ManageEngine
EventLog Analyzer

EventLog Analyzer
Solution Document

www.eventloganalyzer.com

Table of Contents

Purpose of this document

The purpose of this document is to illustrate the capabilities of ManageEngine EventLog Analyzer and how it helps in automating log management, mitigating internal and external security threats, and protecting the network from data breaches. Also, this document explains how EventLog Analyzer's distributed edition caters to the log management and network security needs of organizations spanning across multiple locations.

This solution

- Monitors security events across physical, virtual, and cloud environments.
- Supports 700+ log sources from 40+ vendors.
- Correlates logs to help notice patterns and foresee security threats.
- Continuously receives global threat feeds from STIX/TAXII servers and checks organizations' networks for malicious IPs and URLs.
- Eases the job of security administrators by providing 1000+ predefined meticulously drafted reports and alert criteria for Windows, applications, network devices, and other Syslog infrastructure, that help in identifying anomalous user behavior.

A brief overview of what EventLog Analyzer does

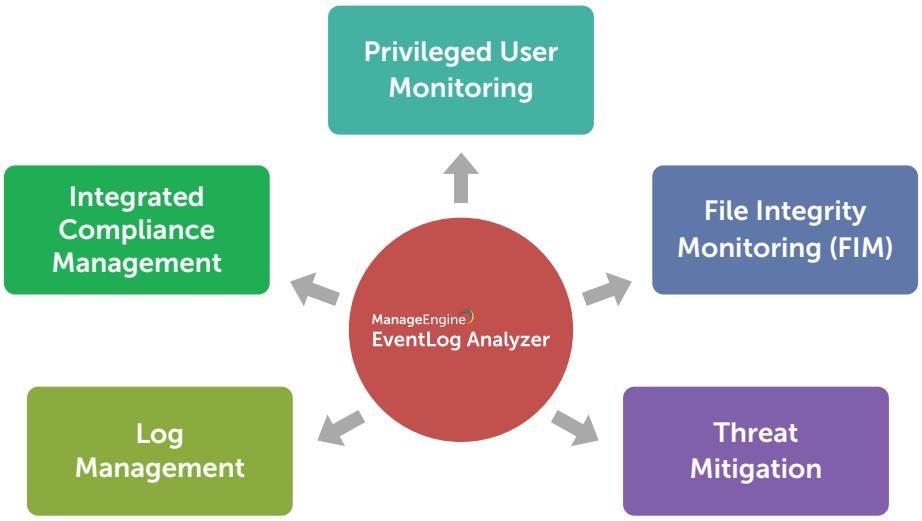


Fig.1 EventLog Analyzer – An overview

EventLog Analyzer as stated before is a comprehensive log management solution that helps in

- ***Managing log data*** across the entire network.
- ***Complying with strict regulatory mandates*** such as PCI DSS, FISMA, HIPAA, the GDPR and more.
- ***Mitigating internal and external security threats*** and data breaches.
- Monitoring and ***auditing privileged user activities.***
- ***Protecting confidential data*** by monitoring critical files/folders.
- ***Conducting root cause and forensic analysis*** to backtrack the attacks.

This solution also comes in a distributed edition which helps in monitoring, managing log data, and ensuring network security for organizations spanning across multiple locations.

The features EventLog Analyzer offers are

- **Log Management** – Centrally collect, normalize, analyze, correlate, and archive log data from sources across the network
- **Integrated Compliance Management** – Various predefined reports and alerts that help meet many major compliance regulatory requirements.
- **Privileged User Monitoring** – Monitor and audit all privileged user activities and get detailed reports that help track privileged user activities.
- **File Integrity Monitoring (FIM)** – Protect confidential and sensitive files by monitoring the critical activities happening on the files/folders.
- **Threat Mitigation** – Mitigate both internal and external security threats by monitoring user activities, preventing network intrusions, and detecting network anomalies and suspicious network behavior.
- **Threat Intelligence** – Ensure no malicious IP or URL tries to establish connection by continuously receiving the latest updates from STIX/TAXII threat feeds.

