Table of Contents

WHAT IS IN THIS GUIDE? ........................................................................................................ 4
INTRODUCTION .................................................................................................................. 5
  Overview ............................................................................................................................. 6
  Release Notes .................................................................................................................... 8
SETUP THE PRODUCT .......................................................................................................... 10
  System Requirements ....................................................................................................... 11
  How to Install and Uninstall EventLog Analyzer ............................................................. 14
  Prerequisites .................................................................................................................... 16
  How to Start and Shutdown EventLog Analyzer .............................................................. 18
  Access EventLog Analyzer Server .................................................................................. 21
  License Details ............................................................................................................... 22
GET STARTED ....................................................................................................................... 25
  Add Hosts ....................................................................................................................... 26
  Import Application Logs ................................................................................................. 36
USER INTERFACE ................................................................................................................. 42
  User Interface Tabs ......................................................................................................... 47
  Customize Dashboard Views ............................................................................................ 51
EVENT REPORTS .................................................................................................................. 54
  Create Custom Reports ................................................................................................... 56
  How to create IBM iSeries (AS/400) custom reports ...................................................... 60
  Host Log Reports ............................................................................................................ 63
  Application Log Reports .................................................................................................. 64
  View Top Hosts Reports .................................................................................................. 74
  User Activity (PUMA) Reports ......................................................................................... 78
  Trend Reports .................................................................................................................. 80
  Ask ME Reports .............................................................................................................. 82
  IBM iSeries (AS/400) Reports ......................................................................................... 84
COMPLIANCE REPORTS

Payment Card Industry – Data Security Standards (PCI-DSS) Compliance Reports
Health Insurance Portability and Accountability Act (HIPAA) Compliance Reports
Federal Information Security Management Act (FISMA) Compliance Reports
Sarbanes-Oxley Act (SOX) Compliance Reports
Gramm-Leach-Bliley Act (GLBA) Compliance Reports
Create New Compliance Reports

SEARCH LOGS

How to Search
Extract New Fields to Parse and Index Logs

EVENT ALERTS

How to Create Alert Profile
How to create IBM iSeries (AS/400) Alert Profile
View Log Alerts

CONFIGURATIONS

Manage Hosts
Manage Applications
Import
Archive
Report Profiles
Alerts
Database Filter
Export, Import Profiles
Custom Patterns for Log Parsing

ADMIN SETTINGS

Install Agent
Manage User
Database Storage Settings
External Authentication

SYSTEM SETTINGS

Working Hour Settings
Configure Email, SMS
EventLog Analyzer Configurations
What is in this guide?

In this guide you will find information for the Administrator and Operator users who use EventLog Analyzer to centrally collect, analyze, search, report, and archive machine generated logs from the network infrastructure consisting of systems, applications, and devices to monitor user behaviors, network anomalies, system downtime, policy violations, internal threats, regulatory compliance, etc. and generate respective reports.

Are you new to EventLog Analyzer?

Go through the following topics. You should be able to deploy, configure, and generate reports using EventLog Analyzer within half an hour.

- How to add host, application and get the logs into EventLog Analyzer?
- What are the reports available?
- How to generate custom reports?
- How to search the logs?
- How to extract additional fields from the logs?
- How to get alert generated and notified?
- How to customize the web client?
Introduction

Security Information and Event Management (SIEM) is an important need of IT Departments in all companies. Machine-generated logs (which include logs generated by network systems, devices and applications) need to be collected, analyzed, archived, searched, and reports generated for the purpose of IT security audit and compliance of various regulatory acts like PCI-DSS, HIPAA, FISMA, SOX, GLBA, etc. This helps companies meet network asset-based SIEM objectives. Apart from this, network administrators and IT managers look at machine-generated logs as a critical source for troubleshooting network anomalies and system performance problems. Efficient event log analysis or syslog analysis reduces system downtime, increases network performance, and helps tighten security policies of the enterprise.

What is EventLog Analyzer?

EventLog Analyzer provides the most cost-effective IT SIEM solution in the market. Using this software, companies can automate the entire process of managing terabytes of machine generated logs by collecting, analyzing, reporting, searching and archiving from one central location. This event log analyzer software helps to mitigate internal threats, conduct log forensics analysis, monitor privileged users and comply to different regulatory compliance requirements by intelligently analyzing the collected logs and instantly generating a variety of reports like user activity reports, regulatory compliance reports, historical trend reports, and more.

This User Guide will help you install EventLog Analyzer on your machine, and gets you familiar with the EventLog Analyzer user interface. If you are unable to find the information you are looking for in this document, please let us know at eventlog-support@manageengine.com
Overview

- Get log data from systems, devices, and applications
- Search any log data and extract new fields to extend search
- Get IT audit reports generated to assess the network security and comply with regulatory acts
- Real-time event correlation, instant alert notification and quick remediation

EventLog Analyzer is a web-based, real-time, log monitoring and compliance management solution for Security Information and Event Management (SIEM) that improves internal network security and helps you to comply with the latest IT audit requirement. Using an agent-less architecture, EventLog Analyzer can collect, analyze, search, report, and archive an extensive array of machine generated logs received from Systems (Windows, Linux, UNIX...), Network Devices (routers, switches, etc...), Applications (Oracle, Apache, etc...) and then provides important insights into network user activities, policy violations, network anomalies, system downtime, and internal threats. It is used by network administrators and IT managers to perform network system audits and generate regulatory compliance reports for SOX, HIPAA, PCI DSS, GLBA, etc.

