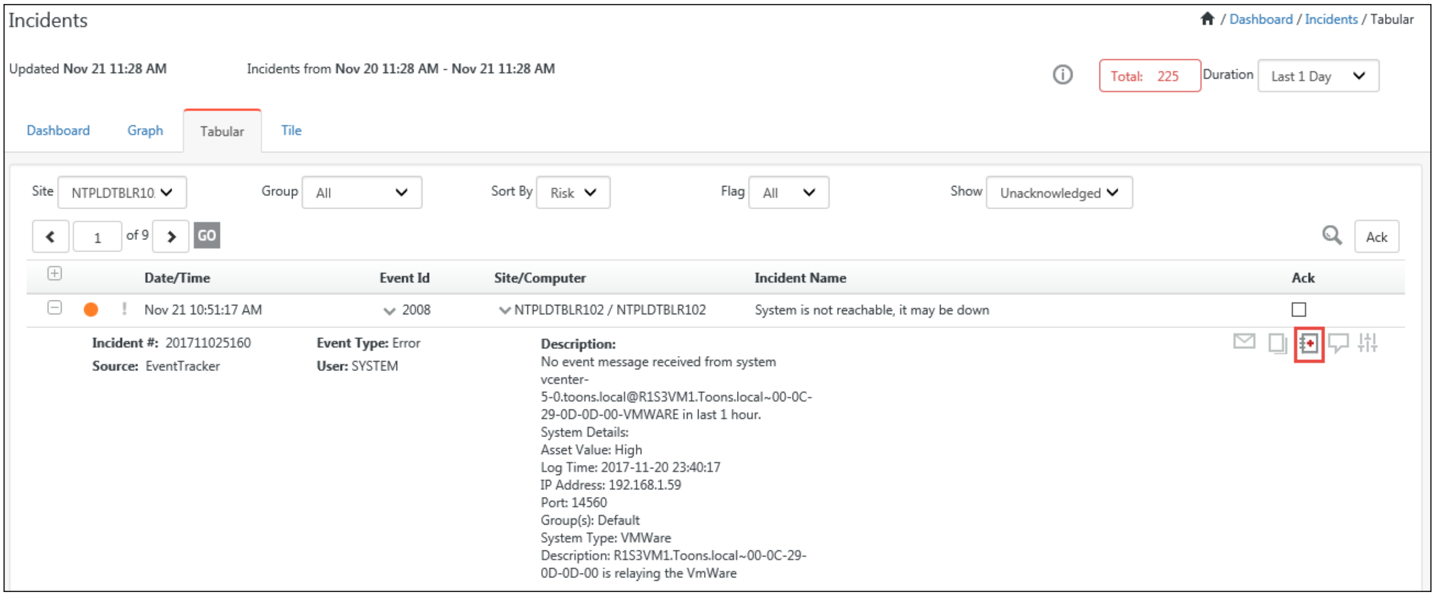
Resource status changed.
Resource Type: System
Resource: [redacted]
Status: Up

Log Name:	Application		
Source:	EventTracker	Logged:	11/18/2017 2:06:47 PM
Event ID:	2257	Task Category:	None
Level:	Information	Keywords:	Classic
User:	SYSTEM	Computer:	[redacted]
OpCode:			
More Information:	Event Log Online Help		

Figure 634

25.2.1 Creating a new Casebook

1. Select the **Incidents** option, and then select the **Tabular** tab.



Incidents

🏠 / Dashboard / Incidents / Tabular

Updated **Nov 21 11:28 AM** Incidents from **Nov 20 11:28 AM - Nov 21 11:28 AM**

Total: 225 Duration Last 1 Day

Site NTPLDTBLR10 Group All Sort By Risk Flag All Show Unacknowledged

			Date/Time	Event Id	Site/Computer	Incident Name	Ack
⊟	●	!	Nov 21 10:51:17 AM	2008	NTPLDTBLR102 / NTPLDTBLR102	System is not reachable, it may be down	□

Incident #: 201711025160
Source: EventTracker

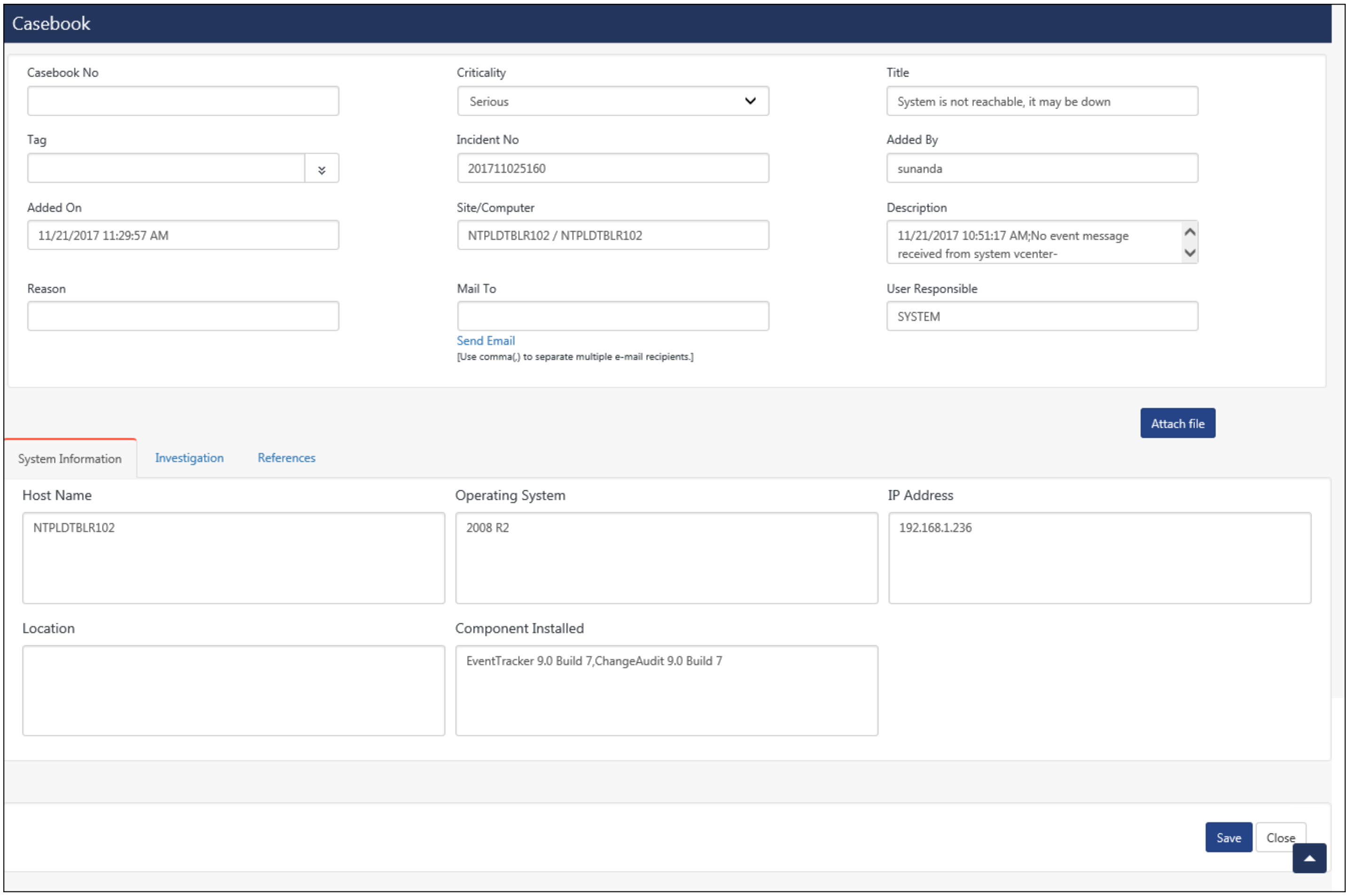
Event Type: Error
User: SYSTEM

Description:
No event message received from system
vcenter-
5-0.toons.local@R1S3VM1.Toons.local~00-0C-
29-0D-0D-00-VMWARE in last 1 hour.
System Details:
Asset Value: High
Log Time: 2017-11-20 23:40:17
IP Address: 192.168.1.59
Port: 14560
Group(s): Default
System Type: VMWare
Description: R1S3VM1.Toons.local~00-0C-29-
0D-0D-00 is relaying the VmWare

Figure 635

2. Select any incident and click the **Casebook** icon.
3. The Casebook window will ask you to either **Add new/ Add to existing**.
4. Select **Add new**.

   Casebook window opens.



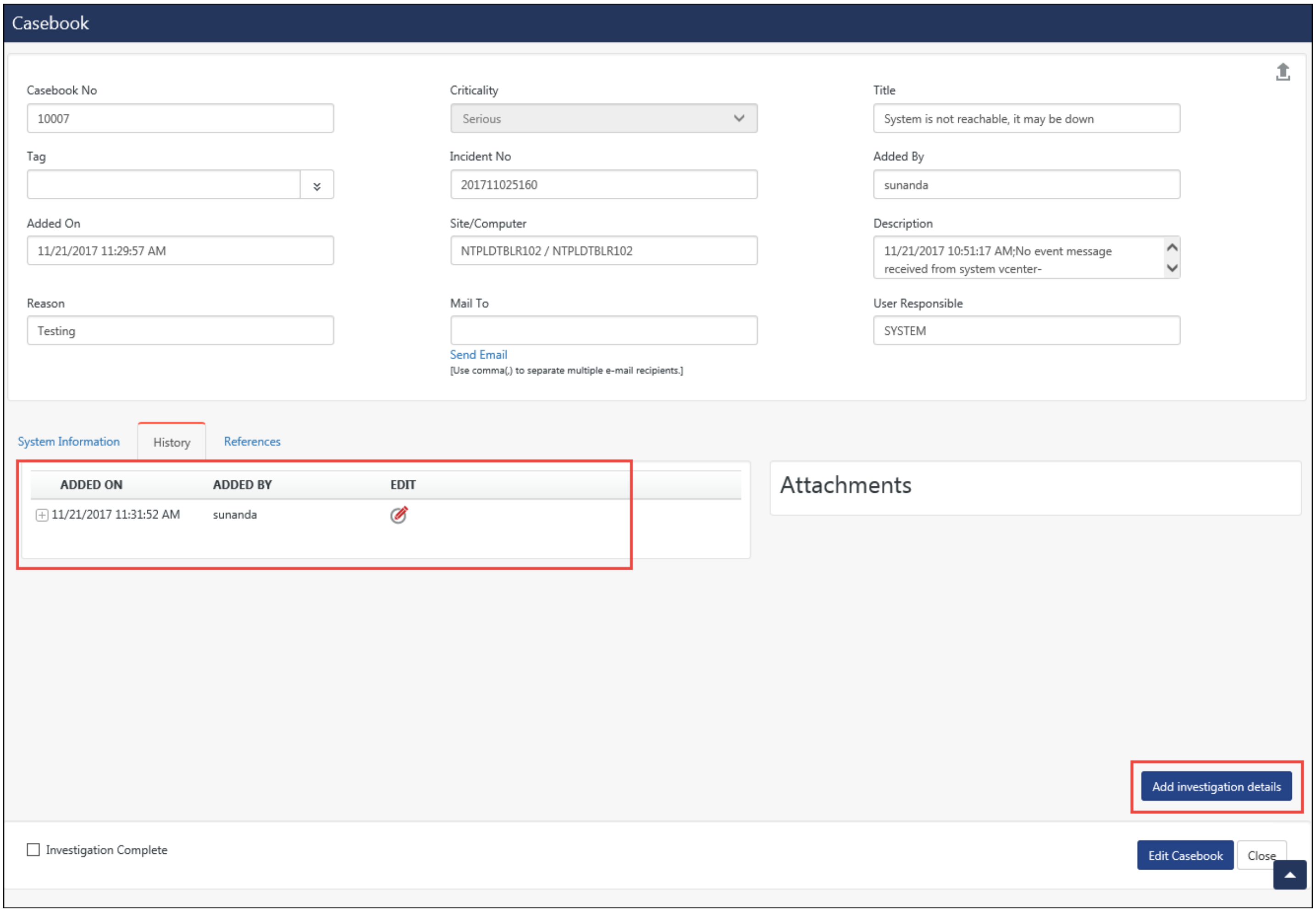
Casebook

Casebook No	Criticality	Title
	Serious	System is not reachable, it may be down
Tag	Incident No	Added By
	201711025160	sunanda
Added On	Site/Computer	Description
11/21/2017 11:29:57 AM	NTPLDTBLR102 / NTPLDTBLR102	11/21/2017 10:51:17 AM;No event message received from system vcenter-
Reason	Mail To	User Responsible
		SYSTEM

Host Name	Operating System	IP Address
NTPLDTBLR102	2008 R2	192.168.1.236
Location	Component Installed	
	EventTracker 9.0 Build 7,ChangeAudit 9.0 Build 7	

Figure 636

5. Enter the relevant information i.e. **Reason, Investigation** information**, Mail To** details etc.
6. If required, update the **Criticality** of the incident.
7. Click **Save**.



Casebook

Casebook No: 10007	Criticality: Serious	Title: System is not reachable, it may be down
Tag:	Incident No: 201711025160	Added By: sunanda
Added On: 11/21/2017 11:29:57 AM	Site/Computer: NTPLDTBLR102 / NTPLDTBLR102	Description: 11/21/2017 10:51:17 AM;No event message received from system vcenter-
Reason: Testing	Mail To:	User Responsible: SYSTEM

Send Email
[Use comma(,) to separate multiple e-mail recipients.]

ADDED ON	ADDED BY	EDIT
11/21/2017 11:31:52 AM	sunanda	

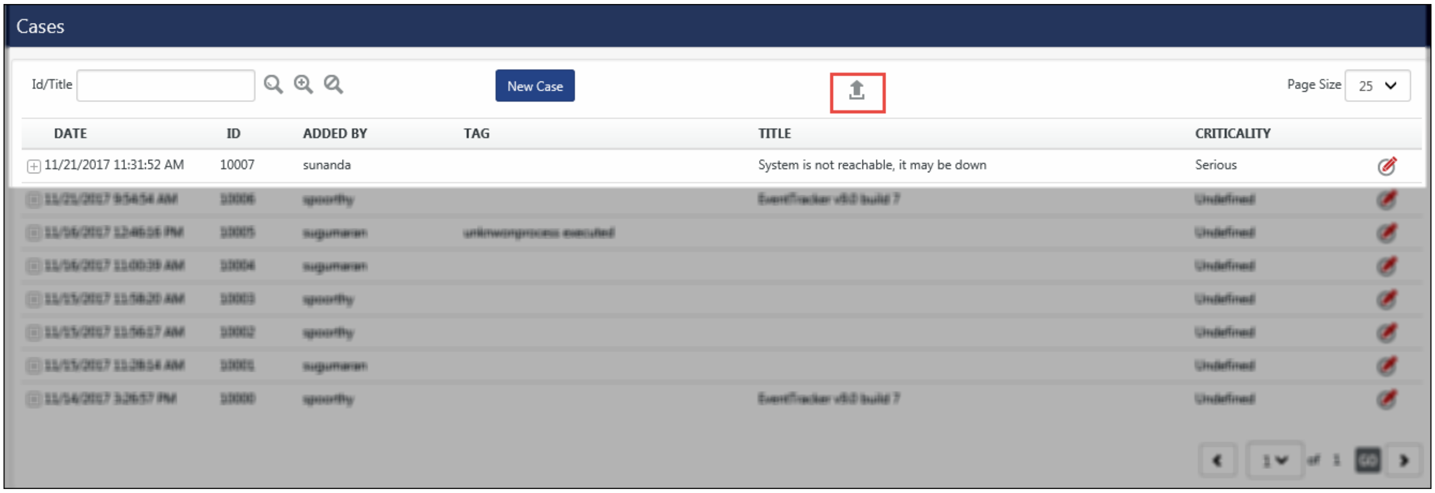
Figure 637

8. To view details of this Incident, click the **History** tab.
9. To add data to the existing Casebook, click **Edit Casebook**.
10. To add more investigation details, click **Add investigation details**.
11. Once the issue is resolved, click the **Investigation Complete** option and then click **Close**.

NOTE

To reopen an issue, click the Investigation Complete option once again. This privilege is available for an administrator only. User does not have the option to edit Casebook after the existing Casebook has been marked as ‘Investigation Complete’.

12. To view details, select the **Tools** menu and then select **Casebook**.



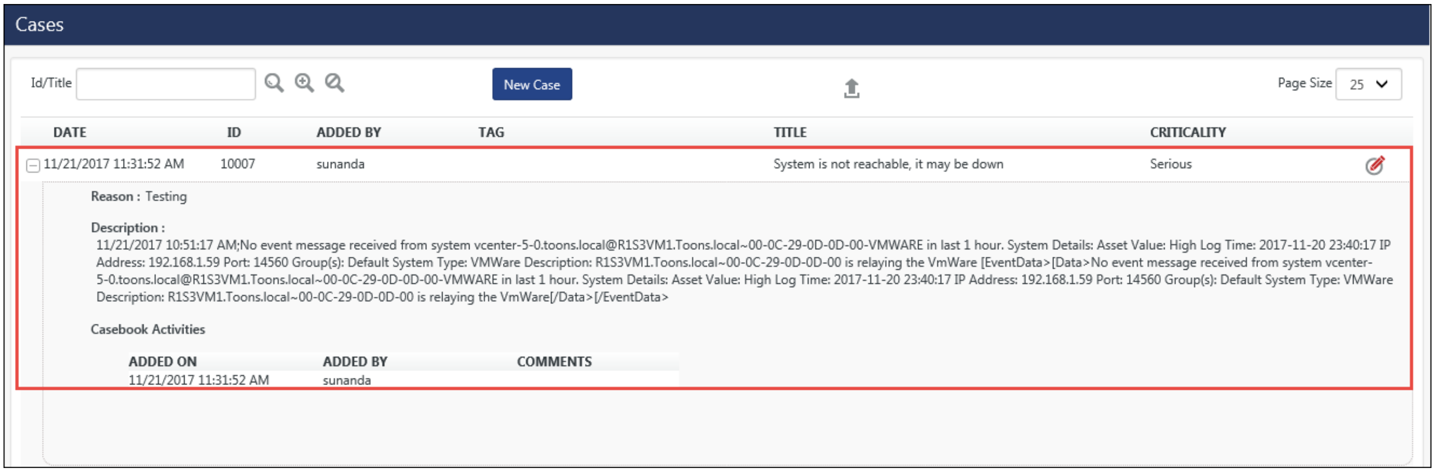
DATE	ID	ADDED BY	TAG	TITLE	CRITICALITY
11/21/2017 11:31:52 AM	10007	sunanda		System is not reachable, it may be down	Serious
11/21/2017 9:54:54 AM	10006	spoorthy		EventTracker v9.0 build 7	Undefined
11/16/2017 12:46:16 PM	10005	sugumaran	unknownprocess executed		Undefined
11/16/2017 11:00:39 AM	10004	sugumaran			Undefined
11/15/2017 11:58:20 AM	10003	spoorthy			Undefined
11/15/2017 11:56:17 AM	10002	spoorthy			Undefined
11/15/2017 11:28:54 AM	10001	sugumaran			Undefined
11/14/2017 3:26:57 PM	10000	spoorthy		EventTracker v9.0 build 7	Undefined

Figure 638

13. To export the search results to Excel file, click the **Export** icon.

25.2.2 Adding data to an existing Casebook

Let us consider an example where a Casebook has already been created as shown in the figure below.



DATE	ID	ADDED BY	TAG	TITLE	CRITICALITY
11/21/2017 11:31:52 AM	10007	sunanda		System is not reachable, it may be down	Serious

Reason : Testing

Description :
11/21/2017 10:51:17 AM;No event message received from system vcenter-5-0.toons.local@R1S3VM1.Toons.local~00-0C-29-0D-0D-00-VMWARE in last 1 hour. System Details: Asset Value: High Log Time: 2017-11-20 23:40:17 IP Address: 192.168.1.59 Port: 14560 Group(s): Default System Type: VMWare Description: R1S3VM1.Toons.local~00-0C-29-0D-0D-00 is relaying the VmWare [EventData>[Data>No event message received from system vcenter-5-0.toons.local@R1S3VM1.Toons.local~00-0C-29-0D-0D-00-VMWARE in last 1 hour. System Details: Asset Value: High Log Time: 2017-11-20 23:40:17 IP Address: 192.168.1.59 Port: 14560 Group(s): Default System Type: VMWare Description: R1S3VM1.Toons.local~00-0C-29-0D-0D-00 is relaying the VmWare[/Data>[/EventData>

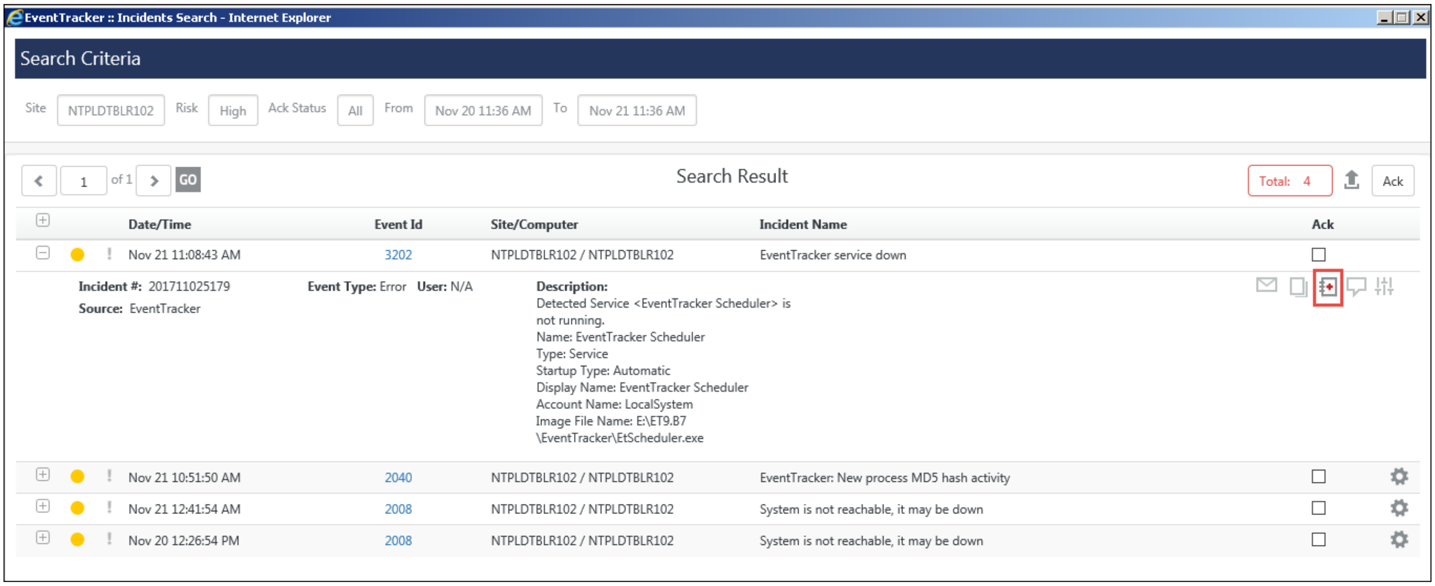
Casebook Activities

ADDED ON	ADDED BY	COMMENTS
11/21/2017 11:31:52 AM	sunanda	

Figure 639

To add information to the existing Casebook from Incidents Dashboard, please follow the steps given below.

a. Logon to EventTracker.
   Select Dashboard from the dropdown list in Incident.
b. Click the relevant incident (graph) available in **Incidents Dashboard**.
   Search Criteria window opens.



Site NTPLDTBLR102 Risk High Ack Status All From Nov 20 11:36 AM To Nov 21 11:36 AM

1 of 1 Search Result Total: 4

			Date/Time	Event Id	Site/Computer	Incident Name	Ack
⊟	●	!	Nov 21 11:08:43 AM	3202	NTPLDTBLR102 / NTPLDTBLR102	EventTracker service down	□

Incident #: 201711025179 **Event Type:** Error **User:** N/A
Source: EventTracker

Description:
Detected Service <EventTracker Scheduler> is not running.
Name: EventTracker Scheduler
Type: Service
Startup Type: Automatic
Display Name: EventTracker Scheduler
Account Name: LocalSystem
Image File Name: E:\ET9.B7\EventTracker\EtScheduler.exe

			Date/Time	Event Id	Site/Computer	Incident Name	Ack
⊞	●	!	Nov 21 10:51:50 AM	2040	NTPLDTBLR102 / NTPLDTBLR102	EventTracker: New process MD5 hash activity	□
⊞	●	!	Nov 21 12:41:54 AM	2008	NTPLDTBLR102 / NTPLDTBLR102	System is not reachable, it may be down	□
⊞	●	!	Nov 20 12:26:54 PM	2008	NTPLDTBLR102 / NTPLDTBLR102	System is not reachable, it may be down	□

Figure 640

c. Select an incident and click ⊞ icon.
Casebook window opens.

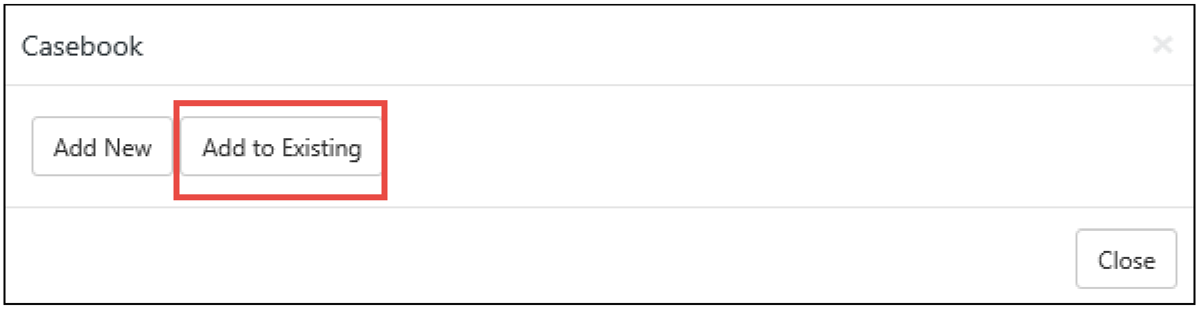
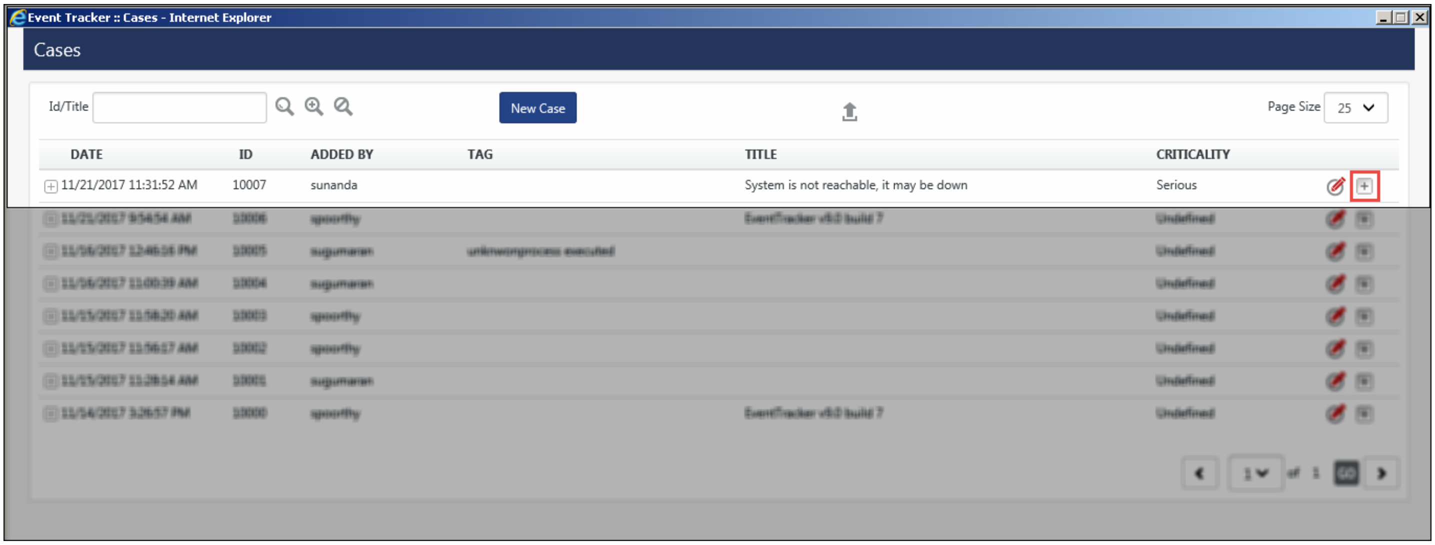


Figure 641

d. Select **Add to existing**.
Details of Casebook entries opens.



DATE	ID	ADDED BY	TAG	TITLE	CRITICALITY
11/21/2017 11:31:52 AM	10007	sunanda		System is not reachable, it may be down	Serious
11/21/2017 9:54:54 AM	10006	spoorthy		EventTracker v9.0 build 7	Undefined
11/16/2017 12:46:16 PM	10005	sugumaran	unknownprocess executed		Undefined
11/16/2017 11:00:39 AM	10004	sugumaran			Undefined
11/15/2017 11:58:20 AM	10003	spoorthy			Undefined
11/15/2017 11:56:17 AM	10002	spoorthy			Undefined
11/15/2017 11:28:14 AM	10001	sugumaran			Undefined
11/14/2017 3:26:57 PM	10000	spoorthy		EventTracker v9.0 build 7	Undefined

Figure 642

e. Click **Add to Casebook** ⊞ icon.
A successful message opens.

f. Click **OK**.

g. To view the existing entries, select the **Tools** menu, and then select **Casebook**.

h. Select **Edit** of respective Casebook entry, and then select the **References** tab.
The incident that has been added to the existing Casebook opens.

i. To export the Casebook in excel format, click the icon ⇪.

NOTE

You can also add data to an existing Casebook from Reports Dashboard and Change Audit accordingly.

26. Event Config

In this chapter, you will learn about:

- Event Config

26.1 Event Config

This feature has been provided to enable/disable events generated in Change Audit and Direct Log Archiver.

1. Login to EventTracker.
2. Select the **Tools** menu, and then select **Event Config**.

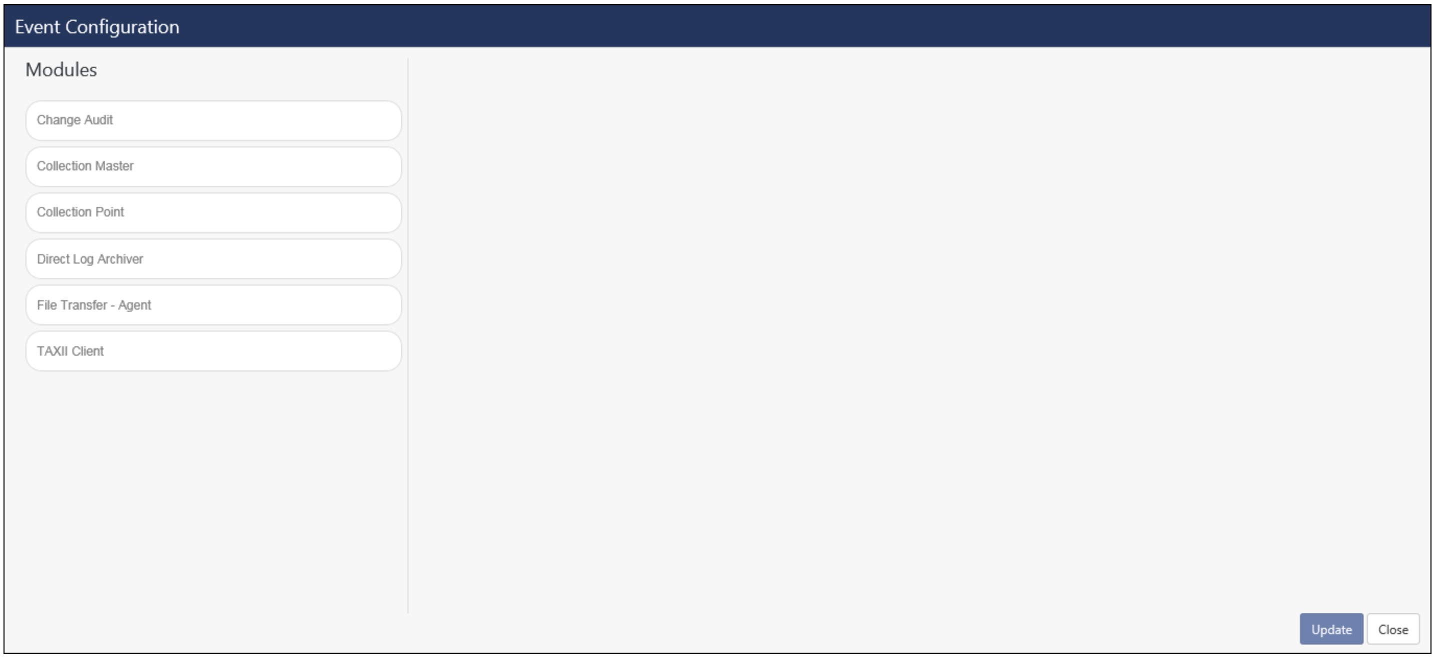
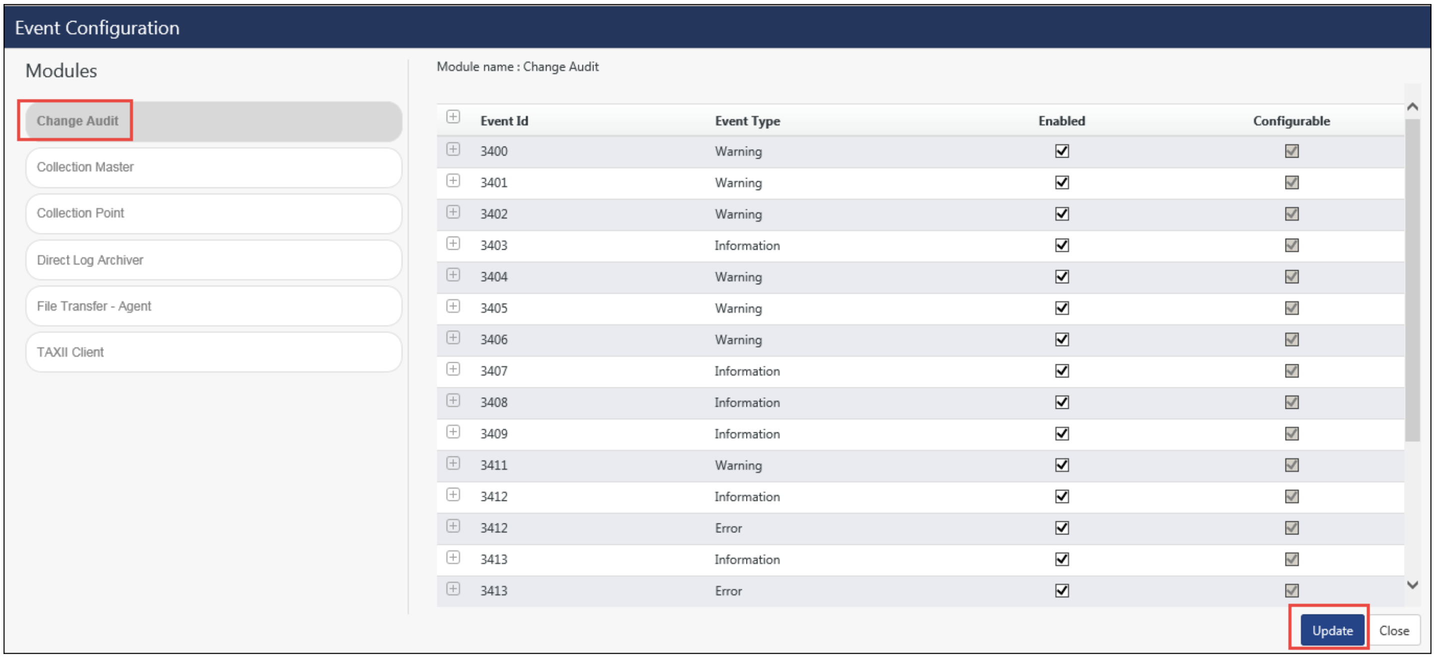


Figure 643

3. Click **Change Audit** in the Module pane.
4. For additional information regarding the **Event ID**, click ⊞ icon.
5. To enable/disable the respective Event Id's, select **Enabled** option, if not selected.



Event Configuration

Modules

- Change Audit
- Collection Master
- Collection Point
- Direct Log Archiver
- File Transfer - Agent
- TAXII Client

Module name : Change Audit

Event Id	Event Type	Enabled	Configurable
3400	Warning	☑	☑
3401	Warning	☑	☑
3402	Warning	☑	☑
3403	Information	☑	☑
3404	Warning	☑	☑
3405	Warning	☑	☑
3406	Warning	☑	☑
3407	Information	☑	☑
3408	Information	☑	☑
3409	Information	☑	☑
3411	Warning	☑	☑
3412	Information	☑	☑
3412	Error	☑	☑
3413	Information	☑	☑
3413	Error	☑	☑

Figure 644

6. Select **Update**.

27. Knowledge Base

In this chapter, you will learn how to:

- Accessing Knowledge Base

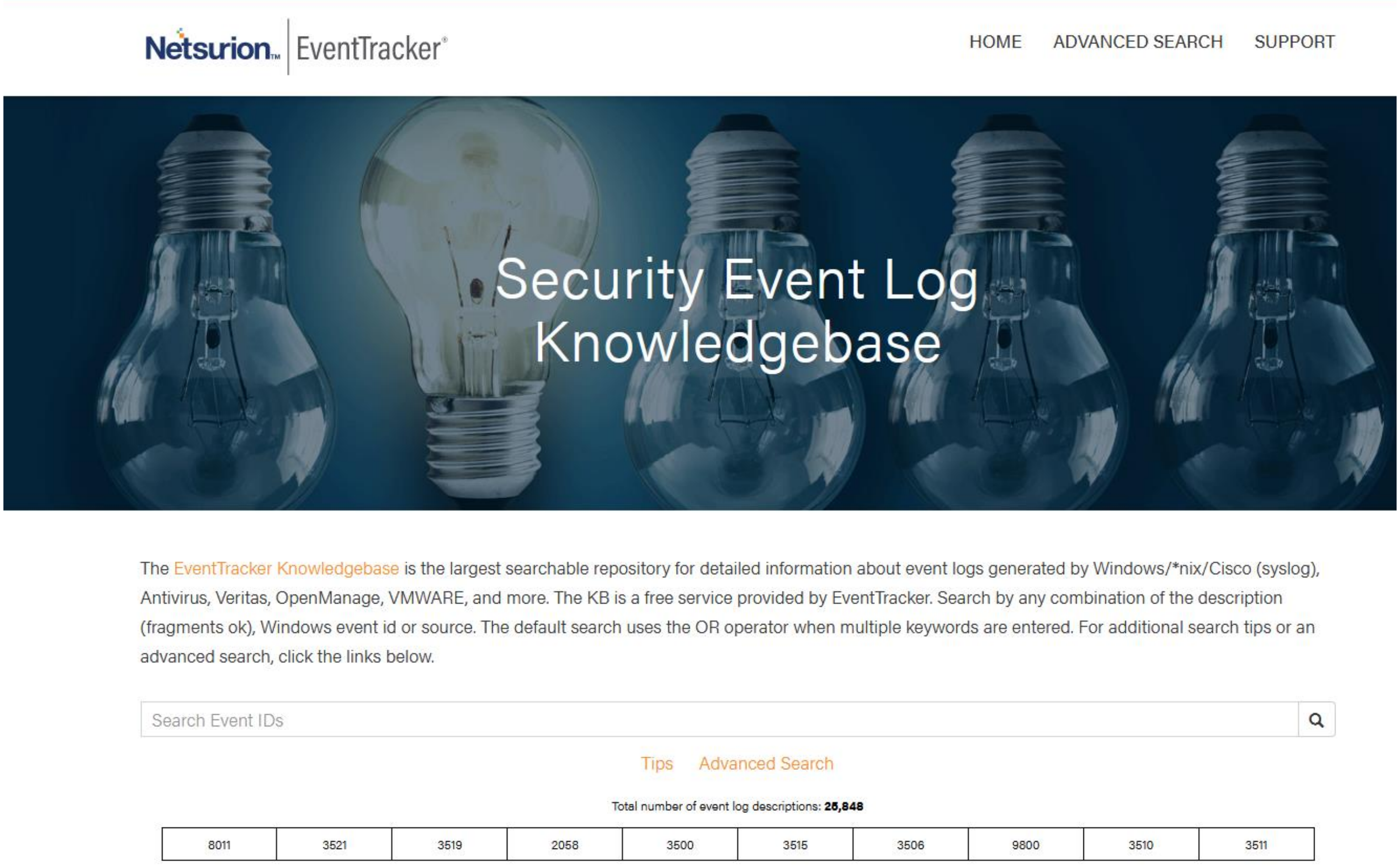
27.1 Knowledge Base

It is a web site containing information about Windows events and custom EventTracker events. Users can search for log-related information in 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.

27.1.1 Accessing Knowledge Base

1 Log on to EventTracker, click **Tools** and then click **Knowledge Base**.

EventTracker redirects to EventTracker Knowledge Base Web site http://kb.eventtracker.com/.



The EventTracker Knowledgebase is the largest searchable repository for detailed information about event logs generated by Windows/*nix/Cisco (syslog), Antivirus, Veritas, OpenManage, VMWARE, and more. The KB is a free service provided by EventTracker. Search by any combination of the description (fragments ok), Windows event id or source. The default search uses the OR operator when multiple keywords are entered. For additional search tips or an advanced search, click the links below.

Total number of event log descriptions: **25,848**

8011	3521	3519	2058	3500	3515	3506	9800	3510	3511

Figure 645

28. Scheduled Scripts

In this chapter, you will learn how to:

- Running Scheduled Scripts
- Verifying Scheduled Scripts
- Creating DLA to generate reports

28.1 Scheduled Scripts

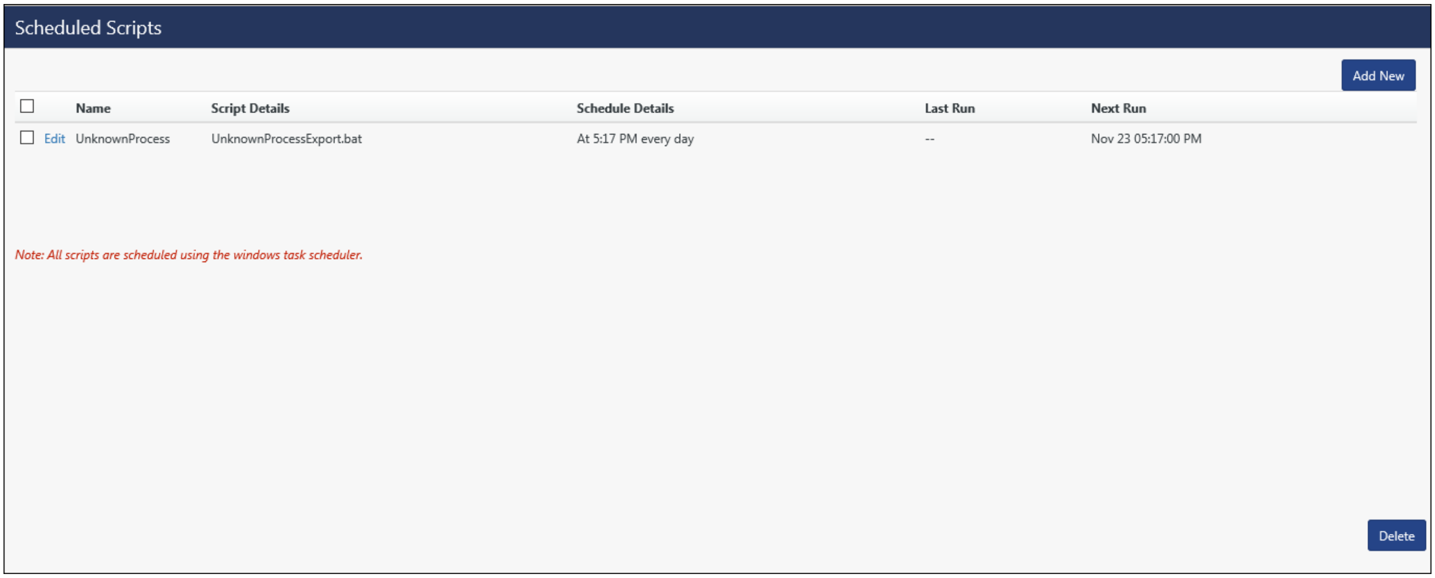
Certain scripts have been added in EventTracker which will run through Windows Task Scheduler. The scripts can be run from Active Directory (AD) data, based on LDAP (Lightweight Directory Access Protocol) query and the output is transferred to excel.

NOTE

- Only administrators having access to Active Directory can run the AD scripts available.
- User cannot edit task name as the reference in the task scheduler is with task name.
- Users can also add their own scripts (like batch file, shell script) apart from the VB Scripts that are already available
- The user should enable "Show file extension" in Windows File Explorer. This will help to download the blacklisted IPs to Active Watch List.

1. Logon to EventTracker.
2. Select the **Tools** menu, and then select **Scheduled Scripts.**

   EventTracker: Scheduled Scripts window opens.



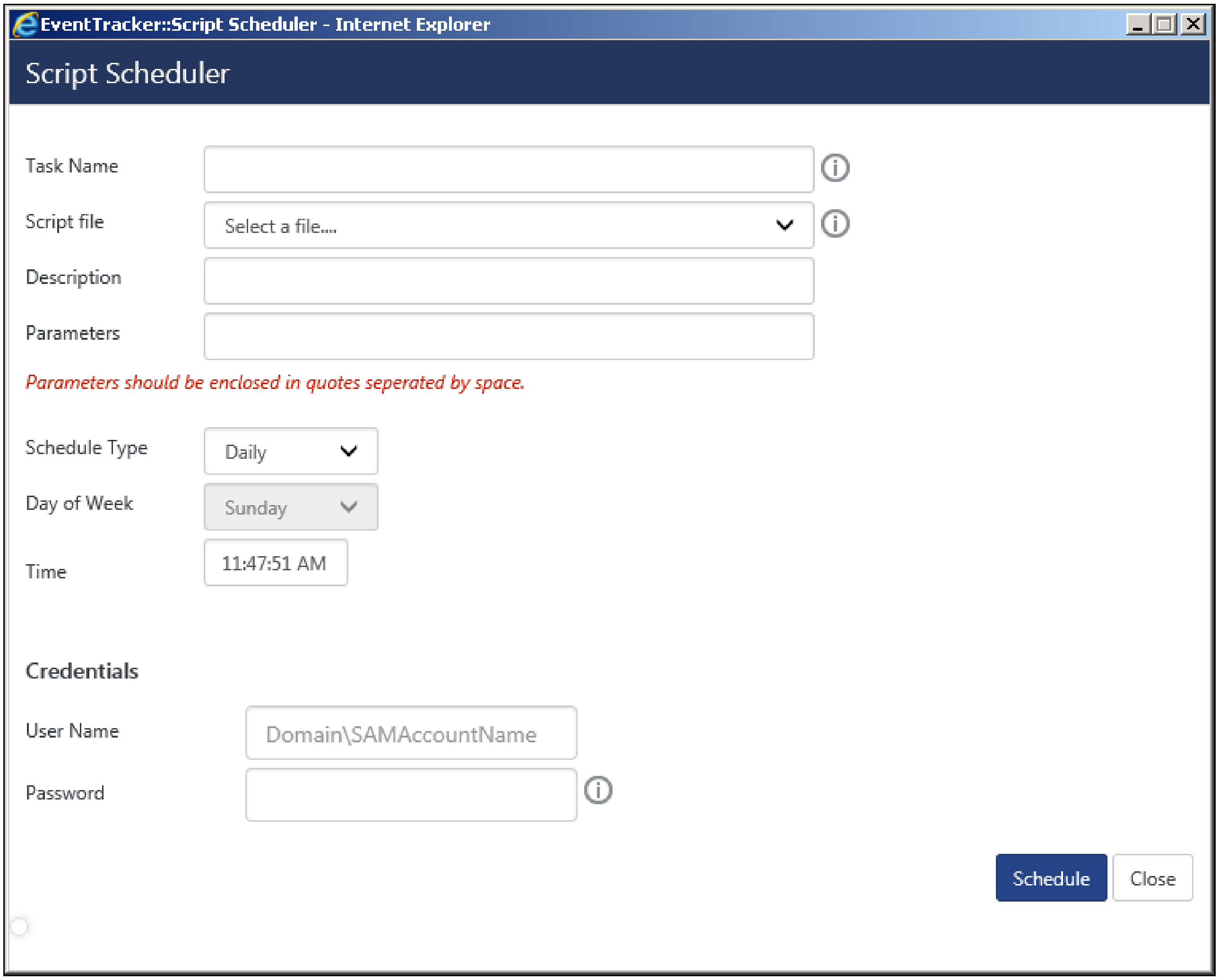
□	Name	Script Details	Schedule Details	Last Run	Next Run
□ Edit	UnknownProcess	UnknownProcessExport.bat	At 5:17 PM every day	--	Nov 23 05:17:00 PM

Note: All scripts are scheduled using the windows task scheduler.

Figure 646

3. Click **Add New**.

   Script scheduler window opens.



Script Scheduler

Task Name

Script file: Select a file....

Description

Parameters

Parameters should be enclosed in quotes seperated by space.

Schedule Type: Daily

Day of Week: Sunday

Time: 11:47:51 AM

Credentials

User Name: Domain\SAMAccountName

Password

Figure 647

4. Enter the required fields i.e. **Task Name, Script file, Description, Parameters, Schedule Type** and **Credentials**.

   Ex:

   - Task Name: Events
   - Script file: AD-Domain Computers.vbs
   - Parameters: It can be any value that has to be passed in the script and should be placed within double quotes. Ex: ”10”
   - User Name: domain\SAMAccountName. The script runs using these credentials. User should be a domain user.

NOTE

User should have the permission to launch Active Directory queries.

5. Click **Schedule**.

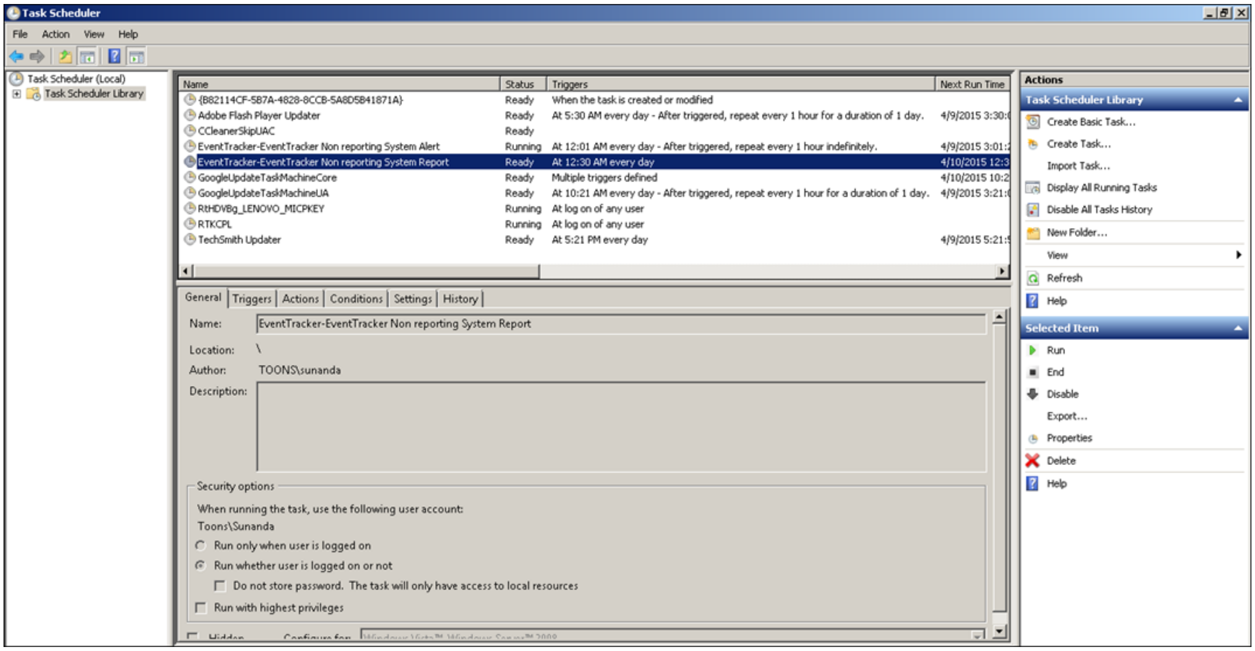
   It schedules the script. Your new task has been created and will run at the user specified time.

28.1.1 Verifying Scheduled Script

To verify the scheduled script, access Task Scheduler.

1. Click **Start -> Control Panel ->Administrative Tools**.
2. Select **Task Scheduler**, and then select **Task Scheduler Library**.
3. Click **'Refresh'** and scroll the list to see your new task.

   It shows in task scheduler library, for example here 'EventTracker-EventTracker Non reporting System Report' task has been created.



Name	Status	Triggers	Next Run Time
{B82114CF-5B7A-4828-8CCB-5A8D5B41871A}	Ready	When the task is created or modified	
Adobe Flash Player Updater	Ready	At 5:30 AM every day - After triggered, repeat every 1 hour for a duration of 1 day.	4/9/2015 3:30:(
CCleanerSkipUAC	Ready		
EventTracker-EventTracker Non reporting System Alert	Running	At 12:01 AM every day - After triggered, repeat every 1 hour indefinitely.	4/9/2015 3:01:2
EventTracker-EventTracker Non reporting System Report	Ready	At 12:30 AM every day	4/10/2015 12:3
GoogleUpdateTaskMachineCore	Ready	Multiple triggers defined	4/10/2015 10:2
GoogleUpdateTaskMachineUA	Ready	At 10:21 AM every day - After triggered, repeat every 1 hour for a duration of 1 day.	4/9/2015 3:21:(
RtHDVBg_LENOVO_MICPKEY	Running	At log on of any user	
RTKCPL	Running	At log on of any user	
TechSmith Updater	Ready	At 5:21 PM every day	4/9/2015 5:21:5

Name: EventTracker-EventTracker Non reporting System Report

Location: \

Author: TOONS\sunanda

Description:

Security options

When running the task, use the following user account:

Toons\Sunanda

○ Run only when user is logged on

● Run whether user is logged on or not

□ Do not store password. The task will only have access to local resources

□ Run with highest privileges

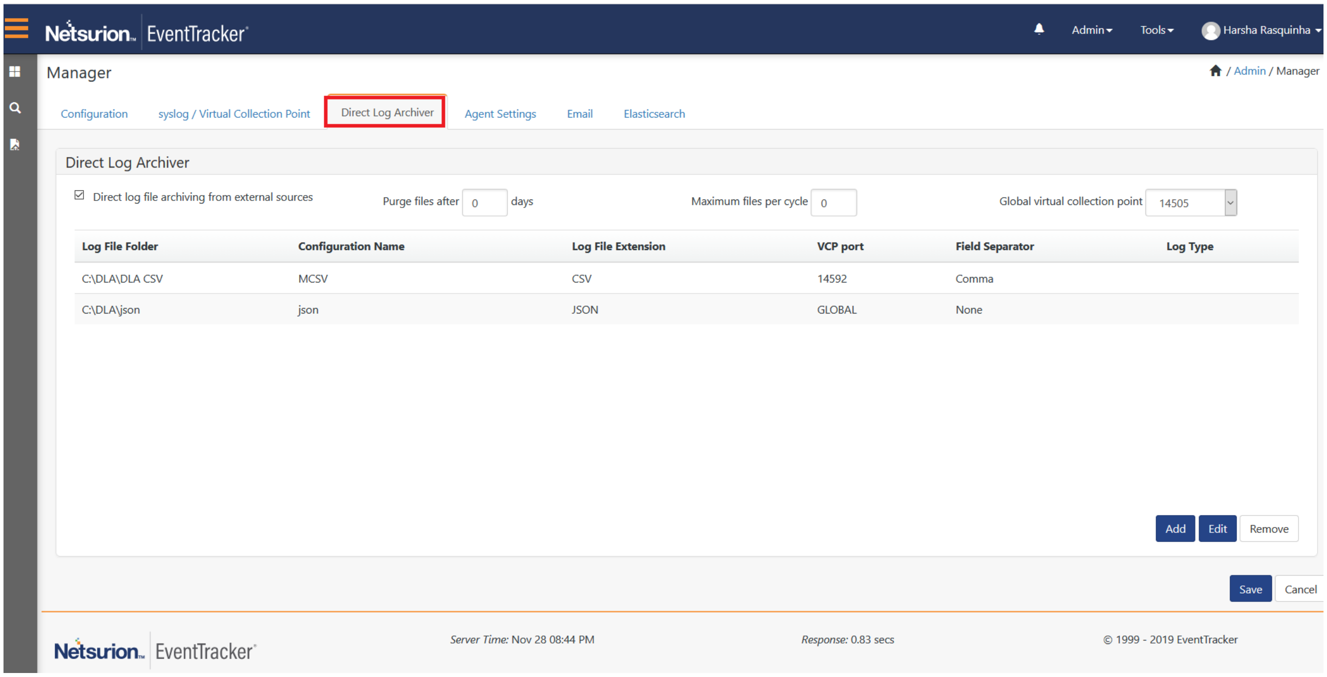
Figure 648

The output is available in **\\InstallDir\EventTracker\SheduledActionScripts** folder in .html format.

28.1.2 Creating DLA to generate reports.

1. Logon to EventTracker.
2. Select the **Admin** menu, and then select **Manager.**

   Manager configuration window opens.
3. Select **Direct Log Archiver** tab.



Direct Log Archiver

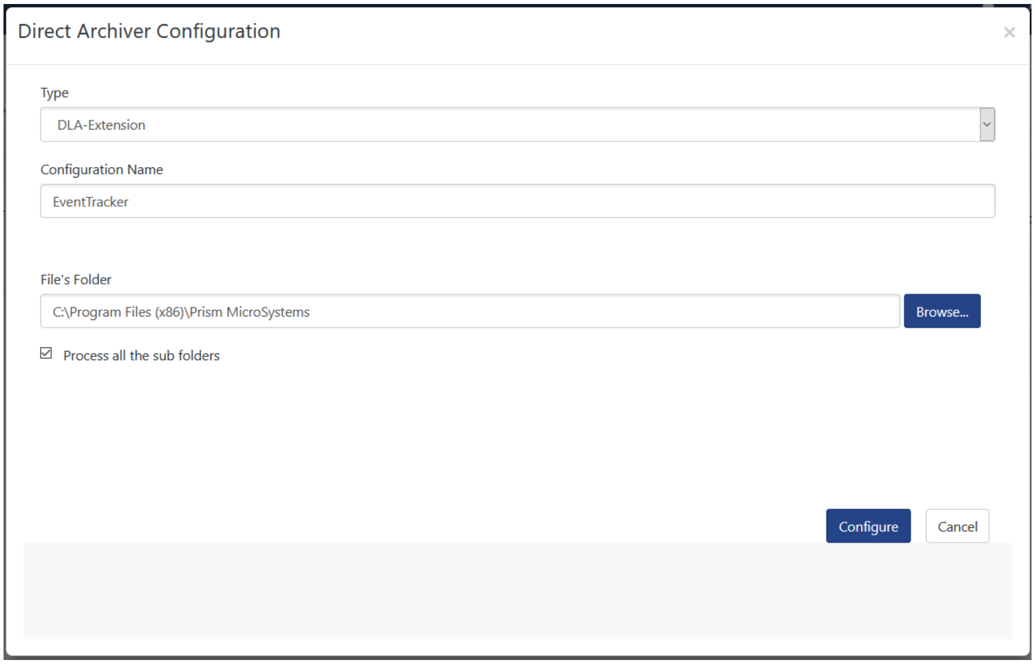
☑ Direct log file archiving from external sources Purge files after 0 days Maximum files per cycle 0 Global virtual collection point 14505

Log File Folder	Configuration Name	Log File Extension	VCP port	Field Separator	Log Type
C:\DLA\DLA CSV	MCSV	CSV	14592	Comma	
C:\DLA\json	json	JSON	GLOBAL	None	

Server Time: Nov 28 08:44 PM *Response:* 0.83 secs © 1999 - 2019 EventTracker

Figure 649

4. Click **Add.**
   Direct archiver configuration window opens.
5. Select **Type** as **DLA-Extension** and then enter **Configuration Name**.



