



Upgrade Guide

Upgrading to EventTracker v7.0 Enterprise

Upgrade Guide

8815 Centre Park Drive

Columbia MD 21045

U.S. Toll Free: 877.333.1433



Publication Date: Oct 05, 2010

Abstract

The purpose of this document is to help users upgrade from EventTracker v.6.4 b50 to EventTracker v7.0 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.

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 V7.0 ENTERPRISE	5
ENHANCEMENTS	6
PREREQUISITES	7
PLANNING	8
COMPLETE UPGRADE PROCEDURE	9
MANAGEMENT CONSOLE	9
UPGRADING FROM V6.4 B50 TO V7.0 ENTERPRISE	9
POST UPGRADE PROCESS	9
VALIDATION	13

Who should use this Guide?

It is incumbent upon all users of EventTracker v.6.4 b50 who wish to upgrade to v7.0 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.
<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 v7.0 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
5. NetFlow Receiver to read NetFlow v5/v9 logs. NetFlow Analyzer interface helps you with easy-to-understand network stats with graphical charts.
 - 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. Agent DLA – an offline method to archive events directly into EventTracker data repository
10. Internal scoring algorithm to automatically compute and rank Alert severity levels
11. 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
12. Digital Certificate based licensing
13. Centralized storage on Manager system to store remote Agent configuration files
14. Manage Asset Value – value indicates how critical the system is
15. Tag Cloud weighting

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 v7.0 Enterprise

1. Uninstall the existing version by retaining old configuration and data.
2. Restart the EventTracker Manager server.
3. Install EventTracker v7.0 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.

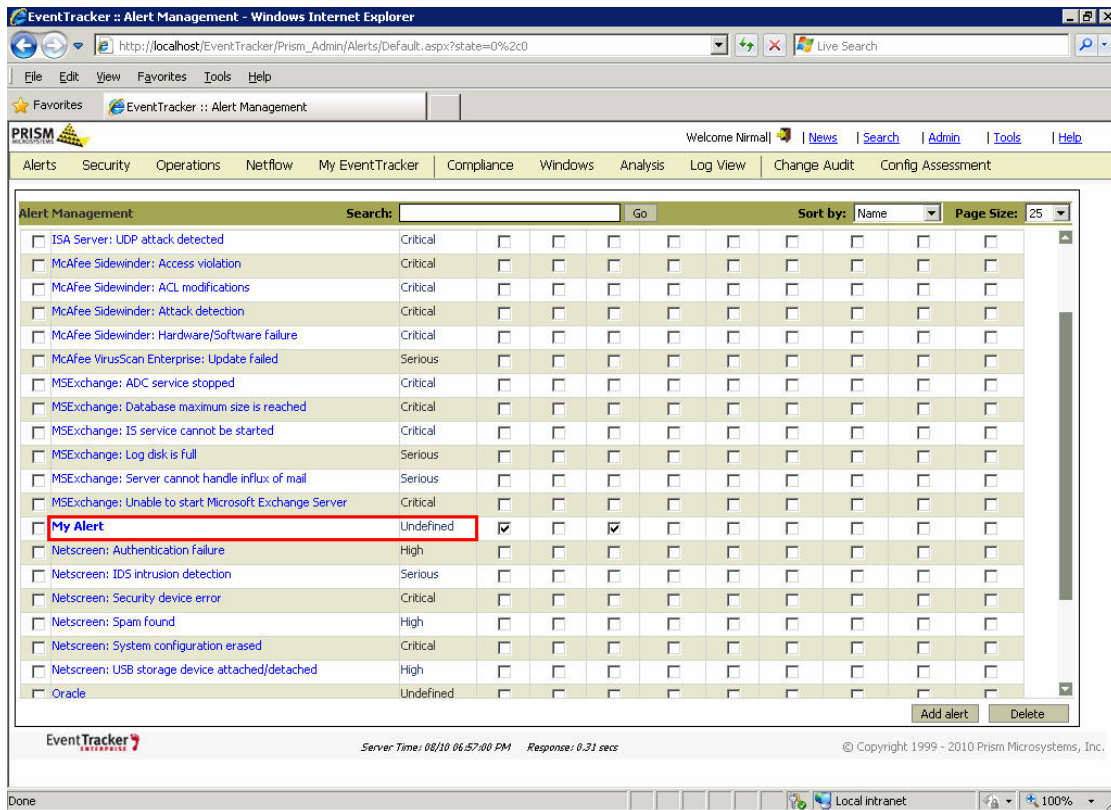
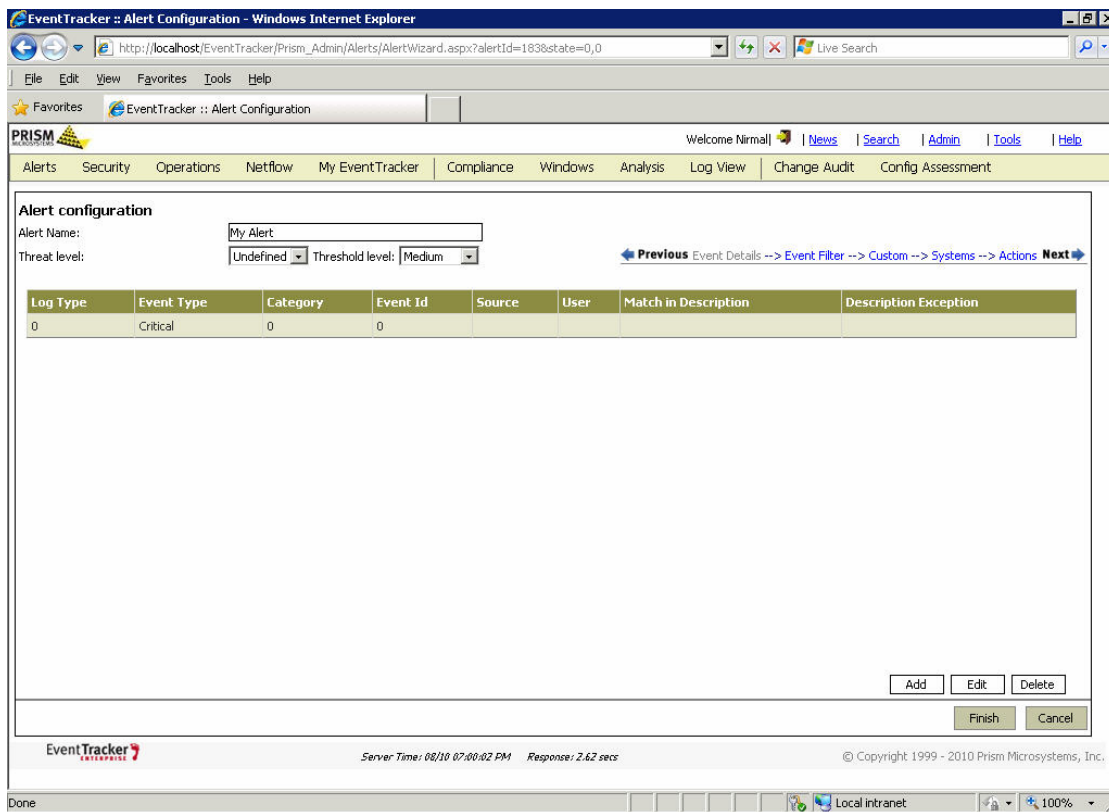