You can use EventLog Analyzer to:

- Monitor network activities of servers, workstations, devices, and applications spread across geographies
- Monitor user activities like user logons/logoffs, failed logons, objects accessed, etc...
- Generate reports for top network events, user activities, and network event trends
- Generate compliance reports for PCI-DSS, HIPAA, FISMA, SOX, GLBA and other regulatory acts
- Perform log forensics by searching across any log format and save the search results as reports
- Configure automatic alert notification through email or SMS for specific events, network anomalies and compliance threshold violations
- Execute custom scripts or programs on alert generation to automatically remediate the security issue
- Create custom IT reports to address internal security audit
- Create custom compliance reports for IT Auditors
- Schedule reports for auto generation and distribution
- Tamper-proof and secure archival of log data for forensic analysis and compliance audits

Get log data from machines and applications

ManageEngine EventLog Analyzer collects, analyzes, searches, reports, and archives on event logs from distributed Windows hosts; syslogs from Linux/UNIX hosts, Routers, Switches and other
syslog devices; application logs from IIS Web/FTP Servers, Print Servers, MS SQL Server, Oracle Database Server, DHCP Windows/Linux Servers. For real-time Windows event log collection, DCOM, WMI, RPC has to be enabled in the remote windows machine for the logs to be collected by EventLog Analyzer. For real-time syslog collection ensure that the syslog listener ports in EventLog Analyzer are configured to listen to the port where the syslog or syslog-ng service is running on that particular (Cisco Device or UNIX or HP-UX or Solaris or IBM AIX) machine. And for application logs, EventLog Analyzer can be scheduled to import logs (HTTP or FTP) periodically from the application hosts. You can also import and analyze the older logs from Windows and Linux machines.

**Search any log data and extract new fields to extend search**

EventLog Analyzer provides a powerful ‘universal log search’ engine for all types of machine generated logs. Universal log search is made possible with the help of ‘field extraction’ procedure, where you can define/extract new fields from your log data, in addition to the set of default fields that EventLog Analyzer automatically parses and indexes. Once a new field has been ‘extracted’, EventLog Analyzer automatically parses and indexes these new fields from the new logs that are received by EventLog Analyzer subsequently; this drastically improves your search performance and helps EventLog Analyzer handle any kind of log formats.

**Get IT audit reports generated to assess the network security and comply with regulatory acts**

EventLog Analyzer provides a set of canned reports addressing important aspects of internal security. The reports are, top N reports about network events, network user activity, network audit (compliance), and network activity trends. The software has the flexibility to create unlimited number of custom reports to address your IT department’s complex requirements. Over and above the set of canned reports for SOX, HIPAA, GLBA, FISMA and PCI, EventLog Analyzer also allows you to create customized reports for other compliance requirements like ISO27001/2, Federal Deposit Insurance Corporation (FDIC) Audit Requirements, etc. With this software you can schedule periodical report generation and distribute to various users in different formats.

**Real-time event correlation, instant alert notification and quick remediation**

EventLog Analyzer comes with another versatile feature, real-time event correlation and instant alert notifications. You can configure alerts to correlate events based on threshold conditions or anomalous events and notify in real-time for any threshold violations or network anomalies. You can get instant notification via email and SMS. You can also execute a custom script or program upon alert generation and take quick remedial action to secure your network assets.
Release Notes

The new features, bug fixes, and limitations in each of the release are mentioned below.

8.0 - Build 8000 (GA)

8.0 - Build 8000 - Standalone Edition

The general features available in this release include all the features of EventLog Analyzer Version 7.2 Build 7200 and

New Features:

- Sleek and stylish user interface with improved functionality and flexibility
- Customizable dashboard widgets provide better visibility into network events, security events, event trend and event alerts
- Enhanced search permits use of boolean operator, phrase, value ranges, wild-cards, and grouped search
- Log field extraction using an interactive regular expression (regex) syntax builder for extracting one or more raw log fields for automatic indexing
- Universal log parsing and indexing (ULPI) enhances support for any log format
- EventLog Analyzer users can now be imported from Active Directory groups
- Viewing and scheduling 'User Based Reports' now support wild-card '*' characters for selecting users
- Customized 'User Activity Reports' can now be edited from the 'My Reports' section of Reports tab
- Added FTP Active Mode support for log file import
- You can now revert the changes made during rebranding of EventLog Analyzer client
- Additional standalone utility to index data (.dat file)

Enhancements

- Improved the speed of Alerts display in the Alerts tab
- Enhanced the alert email notification content and subject with 'Event ID' field
- Enhanced the alert email notification content with 'Display Name' of the Host instead of 'DNS Name'

Bug Fixes:

- When IBM Maximo log file is imported, the report is shown with the current date. Fixed to display the actual date
- Fixed the issue 'new alerts get generated only after a restart'
- Improved the speed of Reports display in the Reports tab

Zoho Corporation Pvt. Ltd.
• Fixed the issue, archive 'load & search' showing blank page for operator users
• Fixed the 'Log collector crash' issue, due to printer log collection
• Fixed the issue, printer logs not getting categorized in case source name is 'printspooler'
• Fixed the alignment issue in the CSV format of scheduled custom report
• Fixed the issue of displaying number of pages printed in descending order in the 'User based on Printed pages' report
• Removed one of the predefined alerts - 'Norman Antivirus found infected file'
• Fixed the issue Print Server logs getting categorized only after manual scan
• Fixed the TLS secure connection issue
• In create custom report wizard, if browser back button is clicked from second or third screen, the filled/selected values of the fields are lost. The issue is fixed
• Fixed the issue of log collector process carashing when 566, 4662 object access events are processed

**Release Impact:**

• In EventLog Analyzer Distributed edition, the Admin Server dashboard graphs mirror the dashboard graphs seen by administrator of the Managed Server
• To improve performance, the 'Host Name' column in the raw log data page will list the DNS Name instead of Display Name
• Local6 messages in Syslog will be categorized under Application logs
Setup the product

- Download the product
- Check the installation requirements
- Install the product
- Ensure the prerequisites are met
- Run the product
- Check whether your requirements are met
- Check the EventLog Analyzer editions available
- Buy the product
System Requirements

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

- Hardware Requirements
- Operating System Requirements
- Supported Web Browsers
- Supported Platforms & Devices
- RAM & Disk Space Approximation
- MySQL Performance Improvement Parameters

Hardware Requirements

To install in 32 bit machine

The minimum hardware requirements for EventLog Analyzer to start running are listed below.