EventLog Analyzer - Distributed Edition

To cater to the IT security needs of MSSPs and enterprises that span across multiple locations, we offer EventLog Analyzer distributed edition. This edition supports centralized log monitoring and provides single console view of log and security data.

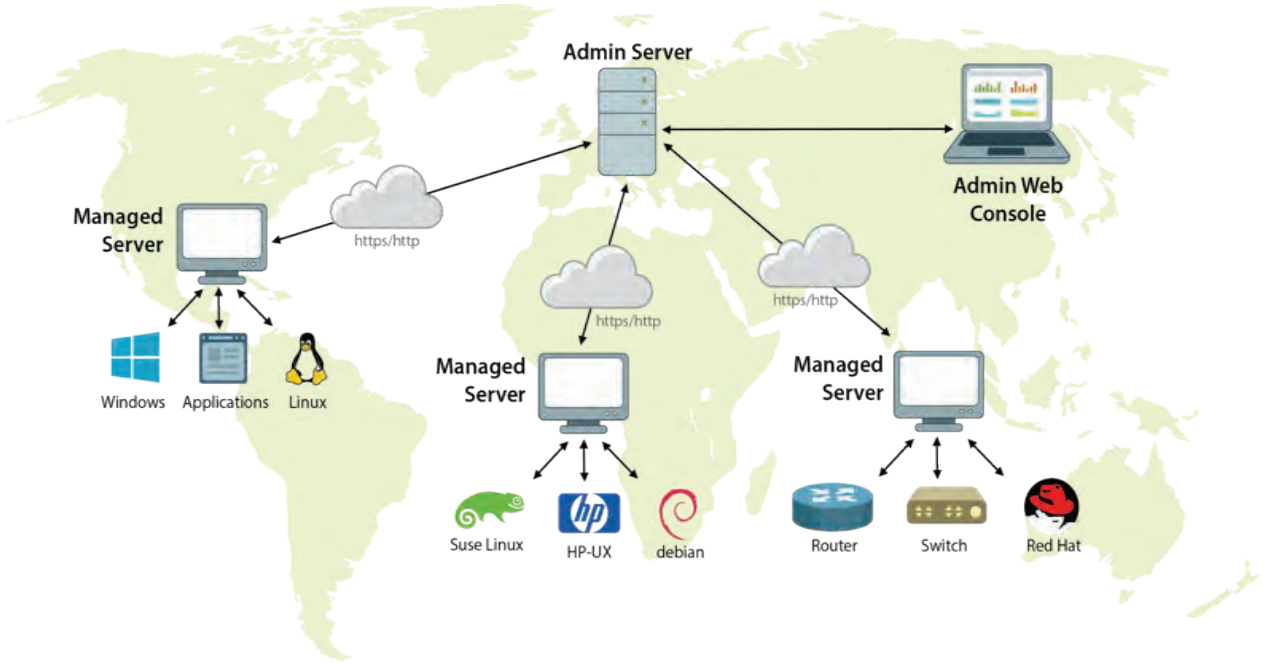


Fig.2 EventLog Analyzer Distributed Edition Architecture

EventLog Analyzer's distributed edition supports deployment of one admin server and many managed servers. The managed servers can be installed at different locations (one per LAN environment) and these can be connected to the central admin server. The admin server helps in aggregating information from all the managed servers and it acts as a single central console displaying the reports, alerts, and other log source information of all the managed servers that are installed.

Highlights

- The distributed edition aggregates and provides a single console view of the log data across multiple locations.
- It provides a scalable architecture supporting up to 20,000 log sources.
- Provides secured and sleek communication using HTTPS.
- Caters to the exclusive needs of MSSPs.

Log Management

Fig.3 Log management process

Log Collection

EventLog Analyzer aggregates logs from heterogeneous log sources such as Windows systems, Unix/Linux systems, applications, databases, firewalls, routers, switches, and IDS/IPS at a central location.

The solution offers both agentless and agent-based log collection mechanisms to meet the diverse requirements of enterprises. It supports universal log collection with its custom log parsing technology, which enables security administrators to decipher and analyze any log data regardless of its source and format. The solution also supports secure log collection by using the TCP protocol.