Direct Archiver Configuration

Type: DLA-Extension

Configuration Name: EventTracker

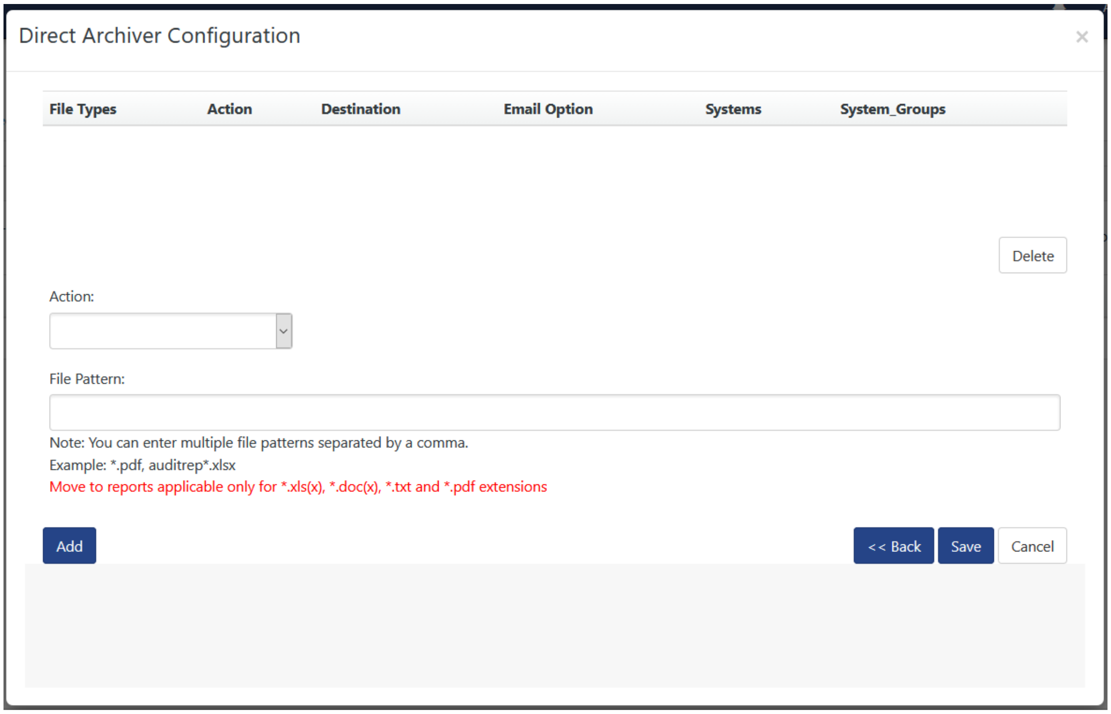
File's Folder: C:\Program Files (x86)\Prism MicroSystems

☑ Process all the sub folders

Figure 650

6. Click **Browse** and select **File's Folder** path.

7. Select **Configure**.



Direct Archiver Configuration

File Types	Action	Destination	Email Option	Systems	System_Groups

Action:

File Pattern:

Note: You can enter multiple file patterns separated by a comma.
Example: *.pdf, auditrep*.xlsx
Move to reports applicable only for *.xls(x), *.doc(x), *.txt and *.pdf extensions

Figure 651

8. In **Action** drop down, select **Move to html reports**, and then click **Save**.
   Now you can generate the respective report in Reports Dashboard.
9. To search for the report, select the **Reports** menu, and then select **Dashboard**.
10. In **Search** box, enter **the report name** and then select the **Search** icon.
11. Select the report name and generate the report accordingly.

29. Sitemap

In this chapter, you will learn how to:

- View Sitemap

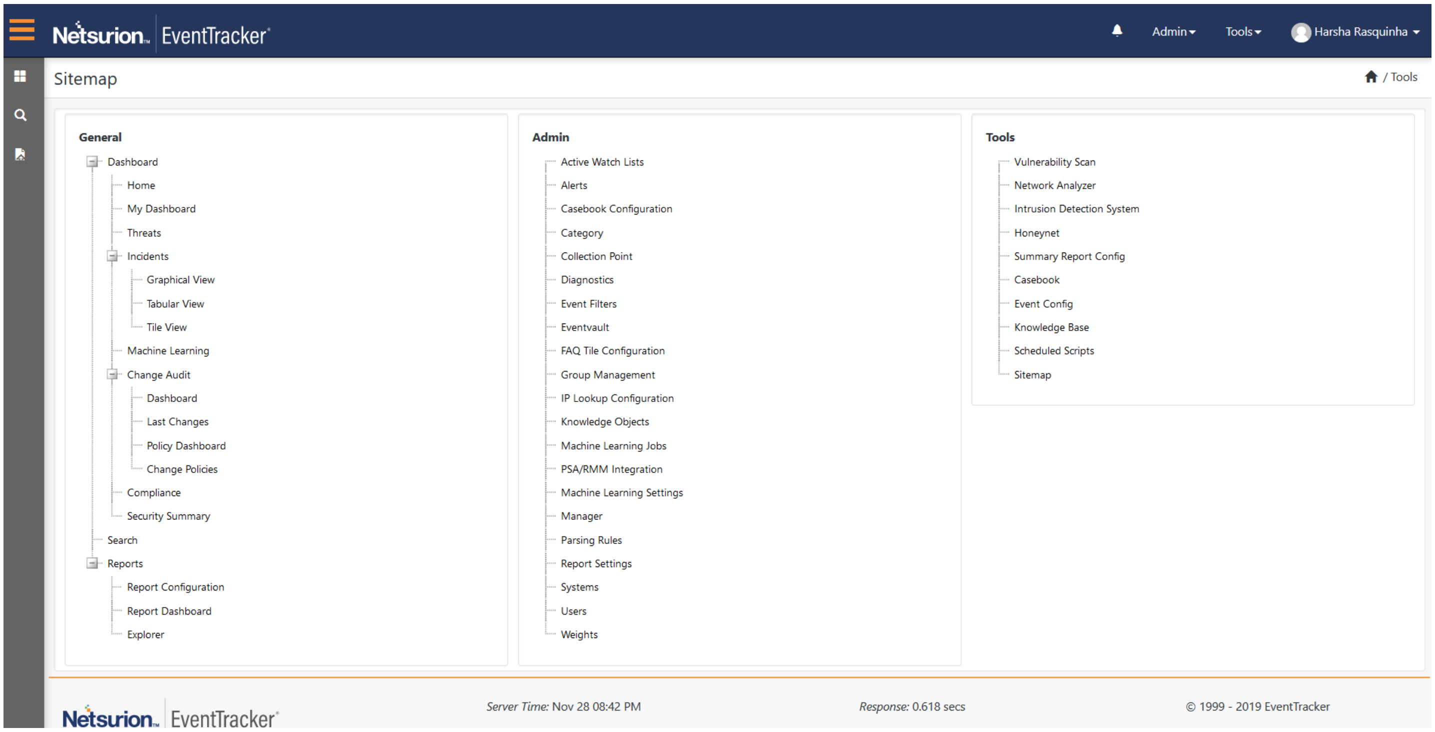
29.1 Sitemap

Sitemap provides a view of index of the web site.

29.1.1 Viewing Sitemap

1 Log on to EventTracker, click **Tools** and then click the **Sitemap**.

EventTracker opens the sitemap.



General

- Dashboard
  - Home
  - My Dashboard
  - Threats
  - Incidents
    - Graphical View
    - Tabular View
    - Tile View
  - Machine Learning
  - Change Audit
    - Dashboard
    - Last Changes
    - Policy Dashboard
    - Change Policies
  - Compliance
  - Security Summary
- Search
- Reports
  - Report Configuration
  - Report Dashboard
  - Explorer

Admin

- Active Watch Lists
- Alerts
- Casebook Configuration
- Category
- Collection Point
- Diagnostics
- Event Filters
- Eventvault
- FAQ Tile Configuration
- Group Management
- IP Lookup Configuration
- Knowledge Objects
- Machine Learning Jobs
- PSA/RMM Integration
- Machine Learning Settings
- Manager
- Parsing Rules
- Report Settings
- Systems
- Users
- Weights

Tools

- Vulnerability Scan
- Network Analyzer
- Intrusion Detection System
- Honeynet
- Summary Report Config
- Casebook
- Event Config
- Knowledge Base
- Scheduled Scripts
- Sitemap

Netsurion. EventTracker *Server Time:* Nov 28 08:42 PM *Response:* 0.618 secs © 1999 - 2019 EventTracker

Figure 652

2 Select any General/Admin/Tools feature or menu to navigate directly to the respective option.

30. EventVault Warehouse Manager

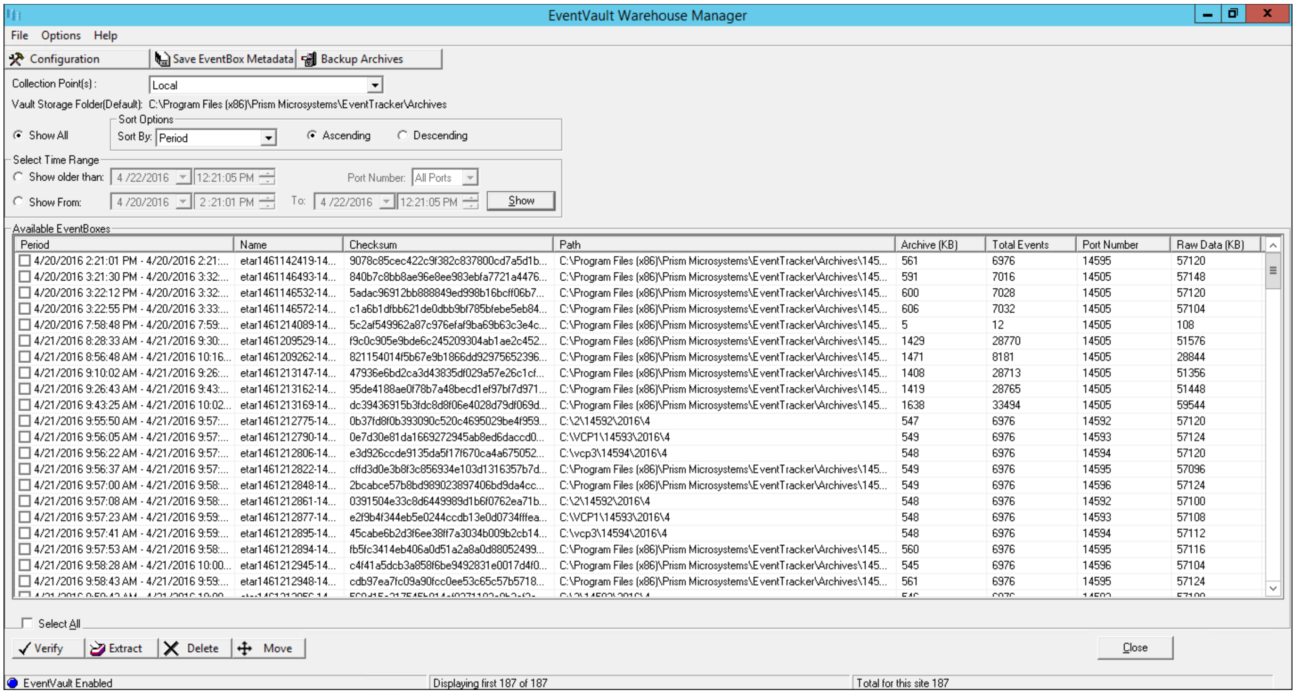
In this chapter, you will learn :

- Using EventVault Warehouse Manager
- Configuration
- Saving EventBox Metadata
- Backup Archives
- Extracting EventBox data
- Moving CAB files
- Deleting an EventBox

30.1 EventVault Warehouse Manager

1. To access **EventVault Warehouse Manager**, click **Start**, select **All Programs**, and then select **Prism Microsystems**.
2. Select **EventTracker**, select **EventTracker Control Panel** and then select **EventVault.**

   EventVault Warehouse Manager window opens.



Collection Point(s) : Local

Vault Storage Folder(Default): C:\Program Files (x86)\Prism Microsystems\EventTracker\Archives

● Show All

Sort Options

Sort By: Period

● Ascending ○ Descending

Select Time Range

○ Show older than: 4 /22/2016 12:21:05 PM Port Number: All Ports

○ Show From: 4 /20/2016 2 :21:01 PM To: 4 /22/2016 12:21:05 PM

Available EventBoxes

Period	Name	Checksum	Path	Archive (KB)	Total Events	Port Number	Raw Data (KB)
☐ 4/20/2016 2:21:01 PM - 4/20/2016 2:21:...	etar1461142419-14...	9078c85cec422c9f382c837800cd7a5d1b...	C:\Program Files (x86)\Prism Microsystems\EventTracker\Archives\145...	561	6976	14595	57120
☐ 4/20/2016 3:21:30 PM - 4/20/2016 3:32:...	etar1461146493-14...	840b7c8bb8ae96e8ee983ebfa7721a4476...	C:\Program Files (x86)\Prism Microsystems\EventTracker\Archives\145...	591	7016	14505	57148
☐ 4/20/2016 3:22:12 PM - 4/20/2016 3:32:...	etar1461146532-14...	5adac96912bb888849ed998b16bcff06b7...	C:\Program Files (x86)\Prism Microsystems\EventTracker\Archives\145...	600	7028	14505	57120
☐ 4/20/2016 3:22:55 PM - 4/20/2016 3:33:...	etar1461146572-14...	c1a6b1dfbb621de0dbb9bf785bfebe5eb84...	C:\Program Files (x86)\Prism Microsystems\EventTracker\Archives\145...	606	7032	14505	57104
☐ 4/20/2016 7:58:48 PM - 4/20/2016 7:59:...	etar1461214089-14...	5c2af549962a87c976efaf9ba69b63c3e4c...	C:\Program Files (x86)\Prism Microsystems\EventTracker\Archives\145...	5	12	14505	108
☐ 4/21/2016 8:28:33 AM - 4/21/2016 9:30:...	etar1461209529-14...	f9c0c905e9bde6c245209304ab1ae2c452...	C:\Program Files (x86)\Prism Microsystems\EventTracker\Archives\145...	1429	28770	14505	51576
☐ 4/21/2016 8:56:48 AM - 4/21/2016 10:16...	etar1461209262-14...	821154014f5b67e9b1866dd92975652396...	C:\Program Files (x86)\Prism Microsystems\EventTracker\Archives\145...	1471	8181	14505	28844
☐ 4/21/2016 9:10:02 AM - 4/21/2016 9:26:...	etar1461213147-14...	47936e6bd2ca3d43835df029a57e26c1cf...	C:\Program Files (x86)\Prism Microsystems\EventTracker\Archives\145...	1408	28713	14505	51356
☐ 4/21/2016 9:26:43 AM - 4/21/2016 9:43:...	etar1461213162-14...	95de4188ae0f78b7a48becd1ef97bf7d971...	C:\Program Files (x86)\Prism Microsystems\EventTracker\Archives\145...	1419	28765	14505	51448
☐ 4/21/2016 9:43:25 AM - 4/21/2016 10:02...	etar1461213169-14...	dc39436915b3fdc8d8f06e4028d79df069d...	C:\Program Files (x86)\Prism Microsystems\EventTracker\Archives\145...	1638	33494	14505	59544
☐ 4/21/2016 9:55:50 AM - 4/21/2016 9:57:...	etar1461212775-14...	0b37fd8f0b393090c520c4695029be4f959...	C:\2\14592\2016\4	547	6976	14592	57120
☐ 4/21/2016 9:56:05 AM - 4/21/2016 9:57:...	etar1461212790-14...	0e7d30e81da1669272945ab8ed6daccd0...	C:\VCP1\14593\2016\4	549	6976	14593	57124
☐ 4/21/2016 9:56:22 AM - 4/21/2016 9:57:...	etar1461212806-14...	e3d926ccde9135da5f17f670ca4a675052...	C:\vcp3\14594\2016\4	548	6976	14594	57120
☐ 4/21/2016 9:56:37 AM - 4/21/2016 9:57:...	etar1461212822-14...	cffd3d0e3b8f3c856934e103d1316357b7d...	C:\Program Files (x86)\Prism Microsystems\EventTracker\Archives\145...	549	6976	14595	57096
☐ 4/21/2016 9:57:00 AM - 4/21/2016 9:58:...	etar1461212848-14...	2bcabce57b8bd989023897406bd9da4cc...	C:\Program Files (x86)\Prism Microsystems\EventTracker\Archives\145...	549	6976	14596	57124
☐ 4/21/2016 9:57:08 AM - 4/21/2016 9:58:...	etar1461212861-14...	0391504e33c8d6449989d1b6f0762ea71b...	C:\2\14592\2016\4	548	6976	14592	57100
☐ 4/21/2016 9:57:23 AM - 4/21/2016 9:59:...	etar1461212877-14...	e2f9b4f344eb5e0244ccdb13e0d0734fffea...	C:\VCP1\14593\2016\4	548	6976	14593	57108
☐ 4/21/2016 9:57:41 AM - 4/21/2016 9:59:...	etar1461212895-14...	45cabe6b2d3f6ee38ff7a3034b009b2cb14...	C:\vcp3\14594\2016\4	548	6976	14594	57112
☐ 4/21/2016 9:57:53 AM - 4/21/2016 9:58:...	etar1461212894-14...	fb5fc3414eb406a0d51a2a8a0d88052499...	C:\Program Files (x86)\Prism Microsystems\EventTracker\Archives\145...	560	6976	14595	57116
☐ 4/21/2016 9:58:28 AM - 4/21/2016 10:00...	etar1461212945-14...	c4f41a5dcb3a858f6be9492831e0017d4f0...	C:\Program Files (x86)\Prism Microsystems\EventTracker\Archives\145...	545	6976	14596	57104
☐ 4/21/2016 9:58:43 AM - 4/21/2016 9:59:...	etar1461212948-14...	cdb97ea7fc09a90fcc0ee53c65c57b5718...	C:\Program Files (x86)\Prism Microsystems\EventTracker\Archives\145...	561	6976	14595	57124

☐ Select All

EventVault Enabled | Displaying first 187 of 187 | Total for this site 187

Figure 653

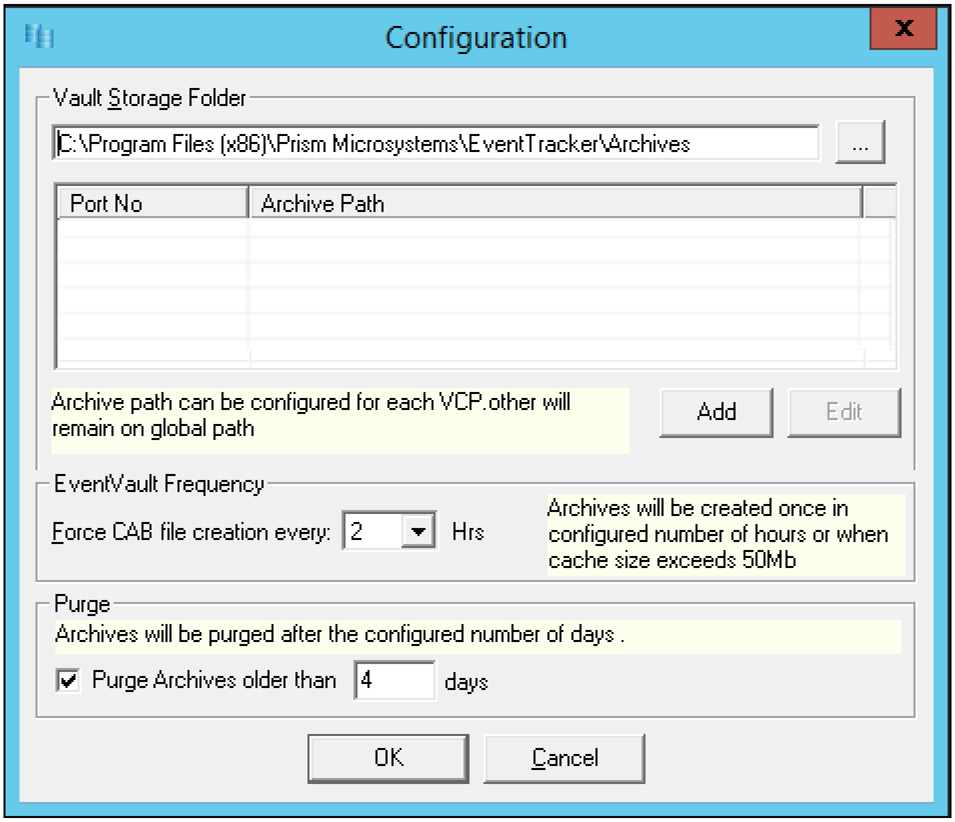
Field	Description
Available EventBoxes	
Period	Time range of events stored in the CAB file.
Name	Name of the CAB file. etar1269949644-14505.cab etar – EventTracker Archive 1269949644 – Time ticks 14505 – Port number (through which EventTracker Receiver service received events) cab – File extension of cabinet files
Checksum	SHA 1 checksum number for tamper proof.
Path	Path of the folder where the archives are stored typically, EventTracker install path\ port number\ year\ month
Size (KB)	Size of the CAB file in KB.
Total Events	Total number of events accommodated in the CAB file.
Port Number	Port number through which the EventTracker Receiver service received the events.

Table 70

3. Select **Collection Point(s):** drop-down; select the Collection Point cab file available. The details of CAB file opens.

30.1.1 Configuration button

1. Click **Configuration**.
   Configuration window opens.



Vault Storage Folder: C:\Program Files (x86)\Prism Microsystems\EventTracker\Archives

Archive path can be configured for each VCP.other will remain on global path

Force CAB file creation every: 2 Hrs

Archives will be created once in configured number of hours or when cache size exceeds 50Mb

Archives will be purged after the configured number of days .

☑ Purge Archives older than 4 days

Figure 654

Vault Storage Folder displays the location of the folder where archives are stored.

2. To change the location of the folder where archives are stored, click **Browse** and then select the new location.

   (OR)
   Manually type the new UNC path in the **Vault Storage Folder** textbox.

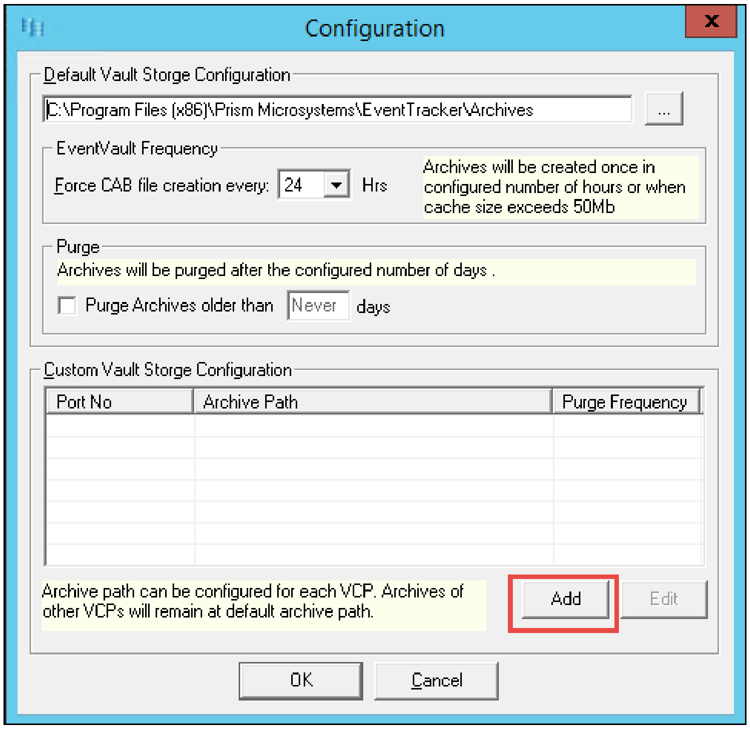
3. To create CAB files, specify the time duration in **Force CAB file creation every:** drop-down Archives will be created for the number of hours specified or when cache size exceeds 50 Mb.
4. To purge archive folders, select **Purge Archives older than** option and specify number of **days**. The user can purge the collection point cab file from the collection master.

30.1.2 Configuring Archive Path for each VCP

The EventVault configuration window will now have a list view, which will display the configured ports and their respective configured archive path.

The Ports configured by the user in **Manager>Syslog/Virtual Collection Point,** will now be listed here and the user can configure archive path for specific VCPs.

1. Click **Configuration** in the EventVault Warehouse Manager window.
2. To configure archive path for a specific VCP, click **Add**.



Configuration

Default Vault Storge Configuration

C:\Program Files (x86)\Prism Microsystems\EventTracker\Archives

EventVault Frequency

Force CAB file creation every: 24 Hrs

Archives will be created once in configured number of hours or when cache size exceeds 50Mb

Purge

Archives will be purged after the configured number of days .

□ Purge Archives older than Never days

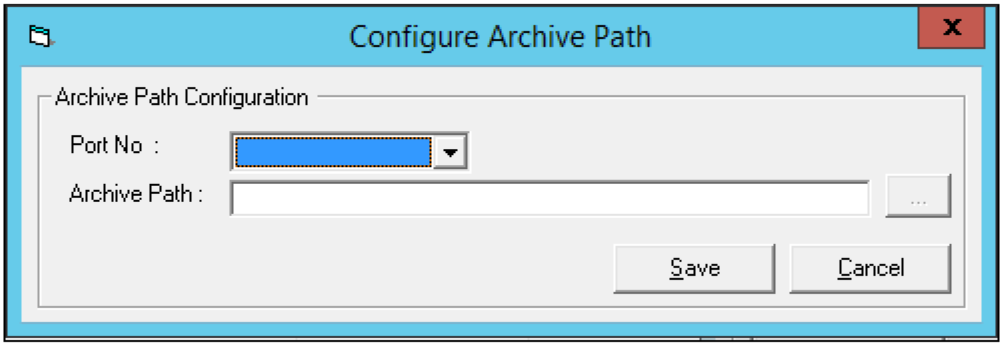
Custom Vault Storge Configuration

Port No	Archive Path	Purge Frequency

Archive path can be configured for each VCP. Archives of other VCPs will remain at default archive path.

Figure 656

Configure Archive Path window opens.



Configure Archive Path

Archive Path Configuration

Port No :

Archive Path :

Figure 657

3. Select the **Port No**: from the dropdown list and browse the new **Archive Path** by clicking the icon .

NOTE

The Port Numbers will only get listed after the user has configured them in Manager -> Syslog/Virtual Collection Point.

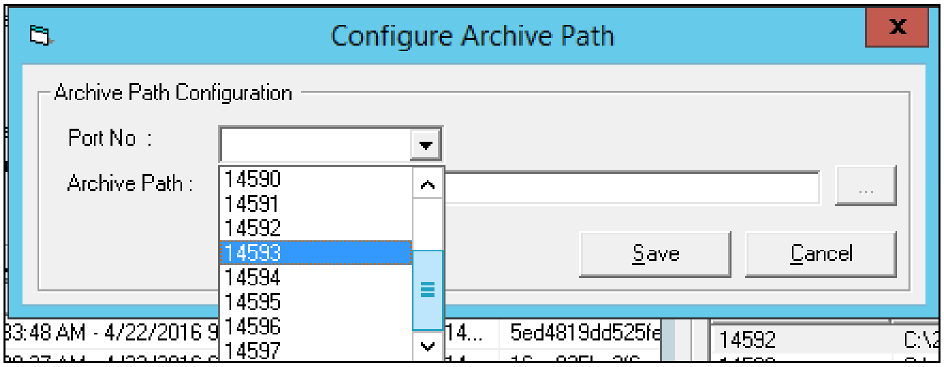
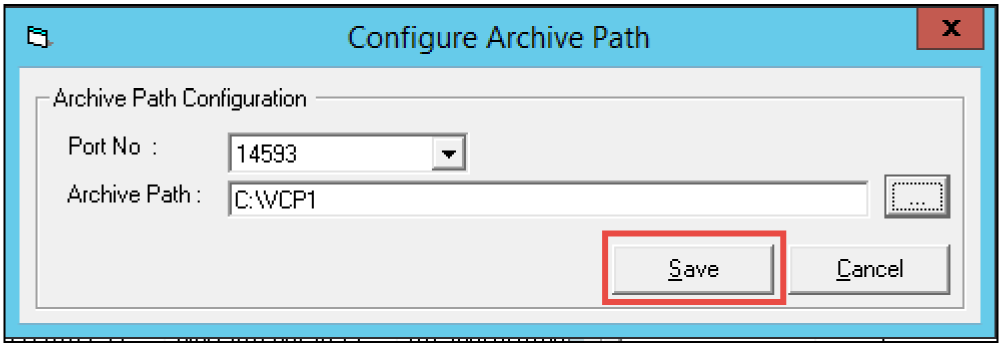


Figure 658

4. Once the archive path is confirmed, click **Save**.



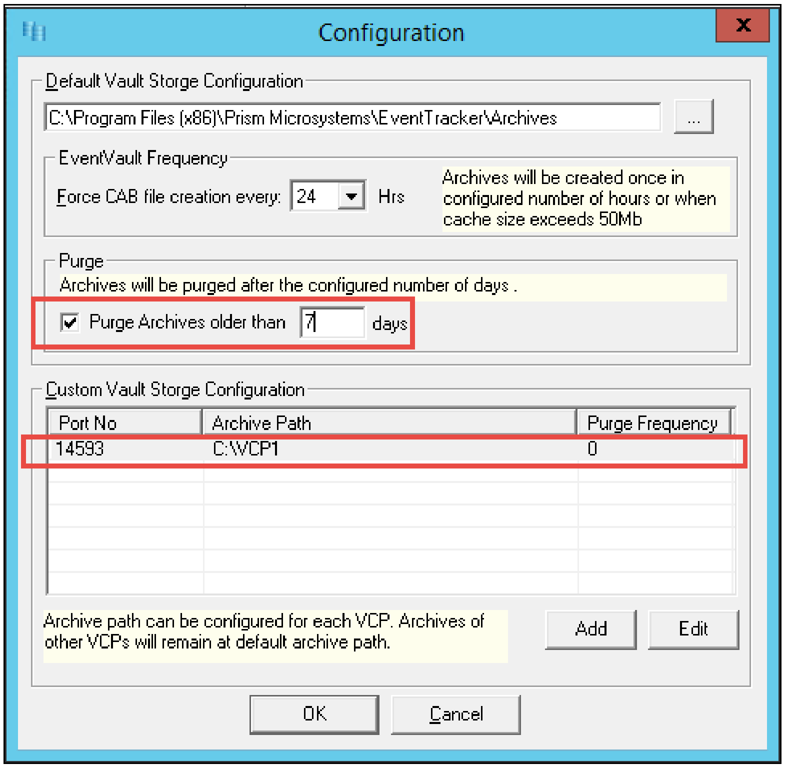
Port No : 14593

Archive Path : C:\VCP1

Figure 659

It will get listed in the configuration window.

NOTE: The user can also purge older archives by checking the “**Purge Archives older than** “option and entering the desired number of days.



Configuration

Default Vault Storge Configuration

C:\Program Files (x86)\Prism Microsystems\EventTracker\Archives

EventVault Frequency

Force CAB file creation every: 24 Hrs

Archives will be created once in configured number of hours or when cache size exceeds 50Mb

Purge

Archives will be purged after the configured number of days .

☑ Purge Archives older than 7 days

Custom Vault Storge Configuration

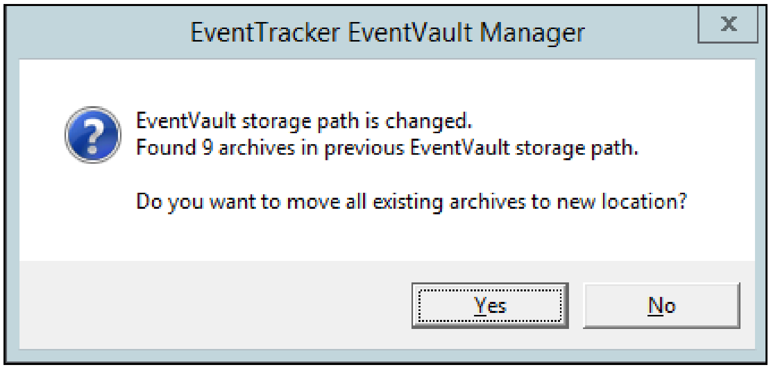
Port No	Archive Path	Purge Frequency
14593	C:\VCP1	0

Archive path can be configured for each VCP. Archives of other VCPs will remain at default archive path.

Figure 660

5. Click **OK**.

   The below message opens.



EventTracker EventVault Manager

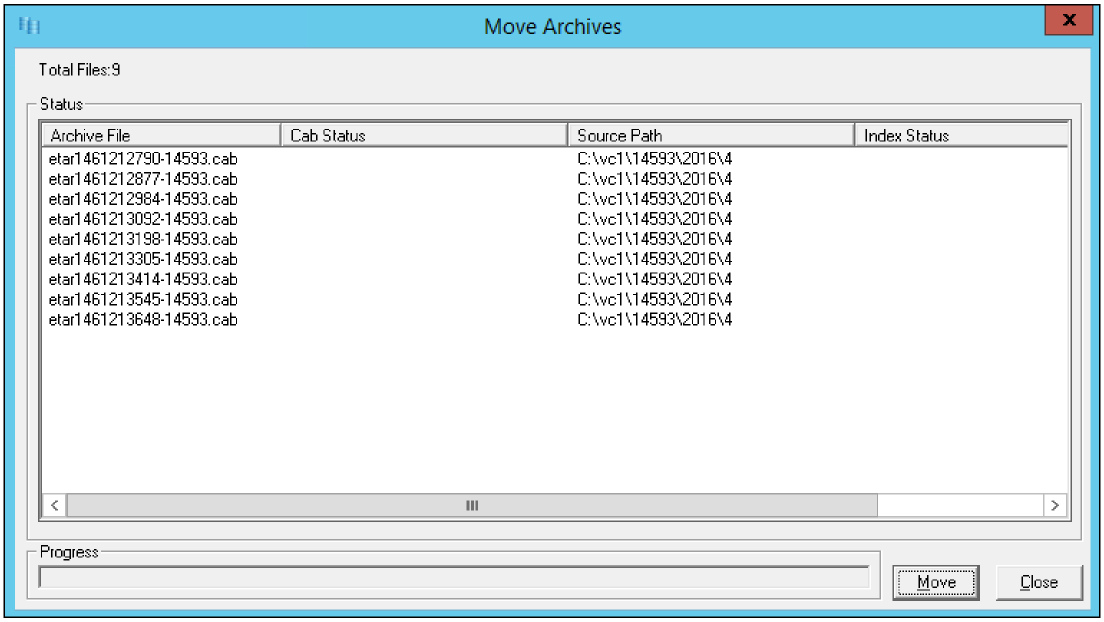
EventVault storage path is changed.
Found 9 archives in previous EventVault storage path.

Do you want to move all existing archives to new location?

Figure 661

6. Click "**Yes**" to move the existing Archives to the new configured location.

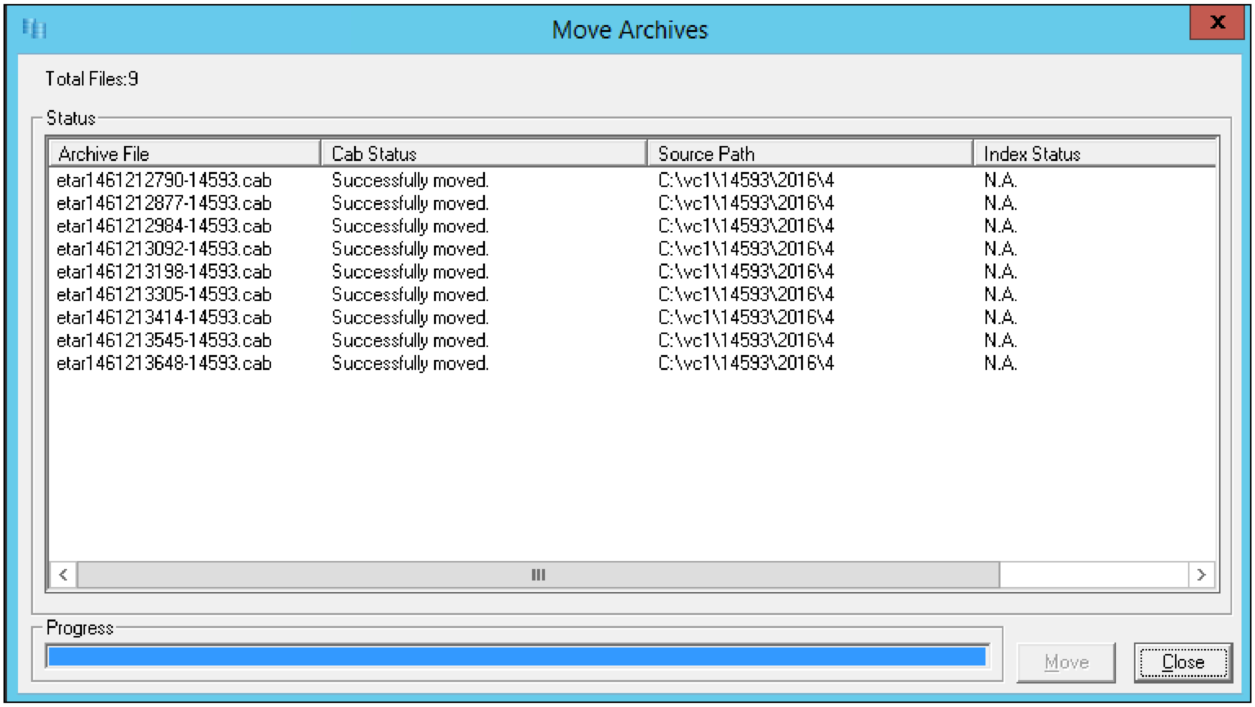
   It will list the existing Archive files with the source path.



Archive File	Cab Status	Source Path	Index Status
etar1461212790-14593.cab		C:\vc1\14593\2016\4	
etar1461212877-14593.cab		C:\vc1\14593\2016\4	
etar1461212984-14593.cab		C:\vc1\14593\2016\4	
etar1461213092-14593.cab		C:\vc1\14593\2016\4	
etar1461213198-14593.cab		C:\vc1\14593\2016\4	
etar1461213305-14593.cab		C:\vc1\14593\2016\4	
etar1461213414-14593.cab		C:\vc1\14593\2016\4	
etar1461213545-14593.cab		C:\vc1\14593\2016\4	
etar1461213648-14593.cab		C:\vc1\14593\2016\4	

Figure 662

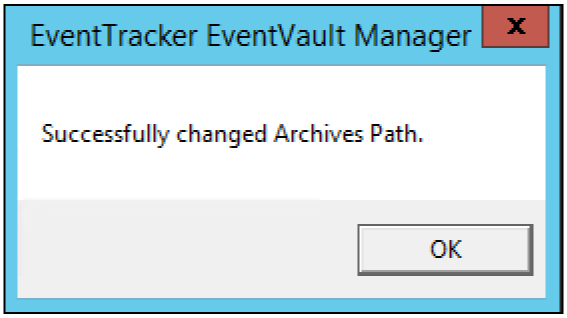
7. Click **Move**. It will successfully transfer all the existing archive files to the new location.



Archive File	Cab Status	Source Path	Index Status
etar1461212790-14593.cab	Successfully moved.	C:\vc1\14593\2016\4	N.A.
etar1461212877-14593.cab	Successfully moved.	C:\vc1\14593\2016\4	N.A.
etar1461212984-14593.cab	Successfully moved.	C:\vc1\14593\2016\4	N.A.
etar1461213092-14593.cab	Successfully moved.	C:\vc1\14593\2016\4	N.A.
etar1461213198-14593.cab	Successfully moved.	C:\vc1\14593\2016\4	N.A.
etar1461213305-14593.cab	Successfully moved.	C:\vc1\14593\2016\4	N.A.
etar1461213414-14593.cab	Successfully moved.	C:\vc1\14593\2016\4	N.A.
etar1461213545-14593.cab	Successfully moved.	C:\vc1\14593\2016\4	N.A.
etar1461213648-14593.cab	Successfully moved.	C:\vc1\14593\2016\4	N.A.

Figure 663

8. Click **Close**. The success message id appears.
9. If you do not want to move the existing archives to the newly configured archive path, click “**NO**”. The success message appears.



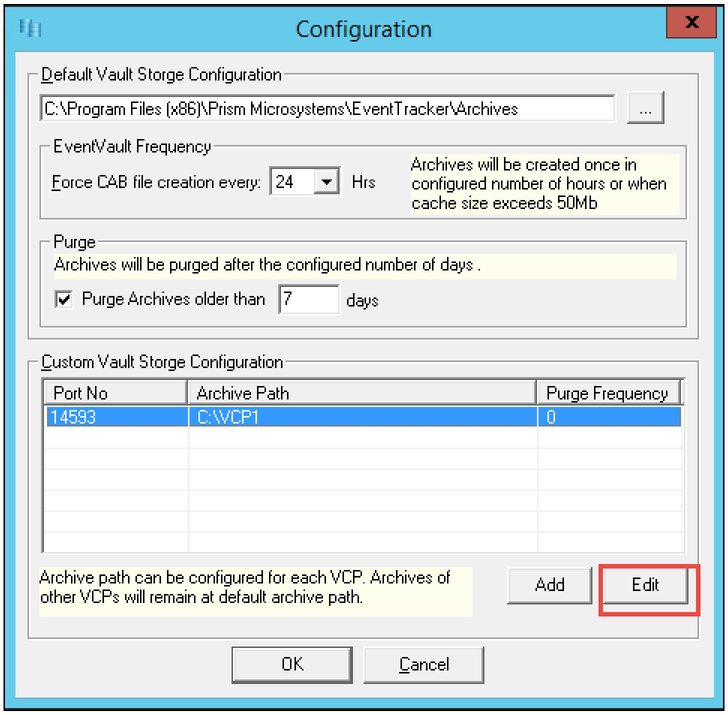
EventTracker EventVault Manager

Successfully changed Archives Path.

Figure 664

To Edit the Archive path for specific VCPs,

1. In the configuration window, select the port number from the list view
2. Click **Edit**.



Configuration

Default Vault Storge Configuration

C:\Program Files (x86)\Prism Microsystems\EventTracker\Archives

EventVault Frequency

Force CAB file creation every: 24 Hrs

Archives will be created once in configured number of hours or when cache size exceeds 50Mb

Purge

Archives will be purged after the configured number of days .

☑ Purge Archives older than 7 days

Custom Vault Storge Configuration

Port No	Archive Path	Purge Frequency
14593	C:\VCP1	0

Archive path can be configured for each VCP. Archives of other VCPs will remain at default archive path.

Figure 665

30.1.3 Saving EventBox Metadata

This option enables you to save the archive summary in a text file. It helps you to locate .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 opens 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**.

30.1.4 Backing 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.

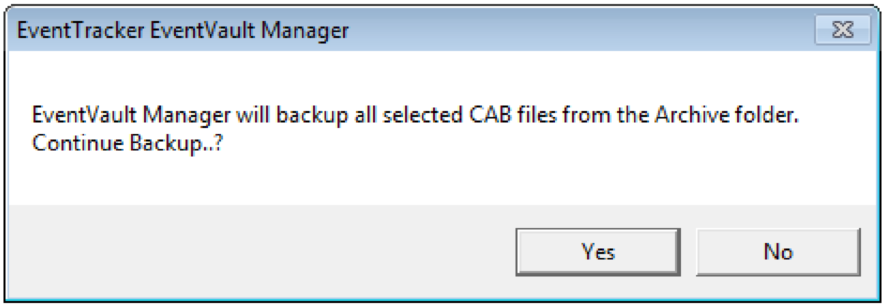
1 Open the EventVault Warehouse Manager.

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 opens the confirmation message box.



EventTracker EventVault Manager

EventVault Manager will backup all selected CAB files from the Archive folder.
Continue Backup..?

Figure 666

4 Click **Yes**.

EventVault Warehouse Manager opens 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.

30.1.5 Extracting EventBox Data

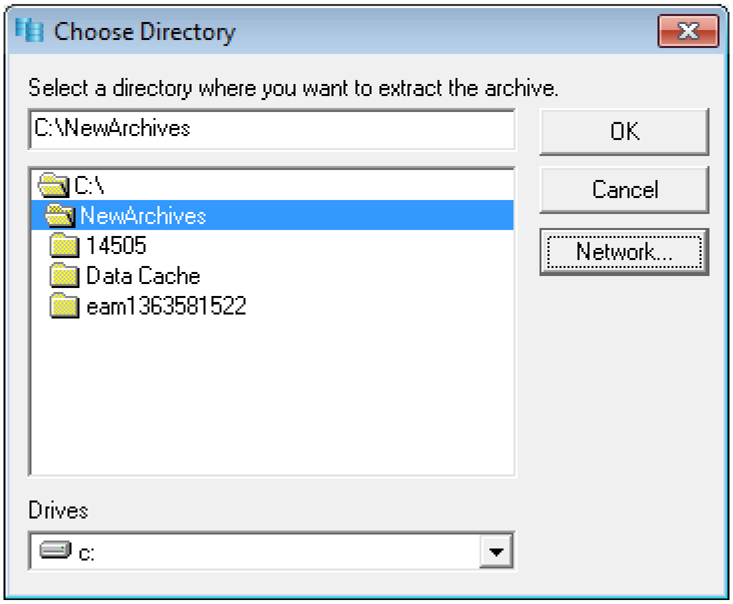
This option enables you to extract EventBox data into an MS Access database.

1 Open EventVault Warehouse Manager.

2 Select the CAB file(s) from the **Available EventBoxes** list.

3 Click **Extract**.

EventVault Manager opens the **Choose Directory** window.


Choose Directory

Select a directory where you want to extract the archive.

C:\NewArchives

Figure 667

4 Select the path where you want to store the event data, and then click **Save**.

After extracting the event data, EventTracker opens 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.

30.1.6 Moving 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 opens the confirmation message box.

4 Click **Yes** to proceed.

EventVault Warehouse Manager opens the Choose Directory dialog box.

5 Select the location (local or network) and then click **OK**.

(OR)

Manually type the new UNC path in the **Vault Storage Folder** textbox and then click **OK**.

EventVault Warehouse Manager moves all the selected files to the new location and displays the ArchIntegrity report in the Notepad.

30.1.7 Deleting 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 opens the Confirmation message box.
5 Click **OK**.

EventVault Warehouse Manager deletes the selected EventBox and displays the ArchIntegrity report in the Notepad.

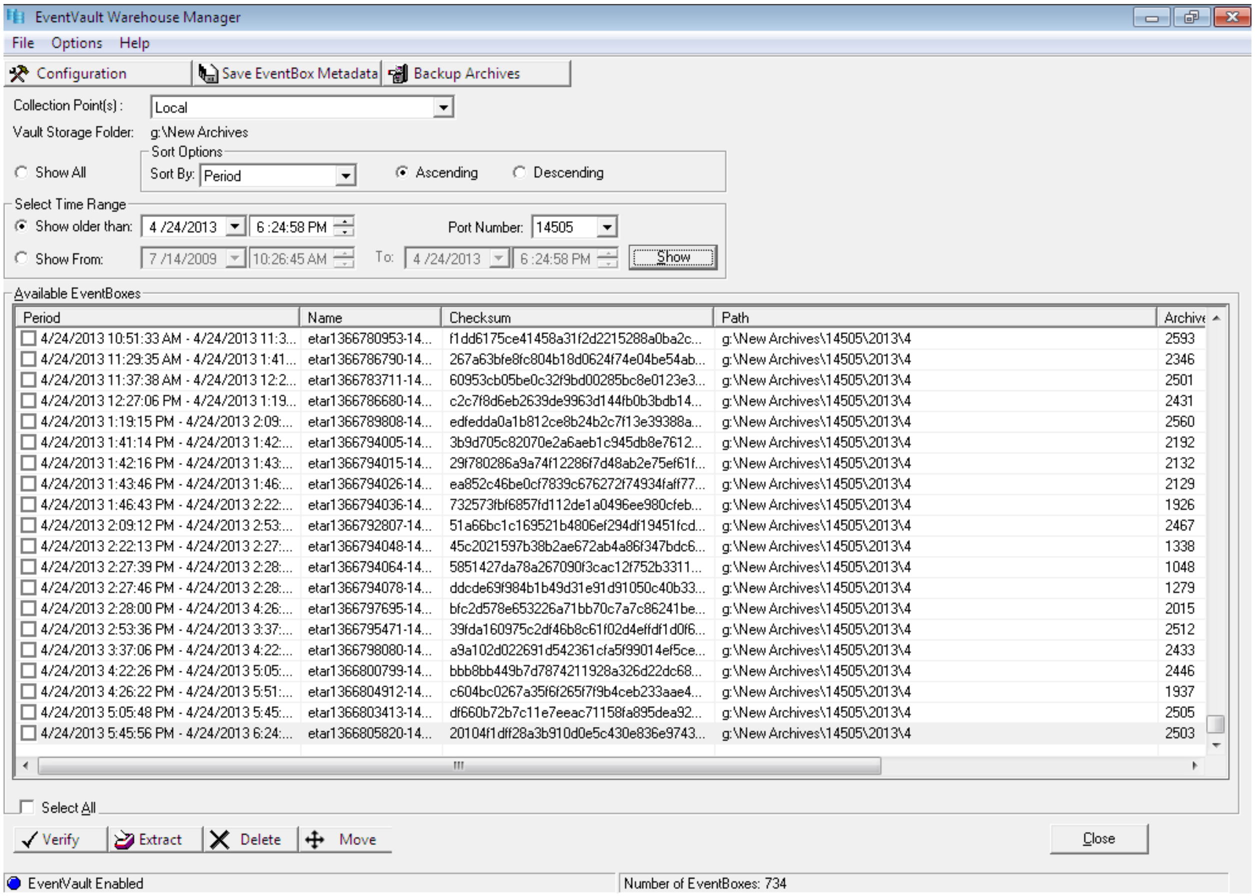
30.1.8 Viewing CAB Files by Port Number

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 opens the CAB files of the selected port for the selected time range.



Collection Point(s) : Local

Vault Storage Folder: g:\New Archives

○ Show All

Sort Options

Sort By: Period

● Ascending ○ Descending

Select Time Range

● Show older than: 4 /24/2013 6 :24:58 PM

Port Number: 14505

○ Show From: 7 /14/2009 10:26:45 AM To: 4 /24/2013 6 :24:58 PM

Available EventBoxes

Period	Name	Checksum	Path	Archive
□ 4/24/2013 10:51:33 AM - 4/24/2013 11:3...	etar1366780953-14...	f1dd6175ce41458a31f2d2215288a0ba2c...	g:\New Archives\14505\2013\4	2593
□ 4/24/2013 11:29:35 AM - 4/24/2013 1:41...	etar1366786790-14...	267a63bfe8fc804b18d0624f74e04be54ab...	g:\New Archives\14505\2013\4	2346
□ 4/24/2013 11:37:38 AM - 4/24/2013 12:2...	etar1366783711-14...	60953cb05be0c32f9bd00285bc8e0123e3...	g:\New Archives\14505\2013\4	2501
□ 4/24/2013 12:27:06 PM - 4/24/2013 1:19...	etar1366786680-14...	c2c7f8d6eb2639de9963d144fb0b3bdb14...	g:\New Archives\14505\2013\4	2431
□ 4/24/2013 1:19:15 PM - 4/24/2013 2:09:...	etar1366789808-14...	edfedda0a1b812ce8b24b2c7f13e39388a...	g:\New Archives\14505\2013\4	2560
□ 4/24/2013 1:41:14 PM - 4/24/2013 1:42:...	etar1366794005-14...	3b9d705c82070e2a6aeb1c945db8e7612...	g:\New Archives\14505\2013\4	2192
□ 4/24/2013 1:42:16 PM - 4/24/2013 1:43:...	etar1366794015-14...	29f780286a9a74f12286f7d48ab2e75ef61f...	g:\New Archives\14505\2013\4	2132
□ 4/24/2013 1:43:46 PM - 4/24/2013 1:46:...	etar1366794026-14...	ea852c46be0cf7839c676272f74934faff77...	g:\New Archives\14505\2013\4	2129
□ 4/24/2013 1:46:43 PM - 4/24/2013 2:22:...	etar1366794036-14...	732573fbf6857fd112de1a0496ee980cfeb...	g:\New Archives\14505\2013\4	1926
□ 4/24/2013 2:09:12 PM - 4/24/2013 2:53:...	etar1366792807-14...	51a66bc1c169521b4806ef294df19451fcd...	g:\New Archives\14505\2013\4	2467
□ 4/24/2013 2:22:13 PM - 4/24/2013 2:27:...	etar1366794048-14...	45c2021597b38b2ae672ab4a86f347bdc6...	g:\New Archives\14505\2013\4	1338
□ 4/24/2013 2:27:39 PM - 4/24/2013 2:28:...	etar1366794064-14...	5851427da78a267090f3cac12f752b3311...	g:\New Archives\14505\2013\4	1048
□ 4/24/2013 2:27:46 PM - 4/24/2013 2:28:...	etar1366794078-14...	ddcde69f984b1b49d31e91d91050c40b33...	g:\New Archives\14505\2013\4	1279
□ 4/24/2013 2:28:00 PM - 4/24/2013 4:26:...	etar1366797695-14...	bfc2d578e653226a71bb70c7a7c86241be...	g:\New Archives\14505\2013\4	2015
□ 4/24/2013 2:53:36 PM - 4/24/2013 3:37:...	etar1366795471-14...	39fda160975c2df46b8c61f02d4effdf1d0f6...	g:\New Archives\14505\2013\4	2512
□ 4/24/2013 3:37:06 PM - 4/24/2013 4:22:...	etar1366798080-14...	a9a102d022691d542361cfa5f99014ef5ce...	g:\New Archives\14505\2013\4	2433
□ 4/24/2013 4:22:26 PM - 4/24/2013 5:05:...	etar1366800799-14...	bbb8bb449b7d7874211928a326d22dc68...	g:\New Archives\14505\2013\4	2446
□ 4/24/2013 4:26:22 PM - 4/24/2013 5:51:...	etar1366804912-14...	c604bc0267a35f6f265f7f9b4ceb233aae4...	g:\New Archives\14505\2013\4	1937
□ 4/24/2013 5:05:48 PM - 4/24/2013 5:45:...	etar1366803413-14...	df660b72b7c11e7eeac71158fa895dea92...	g:\New Archives\14505\2013\4	2505
□ 4/24/2013 5:45:56 PM - 4/24/2013 6:24:...	etar1366805820-14...	20104f1dff28a3b910d0e5c430e836e9743...	g:\New Archives\14505\2013\4	2503

□ Select All

● EventVault Enabled

Number of EventBoxes: 734

Figure 668

NOTE

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.

31. Diagnostics

In this chapter, you will learn how to:

- EventTracker Diagnostic Tool
- Setting Debug levels
- Obfuscating Classified Information
- Diagnostic Alert
- SQL Log
- Back up Configuration option
- Restoring Configuration option
- Advanced Settings

31.1 EventTracker Diagnostic Tool

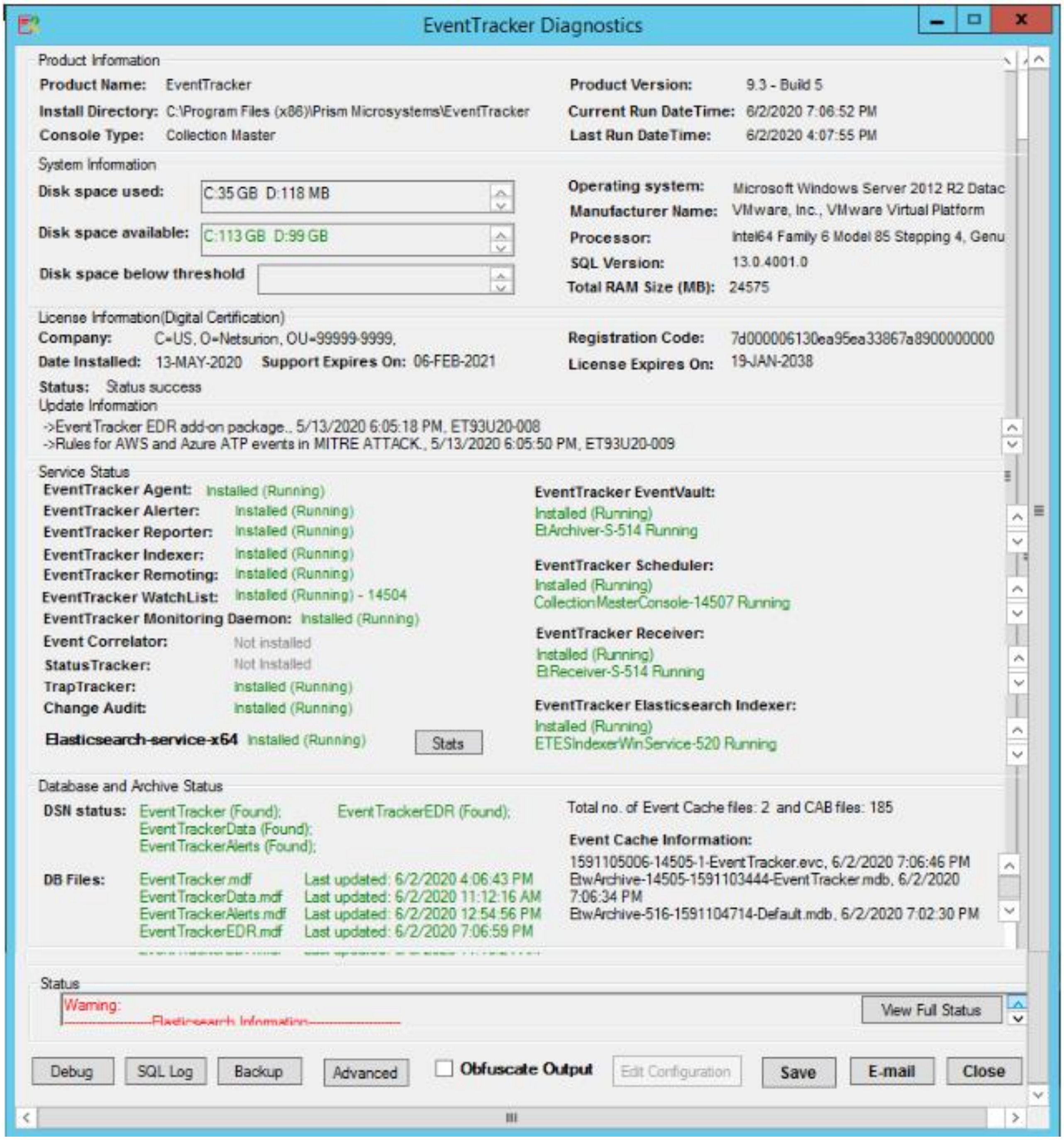
Windows (optionally) adds the Diagnostics Tool as a Startup program after successful installation of EventTracker. Diagnostics Tool alerts you if any problem occurs in the EventTracker.

Diagnostics data includes Product Information, System Information, License Information, Update Information, Service Status, Database, and Archive Status, configuration files, log dumps and SQL Log status. It is further extended to set debug levels and mask sensitive information. You can also back-up and restore files, generate alerts if CAB's are not received from Collection Point to Collection Master for last 24 hrs.

31.1.1 Starting EventTracker Diagnostic Tool

Note: This is a part of the feature update 9.3.2.

1. Click **Start**, select **All Programs**, and then select **Prism Microsystems**.
2. Select **EventTracker**, select **EventTracker Control Panel**, and then select **Diagnostics** icon.
   EventTracker opens **EventTracker Diagnostics** window.



