



Upgrade Guide

Upgrading to EventTracker v6.4 b50

Upgrade Guide

8815 Centre Park Drive

Columbia MD 21045

U.S. Toll Free: 877.333.1433



Publication Date: Feb 17, 2010

Abstract

The purpose of this document is to help users upgrade from EventTracker v.6.3 b31, b37, b53, and b59 to EventTracker v6.4 b50, and to verify the expected functionality and performance of all its components. If you encounter any problems during upgrade process, please contact Support to get quick and thorough instructions.

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

This document is for informational purposes only. Prism Microsystems, Inc. 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 Guide may be freely distributed without permission from Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.

Prism Microsystems, Inc. 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 Prism Microsystems, Inc. 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.

© 2010 Prism Microsystems, Inc. All rights reserved.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

WHO SHOULD USE THIS GUIDE?	4
BEFORE YOU UPGRADE.....	4
WHAT IS NEW IN EVENTTRACKER V6.4 B50	5
ENHANCEMENTS	5
DEFECT RESOLUTION	7
PREREQUISITES	9
PLANNING	10
COMPLETE UPGRADE PROCEDURE	11
MANAGEMENT CONSOLE	11
UPGRADING FROM V.6.3 B31, B37, B53, B59 TO V6.4 B50	11
<i>Post Upgrade Process</i>	12
VALIDATION	15

Who should use this Guide?

It is incumbent upon all users of EventTracker v.6.3 b31, b37, b53, and b59 who wish to upgrade to v6.4 b50.

Prism strongly recommends that you read the entire document thoroughly before you begin the upgrade process.

Before you upgrade

1. Thoroughly read the “EventTracker Architecture” guide. This guide explains the architecture and sample deployment methods with illustrations.
<http://www.prismmicrosys.com/resources/documents/EventTrackerArchitecture.pdf>
2. Contact support@prismmicrosys.com for information regarding license keys.

Important: Users of versions 5.x and below contact support@prismmicrosys.com for complete and thorough instructions.

What is new in EventTracker v6.4 b50

Enhancements

1. New Features

- a.* Alerts Dashboard
- b.* Enterprise Activity Dashboard
- c.* Receiver enhancements
- d.* Event 3278 for multiple Agent configuration change requests
- e.* Event 3277 to notify agent install/upgrade status
- f.* Event 3276 to notify while changing system types
- g.* Event 3249 in Agent configuration changes Category
- h.* Agent health status check enhancements
- i.* Archive Indexer for Local and Collection Points
- j.* BEA WebLogic logs support in DLA

2. New Reports

- a.* Idle Time Report
- b.* USB Device Disabled Report
- c.* USB Device Report (Summary / Detail)
- d.* User Activity

3. New Alerts

- a.* Cisco Catalyst
- b.* Cisco IOS
- c.* Direct Log Archiver
- d.* EventTracker: Agent configuration changed, DLA File processing failed

4. New Knowledge Packs

- a.* Cisco ASA
- b.* Cisco Aironet
- c.* Cisco Director
- d.* F-Secure
- e.* MSSQL Server
- f.* WatchGuard
- g.* Windows Backup
- h.* SQL Server
- i.* Added Enterprise Activity event Categories

- j.* Agent configuration changes Category
 - k.* Certificate Services (Group with 16 categories)
 - l.* CISCO IOS (Group with 27 categories)
 - m.* EventLogCentral: Login failure, Role config changes, User Logoff, User logon, Agent configuration changes, Custom column config changes
 - n.* EventTracker: Direct Log Archiver, Report/Analysis config changes, Windows log backup and clear
- 5.** Updated Knowledge Packs
 - a.* FTP
 - b.* IIS
 - c.* DHCP
 - d.* ELC Logon Category
 - e.* Windows Group Policy
 - f.* Windows System: patches and hotfixes
 - g.* WhatChanged
- 6.** Minor changes
 - a.* Set "Show Only Active Alerts" as default in fresh installs- Minor
 - b.* Adding XML contents in Event description from Vista Event logs- Minor
 - c.* Reading custom event logs from non-vista systems- Minor
 - d.* Enabling Automatic and Manual Collection Masters- Minor
 - e.* Excluding non-windows systems from license upgrade in System Manager - minor
 - f.* Adding keyword analysis to Legacy Log Volume (Traffic) Analyzer
 - g.* Adding notes while exporting details of Reports on Reports
 - h.* Changes in Log Volume Analysis to have one line Event Descriptions
 - i.* Changes in system manager to recognize system type Windows 7
 - j.* Facility to change system type in System Manager
- 7.** Other Changes
 - a.* Include Vista/2008 events in legacy Traffic Analyzer
 - b.* Consider Syslog TCP ports after upgrade
 - c.* Syslog port configuration to define single port for UDP/TCP pair