Highlights

- Supports ***agentless and agent-based log collection.***
- Collects log data in a ***central location.***
- Supports ***universal log collection.***
- Parses any log data format using ***custom log parsing*** technology.
- ***Secure TLS*** based log collection.

Log Analysis

EventLog Analyzer has the capability to normalize and analyze the log data from network devices, systems, applications, and other Syslog devices in real-time and extract meaningful information from them. The following components of the solution facilitate easy and seamless log analysis.

Intuitive dashboards: Actionable security information is presented in the form of graphs and charts. Security administrators can quickly drill down through logs and perform a root cause analysis to identify why and how an incident occurred.

Reporting console: The solution has 1000+ predefined reports that are meticulously drafted and categorized to meet security, compliance, and operational needs. These out-of-the-box reports span across Windows, network devices, applications, Syslog devices, Unix/Linux, and virtual infrastructure. EventLog Analyzer's simple and easy-to-use report builder allows you to build custom reports quickly.

Real-time alerts: Upon the occurrence of any suspicious user behavior, network anomaly, possible attack or attempted data breach, EventLog Analyzer alerts security administrators instantly over email or SMS.

Highlights

- Facilitates ***in-depth log analysis*** via intuitive graphs and dashboard.
- Includes ***1000+ predefined reports*** and ***alert criteria*** to meet security, compliance, and operational needs.
- Sends out ***real-time email or SMS alerts*** upon the detection of anomalous activity or suspicious behavior.

Log Correlation

EventLog Analyzer has a powerful correlation engine that helps security administrators detect security attack attempts as early as possible. It includes predefined correlation rules to detect the most commonly encountered threats. It also has a correlation rule builder with which you can effortlessly build your own rules based on your enterprise's needs.

Security administrators will be notified in real-time upon any threshold violation or network anomaly by an SMS or email. The 30+ predefined correlation rules include the most common and dangerous types of threats, such as installation of a malicious software or service, mining of cryptocurreny, ransomware or worm activity, and brute force attacks.

Highlights

- Includes ***30+ predefined correlation*** rules that help to mitigate security attacks and breaches.
- Early detection of harmful activities such as cryptocurrency mining, ransomware or worm activity, and brute force attacks.
- Provides ***custom rule builder*** that helps to create attack patterns.

Log Search

EventLog Analyzer makes forensic investigation very easy with its powerful log search functionality. This solution provides security administrators an easy-to-use log search interface that allows them to build complex search queries within seconds.

EventLog Analyzer supports various search options including group, range, Boolean, and wild card search. It has the capability to generate forensic reports based on the search results as well.

Highlights

- Powerful yet easy to use search engine.
- Provides various search options including ***Boolean search, range search, wild card search, and group search.***
- Gives option to ***save the search result*** in the form of reports and alert profiles.

Log Archival

EventLog Analyzer retains all log data that are being collected in a centralized repository for a flexible period of time. Security administrators can load the archived log data back to the database at any time to conduct forensic investigations.

The flexible log retention period provided by this solution helps meet stringent compliance requirements and other internal security policies. The log data are archived in a secure fashion using encryption, time stamping, and hashing techniques to ensure that they are tamper-proof.

Highlights

- Flexibility to ***store log data for custom time period.***
- ***Provides secure log archiving*** option using time stamping, hashing, and encryption techniques.
- Provides an option to load archived log data back to the database to ***conduct forensic analysis.***

Integrated Compliance Management

With EventLog Analyzer's integrated compliance management system, security administrators can seamlessly meet the regulatory compliance requirements. The solution provides premade reports for various regulatory mandates such as PCI DSS, FISMA, GLBA, SOX, HIPAA, ISO 27001, GPG13, the GDPR and more.

Further, this solution also allows security administrators to modify the existing compliance reports to meet their internal security policies. It provides the flexibility to create new compliance reports to meet the growing demand of compliance requirement.

To meet a basic requirement of almost every compliance mandate, the solution also supports flexible log retention period. This also helps in conducting forensic analysis on the archived log data at ease.

Highlights

- Provides ***out-of-the-box reports*** to meet the stringent compliance requirements.
- Provides an option to ***modify the existing compliance reports*** to suit the requirements of internal security policies.
- Includes an option to ***build new compliance report*** to meet the demanding growth of compliance requirements.