Product Information

Product Name: EventTracker
Install Directory: C:\Program Files (x86)\Prism Microsystems\EventTracker
Console Type: Collection Master
Product Version: 9.3 - Build 5
Current Run DateTime: 6/2/2020 7:06:52 PM
Last Run DateTime: 6/2/2020 4:07:55 PM

System Information

Disk space used: C:35 GB D:118 MB
Disk space available: C:113 GB D:99 GB
Disk space below threshold
Operating system: Microsoft Windows Server 2012 R2 Datac
Manufacturer Name: VMware, Inc., VMware Virtual Platform
Processor: Intel64 Family 6 Model 85 Stepping 4, Genu
SQL Version: 13.0.4001.0
Total RAM Size (MB): 24575

License Information(Digital Certification)

Company: C=US, O=Netsurion, OU=99999-9999,
Date Installed: 13-MAY-2020 **Support Expires On:** 06-FEB-2021
Registration Code: 7d000006130ea95ea33867a8900000000
License Expires On: 19-JAN-2038
Status: Status success

Update Information

->Event Tracker EDR add-on package., 5/13/2020 6:05:18 PM, ET93U20-008
->Rules for AWS and Azure ATP events in MITRE ATTACK., 5/13/2020 6:05:50 PM, ET93U20-009

Service Status

EventTracker Agent: Installed (Running)
EventTracker Alerter: Installed (Running)
EventTracker Reporter: Installed (Running)
EventTracker Indexer: Installed (Running)
EventTracker Remoting: Installed (Running)
EventTracker WatchList: Installed (Running) - 14504
EventTracker Monitoring Daemon: Installed (Running)
Event Correlator: Not installed
StatusTracker: Not Installed
TrapTracker: Installed (Running)
Change Audit: Installed (Running)
Elasticsearch-service-x64 Installed (Running)

EventTracker EventVault:
Installed (Running)
EtArchiver-S-514 Running

EventTracker Scheduler:
Installed (Running)
CollectionMasterConsole-14507 Running

EventTracker Receiver:
Installed (Running)
EtReceiver-S-514 Running

EventTracker Elasticsearch Indexer:
Installed (Running)
ETESIndexerWinService-520 Running

Database and Archive Status

DSN status: EventTracker (Found); EventTrackerEDR (Found);
EventTrackerData (Found);
EventTrackerAlerts (Found);

DB Files:
EventTracker.mdf Last updated: 6/2/2020 4:06:43 PM
EventTrackerData.mdf Last updated: 6/2/2020 11:12:16 AM
EventTrackerAlerts.mdf Last updated: 6/2/2020 12:54:56 PM
EventTrackerEDR.mdf Last updated: 6/2/2020 7:06:59 PM

Total no. of Event Cache files: 2 and CAB files: 185

Event Cache Information:
1591105006-14505-1-EventTracker.evc, 6/2/2020 7:06:46 PM
EtwArchive-14505-1591103444-EventTracker.mdb, 6/2/2020 7:06:34 PM
EtwArchive-516-1591104714-Default.mdb, 6/2/2020 7:02:30 PM

Status

Warning:
----------------Elasticsearch Information----------------

Figure 669

3. Right-click **Diagnostics Tool** on the taskbar.

   EventTracker opens the shortcut menu.

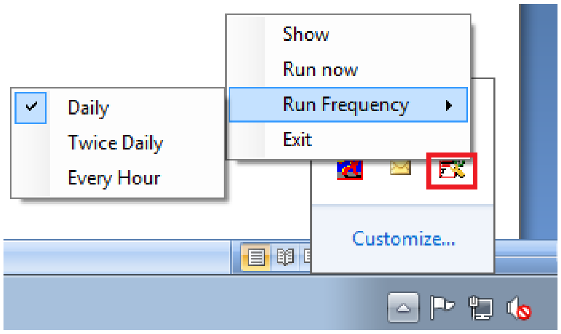


Figure 670

4. To set the frequency, move the mouse pointer over the **Run Frequency** option. EventTracker opens the options to set the frequency.

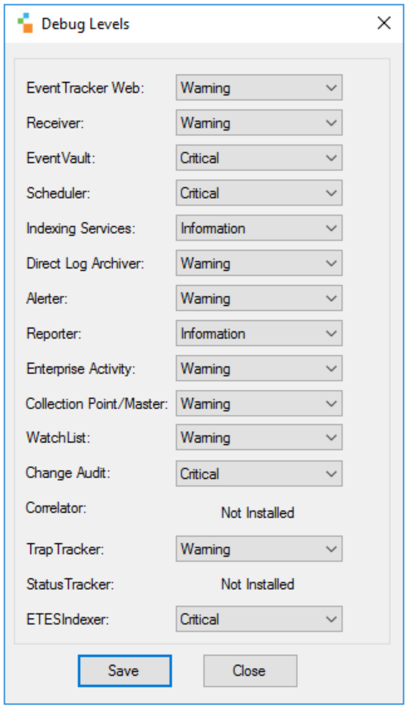
   If there is any error, **Diagnostics Tool** opens the diagnostics message balloon to get your attention.

31.1.2 Setting Debug Levels

This option helps to set log severity levels for EventTracker modules.

1 Launch **EventTracker Control Panel**, click **Diagnostics**, and then click **Debug** button.

Diagnostics Tool opens the Debug Levels window.



EventTracker Web:	Warning
Receiver:	Warning
EventVault:	Critical
Scheduler:	Critical
Indexing Services:	Information
Direct Log Archiver:	Warning
Alerter:	Warning
Reporter:	Information
Enterprise Activity:	Warning
Collection Point/Master:	Warning
WatchList:	Warning
Change Audit:	Critical
Correlator:	Not Installed
TrapTracker:	Warning
StatusTracker:	Not Installed
ETESIndexer:	Critical

Figure 671

EventTracker writes the log messages in the respective log files with the severity levels set.

EventTracker Module	Log File	Folder Path
EventTracker Web	*.*	...\Program Files\Prism Microsystems\EventTrackerWeb\Logs
EventTracker Web	EventTracker.log	...\Program Files\Prism Microsystems\EventTracker\Logs
Receiver	evtrxer*.txt Ex: evtrxlog-514.txt evtrxlog-14505.txt evtrxlog-14509.txt	...\Program Files\Prism Microsystems\EventTracker\Logs
EventVault	evtarlog.txt	...\Program Files\Prism Microsystems\EventTracker
Scheduler	etslog.txt	...\Program Files\Prism Microsystems\EventTracker
Indexing Services	Prism.Keyword.Indexer.*.log	...\Program Files\Prism Microsystems\EventTracker\Logs
Direct Log Archiver	LogFileParser.txt	...\Program Files\Prism Microsystems\EventTracker\Logs
Alerter	ETRSSLog.txt	...\Program Files\Prism Microsystems\EventTracker
Reporter	Prism.EventTracker.Report*.log	...\Program Files\Prism Microsystems\EventTracker\AdvancedReports\Logs
Enterprise Activity	etuserlog.txt	...\Program Files\Prism Microsystems\EventTracker\Logs
Collection Point/Master	evtCPlog.txt	...\Program Files\Prism Microsystems\EventTracker
Change Audit	*.*	...\Program Files\Prism Microsystems\WCWindows\Logs
Correlator	etcorlog.txt	...\Program Files\Prism Microsystems\EventTracker\ETCorrel
TrapTracker	evtrxlog.txt	...\Program Files\Prism Microsystems\TrapTracker

3 Select appropriately in the relevant fields.

4 Click **Save**.

31.1.3 Obfuscating 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, launch **EventTracker Control Panel.**

2 Click **Diagnostics**, and then click the **Obfuscate Output** checkbox.

Diagnostics Tool opens Masking Configuration window.

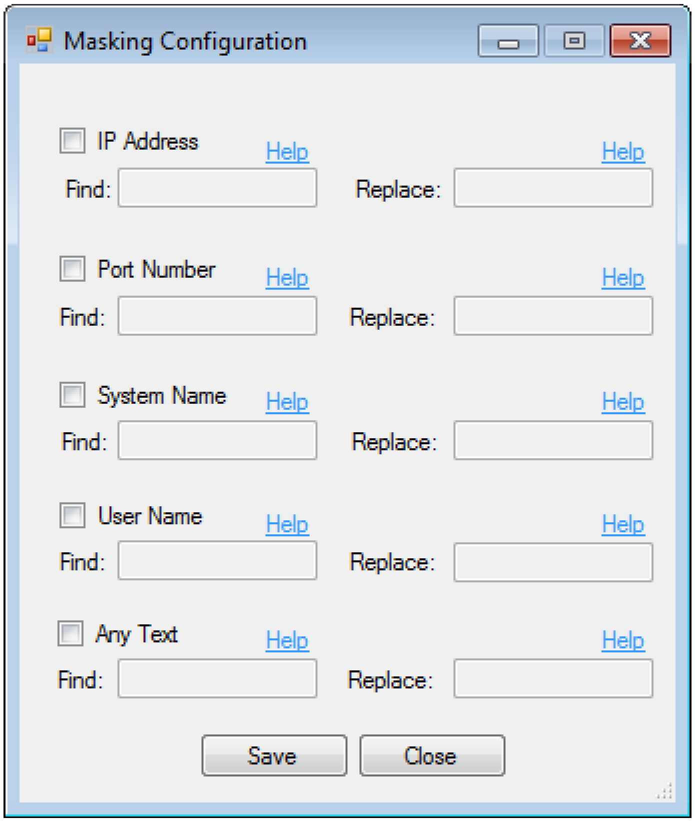


Figure 672

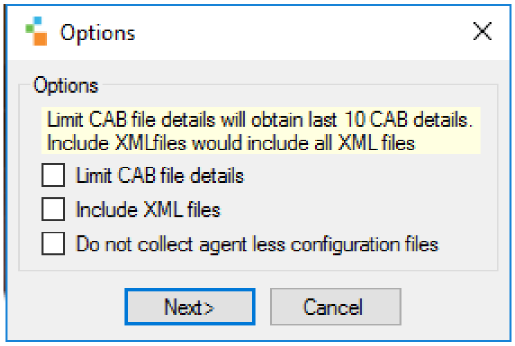
3 Move the mouse pointer over the **Help** hyperlink to view help tips. Select the appropriate checkbox.

4 Click **Save** and then click **OK**.

Diagnostics Tool enables the Edit Configuration button.

5 Click **E-mail** to send log files and configuration files for debugging.

Diagnostics Tool opens the message box indicating to **Limit CAB file details** and/or **Include XML files**.



Options

Options

Limit CAB file details will obtain last 10 CAB details.
Include XMLfiles would include all XML files

□ Limit CAB file details

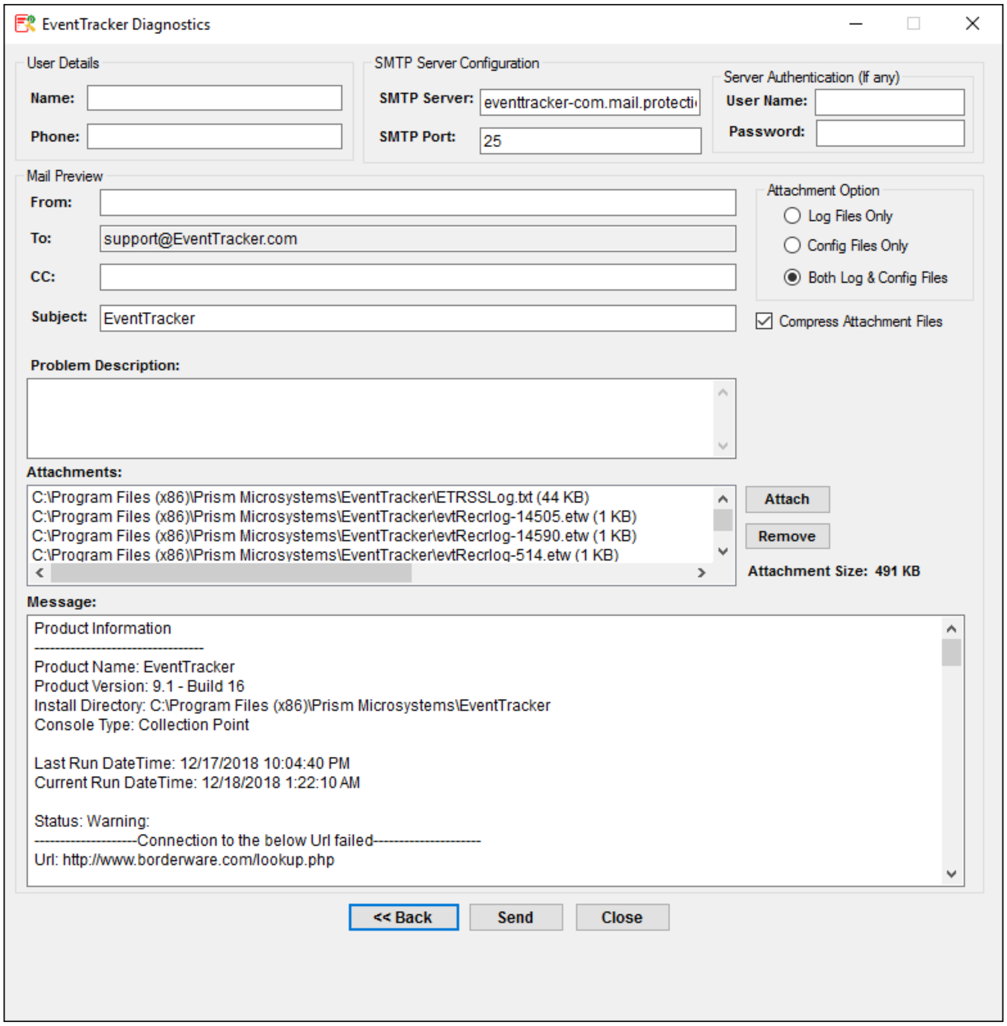
□ Include XML files

□ Do not collect agent less configuration files

Figure 673

6 Click **Next>**.

Diagnostics Tool opens the EventTracker Diagnostics window with more mailing options.



EventTracker Diagnostics

User Details

Name:

Phone:

SMTP Server Configuration

SMTP Server: eventtracker-com.mail.protecti

SMTP Port: 25

Server Authentication (If any)

User Name:

Password:

Mail Preview

From:

To: support@EventTracker.com

CC:

Subject: EventTracker

Attachment Option

○ Log Files Only

○ Config Files Only

● Both Log & Config Files

☑ Compress Attachment Files

Problem Description:

Attachments:

```
C:\Program Files (x86)\Prism Microsystems\EventTracker\ETRSSLog.txt (44 KB)
C:\Program Files (x86)\Prism Microsystems\EventTracker\evtRecrlog-14505.etw (1 KB)
C:\Program Files (x86)\Prism Microsystems\EventTracker\evtRecrlog-14590.etw (1 KB)
C:\Program Files (x86)\Prism Microsystems\EventTracker\evtRecrlog-514.etw (1 KB)
```

Attachment Size: 491 KB

Message:

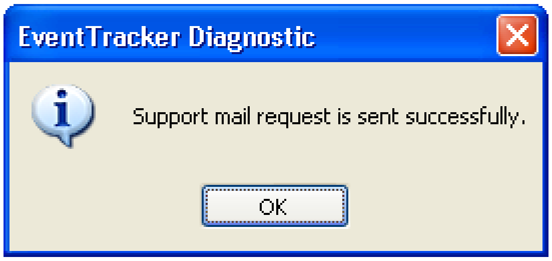
```
Product Information
--------------------------------
Product Name: EventTracker
Product Version: 9.1 - Build 16
Install Directory: C:\Program Files (x86)\Prism Microsystems\EventTracker
Console Type: Collection Point

Last Run DateTime: 12/17/2018 10:04:40 PM
Current Run DateTime: 12/18/2018 1:22:10 AM

Status: Warning:
--------------------Connection to the below Url failed--------------------
Url: http://www.borderware.com/lookup.php
```

Figure 674

7 Enter/select appropriate data in the relevant fields.

8 Click **Send**.

EventTracker Diagnostic window opens the message.

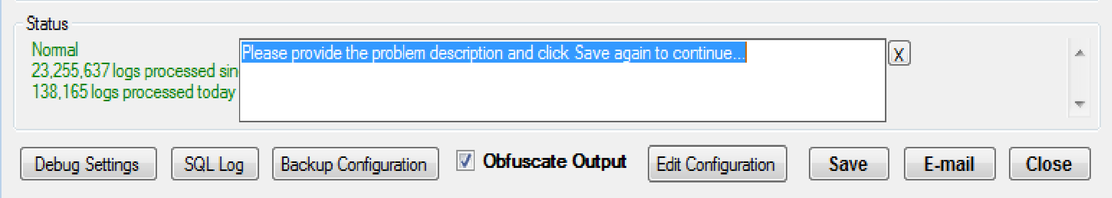


Support mail request is sent successfully.

Figure 675

You can also save the log files and configuration files as a compressed file for future reference.

9 Click **Save** on the EventTracker Diagnostics window.



Normal
23,255,637 logs processed sin
138,165 logs processed today

Please provide the problem description and click Save again to continue...

☑ Obfuscate Output

Figure 676

10 Type the problem description in the provided field.

11 Click **Save**.

31.1.4 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 opens the diagnostic alert indicator.

2 Click 🔔2 icon.

EventTracker opens the File Download pop-up window to open or save the diagnostic report.

3 Click **Open** to view the report.

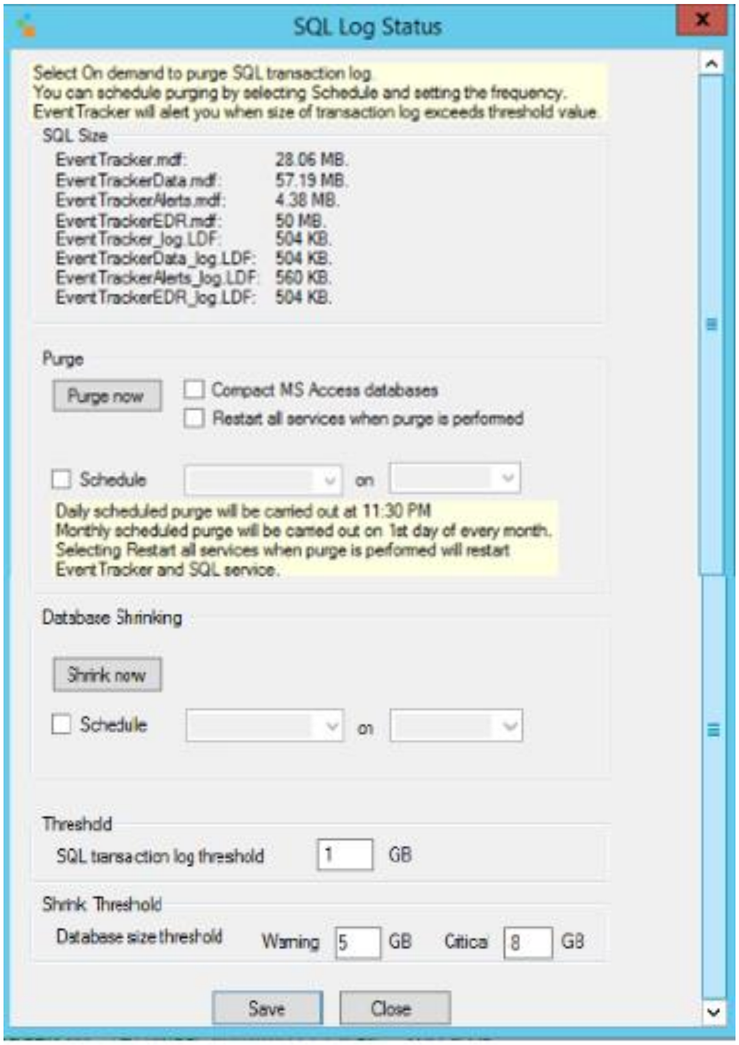
EventTracker opens the report in the Notepad.

31.2 SQL Log

This option provides the status and size of SQL logs. You can purge SQL transaction logs at any time. It also alerts when the size of SQL logs exceeds the threshold value.

1 Open **EventTracker Control Panel,** click **Diagnostics**, and then click **SQL Log**.

SQL Log Status window opens.



Select On demand to purge SQL transaction log
You can schedule purging by selecting Schedule and setting the frequency.
EventTracker will alert you when size of transaction log exceeds threshold value.

SQL Size

EventTracker.mdf:	28.06 MB.
EventTrackerData.mdf:	57.19 MB.
EventTrackerAlerts.mdf:	4.38 MB.
EventTrackerEDR.mdf:	50 MB.
EventTracker_log.LDF:	504 KB.
EventTrackerData_log.LDF:	504 KB.
EventTrackerAlerts_log.LDF:	560 KB.
EventTrackerEDR_log.LDF:	504 KB.

Purge

□ Compact MS Access databases
□ Restart all services when purge is performed

□ Schedule on

Daily scheduled purge will be carried out at 11:30 PM
Monthly scheduled purge will be carried out on 1st day of every month.
Selecting Restart all services when purge is performed will restart EventTracker and SQL service.

Database Shrinking

□ Schedule on

Threshold

SQL transaction log threshold 1 GB

Shrink Threshold

Database size threshold Warning 5 GB Critical 8 GB

Figure 677

2 To purge data immediately, select **Purge now**.

(OR)

Select **Schedule** option, and then select **Hourly/Daily/Weekly/Monthly** from drop down.

3 To shrink data immediately, select **Shrink now**.

Select **Schedule** option, and then select **Hourly/Daily/Weekly/Monthly** from drop down to shrink data at the scheduled time.

4 Shrink Threshold

If the EventTracker databases cross the warning and critical threshold it displays in **View** full status that database has crossed warning or critical.

For persist report if it crosses critical limit it shows in **View** full status that persist report has crossed the critical limit.

5 Enter the **SQL transaction log threshold** value (in GB), and then click **Save**.

31.3 Backup Configuration option

This option helps to take a backup of the files when required.

1 Open **EventTracker Control Panel,** click **Diagnostics**, and then click **Backup**.

Backup & Restore window opens.

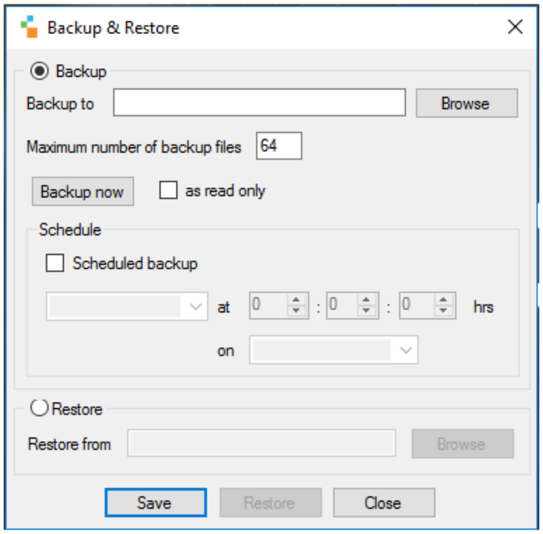


Figure 678

2 To backup data, click **Browse** and select the required location.

Browse for Folder window opens.

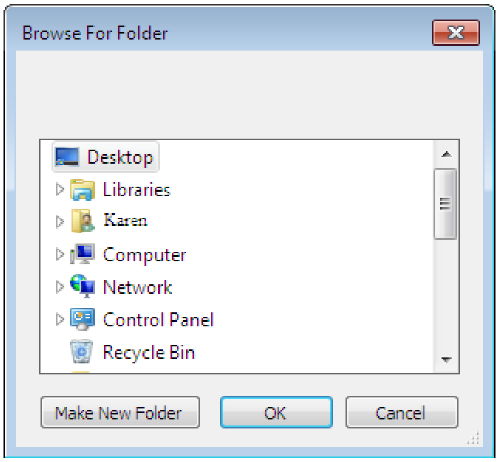


Figure 679

3 Select the required location and then click **OK**.

4 To backup data immediately, click **Backup now**.

(OR)

To schedule a backup, select **Scheduled backup** option. Enter the date and time.

5 Click **Save**.

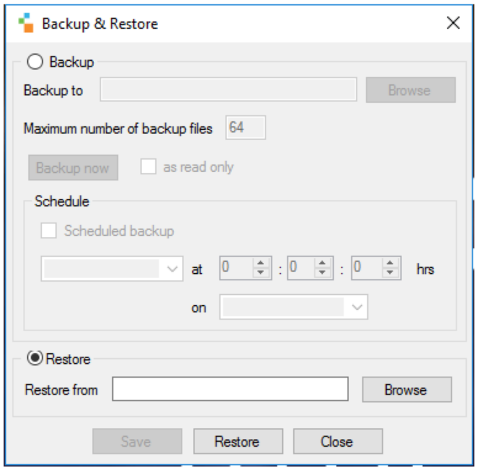
The file is saved in .bkp format in the respective location.

31.4 Restore Configuration option

This option helps to restore the files when required.

1 Open **EventTracker Control Panel,** click **Diagnostics**, and then click the **Backup** button.

Backup & Restore window displays.



Maximum number of backup files 64

at 0 : 0 : 0 hrs

● Restore

Figure 680

2 Select **Restore** option, and then select **Browse** button.

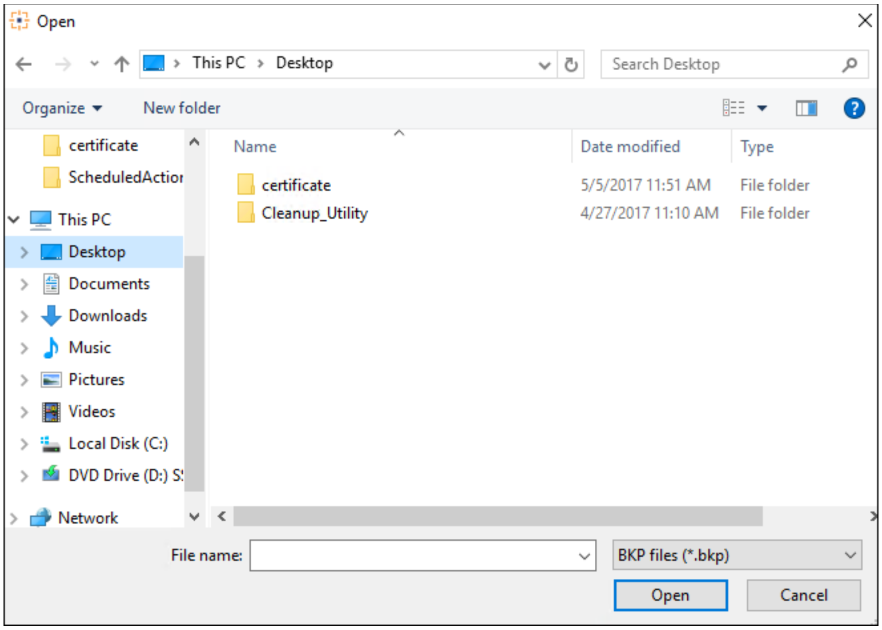


Figure 681

3 Select the location of the file (i.e. *.bkp file) to restore and then click **Open**.

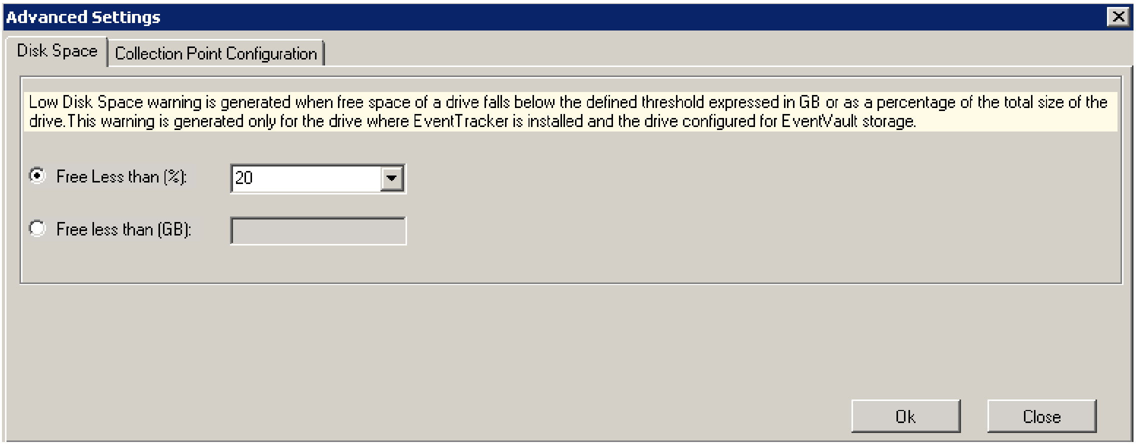
4 Click **Restore**.

31.5 Advanced Settings

If a Collection Point has been configured and no CAB files have been received for a specified duration, then an alert can be generated.

1 Open **EventTracker Control Panel,** click **Diagnostics**, and then click **Advanced**.

Advanced Settings window opens:



Advanced Settings

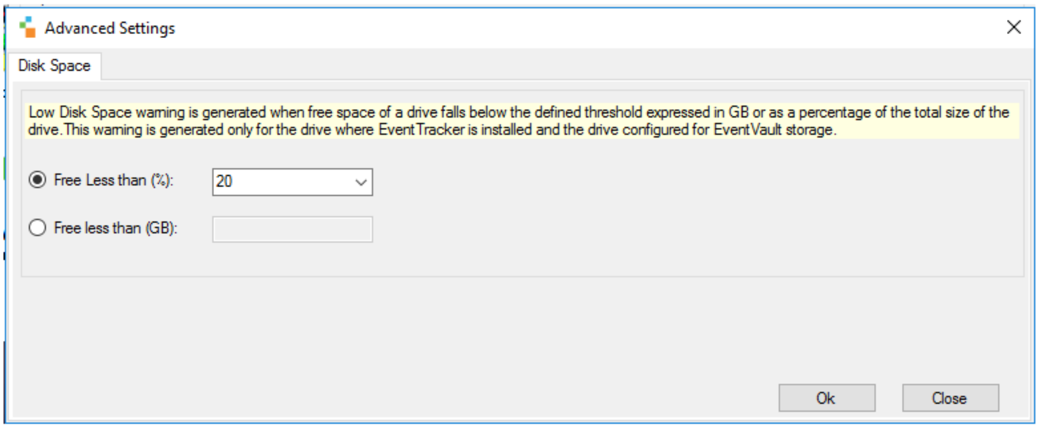
Disk Space | Collection Point Configuration

Low Disk Space warning is generated when free space of a drive falls below the defined threshold expressed in GB or as a percentage of the total size of the drive.This warning is generated only for the drive where EventTracker is installed and the drive configured for EventVault storage.

● Free Less than (%): 20

○ Free less than (GB):

Figure 682(Collection Point Configuration tab not available)



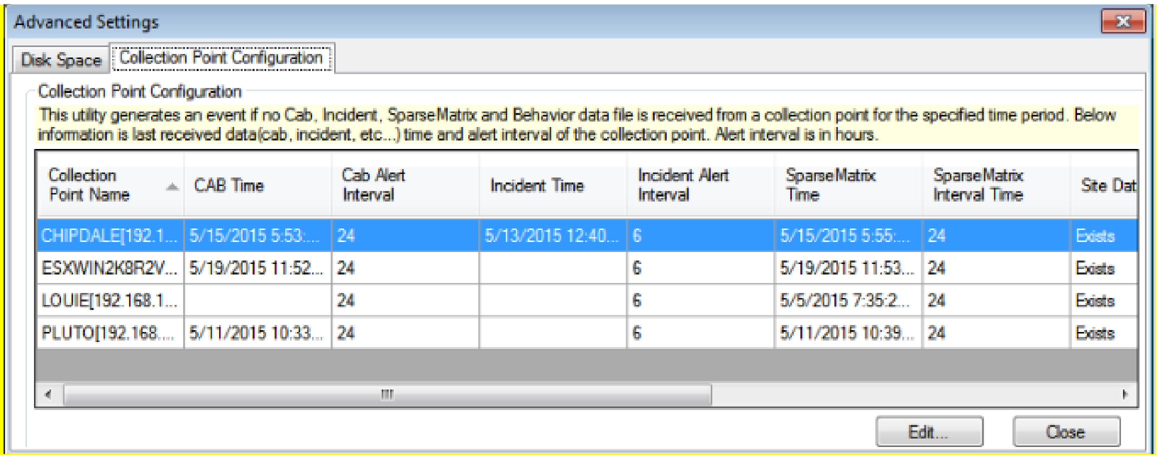
Low Disk Space warning is generated when free space of a drive falls below the defined threshold expressed in GB or as a percentage of the total size of the drive. This warning is generated only for the drive where EventTracker is installed and the drive configured for EventVault storage.

● Free Less than (%): 20

○ Free less than (GB):

Figure 683

2. Enter the Free disk Space as per your requirement by selecting from the dropdown list and click **OK**.
3. In the **Collection Point Configuration** pane, view the details of CPs configured for the CM.



Collection Point Configuration

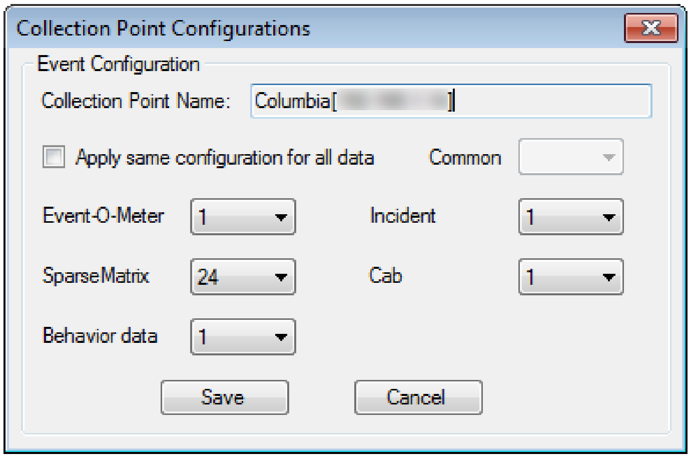
This utility generates an event if no Cab, Incident, SparseMatrix and Behavior data file is received from a collection point for the specified time period. Below information is last received data(cab, incident, etc...) time and alert interval of the collection point. Alert interval is in hours.

Collection Point Name	CAB Time	Cab Alert Interval	Incident Time	Incident Alert Interval	SparseMatrix Time	SparseMatrix Interval Time	Site Dat
CHIPDALE[192.1...	5/15/2015 5:53:...	24	5/13/2015 12:40...	6	5/15/2015 5:55:...	24	Exists
ESXWIN2K8R2V...	5/19/2015 11:52...	24		6	5/19/2015 11:53...	24	Exists
LOUIE[192.168.1...		24		6	5/5/2015 7:35:2...	24	Exists
PLUTO[192.168....	5/11/2015 10:33...	24		6	5/11/2015 10:39...	24	Exists

Figure 684

NOTE: For **Standard** console Type; the Collection Point Configuration pane is not available.

4. In **Collection Point Configuration** pane, click **Edit**.
   Collection Point Configurations window opens.



Collection Point Configurations

Event Configuration

Collection Point Name: Columbia[[redacted]]

☐ Apply same configuration for all data   Common

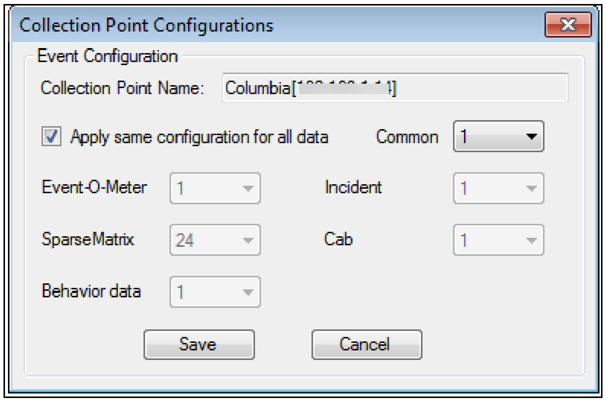
Event-O-Meter: 1   Incident: 1

SparseMatrix: 24   Cab: 1

Behavior data: 1

Figure 685

5. To specify different time interval, select the respective **Event-O-Meter, SparseMatrix, Behavior data, Incident, Cab** drop down and select the duration.
6. To select a common time interval, select **Apply same configuration for all data** option, select **Common** drop down, and then select duration (in hours).



Collection Point Configurations

Event Configuration

Collection Point Name: Columbia[[redacted]]

☑ Apply same configuration for all data   Common: 1

Event-O-Meter: 1   Incident: 1

SparseMatrix: 24   Cab: 1

Behavior data: 1

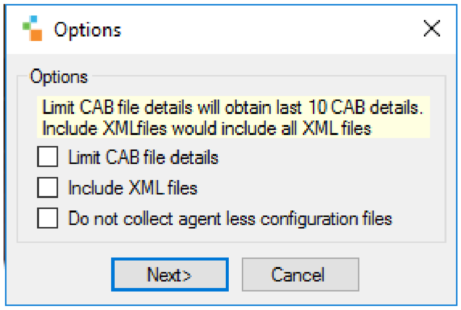
Figure 686

7. Click **Save**.

31.5.1 Do not collect agent less configuration files

If Collection Master should not collect agent less configuration files, then select the option not to collect agent less configuration files.

1. Click **Save**.



Options

Options

Limit CAB file details will obtain last 10 CAB details.
Include XMLfiles would include all XML files

☐ Limit CAB file details

☐ Include XML files

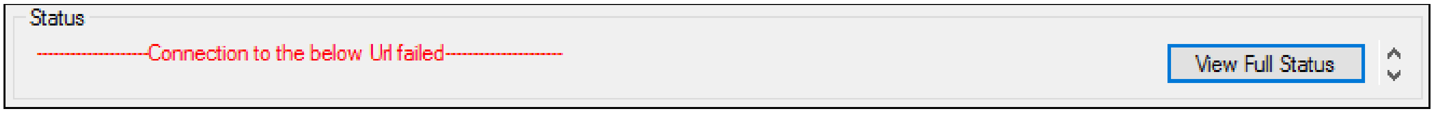
☐ Do not collect agent less configuration files

Figure 687

2. Select **Do not collect agent less configuration files** option, and then click **Next>**.
3. Enter the description, and then click **Save**.

31.6 Status Pane

If the respective alert is triggered, then a notification is displayed in EventTracker Diagnostics Status pane. Refer the figure below.



Status

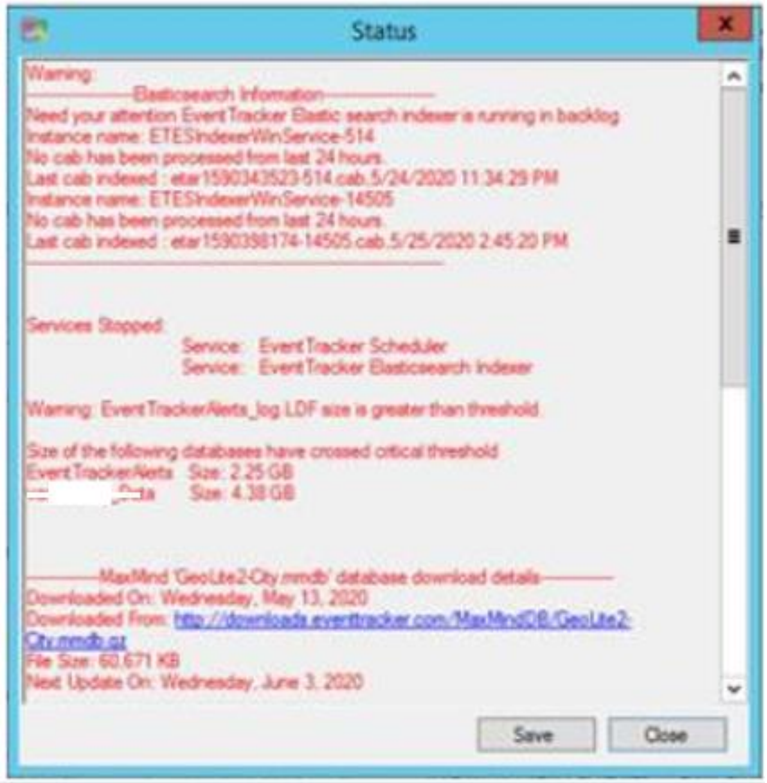
-------------------Connection to the below Url failed--------------------

Figure 688

To save the Diagnostics status,

- Click **View Full Status**.

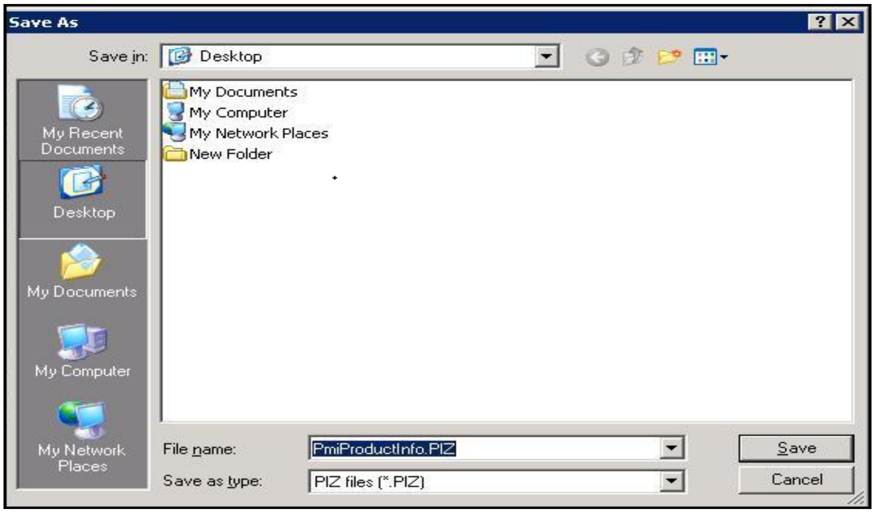
The Status Page opens.



```
Warning:
——————Elasticsearch Information——————
Need your attention EventTracker Elastic search indexer is running in backlog
Instance name: ETESIndexerWinService-514
No cab has been processed from last 24 hours.
Last cab indexed : etar1590343523-514.cab.5/24/2020 11:34:29 PM
Instance name: ETESIndexerWinService-14505
No cab has been processed from last 24 hours.
Last cab indexed : etar1590398174-14505.cab.5/25/2020 2:45:20 PM
————————————————————————


Services Stopped:
                    Service:   EventTracker Scheduler
                    Service:   EventTracker Elasticsearch Indexer

Warning: EventTrackerAlerts_log LDF size is greater than threshold

Size of the following databases have crossed critical threshold
EventTrackerAlerts   Size: 2.25 GB
[redacted]ta         Size: 4.38 GB


——————MaxMind 'GeoLite2-City.mmdb' database download details——————
Downloaded On: Wednesday, May 13, 2020
Downloaded From: http://downloads.eventtracker.com/MaxMindDB/GeoLite2-City.mmdb.gz
File Size: 60,671 KB
Next Update On: Wednesday, June 3, 2020
```

Figure 689

- Click **Save** and save the diagnostics in your system with a file name as shown in the figure below:



File name: PmiProductInfo.PIZ

Save as type: PIZ files (*.PIZ)

Figure 690

32. License Manager

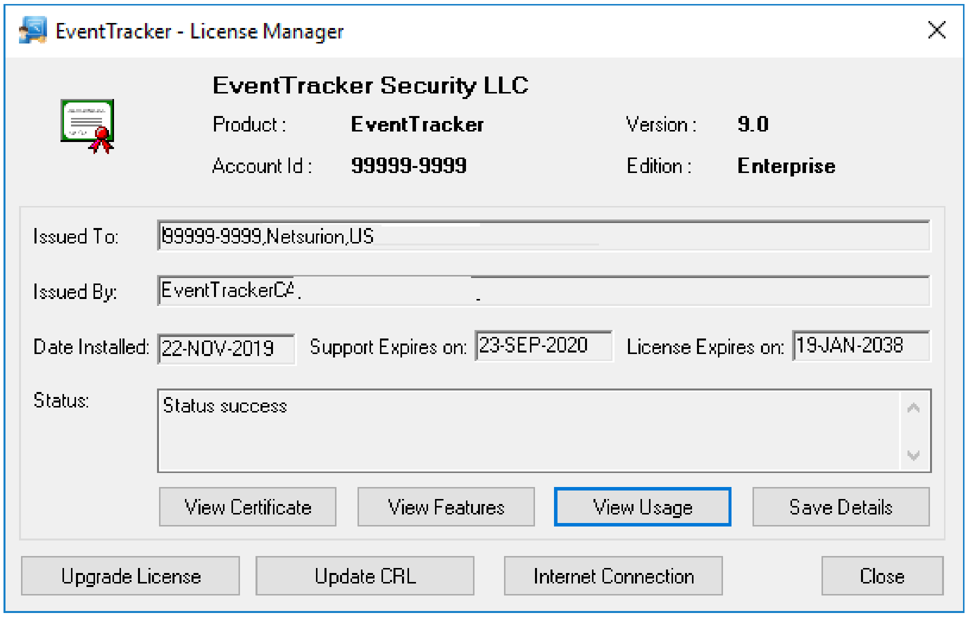
In this chapter, you will learn about:

- Viewing, updating, upgrading License Manager

32.1 License Manager option

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.



EventTracker - License Manager

EventTracker Security LLC

Product : EventTracker

Version : 9.0

Account Id : 99999-9999

Edition : Enterprise

Issued To: 99999-9999,Netsurion,US

Issued By: EventTrackerCA

Date Installed: 22-NOV-2019

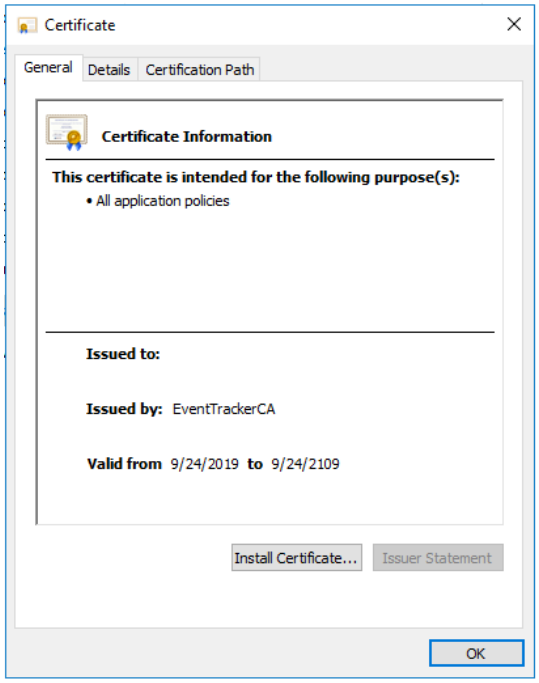
Support Expires on: 23-SEP-2020

License Expires on: 19-JAN-2038

Status: Status success

Figure 691

EventTracker opens the **Windows Certificate Viewer**.



Certificate

Certificate Information

This certificate is intended for the following purpose(s):

- All application policies

Issued to:

Issued by: EventTrackerCA

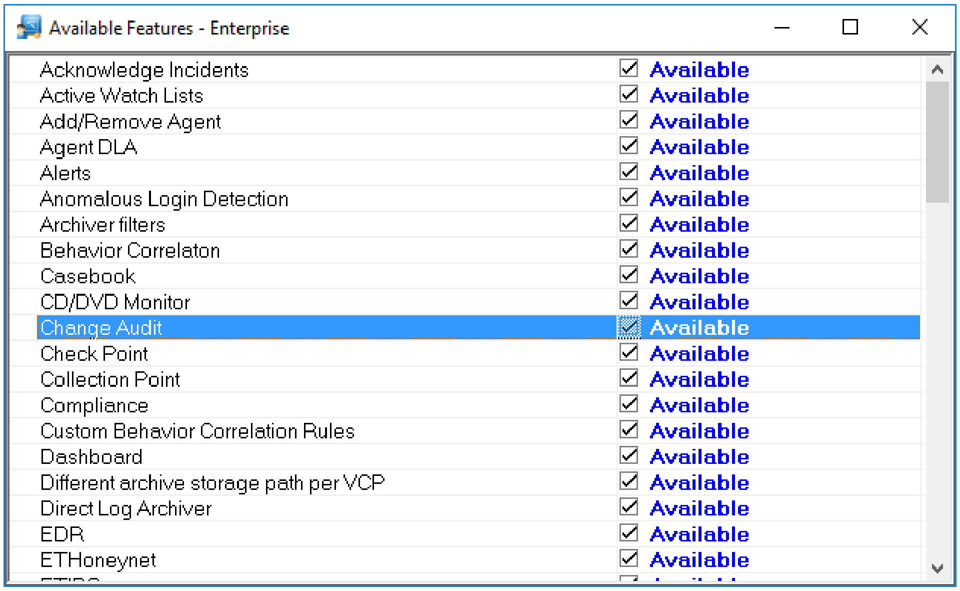
Valid from 9/24/2019 to 9/24/2109

Figure 692

Click **Install Certificate** to import certificate to a certificate store.

A certificate store is the system area where the certificates are kept.

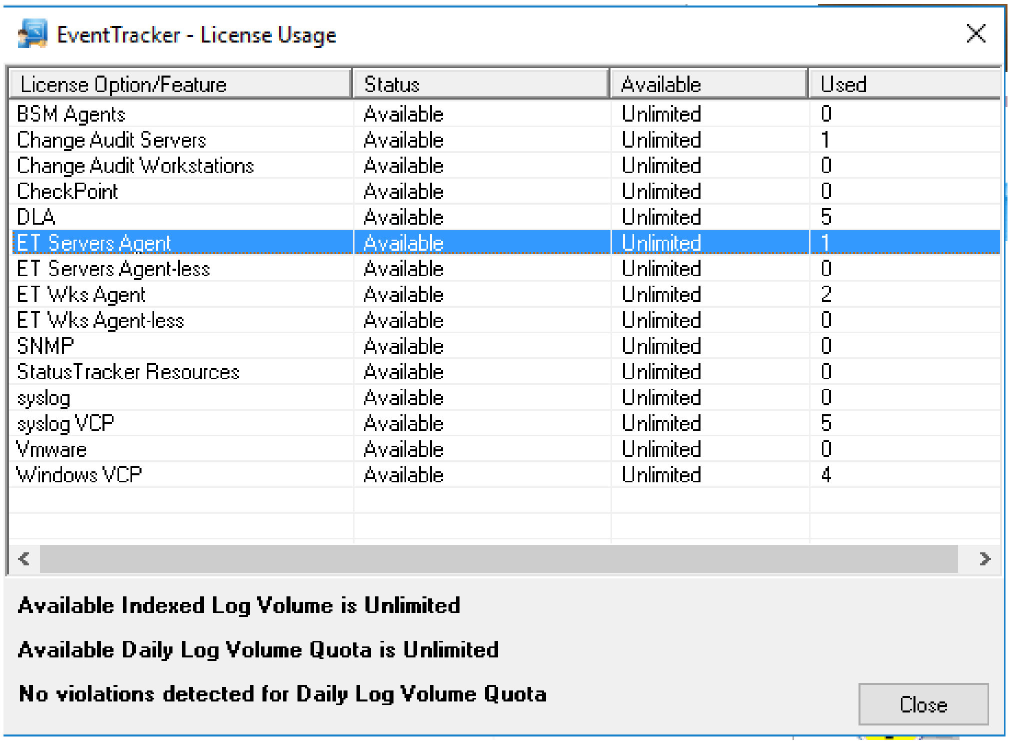
2 Click **View Features** on the License Manager window.



Acknowledge Incidents	☑	Available
Active Watch Lists	☑	Available
Add/Remove Agent	☑	Available
Agent DLA	☑	Available
Alerts	☑	Available
Anomalous Login Detection	☑	Available
Archiver filters	☑	Available
Behavior Correlaton	☑	Available
Casebook	☑	Available
CD/DVD Monitor	☑	Available
Change Audit	☑	Available
Check Point	☑	Available
Collection Point	☑	Available
Compliance	☑	Available
Custom Behavior Correlation Rules	☑	Available
Dashboard	☑	Available
Different archive storage path per VCP	☑	Available
Direct Log Archiver	☑	Available
EDR	☑	Available
ETHoneynet	☑	Available

Figure 693

3 Click **View License Usage**.



License Option/Feature	Status	Available	Used
BSM Agents	Available	Unlimited	0
Change Audit Servers	Available	Unlimited	1
Change Audit Workstations	Available	Unlimited	0
CheckPoint	Available	Unlimited	0
DLA	Available	Unlimited	5
ET Servers Agent	Available	Unlimited	1
ET Servers Agent-less	Available	Unlimited	0
ET Wks Agent	Available	Unlimited	2
ET Wks Agent-less	Available	Unlimited	0
SNMP	Available	Unlimited	0
StatusTracker Resources	Available	Unlimited	0
syslog	Available	Unlimited	0
syslog VCP	Available	Unlimited	5
Vmware	Available	Unlimited	0
Windows VCP	Available	Unlimited	4

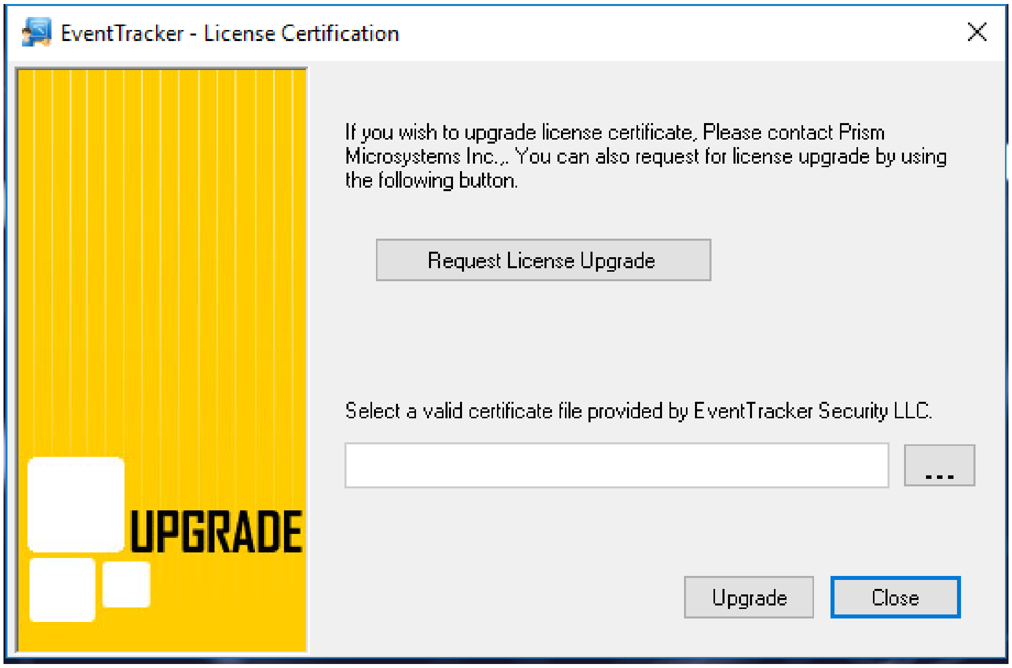
Available Indexed Log Volume is Unlimited

Available Daily Log Volume Quota is Unlimited

No violations detected for Daily Log Volume Quota

Figure 694

4 Click **Upgrade License**.



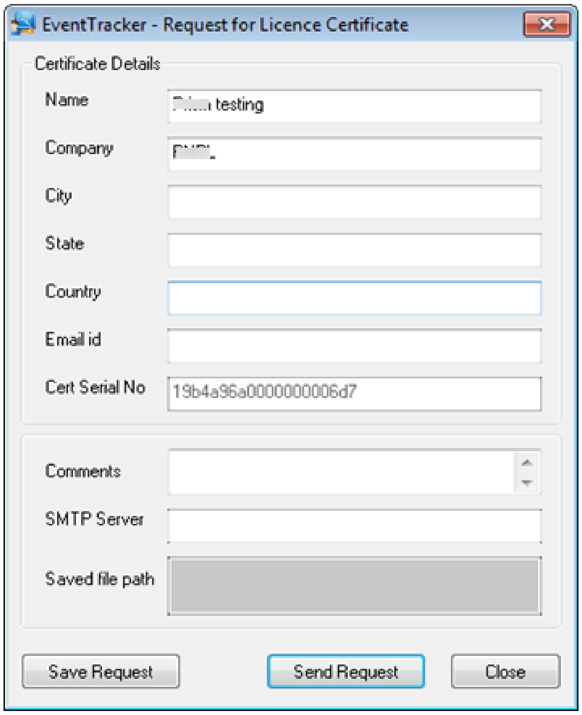
EventTracker - License Certification

If you wish to upgrade license certificate, Please contact Prism Microsystems Inc.,. You can also request for license upgrade by using the following button.

Select a valid certificate file provided by EventTracker Security LLC.

Figure 695

5 Click **Request License Upgrade** to request a new license to upgrade.



EventTracker - Request for Licence Certificate

Certificate Details

Name	[redacted] testing
Company	[redacted]
City	
State	
Country	
Email id	
Cert Serial No	19b4a96a0000000006d7
Comments	
SMTP Server	
Saved file path	

Figure 696

6. Enter appropriate data in the relevant fields.
7. Click **Save Request** to save the request in Notepad and send it later.
8. 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.

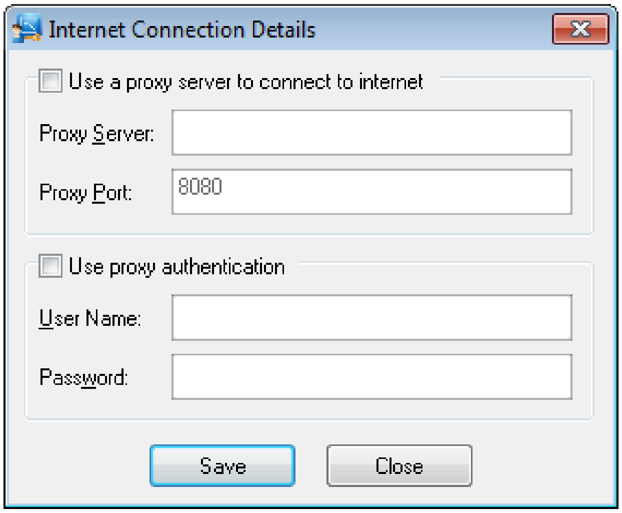
   Click **Open** and then click **Upgrade**.
9. Click **Update CRL** on the **License Manager** window.

   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 repeatedly.

   While installing EventTracker, CRL is downloaded to the default install path typically ...\Program Files\Prism Microsystems

   EventTracker opens the Open dialog box.
10. Select the CRL file and then click **Open**.
11. Click **Internet Connection**. Enter relevant data and then click **Save**.



Internet Connection Details

☐ Use a proxy server to connect to internet

Proxy Server:

Proxy Port: 8080

☐ Use proxy authentication

User Name:

Password:

Figure 697

12. To close License Manager, click **Close**.

33. Export Import Utility

In this chapter, you will learn how to:

- Export and Import
    - ❖ Categories
    - ❖ Filters
    - ❖ Alerts
    - ❖ Systems and Groups
    - ❖ Reports
    - ❖ Behavior Correlation
    - ❖ Token Value
- Import SCAP

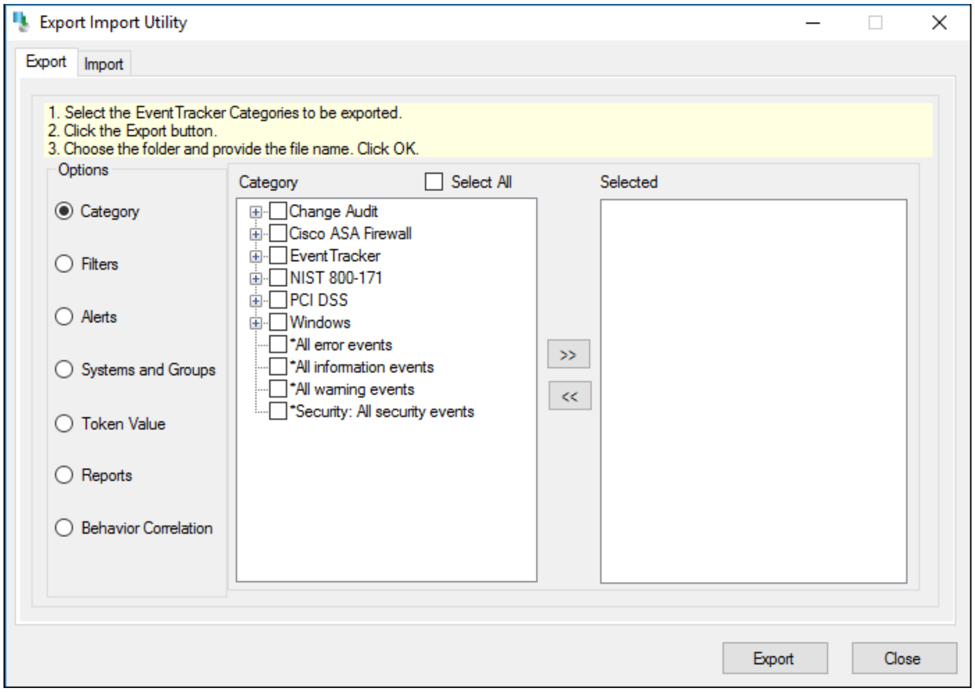
33.1 Exporting and Importing Utility

Export and Import Utility enables you to export/import custom Categories, Filters, Alerts, Reports, Domains, Systems, Token Value and Behavior Correlation 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.

33.1.1 Exporting Categories

1 To export categories, click **Start**, select **All Programs**, and then **select Prism Microsystems.**

2 Select **EventTracker**, select **EventTracker Control Panel**, and then select **Export Import Utility**.
EventTracker opens the **Export Import Utility** window.



1. Select the EventTracker Categories to be exported.
2. Click the Export button.
3. Choose the folder and provide the file name. Click OK.

Options

● Category
○ Filters
○ Alerts
○ Systems and Groups
○ Token Value
○ Reports
○ Behavior Correlation

Category ☐ Select All

- ☐ Change Audit
- ☐ Cisco ASA Firewall
- ☐ EventTracker
- ☐ NIST 800-171
- ☐ PCI DSS
- ☐ Windows
- ☐ *All error events
- ☐ *All information events
- ☐ *All warning events
- ☐ *Security: All security events

Selected

Figure 698

Field	Description
Category	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.
Selected	To remove Category group(s) / Category(s), clear the respective checkbox(s) in the Category list.