- 1 GHz, 32-bit (x86) Pentium Dual Core processor or equivalent
- 2 GB RAM
- 5 GB Hard disk space for the product

To install in 64 bit machine

The minimum hardware requirements for EventLog Analyzer to start running are listed below.

- 2.80 GHz, 64-bit (x64) Xeon® LV processor or equivalent
- 2 GB RAM
- 5 GB Hard disk space for the product

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

Operating System Requirements

EventLog Analyzer can be installed and run on the following operating systems (both 32 Bit and 64 Bit architecture) and versions:

- Linux - RedHat 8.0/9.0, Mandrake/Mandriva, SuSE, Fedora, CentOS
- Ability to run in VMware environment

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

**Supported Platforms & Devices**

EventLog Analyzer can collect, index, analyze, archive, search, and report on any machine-generated logs. Ready-built* support is available for logs from the following operating systems and devices:

- Linux - RedHat 8.0/9.0, Debian
- UNIX - Solaris, HP-UX
- IBM AS/400 - Variants V5R1, V5R2, V5R3, V5R4, V5R5 and V6R1
- IBM AIX
- Cisco Switches and Routers
- VMWare - Syslog versions
- SNARE^ for Windows

Ready-built* support is available for logs from the following applications too:

- IIS W3C Web Server
- IIS W3C FTP Server
- Apache Web Server logs
- MS SQL Server
- Oracle 10 G Release 2 (10.2.0.3) - Audit Logs
- DHCP Windows Logs
- DHCP Linux Logs
- Print Server logs

---

1 – as long as the machine generated log is in human-readable format
* - With ‘Universal Log Parsing & Indexing’ technology, EventLog Analyzer also supports logs received from other machines or applications not listed above
® - For analyzing logs from Windows NT machine, WMI core should have been installed in the Windows NT machine
^ - Syslog’s received from SNARE agents for Windows will be displayed as Windows hosts

**RAM Size and Disk Space Requirement Approximation**

The following table recommends the RAM size and disk space requirements of the machine in which the EventLog Analyzer is installed. The RAM size and disk space requirements depends on the number of host sending log information to EventLog Analyzer, the number of log records

---

*Zoho Corporation Pvt. Ltd.*
received per second or the log data received per day by EventLog Analyzer. The calculation is worked out for 100 hosts and an average log record size of 350 bytes.

<table>
<thead>
<tr>
<th>Log Records Rate or Volume</th>
<th>RAM Size</th>
<th>Hard Disk Space Requirement Per Month to Archive Logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>100/sec or 3 GB/day</td>
<td>1 GB</td>
<td>300 GB</td>
</tr>
<tr>
<td>500/sec or 14 GB/day</td>
<td>2 GB</td>
<td>1440 GB</td>
</tr>
<tr>
<td>1000/sec or 28 GB/day</td>
<td>4 GB</td>
<td>2880 GB</td>
</tr>
</tbody>
</table>

**MySQL Performance Improvement Parameters**

For better performance, you can replace the existing MySQL parameters mentioned in `startDB.bat/sh`, available under `<EventLog Analyzer Home>/bin` directory, with the following MySQL parameter changes corresponding to the EventLog Analyzer servers RAM Size.

<table>
<thead>
<tr>
<th>Hardware RAM Size</th>
<th>MySQL Parameter Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 GB</td>
<td>Default configuration as given in startDB.bat/sh</td>
</tr>
<tr>
<td>2 GB</td>
<td>&quot; --innodb_buffer_pool_size=1200M &quot;</td>
</tr>
<tr>
<td>3 GB</td>
<td>&quot; --innodb_buffer_pool_size=1500M &quot;</td>
</tr>
<tr>
<td>4 GB</td>
<td>&quot; --innodb_buffer_pool_size=1500M &quot;</td>
</tr>
</tbody>
</table>

**Recommended System Setup**

Apart from the System Requirements, the following setup would ensure optimal EventLog Analyzer performance.

- Run EventLog Analyzer on a separate, dedicated PC or server. The software is resource-intensive, and a busy processor may cause problems to collect event logs
- Use the MySQL bundled with EventLog Analyzer that runs on port 33335. You need not start another separate instance of MySQL
- As mentioned in the pre-requisites, for better performance, you can modify the existing MySQL parameters

*Zoho Corporation Pvt. Ltd.*
How to Install and Uninstall EventLog Analyzer

- How to install EventLog Analyzer?
- How to uninstall EventLog Analyzer?

How to install?

If you want to install EventLog Analyzer 32 bit version in Windows OS, execute ManageEngine_EventLogAnalyzer.exe file and to install in Linux OS, execute ManageEngine_EventLogAnalyzer.bin file.

If you want to install EventLog Analyzer 64 bit version in Windows OS, execute ManageEngine_EventLogAnalyzer_64bit.exe file and to install in Linux OS, execute ManageEngine_EventLogAnalyzer_64bit.bin file.

Upon starting the installation you will be provided with two options:
- One Click Install
- Advanced Install

Choose One Click Install option to install the product in a single step. This means you agree to the product licensing terms. The product will be installed in C:\ManageEngine\EventLog folder. It will use port number 8400 for web server. It will be installed as a service.

Choose Advanced Install option to customize your product installation. The wizard screens will guide you through the installation.

Quick view of Advanced Installation
- Agree to the terms and conditions of the license agreement. You may get it printed and keep it for your offline reference
- Choose one of the editions to install. The Editions are Standalone, Distributed, and Free

Standalone Edition for Small and Medium Businesses (SMBs) - If you are small or medium business in a single location and monitor less than 600 devices and/or applications, Standalone edition is suitable for you.

Distributed Edition for Large businesses and MSSPs - If you are a large business or MSSP with geographically distributed environment and monitor less than 12000 devices and/or applications, Distributed edition is suitable for you.