Privileged User Monitoring

EventLog Analyzer monitors all user activities and comes up with exhaustive reports with a complete user audit trail. The solution also generates privileged user monitoring and auditing (PUMA) reports to track the activities of privileged users.

With EventLog Analyzer, security administrators can now get precise information on critical events such as user logons, user logoffs, failed logons, successful audit logs cleared, audit policy changes performed by the users, objects accessed, user account changes, and more.

This solution also provides predefined reports that make user session monitoring easier than ever. All these reports can also be exported in PDF and HTML formats.

Highlights

- ***Monitors and tracks user activities*** across network.
- Provides detailed reports on ***logons, logoff, logon failures, object access, and more.***
- Provides comprehensive ***user session monitoring*** reports.

File Integrity Monitoring

EventLog Analyzer helps to protect confidential and sensitive data of organizations with its real-time file integrity monitoring (FIM) capability. With this feature, security professionals can now centrally track all the critical changes happening to files and folders, such as file and folder creation, deletion, modification, rename, and access.

The exhaustive file integrity monitoring reports provide detailed audit trail information. For example, when a critical change had happened, who performed it, and from where. This critical information helps administrators make quick decisions to mitigate the risk of data breaches.

This solution also sends out real-time email or SMS notification to security administrators whenever a critical change on a confidential data happens.

Highlights

- ***Monitors and tracks critical file and folder changes*** such as file/folder creation, deletion, modification, and rename.
- Provides exhaustive information such as ***who made the change, when it was changed, and from where.***
- Sends out ***real-time email or SMS alerts*** whenever there's change to confidential data.

Threat Mitigation

EventLog Analyzer helps to mitigate both internal and external security threats. It provides detailed privileged user activity monitoring and user overview reports that give complete user audit trail. These reports help in identifying any suspicious user behavior and unauthorized user accesses to mitigate internal security threats.

This solution also supports analysis of log data from various security applications such as vulnerability scanners, threat intelligence solutions, and DLP applications to provide a comprehensive view of security data across the network, which helps in detecting any threat in the network at the earliest.

Further, the solution monitors activities at the perimeter network devices such as firewalls, routers, switches, and IDS/IPS to identify network intrusions in real time and hence helps in proactively mitigating data breaches and security attacks.

Highlights

- Provides detailed ***user activity reports*** that help in combating internal security threats.
- Provides ***single console view of all security data*** that facilitates quick decisions in mitigating external security attacks.
- Prevents network intrusions ***by continuously monitoring perimeter network devices.***

Threat intelligence

EventLog Analyzer's threat intelligence helps you detect attacks at the first sign of trouble by analyzing and correlating a global blacklist of IPs, URLs, and domain names. That way, you can prevent any compromise of network security quickly and efficiently. Receive instant alerts when intrusions occur and discover IPs that are known to be malicious so you can avoid false alarms. The solution tracks data from multiple open source threat feeds, including those based on the STIX/TAXII protocols, a global standard for threat information. Organizations can also configure EventLog Analyzer with their own STIX/TAXII servers.

Highlights

- Integrates with all major open source feeds, ***including STIX/TAXII feeds.***
- Feeds cover ***more than 600 million*** malicious IPs, URLs, and domain names.
- ***Real-time alerts*** when suspicious entity interacts with your network.
- Built-in alert profile with ***no separate configurations*** required.
- Feeds ***updated dynamically*** every 24 hours.

Incident management console

EventLog Analyzer allows you to handle incidents efficiently by automatically assigning tickets to your technicians or administrators as soon as alerts are triggered. Assign tickets to technicians and administrators to create accountability in your security operations center and track the progress of all incoming incidents. In addition to being able to raise tickets within the EventLog Analyzer console itself, you can also integrate EventLog Analyzer with external help desk softwares—ServiceNow, ManageEngine ServiceDesk Plus, Jira Service Desk, Zendesk, Kayako, and BMC Remedy Service Desk—to automatically create a ticket and assign it to the appropriate security admin when an alert is triggered. This real-time alerting system and streamlined incident management mechanism allows you to view and handle security incidents with our SIEM portfolio, helping you efficiently mitigate security attacks.