Table 71

3 In **Export** tab, select the required **Category**, click the **>>** button and then click **Export**.

EventTracker opens 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 opens the **Export Import Utility** message box.

6 Click **OK**.

33.1.2 Exporting Filters

1 To export filters, click **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.

Field	Description
Filters	Select a Filter / Filters from this list. Click Add-> to add filters to the Selected list. Click Add All>> to add all Filters to the Selected list. To select multiple filters, hold down the CTRL key on your keyboard and click the filters.
Selected	Select a Filter / Filters from this list. Click <-Remove to remove the selected Filter / Filters from this list. Click <<Remove All to remove all Filters from this list.

Table 72

4 Select the required **Filters** and then click **Export**.
5 Type the file name in the **File Name** field.

🗎 NOTE

The valid file extension is .isfil.

6 Click **Save**.

EventTracker opens the Export Import Utility message box.

7 Click **OK**.

33.1.3 Exporting Alerts

1 To export alerts, click **Start** button, select **All Programs**, and then select **Prism Microsystems**.
2 Select **EventTracker**, select **EventTracker Control Panel** and then select **Export Import Utility**.

Field	Description
Export E-mail Settings	Select this checkbox to export Alerts along with the corresponding e-mail settings, if any.
Alerts	Select an Alert / Alerts from this list. Click Add-> to add to the Selected list. Click Add All>> to add all Alerts to the Selected list. To select multiple Alerts, hold down the CTRL key on your keyboard and click Alerts.
Selected	Select an Alert / Alerts from this list. Click <-Remove to remove the selected Alert / Alerts from this list. Click <<Remove All to remove all Alerts from this list.

Table 73

3 Select the required alerts and then click **Export**.

4 Type the file name in the **File Name** field.

🗎 NOTE

The valid file extension is .isalt.

5 Click **Save**.

EventTracker opens the Export Import Utility message box.

6 Click **OK**.

33.1.4 Exporting System Groups

1 To export system groups, click = **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 opens the systems groups.

Field	Description
Systems and Groups	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.
Selected	To remove system group(s) / system(s), clear the respective checkbox(s) in the Systems and Groups list.

Table 74

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.

6 Click **Save**.

EventTracker opens the Export Import Utility message box.

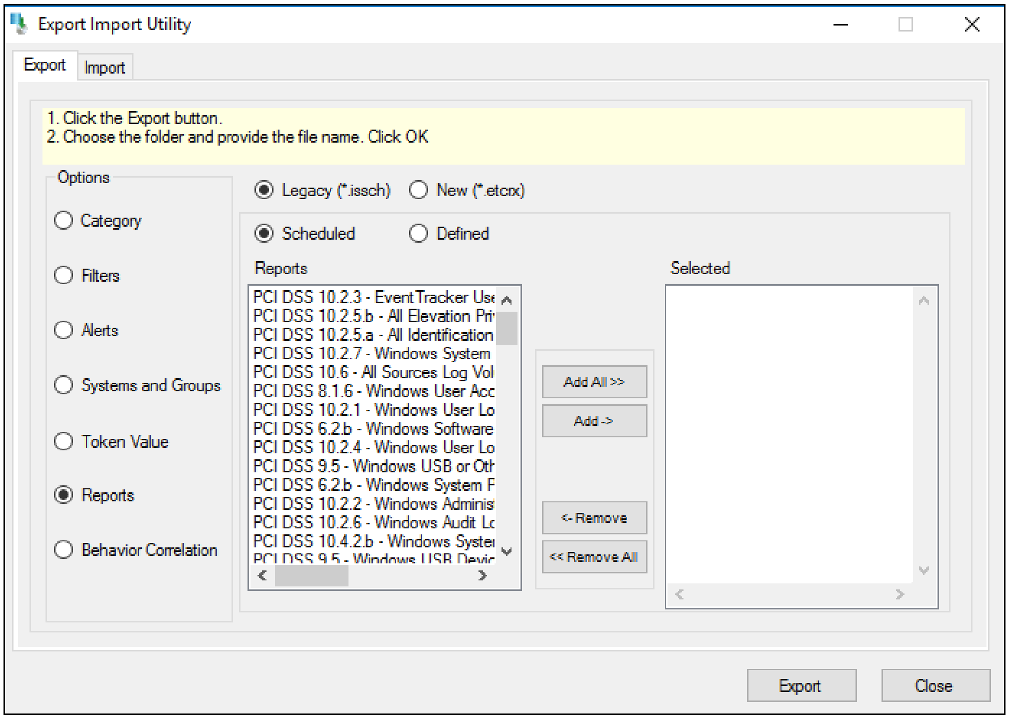
7 Click **OK**.

33.1.5 Exporting Reports

1 To export scheduled reports, click **Start**, select **All Programs**, and then select **Prism Microsystems.**

2 Select **EventTracker**, select **EventTracker Control Panel** and then select **Export Import Utility**.

3 Select the **Reports** option.


Export Import Utility

Export | Import

1. Click the Export button.
2. Choose the folder and provide the file name. Click OK

Options

○ Category
○ Filters
○ Alerts
○ Systems and Groups
○ Token Value
● Reports
○ Behavior Correlation

● Legacy (*.issch) ○ New (*.etcrx)

● Scheduled ○ Defined

Reports

PCI DSS 10.2.3 - EventTracker Use
PCI DSS 10.2.5.b - All Elevation Pri
PCI DSS 10.2.5.a - All Identification
PCI DSS 10.2.7 - Windows System
PCI DSS 10.6 - All Sources Log Vol
PCI DSS 8.1.6 - Windows User Acc
PCI DSS 10.2.1 - Windows User Lo
PCI DSS 6.2.b - Windows Software
PCI DSS 10.2.4 - Windows User Lo
PCI DSS 9.5 - Windows USB or Oth
PCI DSS 6.2.b - Windows System F
PCI DSS 10.2.2 - Windows Adminis
PCI DSS 10.2.6 - Windows Audit Lo
PCI DSS 10.4.2.b - Windows Syste
PCI DSS 9.5 - Windows USB Devic

Selected

Figure 699

Field	Description
Reports	Select a report from this list by selecting **Scheduled or Defined.** Click Add-> to add to the Selected list. Click Add All>> to add all Scheduled/ Defined reports to the Selected list. To select multiple Scheduled/Defined reports, hold down the CTRL key on your keyboard and click Scheduled/Defined reports.
Selected	Select a Scheduled report / Defined report from this list. Click <-Remove to remove the selected Scheduled report / reports from this list. Click <<Remove All to remove all Scheduled/Defined reports from this list.

Table 75

NOTE

The valid file extension for Old type is .issch and for New type is .etcrx. Select the option as per extension.

For Legacy with extension .issch,

1 Select the Legacy option.
2 Select the required **Scheduled /Defined Report** option, and then click **Export**.

3 Type the file name in the **File name** field.

4 Click **Save**.

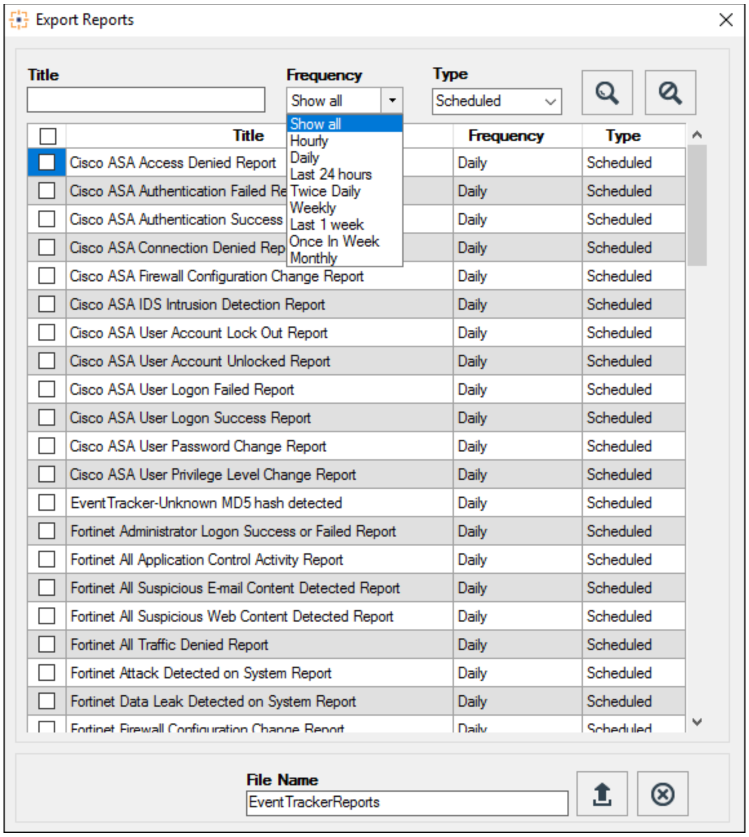
EventTracker opens the below message box:

5 Click **OK**.

For the option **New type** with extension .etcrx,

1 Select the option New type

The export report window opens:



Title:

Frequency: Show all

Type: Scheduled

☐	Title	Frequency	Type
☐	Cisco ASA Access Denied Report	Daily	Scheduled
☐	Cisco ASA Authentication Failed Re	Daily	Scheduled
☐	Cisco ASA Authentication Success	Daily	Scheduled
☐	Cisco ASA Connection Denied Rep	Daily	Scheduled
☐	Cisco ASA Firewall Configuration Change Report	Daily	Scheduled
☐	Cisco ASA IDS Intrusion Detection Report	Daily	Scheduled
☐	Cisco ASA User Account Lock Out Report	Daily	Scheduled
☐	Cisco ASA User Account Unlocked Report	Daily	Scheduled
☐	Cisco ASA User Logon Failed Report	Daily	Scheduled
☐	Cisco ASA User Logon Success Report	Daily	Scheduled
☐	Cisco ASA User Password Change Report	Daily	Scheduled
☐	Cisco ASA User Privilege Level Change Report	Daily	Scheduled
☐	EventTracker-Unknown MD5 hash detected	Daily	Scheduled
☐	Fortinet Administrator Logon Success or Failed Report	Daily	Scheduled
☐	Fortinet All Application Control Activity Report	Daily	Scheduled
☐	Fortinet All Suspicious E-mail Content Detected Report	Daily	Scheduled
☐	Fortinet All Suspicious Web Content Detected Report	Daily	Scheduled
☐	Fortinet All Traffic Denied Report	Daily	Scheduled
☐	Fortinet Attack Detected on System Report	Daily	Scheduled
☐	Fortinet Data Leak Detected on System Report	Daily	Scheduled
☐	Fortinet Firewall Configuration Change Report	Daily	Scheduled

File Name: EventTrackerReports

Figure 700

2 In the **Title** field, enter a suitable title.

3 In the **Frequency** field, select the option **hourly/daily/last 24 hours/ twice daily/weekly/last 1 week/once in week/monthly,** from the dropdown list.

4 In the **Type** field, select the report type from the dropdown list and click the search logo .

5 Select the reports to be exported by clicking the checkbox.

6 In the File Name field, enter the report name and select the export icon .

7 Click **Save**.

EventTracker opens the Export Import Utility message box.

3 Click **OK**.

33.1.6 Exporting Machine Learning

1 To export Machine Learning Jobs, click **Start**, select **All Programs**, and then select **Prism Microsystems.**

2 Select **EventTracker**, select **EventTracker Control Panel** and then select **Export Import Utility**.

3 Select the **MachineLearning** option.

Field	Description
Machine Learning	Select a Machine Learning from this list. Click Add-> to add to the Selected list. Click Add All>> to add all Machine Learning Jobs to the Selected list. To select multiple Machine Learning, hold down the CTRL key on your keyboard and click Machine Learning.
Selected	Select a Machine Learning from this list. Click <-Remove to remove the selected Machine Learning from this list. Click <<Remove All to remove all Machine Learning Jobs from this list.

Table 76

4 Click **Export**.

5 Type the file name in the **File name** field.

🗎 NOTE

The valid file extension is .isrule.

6 Click **Save**.

EventTracker opens the Export Import Utility message box.

7 Click **OK**.

33.1.7 Exporting Token Value

1 To export Machine Learning Jobs, click **Start**, 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.

Field	Description
Token Value	Select a Token Value from this list. Click Add-> to add to the Selected list. Click Add All>> to add all Machine Learning Jobs to the Selected list. To select multiple Token Values, hold down the CTRL key on your keyboard and click Token Value.
Selected	Select a Token Value from this list. Click <-Remove to remove the selected Token Value from this list. Click <<Remove All to remove all Token Value from this list.

Table 77

4 Click **Export**.

5 Type the file name in the **File name** field.

NOTE

The valid file extension is .istoken.

6 Click **Save**.

EventTracker opens the Export Import Utility message box.

7 Click **OK**.

33.1.8 Importing Categories

1 Click **Start** , 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 Browse ... .

EventTracker opens 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 opens the Export Import Utility message box.

8. Click **OK**.

33.1.9 Importing Filters

1. Click **Start** , 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 Browse [...].

   EventTracker opens 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 opens the Export Import Utility message box.

7. Click **OK**.

33.1.10 Importing Alerts

1. Click **Start**, 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 Browse [...] .

   EventTracker opens 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 **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 opens the Export Import Utility message box.

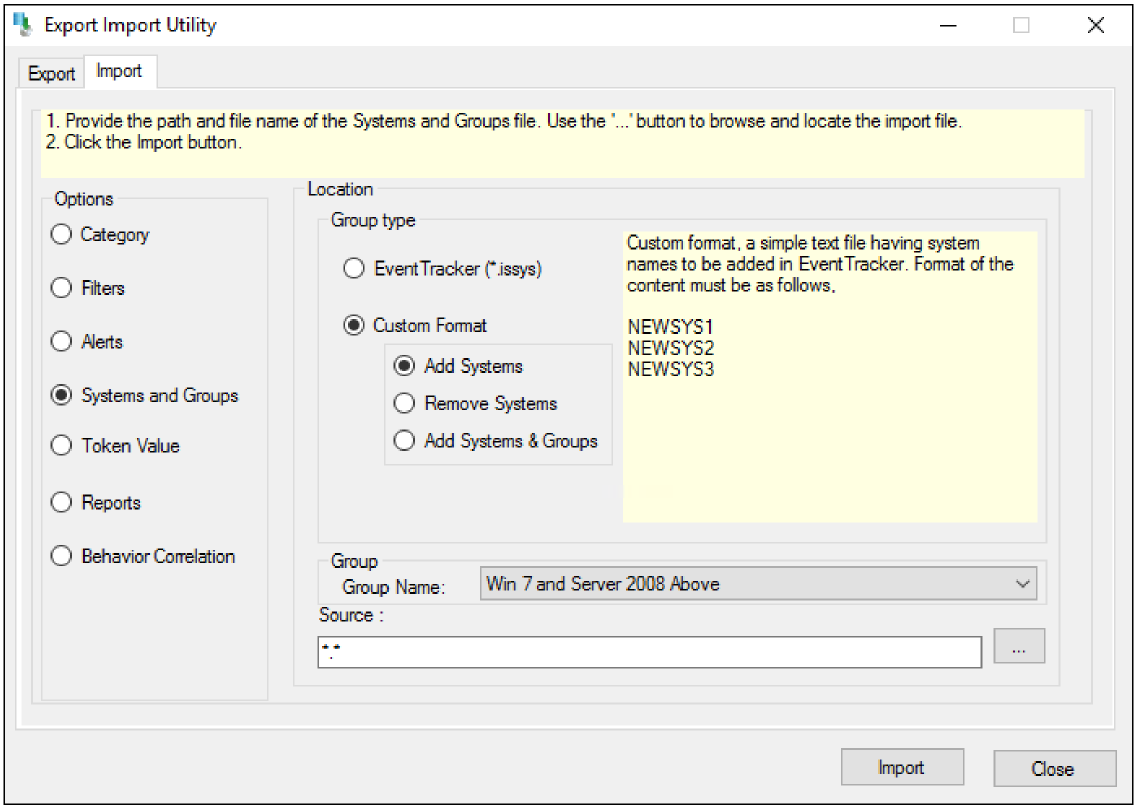
8 Click **OK**.

33.1.11 Importing System Groups

1 Click **Start**, 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 **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.



Export Import Utility

Export | Import

1. Provide the path and file name of the Systems and Groups file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

Options
○ Category
○ Filters
○ Alerts
● Systems and Groups
○ Token Value
○ Reports
○ Behavior Correlation

Location
Group type
○ EventTracker (*.issys)
● Custom Format
● Add Systems
○ Remove Systems
○ Add Systems & Groups

Custom format, a simple text file having system names to be added in EventTracker. Format of the content must be as follows,

NEWSYS1
NEWSYS2
NEWSYS3

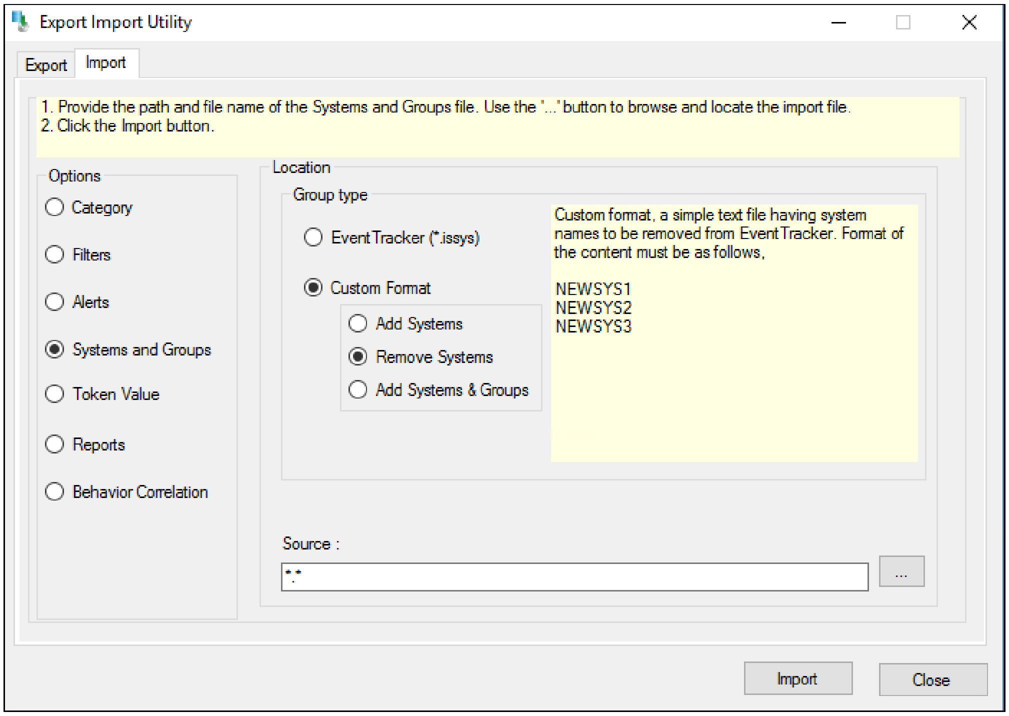
Group
Group Name: Win 7 and Server 2008 Above

Source : *.*

Figure 701

Text file contains one system name per line.

- Click **Remove systems** option.



Export Import Utility

1. Provide the path and file name of the Systems and Groups file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

Options

○ Category
○ Filters
○ Alerts
● Systems and Groups
○ Token Value
○ Reports
○ Behavior Correlation

Location

Group type

○ Event Tracker (*.issys)
● Custom Format
○ Add Systems
● Remove Systems
○ Add Systems & Groups

Custom format, a simple text file having system names to be removed from Event Tracker. Format of the content must be as follows,

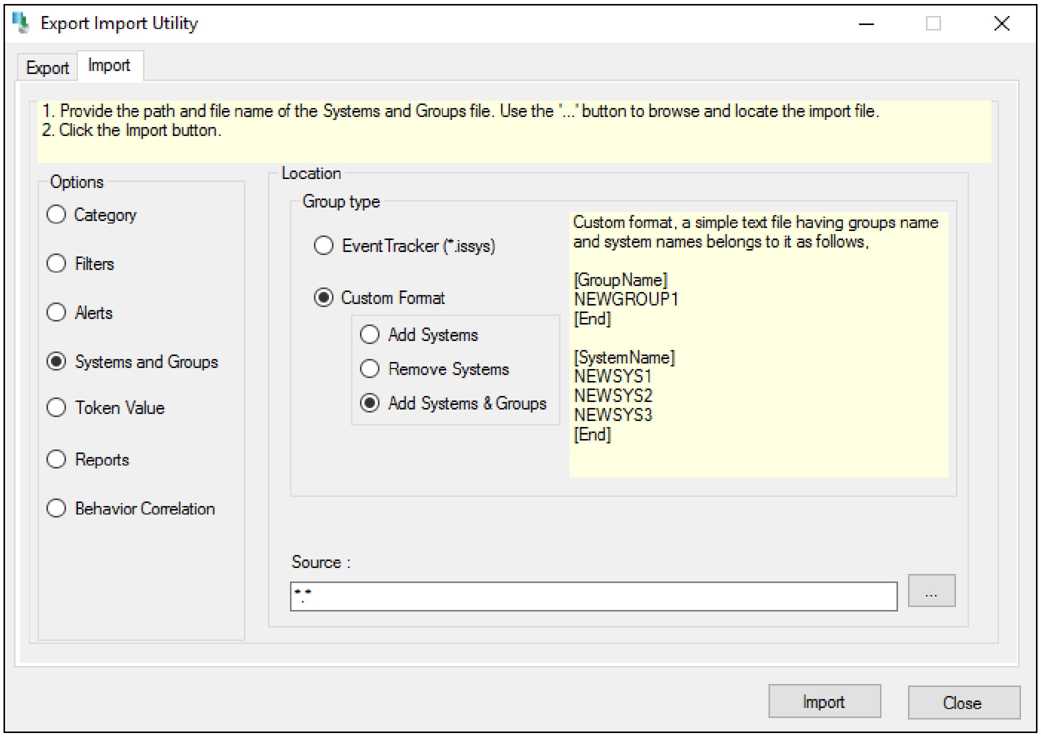
NEWSYS1
NEWSYS2
NEWSYS3

Source : *.*

Figure 702

No system name included in the text file.

- Select **Add systems & Groups** option.



Export Import Utility

1. Provide the path and file name of the Systems and Groups file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

Options

○ Category
○ Filters
○ Alerts
● Systems and Groups
○ Token Value
○ Reports
○ Behavior Correlation

Location

Group type

○ EventTracker (*.issys)
● Custom Format
○ Add Systems
○ Remove Systems
● Add Systems & Groups

Custom format, a simple text file having groups name and system names belongs to it as follows,

[GroupName]
NEWGROUP1
[End]

[SystemName]
NEWSYS1
NEWSYS2
NEWSYS3
[End]

Source : *.*

Figure 703

Text file contains system and group name.

5 Click **Browse** ... .

EventTracker opens 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.

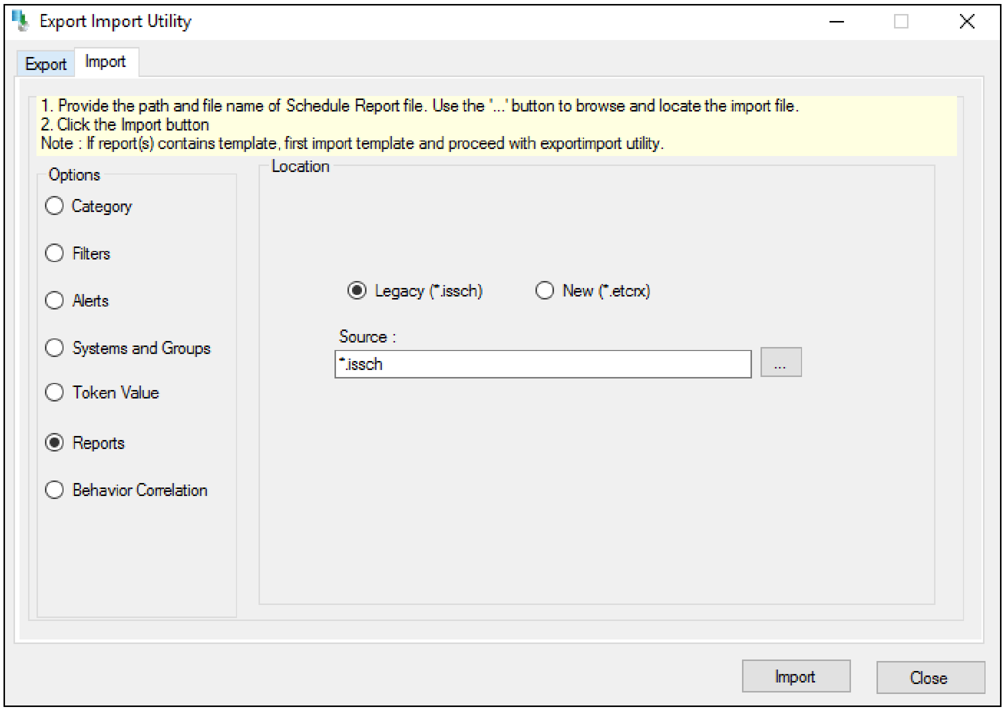
7 Click **Import**.

EventTracker opens the Export Import Utility message box.

8 Click **OK**.

33.1.12 Importing Reports

1 Click **Start**, 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 **Reports** option.



1. Provide the path and file name of Schedule Report file. Use the '...' button to browse and locate the import file.
2. Click the Import button
Note : If report(s) contains template, first import template and proceed with exportimport utility.

Source : *.issch

Figure 704

NOTE

The valid file extension for Legacy is .issch and for New type is .etcrx. Select the option as per extension.

For the option Legacy type:

1 Click **Browse** ... .

EventTracker opens the Open pop-up window.

2 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.

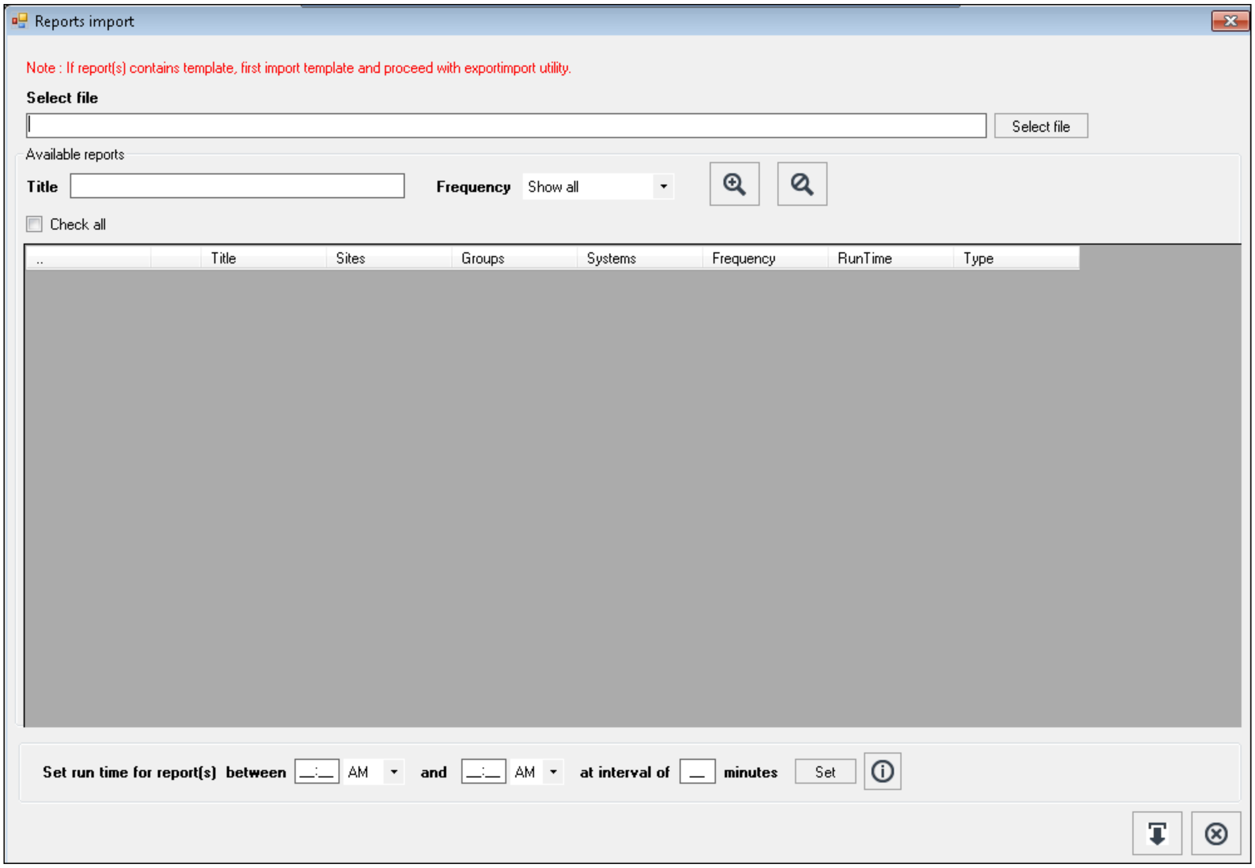
3 Click **Import**.

EventTracker opens the **Export Import Utility** message box.

4 Click **OK**.

For the option New type:

1 When the New type option is selected, EventTracker opens the Reports Import window.



Reports import

Note : If report(s) contains template, first import template and proceed with exportimport utility.

Select file

Available reports

Title

Frequency: Show all

□ Check all

..	Title	Sites	Groups	Systems	Frequency	RunTime	Type

Set run time for report(s) between __:__ AM and __:__ AM at interval of __ minutes

Figure 705

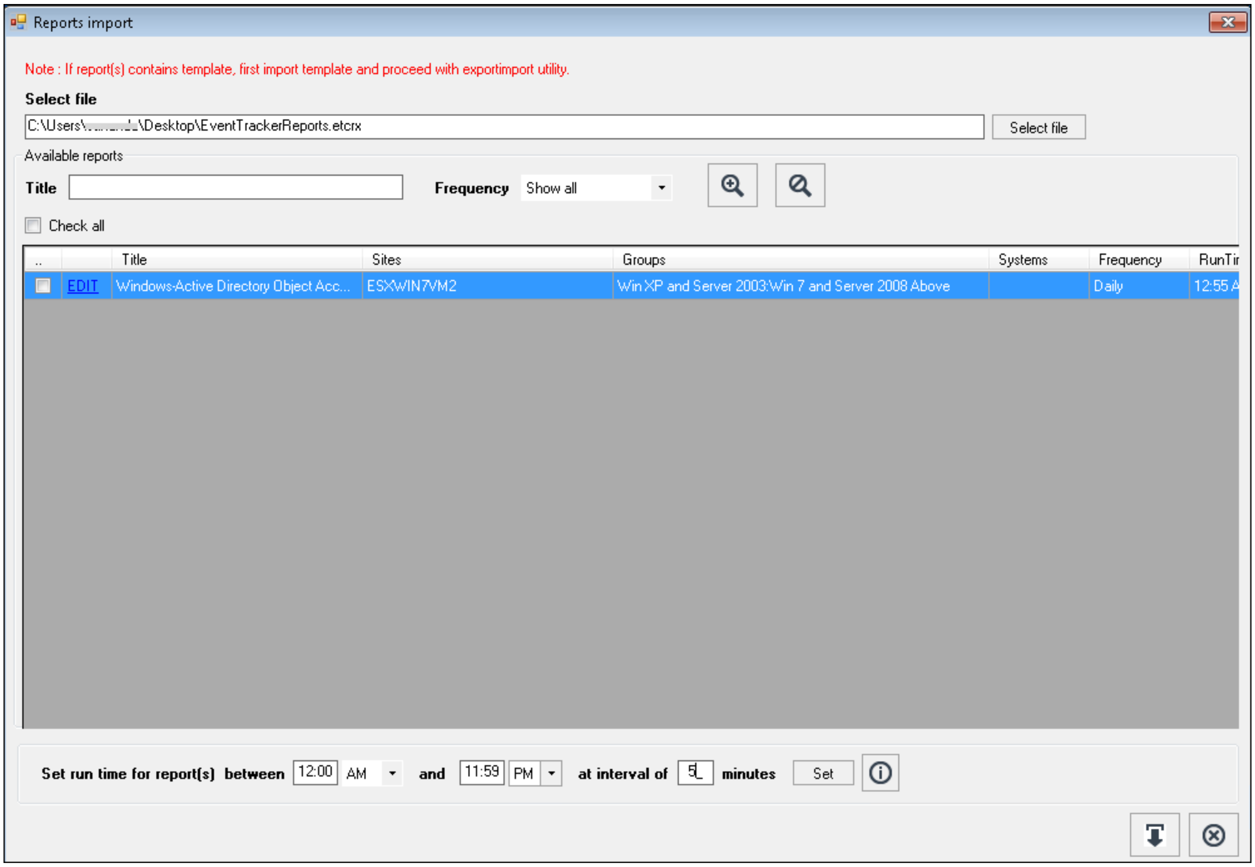
2 Browse the report file by click **Select file**.

3 Give a suitable title in the **Title** field.

4 Select the run time option and click **Set**.

NOTE: If report(s) contains template, the user will first have to import the templates and then proceed with the Export Import Utility.

The report(s) gets opens as shown in the figure below:



Note : If report(s) contains template, first import template and proceed with exportimport utility.

Select file

C:\Users\[redacted]\Desktop\EventTrackerReports.etcrx

Available reports

Title

Frequency Show all

□ Check all

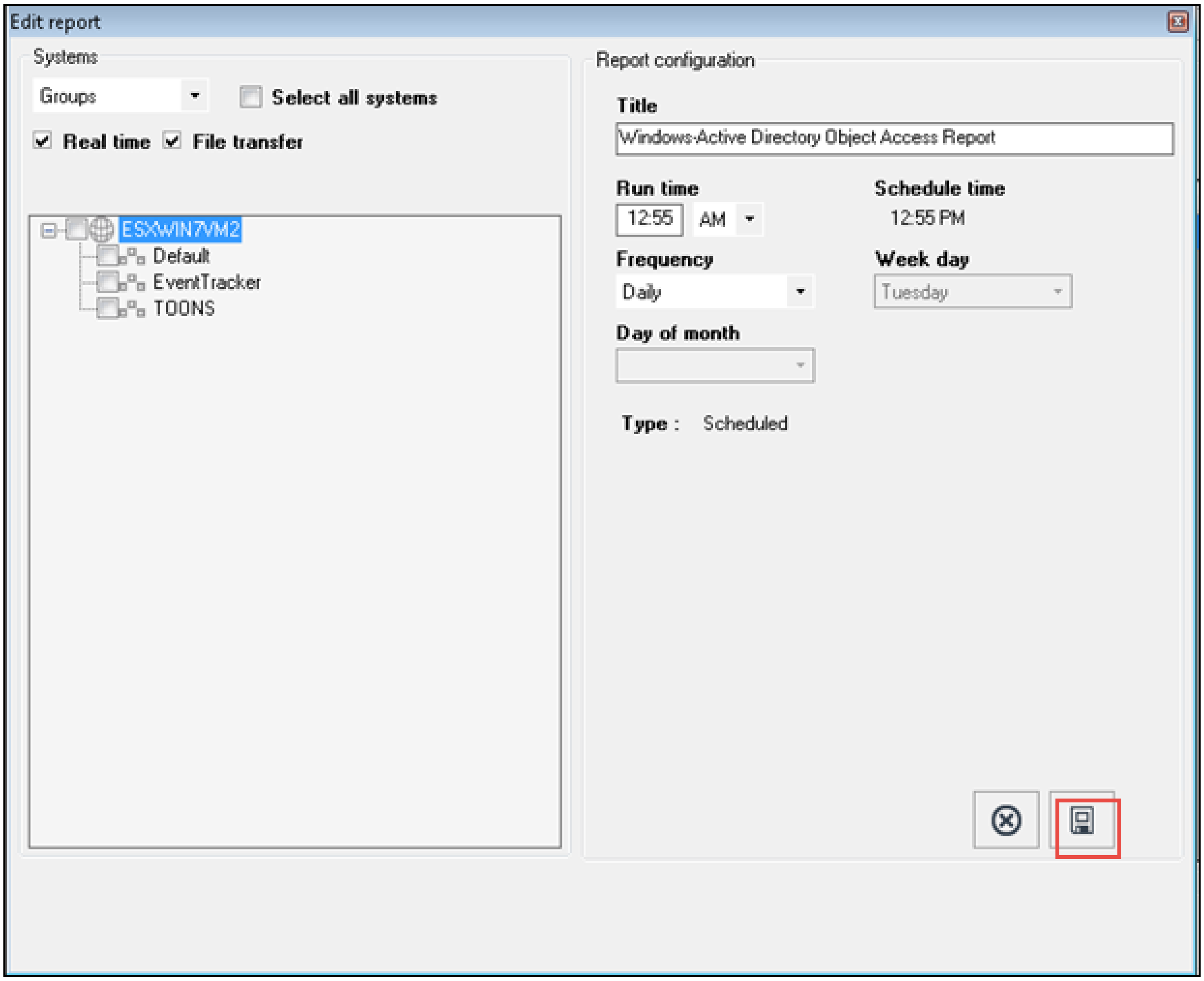
..		Title	Sites	Groups	Systems	Frequency	RunTi
□	EDIT	Windows-Active Directory Object Acc...	ESXWIN7VM2	Win XP and Server 2003:Win 7 and Server 2008 Above		Daily	12:55 A

Set run time for report(s) between 12:00 AM and 11:59 PM at interval of 5 minutes

Figure 706

5 Click the **EDIT** hyperlink to make changes in the report.

The Edit Report window opens.



Edit report

Systems

Groups

☐ Select all systems

☑ Real time ☑ File transfer

Report configuration

Title: Windows-Active Directory Object Access Report

Run time: 12:55 AM

Schedule time: 12:55 PM

Frequency: Daily

Week day: Tuesday

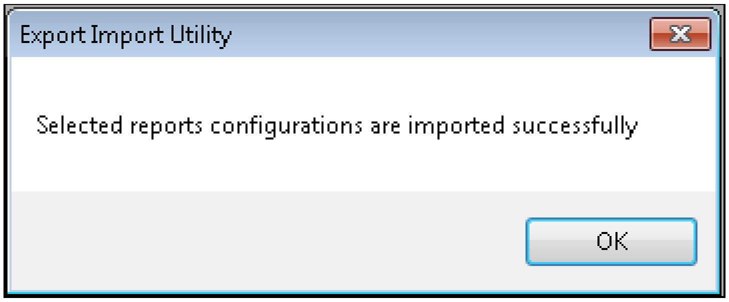
Day of month:

Type : Scheduled

Figure 707

6 Click **save** as highlighted in the figure above.

7 Select the reports by clicking the checkbox and then click **import** ⤓ in the Report Import window. EventTracker opens the below message:



Export Import Utility

Selected reports configurations are imported successfully

Figure 708

33.1.13 Importing Machine Learning

1 Click **Start**, select **All Programs**, and then select **Prism Microsystems**.
2 Select **EventTracker**, select **EventTracker Control Panel**, and then select **Export Import Utility**.
3 Click **Import** tab, Select the **Machine Learning** option.
4 Click **Browse** … .

EventTracker opens the Open pop-up window.

5 Navigate and locate the Machine Learning file you want to import. Click **Open**.

EventTracker updates the Source field with the path of the Machine Learning Jobs file.
(OR)
Type the path of the Machine Learning file in the **Source** field.

6 Click **Import**.

EventTracker opens the **Export Import Utility** message box.

7 Click **OK**.

33.1.14 Importing Token Value

1 Click **Start**, 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 **Token Value** option.
4 Click **Browse** … .

EventTracker opens the Open pop-up window.

5 Navigate and locate the Machine Learning 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.

6 Click **Import**.

EventTracker opens the **Export Import Utility** message box.

7 Click **OK**.

34. Append Archives

In this chapter, you will learn how to:

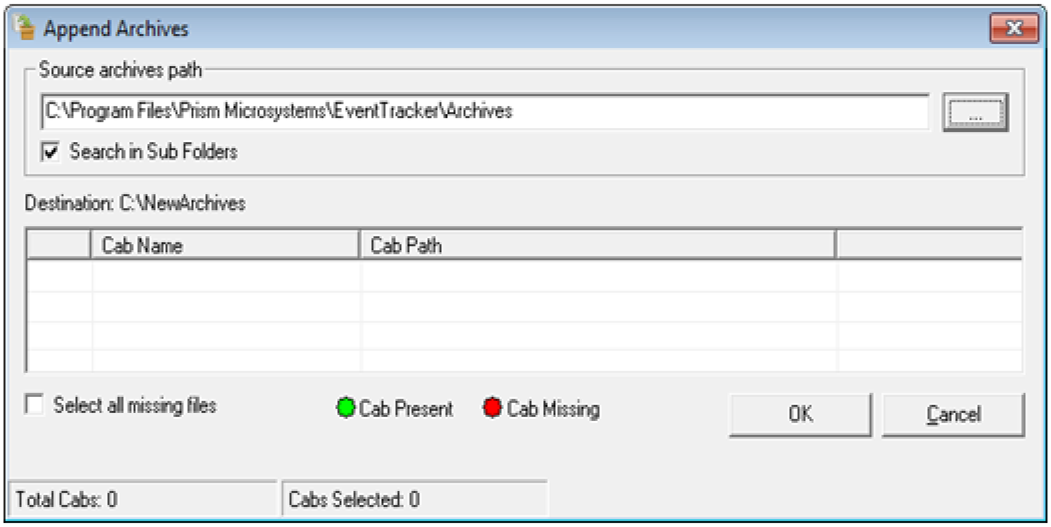
- Append CAB files

34.1 Appending 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 opens **Append Archives window.**



Append Archives

Source archives path

C:\Program Files\Prism Microsystems\EventTracker\Archives

☑ Search in Sub Folders

Destination: C:\NewArchives

	Cab Name	Cab Path	

□ Select all missing files 🟢 Cab Present 🔴 Cab Missing

Total Cabs: 0

Cabs Selected: 0

Figure 709

🟢 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.

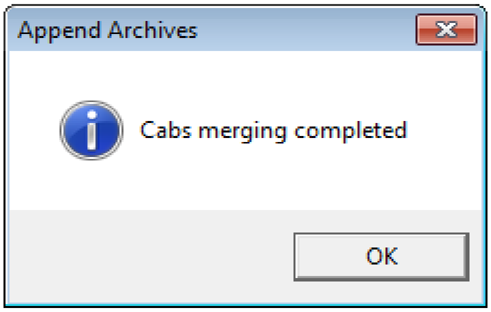
2 Click ... and select the path of the folder where you have stored the CAB files. Click **OK**.

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.

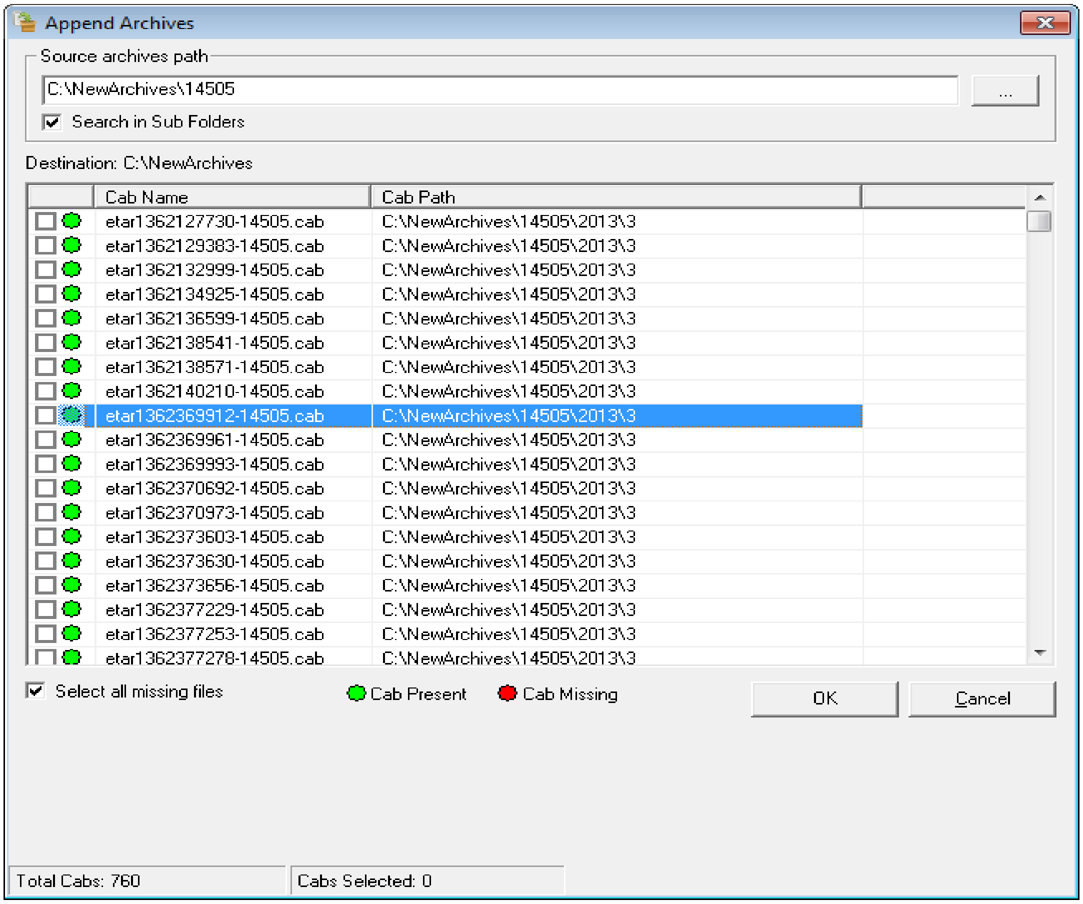


Append Archives

Cabs merging completed

Figure 710

4 Click **OK**.



Append Archives

Source archives path: C:\NewArchives\14505

☑ Search in Sub Folders

Destination: C:\NewArchives

	Cab Name	Cab Path
□ ●	etar1362127730-14505.cab	C:\NewArchives\14505\2013\3
□ ●	etar1362129383-14505.cab	C:\NewArchives\14505\2013\3
□ ●	etar1362132999-14505.cab	C:\NewArchives\14505\2013\3
□ ●	etar1362134925-14505.cab	C:\NewArchives\14505\2013\3
□ ●	etar1362136599-14505.cab	C:\NewArchives\14505\2013\3
□ ●	etar1362138541-14505.cab	C:\NewArchives\14505\2013\3
□ ●	etar1362138571-14505.cab	C:\NewArchives\14505\2013\3
□ ●	etar1362140210-14505.cab	C:\NewArchives\14505\2013\3
□ ●	etar1362369912-14505.cab	C:\NewArchives\14505\2013\3
□ ●	etar1362369961-14505.cab	C:\NewArchives\14505\2013\3
□ ●	etar1362369993-14505.cab	C:\NewArchives\14505\2013\3
□ ●	etar1362370692-14505.cab	C:\NewArchives\14505\2013\3
□ ●	etar1362370973-14505.cab	C:\NewArchives\14505\2013\3
□ ●	etar1362373603-14505.cab	C:\NewArchives\14505\2013\3
□ ●	etar1362373630-14505.cab	C:\NewArchives\14505\2013\3
□ ●	etar1362373656-14505.cab	C:\NewArchives\14505\2013\3
□ ●	etar1362377229-14505.cab	C:\NewArchives\14505\2013\3
□ ●	etar1362377253-14505.cab	C:\NewArchives\14505\2013\3
□ ●	etar1362377278-14505.cab	C:\NewArchives\14505\2013\3

☑ Select all missing files

🟢 Cab Present 🔴 Cab Missing

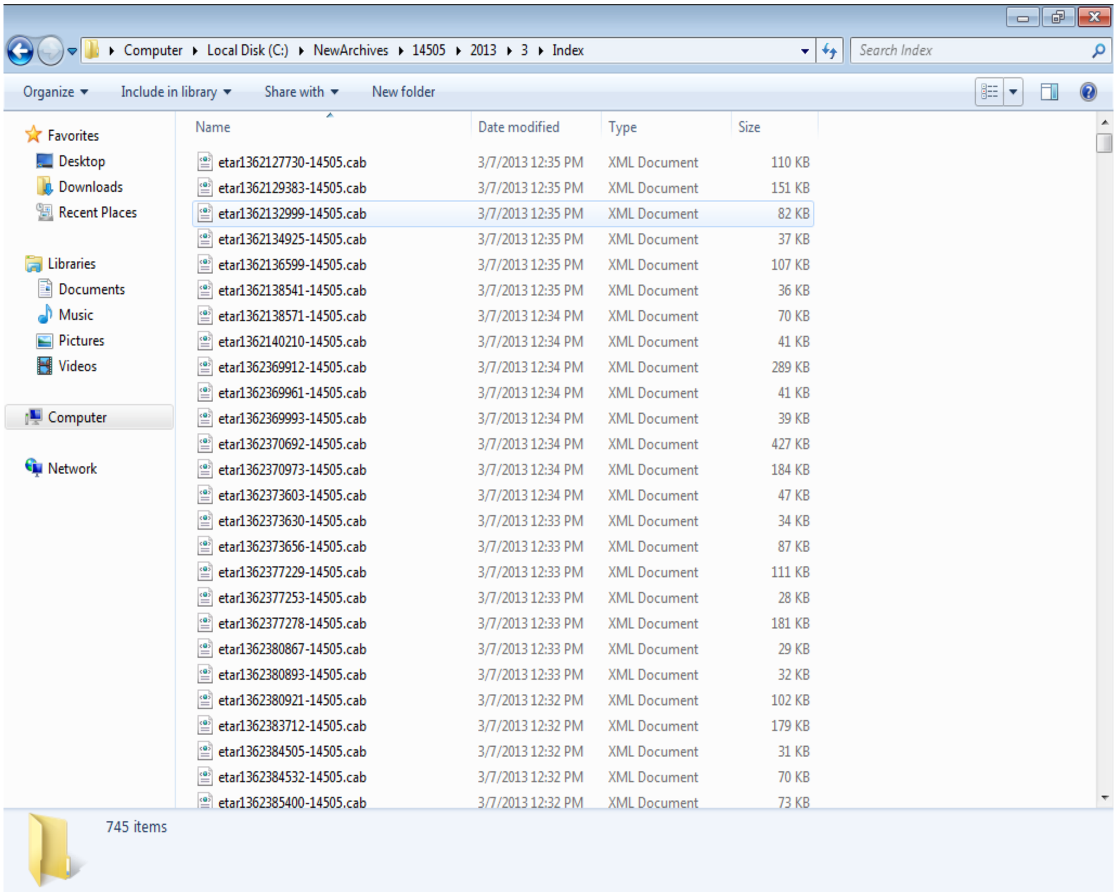
Total Cabs: 760

Cabs Selected: 0

Figure 711

EventVault Warehouse Manager opens the **Append Archives** window with list of CAB files appended.

EventVault Warehouse Manager appends the cab files to the appropriate folders.



Name	Date modified	Type	Size
etar1362127730-14505.cab	3/7/2013 12:35 PM	XML Document	110 KB
etar1362129383-14505.cab	3/7/2013 12:35 PM	XML Document	151 KB
etar1362132999-14505.cab	3/7/2013 12:35 PM	XML Document	82 KB
etar1362134925-14505.cab	3/7/2013 12:35 PM	XML Document	37 KB
etar1362136599-14505.cab	3/7/2013 12:35 PM	XML Document	107 KB
etar1362138541-14505.cab	3/7/2013 12:35 PM	XML Document	36 KB
etar1362138571-14505.cab	3/7/2013 12:34 PM	XML Document	70 KB
etar1362140210-14505.cab	3/7/2013 12:34 PM	XML Document	41 KB
etar1362369912-14505.cab	3/7/2013 12:34 PM	XML Document	289 KB
etar1362369961-14505.cab	3/7/2013 12:34 PM	XML Document	41 KB
etar1362369993-14505.cab	3/7/2013 12:34 PM	XML Document	39 KB
etar1362370692-14505.cab	3/7/2013 12:34 PM	XML Document	427 KB
etar1362370973-14505.cab	3/7/2013 12:34 PM	XML Document	184 KB
etar1362373603-14505.cab	3/7/2013 12:34 PM	XML Document	47 KB
etar1362373630-14505.cab	3/7/2013 12:33 PM	XML Document	34 KB
etar1362373656-14505.cab	3/7/2013 12:33 PM	XML Document	87 KB
etar1362377229-14505.cab	3/7/2013 12:33 PM	XML Document	111 KB
etar1362377253-14505.cab	3/7/2013 12:33 PM	XML Document	28 KB
etar1362377278-14505.cab	3/7/2013 12:33 PM	XML Document	181 KB
etar1362380867-14505.cab	3/7/2013 12:33 PM	XML Document	29 KB
etar1362380893-14505.cab	3/7/2013 12:33 PM	XML Document	32 KB
etar1362380921-14505.cab	3/7/2013 12:32 PM	XML Document	102 KB
etar1362383712-14505.cab	3/7/2013 12:32 PM	XML Document	179 KB
etar1362384505-14505.cab	3/7/2013 12:32 PM	XML Document	31 KB
etar1362384532-14505.cab	3/7/2013 12:32 PM	XML Document	70 KB
etar1362385400-14505.cab	3/7/2013 12:32 PM	XML Document	73 KB

Figure 712

35. Agent Configuration

In this chapter, you will learn how to:

- Manage Windows and syslog Managers
- Filter the events
- Monitor System
- Monitor Processes
- Monitor Services
- Monitor Log Files
- Monitor Network Connection
- Monitor Performance
- Maintain Log Backup
- Transfer Log Files
- Syslog FTP sever
- Backup Current Configuration

35.1 Agent Configuration

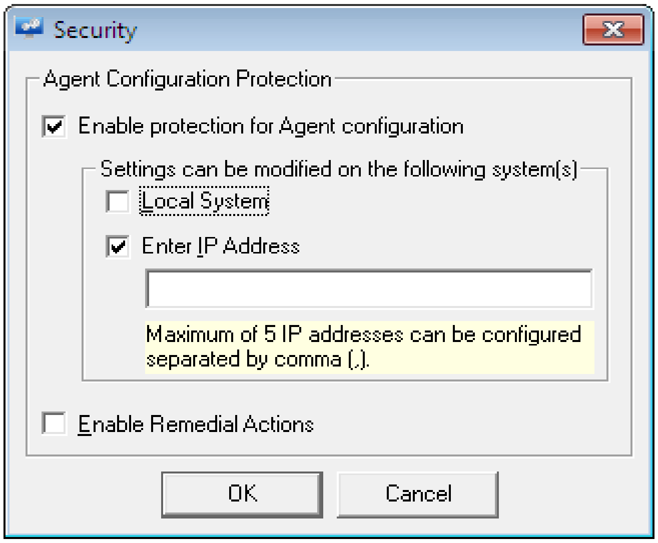
All configurations for agent(s) are set by default during installation. If you are interested in changing these default configuration settings, then it can be done in EventTracker Agent Configuration.

35.2 Security - Protect Agent Configuration Settings

This option enables you to protect the EventTracker agent configuration settings. You ca n 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.

1 Login to **EventTracker Control Panel**. Double click **EventTracker Agent Configuration**.
 EventTracker Agent Configuration window opens.

2 Select the **File** menu, and then select **Security**.
 EventTracker opens **Agent Configuration Protection** pane.



Security

Agent Configuration Protection

☑ Enable protection for Agent configuration

Settings can be modified on the following system(s)

☐ Local System

☑ Enter IP Address

Maximum of 5 IP addresses can be configured separated by comma (,).

☐ Enable Remedial Actions

Figure 713

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.

Table 78

1 Select the **Enable protection for Agent configuration** checkbox.
2 Select/enter appropriate data in relevant fields, and then click **Save**.

35.3 Loading a Template

For loading an Agent Template,

1. Select **File** from the menu and click on the **Load a Template** option from the dropdown list.

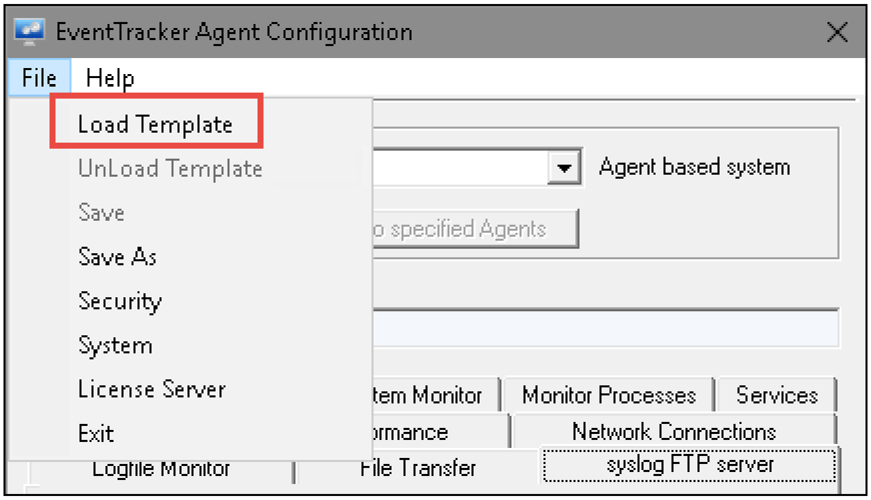
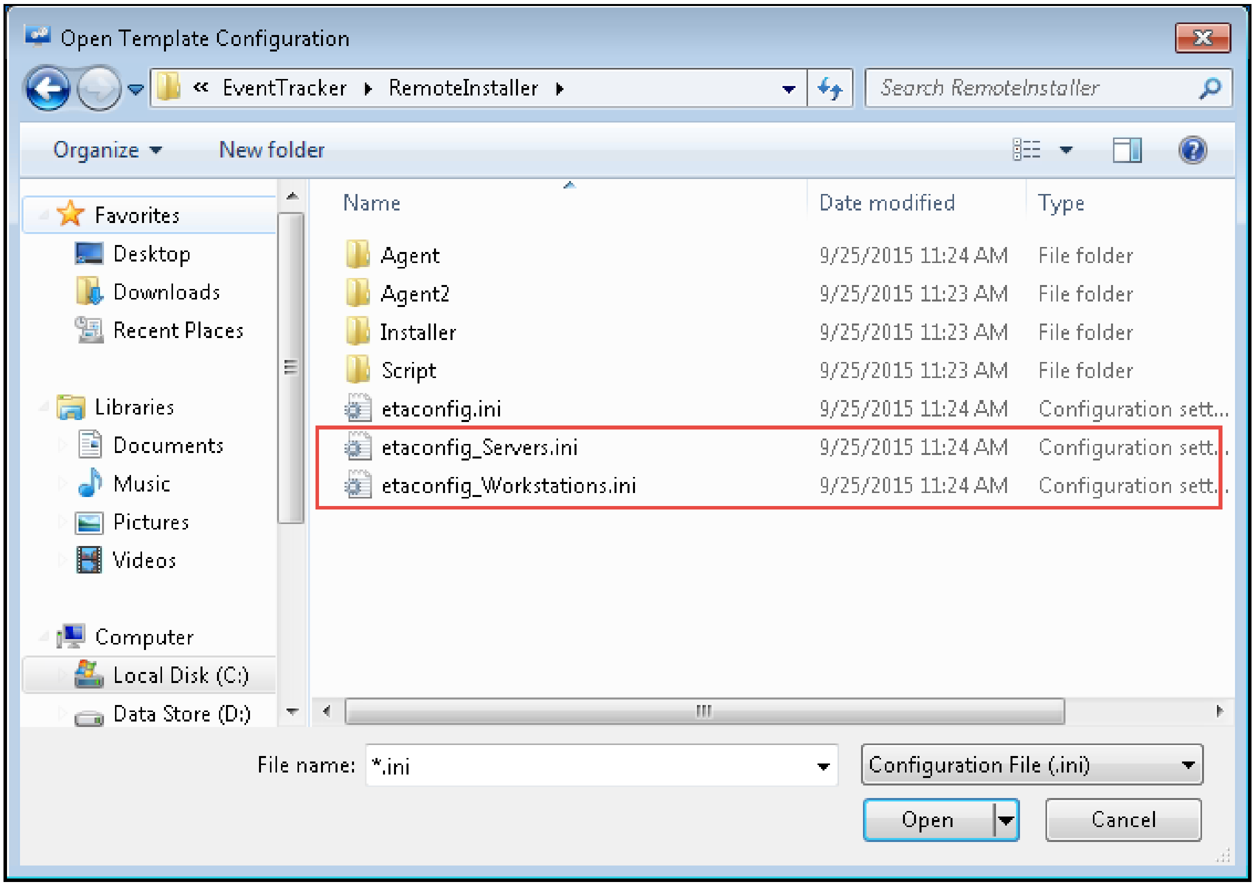


Figure 714

2. Browse the template to be selected and click **Open** (Select the **etaconfig_Servers.ini** or **etaconfig_Workstations.ini** from the RemoteInstaller folder).



