Upgrade Guide

Upgrading to EventTracker Enterprise v7.1

Upgrade Guide

8815 Centre Park Drive
Columbia MD 21045
U.S. Toll Free: 877.333.1433

Publication Date: Apr 11, 2011

Abstract

The purpose of this document is to help users upgrade from EventTracker v.7.0 to EventTracker v7.1, 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.7.0 who wish to upgrade to v7.1.

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.

What is New in EventTracker v7.1

EventTracker v7.1 (Build 52)

1. Filter Event id(s) and Event Source(s) when generating a report/analysis.
2. Configurable option to show/hide the statistics & graph display in log search page
3. Custom data feature for system selection in EventTracker Agent Management Tool
4. Facility to import/delete custom list of systems in Import Export Utility

EventTracker v7.1 (Build 38)

1. DLA-Extensions (Other File Transfer Option)
2. Reading SQL DB Trace logs via DLA
3. Reading EVTX log files in DLA
4. CD/DVD monitoring (only Windows Explorer)
5. CP-CM to transfer index info files.
6. Standalone utility for analyzing event traffic from eventlog (enhanced GetAllEvt)
7. Change Audit, Change Assessment and Configuration Assessment dashlets added.
8. WebSlice for Alerts added
9. Diagnostic/Application information dashlets
10. Smart Card reader
11. Extending CP-CM Data transfer for V7 features, changes done in Log Search page to provide a drop down to show the list of CPs.
12. New categories for StatusTracker audit events

EventTracker v7.1 (Build 16)

1. DLA-Extensions (Other File Transfer Option).
2. Reading SQL DB Trace logs via DLA.
3. Reading EVTX log files in DLA.
4. CD/DVD monitoring (only Windows Explorer).
5. CP-CM to transfer index info files.
6. Standalone utility for analyzing event traffic from eventlog (enhanced GetAllEvt).
7. Change Audit, Change Assessment and Configuration Assessment dashlets added.
8. WebSlice for Alerts added.
9. System search (Enhanced feature to overcome limitations existing in the current release).
10. Diagnostic/Application information dashlets.
11. Extending CP-CM Data transfer for V7 features, changes done in Log Search page to provide a drop down to show the list of CPs.
12. EventTracker XML API (Available as Patch).
13. Remote Indexer API (Available as Patch).

14. Smartcard login support in EventTracker Web (Available as Patch).

Changes & Bug Fixes

EventTracker v7.1 (Build 52)

1. Fix for EventTracker Receiver buffer overflow issues when Alert Notification Status option is disabled.
2. Fix for the issue where event filters and exceptions are not getting evaluated properly.
3. Fix for data mismatch in Netflow reports.
4. Fix for TCP connection issues due to incomplete message header during DLA file transfer.
5. Fix for the issue where some of the events were getting missed in DLA mode from vista agent.
6. Fix for EventTracker Receiver high CPU usage while processing TCP connections.
7. Fix for synchronization issues with Collection Point configuration database.
8. Fix to display the report/analysis configured for a CP.
9. Fix for issue, reports not being processed as the service fails to respond.
10. Fix for Alert notification cache purging issues.
11. Fix for the issue where application crashes for some benchmarks.
12. Fix for issue, EventTracker Diagnostics locking cache files and causing EC file backlog.
13. Fix for EventTracker Agent deployment failures due to password encryption issues.
14. Fix for the issue where alert action was being performed even if the risk is less than the threshold value.

EventTracker v7.1 (Build 38)

1. Changed Alert "USB insert alert" to "Media insert alert"
2. Added missing admin activity events in EA.
3. EventVault GUI crash while verifying checksum value.
4. Site Map error when NetFlow, Config assessment features are not available.
5. Port-0 EC2 files backlog at Cache\ttw folder
6. Improper OS type and asset value issues.
7. Event Correlator service crash.
8. Compressed files left in Cache\ttw folder by Agent file transfer.
9. Missing CAB files when commit failed on EventVault.
10. Forward Traps issue, Alerts configuration issues in TrapTracker
11. Changes in Resource Access Success/Failure report to process event id: 5145
12. System filter issue in alerts configured with multiple groups.
13. Results summary console incorrectly displays database error.
14. Add CAB files to CP queue fails when multiple CM configured.
15. Change Assessment Scheduled reports issue (Improvements in handling of scheduled actions)
16. Log-View performance issues
17. Error when generating report on reports on Collection Master
18. Changes to remember the page count & sort order in System Manager

EventTracker v7.1 (Build 16)

1. Added missing admin activity events in EA.
2. Fix for EventVault GUI crash while verifying checksum value.
3. Fix for Site Map error when Netflow, Config assessment features are not available.
4. Fix for Port-0 EC2 files backlog at Cache\ttw folder.
5. Fix for improper OS type and asset value issues.
6. Fix for Event Correlator service crash.
7. Fix for issue, compressed files left in Cache\ttw folder by Agent file transfer.
8. Fix for missing CAB files when commit failed on EventVault.
9. Fix for Forward Traps issue, Alerts configuration issues in TrapTracker.
10. Changes in Resource Access Success/Failure report to process event id: 5145.
11. Fix for system filter issue in alerts configured with multiple groups.
12. Fix for the issue in Results summary console incorrectly displays database error.
13. Fix for issue, Add CAB files to CP queue fails when multiple CM configured.
14. Change Assessment Scheduled reports issue (Improvements in handling of scheduled actions).
15. Fix for Log-View performance issues.
16. Fix for error when generating report on reports on Collection Master.
17. Changes to remember the page count & sort order in System Manager.

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 Manager 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. Close/terminate all the EventTracker components like Management Console and Reports Console, including **RDP (Remote Desktop Protocol) sessions**.

Upgrading from v7.0 to v7.1

1. Uninstall the existing version by retaining old configuration and data
2. Restart the EventTracker Manager server
3. Install EventTracker v7.1
4. Verify that the Categories, Alerts, Filters, and RSS Feeds are intact
5. Upgrade all Windows Agents using the System Manager

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.