Highlights

- ***Built-in*** incident management console.
- Assign tickets and ***track details*** such as status and priority.
- ***Automatically assign*** tickets based on customizable criteria.
- ***Forward tickets*** to external ticket systems – ServiceNow, ManageEngine ServiceDesk Plus, Jira Service Desk, Zendesk, Kayako, and BMC Remedy Service Desk.

A typical use case scenario

Every organization has definite working hours and non-working hours. Activities such as failed logons during non-working hours should attract the attention of security administrators to probe the event, and check whether it is an anomaly or not.

Identifying a network intrusion at its early stage largely depends on determining whether an access or logon activity is authorized or not. This use case elaborates how EventLog Analyzer helps security administrators in ascertaining an attempted access as an unauthorized one by analyzing the reasons for logon failures.

There could be many reasons for logon failures. To validate the event as an anomaly or not, it is necessary for a security administrator to know the reason for the logon failure and other details such as the user who tried to logon.

EventLog Analyzer comes in handy to security administrators right here. It helps in validating logon failure event with its detailed reports. This would be the first step of investigation when it comes to the internal security threat and EventLog Analyzer makes detection as easy as pie.

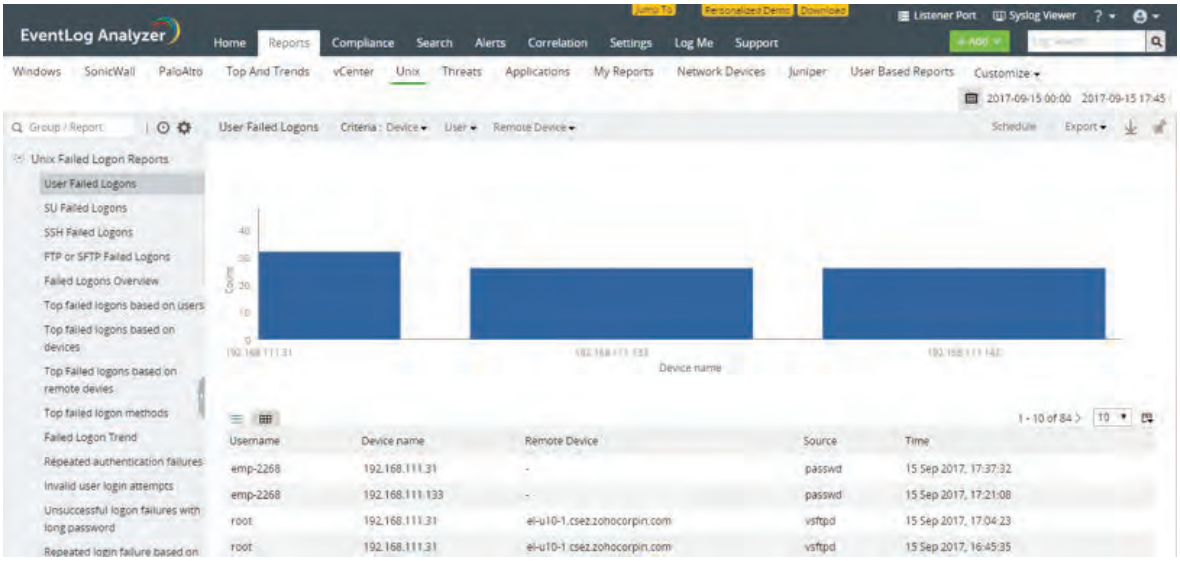


Fig.4 Screenshot for logon failure report

Why should you choose EventLog Analyzer?

- **The features EventLog Analyzer offers are**
  - Rapidly transforms *machine generated logs into actionable information.*
  - Has high log processing rate of *20,000 Syslog/second and 2,000 event logs/second.*
  - Supports both *agent-less and agent based log collection* mechanisms.
  - Includes *intuitive graphical dashboards and reports* that help to analyze the log data better.
  - Provides the *flexibility to customize reports* to meet the demanding needs of compliance regulations.

