Upgrade Guide

Upgrading to EventTracker v7.1 Enterprise
Abstract

The purpose of this document is to help users upgrade from EventTracker v.6.4 b50 to EventTracker v7.1 Enterprise, 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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>WHO SHOULD USE THIS GUIDE?</td>
<td>4</td>
</tr>
<tr>
<td>BEFORE YOU UPGRADE</td>
<td>4</td>
</tr>
<tr>
<td>WHAT IS NEW IN EVENTTRACKER V7.1 ENTERPRISE</td>
<td>5</td>
</tr>
<tr>
<td>ENHANCEMENTS</td>
<td>6</td>
</tr>
<tr>
<td>PREREQUISITES</td>
<td>7</td>
</tr>
<tr>
<td>PLANNING</td>
<td>8</td>
</tr>
<tr>
<td>COMPLETE UPGRADE PROCEDURE</td>
<td>9</td>
</tr>
<tr>
<td>MANAGEMENT CONSOLE</td>
<td>9</td>
</tr>
<tr>
<td>Upgrading from V6.4 b50 to V7.1 ENTERPRISE</td>
<td>9</td>
</tr>
<tr>
<td>POST UPGRADE PROCESS</td>
<td>9</td>
</tr>
<tr>
<td>VALIDATION</td>
<td>13</td>
</tr>
</tbody>
</table>
Who should use this Guide?

It is incumbent upon all users of EventTracker v.6.4 b50 who wish to upgrade to v7.1 Enterprise.
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.
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 v7.1 Enterprise

1. The Web interface has been given a comprehensive facelift to improve workflow and productivity
2. Integrated framework of EventTracker plug-ins (TrapTracker, StatusTracker)
3. FIPS 140-2 accredited cryptographic modules
4. Revamped Behavior Dashboard
   a. Dashlets – snippets of information with drill-down facility
   b. configure custom Behavior Rules
   c. add custom Behavior Rules as Dashlets
   a. in-depth visibility into network traffic and its patterns
   b. closely monitor and identify bandwidth abusers
   c. identify malicious applications running on the network
6. SCAP based Configuration Assessment
   a. assess configurations against compliance mandates such as FDCC
   b. rapidly detect and declare deviations
   c. create Plans of Actions and Milestones for the associated remediation
   d. generate XCCDF bundle for configuration reporting
7. Integrated Change auditing
8. Vulnerability Parsers
   a. to read and extract vulnerability information from XML reports generated by Vulnerability Scanners on EventTracker managed systems
   b. analyze extracted vulnerability information to evaluate potential impact
9. Integrated StatusTracker
10. EventVault Explorer
11. Agent DLA – an offline method to archive events directly into EventTracker data repository
12. Reports Transfer Facility in DLA
13. Internal scoring algorithm to automatically compute and rank Alert severity levels
14. New services
   a. EventTracker Remoting service – manage deployments of EventTracker Windows and Change Audit Agents
   b. EventTracker Indexer service – indexes CAB files to quickly search and find relevant information
15. Digital Certificate based licensing
16. Centralized storage on Manager system to store remote Agent configuration files
17. Manage Asset Value – value indicates how critical the system is
18. Tag Cloud weighting
19. Web Slices
20. Changed Alert "USB insert alert" to "Media insert alert"
21. New categories for StatusTracker audit events

**Enhancements**

1. EventTracker Agent service – receives and performs configuration assessment requests and sends back the assessment results
2. EventTracker Scheduler service – fetches configuration assessment requests from queue and dispatches the request to EventTracker Agents running on target system
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. Backup all custom Categories, Alerts (Please check the "Export E-mail Settings" check box), Filters, Scheduled Reports, and RSS Feeds using Export Import Utility.
2. Close/terminate all the EventTracker components like Management Console and Reports Console, including RDP (Remote Desktop Protocol) sessions.
3. 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 v6.4 b50 to v7.1 Enterprise

1. Uninstall the existing version by retaining old configuration and data.
2. Restart the EventTracker Manager server.
3. Install EventTracker v7.1 Enterprise.
4. Using Export Import Utility, import all the custom Categories, Alerts, Filters, and RSS Feeds.
5. Verify that the Categories, Alerts, Filters, and RSS Feeds are intact.
6. Upgrade all agents using the System Manager.
7. Update the Trusted List with the changes you have noted down earlier.

Post Upgrade Process

By default, EventTracker sets the Threat level of Alerts imported from v6.4 as Undefined as shown in the following figure. You need to explicitly set the Threat level as per your requirement.
Figure 1

1. To set the Threat level, click the title of the Alert.

EventTracker displays the Alert configuration page.
Figure 2

2. Select an appropriate option, for example, Critical from the Threat level drop-down list.

3. Click Finish.

EventTracker saves the configuration settings.
### Figure 3

![EventTracker Alert Management Interface](image)

The image shows the EventTracker Alert Management interface with a list of alerts. The alerts include:

- **ISA Server: Spooftach detected**
- **ISA Server: UDR attack detected**
- **RAS Server: Access violation**
- **RAS Server: AO, notifications**
- **RAS Server: Attack detection**
- **RAS Server: Hardware/Software failure**
- **RAS Server: Vacation Enterprise Update Failed**
- **Microsoft Exchange: AD service stopped**
- **Microsoft Exchange: Database mail size is reached**
- **Microsoft Exchange: ES service cannot be started**
- **Microsoft Exchange: Log disk full**
- **Microsoft Exchange: Server cannot handle influx of mail**
- **Microsoft Exchange: Unable to start Microsoft Exchange Server**
- **My Alert**

Each alert is categorized by its level of severity (Critical, Major, Minor, Informational, Warning) and has options for notification methods (Email, SNMP, SYSLOG).
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.