



Features & Benefits

**Distributed Edition**

Monitor hosts distributed around the globe and manage them from a central location with centralized log archive. Massive Scalability achieved with distributed monitoring. Suitable for NOCs, MSP/MSSPs and Large Enterprises

**Comprehensive Event Collection** – collects application, system and security event data from enterprise wide Windows and Unix/Linux systems, applications, databases, Routers, Switches and other Syslog devices. Normalizes, filters and stores them all in a centralized event database for analysis.

**Optional Remote Agent** – by default EventLog Analyzer collects logs without agent from the sources. Optionally, it can collect the logs using remote agent.

**Internal Security Analysis** – identifies unauthorized and failed logins, and rogue user(s). Set alerts for suspicious hosts, and monitor events exclusively.

**Pre-built & Instant Reports in Multiple Formats** – comprehensive reports include top reports on events generated across hosts, users, processes, and host groups, apart from top events by count. Generate and view reports in HTML, PDF, and CSV formats.

**Compliance Reporting** – generate pre-defined and custom reports for Event logs & Syslogs, to meet HIPAA, GLBA, PCI and SOX compliance act requirements.

**PUMA Reports** – generate reports exclusively to monitor users in particular Privileged User to mitigate internal threats.

**Schedule and Distribute Reports** – automatically generate reports at specified time intervals and get them delivered via Email.

**Trend Reports** – view trends of events based on event severity and event type. Trends on alerts triggered are also available.

**Real-time Alerting & Notification** – automatic alerting allows you to set the specific criteria on hosts for which you need to be notified through Email, SMS or Program execution.

**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.

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

**User Authentication with External Applications** – allows you to use Active Directory and RADIUS server based authentication and also default local user authentication

**Secured Archive** – archive log storage is encrypted to secure the contents and hashed, time-stamped to make it tamper-proof.

**Anytime, Anywhere Access and Management** – monitor hosts, generate reports and set up archive from just a web browser.

**Bundled Database** – MySQL database is pre-configured and bundled to store all log data. Additionally, MS SQL database supported.

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



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

**Supported Hosts and Applications**

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

- Windows® NT, 2000, XP, Vista, 7 & Windows® Server 2000, 2003 & 2008
- Linux - RedHat, Debian,
- UNIX - Solaris, HP-UX
- IBM AS/400, Switches and Routers - Cisco
- VMWare - Syslog versions
- SNARE for Windows & any Syslog supported device
- Microsoft IIS W3C Web, FTP Servers
- Windows, Linux DHCP Servers
- Microsoft SQL Server & Oracle - Audit Logs

**For more information**

Website: [www.eventloganalyzer.com](http://www.eventloganalyzer.com)  
 Email: [eventlog-support@manageengine.com](mailto:eventlog-support@manageengine.com)  
 Phone: +1 888 720 9500