Upgrade Guide

Upgrading to EventTracker v7.1 Enterprise

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.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

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. 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 v7.1 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
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. 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.

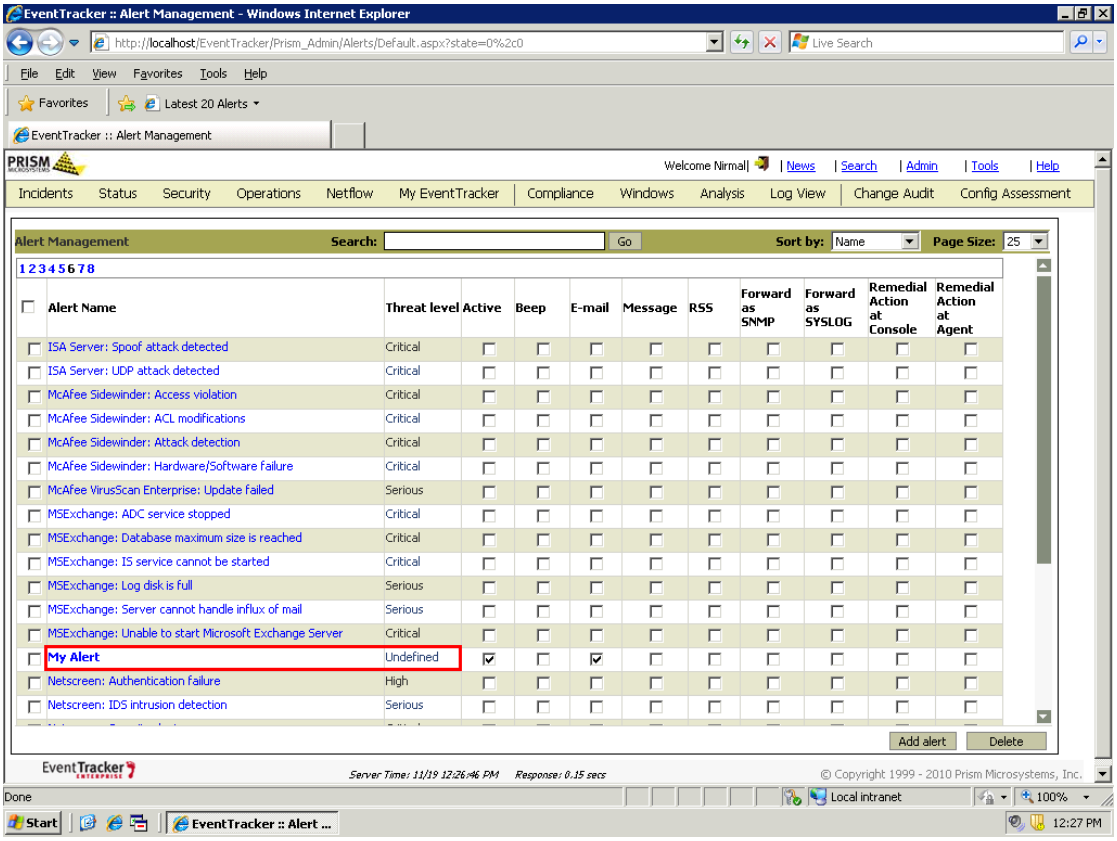

Figure 1

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

EventTracker displays the Alert configuration page.

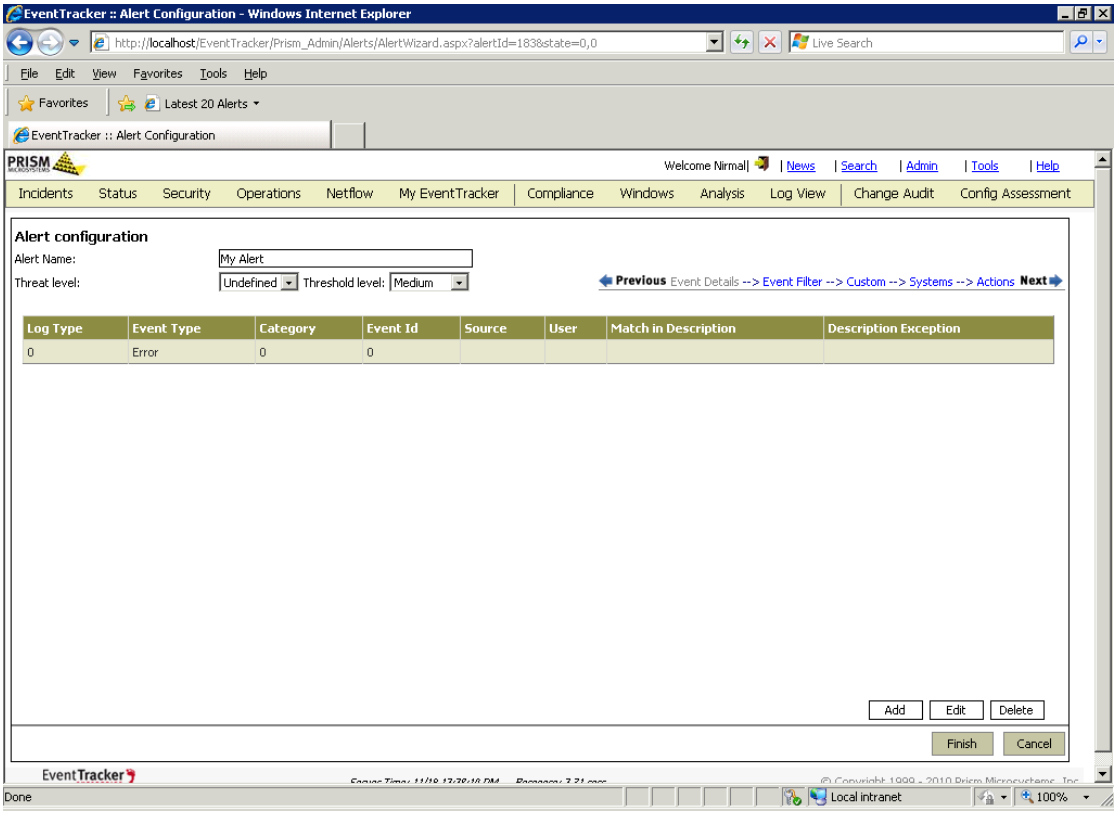

Figure 2

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

   EventTracker saves the configuration settings.