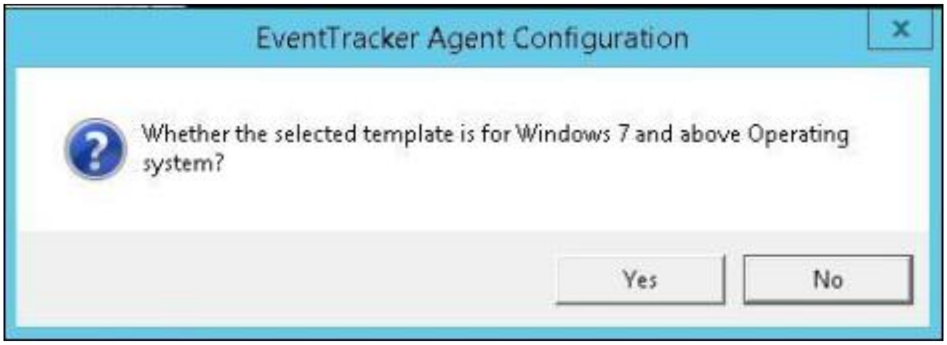
Name	Date modified	Type
Agent	9/25/2015 11:24 AM	File folder
Agent2	9/25/2015 11:23 AM	File folder
Installer	9/25/2015 11:23 AM	File folder
Script	9/25/2015 11:23 AM	File folder
etaconfig.ini	9/25/2015 11:24 AM	Configuration sett...
etaconfig_Servers.ini	9/25/2015 11:24 AM	Configuration sett...
etaconfig_Workstations.ini	9/25/2015 11:24 AM	Configuration sett...

File name: *.ini

Configuration File (.ini)

Figure 715

A pop-up message opens.



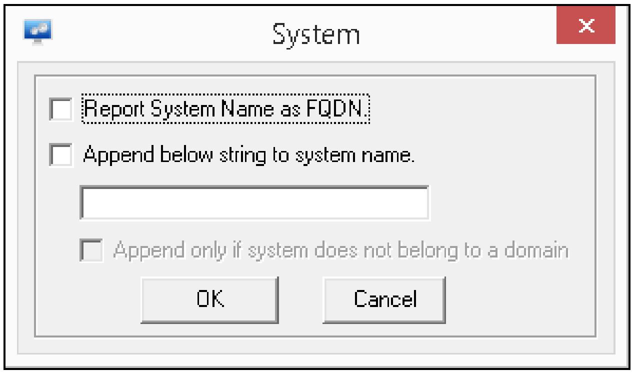
Whether the selected template is for Windows 7 and above Operating system?

Figure 716

3. Depending on the Operating system, select **Yes/No**, to get the configuration according to the selected template.

35.4 Systems option

- Click the **File** option and select **Systems** from the dropdown list.
  The System window opens.



□ Report System Name as FQDN

□ Append below string to system name.

□ Append only if system does not belong to a domain

Figure 717

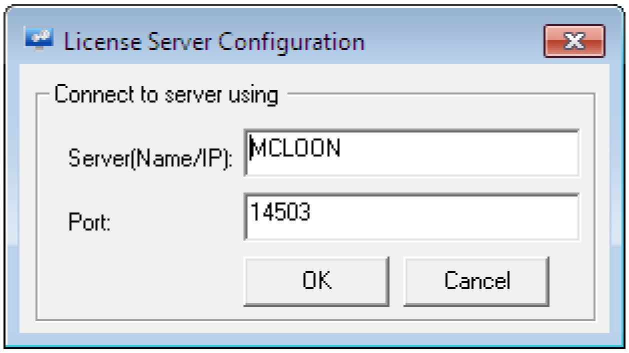
35.4.1 To Report system name as FQDN

For more Information on this section, Refer: https://www.netsurion.com/Corporate/media/Corporate/Files/Support-Docs/Enhancement-in-Agent-syslog-collector-to-resolve-sender-IP-Address.pdf

35.5 License Server Configuration

1 To enter/update license server configuration details, login to **EventTracker Control Panel**. Double click **EventTracker Agent Configuration**.

EventTracker Agent Configuration window opens.



License Server Configuration

Connect to server using

Server(Name/IP): MCLOON

Port: 14503

Figure 718

2 Select the **File** menu, and then select **License Server**.
  By default, the license server details are already updated.

3 Update/Enter **Server (Name/IP):** and **Port:** number details, if required.

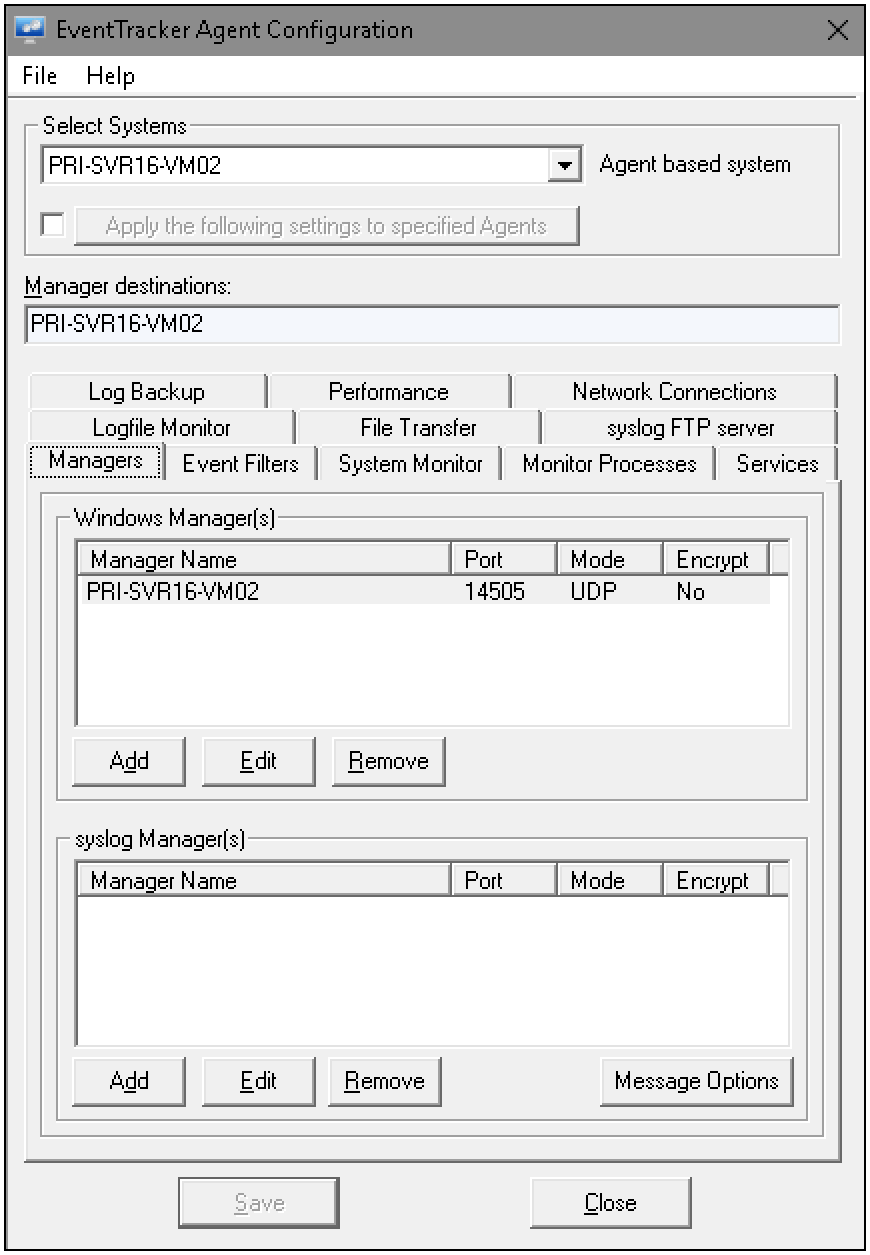
4 Click **OK**.

35.6 Managers tab

The amount of free space to be left on storage device can be entered in terms of percentage (%) or in MB.

1. To update settings in EventTracker Manager, open **EventTracker Control Panel**. Double-click **EventTracker Agent Configuration**.

   Managers tab opens by default.



EventTracker Agent Configuration

Select Systems: PRI-SVR16-VM02 — Agent based system

□ Apply the following settings to specified Agents

Manager destinations: PRI-SVR16-VM02

Windows Manager(s)

Manager Name	Port	Mode	Encrypt
PRI-SVR16-VM02	14505	UDP	No

syslog Manager(s)

Manager Name	Port	Mode	Encrypt

Figure 719

2. Click appropriate tabs and configure the agent as per the requirement.
3. To configure the amount of free space on storage devices, click **Add**.
   Add Destination window opens.
4. Select **Guaranteed Delivery Mode (TCP)** option.

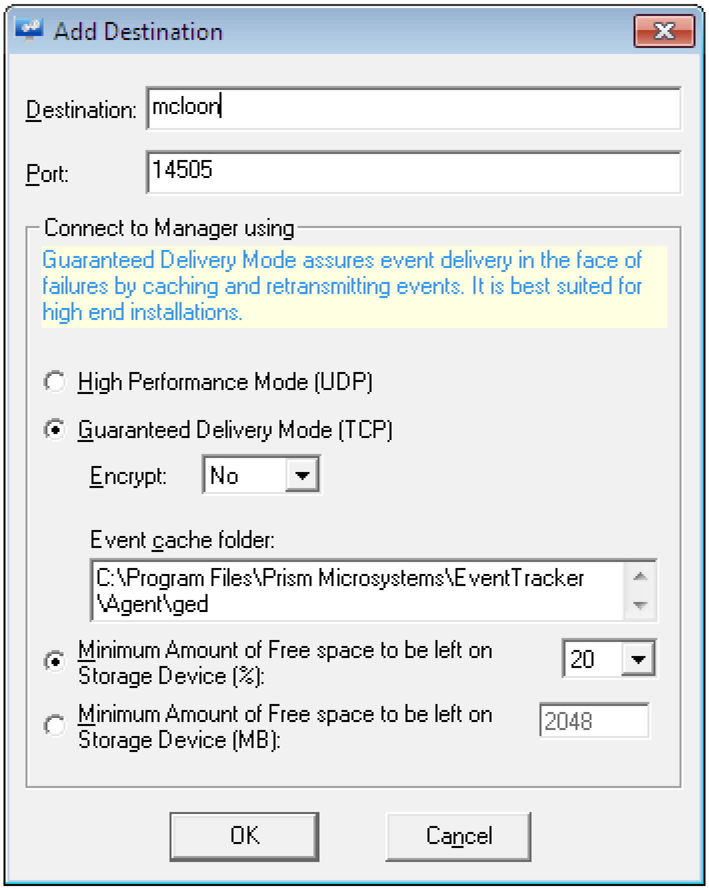

Add Destination
Destination: mcloon
Port: 14505
Connect to Manager using
Guaranteed Delivery Mode assures event delivery in the face of failures by caching and retransmitting events. It is best suited for high end installations.
○ High Performance Mode (UDP)
● Guaranteed Delivery Mode (TCP)
Encrypt: No
Event cache folder:
C:\Program Files\Prism Microsystems\EventTracker\Agent\ged
● Minimum Amount of Free space to be left on Storage Device (%): 20
○ Minimum Amount of Free space to be left on Storage Device (MB): 2048
OK
Cancel

Figure 720

5. Select **Minimum Amount of Free space to be left on Storage Device (%) or Minimum Amount of Free space to be left on Storage Device (MB)** option.

   Default value for (%) is 20 and default value for MB is 2048 MB.

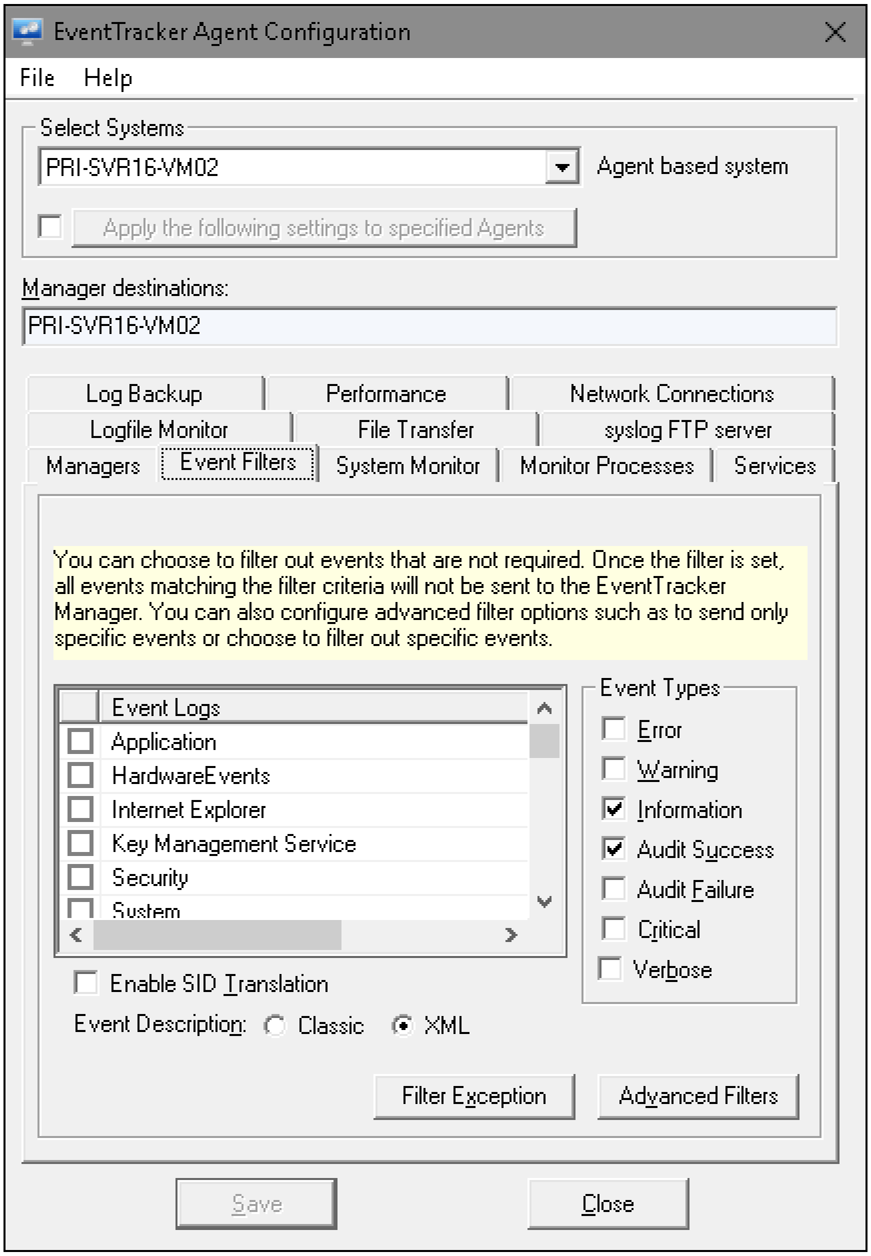
35.7 Event Filters option

This option enables you to filter events being sent to the Manager. Select appropriate checkboxes under Basic Logs, Special Logs, and Event Types. Event Logs is a dynamic list of Channels. Whenever a new Channel is provided for subscription, EventTracker updates this list automatically.

1 To filter events, double click **EventTracker Control Panel**, select **EventTracker Agent Configuration**.

2 Select the system from the **Select System** hyperlink. Select **Event Filters** tab.

EventTracker opens the Event Filters tab.



Select Systems

PRI-SVR16-VM02 Agent based system

□ Apply the following settings to specified Agents

Manager destinations: PRI-SVR16-VM02

You can choose to filter out events that are not required. Once the filter is set, all events matching the filter criteria will not be sent to the EventTracker Manager. You can also configure advanced filter options such as to send only specific events or choose to filter out specific events.

	Event Logs
□	Application
□	HardwareEvents
□	Internet Explorer
□	Key Management Service
□	Security
□	System

Event Types

- □ Error
- □ Warning
- ☑ Information
- ☑ Audit Success
- □ Audit Failure
- □ Critical
- □ Verbose

□ Enable SID Translation

Event Description: ○ Classic ● XML

Figure 721

Field	Description
Basic Logs	Select appropriate checkboxes to filter the events being sent to the Manager.
Special Logs	Select appropriate checkboxes to filter the events being sent to the Manager.
Event Types	Select appropriate checkboxes to filter the events being sent to the Manager. Example: Event Types -> Warning The filter is now set and all events with Event Type Warning will be filtered out and will not be sent to EventTracker Manager.
Enable SID Translation	Select this checkbox to enable SID translation. For more information on SID translation, refer SID-translate.pdf in the EventTracker installation folder.
Enable High Performance mode	Select this checkbox to switch the Agent performance modes.
Filter Exception	Click this button to set the filter exceptions for specific events that you want to monitor.
Advanced Filters	Click this button to set the filters for the specific events that you do not want to monitor.

Table 79

By default, EventTracker filters Information and Audit Success events.

3 Set the available filter options appropriately, and then click **Save**.

35.7.1 Filtering 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.

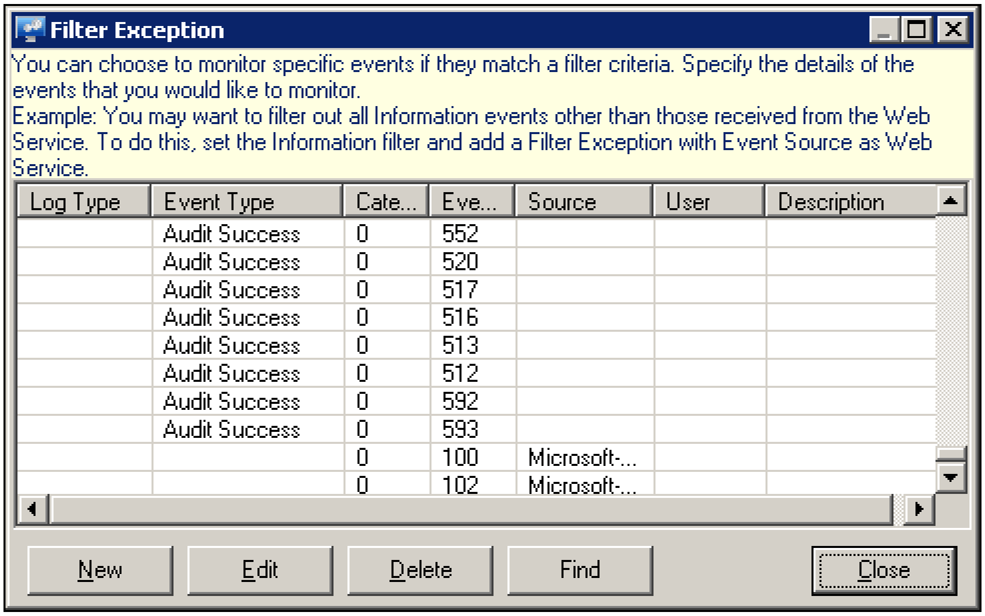
1 To filter events with exception, double-click **EventTracker Control Panel**, select **EventTracker Agent Configuration**.

2 Select the system from the **Select System** hyperlink. Select **Event Filters** tab.

EventTracker opens the Event Filters tab.

3 Click **Filter Exception**.

EventTracker opens the Filter Exception pop-up window with a list of events exempted from filtering.



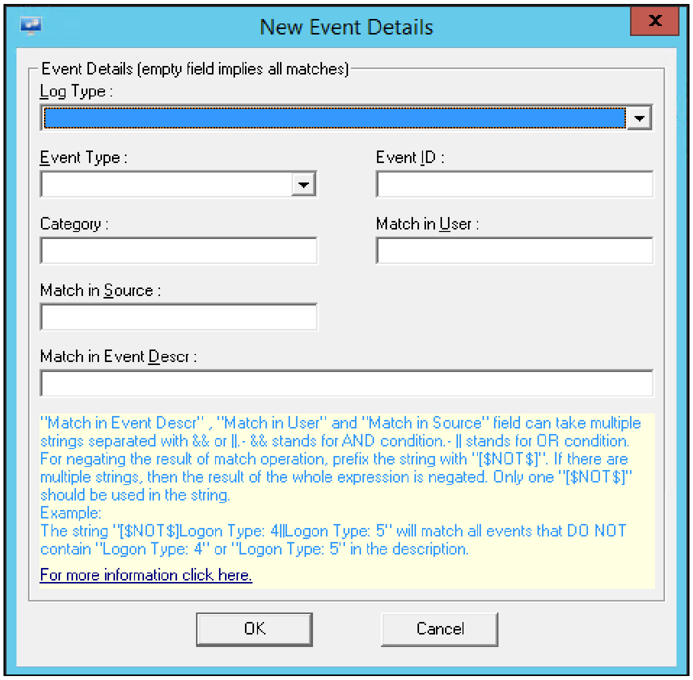
You can choose to monitor specific events if they match a filter criteria. Specify the details of the events that you would like to monitor.
Example: You may want to filter out all Information events other than those received from the Web Service. To do this, set the Information filter and add a Filter Exception with Event Source as Web Service.

Log Type	Event Type	Cate...	Eve...	Source	User	Description
	Audit Success	0	552			
	Audit Success	0	520			
	Audit Success	0	517			
	Audit Success	0	516			
	Audit Success	0	513			
	Audit Success	0	512			
	Audit Success	0	592			
	Audit Success	0	593			
		0	100	Microsoft-...		
		0	102	Microsoft-...		

Figure 722

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 find event details, click **Find**.
8 To add filter exceptions, click **New**.

EventTracker opens the Filter Exception pop-up window to select/enter event details.

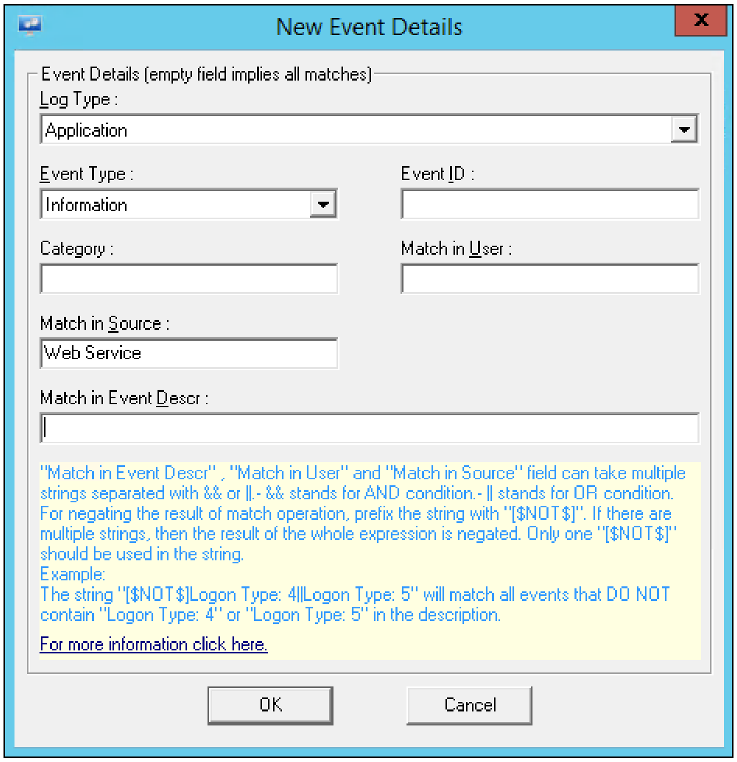


"Match in Event Descr" , "Match in User" and "Match in Source" field can take multiple strings separated with && or ||.- && stands for AND condition.- || stands for OR condition.
For negating the result of match operation, prefix the string with "[NOT]". If there are multiple strings, then the result 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.

Figure 723

9 Enter appropriate data in the relevant fields.

For example - Log Type: Application, Event Type: Information, Match in Source: Web Service



Log Type : Application

Event Type : Information

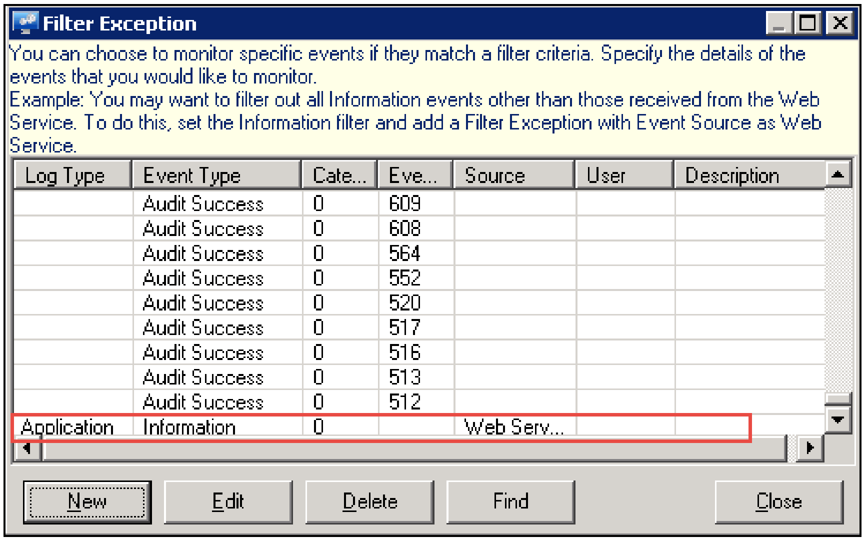
Match in Source : Web Service

"Match in Event Descr" , "Match in User" and "Match in Source" 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.

Figure 724

10 Click **OK**.

EventTracker opens the Filter Exception pop-up window with the newly added filter exception.



Filter Exception

You can choose to monitor specific events if they match a filter criteria. Specify the details of the events that you would like to monitor.
Example: You may want to filter out all Information events other than those received from the Web Service. To do this, set the Information filter and add a Filter Exception with Event Source as Web Service.

Log Type	Event Type	Cate...	Eve...	Source	User	Description
	Audit Success	0	609			
	Audit Success	0	608			
	Audit Success	0	564			
	Audit Success	0	552			
	Audit Success	0	520			
	Audit Success	0	517			
	Audit Success	0	516			
	Audit Success	0	513			
	Audit Success	0	512			
Application	Information	0		Web Serv...		

Figure 725

11 Click **Close**, and then click **Save**.

For negating the results of User and Source in the Filter Exception list:

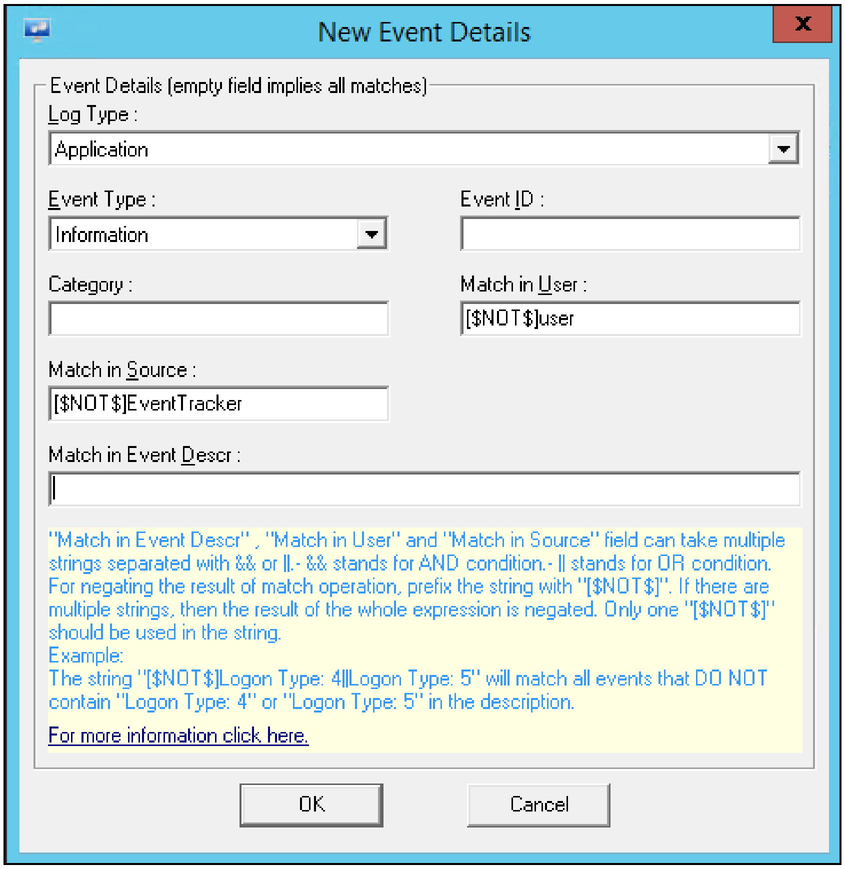
a) In EventTracker Agent Configuration window, under **Event Filters** tab, click the **Filter Exception** button.

b) Click **New**.

EventTracker opens the New Event Detail window.

c) Enter appropriate data in the relevant fields.

For example - Log Type: Application, Event Type: Information, Match in User: [NOT]user, Match in Source: [NOT]EventTracker



New Event Details

Event Details (empty field implies all matches)

Log Type : Application

Event Type : Information

Event ID :

Category :

Match in User : [NOT]user

Match in Source : [NOT]EventTracker

Match in Event Descr :

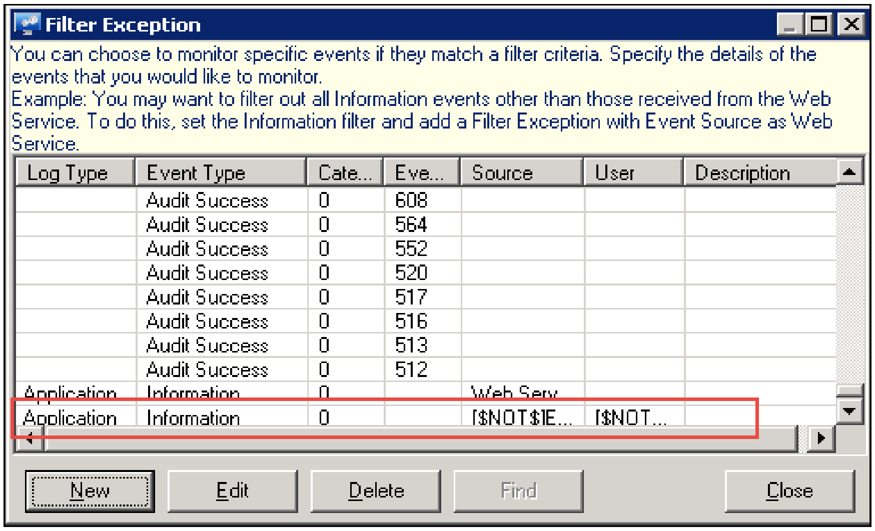
"Match in Event Descr" , "Match in User" and "Match in Source" field can take multiple strings separated with && or ||.- && stands for AND condition.- || stands for OR condition. For negating the result of match operation, prefix the string with "[NOT]". If there are multiple strings, then the result 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.

Figure 726

d) Click **OK**.

EventTracker opens the Filter Exception pop-up window with the newly added User and Source filter exception.



Filter Exception

You can choose to monitor specific events if they match a filter criteria. Specify the details of the events that you would like to monitor.
Example: You may want to filter out all Information events other than those received from the Web Service. To do this, set the Information filter and add a Filter Exception with Event Source as Web Service.

Log Type	Event Type	Cate...	Eve...	Source	User	Description
	Audit Success	0	608			
	Audit Success	0	564			
	Audit Success	0	552			
	Audit Success	0	520			
	Audit Success	0	517			
	Audit Success	0	516			
	Audit Success	0	513			
	Audit Success	0	512			
Application	Information	0		Web Serv...		
Application	Information	0		[NOT]E...	[$NOT...	

Figure 727

e) Click **Close** and then click **Save** in the Agent Configuration window.

🗎 NOTE

Multiple strings separated with && (And) and II (OR) operators can now be used for both "Match in User" and Match in Source".

35.7.2 Filtering 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**.

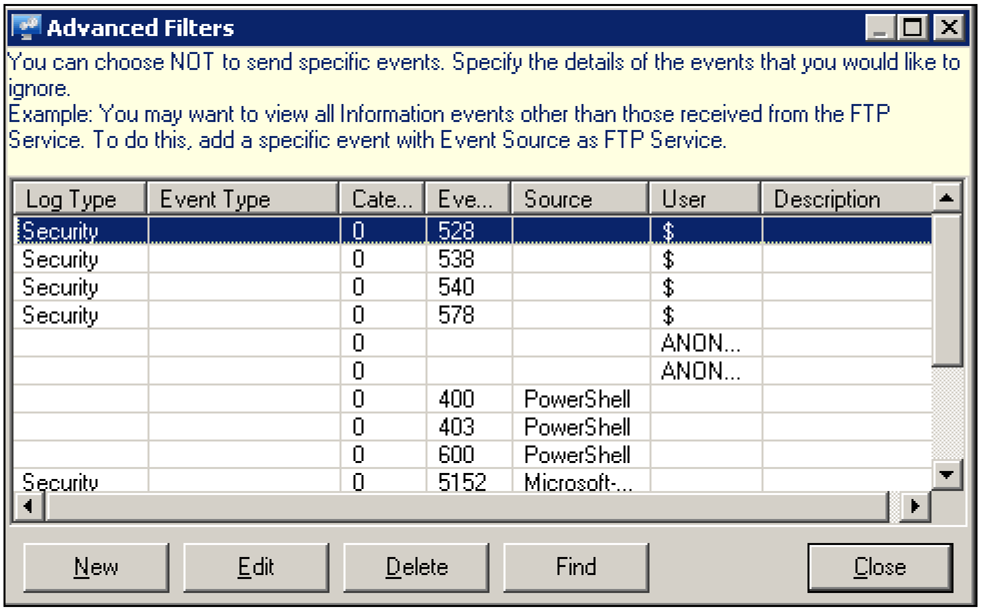
2 Select the system from the **Select System** hyperlink.

3 Click the **Event Filters** tab.

EventTracker opens the Event Filters tab.

4 Click **Advanced Filters.**

EventTracker opens the **Advanced Filters** pop-up window with a list of advanced filters.



Advanced Filters

You can choose NOT to send specific events. Specify the details of the events that you would like to ignore.
Example: You may want to view all Information events other than those received from the FTP Service. To do this, add a specific event with Event Source as FTP Service.

Log Type	Event Type	Cate...	Eve...	Source	User	Description
Security		0	528		$	
Security		0	538		$	
Security		0	540		$	
Security		0	578		$	
		0			ANON...	
		0			ANON...	
		0	400	PowerShell		
		0	403	PowerShell		
		0	600	PowerShell		
Security		0	5152	Microsoft-...		

Figure 728

5 Click **New**.

EventTracker opens the Advanced Filters pop-up window to select/enter event details.

6 Enter appropriate data in the relevant fields and then click **OK**.

EventTracker opens the Advanced Filters pop-up window with the newly added filter.

7 Click **Close**.

8 Click **Find** to find event details by entering appropriate data

9 Click **OK** and then click **Close** in the Advanced Filters window.

🗎 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.

10 Click **Save**.

35.7.3 Enabling SID Translation

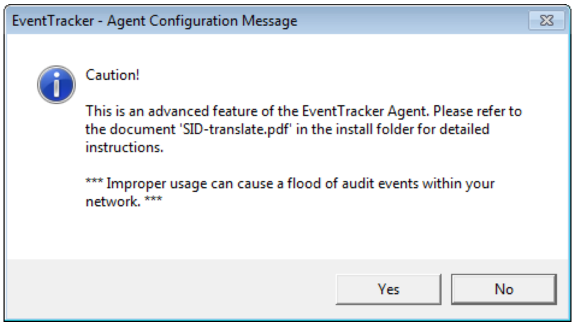
This option helps you enable SID translation.

1 Double click **EventTracker Control Panel** select **EventTracker Agent Configuration**.

2 Select the system from the **Select System** hyperlink. Click **Event Filters** tab. EventTracker displays the Event Filters tab.

3 Select the **Enable SID Translation** option.

EventTracker open the Caution message box.



Caution!

This is an advanced feature of the EventTracker Agent. Please refer to the document 'SID-translate.pdf' in the install folder for detailed instructions.

*** Improper usage can cause a flood of audit events within your network. ***

Figure 729

4 Click **Yes** and then click **Save**.

🗎 NOTE

This feature works in all versions of EventTracker. For more information please go through SID-translate.pdf found in the EventTracker installation folder typically, ...\Program Files\Prism Microsystems\EventTracker.

35.8 Monitoring System

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.

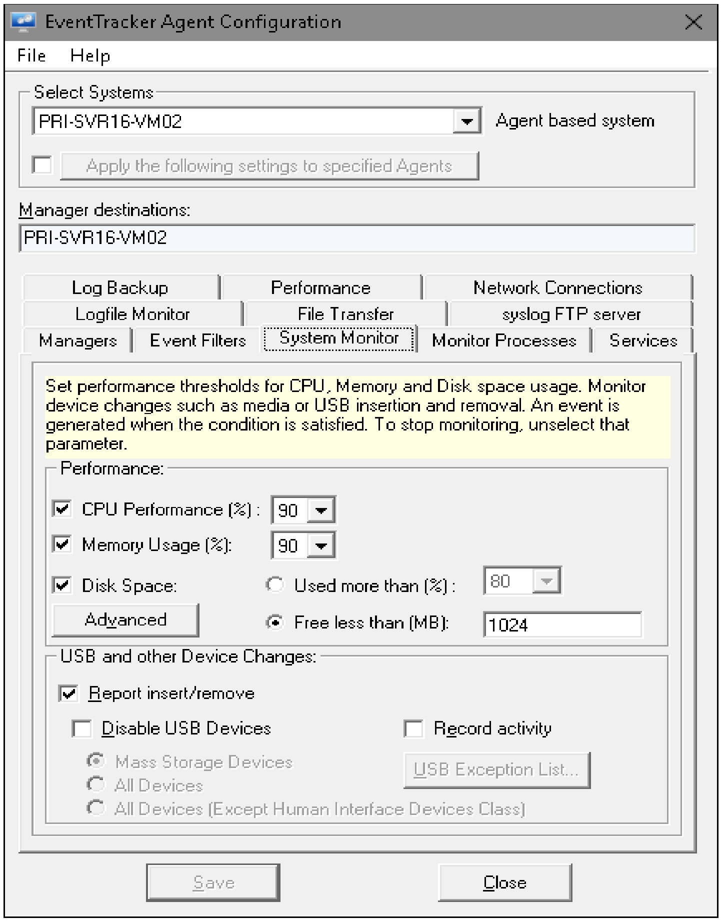
The default threshold limits are 90% for all variables. A configuration of 0% would disable the monitoring for that specific variable.

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.

35.8.1 Configuring 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 opens the System Monitor tab.



Select Systems

PRI-SVR16-VM02 Agent based system

□ Apply the following settings to specified Agents

Manager destinations:

PRI-SVR16-VM02

Set performance thresholds for CPU, Memory and Disk space usage. Monitor device changes such as media or USB insertion and removal. An event is generated when the condition is satisfied. To stop monitoring, unselect that parameter.

Performance:

☑ CPU Performance (%) : 90

☑ Memory Usage (%): 90

☑ Disk Space: ○ Used more than (%) : 80

Advanced ● Free less than (MB): 1024

USB and other Device Changes:

☑ Report insert/remove

□ Disable USB Devices □ Record activity

● Mass Storage Devices USB Exception List...

○ All Devices

○ All Devices (Except Human Interface Devices Class)

Figure 730

Field	Description
Performance	
CPU Performance (%)	Select a threshold limit to monitor CPU performance from the drop-down list.
Memory Usage (%)	Select a threshold limit to monitor memory usage from the drop-down list.
Disk Space Usage (%)	Select a threshold limit to monitor disk space usage from the drop-down list.
Handle	Select a threshold limit to monitor handle usage of the system.
Thread	Select a threshold limit to monitor thread usage of the system.
USB and other Device Changes	
Report insert/remove	Select this checkbox to track insertion or removal of USB or other devices. This checkbox is selected by default.
Record activity	Select this checkbox to monitor file transactions occur in the inserted devices.
Disable USB Devices	Select this checkbox to disable USB devices. The selection will enable the 'USB Exception List' button.
USB Exception List	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.

Table 80

To change the disk space configuration values,

1. Click the **Advanced** button.
   Advanced Configuration window opens.

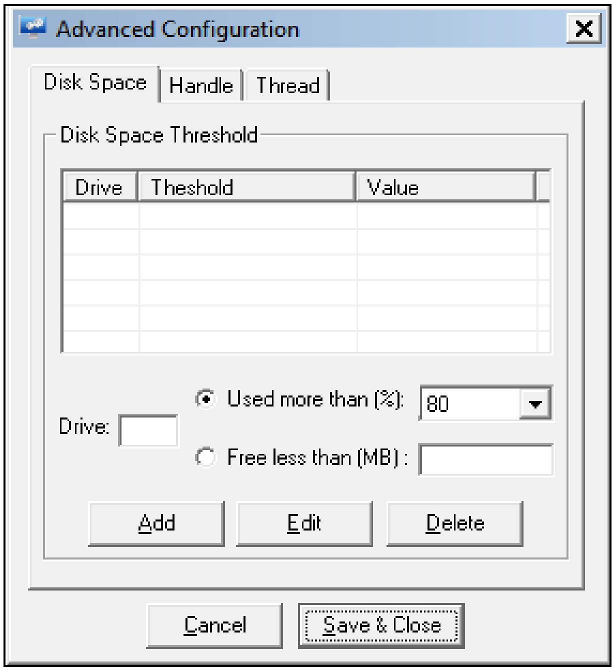
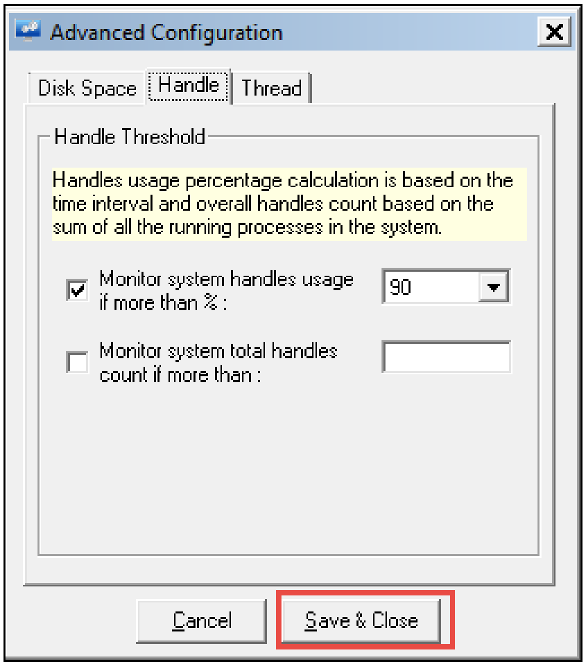


Figure 731

2 Under the Disk Space, enter the Drive: name
3 Select/Enter the required value in **Used more than %** drop-down or **Free less than (MB)**.
4 To edit or delete the disk space configuration, click the **Edit** or **Delete** button accordingly.
5 Click **Save & Close** once necessary changes have been done.
6 Select the required **Performance, USB and other Device Changes** options.
7 Click **Save & Close**.

To configure handles usage,

1 In the Advanced Configuration window, click on **Handle** in the menu bar.
2 Select the count from the dropdown box.
Ex: For "**Monitor System handles usage if more than %**", 90 is selected (Default).
3. Click **Save & Close.**



Advanced Configuration

Handle Threshold

Handles usage percentage calculation is based on the time interval and overall handles count based on the sum of all the running processes in the system.

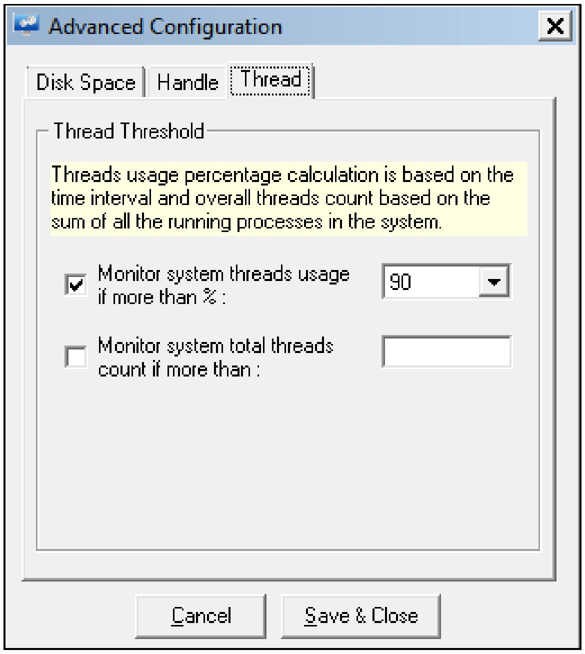
☑ Monitor system handles usage if more than % : 90

☐ Monitor system total handles count if more than :

Figure 732

To configure Thread usage,

1 Select the count from the dropdown box.
  Ex: For "**Monitor System threads usage if more than %**", 90 is selected (Default).
2. Click **Save & Close.**



Advanced Configuration

Thread Threshold

Threads usage percentage calculation is based on the time interval and overall threads count based on the sum of all the running processes in the system.

☑ Monitor system threads usage if more than % : 90

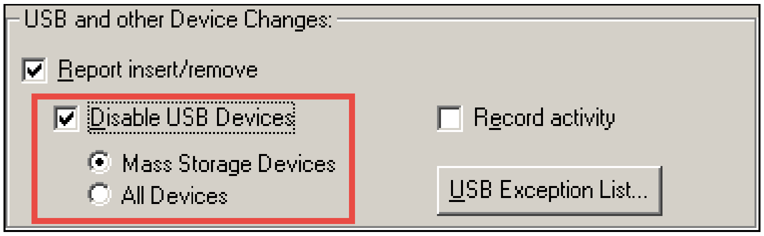
☐ Monitor system total threads count if more than :

Figure 733

35.8.2 USB and Other Device Changes

For Blocking all types of USB devices, go to the **USB and other device changes** pane.

1. Click the **Disable USB Devices** checkbox.
2. Sub-option gets enabled, namely, **Mass Storage Device** and **All Device.**
3. By enabling the **Mass storage Device** option, the user can block USB Devices like Pen Drive, Hard Disk.
4. When the **All Devices** option is enabled, it will block or disable all the devices like mouse, pen drive, external CD-DVD, external hard disk, USB ear phone/head phone, tablet and mobile devices connected either USB storage device, or MTP or PTP type.



USB and other Device Changes:

☑ Report insert/remove

☑ Disable USB Devices

● Mass Storage Devices

○ All Devices

□ Record activity

Figure 734

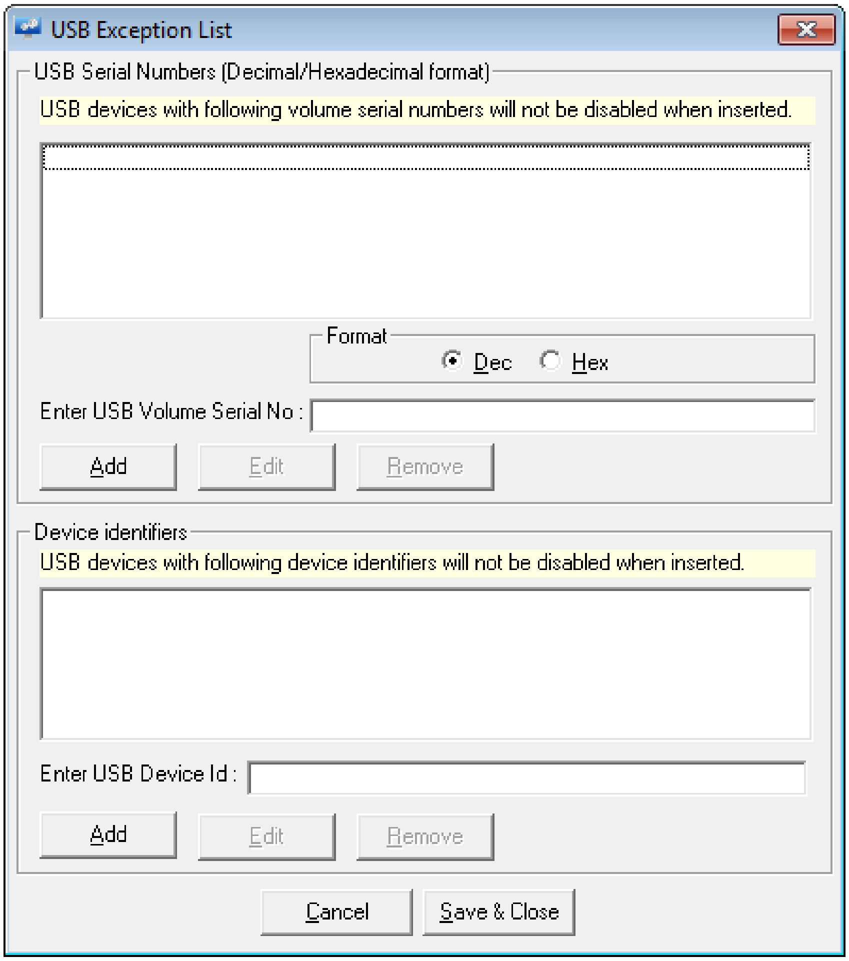
35.9 Adding USB device in the Exception List

While disabling USB Devices on a computer, you can also exempt and enable USB devices from monitoring.

1 To configure USB Exception List, select the **Disable USB Devices** checkbox.

2 Click **USB Exception List** button.

EventTracker opens the ‘USB Exception List’ pop-up window.



USB Exception List

USB Serial Numbers (Decimal/Hexadecimal format)

USB devices with following volume serial numbers will not be disabled when inserted.

Format: ● Dec ○ Hex

Enter USB Volume Serial No :

Device identifiers

USB devices with following device identifiers will not be disabled when inserted.

Enter USB Device Id :

Figure 735

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 **Add**.

EventTracker adds the newly entered serial number or device Id in the exception list.

5 Click **Save & Close**.

6 In '**Windows Agent Configuration'** page, click **Save** to save the configuration changes.

NOTE

Please refer How to – Monitor Removable Media Devices document for more details on creating exception list and its functionality.

35.10 Monitoring Processes

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 tacking the application usage.

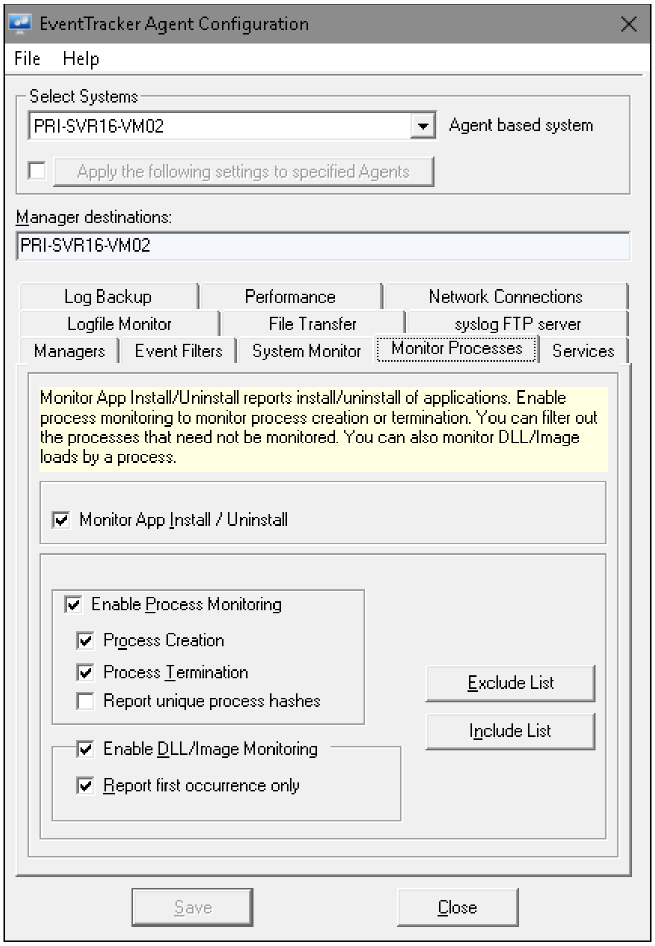
EventTracker monitors all processes specified in ‘Include List’ and ignores processes specified in ‘Exclude List’.

The option **Enable process monitoring** will help in monitoring the process created and terminated. The user can also filter out the processes that need not be monitored.DLL and image files can also be monitored that are load by a process.

35.10.1 Monitoring 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 Processes** tab.

EventTracker opens the ‘**Monitor Processes’** tab.



Select Systems: PRI-SVR16-VM02 Agent based system

☐ Apply the following settings to specified Agents

Manager destinations: PRI-SVR16-VM02

Monitor App Install/Uninstall reports install/uninstall of applications. Enable process monitoring to monitor process creation or termination. You can filter out the processes that need not be monitored. You can also monitor DLL/Image loads by a process.

☑ Monitor App Install / Uninstall

☑ Enable Process Monitoring
☑ Process Creation
☑ Process Termination
☐ Report unique process hashes

☑ Enable DLL/Image Monitoring
☑ Report first occurrence only

Figure 736

Field	Description
Monitor App Install/ Uninstall	Select this checkbox to monitor installation and un-installation of applications.
Enable Process Monitoring	Select this checkbox to monitor processes. This selection enables the Exclude List and Include List buttons.
Exclude List	Enables you to set the processes that you do not wish to monitor.
Include List	Enables you to set the processes that you wish to monitor.

Table 81

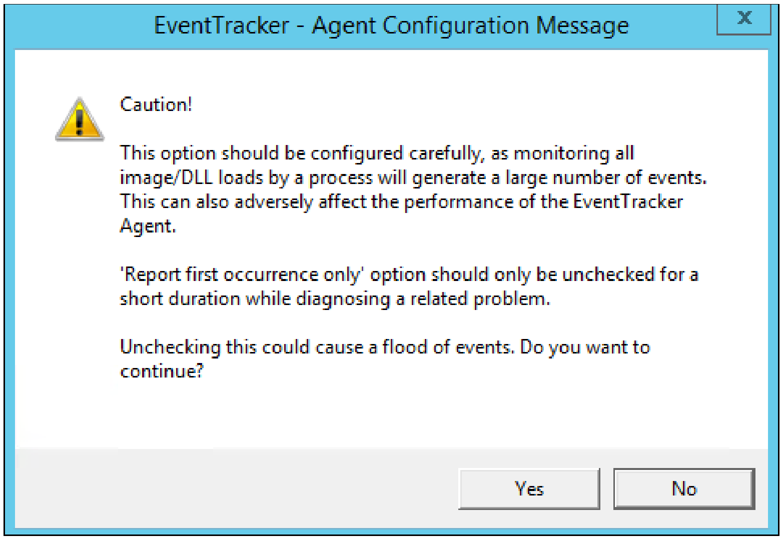
🗎 NOTE

Enable Process Monitoring option is a licensed feature and will be available only if the license is purchased.

4 Select appropriately the **Monitor App Install / Uninstall** and **Enable Process Monitoring** options**.**

Under the Option **"Enable Process Monitoring"**

- The option **Process Creation/Process Termination** helps in monitoring the process launched/closed.
- The option **Enable DLL/Image Monitoring** helps in monitoring the DLL's and the image file loaded by the process.
- The option "**Report occurrence only**" will be checked by default. If you wish to uncheck it, the following message opens.



EventTracker - Agent Configuration Message

Caution!

This option should be configured carefully, as monitoring all image/DLL loads by a process will generate a large number of events. This can also adversely affect the performance of the EventTracker Agent.

'Report first occurrence only' option should only be unchecked for a short duration while diagnosing a related problem.

Unchecking this could cause a flood of events. Do you want to continue?

Figure 737

5 Click **Save**.

35.10.2 Filtering processes 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** drop down.

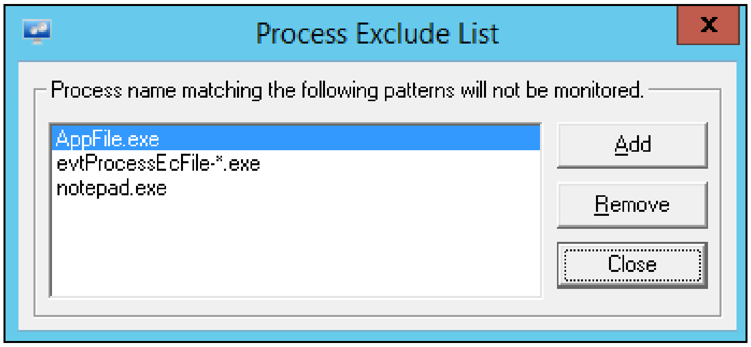
3 Click **Monitor Processes** tab.

EventTracker opens the '**Monitor Processes'** tab.

4 Select the **Enable Process Monitoring** checkbox, if not selected.

5 Select **App Exceptions**.

EventTracker opens '**Process Exclude List**' dialog box.



Process Exclude List

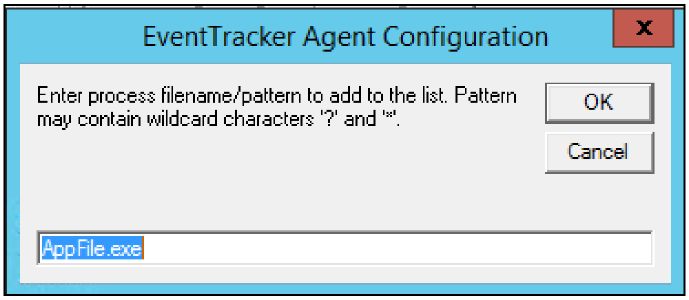
Process name matching the following patterns will not be monitored.

AppFile.exe
evtProcessEcFile-*.exe
notepad.exe

Figure 738

6 Click **Add**.

EventTracker opens a textbox to type the file name of the process.



EventTracker Agent Configuration

Enter process filename/pattern to add to the list. Pattern may contain wildcard characters '?' and '*'.

AppFile.exe

Figure 739

7 Type the application name with .exe extension that you do not want to monitor.

For Example: AppFile.exe

NOTE

The process name should be in .exe format.

8 Click **OK** and then click **Save**.

35.10.3 Filtering processes that need to be monitored

1 To filter applications that need to be monitored, double click **EventTracker Control Panel**, select **EventTracker Agent Configuration**.

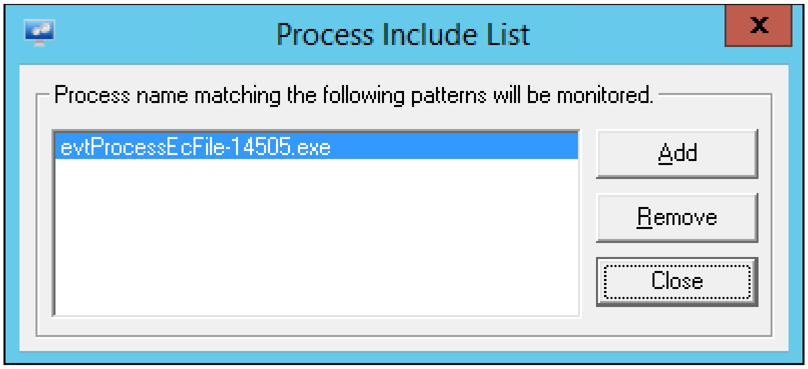
2 Select the system from the **Select System** drop down. Click **Monitor Processes** tab.

EventTracker opens the '**Monitor Processes'** tab.

3 Select the **Enable Process Monitoring** checkbox, if not selected

4 Click **Include List**.

EventTracker opens '**Process Include List**' dialog box.



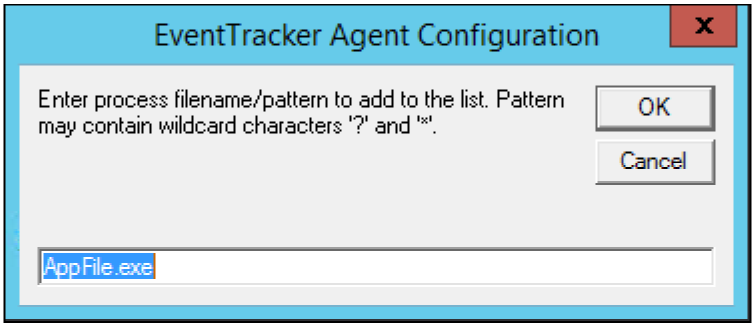
Process name matching the following patterns will be monitored.

evtProcessEcFile-14505.exe

Figure 740

5 Click **Add**.

EventTracker opens a textbox to type the file name of the process.



Enter process filename/pattern to add to the list. Pattern may contain wildcard characters '?' and '*'.

AppFile.exe

Figure 741

6 Type the application name with .exe extension that you want to monitor.

7 Click **OK** and then click **Save**.

35.11 Monitoring 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 restart.

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.