Free Edition - If you are micro business or SOHO and want to monitor not more than five hosts, you can download the ManageEngine_EventLogAnalyzer exe or bin file of Standalone edition and install it as a Free edition.
- Select the folder to install the product. Use the **Browse** option. The default installation location will be \( \text{C:}\backslash \text{ManageEngine}\backslash \text{EventLog} \) folder. If the new folder or the default folder does not exist, it will be created and the product will be installed.
- Enter the web server port. The default port number will be 8400. Ensure that the default port or the port you have selected is not occupied by some other application. Choose the language (Simplified Chinese, Traditional Chinese, English, Japanese, Others). Ensure that the browser supports the selected language. Choose the web protocol (HTTP/HTTPS). Use HTTP for unsecured and HTTPS for secured communication.
- Select **Install EventLog Analyzer as service** option to install the product as Windows or Linux service. By default this option is selected. Unselect this option to install as application. You can install as application and later convert the same as service. ManageEngine recommends you to install it as service.
- Enter the folder name in which the product will be shown in the Program Folder. By default it will be **ManageEngine EventLog Analyzer <version number>** folder.
- Enter your personal details to get assistance.

At the end of the procedure, the wizard opts to display the ReadMe file and start the EventLog Analyzer server.

With this the EventLog Analyzer product installation is complete.

**Note:** EventLog Analyzer can be installed in three languages, namely, English, Chinese and Japanese. There is a fourth option ‘Other’. If the user wants EventLog Analyzer to support the double byte (UTF-8) languages, the user should select the ‘Other’ option during installation.

**How to uninstall?**

The procedure to uninstall for both 64 Bit and 32 Bit versions remains same.

**Windows:**

1. Navigate to the Program folder in which EventLog Analyzer has been installed. By default, this is **Start > Programs > ManageEngine EventLog Analyzer.**
2. Select the option **Uninstall EventLog Analyzer.**
3. You will be asked to confirm your choice, after which EventLog Analyzer is uninstalled.

**Linux:**

1. Navigate to the **<EventLog Analyzer Home>/server/_uninst** directory.
2. Execute the command `/uninstaller.bin`
3. You will be asked to confirm your choice, after which EventLog Analyzer is uninstalled.
Prerequisites

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 MySQL:

<table>
<thead>
<tr>
<th>Port Numbers</th>
<th>Ports Usage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8400</td>
<td>Web server port</td>
<td>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.</td>
</tr>
<tr>
<td>513, 514</td>
<td>Syslog port</td>
<td>These are the default Syslog listener ports. Ensure that the hosts are configured to send Syslogs to any one of these ports.</td>
</tr>
<tr>
<td>33335</td>
<td>MySQL database port</td>
<td>This is the port used for connecting to the MySQL database in EventLog Analyzer.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Port Numbers</th>
<th>Ports Usage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>135, 445, 139</td>
<td>WMI, DCOM, RPC - Incoming traffic ports</td>
<td>Incoming Traffic Ports - Windows services DCOM, WMI, RPC will be using these ports and EventLog Analyzer in turn use these services to collect logs from Windows machines in default mode (Event Log mode).</td>
</tr>
<tr>
<td>1024-65534</td>
<td>WMI, DCOM, RPC - Outgoing traffic ports</td>
<td>Outgoing Traffic Ports - DCOM will use callback mechanism and uses random ports (1024-65534) and hence open the ports above &gt;1024.</td>
</tr>
</tbody>
</table>
EventLog Analyzer uses the following ports for agent to server UDP communication:

<table>
<thead>
<tr>
<th>Port Numbers</th>
<th>Ports Usage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5000, 5001</td>
<td>UDP ports for EventLog Analyzer agent-server communication</td>
<td>EventLog Analyzer will be using these UDP ports internally for agent to server communication. Ensure that the ports are free and not occupied by other local application running in the machine. These ports need not be opened in the Firewall.</td>
</tr>
</tbody>
</table>

For IBM AS/400

<table>
<thead>
<tr>
<th>Port Numbers</th>
<th>Ports Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>446-449, 8470-8476, 9470-9476</td>
<td>Keep the mentioned ports opened to access IBM AS/400 machines.</td>
</tr>
</tbody>
</table>

How to change the default ports used by EventLog Analyzer?

Procedure to change the default web server port:

- Edit the `sample-bindings.xml` file present in the `<EventLog Analyzer Home>/server/default/conf` directory.
- Change the port number in the following line to the desired port number:
  `<binding port="8400"/>
- Save the file and restart the server.

Procedure to change the default UDP port for Syslog:

By default, EventLog Analyzer listens to the UDP ports 513 and 514 for syslogs.

- Stop the EventLog Analyzer service.
- Edit the file `runsec.bat`, which is located at `<EventLog Analyzer Home>/bin` folder.
- Edit (in notepad) the entry "bin\SysEvtCol.exe -loglevel 2 -port 513 514" for default port change and remove ports that are not required. For example, if you do not want port 514 as default, the edited line will look like: "bin\SysEvtCol.exe -loglevel 2 -port 513".
- In case, you do not want any default port to be listening for Syslog, remove the "-port" option in the above line.
- After saving the `runsec.bat`, restart the EventLog Analyzer service/server for the changes to take effect.

Procedure to change the default MySQL port:

- Edit the `mysql-ds.xml` file present in the `<EventLog Analyzer Home>/server/default/deploy` directory.
- Change the port number in the following line to the desired port number:
  `<connection-url>jdbc:mysql://localhost:33335/eventlog</connection-url>`
- Save the file and restart the server.
How to Start and Shutdown EventLog Analyzer

Once you have successfully installed EventLog Analyzer, start the EventLog Analyzer server by following the steps below.

- How to start EventLog Analyzer Server/Service?
- How to shutdown EventLog Analyzer Server/Service?

How to start?