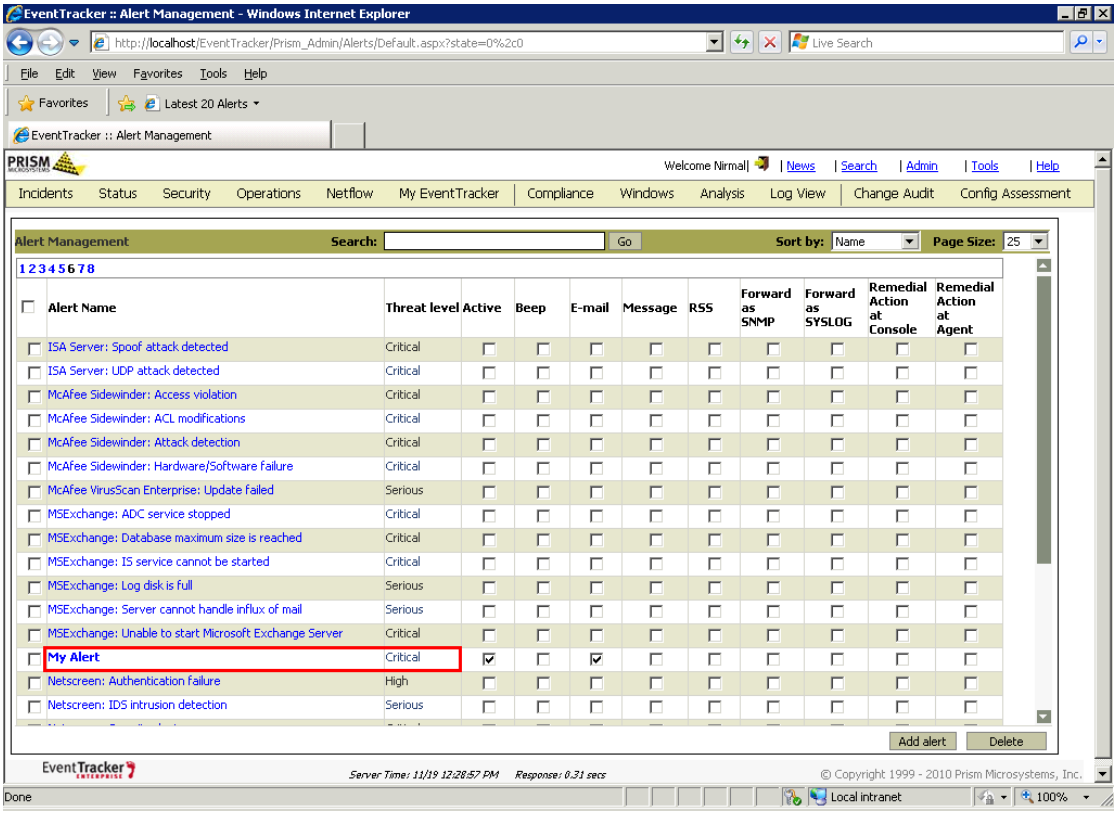
EventTracker :: Alert Management - Windows Internet Explorer
http://localhost/EventTracker/Prism_Admin/Alerts/Default.aspx?state=0%2c0
File Edit View Favorites Tools Help
Favorites
Latest 20 Alerts
EventTracker :: Alert Management
PRISM
Welcome Nirmal | News | Search | Admin | Tools | Help
Incidents Status Security Operations Netflow My EventTracker Compliance Windows Analysis Log View Change Audit Config Assessment
Alert Management
Search:
Go
Sort by: Name
Page Size: 25
1 2 3 4 5 6 7 8
Alert Name
Threat level
Active
Beep
E-mail
Message
RSS
Forward as SNMP
Forward as SYSLOG
Remedial Action at Console
Remedial Action at Agent
ISA Server: Spoof attack detected Critical
ISA Server: UDP attack detected Critical
McAfee Sidewinder: Access violation Critical
McAfee Sidewinder: ACL modifications Critical
McAfee Sidewinder: Attack detection Critical
McAfee Sidewinder: Hardware/Software failure Critical
McAfee VirusScan Enterprise: Update failed Serious
MSExchange: ADC service stopped Critical
MSExchange: Database maximum size is reached Critical
MSExchange: IS service cannot be started Critical
MSExchange: Log disk is full Serious
MSExchange: Server cannot handle influx of mail Serious
MSExchange: Unable to start Microsoft Exchange Server Critical
My Alert Critical
Netscreen: Authentication failure High
Netscreen: IDS intrusion detection Serious
Add alert
Delete
EventTracker
Server Time: 11/19 12:28:57 PM
Response: 0.31 secs
© Copyright 1999 - 2010 Prism Microsystems, Inc.
Done
Local intranet
100%

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.