Defect Resolution

1. Install issue with EventTracker Alerter service in Vista/2k8
2. Printer Usage reports failure in 2008
3. LFM exceptions in EventTracker Agent
4. License count issues with Windows 7 in License usage
5. Offline agent configuration event translation issues
6. Retaining Alerts folder & files while retaining data during uninstall
7. Agent exceptions while sending events
8. Offline Agent Configuration updates
9. Diagnostics issue, picking archiver index db always from default path
10. Retaining original system information in Syslog description
11. Agent upgrade issues with Remote Agent Installer
12. Agent error log growing issue, unknown exceptions, and connection errors due to DNS lookup
13. Custom remedial actions not working at Agent side
14. Reports Quick View refine event description issue
15. Non-vista agent, where it was checking for backup directory even when archiving is disabled
16. Import/Export missing Report description
17. Log Search issues with user names
18. EventVault service struck issues while purging CAB files
19. Report configuration change audit events (3283) issue while configuring more number of systems
20. CAB transfer issues with Collection Point/Master
21. EventVault service struck issues while purging CAB files
22. Agent Configuration Console slowness issue while applying configuration changes to all Agents
23. Append Archives utility crash
24. Blank report on Agent Management Tool when group name contains "-" character
25. Service access privilege issues in EventTracker Receiver
26. Syslog Receiver Crash
27. Scheduled Report execution, status and e-mailing, timing overlap issues
28. Exception in CPU performance report
29. issdb size growing issue because of frequent system information updates
30. Domain\username issue in Reports Quick View
31. Duplicate event counts on receiver load file (etw) for Syslogs
32. Logs Summary for Event User (Vista event id: 4768). Backslash missing
33. Refine option is missing in the Quick View window of Alerts detail/Summary
34. File not found error when we try to send the published HTML report through mail

35. Default Alerts/Reports during installation
36. EC files processing failures (PDU extraction failed)
37. Management console crashes when installed in other than default path
38. Highlighting errors while refining systems in log search
39. No matching records in Alerts Category, when Alerts Category is having too many rule sets
40. Empty window displayed in quick view when the event count is in the multiples of 1000
41. Redundant values displayed in Syslog fwd action configuration
42. Agentless offset errors/log clearing issues
43. Event truncation issues in VISTA/2K8
44. Delay in Alert processing, writing into cache in Rxer
45. Invalid duration in scheduled run-now option
46. Correlator service high CPU usage
47. Receiver drops events when more number of Agents connected
48. Report exception "Cannot access the disposed object "
49. Log backup when Eventlog is full
50. Agent crash while applying remote Agent configurations
51. Report/analysis issue with upgrade
52. Receiver crash in TCP mode
53. Agent Management tool crash in VISTA/2k8
54. Report migration error "input string was not in a correct format" during upgrade
55. Checksum verification issues with log search

Prerequisites

Before you begin the upgrade process, please follow this checklist and make sure that you have all the components in place to perform a successful upgrade.

The most effective upgrade method is to first export all the custom settings using Export Import Utility, install the new version and import the custom settings. There is no need to export all policy settings since all the Categories included in any prior versions have been retained.

The recommended method is to first upgrade the Management Console and validate all its functionality, next upgrade the Agents and lastly verify the performance.

Planning

This section gives you a rough estimation of time required for upgrading as well as monitoring the successful upgrade. It might take 60 – 90 minutes for you to read this document and to complete the upgrade process gracefully. You will also require spending a few minutes the following day after the upgrade, to verify all your Scheduled Reports are being generated. If any reports fail to generate, then please read the Validation section at the end of this document.

Complete Upgrade Procedure

Verify that all the prerequisites described above have been satisfied.

Management Console

Before the upgrade process begins,

1. Backup all the custom Categories, Alerts (Please check the “Export E-mail Settings” check box), Filters, Domains, Systems, Scheduled Reports, and RSS Feeds using Export Import Utility.
2. Backup issdbv3.mdb and ETReports.mdb files (...Program Files\Prism Microsystems\Common).
3. If you are using the Agentless monitoring option, export all Systems to retain polling list and other settings.
4. Close/terminate all the EventTracker components like Management Console and Reports Console, including **RDP (Remote Desktop Protocol) sessions**.
5. Open the Windows Task Manager and check if the following processes are running in the background, if so, terminate them:
 - ETConsole3exe
 - ETWReporter2.exe
 - EtwControlPanel.exe
 - evtCabIntChkMgr.exe
 - ETReporter.exe
6. Note down the custom changes you have made in the Trusted List (Agent Configuration -> Network Connection Monitor -> Suspicious Traffic Only (SNAM) -> Trusted List).