Windows Application:

- Select Start > Programs > ManageEngine EventLog Analyzer <version number> > EventLog Analyzer to start the server.
- Alternatively, you can navigate to the <EventLog Analyzer Home>/bin folder and invoke the run.bat file.

Windows Service:

Ensure that the EventLog Analyzer application is installed as Windows Service. When you install with single click, by default it will be installed as Windows Services. If you have carried out custom installation, and chose not to install the software as Windows Service, carry out the procedure to convert the software installation as Windows Service.

Once the software is installed as a service, follow the steps given below to start Windows Service.

- Go to the Windows Control Panel > Administrative Tools > Services. Right click ManageEngine EventLog Analyzer <version number> and select Start in the menu.
- Alternatively, select Properties > <Service> Properties screen. In the General tab, check the Service status is ‘Stopped’ and Start button is in enabled state and other buttons are grayed out. Click Start button to start the server as windows service.

Linux Application:

- Navigate to the <EventLog Analyzer Home>/bin directory and execute the run.sh file.

When the respective run.sh file is executed, a command window opens up and displays the startup information of several EventLog Analyzer modules. Once all the modules are successfully started, the following message is displayed:

Zoho Corporation Pvt. Ltd.
Server started.

Please connect your client at http://localhost:8400
The 8400 port is replaced by the port you have specified as the web server port during installation.

**Note:** If the default syslog listener port of EventLog Analyzer is not free then EventLog Analyzer displays "Can't Bind to Port <Port Number>" when logging-in into the UI.

**Linux Service:**

Ensure that the EventLog Analyzer software is installed as Linux Service. When you install with single click, by default it will be installed as Linux Service. If you have custom installed, and chose not to install the software as Linux Service, carry out the procedure to convert the software installation as Linux Service. Once the software is installed as a service, follow the steps given below to start Linux Service.

```
/etc/init.d/eventloganalyzer start
```

Check the status of EventLog Analyzer service

```
/etc/init.d/eventloganalyzer status
```

ManageEngine EventLog Analyzer 8.0 is running (<Process ID>).

**How to shutdown?**

Follow the steps below to shut down the EventLog Analyzer server. Note that once the server is successfully shut down, the MySQL database connection is automatically closed, and all the ports used by EventLog Analyzer are freed.

**Windows Application:**

- Navigate to the Program folder in which EventLog Analyzer has been installed. By default, this is **Start > Programs > ManageEngine EventLog Analyzer <version number>**. Select the **Shut Down EventLog Analyzer** option.
- Alternatively, you can navigate to the `<EventLog Analyzer Home>in` folder and execute the `shutdown.bat` file. You will be asked to confirm your choice, after which the EventLog Analyzer server is shut down.

**Windows Service:**

Ensure that the EventLog Analyzer software is installed and running as Windows Service.

To stop Windows Service, follow the steps given below.

- Go to the Windows **Control Panel**. Select **Administrative Tools > Services**. Right click **ManageEngine EventLog Analyzer <version number>**, and select **Stop** in the menu.

*Zoho Corporation Pvt. Ltd.*
• Alternatively, select **Properties > <Service> Properties** screen. In the **General** tab of the screen, check the **Service status** is ‘Started’ and **Stop** button is in enabled state and other buttons are grayed out. Click **Stop** button to stop the windows service.

**Linux Application:**

• Navigate to the `<EventLog Analyzer Home>/bin` directory. Execute the **shutdown.sh** file. You will be asked to confirm your choice, after which the EventLog Analyzer server is shut down.

**Linux Service:**

Ensure that the software is installed and running as a service, follow the steps given below to stop Linux Service.

```
/etc/init.d/eventloganalyzer stop
```

Stopping ManageEngine EventLog Analyzer <version number>...

Stopped ManageEngine EventLog Analyzer <version number>

Check the status of the service again

```
/etc/init.d/eventloganalyzer status
```

ManageEngine EventLog Analyzer <version number> is not running.
Access EventLog Analyzer Server

Once the server has successfully started, follow the steps below to access EventLog Analyzer.

- Open a supported web browser. Type the URL address as http://<hostname>:8400 (where <hostname> is the name of the machine in which EventLog Analyzer is running, and 8400 is the default web server port)
- Log in to EventLog Analyzer using the default username/password combination of admin/admin.
- If you import users from Active Directory or add RADIUS server details, you will find that the options are listed in the Log on to field below the Password field of Login screen. In this case, enter the User Name, Password, and select one of the three options in Log on to (Local Authentication or Radius Authentication or Domain Name). Click Login button to connect to EventLog Analyzer.

EventLog Analyzer provides two external authentication options apart from the local authentication. They are Active Directory and Remote Authentication Dial-in User Service (RADIUS) authentication. The Log on to field will list the following options:

- Local Authentication - If the user details are available in local EventLog Analyzer server user database
- Radius Authentication - If the user details are available in RADIUS server and dummy user entry should be available in local EventLog Analyzer server user database
- Domain Name(s) - If the details of the user of a domain is imported from Active Directory into the local EventLog Analyzer server user database

Once you log in, make EventLog Analyzer to start collecting event logs, generate event reports, and more.
License Details

Unlike some of our competitors, who charge based on log volume processed, ManageEngine EventLog Analyzer offers a simple licensing model. Licensing is based on the edition, license model and number of devices. The editions are, Standalone – Premium, Standalone – Professional, and Distributed. The license models are, Perpetual (Standard) and Annual Subscription Model (ASM).

Standalone Edition:

If your company is a Small or Medium Business (SMB), the network is in a single geographical location, and the number hosts and/or applications to be monitored is less than 600, Standalone edition is suitable for your company.