Figure 1

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.

EventTracker :: Alert Management - Windows Internet Explorer

http://localhost/EventTracker/Prism_Admin/Alerts/Default.aspx?state=0%2c0

PRISM Microsystems

Welcome Nirral | News | Search | Admin | Tools | Help

Alerts Security Operations Netflow My EventTracker Compliance Windows Analysis Log View Change Audit Config Assessment

Alert Management Search: [] Go Sort by: Name Page Size: 25

Alert Name	Threat level	Active	Beep	E-mail	Message	RSS	Forward as SNMP	Forward as SYSLOG	Remedial Action at Console	Remedial Action at Agent
<input type="checkbox"/> ISA Server: Spoof attack detected	Critical	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> ISA Server: UDP attack detected	Critical	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> McAfee Sidewinder: Access violation	Critical	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> McAfee Sidewinder: ACL modifications	Critical	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> McAfee Sidewinder: Attack detection	Critical	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> McAfee Sidewinder: Hardware/Software failure	Critical	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> McAfee VirusScan Enterprise: Update failed	Serious	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> MExchange: ADC service stopped	Critical	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> MExchange: Database maximum size is reached	Critical	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> MExchange: IS service cannot be started	Critical	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> MExchange: Log disk is full	Serious	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> MExchange: Server cannot handle influx of mail	Serious	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> MExchange: Unable to start Microsoft Exchange Server	Critical	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> My Alert	Critical	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Netscreen: Authentication failure	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Netscreen: IDS intrusion detection	Serious	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

EventTracker Server Time: 08/10 07:01:00 PM Response: 0.31 secs © Copyright 1999 - 2010 Prism Microsystems, Inc.

Figure 3

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.