Upgrading from v.6.3 b31, b37, b53, b59 to v6.4 b50

1. Uninstall the existing version by retaining old configuration and data.
2. Restart the EventTracker Manager server.
3. Install EventTracker v6.4 b50
4. Remove all Categories.
 - a. Open the Management Console.
 - b. Click the **Configure** menu and select the **Manage Categories** option.
 - c. Right-click the **All Categories** Categories group.
 - d. From the shortcut menu, choose **Delete All**.

5. Using Export Import Utility, import **Complete Categories.iscat** file from the EventTracker installation folder typically ...\\Program Files\\Prism Microsystems\\EventTracker\\Configuration Files.
6. Using Export Import Utility, import all the custom Categories, Alerts, Filters, Domains, Systems, Scheduled Reports, and RSS Feeds.
7. Verify that the Scheduled Reports, RSS Feeds, Categories, Filters, Alerts, Systems, and Domains are intact.
8. Upgrade all agents using the System Manager.
9. Update the Trusted List with the changes you have noted down earlier.
10. Compact the databases.
 - a. Double-click **Maintenance Tools** on the Control Panel.
 - b. Double-click **Compaction Utility**.
 - c. Select the check boxes against `issdbv3.mdb` & `ETReports.mdb` and then click **Compact Now**.
11. If you do not want to view All Alerts and prefer to view only Active Alerts on the Management Console, do the following:
 - a. Open the Management Console.
 - b. Click the **Configure** menu and select the **Configure Manager** option.
 - c. Select the **Show Only Active Alert events in Console** check box.
 - d. Click OK.

Active Alerts: Active Alerts are Alert events that have at least one action set.

Show Only Active Alert events in Console: To view only active Alerts, select the **Show only Active Alert events in Console** check box. When this check box is selected, EventTracker stores all Alert events in the database, but displays only the active Alerts on the Management Console. Since all Alert events are stored in the database analysis could be done on all Alert events.

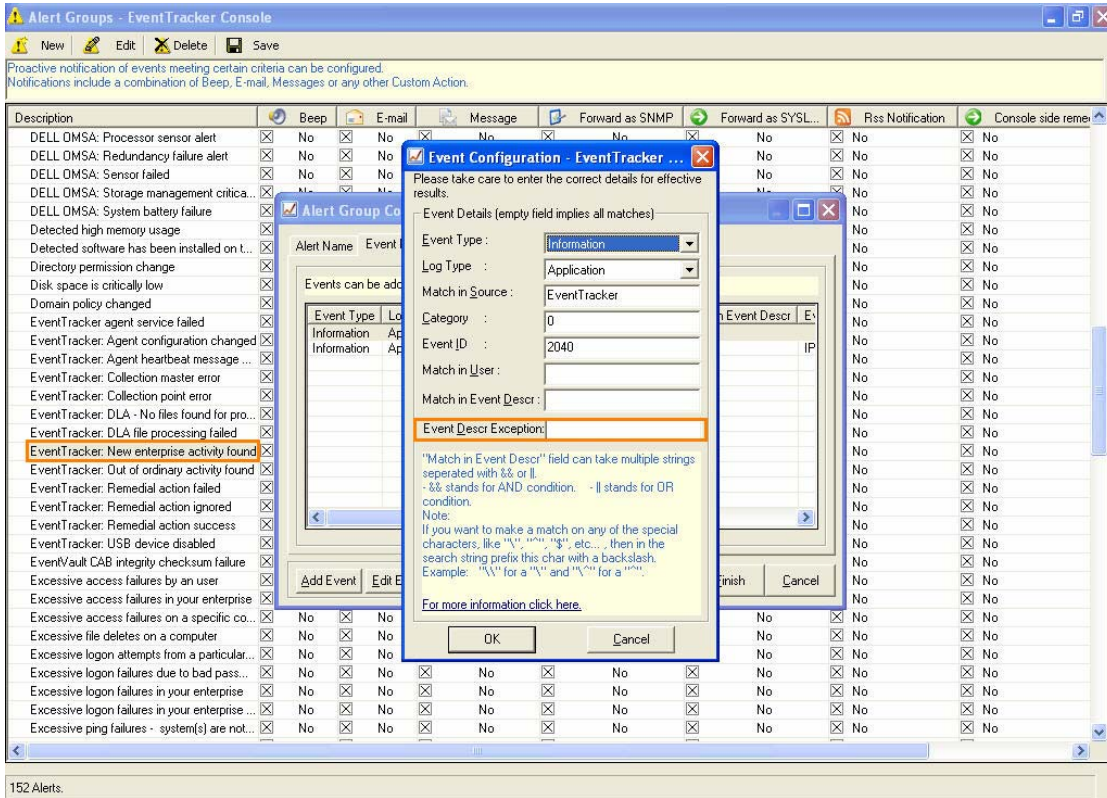
Store Only Active Alert events: To store only active Alerts, select the **Store only Active Alert events** check box. When this check box is selected, EventTracker stores only the active Alerts events in the database. Analysis could be done only on active Alert events. "Show only Active Alert events in Console" option is enabled by default, if you select this check box.