Sub-editions of Standalone Edition

- **Premium Edition** - This edition offers complete Security Information Management (SIM) function with basic log management features and value added SIM features. ManageEngine recommends this edition for wholesome internal network security and future needs of your IT network
- **Professional Edition** - This edition offers basic log management and minimum required Security Information Management (SIM) function to secure your company IT network

Distributed Edition:

If your company is a Large Business, the network is in multiple geographical locations, and the number hosts and/or applications to be monitored is more than 600 and less than 12000, Distributed edition is suitable for your company. The Distributed edition is packed with all the Standalone – Premium Edition features and the Distributed Edition features

Further the license is available in two models Perpetual and Subscription.

- **Perpetual model**
  In this model, the licensing is perpetual and a nominal amount is charged as Annual Maintenance and Support (AMS) fee to provide the maintenance, support, and updates.
- **Subscription model**
  In this model, the license is valid for one year and after that the license gets expired. To continue the license should be renewed every year. Annual Maintenance and Support (AMS) fee is included in the subscription price and not charged separately.

Advantages of ManageEngine Licensing

- Simple host/application based, cost conscious, need based licensing
- The 64 bit installation is also of the same price as 32 bit installation
- The Distributed license is applied on the Admin server and there will be no restriction on the number of Managed servers’ deployment
How to choose the license

- Assess your network and decide upon Standalone or Distributed.
- In Distributed edition, choose Perpetual model for license with no expiry and choose Annual Subscription Model for low entry cost and then decide upon the number of hosts/applications to be monitored.
- In Standalone edition, choose Premium edition if you want to monitor hosts/applications plus value added features and choose Professional edition if you want to monitor only hosts without value added features. Choose Perpetual model for license with no expiry and choose Annual Subscription Model for low entry cost and then decide upon the number of host/applications to be monitored.

Decision Chart to decide EventLog Analyzer Edition
How to upgrade the evaluator license to purchased license

- Before upgrading the current license, ensure that you save the new license file from ZOHO Corp. on the machine in which EventLog Analyzer is installed
- Browse for the new license file and select it
- Click Upgrade to apply the new license file

**Note:** The new license is applied with immediate effect. You do not have to shut down and restart the server after the license is applied.

**Display license details**

After you log in to EventLog Analyzer, click the Upgrade License link present in the top-right corner of the UI. The License window that opens up displays the license information for the current EventLog Analyzer installation.

The License window displays the following information:
- Type of license applied - Free or Professional or Premium
- Number of days remaining for the license to expire

Maximum number of hosts that you are allowed to manage
Get Started

Get the Log Data from Hosts and Applications

EventLog Analyzer is setup, started, and connected through web UI. It can get the machine-generated logs from:

Hosts:

- Windows hosts
- Linux/Unix hosts
- Cisco devices
- Syslog devices
- IBM AS/400 (iSeries)

Applications:

- MS IIS W3C Web Server
- MS IIS W3C FTP Server
- Apache Web Server
- DHCP Windows Server
- DHCP Linux Server
- Print Server
- MS SQL Database Server
- Oracle Database Server

Note: With ‘Universal Log Parsing & Indexing ’ technology, EventLog Analyzer also supports logs received from other machines or applications not listed above, as long as these logs are ‘received by’ or ‘imported into’ EventLog Analyzer in human-readable (unencrypted) format.

Welcome screen on the dashboard will guide you to add host(s), application(s) to get the logs. The options in the welcome screen are:

- How to add Windows host to collect event logs and Linux, Unix-host, any Syslog device, and Cisco devices to collect syslogs
- How to import application logs to monitor
Add Hosts

Add a host in the user interface, using any one of the following menu options:

- **Home tab > Hosts > +Hosts**
- **Tabs: +Add > Hosts**
- **Settings tab > Manage Hosts: Add**

**Note**: The default Host Types are Windows, UNIX, IBM AS/400, Cisco Device and Syslog Device. For adding custom/new host types click on the ‘+’ icon and enter the new host type name.

- Adding Windows Host
- Adding UNIX Host
- Adding Cisco Devices (Switches and Routers), Hypervisor, and VMware, or any other Syslog devices
- Adding IBM iSeries (AS/400) Host
- Adding VMware Host
- Adding Oracle Host
- Adding Print Server
- Configuring the Syslog Service on a UNIX Host
- Configuring the Syslog Service on a HP-UX/Solaris/AIX Host
- Configuring the Syslog Service on VMware
- Configuring the Syslog on Cisco Switches

**Add Windows host**

In all Windows hosts, ensure that WMI, DCOM are enabled; logging is enabled for respective module/ object. To forward the Windows event logs in the syslog format use the third party utility like SNARE.
1. Select the host type as Windows. Optionally, use the '+’ icon to create new host type for your host.
2. Enter the host name(s). Enter multiple host names separated by comma. Tip: you can also copy the comma separated host names from a text file and paste in this field.
3. If you have logged in with Administrator rights, you will see the Pick Hosts option. Use the Pick Hosts link to select one or multiple hosts from the Windows workgroups and domains and all the hosts of a workgroup or domain.
4. Select the host group. For Windows host type, Windows Group will be the default selection. Optionally, use the '+’ icon to create new host group to assign the configured host(s).
5. The Domain Name field is optional only if the host machine is in the local workgroup. Ensure to manually type-in the domain name of the host(s). If Pick Hosts menu is used, Domain Name field will be filled automatically.
6. Enter the Login Name (refers to user name) and Password to access the configured host(s). The user account should have admin privileges to fetch the logs. Use the Verify Login link to validate the credentials. If multiple hosts are selected, ensure that the credentials are valid for all the hosts.
7. Enter the Monitor Interval to configure the frequency at which EventLog Analyzer should fetch the log from the hosts. By default, 10 minutes is the minimum monitor interval.
8. Click Save button to add the host(s). Use Save & Add More button to add more hosts.

