EventTracker
Secure. Comply. Succeed.

Feature List

EventTracker v7.6

Publication Date: Sep 15, 2014

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

Abstract

This document gives a brief overview regarding the features that are newly introduced in EventTracker Enterprise v7.6 version.

Target Audience

EventTracker users who wish to know about the new features added in EventTracker Enterprise v7.6 version.

Table of Contents

Major improvements in v7.6

- Smart search (targets IOT)
- Support for Azure Storage Analytics Log Format
- Improved dashboard features (parameterized dashlet support)
- Log Watch feature (option provided in Advanced search)
- Amazon AWS integration items
  - Support for JSON format (AWS CloudTrail)
  - Support for SMTP server via AWS SES (START TLS)
- Collection Master improvements for MSP and Cloud
  - Multiple ports can be configured to collect data from collection points
  - Centralized dashboard of all sites on collection master
  - Centralized Event-o-Meter for all sites on collection master
  - Centralized view of Behavior data for all sites on collection master
  - Full white label support
  - Customized branding per user
- Upgraded to .NET 4.0 using VS 2012, Crystal reports V13
- Support for Server 2012 R2 Server Core
- Main menu changes, new rotate options
- Simplified installation process
- Knowledge Packs - http://www.eventtracker.com/knowledge-center/
  - Centrify
  - LOGbinder SQL
  - TrendMicro
  - Symantec End Point Protection
  - Cisco Identity Services Engine
  - Websense WSG
  - Sonicwall UTM
  - Clavister Security Gateway
  - Cisco IronPort ESA and WSA
  - Fortigate OS 5
  - Windows 8.1 and 2012 R2

Minor improvements

- Support for multiple VMware or Checkpoint sources in LFM
- Version number included for categories and alerts
- DLA now includes
  - Multiline support
  - JSON format log files
  - Starting line offset
  - Custom separator
  - Disable event generation - Option in Direct Log Archiver to individually disable the generation of each event
- Remove dependency on .cer files while installing agent
- SNMP v3 support in TrapTracker and forward alert action
- Log search improvements
  - Support for regular expression
  - Log search option to search for 'Event Id does not contain'
- Behavior engine can suppress correlation check for custom rules
- Specify different VCP ports for real-time and file-transfer events from the same agent
- Enable/disable events from Change Audit
- Custom duration selection in Behavior
- Optimization of EventTracker Backup, Traffic Analyzer, Diagnostics
- Run Now for a longer period will produce a single report
- Purging settings per VCP
- Purging settings for individual CPs at a CM
- Agent to Manager Apply config requests where agent periodically connects to EventTracker Manager and fetches pending Apply config requests
- GED cache space configurable in both % as well as MB
- Updated Categories

- Cisco PIX: User login failed
- Cisco PIX: User account locked out
- Cisco Switch: User login failed
- Syslog: Object access failed
- Syslog: Object creation failed
- Syslog: Object deletion failure
- Syslog: Object modification failure
- *Security: User account unlocked

❖ Alerts

- Cisco ASA: System password changed
- Cisco ASA: User account locked out
- Cisco ASA: User login failed
- Cisco PIX: User account locked out
- Cisco PIX: User login failed
- Cisco Switch: User login failed
- Syslog: Object access failed
- Syslog: Object creation failed
- Syslog: Object deletion failure
- Syslog: Object modification failure
- *Security: User account unlocked

❖ Flex Reports

- Windows-AD object access detail report
- EventTracker-New enterprise activity report
- EventTracker-Out of ordinary activity report

❖ Export of incident dashboard possibly with graph

❖ Customized image display for each login user

❖ User preference - providing user based customization

❖ Launching of log search while adding a constraint in KO.

❖ Category and alert versioning

❖ New license options - To control number of CheckPoint and Vmware sources

❖ Juniper OS

❖ Import/Export functionality

❖ Edit expression functionality

- Write audit log after database actions such as insert/update/delete of knowledge objects
- Updated the product banner and splash screen.
- Added SMTP STARTTLS (Explicit TLS) support in mail client.