For all upgrades, suggested settings would be **Store Only Active Alert events** to speed up the archiving process, as this option helps to work only on active alert rules.

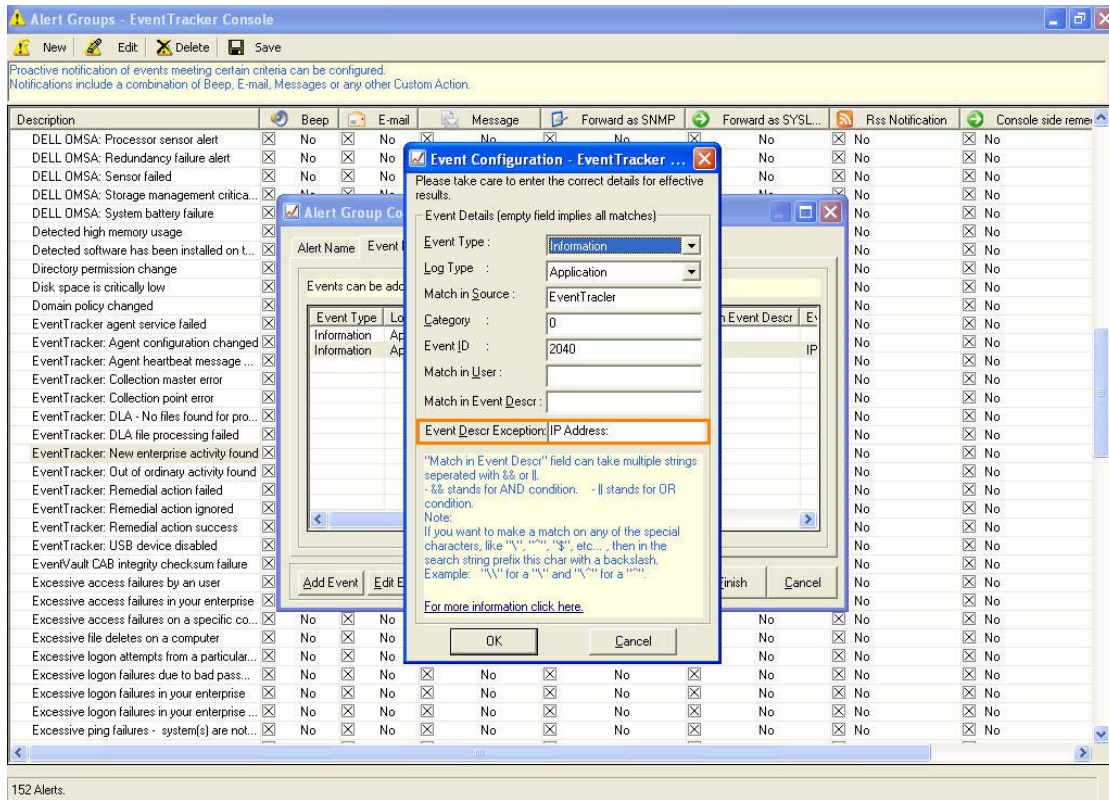
12. If any e-mail security application like Symantec, McAfee, Trend Micro is installed, then add "Prism.Reports.ServiceProcessor.exe" to the exception list.

Post Upgrade Process

1. Double-click **Alerts Dashboard** on the EventTracker Control Panel.
2. Click the **Alert Config** hyperlink at the right-upper corner.
EventTracker displays the Alert Groups console.
3. Scroll down and double-click the **EventTracker: New enterprise activity found** Category.
EventTracker displays the Alert Group Configuration window.
4. If there are two entries for event id 2040, remove the one that has no **Event Descr Exception** specified.



5. Retain the entry that has Event Descr Exception specified as IP Address:



6. Click **Save** to save the changes.

Validation

After successfully completing the upgrade process, please verify that the Backup Directory path, Directory Path for Scheduled Reports copies and Report Data Cache path are properly configured.