Pick Host
1. Select the domain or workgroup from which you want to choose the host(s).
2. Use Select All option to select all the hosts of the workgroup or domain listed in the box below. Alternatively, use the search box to search for the required host(s). The search result will be listed in the box below and select the required host(s)
3. The box lists all the hosts of the selected domain or workgroup or host(s) of the search result
4. Use the Login as Domain User option to access the all selected host(s) with domain user credentials
5. Click Update button to add the hosts using Pick Host option
6. If you cannot find host(s) of your interest listed in the selected domain or workgroup, use the Re-Scan the <domain or workgroup> link to scan the selected domain or workgroup
7. If you cannot find host(s), domain(s), OU(s), work group(s) of your interest, listed in the whole network, use the Re-Scan the complete network link to scan the complete network

**Caution:** If EventLog Analyzer has been installed on a UNIX machine, it cannot collect event logs from Windows hosts. However, third party applications can be used to convert the Windows event logs to Syslog and forward it to EventLog Analyzer.

**Note:**

**Collect Logs:** If you want to collect historic logs present in the Windows event viewer, click the Collect Logs 'folder' icon on the top right side of the Add New Host screen. The Collect Logs window pops down. In that, select the check box 'Collect Historic Logs present in EventViewer' to collect the historic logs. If the check box is selected, EventLog Analyzer will collect all the historical logs present in the Windows Event Viewer. If the check box is unselected, EventLog Analyzer will collect only the logs of the past one hour. **Caution:** Historic Log collection activity is CPU and Memory resource intensive. We suggest you to use it judiciously.

**Add UNIX host / Cisco devices / Syslog devices**

UNIX/ Linux hosts configured to send Syslog data to the EventLog Analyzer on either of the default Syslog ports (513 & 514) need not be added as UNIX hosts in EventLog Analyzer and they will be automatically added to the list of hosts.

**Troubleshoot if UNIX/ Linux hosts/ devices not automatically added to the list of hosts**

If the hosts, devices are not added in the Hosts list, follow the troubleshooting procedure given below.

- Check the connectivity between the EventLog Analyzer server and the UNIX/ Linux host or device. Use the 'ping' command and check if UNIX/ Linux machine is reachable from Eventlog Analyzer server and vice-versa

*Zoho Corporation Pvt. Ltd.*
• Logon to EventLog Analyzer user interface, click on **Show Listener Port(s) Details** and check if the ports 513, 514 are up and getting listened

• In case, the default port is down, meaning the port is occupied by some other application, then you can forward the syslog to any other port which is free and ensure that you add that port in EventLog Analyzer product or free the port by stopping the application which uses it

• Check whether the packets are forwarded in the default UDP ports 513, 514 or the custom configured port from the UNIX/Linux machines

• If the machine is not getting added still, check if any firewall (like Windows Firewall or any other services) is blocking the port. If so, unblock the port

• If the issue persists, use any packet capturing tool like Wireshark or Ethereal and ensure that syslogs are forwarded from the UNIX/Linux machine

**Cisco Devices (Switches and Routers), Hypervisor, and VMware, or any other Syslog devices**

In the case of **Cisco Devices (Switches and Routers), Hypervisor, and VMware, or any other Syslog devices**, you have add them as UNIX hosts in EventLog Analyzer. Before adding them as hosts, ensure that Syslog Daemon is configured in those hosts or devices.

1. Select the host type as UNIX. Optionally, use the + icon to create new host type for your host
2. Enter the host name(s). Enter multiple host names separated by comma. **Tip:** you can also copy the comma separated host names from a text file and paste in this field.

3. Select the host group. For UNIX host type, **UNIX Group** will be the default selection. Optionally, use the + icon to create new host group to assign the configured host(s).

4. Enter the Syslog Listener Port through which the UNIX host(s) will be sending the syslog.

5. Click **Save** button to add the host(s).

6. Use **Save & Add More** button to add more hosts.

**Note:** In Linux hosts, ensure that the syslog daemon is running and verify the port number to configure in EventLog Analyzer.

**Use host groups**

While adding the host, you can assign it to one of the existing host groups. The existing groups are Default, Windows, and UNIX. You can also create a new group and assign the host(s) to it. For the default host types, respective host groups will be selected by default.

**Adding IBM iSeries (AS/400) Host**

Keep the ports 446-449,8470-8476,9470-9476 open in EventLog Analyzer to receive IBM AS/400 machine logs.
1. From the Add New Host page, choose **IBM AS/400** as the **Host Type**
2. Use the Host Name box to type a single host name, or a list of host names separated by commas
3. Select the Host Group to which the hosts need to be added. Click the ‘+’ icon to create a new host group
4. Enter the Administrator login name and password for the selected host. Besides the **Password** text box, **Verify Login** link is available. Click the **Verify Login** link to verify the validity of the credentials for the particular host
5. Provide the **Monitor Interval** to configure the frequency at which EventLog Analyzer should fetch the log from the IBM AS/400 machines. By default, 10 minutes is the minimum monitor interval.
6. Select the **Date Format** and the **Delimiter Date Format in the log**. This is the date format used in the logs that will be collected from the IBM AS/400 hosts

If you are done, click **Save** to add this host and return to the list of hosts monitored. If you want to add more hosts, click **Save and Add More** to add this host, and then add more hosts

The user account with which the EventLog Analyzer is logging in to AS400 must have the **authority level** of **50**. Otherwise, the application will not be able to login to fetch History logs.

**Adding VMware Host**

1. From the Add New Host page, choose **UNIX** as the **Host Type** and add the VMware host as UNIX host as per the steps given above.
2. Configure the syslog in the VMware as per the steps given below.
3. After the EventLog Analyzer starts receiving the syslogs from the VMware host, edit the VMware host details and make host type as Hypervisor. Follow the steps given below:
   - Click the **Edit Host Details** icon of VMware host, **Edit Host Details** page opens up.
   - In that, choose **Hypervisor** as the **Host Type**.
   - Click **Save Host Details** to make this host as VMware host and return to the list of hosts monitored.

**Adding Oracle Application**

To configure hosts for which you want to monitor Oracle logs carry out the procedure given below.