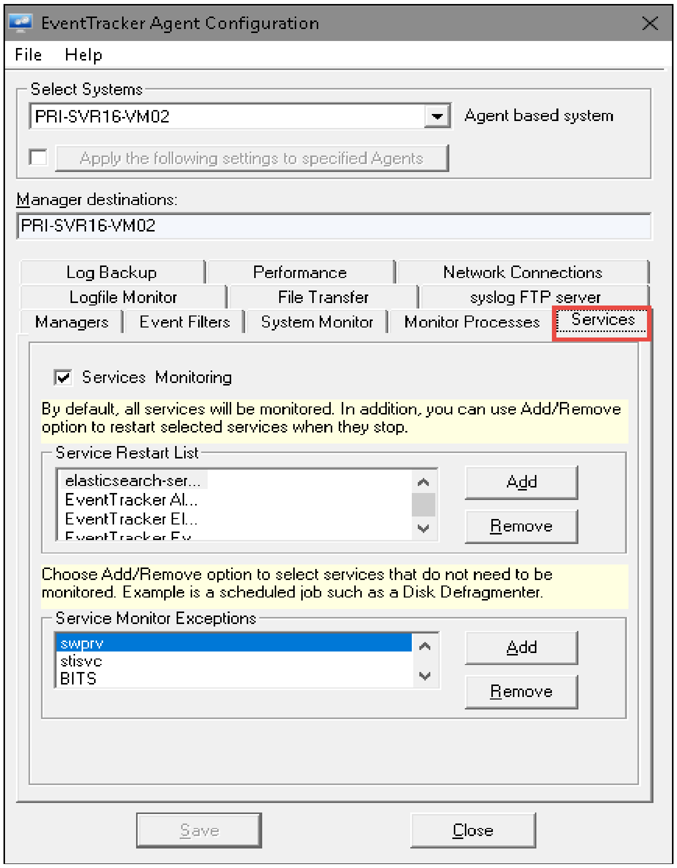
35.11.1 Configuring service restart list

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. Click the **Services** tab.

EventTracker open the **Services** tab.



☑ Services Monitoring

By default, all services will be monitored. In addition, you can use Add/Remove option to restart selected services when they stop.

Choose Add/Remove option to select services that do not need to be monitored. Example is a scheduled job such as a Disk Defragmenter.

Figure 742

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; EventTracker Elasticsearch Indexer EventTracker EventVault; TrapTracker EventTracker Indexer; EventTracker Reporter EventTracker Receiver; WcwService EventTracker Remoting; EventTracker Scheduler Click Add to add selected services to restart when they stop. Click 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.

Table 82

3 Click **Add** under **Service Restart List**.
EventTracker open the **Enter Service Name** field to type the name of the service.

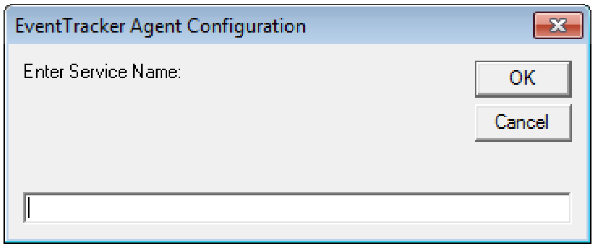


Figure 743

4 Type the name of the service, and then click **OK**.

5 Click **Save**.

35.11.2 Filtering 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 **Add** 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**.

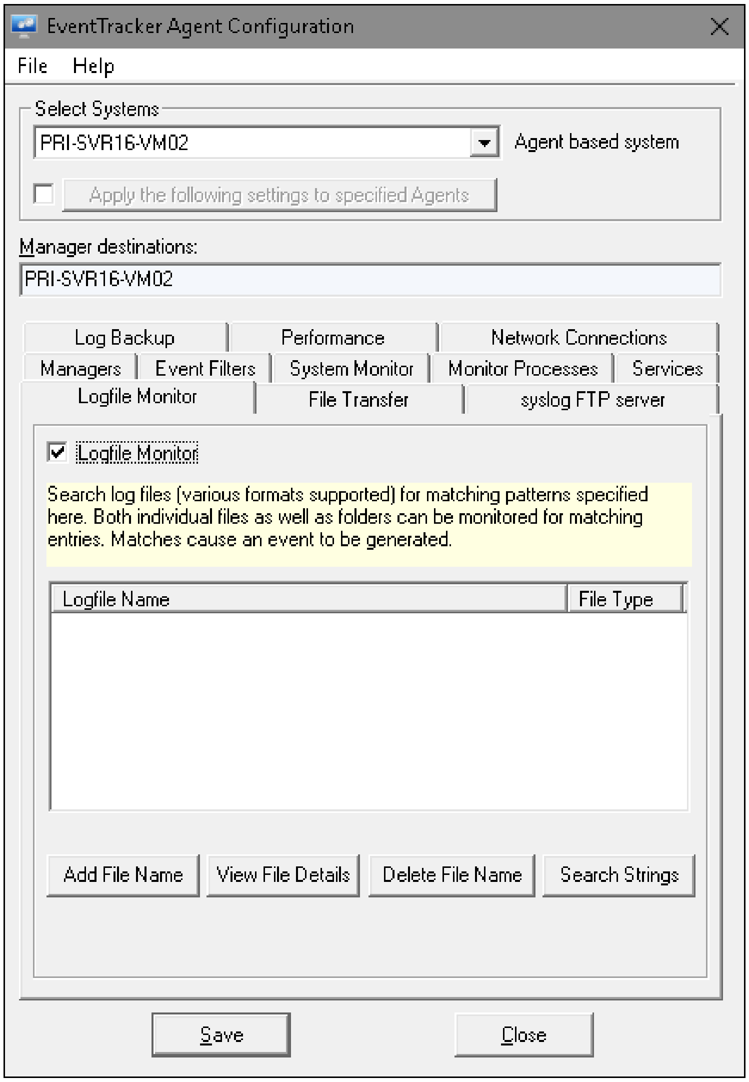
35.12 Logfile Monitor

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 (Web GUI), you can only view the Logfile monitoring settings.

1 Double-click **EventTracker Agent Configuration** on the **EventTracker Control Panel**.

2 Select the system from the **Select System** drop-down, and then select **Logfile Monitor** tab.

EventTracker opens the 'Logfile Monitor' tab.



Search log files (various formats supported) for matching patterns specified here. Both individual files as well as folders can be monitored for matching entries. Matches cause an event to be generated.

Logfile Name	File Type

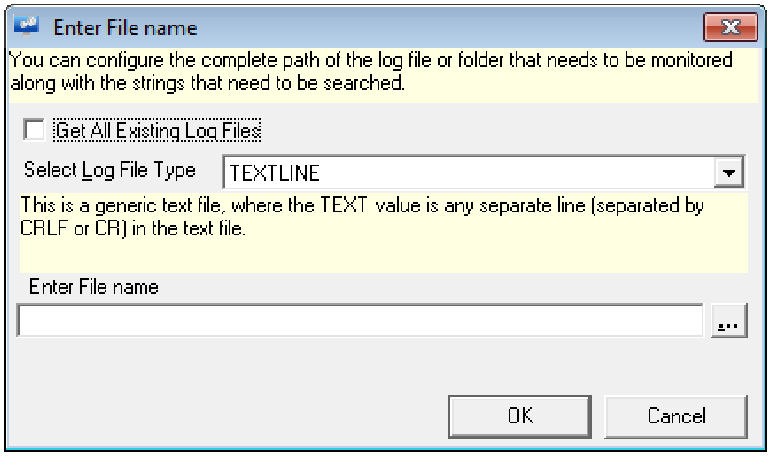
Figure 744

Click	To
Add File Name	Add a log file that you wish to monitor.
View File Details	View log file details.
Delete File Name	Delete the log file name from the list.
Search Strings	Configure the strings to search.

Table 83

3 Click **Add File Name**.

EventTracker opens the ‘Enter File Name’ window.



You can configure the complete path of the log file or folder that needs to be monitored along with the strings that need to be searched.

□ Get All Existing Log Files

Select Log File Type: TEXTLINE

This is a generic text file, where the TEXT value is any separate line (separated by CRLF or CR) in the text file.

Enter File name:

Figure 745

NOTE

We have provided standard and custom date and time formats to configure Agent LFM. Now the configured files in the Agent LFM will be parsed as per the selected date and time formats.

For more Information, refer: https://www.netsurion.com/Corporate/media/Corporate/Files/Support-Docs/Enhancement-in-LFM-to-consider-the-date-and-time-mentioned-in-the-log-file.pdf

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 **Browse** to locate the log file.

EventTracker opens the 'Select Folder/File Name' dialog box.

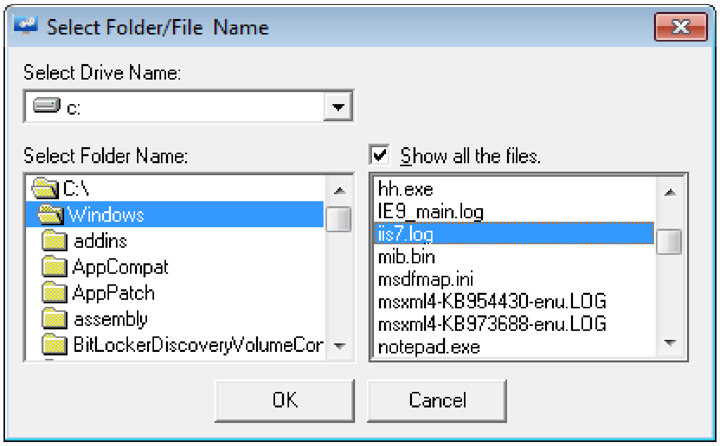


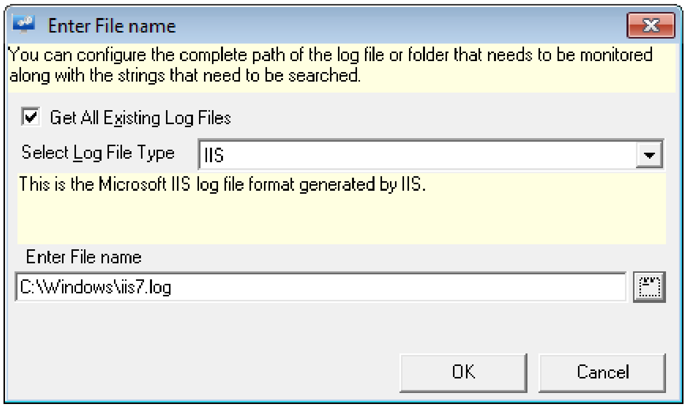
Figure 746

7 In **Select Folder name:** select appropriate folder associated with selected Log File Type.

8 Select the **Show all the files** checkbox to view all files with different file extensions.

9 Click **OK**.

EventTracker opens the 'Enter File Name' window with the file location.



You can configure the complete path of the log file or folder that needs to be monitored along with the strings that need to be searched.

☑ Get All Existing Log Files

Select Log File Type: IIS

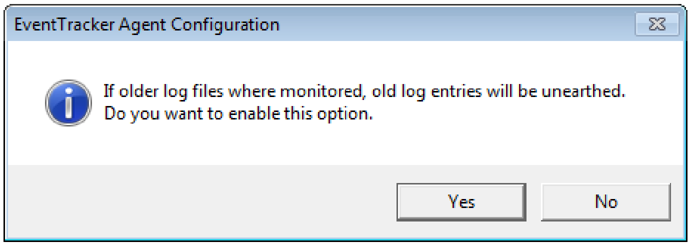
This is the Microsoft IIS log file format generated by IIS.

Enter File name: C:\Windows\iis7.log

Figure 747

10 Click **OK**.

EventTracker opens the 'EventTracker Agent Configuration' message box.

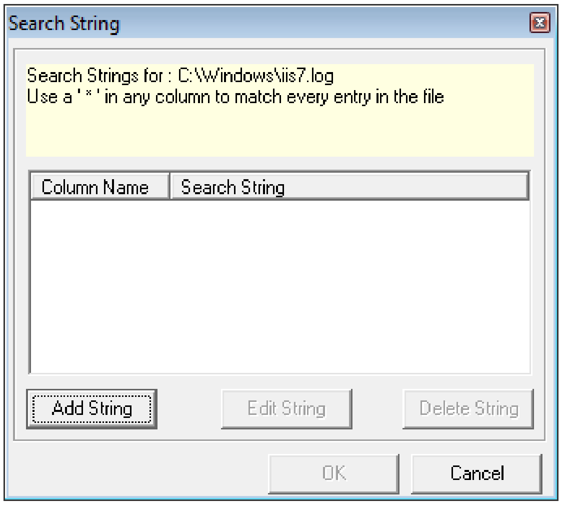


If older log files where monitored, old log entries will be unearthed.
Do you want to enable this option.

Figure 748

11 Click **Yes**.

EventTracker opens the Search String dialog box.



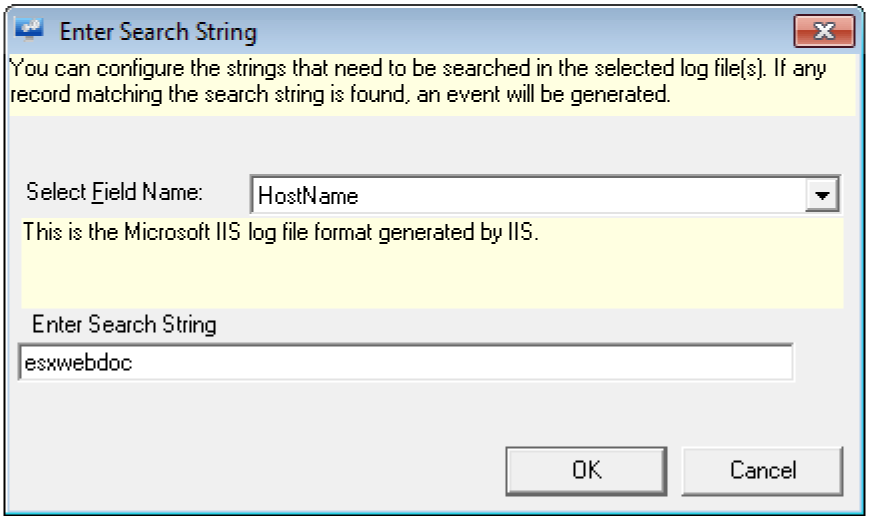
Search Strings for : C:\Windows\iis7.log
Use a ' * ' in any column to match every entry in the file

Column Name	Search String

Figure 749

12 Click **Add String**.

EventTracker opens the 'Enter Search String' dialog box.



You can configure the strings that need to be searched in the selected log file(s). If any record matching the search string is found, an event will be generated.

Select Field Name: HostName

This is the Microsoft IIS log file format generated by IIS.

Enter Search String: esxwebdoc

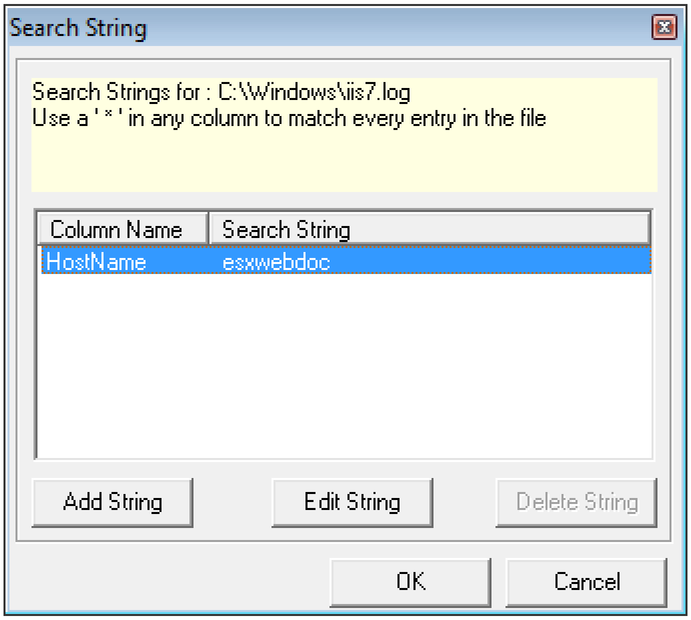
Figure 750

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 opens the Enter Search String dialog box.

15 Click **OK**.

EventTracker opens the Search String dialog box.



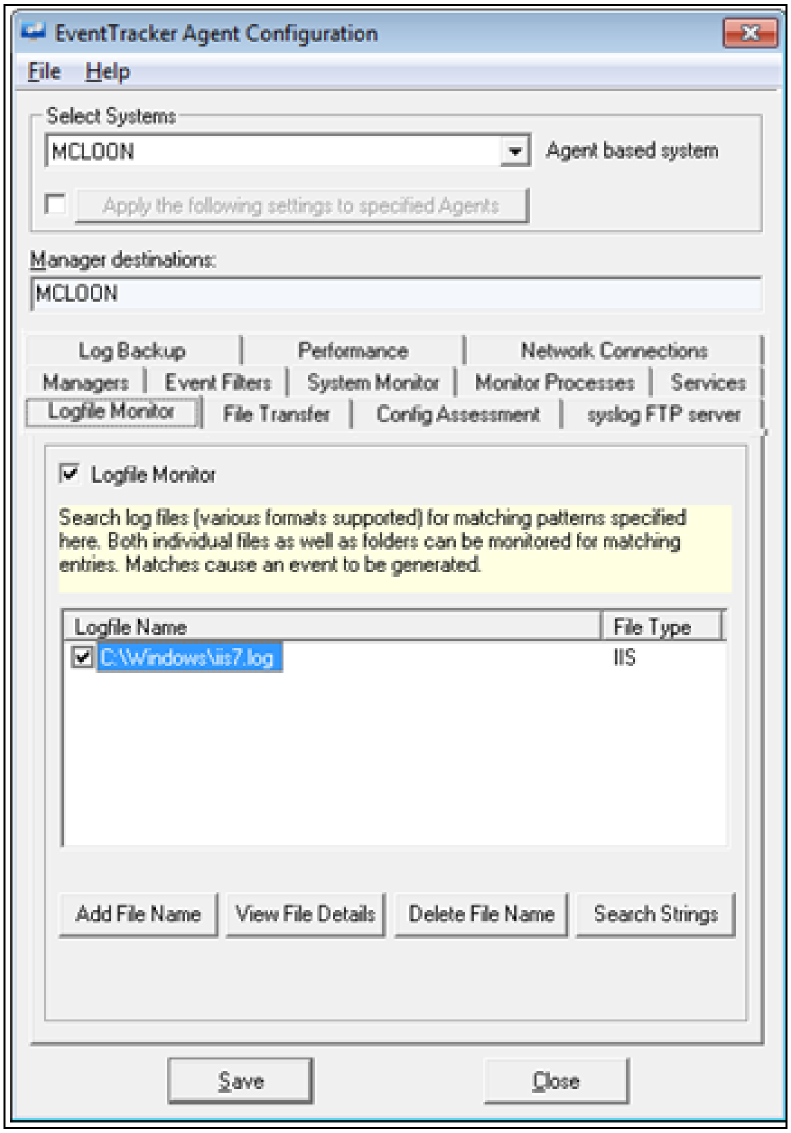
Search Strings for : C:\Windows\iis7.log
Use a ' * ' in any column to match every entry in the file

Column Name	Search String
HostName	esxwebdoc

Figure 751

16 Click **OK**.

EventTracker opens the ‘Agent Configuration’ window with the newly added Logfile entry.



Search log files (various formats supported) for matching patterns specified here. Both individual files as well as folders can be monitored for matching entries. Matches cause an event to be generated.

Logfile Name	File Type
☑ C:\Windows\iis7.log	IIS

Figure 752

17 Click **Save**.

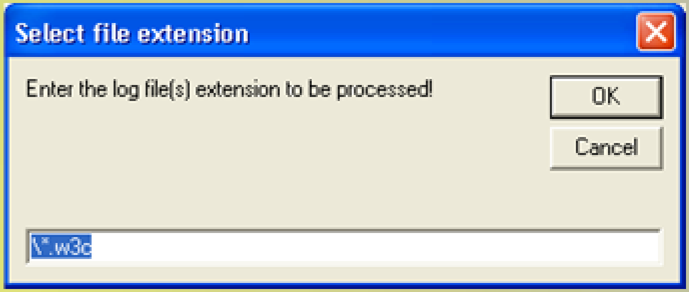
GOOD TO KNOW:

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.

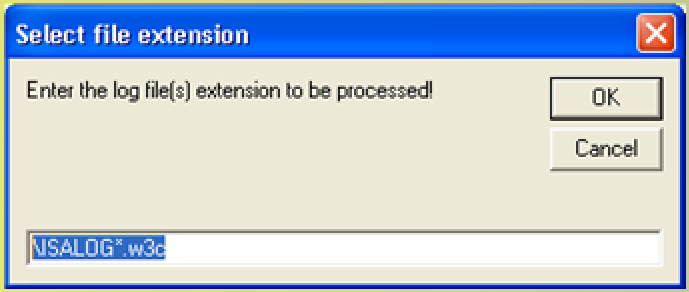


Enter the log file(s) extension to be processed!

*.w3c

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.

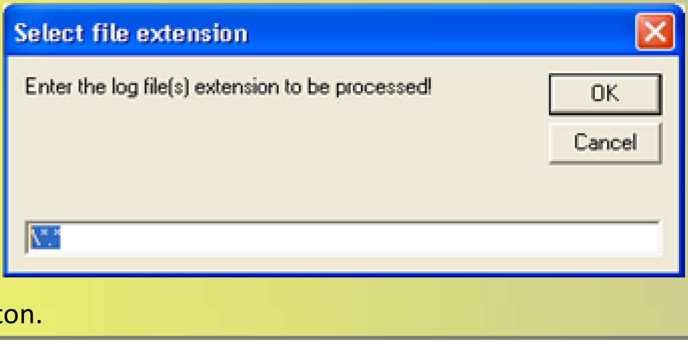
If you are specifically interested in monitoring ISA Firewall log files, type the file name as "**ISALOG***"



Enter the log file(s) extension to be processed!

\ISALOG*.w3c

To select multiple files irrespective of file extensions, type '***.***'.



Enter the log file(s) extension to be processed!

.

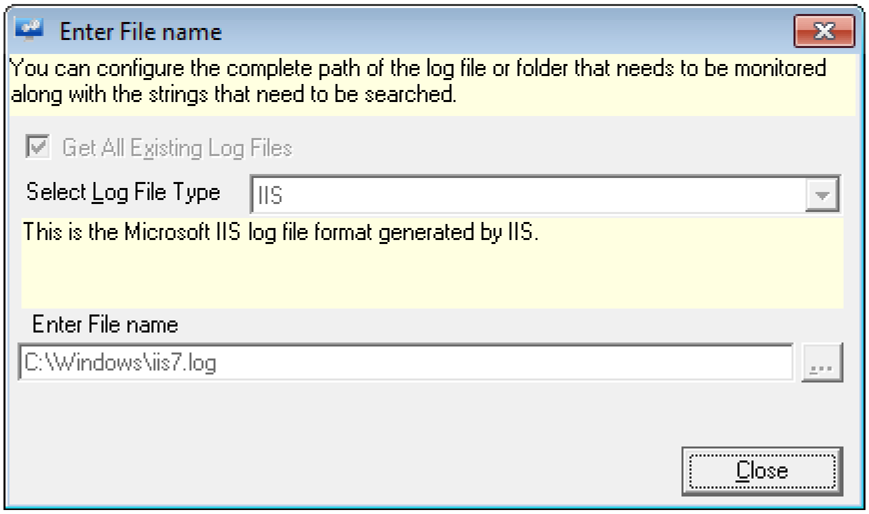
1. Click the **OK** button.

Figure 753

35.12.1 Viewing 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 opens the 'Enter File Name' window.



You can configure the complete path of the log file or folder that needs to be monitored along with the strings that need to be searched.

☑ Get All Existing Log Files

Select Log File Type: IIS

This is the Microsoft IIS log file format generated by IIS.

Enter File name: C:\Windows\iis7.log

Figure 754

6 Click **Close**.

35.12.2 Deleting Log File Monitoring Settings

This option helps you delete log file monitoring settings.

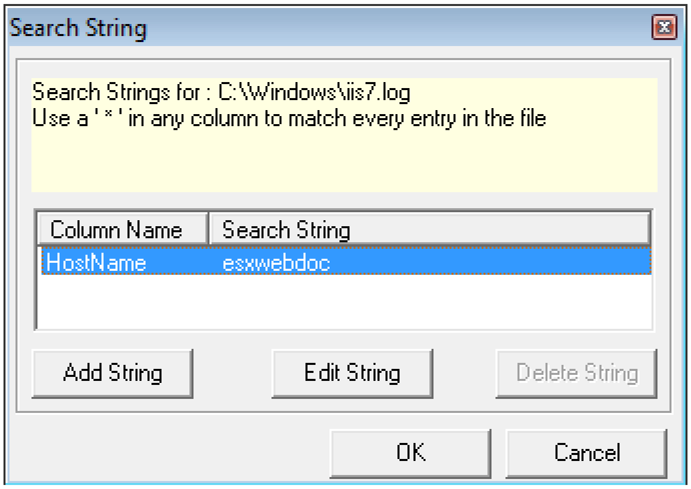
1 To delete log file monitor settings in EventTracker Control panel, open the **EventTracker Agent Configuration** window.
2 Select the system from the **Select Systems** drop-down list, and then select the **Logfile Monitor** tab.
3 Select the log file from the **Logfile Name** list, and then select **Delete File Name**.
4 Click **Save** on the Agent Configuration window.

35.12.3 Search Strings option

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.

3 Click the **Logfile Monitor** tab.
4 Select the log file from the **Logfile Name** list.
5 Click **Search Strings**.



Search Strings for : C:\Windows\iis7.log
Use a ' * ' in any column to match every entry in the file

Column Name	Search String
HostName	esxwebdoc

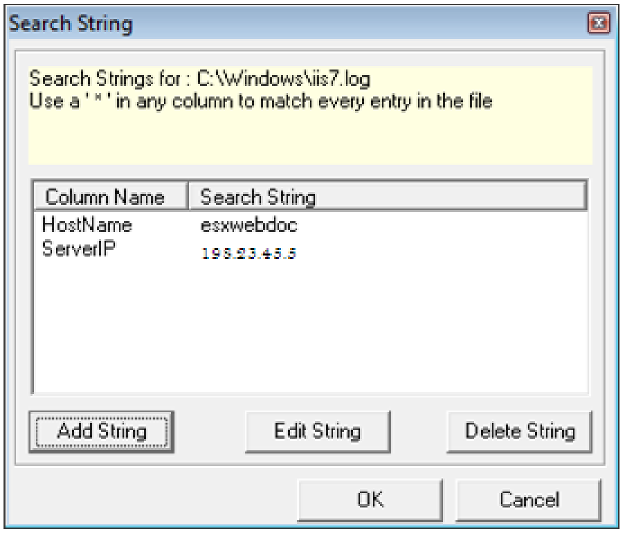
Figure 755

6 Click **Add String**.

EventTracker opens the Enter Search String dialog box.

7 Select the file name from the **Select Field Name** drop-down list.
8 Type the string that you want to search in the **Enter Search String** field.

EventTracker opens the Enter Search String dialog box with newly added search string entry.



Search Strings for : C:\Windows\iis7.log
Use a ' * ' in any column to match every entry in the file

Column Name	Search String
HostName	esxwebdoc
ServerIP	193.23.45.5

Figure 756

9 Click **OK**.

EventTracker opens 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.

10 Click **OK** on the 'Search String' dialog box.

EventTracker opens the 'Agent Configuration' window with the modified settings.

11 Click **Save**.

NOTE: When LFM is configured there are possibilities that CPU usage of the EventTracker Agent might go high.

35.12.4 Monitoring Check Point Logs

This option helps you monitor logs generated by Check Point.

NOTE

Severity level of mapping for Checkpoint logs with EventTracker log and event type is given in the table below.

Checkpoint log attribute (ET event category)	Checkpoint log attribute value	EventTracker log type	EventTracker Event type
Alert 0 ("Alert')	Alert	Application	Warning
Alert 1 ("snmptrap')	snmptrap	Application	Warning
Alert 2("mail')	Mail	Application	Warning
Alert 3 ("useralert')	Useralert	Application	Warning
Alert 4 ("useralert2')	Useralert2	Application	Warning
Alert 5 ("useralert3')	Useralert3	Security	Audit Failure
Audit Status 0	Failure	Security	Audit Success
Audit Status 0	*	Security	Audit Success
* 0	*	Application	Information

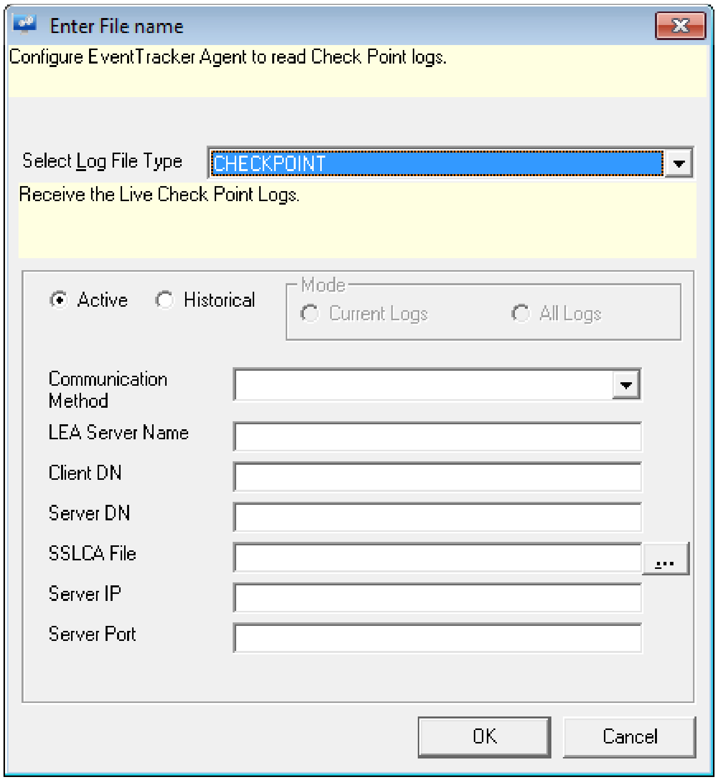
Table 84

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 **Add File Name**.

EventTracker opens the Enter File Name dialog box.

4 Select the logfile type as ‘**CHECKPOINT**’ from the **Select Log File Type** drop-down list.

EventTracker unfolds a pane with configuration options.



Enter File name

Configure EventTracker Agent to read Check Point logs.

Select Log File Type: CHECKPOINT

Receive the Live Check Point Logs.

● Active ○ Historical

Figure 757

5 Select an option from the **Communication Method** drop-down list.

Communication method options	Description
OPSEC_SSLCA	Encryption Method: 3DES Compressed: No
OPSEC_SSLCA_COMP	Encryption Method: 3DES Compressed: Yes

Table 85

6 Type **LEA Server Name**. Type the **Client DN**.
Check Point generated this string while configuring the OPSEC Application.

7 Type the **Server DN**.
This is the Check Point Gateway DN.

8 Click **Browse** ... to locate SSLCA file.

9 Select the SSLCA file and then click **Open**.
EventTracker populates the SSLCA file field

10 Type the **Server IP**.
This is the IP of the host where Check Point is installed.

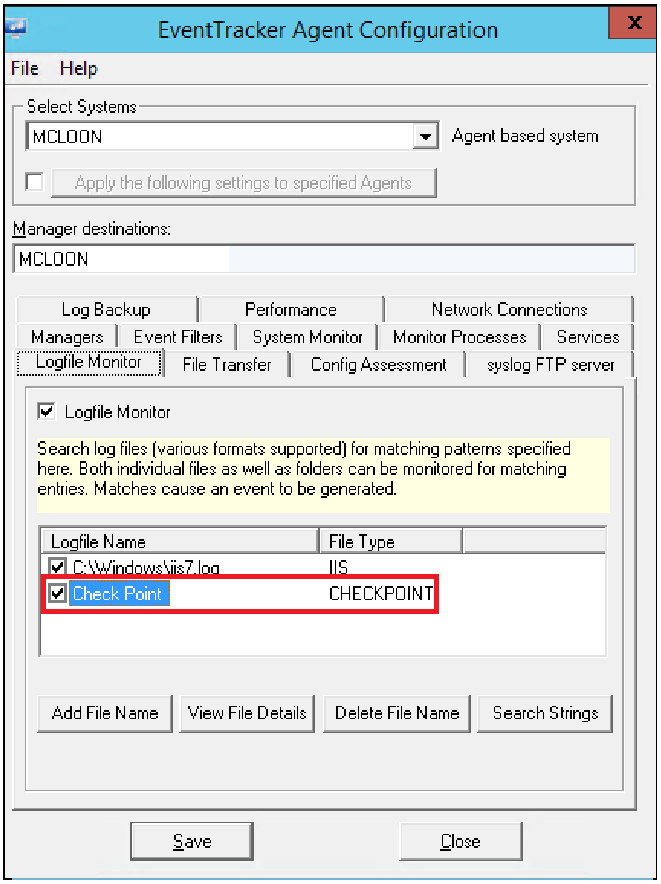
11 Type the **Server Port**.
This can be any port but should be consistent with what you have entered earlier in the fwopsec.conf file.

Field	Description
Active	This option is selected by default. Select this option to receive live Check Point logs from the point in time the configuration takes effect.
Historical	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.

Table 86

12 Click **OK**.

EventTracker opens the 'Agent Configuration' window.



Select Systems: MCLOON — Agent based system

□ Apply the following settings to specified Agents

Manager destinations: MCLOON

☑ Logfile Monitor

Search log files (various formats supported) for matching patterns specified here. Both individual files as well as folders can be monitored for matching entries. Matches cause an event to be generated.

Logfile Name	File Type
☑ C:\Windows\iis7.log	IIS
☑ Check Point	CHECKPOINT

Figure 758

13 Click **Save**.

For information regarding How to configure EventTracker Agent to read CheckPoint logs, please refer https://www.netsurion.com/Corporate/media/Corporate/Files/Support-Docs/How-to-Configure-CheckPoint-Logs.pdf

35.12.5 Monitoring VMware Logs

This option helps you monitor logs generated by VMware. VMware severity values are mapped to EventTracker event types.

The mapping of VMware log severity value:

VMware severity	ET event type	Description
Error	Error	If VMware logs on severity value as 'Error', then EventTracker agent also generates event type as Error.
Info	Information	If VMware logs on severity value as 'Info', then EventTracker agent generates event type as Information.
Warning	Warning	If VMware generates logs on severity value as 'Warning', then EventTracker generates event type as Warning.
User	Information	If VMware generates log with severity value 'User', then EventTracker generates event type as Information.

Table 87

The mapping of VMware task state with event type:

Task State	ET Event type	Description
Error	Error	If VMware logs on Task state as 'Error', then EventTracker agent also generates event type as Error.
Queued	Information	If VMware logs on Task state as 'Queued', then EventTracker agent generates event type as Information.
Running	Information	If VMware logs on Task state as 'Running', then EventTracker agent generates event type as Information.
Success	Audit Success	If VMware logs on Task state as 'Success', then EventTracker agent generates event type as Audit Success.

Table 88

1 To monitor VMware logs in **EventTracker Control Panel**, open the **EventTracker Agent Configuration** window.

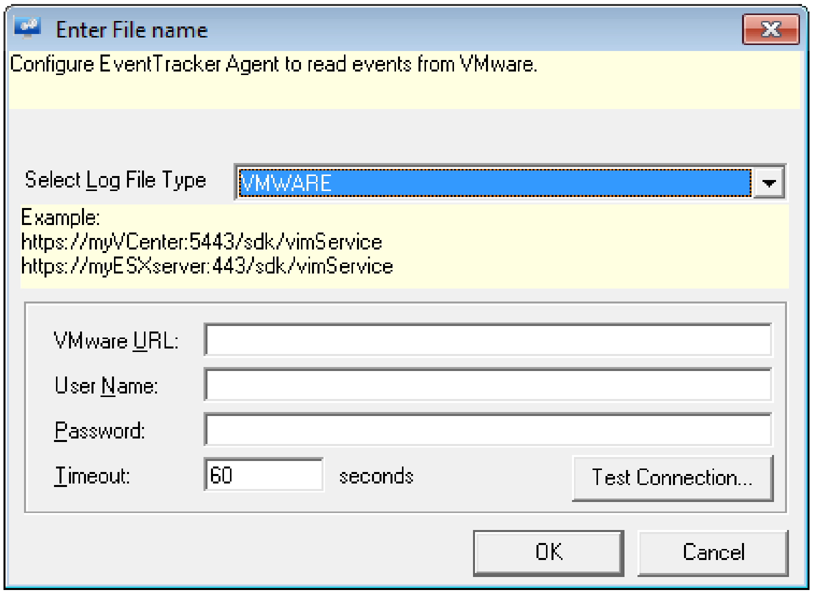
2 Select the system from the **Select System** drop-down list.

3 Click the **Logfile Monitor** tab.

4 Click **Add File Name**.

EventTracker opens 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.



Enter File name

Configure EventTracker Agent to read events from VMware.

Select Log File Type: VMWARE

Example:
https://myVCenter:5443/sdk/vimService
https://myESXserver:443/sdk/vimService

VMware URL:

User Name:

Password:

Timeout: 60 seconds

Figure 759

Field	Description
VMware URL	Type a valid URL, e.g. https://esxvcserver/sdk/vimService You can also replace the server name with the IP address.
User Name	Type valid user name.
Password	Type valid password.
Timeout	Connection timeout.

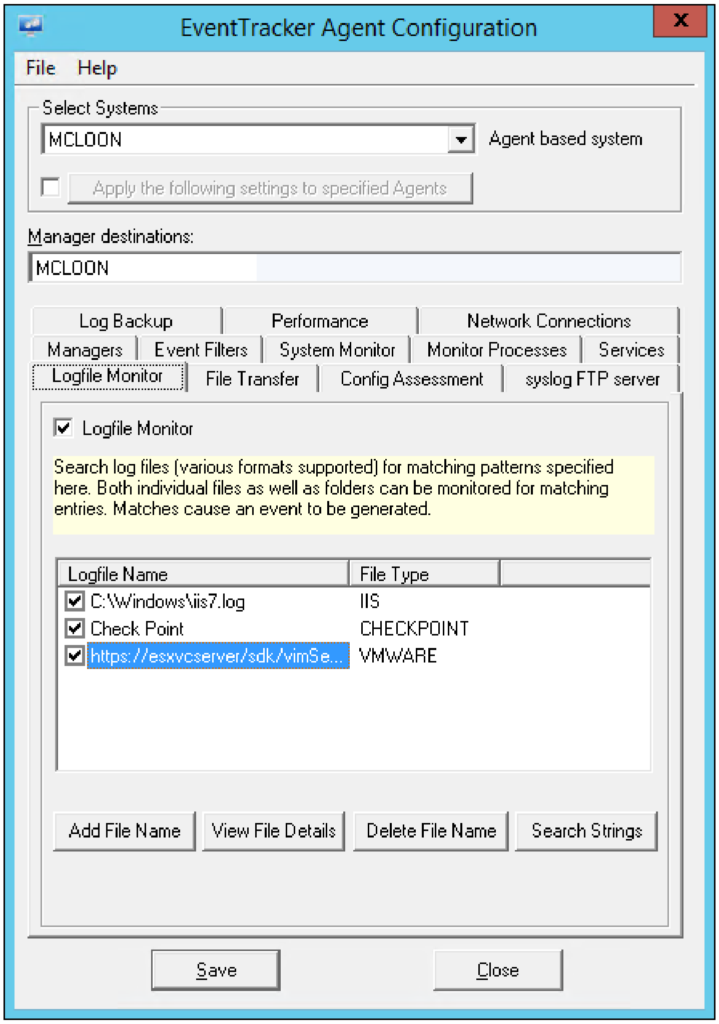
Table 89

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 opens the Agent Configuration window.



Search log files (various formats supported) for matching patterns specified here. Both individual files as well as folders can be monitored for matching entries. Matches cause an event to be generated.

Logfile Name	File Type
☑ C:\Windows\iis7.log	IIS
☑ Check Point	CHECKPOINT
☑ https://esxvcserver/sdk/vimSe...	VMWARE

Figure 760

9 Click **Save**.

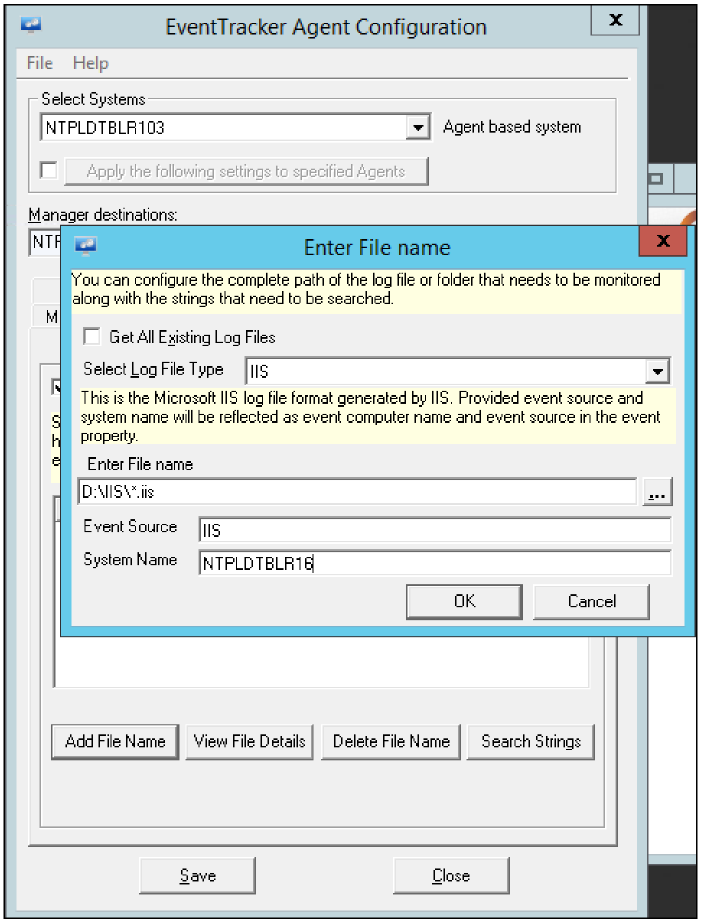
35.12.6 Specifying the System Name and Event Source for LFM logs

An option is provided to get the log source and computer name from user(s) for all supported format.

Event id 3230 will get generated based on this property. If user does not give any value then by default it will consider Source as "EventTracker" and System Name as "Local computer name"

1. Select **Add File Name**.

NOTE: System name allowed special characters are “-“and “_”.



You can configure the complete path of the log file or folder that needs to be monitored along with the strings that need to be searched.

□ Get All Existing Log Files

Select Log File Type: IIS

This is the Microsoft IIS log file format generated by IIS. Provided event source and system name will be reflected as event computer name and event source in the event property.

Enter File name: D:\IIS\*.iis

Event Source: IIS

System Name: NTPLDTBLR16

Figure 761

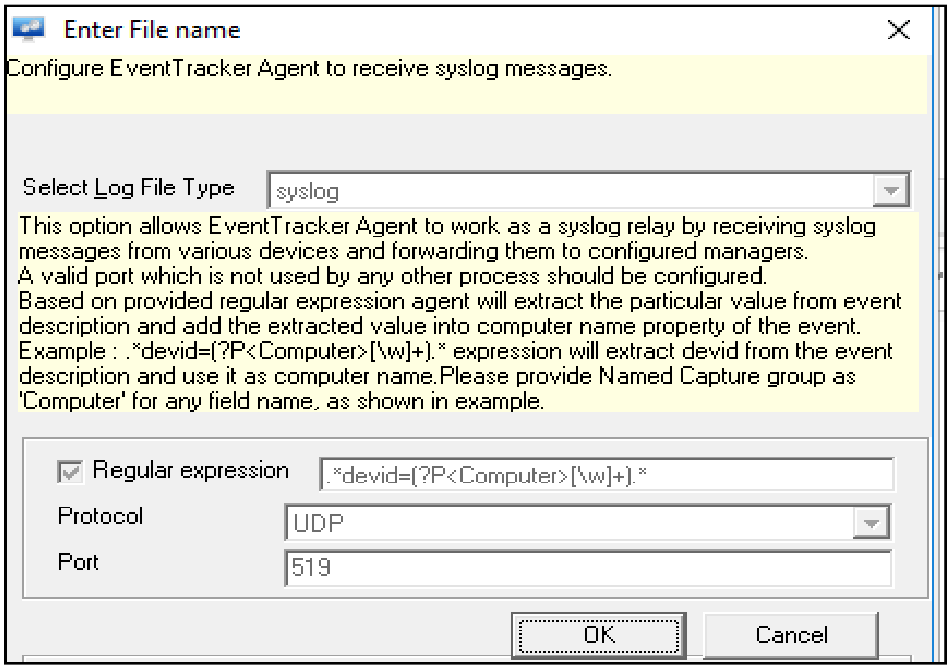
2. In the Enter File Name window, enter the file path, the Event Source and the System name and click **OK**.

NOTE: For VMware, Checkpoint, Evt and syslog, this new option will not be available.

35.12.7 Extracting Device ID from syslog devices

Another enhancement is extracting the device ID from syslog device while it is relaying. It will extract the Device ID from event description by using regular expression. After extracting the value from description it assigns it to "Computer Name" standard property.

Example: FG1K5D3I14802285@ntpldtblr104-syslog



Configure EventTracker Agent to receive syslog messages.

Select Log File Type syslog

This option allows EventTracker Agent to work as a syslog relay by receiving syslog messages from various devices and forwarding them to configured managers.
A valid port which is not used by any other process should be configured.
Based on provided regular expression agent will extract the particular value from event description and add the extracted value into computer name property of the event.
Example : .*devid=(?P<Computer>[\w]+).* expression will extract devid from the event description and use it as computer name.Please provide Named Capture group as 'Computer' for any field name, as shown in example.

☑ Regular expression .*devid=(?P<Computer>[\w]+).*

Protocol UDP

Port 519

Figure 762

NOTE: The allowed special characters for system name are ".", "_" and "-"

35.12.8 Monitoring 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.

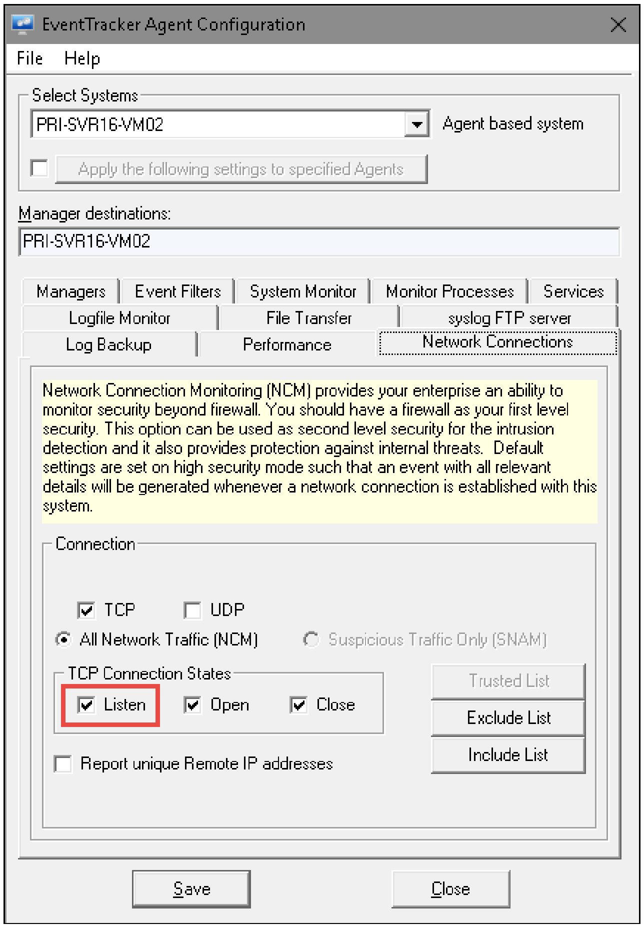
The NCM functionality facilitates to achieve the following key objectives:

- 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

35.12.9 Monitoring 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 Connections** tab.

EventTracker opens the 'Network Connection' tab.



EventTracker Agent Configuration

Select Systems: PRI-SVR16-VM02 — Agent based system

□ Apply the following settings to specified Agents

Manager destinations: PRI-SVR16-VM02

Network Connection Monitoring (NCM) provides your enterprise an ability to monitor security beyond firewall. You should have a firewall as your first level security. This option can be used as second level security for the intrusion detection and it also provides protection against internal threats. Default settings are set on high security mode such that an event with all relevant details will be generated whenever a network connection is established with this system.

Connection

☑ TCP □ UDP

● All Network Traffic (NCM) ○ Suspicious Traffic Only (SNAM)

TCP Connection States: ☑ Listen ☑ Open ☑ Close

□ Report unique Remote IP addresses

Figure 763

🗎 NOTE

- The "Listen" option is provided to monitor the process whose ports are in listen state. The option will be disabled by default. The user needs to enable it for monitoring the ports in listen state.

For more information, refer: https://www.netsurion.com/Corporate/media/Corporate/Files/Support-Docs/Enhancement-in-Network-monitoring-to-monitor-listening-ports.pdf

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	
Listen	To monitor the process whose ports are in listen state.
Open	This checkbox is selected by default to monitor opened TCP/UDP connections.
Close	This checkbox is selected by default to monitor closed TCP/UDP connections.
All Network Traffic (NCM): By default, EventTracker selects this option.	
Exclude List	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.
Include List	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'.
Suspicious Traffic Only (SNAM)	
Trusted List	Click this button to view and configure trusted network connections.

Table 90

4 Select or clear the **TCP** or **UDP** checkbox.

5 Click **Save**.

35.12.10 Excluding Network Connections

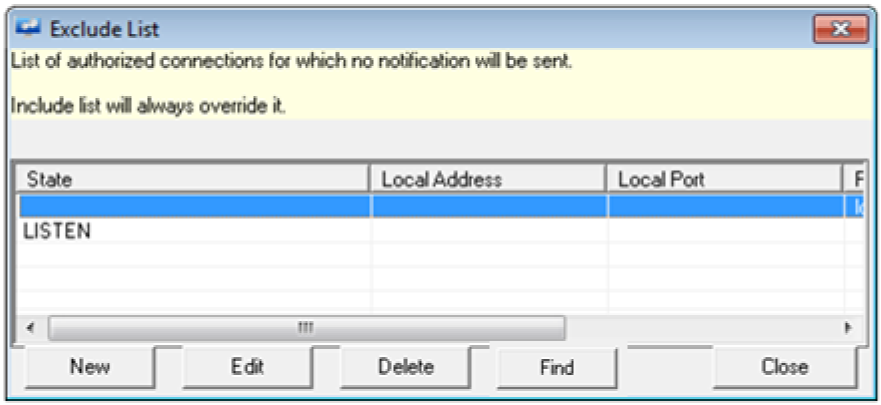
1 Double click **EventTracker Control Panel**; select '**EventTracker Agent Configuration'**.

2 Select the system from the **Select System** hyperlink. Select **Network Connections** tab.

EventTracker opens the 'Network Connections' tab.

3 Select **Exclude List**.

EventTracker displays the Exclude List pop-up window.



Exclude List

List of authorized connections for which no notification will be sent.

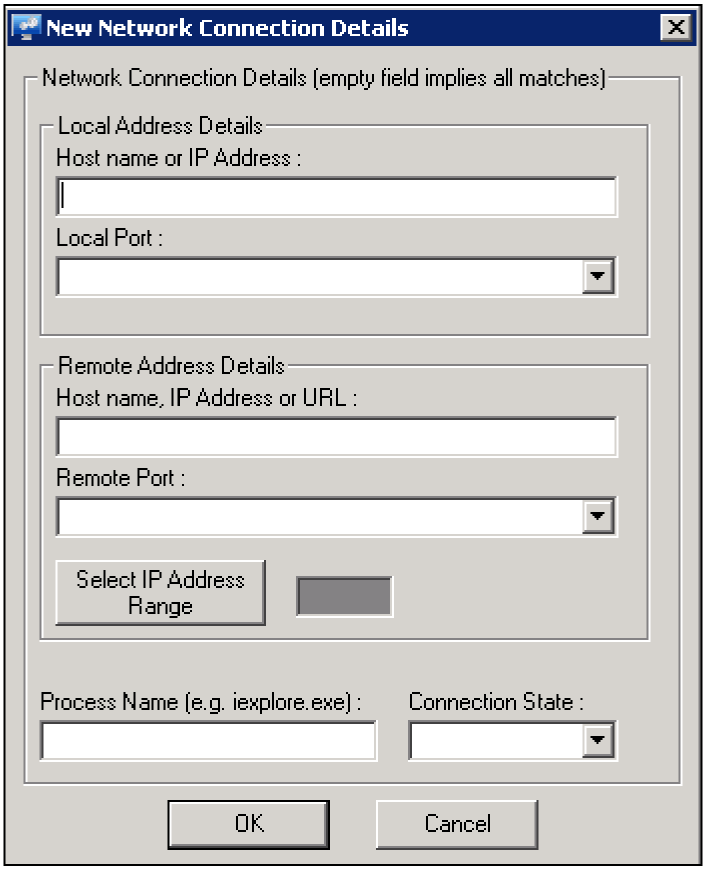
Include list will always override it.

State	Local Address	Local Port	F
LISTEN			

Figure 764

4 Click **New**.

EventTracker opens the Exclude List window to type New Network Connection Details.



New Network Connection Details

Network Connection Details (empty field implies all matches)

Local Address Details

Host name or IP Address :

Local Port :

Remote Address Details

Host name, IP Address or URL :

Remote Port :

Process Name (e.g. iexplore.exe) :

Connection State :

Figure 765

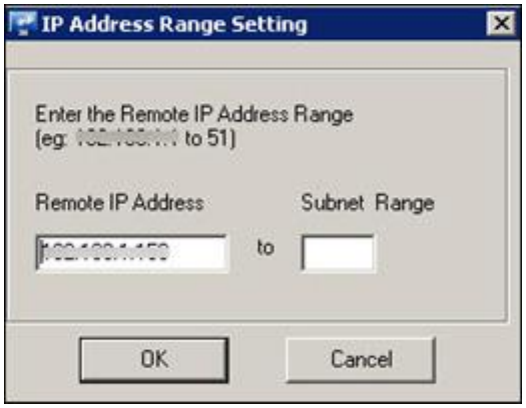
Field	Description
Local Address Details	
Host Name or IP Address	Type the host name or the IP address in this field.
Local Port	Select a local port from the drop-down list.
Remote Address Details	
Host name, IP Address or URL	Type the host name, IP address or URL in this field.
Remote Port	Select a remote port from the drop-down list.
Select IP Address Range	Click this button to add IP address range. EventTracker displays the IP Address Range Setting dialog box.  Enter the Remote IP Address Range (eg: [redacted] to 51) Remote IP Address: [redacted] to Subnet 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 Host name, IP address or URL field.
Process Name	Type the process name in this field.
Connection State	Select a connection state from the drop-down list.

Table 91

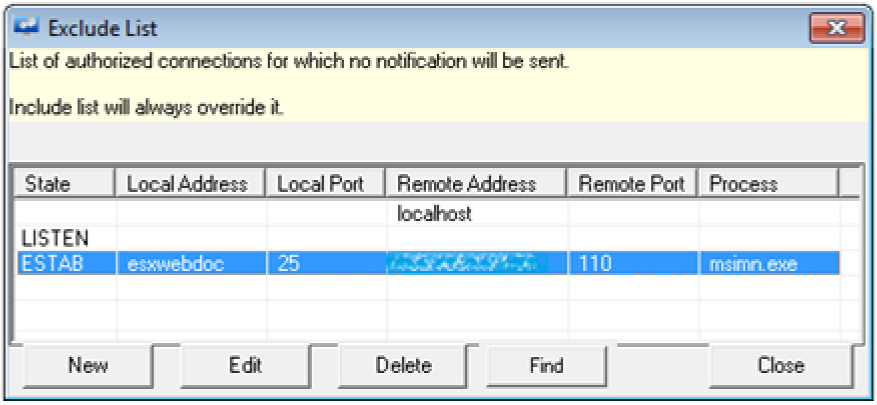
🗎 NOTE

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.

5 Enter appropriate data in relevant fields.

6 Click **OK**.

EventTracker opens the Exclude List with the newly added entry.



List of authorized connections for which no notification will be sent.

Include list will always override it.

State	Local Address	Local Port	Remote Address	Remote Port	Process
			localhost		
LISTEN					
ESTAB	esxwebdoc	25	[redacted]	110	msimn.exe

Figure 766

7 To modify the network connection details, click **Edit**.

8 To delete the network connection details, select the network connection details you want to delete from the list, and then click **Delete**.

9 To find network connection detail, click the **Find** button and enter appropriate data in the required field.

10 Click **Close** on the Exclude List pop-up window.

11 Click **Save**.

35.12.11 Including 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 Connections** tab.

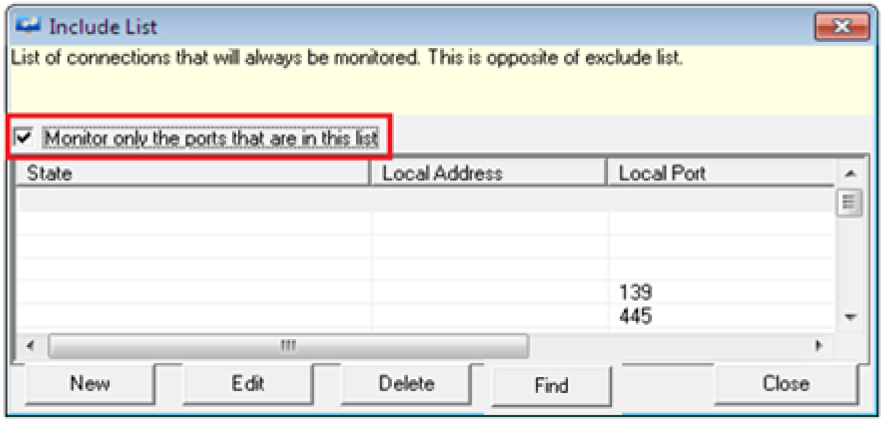
EventTracker opens the 'Network Connection' tab.

4 Select the appropriate checkboxes.

5 Click **Include List**.

EventTracker opens 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

List of connections that will always be monitored. This is opposite of exclude list.

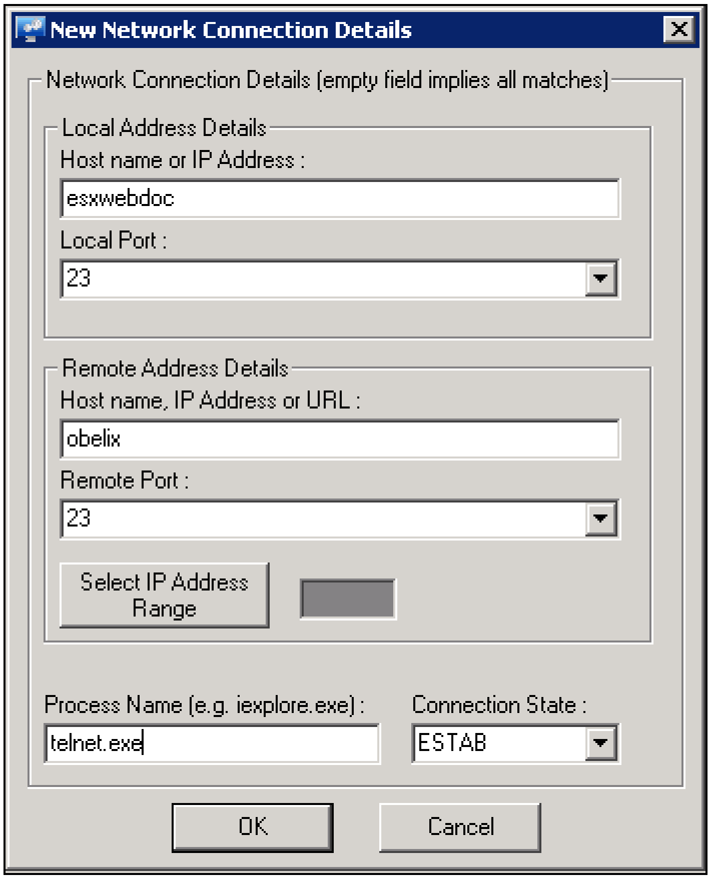
☑ Monitor only the ports that are in this list

State	Local Address	Local Port
		139
		445

Figure 767

7 To add more network connection details, click **New**.
EventTracker opens the Include List window to type the New network connection details.