- **Supports distributed (multiple site) environments**
  - Scales up to *20,000 devices.*
  - *Unified single console view* to monitor log sources deployed across multiple locations even deployed across the globe.
  - *Sleek communication* between managed and admin servers to ensure minimal bandwidth usage.

- **Comprehensive security suite**
  - *Mitigates internal and external security threats* with powerful log analysis feature.
  - *Includes 1000+ predefined reports and alert criteria* to meet the security, compliance, and operational needs.
  - *Powerful* yet easy to use *log search engine.*
  - Provides *instant email and SMS alerts* upon occurrence of network anomalies.

- **Attractive TCO and Rapid ROI**
  - No additional hardware required.
  - Minimal IT overhead.
  - Easy deployment and smooth learning curve

System Requirements

This section lists the minimum system requirements for installing and working with EventLog Analyzer.

Hardware Requirements

For 32 bit machines

1 GHz, 32-bit (x86) Pentium Dual Core processor or equivalent

4GB RAM

5 GB Hard disk space for the product

For 64 bit machines

2.80 GHz, 64-bit (x64) Xeon® LV dual core processor or equivalent.

4GB RAM

5 GB Hard disk space for the product

EventLog Analyzer is optimized for 1024x768 monitor resolution and above.

Supported Web Browsers

EventLog Analyzer has been tested to support the following browsers and versions:

Internet Explorer 8 and later

Firefox 4 and later

Chrome 8 and later

Operating System Requirements

EventLog Analyzer can be installed and run on the following operating systems

(both 32 Bit and 64 Bit architecture) and versions:

Windows®	Linux	VMware
Windows 2008 Server and above. Windows 7 and above.	Linux - RedHat RHEL Linux - Mandrake Linux - Mandriva Linux - SuSE Linux - Fedora Linux - CentOS Linux - Ubuntu Linux - Debian	VMware environment

Supported Logs and Data Sources

EventLog Analyzer can collect, index, analyze, archive, search and report on logs from over hundreds of devices, platforms and services. To know the latest supported logs and data sources visit http://manageengine.com/eventlog/supported-data-sources.html

Note:

- With its custom log parsing technology, EventLog Analyzer can support any log and data source that is in human-readable format.
- Syslogs received from SNARE agents for Windows will be displayed as Windows devices.

Supported Databases

Bundled with the product

PostgreSQL

External Databases

MS SQL 2005 and above

Hardware Requirements

The hardware requirements for an EventLog Analyzer server installation depend on two factors:

- The volume of logs
- The type of logs generated by the log sources in your network

When you know the above two criteria, you can easily estimate your requirements such as the number of physical CPU cores, RAM, disk space, network card capacity, and the CPU architecture.

Minimum Requirements

- A dual core processor.
- 4 GB RAM.

Note: The number of processor cores determines the indexing and search performance of the installation. More the number of cores, better the performance of the tool.

Calculating your log flow rate:

Log flow rate is the number of logs EventLog Analyzer can parse in a second. Generally, EventLog Analyzer can parse up to 20,000 syslogs in a second but this number can vary according to the size and type of the log.

To help you calculate the approximate number of Events Per Second (EPS) we have formulated a value called the "Normalization Factor".

Table 1: Normalization factor for different log formats

Type	Log Sources	Normalization Factor
Type 1 Syslogs (150 bytes)	HP, pfSense, Linux, H3C	1
Type 2 Syslogs (300 bytes)	Cisco, Sonicwall, Huawei, Juniper, Netscreen, Meraki	2
Type 3 Syslogs (600 bytes)	Barracuda, Palo Alto, Sophos, f5, Firepower, Fortinet, Checkpoint	4
Type 4 Windows logs (900 bytes)	Windows Event Logs	6

Based on the normalization factor from above table, calculate your log flow rate with the formula:

Log flow rate = number of incoming logs x normalization factor

Scenario 1

If you have a Cisco firewall that generates 1000 logs in a second, your log flow rate will be

1000 x 2 = 2000

Scenario 2

If you have a Windows workstation, an F5 switch, and a Meraki firewall that generate 1000, 2000 and 500 logs per second respectively.

Your log flow rate will be 1000 x 6 + 2000 x 4 + 500 x 2

6000 + 8000+ 1000 = 15,000.

