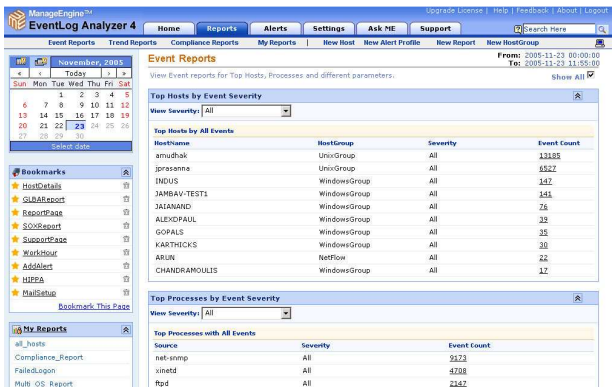
Centralized Event Log Management

Event log management is an important need in almost all enterprises. Logs need to be archived for the purpose of network auditing and more recently to comply with various regulations such as HIPAA, GLBA, PCI and Sarbanes-Oxley. Apart from this, system administrators look at event logs as a critical source to troubleshoot performance problems on hosts across the network. The need for a complete event log management solution is often underestimated; leading to long hours spent sifting through tons of syslog messages to troubleshoot a single problem. Efficient event log analysis reduces system downtime, increases network performance, and helps tighten security policies in the enterprise.

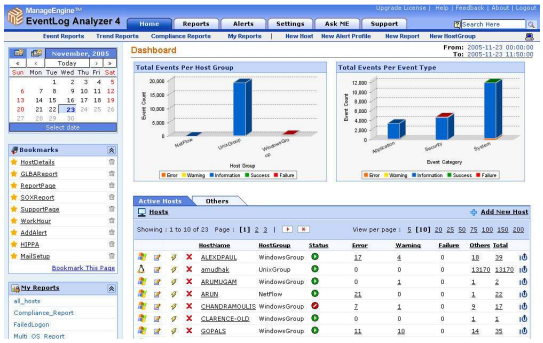
ManageEngine® EventLog Analyzer is a web-based, real-time event management solution that collects, analyzes, and reports on event logs from distributed Windows and UNIX hosts, Cisco Routers and Switches, and other Syslog devices. EventLog Analyzer uses a built-in MySQL database for reporting, and archives all event logs collected, at periodic intervals. With advanced data filtering and log management, EventLog Analyzer helps administrators manage and report on event logs across the enterprise, in a simple and effective manner.



Event-based reports show you at one glance, which hosts have generated maximum important events

Key Features

- Centralized event management
- Real time monitoring
- Comprehensive set of pre-defined reports
- Customizable report profiles
- Scheduled event reporting
- Compliance reporting to meet GLBA, HIPAA, PCI, and SOX acts
- Historical trending
- Advanced filtering & data management
- Real time alerting & notification



The Dashboard shows you all the information you need to see at one place

How can EventLog Analyzer help you?

- Zero in on applications causing performance and security problems
- Determine unauthorized access attempts and other policy violations
- Identify trends in user activity, server activity, peak usage times, etc.
- Understand security risks in your network
- Monitor critical servers exclusively and set alerts
- Understand server and network activity in real-time
- Alert on hosts generating large amounts of log events indicating potential virus activity
- Identify applications and system hardware that may not be functioning optimally

Features & Benefits

Comprehensive Event Collection – collects application, system, and security event data from enterprise-wide Windows and UNIX systems, Cisco Routers and Switches, and other Syslog devices.. Automatically stores them all in a centralized event database.

Real-time Alerting & Automatic Notification – automatic alerting allows you to set the specific criteria on hosts for which you need to be notified.

Trending – view trends of events based on event severity, and event type. Trends on alerts triggered are also available.

Compliance Reporting – generate pre-defined reports to meet HIPAA, GLBA, PCI, and Sarbanes-Oxley compliance requirements.

Pre-defined Event Reports – comprehensive reports include top reports on events generated across hosts, users, processes, and host groups, apart from top events by count.

Instant Reports – generate reports in real-time and get instant access into last events generated. View last ten events generated, for any host from which event logs are collected.

Powerful Multi-level Filters and Drill-down – define event filter to specify criteria such as event type, severity, etc. in reports. Drill down from event reports to see specific event details about a host or a group.

Security Analysis – identify unauthorized and failed logins, and malicious user(s). Set alerts for suspicious hosts, and monitor events exclusively.

Host Grouping – group hosts together based on your business needs, generate event reports, and analyze trend patterns exclusively.

Anytime, Anywhere Access & Management – generate reports and set up archiving from just a web browser.

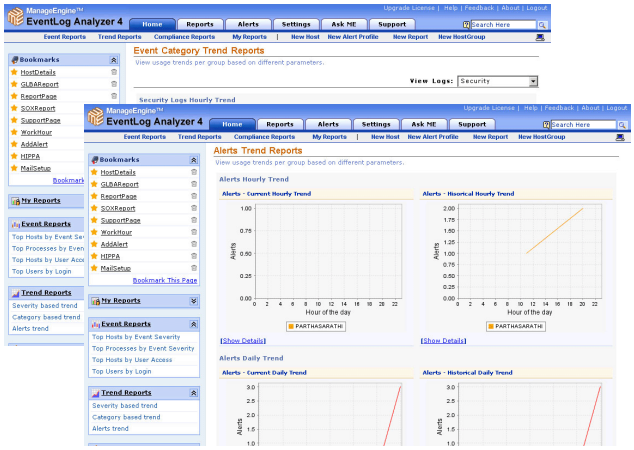
Built-in Database –integrated MySQL database is already configured to store all log data. No external database configurations are needed.

Host OS Support – Can be installed and run on Windows and Linux systems making it suitable for deployment in a wide range of enterprises.

Customizable Reports – build custom reports with event filters and report format options tailored to meet your specific needs.

Report Scheduling – automatically generate reports at specified time intervals and get them delivered via e-mail.

Multiple Report Export Formats – generate and view reports in HTML, PDF, and CSV formats.



Trend reports show you event patterns across hosts for various event types and event severity parameters.

Supported Operating Systems

EventLog Analyzer can collect and report on event logs from the following operating systems and devices:

- Windows NT/2000/2003/XP
- Linux - RedHat, Debian
- UNIX – Solaris, HP-UX
- Cisco Switches and Routers
- SNORT for Windows
- And, Other Syslog devices

For more information

Website: www.eventloganalyzer.com

Email : support@eventloganalyzer.com

Phone : +1 888 720 9500

Hardware Requirements: Pentium 4, 1GHz, 512MB RAM, 1GB disk space for the product, monitor that supports 1024x768 resolution.
Platform Requirements: Windows 2000/2003/XP, or RedHat Linux 8.0/9.0