8 Enter appropriate data in the relevant fields.



New Network Connection Details

Network Connection Details (empty field implies all matches)

Local Address Details

Host name or IP Address : esxwebdoc

Local Port : 23

Remote Address Details

Host name, IP Address or URL : obelix

Remote Port : 23

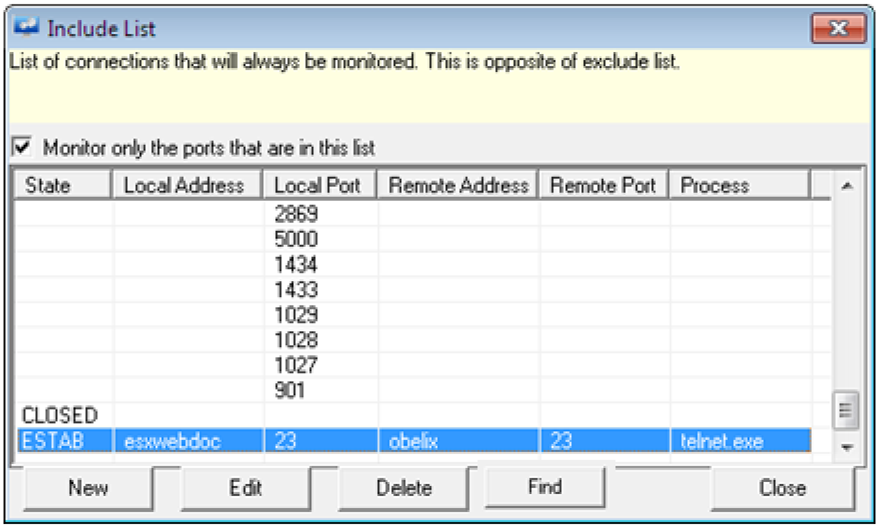
Process Name (e.g. iexplore.exe) : telnet.exe

Connection State : ESTAB

Figure 768

9 Click **OK**.

EventTracker opens the Include List with the newly added entry.



List of connections that will always be monitored. This is opposite of exclude list.

☑ Monitor only the ports that are in this list

State	Local Address	Local Port	Remote Address	Remote Port	Process
		2869			
		5000			
		1434			
		1433			
		1029			
		1028			
		1027			
		901			
CLOSED					
ESTAB	esxwebdoc	23	obelix	23	telnet.exe

Figure 769

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**.

35.12.12 Suspicious Connections feature

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.

35.12.13 Monitoring 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.

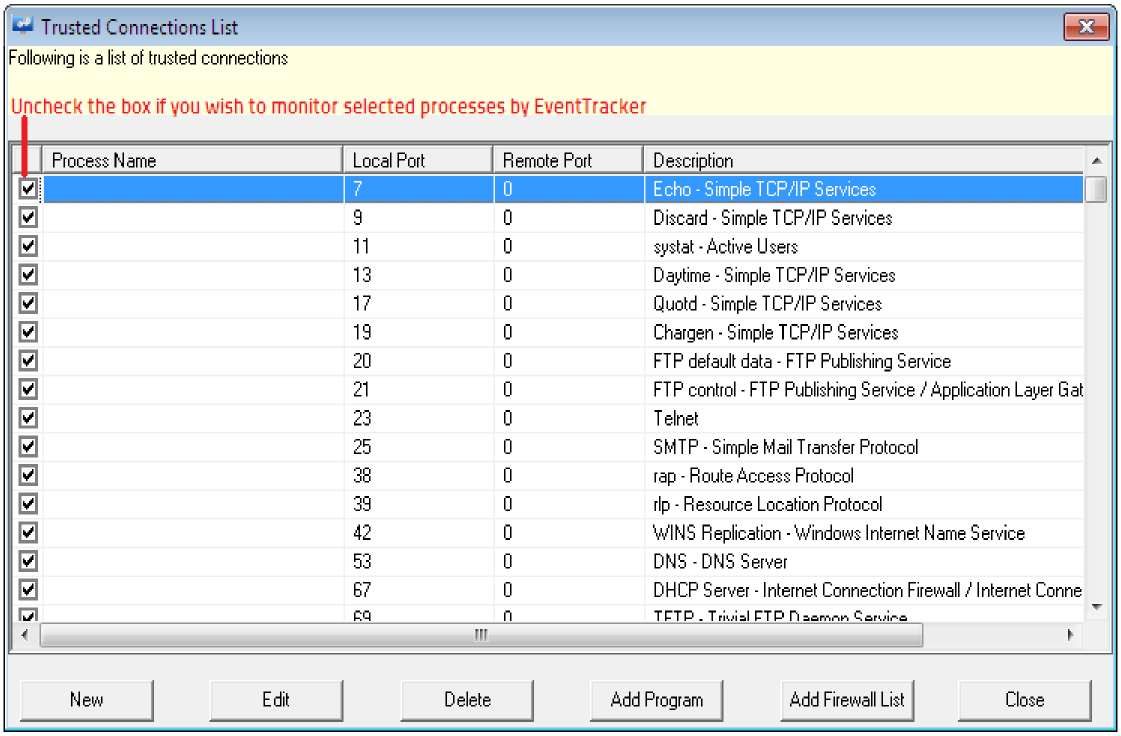
1 To view Trusted List in EventTracker Control panel, open the **EventTracker Agent Configuration** window.

2 Select the system from the **Select Systems** drop-down list.

3 Click the **Network Connections** tab.

EventTracker opens the Network Connections tab.

4 Select **Suspicious Traffic Only (SNAM)** option. Select the **Trusted List** button. EventTracker opens the 'Trusted Connections List' dialog box



Trusted Connections List

Following is a list of trusted connections

Uncheck the box if you wish to monitor selected processes by EventTracker

	Process Name	Local Port	Remote Port	Description
☑		7	0	Echo - Simple TCP/IP Services
☑		9	0	Discard - Simple TCP/IP Services
☑		11	0	systat - Active Users
☑		13	0	Daytime - Simple TCP/IP Services
☑		17	0	Quotd - Simple TCP/IP Services
☑		19	0	Chargen - Simple TCP/IP Services
☑		20	0	FTP default data - FTP Publishing Service
☑		21	0	FTP control - FTP Publishing Service / Application Layer Gat
☑		23	0	Telnet
☑		25	0	SMTP - Simple Mail Transfer Protocol
☑		38	0	rap - Route Access Protocol
☑		39	0	rlp - Resource Location Protocol
☑		42	0	WINS Replication - Windows Internet Name Service
☑		53	0	DNS - DNS Server
☑		67	0	DHCP Server - Internet Connection Firewall / Internet Conne
☑		69	0	TFTP - Trivial FTP Daemon Service

Figure 770

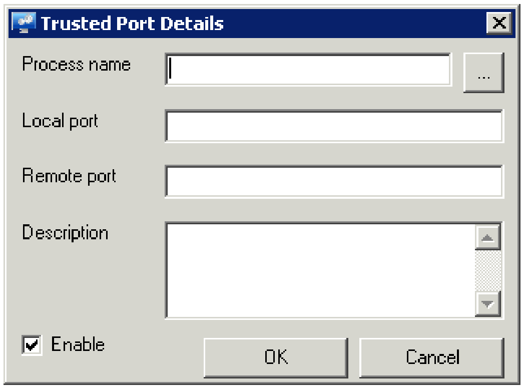
Click	To
New	Add new trusted connections. EventTracker opens Trusted Port Details' dialog box.  Trusted Port Details Process name ... Local port Remote port Description OK Cancel ☑ Enable **Type appropriate details in the relevant fields and then click OK. You can use wild cards to search processes. 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 to locate the process.**
Edit	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.
Delete	Select a process from the list, and then click Delete. EventTracker displays confirmation message box. Click Yes to delete the selected entry.
Add Program	Add programs installed in your computer to the trusted list.
Add Firewall List	Add programs included in the Firewall Exceptions list to the trusted list.
Close	Close the 'Trusted Connections List' dialog box.

Table 92

GOOD TO KNOW:

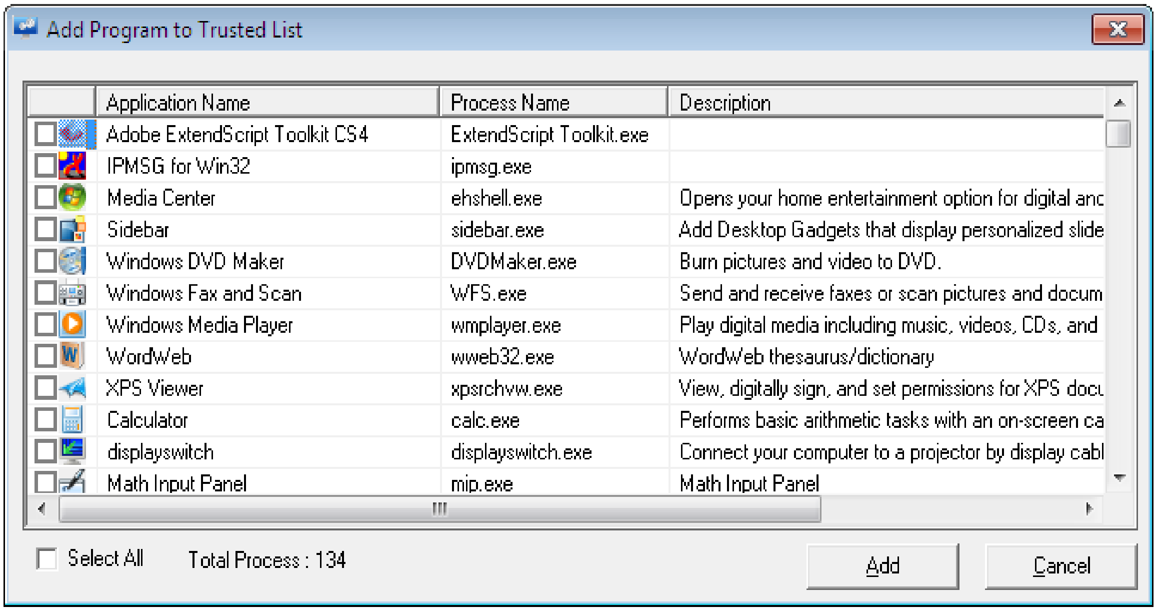
- **Suspicious Traffic Only (SNAM)** option helps you to view, enable, and disable predefined trusted connections list. The connections listed in the **Trusted List** are exempted from monitoring.
- The trusted list contains a list of known good applications and ports through which the usual network 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.

35.12.14 Adding 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 opens the 'Add Program to Trusted List' window.



	Application Name	Process Name	Description
□	Adobe ExtendScript Toolkit CS4	ExtendScript Toolkit.exe	
□	IPMSG for Win32	ipmsg.exe	
□	Media Center	ehshell.exe	Opens your home entertainment option for digital anc
□	Sidebar	sidebar.exe	Add Desktop Gadgets that display personalized slide
□	Windows DVD Maker	DVDMaker.exe	Burn pictures and video to DVD.
□	Windows Fax and Scan	WFS.exe	Send and receive faxes or scan pictures and docum
□	Windows Media Player	wmplayer.exe	Play digital media including music, videos, CDs, and
□	WordWeb	wweb32.exe	WordWeb thesaurus/dictionary
□	XPS Viewer	xpsrchvw.exe	View, digitally sign, and set permissions for XPS docu
□	Calculator	calc.exe	Performs basic arithmetic tasks with an on-screen ca
□	displayswitch	displayswitch.exe	Connect your computer to a projector by display cabl
□	Math Input Panel	mip.exe	Math Input Panel

□ Select All Total Process : 134

Figure 771

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.

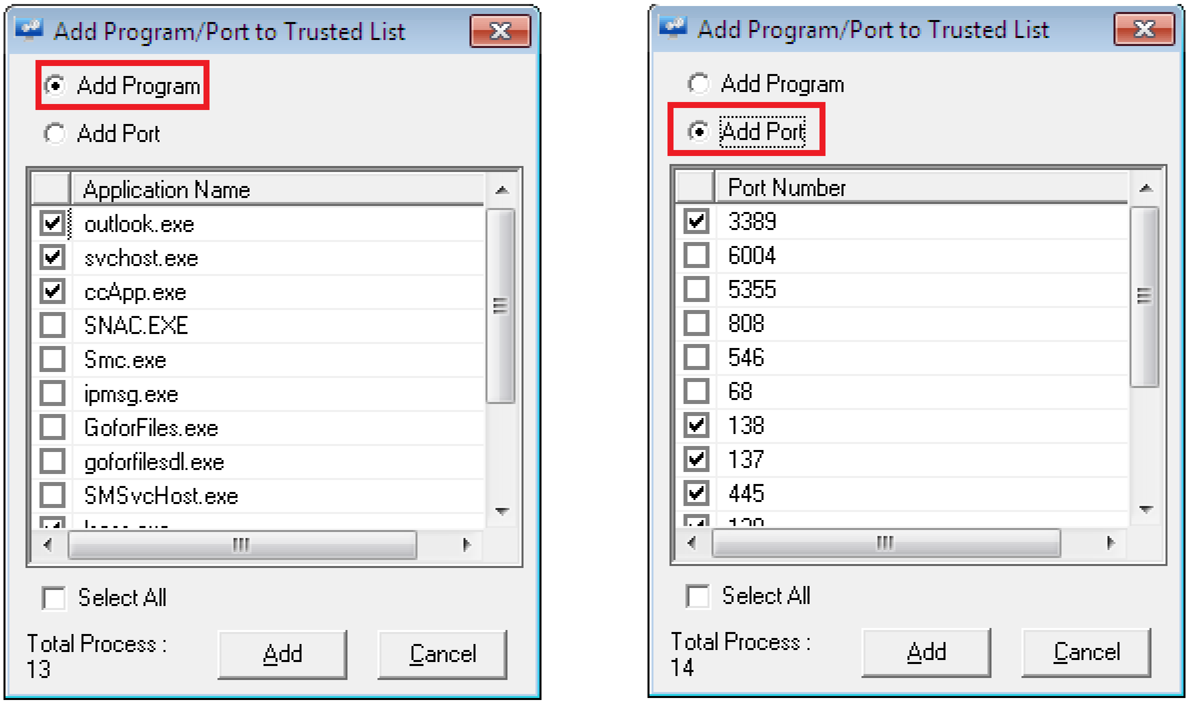
4 Click **Close** and then click **Save**.

35.12.15 Adding 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 opens the 'Add Program/Port to Trusted List' window.



Add Program/Port to Trusted List

● Add Program
○ Add Port

	Application Name
☑	outlook.exe
☑	svchost.exe
☑	ccApp.exe
□	SNAC.EXE
□	Smc.exe
□	ipmsg.exe
□	GoforFiles.exe
□	goforfilesdl.exe
□	SMSvcHost.exe

□ Select All

Total Process : 13

Add Cancel

Add Program/Port to Trusted List

○ Add Program
● Add Port

	Port Number
☑	3389
□	6004
□	5355
□	808
□	546
□	68
☑	138
☑	137
☑	445

□ Select All

Total Process : 14

Add Cancel

Figure 772

By default, EventTracker selects the **Add Program** option and displays the programs in the exceptions list.

(OR)

Select the **Add Port** option, EventTracker opens available ports in the exception list.

2 Select the programs or select the **Select All** checkbox and then select **Add** to add programs to the trusted list.

EventTracker adds the selected items to the 'Trusted Connections' List.

35.13 Monitoring Performance

Performance 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.

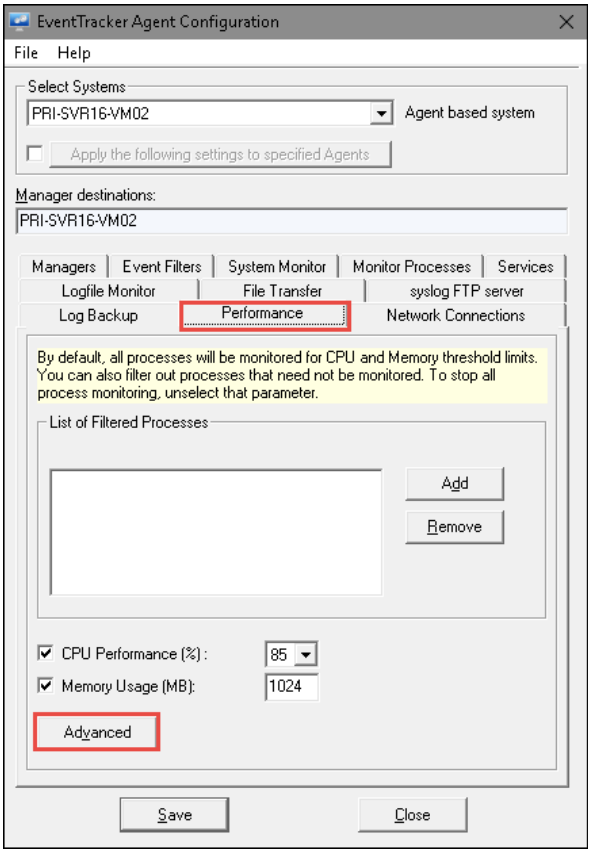
By default, all processes will be monitored, and the default threshold limits are 1024MB of Memory Usage and 85% of CPU.

You can also choose to filter out processes that you do not want to monitor. By default, all processes will be monitored.

35.13.1 Monitoring 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 **Performance** tab.

   EventTracker opens the **Performance** tab.



EventTracker Agent Configuration

File Help

Select Systems

PRI-SVR16-VM02 Agent based system

□ Apply the following settings to specified Agents

Manager destinations:

PRI-SVR16-VM02

Managers | Event Filters | System Monitor | Monitor Processes | Services | Logfile Monitor | File Transfer | syslog FTP server | Log Backup | Performance | Network Connections

By default, all processes will be monitored for CPU and Memory threshold limits. You can also filter out processes that need not be monitored. To stop all process monitoring, unselect that parameter.

List of Filtered Processes

Add

Remove

☑ CPU Performance (%) : 85

☑ Memory Usage (MB): 1024

Advanced

Save Close

Figure 773

Field	Description
☑ CPU Performance (%): 85 ☑ Memory Usage (MB): 1024	
CPU Performance (%)	Select CPU Performance threshold limit from the drop-down list.
Memory Usage (MB)	Type the memory usage threshold limit in MB in this field.
Handle	Select a threshold to monitor handle usage of a running process.
Thread	Select a threshold to monitor thread usage of a running process.
Specific Process	Provide Individual CPU and memory threshold for specific processes.

Table 93

3 Click **Add**.

EventTracker unfolds an option to type the process name.

4 Type the process name in the **Enter Process Name** field.

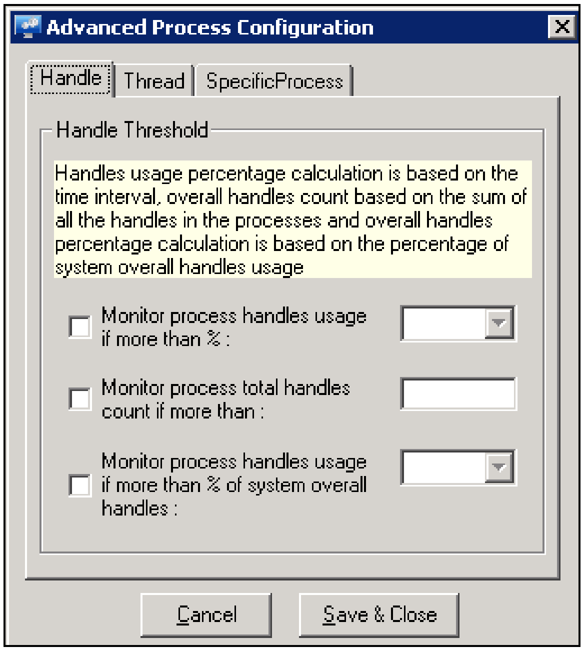
5 Click **OK**.

EventTracker adds the process to the **List of Filtered Processes** pane.

6. Click **Advanced**.

   Advanced Process Configuration window opens.

7. In the **Handle** tab, select the handle counts as per requirement.



Handles usage percentage calculation is based on the time interval, overall handles count based on the sum of all the handles in the processes and overall handles percentage calculation is based on the percentage of system overall handles usage

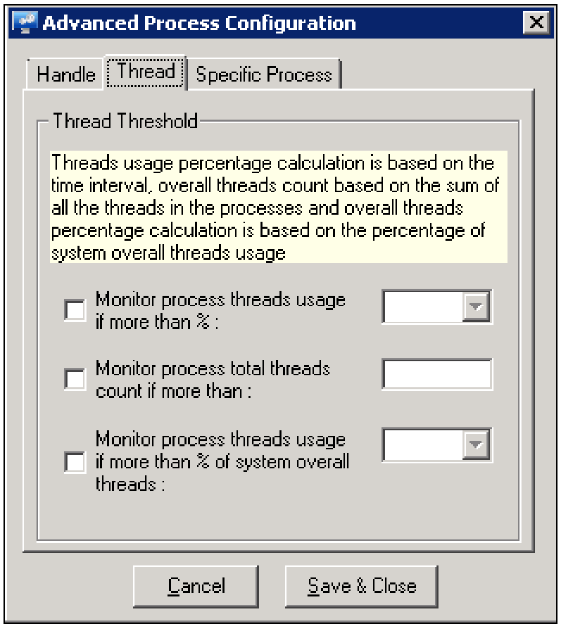
□ Monitor process handles usage if more than % :

□ Monitor process total handles count if more than :

□ Monitor process handles usage if more than % of system overall handles :

Figure 774

8 In the **Thread** tab, select the thread count as per requirement.



Threads usage percentage calculation is based on the time interval, overall threads count based on the sum of all the threads in the processes and overall threads percentage calculation is based on the percentage of system overall threads usage

□ Monitor process threads usage if more than % :

□ Monitor process total threads count if more than :

□ Monitor process threads usage if more than % of system overall threads :

Figure 775

9 In the **Specific Process** tab, enter individual CPU and Memory threshold.

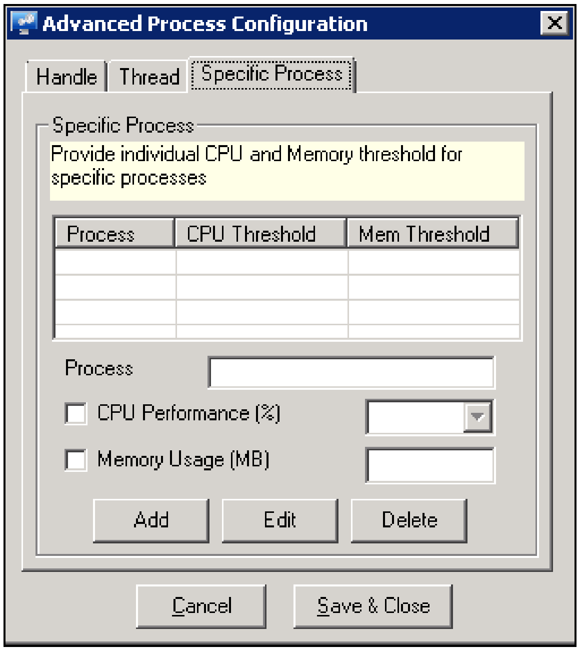


Figure 776

10 Click **Add/Edit/Delete** button as per requirement.

11 Click **Save & Close**.

> 🗎 NOTE
>
> EventTracker generates the process event when the set threshold value crosses the limit for more than 3 minutes.

35.13.2 Removing 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 **Performance** tab. EventTracker displays the **Performance** tab.

3 Select the process from **List of Filtered processes** pane, click **Remove** and then click **Save**.

35.14 Maintaining Log Backup

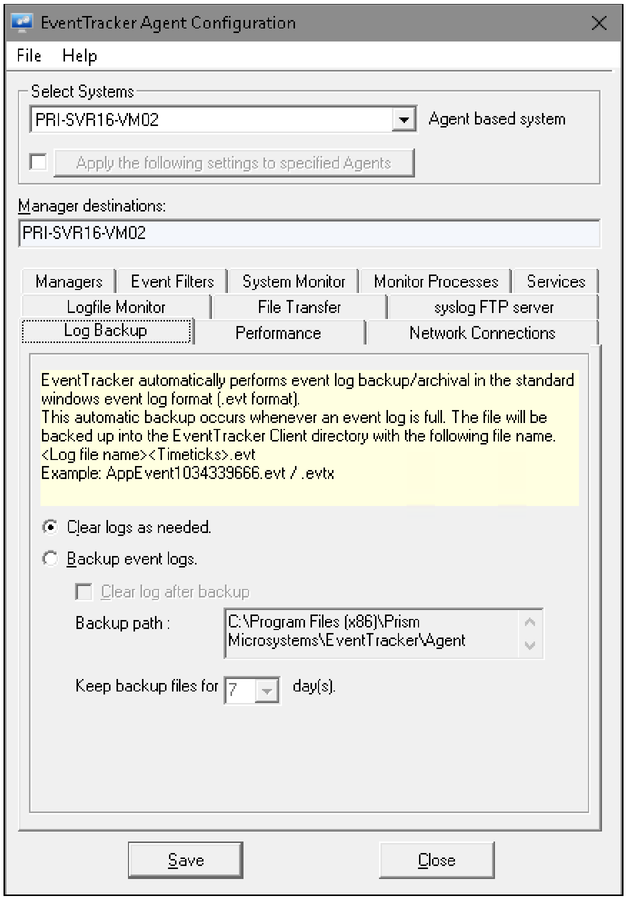
This option enables you to backup event logs automatically in the EventTracker Agent directory whenever the event logs are full. EventTracker automatically performs event log backup or archival in the standard Windows event log format (.evt /.evtx format).

35.14.1 Backing up 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 opens the Log Backup tab.



EventTracker automatically performs event log backup/archival in the standard windows event log format (.evt format).
This automatic backup occurs whenever an event log is full. The file will be backed up into the EventTracker Client directory with the following file name.
<Log file name><Timeticks>.evt
Example: AppEvent1034339666.evt / .evtx

● Clear logs as needed.

○ Backup event logs.

□ Clear log after backup

Backup path : C:\Program Files (x86)\Prism Microsystems\EventTracker\Agent

Keep backup files for 7 day(s).

Figure 777

Field	Description
Clear logs as needed	If selected, EventTracker Agent clears log file if and only if offset error is encountered. After clearing, Agent inserts “3241” event to notify the user. In this case, no backup is taken. This is true for any setting of the Windows Event Log’s “When maximum log size is reached” 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 Log file name: Application Log file backup: Not applicable Log file clear: Success Reason: Received invalid offset error while reading the event log. For more information see Microsoft KB Article #177199.
Backup event logs	If the “Backup event logs” option is selected, and If the offset is lost at any point, no matter whether “Clear log after backup” 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 Log file name: Security Log file backup: C:\Program Files\Prism Microsystems\EventTracker\Agent\ EXCHTEST\ Eventlog_Backup_Security1221683647.evt Log file clear: Success Reason: Invalid offset error while reading the event log. For more information see Microsoft KB Article #177199.
Backup Path	**By default backed up log files are stored in the EventTracker installation folder typically, ...\Program Files\Prism Microsystems\EventTracker\Agent**
Keep backup files for	If selected, backup files older than selected number of days will be automatically deleted by the agent.

Table 94

3 Select the required options and then click **Save**.

35.15 Transferring Log Files

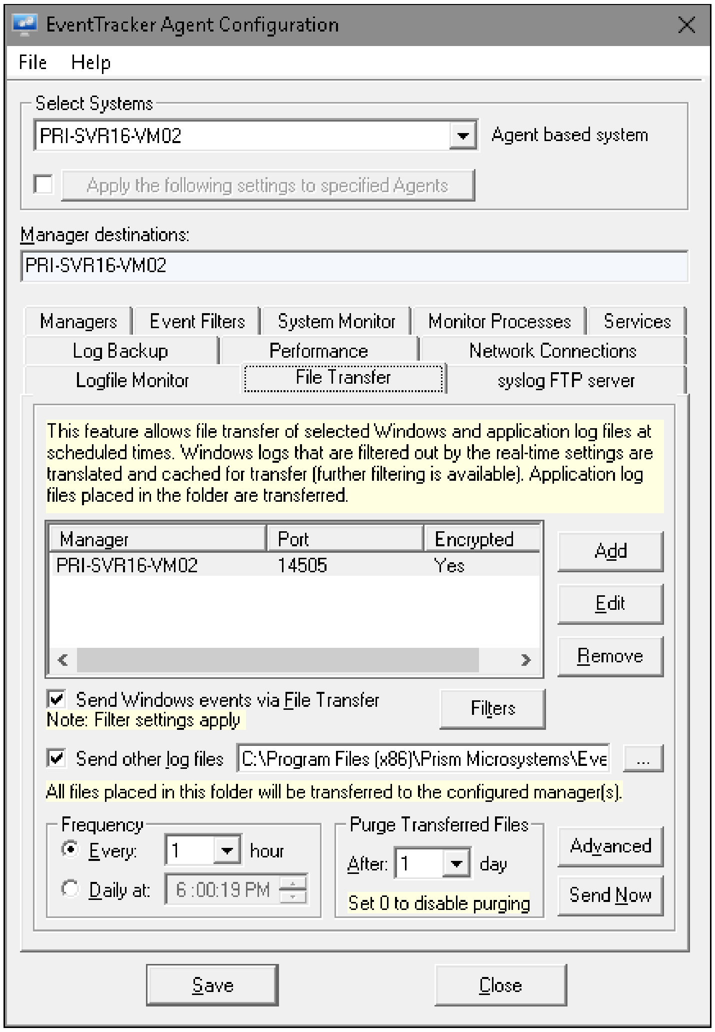
This option enables you to transfer Windows and other application log files at scheduled times to the manager. Windows logs that are filtered out by the real time settings are cached for transfer (further filtering is available). This minimizes the EventTracker Receiver service workload and conserves the network bandwidth.

A new option has been added to configure offline events. To achieve this, configure the port to send offline events.

35.15.1 Transferring 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 opens the **File Transfer tab.**


EventTracker Agent Configuration

Select Systems: PRI-SVR16-VM02 — Agent based system

□ Apply the following settings to specified Agents

Manager destinations: PRI-SVR16-VM02

This feature allows file transfer of selected Windows and application log files at scheduled times. Windows logs that are filtered out by the real-time settings are translated and cached for transfer (further filtering is available). Application log files placed in the folder are transferred.

Manager	Port	Encrypted
PRI-SVR16-VM02	14505	Yes

☑ Send Windows events via File Transfer
Note: Filter settings apply

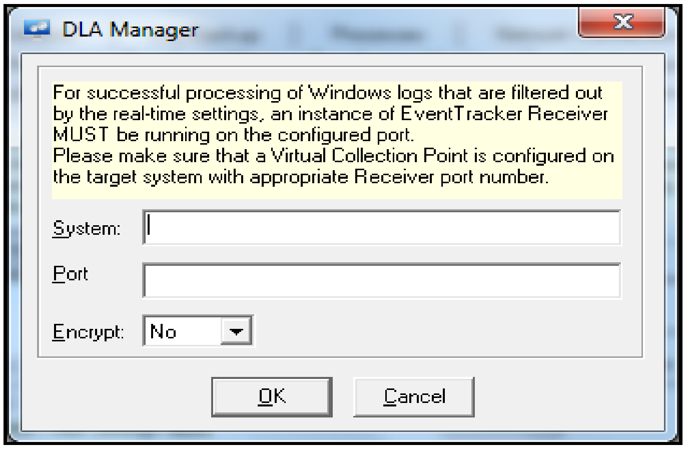
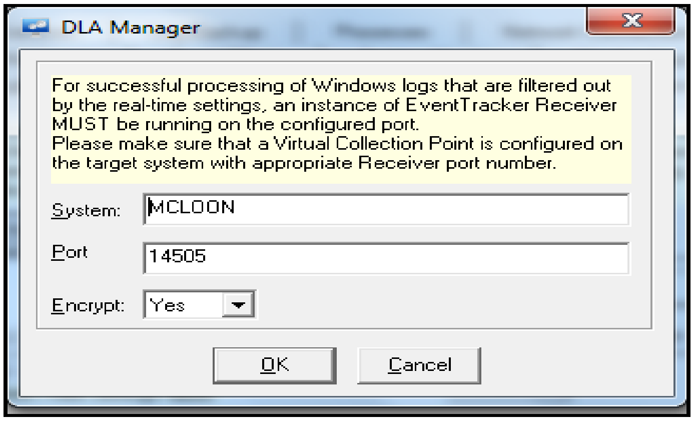
☑ Send other log files C:\Program Files (x86)\Prism Microsystems\Eve

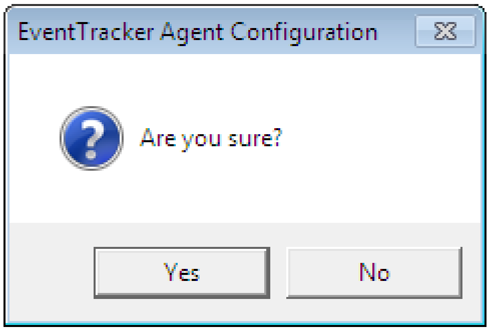
All files placed in this folder will be transferred to the configured manager(s).

Frequency: ● Every: 1 hour; ○ Daily at: 6:00:19 PM

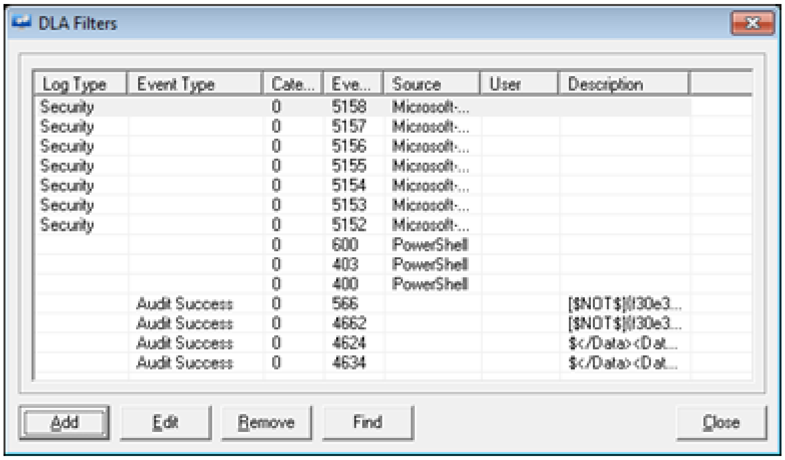
Purge Transferred Files: After: 1 day
Set 0 to disable purging

Figure 778

Click	To
Add	DLA Manager window opens.  DLA Manager For successful processing of Windows logs that are filtered out by the real-time settings, an instance of EventTracker Receiver MUST be running on the configured port. Please make sure that a Virtual Collection Point is configured on the target system with appropriate Receiver port number. System: Port Encrypt: No a) Enter the **System:** name or IP address, Port to configure. b) If the events must be encrypted is required, select **Yes** or **No** as per requirement. c) Select an option from the Encrypt drop-down list to encrypt and securely transfer the cached events to the destination. d) Click OK.
Edit	You can edit the manager name or IP address and even can change the encryption option. a) To update the details of Manager, click the **Edit** button.  DLA Manager For successful processing of Windows logs that are filtered out by the real-time settings, an instance of EventTracker Receiver MUST be running on the configured port. Please make sure that a Virtual Collection Point is configured on the target system with appropriate Receiver port number. System: MCLOON Port 14505 Encrypt: Yes b) Enter required information and then click **OK**.

<table>
<tr>
<td>Remove</td>
<td>Delete the destination, i.e. manager name or IP address.
a) To remove file transferring of events in Manager, click <b>Remove</b>.
EventTracker Agent Configuration opens a message.


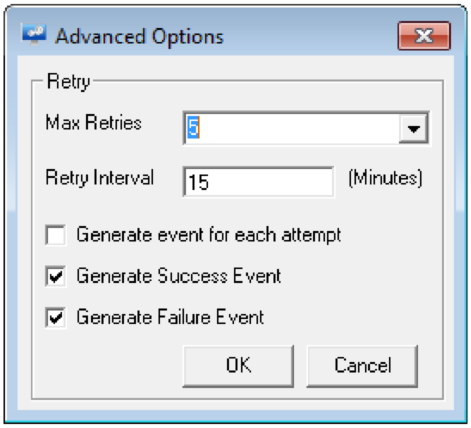
Are you sure?

b) Click <b>Yes</b>.</td>
</tr>
<tr>
<td>Filter</td>
<td>Click <b>Filter</b>.


<table>
<tr><th>Log Type</th><th>Event Type</th><th>Cate...</th><th>Eve...</th><th>Source</th><th>User</th><th>Description</th></tr>
<tr><td>Security</td><td></td><td>0</td><td>5158</td><td>Microsoft-...</td><td></td><td></td></tr>
<tr><td>Security</td><td></td><td>0</td><td>5157</td><td>Microsoft-...</td><td></td><td></td></tr>
<tr><td>Security</td><td></td><td>0</td><td>5156</td><td>Microsoft-...</td><td></td><td></td></tr>
<tr><td>Security</td><td></td><td>0</td><td>5155</td><td>Microsoft-...</td><td></td><td></td></tr>
<tr><td>Security</td><td></td><td>0</td><td>5154</td><td>Microsoft-...</td><td></td><td></td></tr>
<tr><td>Security</td><td></td><td>0</td><td>5153</td><td>Microsoft-...</td><td></td><td></td></tr>
<tr><td>Security</td><td></td><td>0</td><td>5152</td><td>Microsoft-...</td><td></td><td></td></tr>
<tr><td></td><td></td><td>0</td><td>600</td><td>PowerShell</td><td></td><td></td></tr>
<tr><td></td><td></td><td>0</td><td>403</td><td>PowerShell</td><td></td><td></td></tr>
<tr><td></td><td></td><td>0</td><td>400</td><td>PowerShell</td><td></td><td></td></tr>
<tr><td></td><td>Audit Success</td><td>0</td><td>566</td><td></td><td></td><td>[NOT](?i)30e3...</td></tr>
<tr><td></td><td>Audit Success</td><td>0</td><td>4662</td><td></td><td></td><td>[NOT](?i)30e3...</td></tr>
<tr><td></td><td>Audit Success</td><td>0</td><td>4624</td><td></td><td></td><td>$</Data><Dat...</td></tr>
<tr><td></td><td>Audit Success</td><td>0</td><td>4634</td><td></td><td></td><td>$</Data><Dat...</td></tr>
</table>

Select the required options to <b>Add/Edit/Remove/Find</b> DLA Filters and click <b>Close</b>.</td>
</tr>
</table>

Table 95

Field	Description
Frequency	Set the frequency of file transfer. You can set file transfer to occur every configure hours or daily at a particular time.
Purge Transferred Files	Set this option to purge files that are transferred to the Manager.
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.
Advanced	a) Click **Advanced**. Advanced Option window opens.  Advanced Options Retry Max Retries 5 Retry Interval 15 (Minutes) ☐ Generate event for each attempt ☑ Generate Success Event ☑ Generate Failure Event OK Cancel b) Select the required options, and then click **OK**.

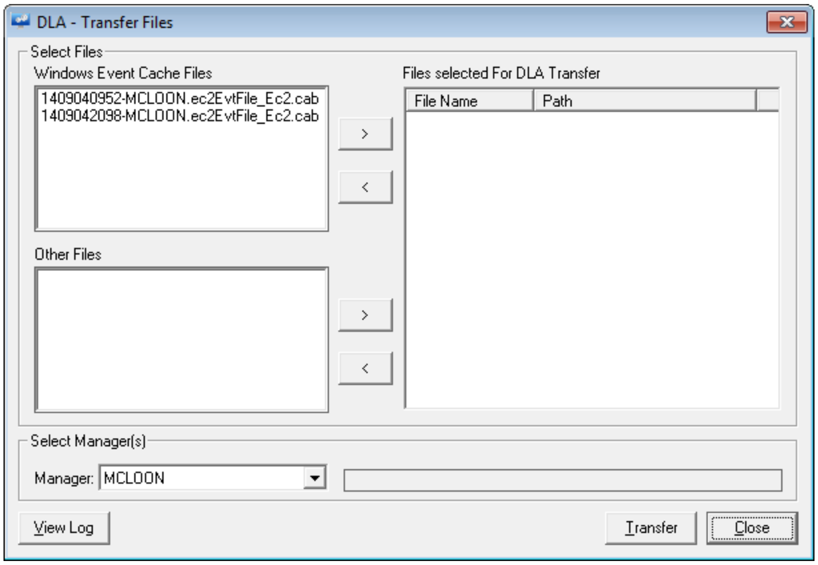
Send Now	Click this option to override the Frequency option and transfer the files immediately. This option is available only under EventTracker Control panel >> File Transfer. a) Click **Send Now**. DLA – Transfer Files window opens.  1409040952-MCLOON.ec2EvtFile_Ec2.cab 1409042098-MCLOON.ec2EvtFile_Ec2.cab Manager: MCLOON DLA - Transfer Files Select Files Windows Event Cache Files Files selected For DLA Transfer File Name Path Other Files Select Manager(s) View Log Transfer Close b) In **Select Files** pane, select **Windows Event Cache Files**, and then select **>** button. c) Click **Transfer**. d) To view the logs, click **View Log**.

Table 96

3 Select the required options and then select **Save**.

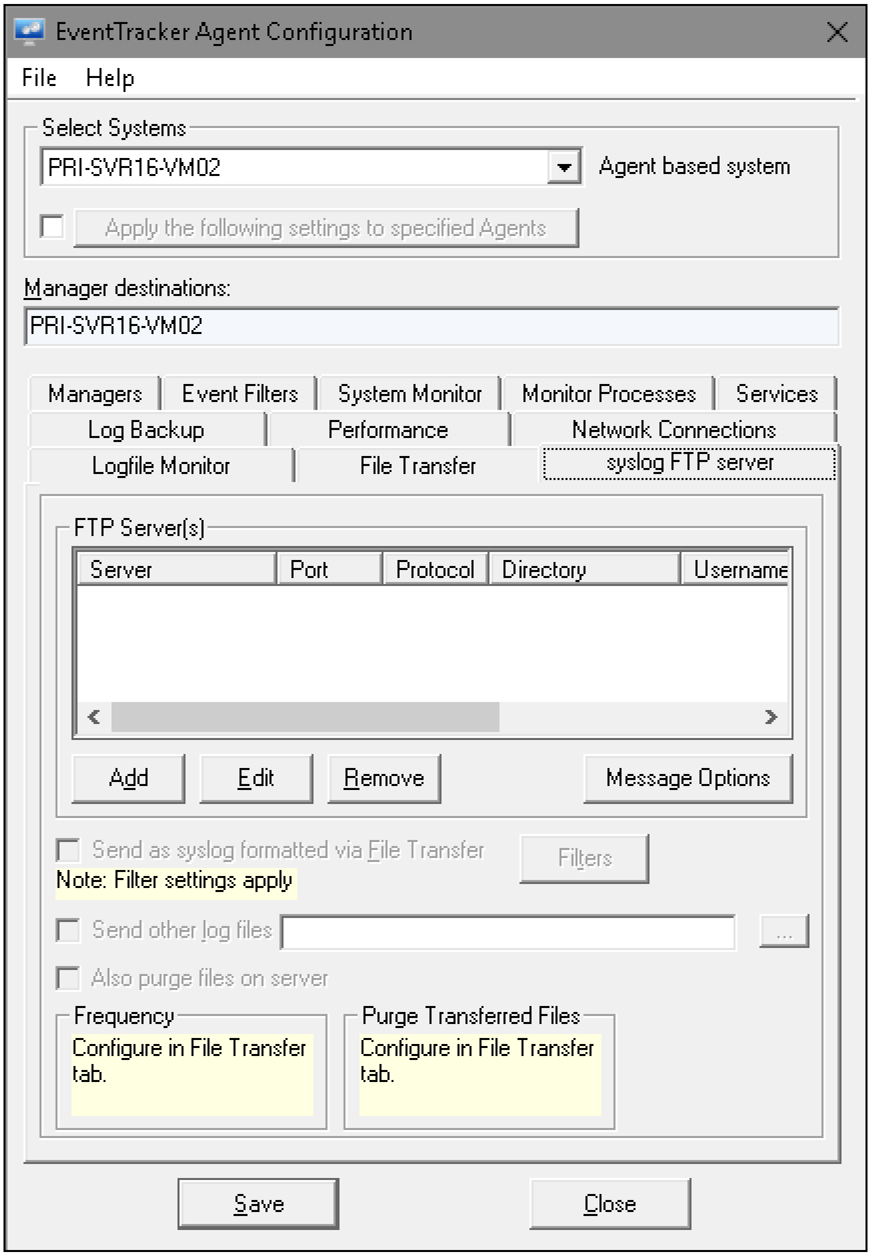
35.16 Syslog FTP Server

This new feature is introduced to transmit windows events from local systems, as text files containing syslog messages.

35.16.1 Transferring 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 opens.



Note: Filter settings apply

Configure in File Transfer tab.

Configure in File Transfer tab.

Figure 779

2 Click **Add**.

EventTracker opens Syslog FTP destination window.

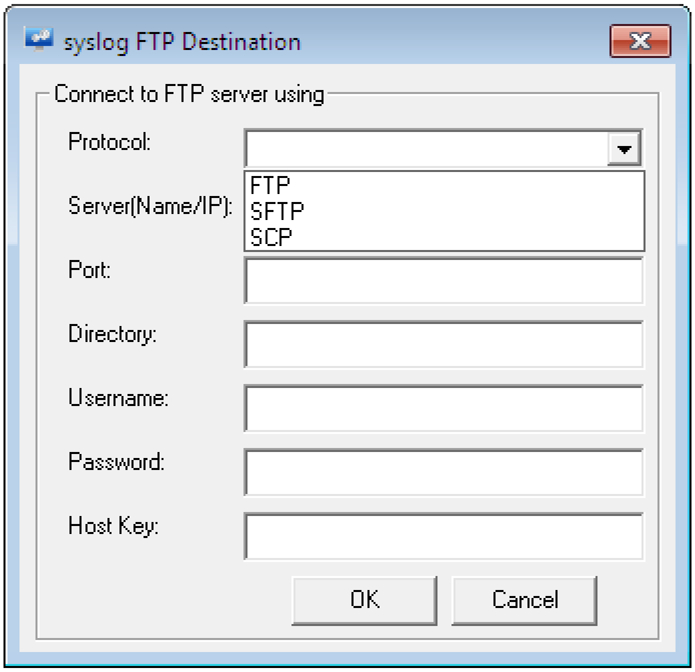


Figure 780

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.

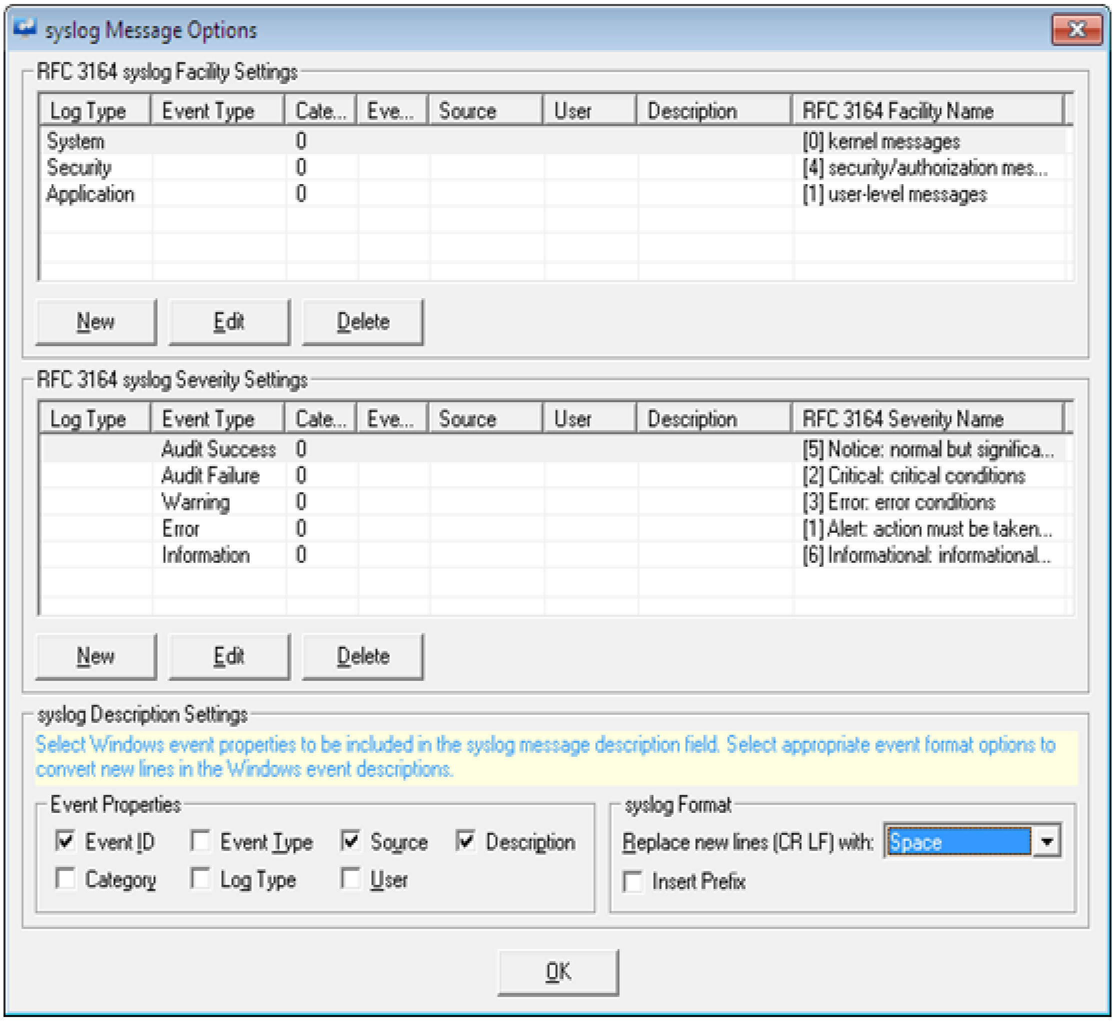
10 To send other log files, select **Send other log files** option, and then click ⬚ **Browse**.
EventTracker displays **Browse for folder** pop-up window.

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.

A syslog Message Options window opens.



RFC 3164 syslog Facility Settings

Log Type	Event Type	Cate...	Eve...	Source	User	Description	RFC 3164 Facility Name
System		0					[0] kernel messages
Security		0					[4] security/authorization mes...
Application		0					[1] user-level messages

RFC 3164 syslog Severity Settings

Log Type	Event Type	Cate...	Eve...	Source	User	Description	RFC 3164 Severity Name
	Audit Success	0					[5] Notice: normal but significa...
	Audit Failure	0					[2] Critical: critical conditions
	Warning	0					[3] Error: error conditions
	Error	0					[1] Alert: action must be taken...
	Information	0					[6] Informational: informational...

syslog Description Settings

Select Windows event properties to be included in the syslog message description field. Select appropriate event format options to convert new lines in the Windows event descriptions.

Event Properties

☑ Event ID ☐ Event Type ☑ Source ☑ Description
☐ Category ☐ Log Type ☐ User

syslog Format

Replace new lines (CR LF) with: Space
☐ Insert Prefix

Figure 781

16 Select the required **Event Properties**, **syslog Format**.

17 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.

18 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.

19 Click **OK**, click **Save** and then click **Close**.
All the files placed in this folder will be transferred to the configured manager.

35.16.2 Saving Current Configuration

This option enables you to save the current configuration settings in agent configuration.

1 To save current configuration settings, open **EventTracker Control panel**, and then select **EventTracker Agent Configuration**.

2 Select the system from the **Select Systems** drop down, select the **File** menu, and then select the **Save as** option.

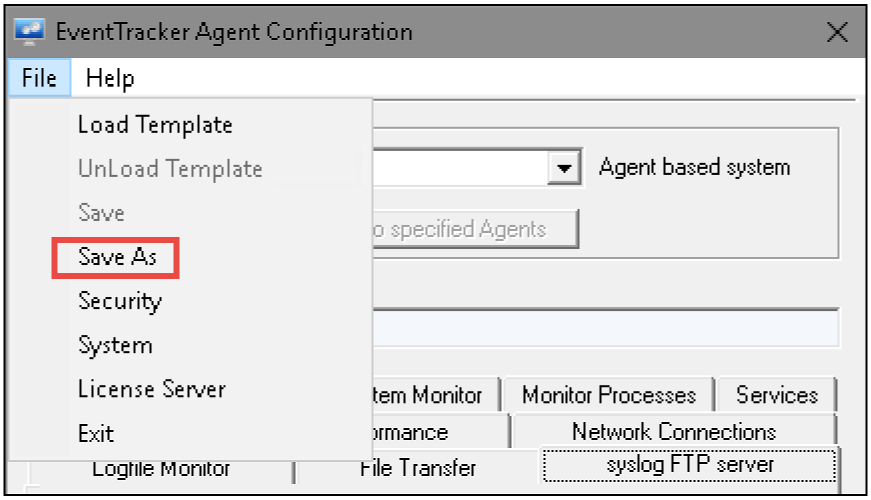


Figure 782

3 Select appropriate path to backup the current configuration settings. Enter the file name in the **File name** field.
The valid file extension is '***.ini**'.

4 Click **Save**.

EventTracker opens the 'EventTracker Agent Configuration' message box.

5 Click **OK**.

36. Traffic Analyzer

In this chapter, you will learn :

Analyze Traffic by

- Category
- Event ID
- Custom Selection
- Keywords Analysis

36.1 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. Most 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, 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.

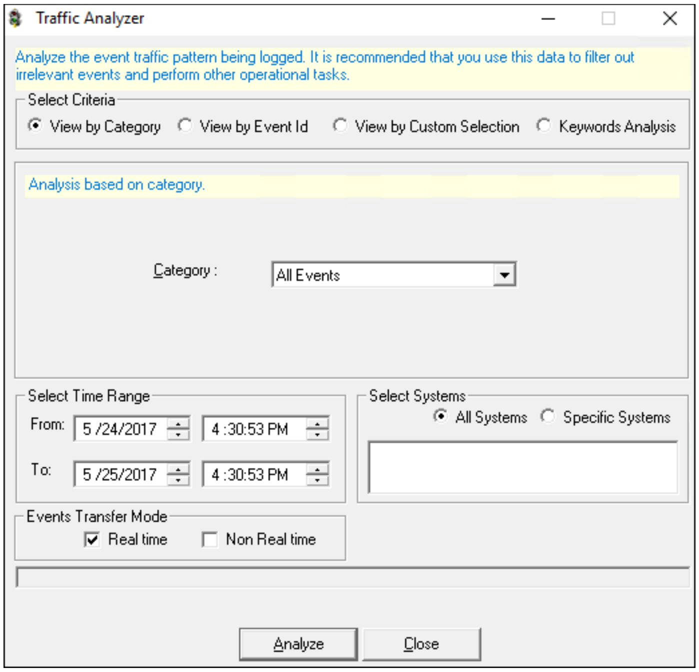
This report provides total counts per system for each event id. Filter and display event count details based on user-defined criteria.

Usage: Analyze Windows specific security events, correlate events, broad searches per criteria with subsequent sorting and ordering of the result set.

36.1.1 Starting Traffic Analyzer

1 Double-click **Traffic Analyzer** on the **EventTracker Control Panel.**

Traffic Analyzer window opens.



Traffic Analyzer

Analyze the event traffic pattern being logged. It is recommended that you use this data to filter out irrelevant events and perform other operational tasks.

Select Criteria

● View by Category ○ View by Event Id ○ View by Custom Selection ○ Keywords Analysis

Analysis based on category.

Category : All Events

Select Time Range

From: 5 /24/2017 4 :30:53 PM

To: 5 /25/2017 4 :30:53 PM

Select Systems

● All Systems ○ Specific Systems

Events Transfer Mode

☑ Real time □ Non Real time

Figure783

36.2 Viewing 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.

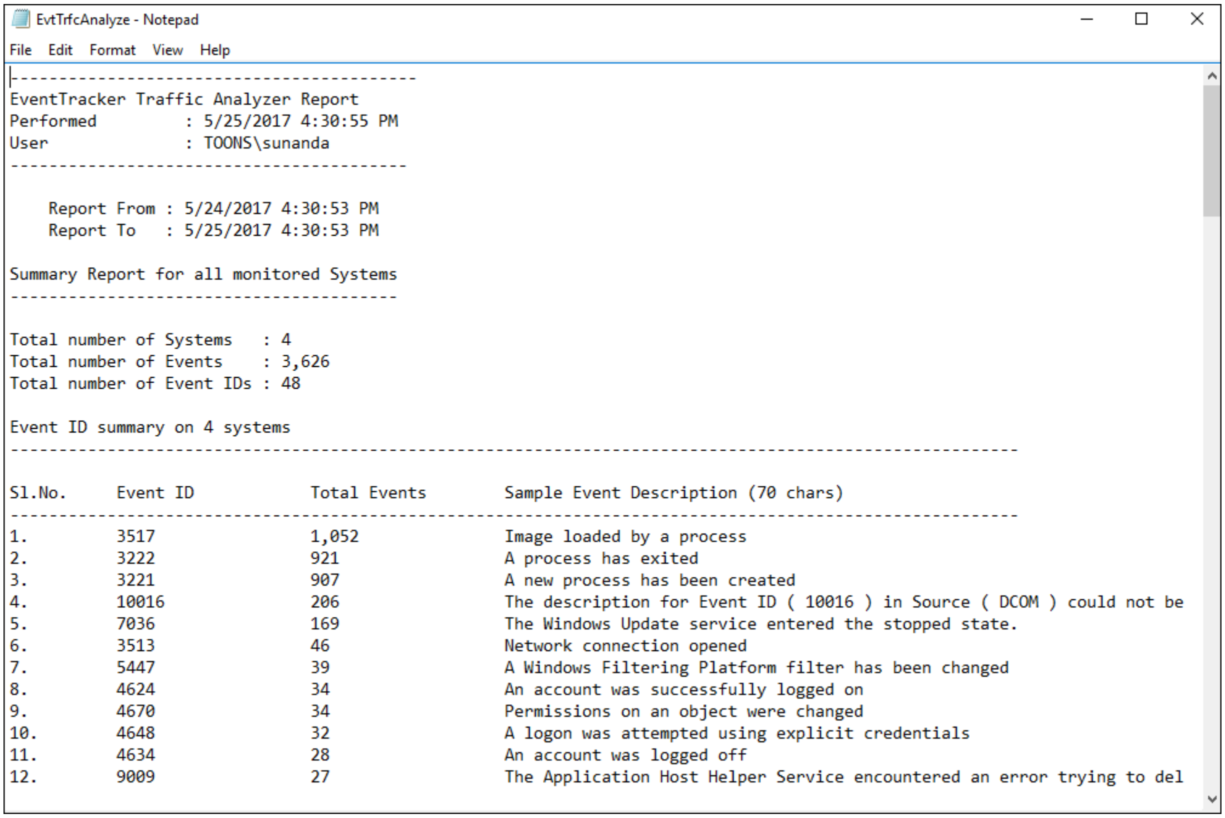
3 Set the **Select Time Range** in **From**, **To** drop-down list.

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 opens the report in the Notepad.



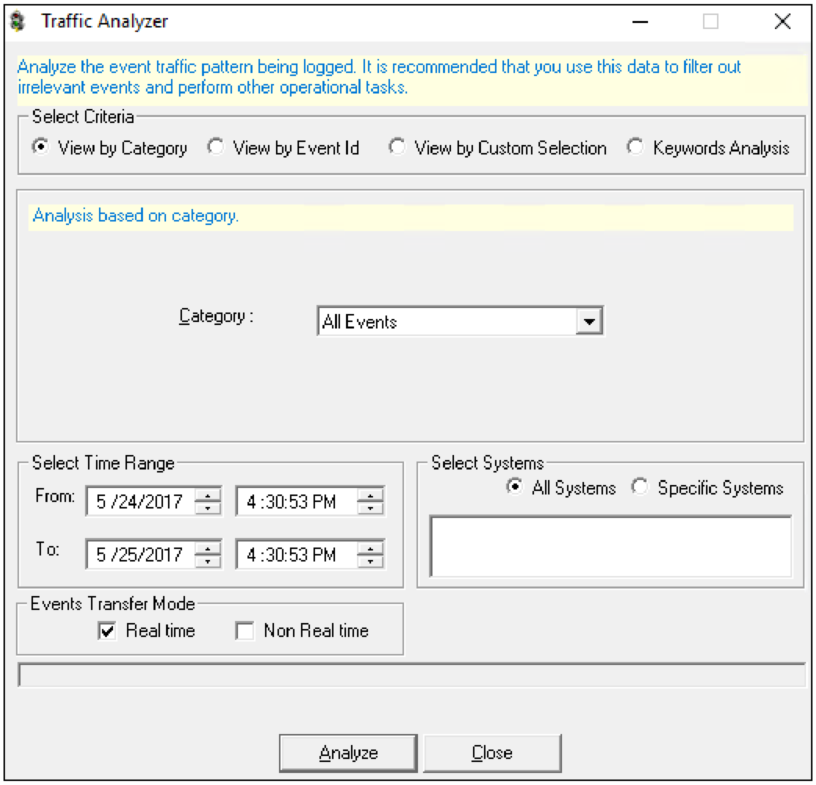
```
------------------------------------------
EventTracker Traffic Analyzer Report
Performed          : 5/25/2017 4:30:55 PM
User               : TOONS\sunanda
-----------------------------------------

    Report From : 5/24/2017 4:30:53 PM
    Report To   : 5/25/2017 4:30:53 PM

Summary Report for all monitored Systems
----------------------------------------

Total number of Systems   : 4
Total number of Events    : 3,626
Total number of Event IDs : 48

Event ID summary on 4 systems
----------------------------------------------------------------------------------------------------------

Sl.No.     Event ID            Total Events        Sample Event Description (70 chars)
----------------------------------------------------------------------------------------------------------
1.         3517                1,052               Image loaded by a process
2.         3222                921                 A process has exited
3.         3221                907                 A new process has been created
4.         10016               206                 The description for Event ID ( 10016 ) in Source ( DCOM ) could not be
5.         7036                169                 The Windows Update service entered the stopped state.
6.         3513                46                  Network connection opened
7.         5447                39                  A Windows Filtering Platform filter has been changed
8.         4624                34                  An account was successfully logged on
9.         4670                34                  Permissions on an object were changed
10.        4648                32                  A logon was attempted using explicit credentials
11.        4634                28                  An account was logged off
12.        9009                27                  The Application Host Helper Service encountered an error trying to del
```

Figure 784

36.3 Viewing 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.



Traffic Analyzer

Analyze the event traffic pattern being logged. It is recommended that you use this data to filter out irrelevant events and perform other operational tasks.