Planning your architecture with fault tolerance:

If the log flow rate is 15,000, then it is essential to plan your resources for an **additional 25% flow** to handle the peak performance. The log flow rate that you should plan for is 15,000 + 3,750 (3,750 is 25% of 15,000) = 18,750. This is because, if the solution stops due to mishaps, the logs collected during the downtime will be parsed and processed once it's up. This will cause the solution to handle more log flow than the actual scenario. Therefore, it's always advisable to have an additional log flow as a buffer. If your resources are insufficient to handle this additional flow of logs, your systems could slow down as a result of this.

Table 2: Suggested hardware requirements based on log flow rate

	Log Flow Rate of 2000 or less	Log Flow Rate of 2000 to 10,000	Log Flow Rate of 10,000 to 15,000	Log Flow Rate of 15,000 to 20,000
Physical CPU cores	2	8	12	16
RAM	4 GB+	8 GB+	12 GB+	16 GB+
Disk Throughput*	6 MB/s	20 MB/s	28 MB/s	38 MB/s
Disk space	300 GB	1.5 TB	2.3 TB	3 TB
Network card capacity	1 Gb/s	1 Gb/s	6 Gb/s	10 Gb/s
CPU architecture	32/64 bit	64 bit	64 bit	64 bit

If the log flow rate is **above 20,000,** it the distributed edition of EventLog Analyzer is recommended.

Please contact eventlogsupport@manageengine.com and upgrade to Distributed Edition.

**Disk throughput refers to the speed (megabytes/second) at which EventLog Analyzer writes on the disk without impacting the performance.*

Please note that the above values are just approximates that are provided to help your planning.

Prerequisites

Prerequisites applicable for EventLog Analyzer

Before starting EventLog Analyzer in your environment, ensure that the following are taken care of.

- What are the ports required for EventLog Analyzer?
- How to change the default ports used by EventLog Analyzer

What are the ports required for EventLog Analyzer?

EventLog Analyzer requires the following ports to be free for web server, syslog, and PostgreSQL/MySQL:

Port Numbers	Ports Usage	Description
8400 (TCP)	Web server port	This is the default web server port used by EventLog Analyzer. This port is used for connecting to EventLog Analyzer using a web browser. You can change this port during installation.
513, 514 (UDP)	Syslog listener port	These are the default Syslog listener ports for UDP. Ensure that devices are configured to send Syslogs to any one of these ports.
514 (TCP)	Syslog listener port	This is the default Syslog listener port for TCP. Ensure that devices are configured to send Syslogs to this port.
33335 (TCP)	PostgreSQL/MySQL database port	This is the port used for connecting to the PostgreSQL/MySQL database in EventLog Analyzer.

EventLog Analyzer uses the following ports for WMI, RPC, and DCOM:

Port Numbers	Ports Usage	Description
135, 445, 139 (TCP)	WMI, DCOM, RPC - Incoming traffic ports	Incoming Traffic Ports - Windows services DCOM, WMI, RPC uses these ports and EventLog Analyzer in turn uses these services to collect logs from Windows machines in default mode (Event Log mode).
1024-65534 (TCP)	WMI, DCOM, RPC - Outgoing traffic ports	Outgoing Traffic Ports - DCOM uses callback mechanism on random ports between 1024-65534. Hence, open the ports above 1024.

EventLog Analyzer uses the following ports for local agent to server UDP communication:

Port Numbers	Ports Usage	Description
5000, 5001 (UDP)	UDP ports for EventLog Analyzer local agent-server communication	EventLog Analyzer uses these UDP ports internally for agent to server communication. Ensure that the ports are free and not occupied by other local applications running in the machine. These ports need not be opened in the Firewall.

EventLog Analyzer uses the following ports for remote agent to server TCP communication:

Port Numbers	Ports Usage	Description
8400 (TCP)	TCP port for EventLog Analyzer remote agent-server communication	EventLog Analyzer uses this TCP port for remote agent to server communication. Ensure that the port is free and not occupied by other local applications running in the machine. This port need not be opened in the Firewall. **Note:** During automatic agent installation, the WMI, RPC, and DCOM ports are used once.

