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.6.2.x 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.

Table of Contents

Who should use this Guide?

It is incumbent upon all users of EventTracker v.6.2.x 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. Agent health status check enhancements
    h. Archive Indexer for Local and Collection Points
    i. Search based Management Console
    j. Added simplified log search interface
    k. VMware Agent
2. New Knowledge Packs
    a. Juniper JUNOS
    b. Motorola Wireless Switch
    c. Cisco ASA
    d. Cisco Aironet
    e. Cisco Director
    f. F-Secure
    g. MSSQL Server
    h. WatchGuard
    i. Enterprise Activity event Categories
    j. Windows Backup
    k. SQL Server
    l. Certificate Services
    m. EventTracker: Windows log backup and clear
    n. EventTracker: Direct log archiver
    o. CISCO IOS
    p. EventTracker: Agent configuration changes
    q. Oracle Categories
    r. Hyper-V

s. Cisco Catalyst Switch
t. Juniper SBR
u. VMware
v. Dell OMSA

3. Updated Knowledge Packs
   a. FTP
   b. IIS
   c. DHCP
   d. Vista
   e. Active Directory events
   f. Group Policy Categories
   g. System Patches and hot fixes Category
   h. WhatChanged Categories
   i. ELC logon Categories
4. New Alerts
   a. Cisco Catalyst
   b. Cisco IOS
   c. VMware
   d. Dell OMSA
   e. Oracle
5. New Reports
   a. User Activity
   b. Idle Time Report
   c. OWASP (Web Attack)
   d. SharePoint Traffic Top Hits and Bandwidth Report
   e. Consensus Audit Guidelines under Compliance
6. Minor enhancements
   a. Changes to accept user credentials while upgrading license on remote agents
   b. Set "Show Only Active Alerts" as default in fresh installs
   c. Adding XML contents in Event description from Vista Event logs
   d. Reading custom event logs from non-vista systems
   e. Enabling Automatic and Manual Collection Masters
   f. Adding keyword analysis to Legacy Log Volume (Traffic) Analyzer
   g. Adding notes while exporting details of Reports on Reports
   h. Facility to change system type in System Manager
   i. Added "Smart Viewer" facility in reports to enable detailed views from summary views
   j. Added SHA1 checksum in Archiver for integrity verifications
   k. Facility "Show Alert" to locate the Alert rule from the Alert event displayed in Management Console

l. GUI for Direct Log Archiver
m. Facility to configure scheduled/defined report from published reports
n. New alert action "Forward events as SYSLOG messages"

7. Other changes
   a. System manager to recognize system type Windows 7
   b. Log Volume Analysis to have one line Event Descriptions
   c. Syslog port configuration to define single port for UDP/TCP pair
   d. Include Vista/2008 events in legacy Traffic Analyzer

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. Agent Configuration Console slowness issue while applying configuration changes to all Agents
21. Scheduled Report execution, status and e-mailing, timing overlap issues
22. Blank report on Agent Management Tool when group name contains "-" character
23. Exception in CPU performance report
24. issdb size growing issue because of frequent system information updates
25. Domain\username issue in Reports Quick View
26. Duplicate event counts on receiver load file (etw) for Syslogs
27. Logs Summary for Event User (Vista event id: 4768). Backslash missing
28. Refine option is missing in the Quick View window of Alerts detail/Summary
29. File not found error when we try to send the published HTML report through mail
30. Default Alerts/Reports during installation
31. EC files processing failures (PDU extraction failed)
32. Management console crashes when installed in other than default path
33. Highlighting errors while refining systems in log search
34. No matching records in Alerts Category, when Alerts Category is having too many rule sets

35. Empty window displayed in quick view when the event count is in the multiples of 1000
36. Redundant values displayed in Syslog fwd action configuration
37. Agentless offset errors/log clearing issues
38. Event truncation issues in VISTA/2K8
39. Delay in Alert processing, writing into cache in Rxer
40. Invalid duration in scheduled run-now option
41. Correlator service high CPU usage
42. Append Archives utility crash
43. Exhausted License warning message in Console & Agent Installer
44. CP/CM Encryption issues
45. EventVault service struck issues while purging CAB files
46. Append Archives utility crash
47. Service access privilege issues in EventTracker Receiver
48. Receiver drops events when more number of agents connected
49. Syslog Receiver crash
50. TrapTracker licensing expiry issue
51. USB Tracking event user issues
52. Importing Alerts with remedial actions
53. Append archives, Archiver re-indexer utilities to support CAB files generated by multiple ports.
54. E-mail failures in alerts in case default reports not installed
55. "invalid use of null" issue in System Manager during Agent deployment
56. Upgrade issue, Check Point configurations are not retained
57. Archiver not updating bin file when deleting CAB files in EventVault
58. RSS feed configuration not getting retained
59. Vista Agent SID translation issue
60. DB Compaction Utility issues
61. Fix for User Authentication for e-mail delivery in case of Schedule Reports
62. Trap buffer overflow issue in Rxer
63. 100% CPU utilization issues in Vista/2k8
64. Vista Agent filter issue

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**:**
   - ETConsole2.exe
   - ETWReporter2.exe
   - EVTRptmgr.exe
   - EtwControlPanel.exe
   - evtCabIntChkMgr.exe
   - ETRptSchedulerMgr.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 v6.2.x 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.

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.