Select Criteria

● View by Category ○ View by Event Id ○ View by Custom Selection ○ Keywords Analysis

Analysis based on category.

Category : All Events

Select Time Range

From: 5 /24/2017 4 :30:53 PM

To: 5 /25/2017 4 :30:53 PM

Select Systems

● All Systems ○ Specific Systems

Events Transfer Mode

☑ Real time ☐ Non Real time

Figure 785

Field	Description
Display all records: By default, this option is selected. All records will be displayed in report in descending order.	
Display only top: Select this option if you want only a specified number of records to be displayed in the report.	
Select Event Id: Select 5 hard coded Windows security events for event traffic analysis.	
540 Successful Network Logon	Selecting this id will generate 2 reports sorted by Username and IP address.
672 Authentication Ticket Granted	Selecting this id will generate 2 reports sorted by Username and IP address.
673 Service Ticket Granted	Selecting this id will generate 1 report sorted by IP Address.
675 Pre-authentication failed	Selecting this id will generate 2 reports sorted by Username and IP address.
680 Logon attempt	Selecting this id will generate 2 reports sorted by Username and Computer.

Table 97

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.

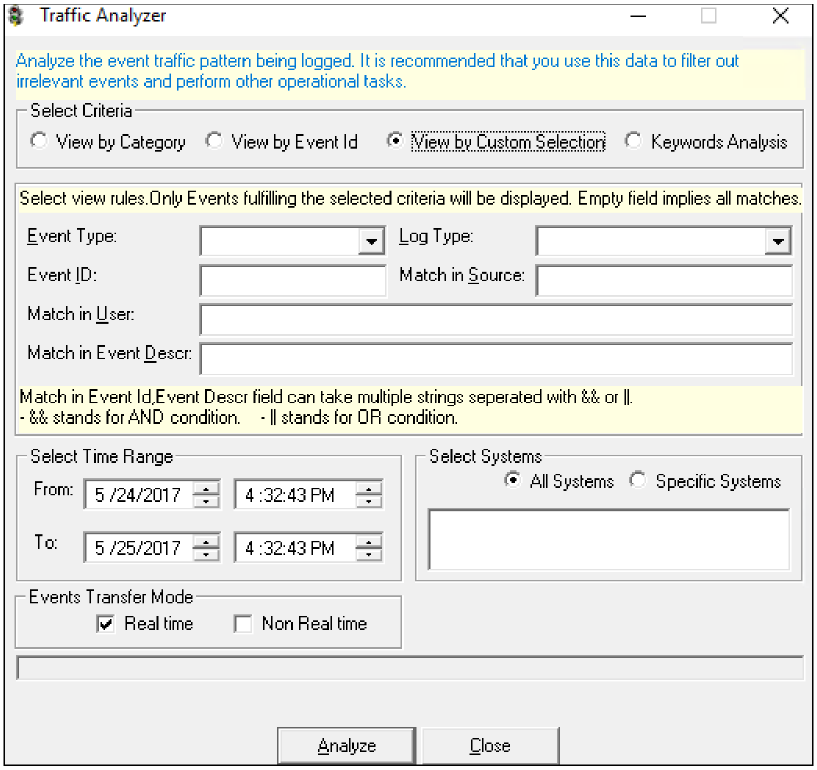
4 Select **Analyze**.

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.

36.4 Viewing by Custom Selection

This option helps you customize the selection criteria.

1 Select the **View by Custom Selection** option.



Traffic Analyzer

Analyze the event traffic pattern being logged. It is recommended that you use this data to filter out irrelevant events and perform other operational tasks.

Select Criteria
○ View by Category ○ View by Event Id ● View by Custom Selection ○ Keywords Analysis

Select view rules.Only Events fulfilling the selected criteria will be displayed. Empty field implies all matches.

Event Type:
Log Type:
Event ID:
Match in Source:
Match in User:
Match in Event Descr:

Match in Event Id,Event Descr field can take multiple strings seperated with && or ||.
- && stands for AND condition. - || stands for OR condition.

Select Time Range
From: 5 /24/2017 4 :32:43 PM
To: 5 /25/2017 4 :32:43 PM

Select Systems
● All Systems ○ Specific Systems

Events Transfer Mode
☑ Real time □ Non Real time

Figure 786

2 Enter appropriate values 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.

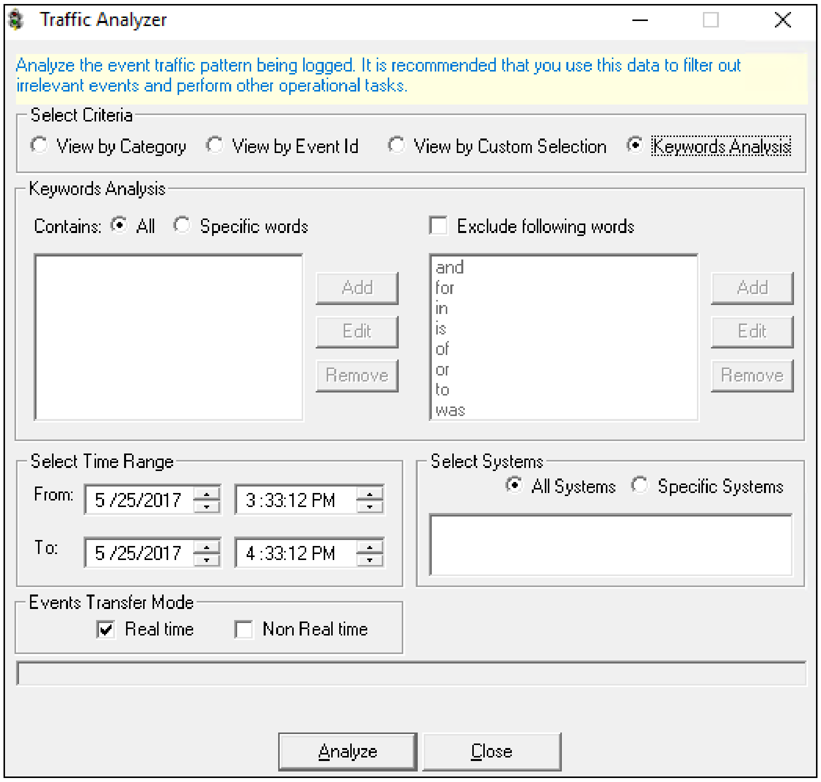
4 Click **Analyze**.

Traffic Analyzer opens the report in the Notepad.

36.5 Keyword Analysis option

This option helps to analyze traffic by keywords.

1 Select the **Keywords Analysis** option.



Traffic Analyzer

Analyze the event traffic pattern being logged. It is recommended that you use this data to filter out irrelevant events and perform other operational tasks.

Select Criteria: ○ View by Category ○ View by Event Id ○ View by Custom Selection ● Keywords Analysis

Keywords Analysis

Contains: ● All ○ Specific words

□ Exclude following words

and
for
in
is
of
or
to
was

Select Time Range

From: 5 /25/2017 3 :33:12 PM

To: 5 /25/2017 4 :33:12 PM

Select Systems: ● All Systems ○ Specific Systems

Events Transfer Mode: ☑ Real time □ Non Real time

Figure 787

Field	Description
Keywords Analysis: Helps to analyze events by keywords.	
Contains All	Analyze logs that contain all keywords.
Contains Specific words	Analyze logs that contain specific keywords.
Excluding following words	Select this checkbox to exclude commonly occurring words.

Table 98

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 opens the report in the Notepad.

36.5.1 Add Keywords for Analysis option

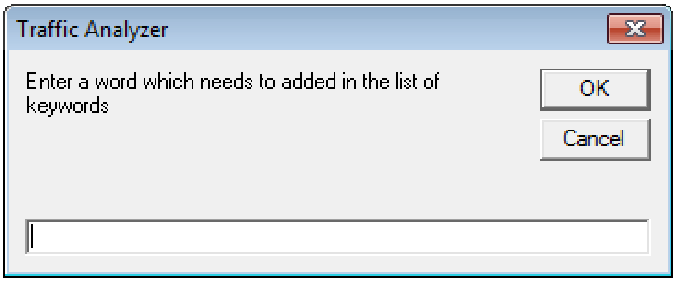
This option helps to add keywords.

1 Select the **Specific words** option.

Traffic Analyzer enables the **Add, Edit,** and **Remove** buttons.

2 Click **Add**.

Traffic Analyzer opens the Traffic Analyzer dialog box.


Traffic Analyzer

Enter a word which needs to added in the list of keywords

Figure 788

3 Type the keyword in the text box provided.
Example: ETAdmin

4 Click **OK**.

Traffic Analyzer adds the keyword to the list of keywords.

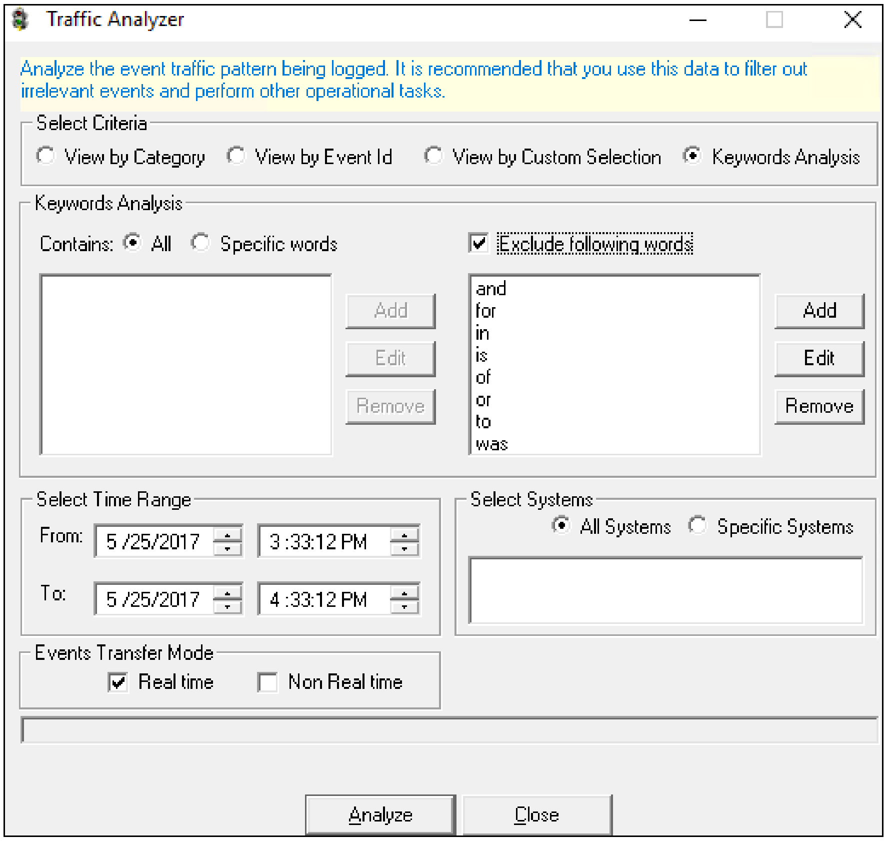
5 To analyze logs that contain a specific keyword, select a keyword from the list and then click **Analyze**.

36.5.2 Add Commonly Occurring Words to Exclude from Analysis option

This option helps to add most commonly occurring words to exclude from analysis.

1 Select the **Exclude following words** option.

Traffic Analyzer opens the list of commonly occurring words, enables **Add**, **Edit**, and **Remote**.



Traffic Analyzer

Analyze the event traffic pattern being logged. It is recommended that you use this data to filter out irrelevant events and perform other operational tasks.

Select Criteria: ○ View by Category ○ View by Event Id ○ View by Custom Selection ● Keywords Analysis

Keywords Analysis

Contains: ● All ○ Specific words

☑ Exclude following words

and
for
in
is
of
or
to
was

Select Time Range

From: 5 /25/2017 3 :33:12 PM

To: 5 /25/2017 4 :33:12 PM

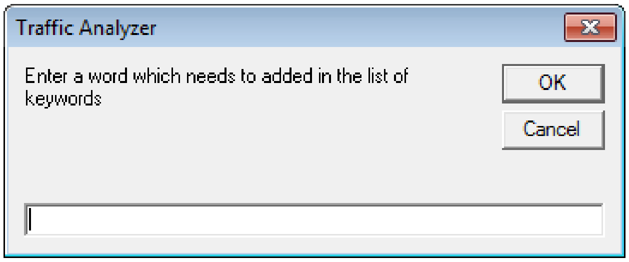
Select Systems: ● All Systems ○ Specific Systems

Events Transfer Mode: ☑ Real time ☐ Non Real time

Figure 789

2 Click **Add**.

Traffic Analyzer opens the Traffic Analyzer dialog box.



Traffic Analyzer

Enter a word which needs to added in the list of keywords

Figure 790

3 Type the keyword in the text box provided.

4 Click **OK**.

Traffic Analyzer adds the new keyword to the list for exclusion.

37. Agent Management Tool

In this chapter, you will learn how to:

- Accessing Agent Management Tool
- Querying Agent Service
- Restarting Agent Service
- Querying Agent Version
- Removing Agent Component
- Deleting Systems from Agent Service
- Querying for Agent Update Info

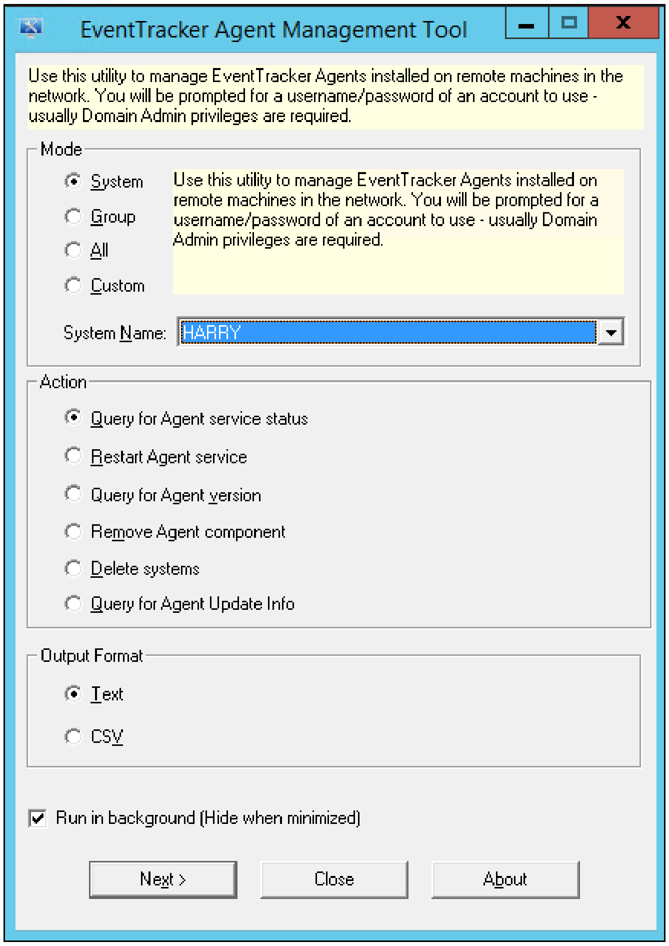
37.1 Windows Agent Management Tool

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 must have Domain Admin privilege to use this utility.

37.1.1 Accessing Agent Management Tool

- Double-click **Agent Management Tool** on the EventTracker Control Panel.

  EventTracker opens the Agent Management Tool.



EventTracker Agent Management Tool

Use this utility to manage EventTracker Agents installed on remote machines in the network. You will be prompted for a username/password of an account to use - usually Domain Admin privileges are required.

Mode

● System
○ Group
○ All
○ Custom

Use this utility to manage EventTracker Agents installed on remote machines in the network. You will be prompted for a username/password of an account to use - usually Domain Admin privileges are required.

System Name: HARRY

Action

● Query for Agent service status
○ Restart Agent service
○ Query for Agent version
○ Remove Agent component
○ Delete systems
○ Query for Agent Update Info

Output Format

● Text
○ CSV

☑ Run in background (Hide when minimized)

Figure 791

Field	Description
System	Works on a selected system which is managed with EventTracker Agent
Group	Works on all EventTracker managed systems belonging to selected Group/Domain
All	Works on all EventTracker managed systems
Custom	Works on systems which are listed in a plain text file

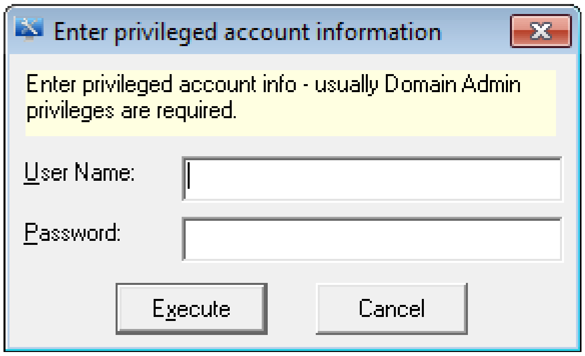
Table 99

37.1.2 Querying 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

Enter privileged account info - usually Domain Admin privileges are required.

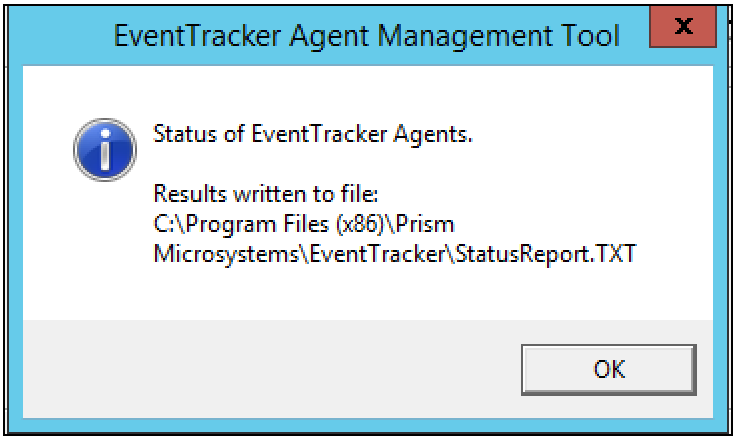
User Name:

Password:

Figure 792

7 Enter valid credentials, and then click **Execute**.

EventTracker opens the **EventTracker Management Tool message box.**



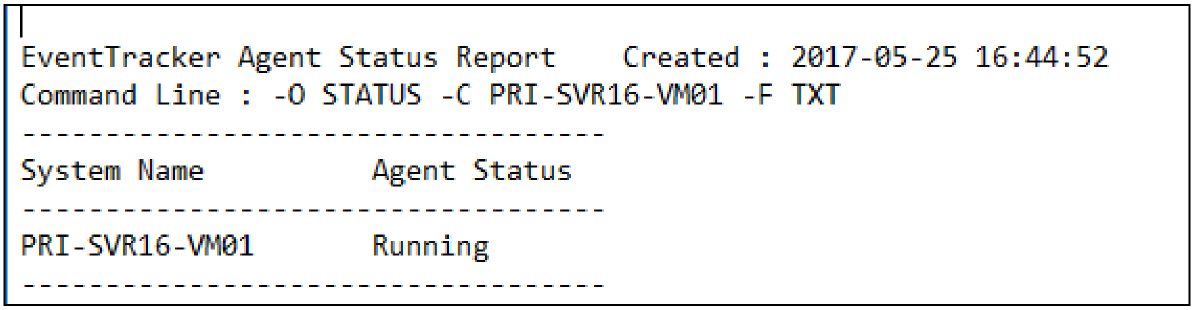
Status of EventTracker Agents.

Results written to file:
C:\Program Files (x86)\Prism Microsystems\EventTracker\StatusReport.TXT

Figure 793

8 Click **OK**.

EventTracker opens the result in the Notepad.



```
EventTracker Agent Status Report    Created : 2017-05-25 16:44:52
Command Line : -O STATUS -C PRI-SVR16-VM01 -F TXT
-----------------------------------
System Name           Agent Status
-----------------------------------
PRI-SVR16-VM01        Running
-----------------------------------
```

Figure 794

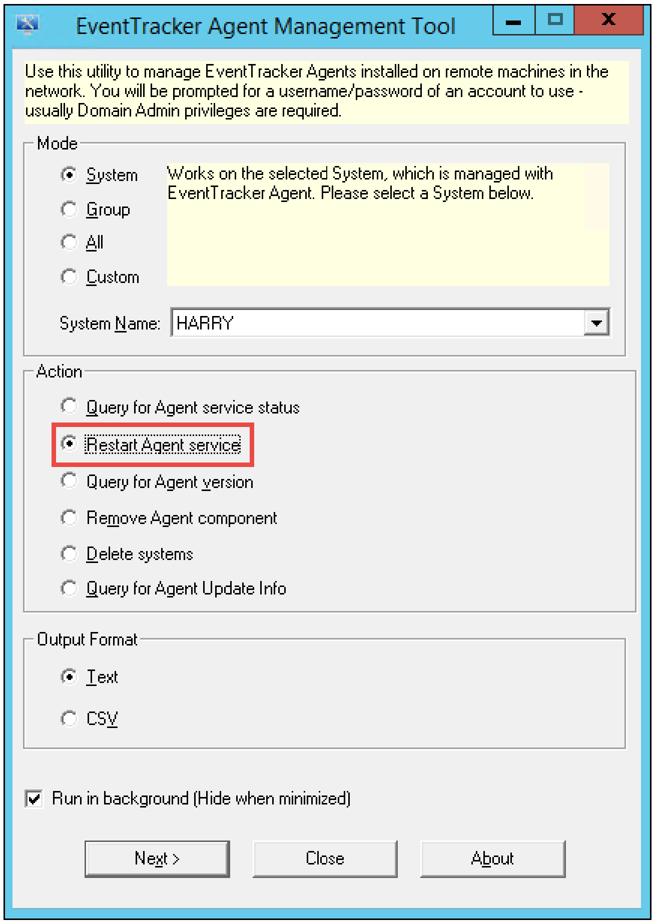
🗎 NOTE

Similarly, you can select and manage EventTracker Agent in a Group, All, Custom.

37.1.3 Restarting 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.



Use this utility to manage EventTracker Agents installed on remote machines in the network. You will be prompted for a username/password of an account to use - usually Domain Admin privileges are required.

Mode

- ● System
- ○ Group
- ○ All
- ○ Custom

Works on the selected System, which is managed with EventTracker Agent. Please select a System below.

System Name: HARRY

Action

- ○ Query for Agent service status
- ● Restart Agent service
- ○ Query for Agent version
- ○ Remove Agent component
- ○ Delete systems
- ○ Query for Agent Update Info

Output Format

- ● Text
- ○ CSV

☑ Run in background (Hide when minimized)

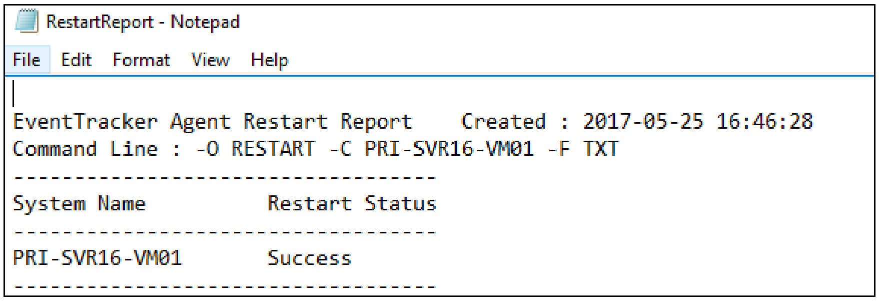
Figure 795

4 Click **Next >**.
EventTracker opens the **Enter privileged account information** dialog box.

5 Type valid username and password. Click **Execute**.
EventTracker opens the **EventTracker Agent Management Tool** message box.

6 Click **OK**.

EventTracker displays the result in the Notepad.



```
EventTracker Agent Restart Report    Created : 2017-05-25 16:46:28
Command Line : -O RESTART -C PRI-SVR16-VM01 -F TXT
----------------------------------
System Name           Restart Status
----------------------------------
PRI-SVR16-VM01        Success
----------------------------------
```

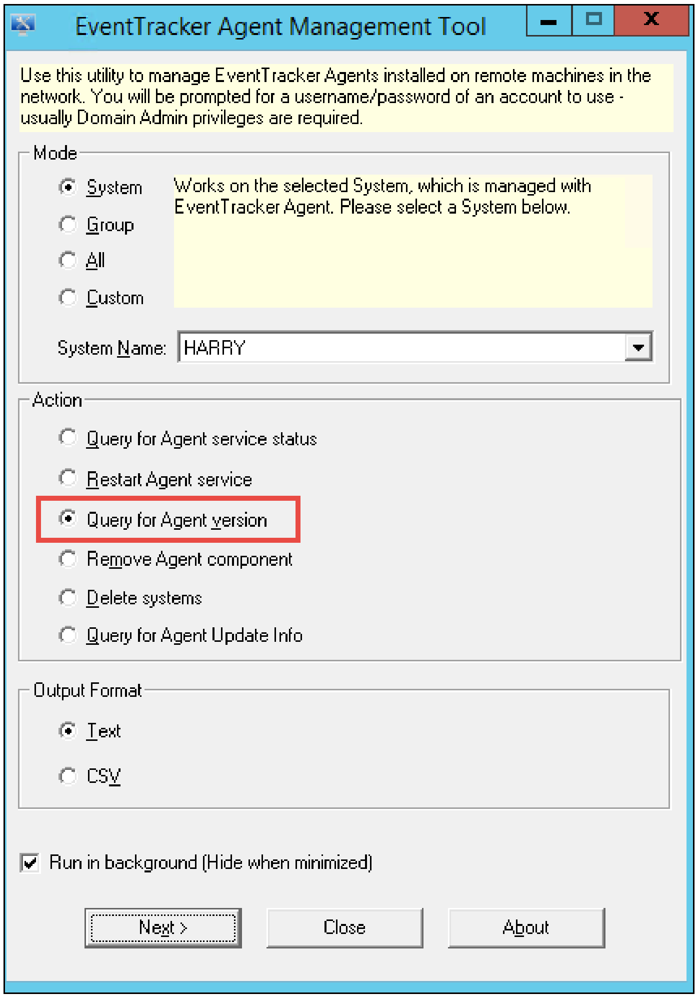
Figure 796

37.1.4 Querying 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. Select the **Query for Agent version** option.



EventTracker Agent Management Tool

Use this utility to manage EventTracker Agents installed on remote machines in the network. You will be prompted for a username/password of an account to use - usually Domain Admin privileges are required.

Mode

● System
○ Group
○ All
○ Custom

Works on the selected System, which is managed with EventTracker Agent. Please select a System below.

System Name: HARRY

Action

○ Query for Agent service status
○ Restart Agent service
● Query for Agent version
○ Remove Agent component
○ Delete systems
○ Query for Agent Update Info

Output Format

● Text
○ CSV

☑ Run in background (Hide when minimized)

Figure 797

3 Click **Next >**.

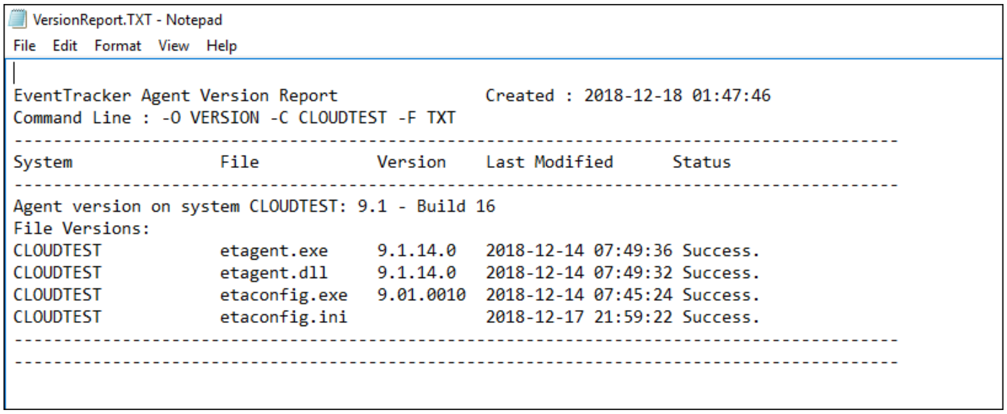
EventTracker opens the **Enter privileged account information** dialog box.

4 Enter valid username and password. Select **Execute**.

EventTracker opens the **EventTracker Agent Management Tool** message box.

5 Click **OK**.

EventTracker displays the result in the Notepad.



VersionReport.TXT - Notepad

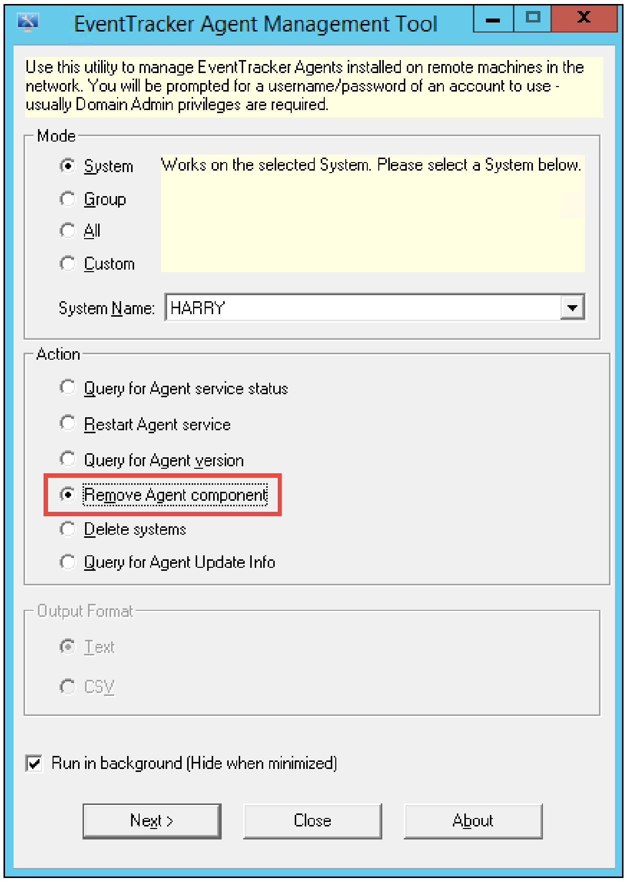
```
EventTracker Agent Version Report              Created : 2018-12-18 01:47:46
Command Line : -O VERSION -C CLOUDTEST -F TXT
--------------------------------------------------------------------------------
System               File            Version    Last Modified      Status
--------------------------------------------------------------------------------
Agent version on system CLOUDTEST: 9.1 - Build 16
File Versions:
CLOUDTEST            etagent.exe     9.1.14.0   2018-12-14 07:49:36 Success.
CLOUDTEST            etagent.dll     9.1.14.0   2018-12-14 07:49:32 Success.
CLOUDTEST            etaconfig.exe   9.01.0010  2018-12-14 07:45:24 Success.
CLOUDTEST            etaconfig.ini              2018-12-17 21:59:22 Success.
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
```

Figure 798

37.1.5 Removing the Agent Component - System / Group / All / Custom

This option enables you 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 Agent Management Tool

Use this utility to manage EventTracker Agents installed on remote machines in the network. You will be prompted for a username/password of an account to use - usually Domain Admin privileges are required.

Mode

● System
○ Group
○ All
○ Custom

Works on the selected System. Please select a System below.

System Name: HARRY

Action

○ Query for Agent service status
○ Restart Agent service
○ Query for Agent version
● Remove Agent component
○ Delete systems
○ Query for Agent Update Info

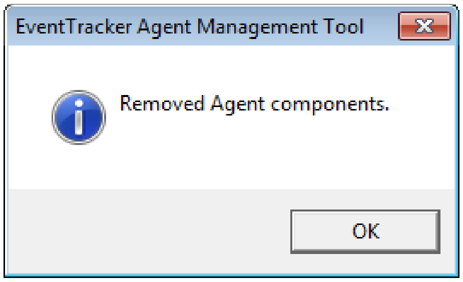
Output Format

● Text
○ CSV

☑ Run in background (Hide when minimized)

Figure 799

EventTracker displays **EventTracker Agent Management Tool** window.



EventTracker Agent Management Tool

Removed Agent components.

Figure 800

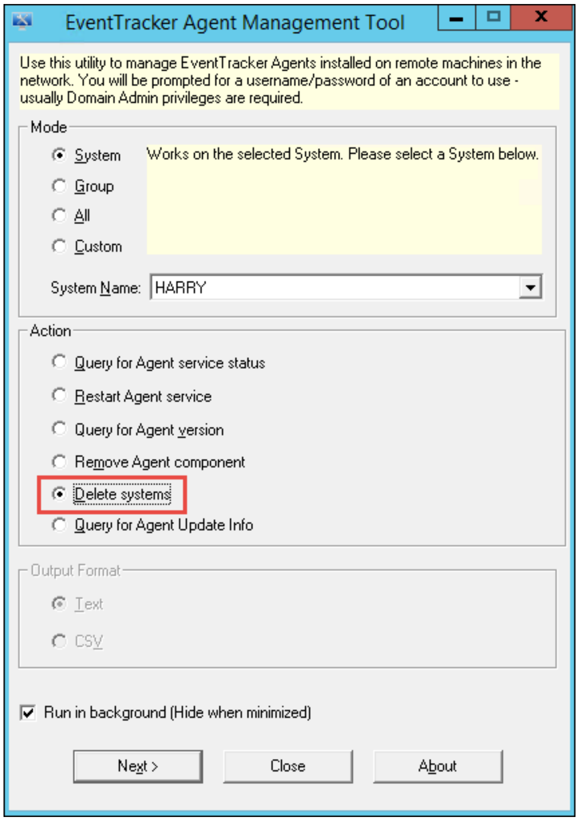
3. Click **OK.**

   The selected system(s) from the drop down will be removed.

37.1.6 Deleting Systems from 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

Use this utility to manage EventTracker Agents installed on remote machines in the network. You will be prompted for a username/password of an account to use - usually Domain Admin privileges are required.

Mode

● System
○ Group
○ All
○ Custom

Works on the selected System. Please select a System below.

System Name: HARRY

Action

○ Query for Agent service status
○ Restart Agent service
○ Query for Agent version
○ Remove Agent component
● Delete systems
○ Query for Agent Update Info

Output Format

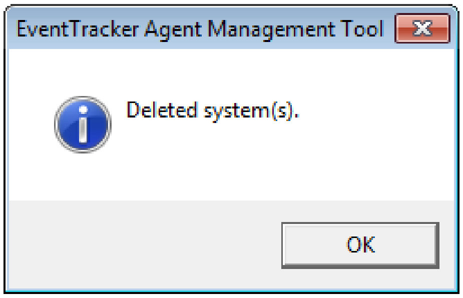
● Text
○ CSV

☑ Run in background (Hide when minimized)

Figure 801

2 Select **Delete systems** and then select **Next >**.

   EventTracker displays **EventTracker Management Tool** window.



Deleted system(s).

Figure 802

3 Click **OK**

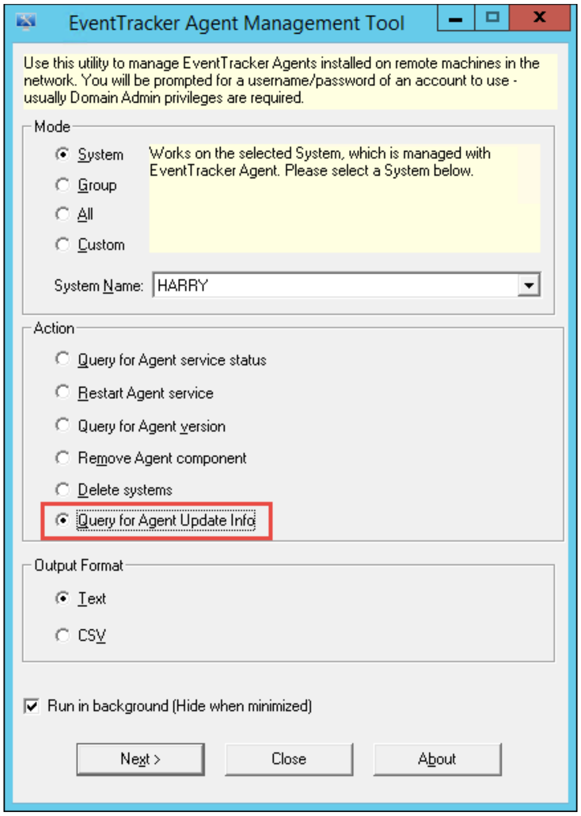
The selected system(s) will be deleted.

37.1.7 Querying for Agent Update Info - System / Group / All / Custom

This option enables you to query the file details and update info of the agent service in the selected system / group / all / specified systems.

1 To query the update info of the agent service in the selected system, select the relevant **Mode** option.

2 Select the system from the **System Name** drop-down list. Select the **Query for Agent Update Info** option.



Use this utility to manage EventTracker Agents installed on remote machines in the network. You will be prompted for a username/password of an account to use - usually Domain Admin privileges are required.

Mode

● System
○ Group
○ All
○ Custom

Works on the selected System, which is managed with EventTracker Agent. Please select a System below.

System Name: HARRY

Action

○ Query for Agent service status
○ Restart Agent service
○ Query for Agent version
○ Remove Agent component
○ Delete systems
● Query for Agent Update Info

Output Format

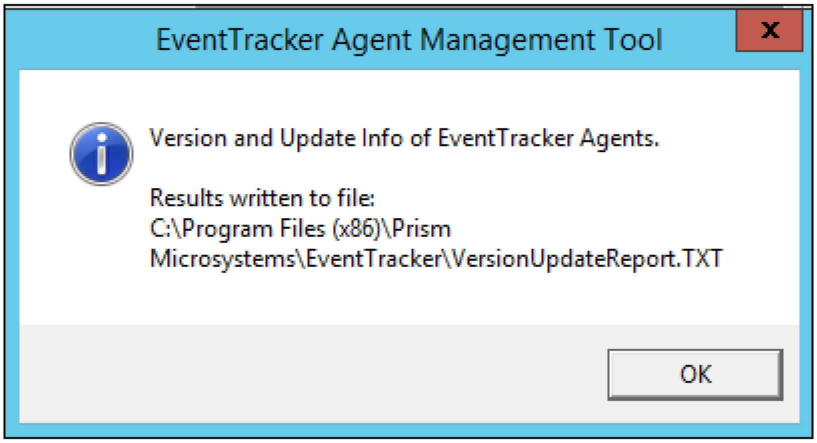
● Text
○ CSV

☑ Run in background (Hide when minimized)

Figure 803

3 Click **Next >**.

EventTracker displays the below message box:



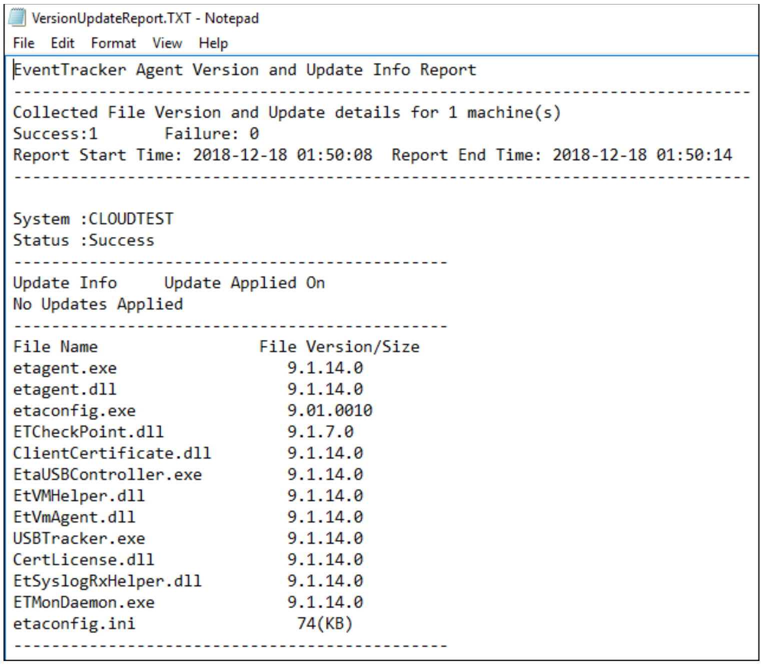
Version and Update Info of EventTracker Agents.

Results written to file:
C:\Program Files (x86)\Prism Microsystems\EventTracker\VersionUpdateReport.TXT

Figure 804

4 Click **OK**.

EventTracker displays the result in the Notepad.



```
EventTracker Agent Version and Update Info Report
------------------------------------------------------------------------------
Collected File Version and Update details for 1 machine(s)
Success:1       Failure: 0
Report Start Time: 2018-12-18 01:50:08  Report End Time: 2018-12-18 01:50:14
------------------------------------------------------------------------------

System :CLOUDTEST
Status :Success
----------------------------------------------
Update Info     Update Applied On
No Updates Applied
----------------------------------------------
File Name                 File Version/Size
etagent.exe                  9.1.14.0
etagent.dll                  9.1.14.0
etaconfig.exe                9.01.0010
ETCheckPoint.dll             9.1.7.0
ClientCertificate.dll        9.1.14.0
EtaUSBController.exe         9.1.14.0
EtVMHelper.dll               9.1.14.0
EtVmAgent.dll                9.1.14.0
USBTracker.exe               9.1.14.0
CertLicense.dll              9.1.14.0
EtSyslogRxHelper.dll         9.1.14.0
ETMonDaemon.exe              9.1.14.0
etaconfig.ini                 74(KB)
----------------------------------------------
```

Figure 805

38. Port Configuration

In this chapter, you will learn how to:

- About Port Configuration

38.1 About Port Configuration

Port configuration utility is a simple tool that allows EventTracker users to change the port of the website which runs the EventTracker.

Apart from this, the utility allows the end user to generate an excel file which will display the list of ports that are normally used by EventTracker products. With the use of the generated list, the network administrators can unblock those ports through a firewall.

For more information, refer: https://www.netsurion.com/Corporate/media/Corporate/Files/Support-Docs/How-to-Configure-Port-of-EventTracker-Website.pdf

39. Trap Tracker

In this chapter, you will learn how to:

- About Trap Tracker
- Trap Tracker Components

39.1 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.

39.2 TrapTracker Components

TTW has the following components:

- A background process that receives and processes generic SNMP v1, v2 and v3 traps; propagated by SNMP compliant devices.
- Feature-rich GUI application to categorize traps filters traps for customized views, configure Alerts, upgrade license etc.
- A MibCompiler.

For detailed information please refer Trap Tracker Online Web Help.

40. Change Audit

In this chapter, you will learn how to:

- Results Summary Console
- Changing Policy Dashboard
- Configuration Policy Dashboard

40.1 EventTracker Inventory Manager

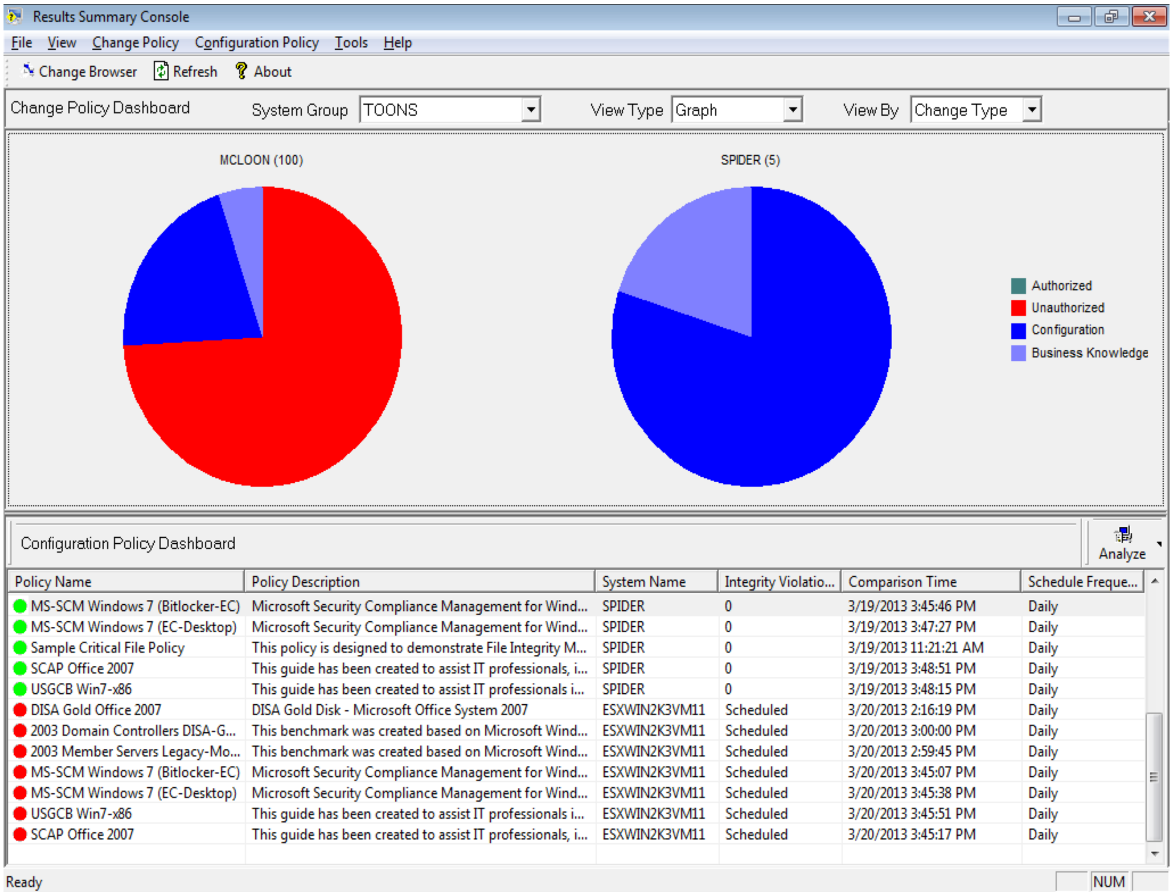
EventTracker Inventory is an automated asset management tool, which scans all Change Audit, manage computers, and displays them in an easily accessible web and legacy interface.

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

For detail information regarding this chapter please refer Change Audit.

40.2 Changing Audit Results Summary Console

The Change Audit Results Summary Console consists of Change Policy Dashboard and Configuration Policy Dashboard.



System Group: TOONS

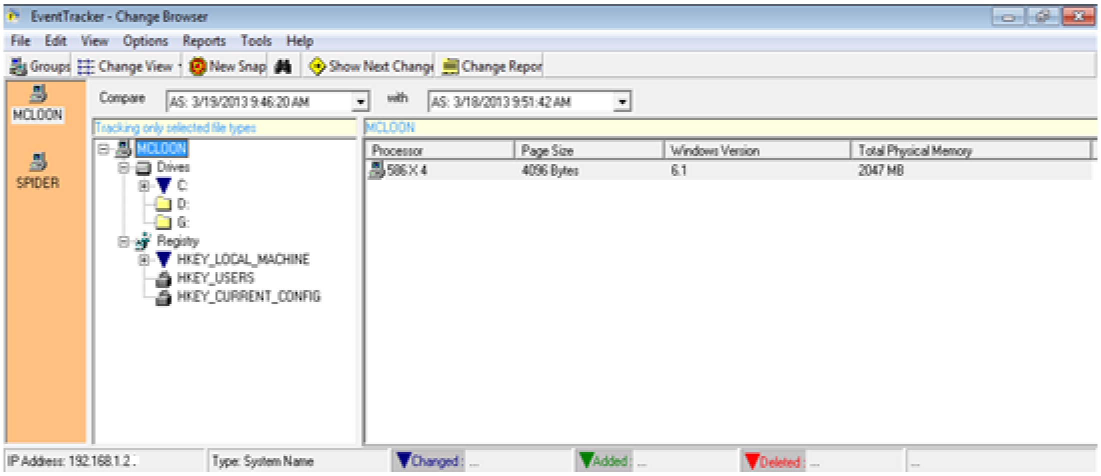
View Type: Graph

View By: Change Type

Policy Name	Policy Description	System Name	Integrity Violatio...	Comparison Time	Schedule Freque...
● MS-SCM Windows 7 (Bitlocker-EC)	Microsoft Security Compliance Management for Wind...	SPIDER	0	3/19/2013 3:45:46 PM	Daily
● MS-SCM Windows 7 (EC-Desktop)	Microsoft Security Compliance Management for Wind...	SPIDER	0	3/19/2013 3:47:27 PM	Daily
● Sample Critical File Policy	This policy is designed to demonstrate File Integrity M...	SPIDER	0	3/19/2013 11:21:21 AM	Daily
● SCAP Office 2007	This guide has been created to assist IT professionals, i...	SPIDER	0	3/19/2013 3:48:51 PM	Daily
● USGCB Win7-x86	This guide has been created to assist IT professionals i...	SPIDER	0	3/19/2013 3:48:15 PM	Daily
● DISA Gold Office 2007	DISA Gold Disk - Microsoft Office System 2007	ESXWIN2K3VM11	Scheduled	3/20/2013 2:16:19 PM	Daily
● 2003 Domain Controllers DISA-G...	This benchmark was created based on Microsoft Wind...	ESXWIN2K3VM11	Scheduled	3/20/2013 3:00:00 PM	Daily
● 2003 Member Servers Legacy-Mo...	This benchmark was created based on Microsoft Wind...	ESXWIN2K3VM11	Scheduled	3/20/2013 2:59:45 PM	Daily
● MS-SCM Windows 7 (Bitlocker-EC)	Microsoft Security Compliance Management for Wind...	ESXWIN2K3VM11	Scheduled	3/20/2013 3:45:07 PM	Daily
● MS-SCM Windows 7 (EC-Desktop)	Microsoft Security Compliance Management for Wind...	ESXWIN2K3VM11	Scheduled	3/20/2013 3:45:38 PM	Daily
● USGCB Win7-x86	This guide has been created to assist IT professionals i...	ESXWIN2K3VM11	Scheduled	3/20/2013 3:45:51 PM	Daily
● SCAP Office 2007	This guide has been created to assist IT professionals, i...	ESXWIN2K3VM11	Scheduled	3/20/2013 3:45:17 PM	Daily

Figure 806

- Click the **Change Browser** button.
  EventTracker – Change Browser window displays.



Compare AS: 3/19/2013 9:46:20 AM with AS: 3/18/2013 9:51:42 AM

MCLOON

Processor	Page Size	Windows Version	Total Physical Memory
586 X 4	4096 Bytes	6.1	2047 MB

IP Address: 192.168.1.2 Type: System Name

Figure 807

For detail information regarding this chapter, please refer Change Audit.

40.3 Changing Policy Dashboard

This dashboard gives the same view as in **Change Audit menu -> Last Changes** in EventTracker. Please refer Change Audit for detail information.

40.4 Configuring 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.

- Click Analyze Analyze.

  For detail information regarding this, please refer Change Audit.

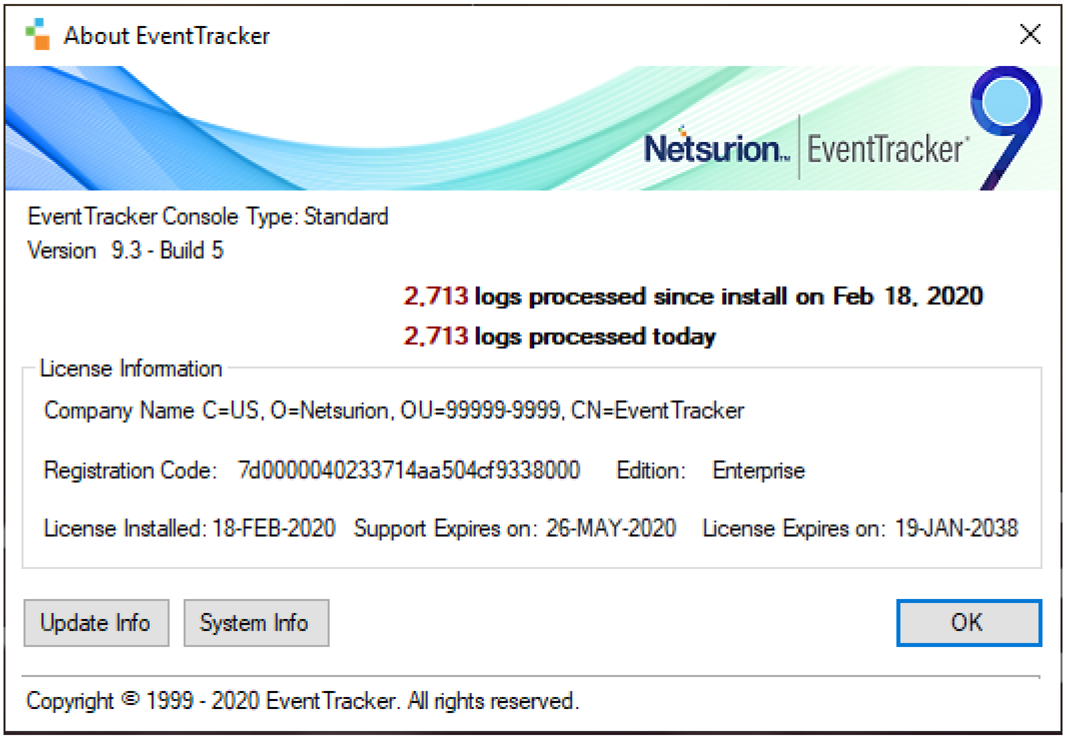
41. About EventTracker

In this chapter, you will learn about:

- EventTracker and License Information

41.1 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.



About EventTracker

EventTracker Console Type: Standard

Version 9.3 - Build 5

2,713 logs processed since install on Feb 18, 2020

2,713 logs processed today

License Information

Company Name C=US, O=Netsurion, OU=99999-9999, CN=EventTracker

Registration Code: 7d0000040233714aa504cf9338000 Edition: Enterprise

License Installed: 18-FEB-2020 Support Expires on: 26-MAY-2020 License Expires on: 19-JAN-2038

Copyright © 1999 - 2020 EventTracker. All rights reserved.

Figure 808

1. Click **Update Info** to view any updates that has been installed.
2. Click **System Info** to view system information.

42. IT Glue Integration

IT Glue is an IT documentation software designed to help maximize the efficiency, transparency, and consistency of your team. It allows organizations to upload any documents, reports or any flexible records and provide access to the users securely. It provides Rest API which is used to upload reports to IT Glue as flexible records. Any organization can use IT Glue for day-to-day activities. IT Glue allows users to define the flexible asset template and upload the reports as per the template.

MSP's using the IT Glue will be able to view EventTracker generated security and compliance summary reports under the "EventTracker Reports" flexible asset template in the same IT Glue portal.

For detailed information regarding this, refer please IT Glue User Guide.

43. ConnectWise integration

ConnectWise Manage is a business process automation platform that allows your business to sell, service and support technology more efficiently and in a more streamlined way. The business management tool allows your business to centralize all information, automate business processes, real-time visibility in operations, and provide better customer support.

For detailed information regarding this, please refer ConnectWise User Guide.

44. Anomalous Login Detection in EventTracker

Anomalous Login is a method of attack such as a brute force attack by which the attacker is identifying the username and password of the system or web page randomly. By generating the username or password from a remote location, it can be compromised over time. From an unknown source, an attacker can try this by simulating a random number of passwords.

EventTracker agent is introducing a new kind of capability to identify Anomalous Login activity. Anomalous Login identification is based on username and IP address.

For detailed information regarding this, please refer Anomalous Login Detection in EventTracker User Guide.

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 state 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 should be recorded and monitored for possible abuse.

User Logoff report

GLBA requirements state that user accesses to the system should 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 ach 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 permission 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' 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.

Appendix – BASEL II

BASEL II

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 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 systems supporting 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.

Appendix – PCI DSS

PCI DSS

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

Term	Description
Agent Configuration	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.
Alert Configuration	Process of configuring alert notifications in the form of Sound, E-mail, Console message or any Custom action.
Alerts	A feature that instructs programs that notify timely information about the events.
Analyzing Event Traffic	The process to analyze the event traffic patterns. The data can be used to filter out irrelevant events and perform other operation tasks.
Audible Alert	A feature that instructs programs that usually notifies information by sound.
Auto Discover Mode	Process of adding computers from your network automatically.
Change Audit	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.
Change Management	The process that enables the user to monitor, analyze, understand, and recover from change.
Console Message Alert	A feature that instructs programs that usually notifies information to the selected machine.
CPU Performance	A term used to monitor the CPU performance.
CRL	A CRL is a list identifying revoked certificates, which is signed by a CA and made freely available at a public distribution point.
Custom Alert	A feature that instructs programs to execute custom action on receipt of an event.
Disk Space Usage	A term used to monitor the disk space usage.
E-mail Alert	A feature that instructs programs that usually notifies information by E-mail.
Event Filtering	Process of filtering the events that are not important. Monitoring unimportant events cause the database to occupy more disk space.
Event Information	A window pane that displays the summary of event details in the EventTracker Management console.

Term	Description
Event Logs	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.
Event Monitoring	A window pane that displays the real-time event information in the EventTracker Management console.
EventBox	An archived event data file. You can create an EventBox by using EventVault Warehouse Manager console.
EventTracker	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.
EventVault	The console used to archive the events from EventTracker database. EventVault can operate in Automatic Archival and EventBox on demand methods.
Exclude List	The process to configure the network connections that need not to be monitored.
Filters	The process to filter out events that you do not want to monitor.
Include List	The process to configure the network connections to monitor. Include list Network connections always override the Exclude list Network connections.
IP Subnet	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.
Knowledge Base	A Web site containing information about Windows events and custom EventTracker events.
Flex Report	Process of analyzing the event details by setting criteria such as date range, time range, rule, and computer.
Log Backup	A backup that copies event logs automatically in the EventTracker Agent directory whenever the event logs are full.
Logfiles	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.
Manager Configuration	It comprises of various options to configure Alert events, Keyword indexing, Syslog/virtual collection point, Direct Log Archiver / NetFlow Receiver, Agent File transfer settings, and SMTP server settings.
Memory Usage	A term used to monitor the memory usage.
Monitor Syslog	The process to monitor Syslog being sent by an UNIX system.
NetFlow	A Cisco-proprietary IP statistics collection feature that collects information on IP flows passing through a router.
Quick Statistics	The process to view the summary of event statistics such as Total events received, Total alerts received, Total systems monitored, and so on.

Term	Description
SNMP Event Manager	An application called TrapTracker used to monitor and manage critical traps emitted by network devices in your enterprise.
SNMP Traps	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.
Syslog Receiver	The process to set the SYSLOG receiver. After setting this option, the Manager will receive any SYSLOG being sent by an UNIX system.
System Information	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.
System Manager	A console helps you to manage groups, systems, and Agents.
System Performance	The process to monitor the system performance in graph, histogram, or report form.
System Statistics	A window that displays the system statistics in EventTracker Management console.
TCP	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.
UDP	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.
Vulnerability	Vulnerabilities are weaknesses in process, administration, or technology that can be exploited to compromise your IT security.
Vulnerability Parsers	The parser reads the XML report generated by Vulnerability scanners and extracts vulnerability information from it.
Vulnerability Scanners	A vulnerability scanner is a computer program designed to assess computers, computer systems, networks, or applications for weaknesses.