EventLog Analyzer uses the following port for Elasticsearch server:

Port Numbers	Ports Usage	Description
Any port in range 9300-9400 (TCP)	Elasticsearch server port	This is the port used by Elasticsearch server in EventLog Analyzer.

EventLog Analyzer uses the following port for centralized archiving:

Port Numbers	Ports Usage	Description
Default port number: 8080 Users can assign the port as 22 or any port in range 1024-65535. (SSH)	SSH port for centralized archiving.	This is the port used by EventLog Analyzer to perform centralized archiving. **Note:** When SSH port is enabled, the following firewall setting changes are required. **In Admin Server:** Configure Inbound Rules to allow Admin Server IP and SSH port. **In Managed Server:** Configure Outbound Rules to allow Admin Server IP and SSH port.

For IBM AS/400

Port Numbers	Ports Usage
446-449, 8470-8476, 9470-9476 (TCP)	Keep the mentioned ports opened for access to IBM AS/400 machines.

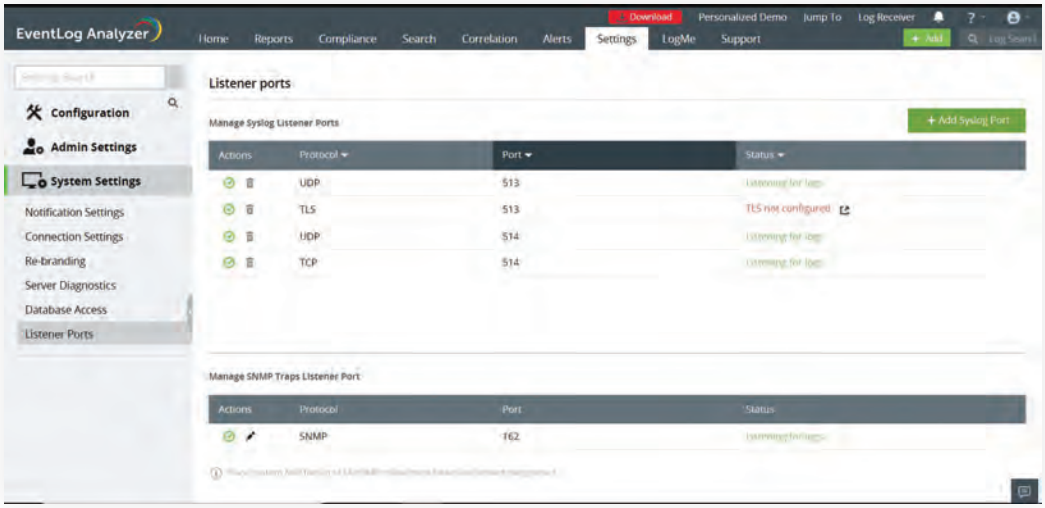
How to change the default ports used by EventLog Analyzer

Procedure to change the default web server port:

- Navigate to *Settings > System Settings > Connection Settings.* You can specify the desired Application port number here.
- To enable HTTPS, select the **Enable SSL** option and mention the desired port number.
- Click **Save.**

Procedure to stop listening for syslogs at the default UDP ports:

- To manage listener ports, navigate to *Settings > System Settings > Listener Ports.* You can disable default ports or add new ports here.
- To add a new port, click **Add Syslog Port.** Enter the **Port number** and select the **Protocol** from the drop down list.
- Click **Add.**



Procedure to change the default PostgreSQL port:

- Edit the **database_params.conf** file, which is located in the *<EventLog Analyzer Home>\conf* folder.
- Change the port number in the following line to the desired port number:
  url=jdbc:postgresql://localdevice:**33335**/eventlog?stringtype=unspecified
- Save the file and restart the server.

Summary

ManageEngine EventLog Analyzer is a comprehensive log management tool that meets the log management and network security needs. Deployment of this solution is simple and its web-based console is user-friendly and intuitive which enables to quickly detect any network anomalies, mitigate security threats, and prevent data breaches.

This solution also comes in Distributed Editions to cater to the log management and network security needs of enterprises span across multiple locations and MSSPs.