- In the **Add New Host** page
  
  Add the **Oracle Application** server as a new **Windows Host** (if the Oracle application is running on a Windows machine) as per the procedure given or as a new **Linux Host** (if the Oracle application is running on a UNIX machine) as per the procedure given.
  
- In the **Settings** page
After adding as Windows or Linux Host, select **Settings** > Configurations: Manage Applications: Add: **Oracle** menu. The **Configure Oracle Hosts** page opens up. In the **Add Host** text field, enter the host name of the Oracle application server. Click the **Save** icon besides the text field. Existing Oracle Application hosts are listed below the text field as **Existing Hosts**.

### Adding Print Server

To configure Print Servers for which you want to monitor the logs carry out the procedure given below.

- In the **Add New Host** page
  Add the **Print Server** as a new **Windows Host** as per the procedure given.

- In the **Settings** page
  After adding as Windows, select **Settings** > Configurations: Manage Applications: Add: **Print Server** menu. The **Configure Print Server** page opens up. In the **Add Host** text field, enter the host name of the Print Server. Click the **Save** icon besides the text field. Existing Print Servers are listed below the text field as **Existing Hosts**.

After Configuring Print Server in EventLog Analyzer, carry out the configuration given below in Print Server.

- **Print Server Configuration**
- **Enable Print Server Log**

Open **Event Viewer** > **Application and Service Logs** > **Print Service**, right click and select **'Enable Log'**. This will enable logging for the corresponding 'Admin', 'Debug' or 'Operational' processes. The logs will be available under Event Viewer.

**Note**: If the Print Server host is a 64 bit Windows OS machine (i.e., Windows Vista and above), carry out the following registry configuration:

- Open the registry editor ‘**regedit**’ of the Print Server machine in the Command Line Window
- Navigate to `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\`
- Right click on **eventlog**. Click new > key and create **Microsoft-Windows-PrintService/Operational or Admin or Debug**

This will convert the Logtype to Administrative then only we can able to query the logs using ELA. This configuration is not required for 32 bit Windows OS versions.
Configuring the Syslog Service on a UNIX Host

1. Login as root user and edit the syslog.conf file in the /etc directory.
2. Append 
   
   *.*<space/tab>\@<server_name>

   at the end, where <server_name> is the name of the machine on which EventLog Analyzer is running.
3. Save the configuration and exit the editor.
4. Edit the services file in the /etc directory.
5. Change the syslog service port number to 514, which is one of the default listener ports of EventLog Analyzer. But if you choose a different port other than 514 then remember to enter that same port when adding the host in EventLog Analyzer.
6. Save the file and exit the editor.
7. Restart the syslog service on the host using the command:

        /etc/rc.d/init.d/syslog restart

For configuring syslog-ng daemon in a Linux host, append the following entries

    destination eventloganalyzer { udp("<server_name>" port(514)); };
    log { source(src); destination(eventloganalyzer); };

at the end of /etc/syslog-ng/syslog-ng.conf, where <server_name> is the ip address of the machine on which EventLog Analyzer is running.

Configuring the Syslog Service on a HP-UX/Solaris/AIX Host

1. Login as root user.
2. Edit the syslog.conf file in the /etc directory as shown below.

    * emerg;* .alert;* .crit;* .err;* .warning;* .notice;* .info;* .debug <tab-separation>@<server_name>

   Note: For Solaris host, it is just enough to include *.debug<tab-separation>@<server_name> in the syslog.conf file.

   where, <server_name> is the name of the machine where EventLog Analyzer server or Service is running. Just ensure that only a tab separation alone is there in between *.debug and @<server_name>.
3. Save the configuration and exit the editor.
4. Edit the services file in the /etc directory.
5. Change the syslog service port number to 514, which is one of the default listener ports of EventLog Analyzer. But if you choose a different port other than 514 then remember to enter that same port when adding the host in EventLog Analyzer.
6. Start the syslog daemon running on the OS. You need to just execute the below command.

    Usage : /sbin/init.d/syslogd {start|stop}

    Command to be executed :
    (for HP-UX) /sbin/init.d/syslogd start
    (for Solaris) /etc/init.d/syslog start
    (for Solaris 10) svcadm -v restart svc:/system/system-log:default
    (for IBM AIX) startsrc -s syslogd

Zoho Corporation Pvt. Ltd.
**Configuring the Syslog Service on VMware**

All ESX and ESXi hosts run a syslog service (syslogd), which logs messages from the VMkernel and other system components to a file.

**To configure syslog for an ESX host:**

Neither vSphere Client nor vicfg-syslog can be used to configure syslog behavior for an ESX host. To configure syslog for an ESX host, you must edit the `/etc/syslog.conf` file.

**To configure syslog for an ESXi host:**

On ESXi hosts, you can use the vSphere Client or the vSphere CLI command vicfg-syslog to configure the following options:

- **Log file path:** Specifies a datastore path to the file syslogd logs all messages.
- **Remote host:** Specifies a remote host to which syslog messages are forwarded. In order to receive the forwarded syslog messages, your remote host must have a syslog service installed.
- **Remote port:** Specifies the port used by the remote host to receive syslog messages.

**To configure syslog using vSphere CLI command:**

For more information on vicfg-syslog, refer the vSphere Command-Line Interface Installation and Reference Guide.

**To configure syslog using vSphere Client:**

1. In the vSphere Client inventory, click on the host.
2. Click the **Configuration** tab.
3. Click **Advanced Settings** under **Software**.
4. Select **Syslog** in the tree control.
5. In the **Syslog.Local.DatastorePath** text box, enter the datastore path to the file where syslog will log messages. If no path is specified, the default path is `/var/log/messages`.

The datastore path format is `[<datastorename>] <path/to/file>` where the path is relative to the root of the volume backing the datastore.

**Example:** The datastore path `[storage1] var/log/messages` maps to the path `/vmfs/volumes/storage1/var/log/messages`.

6. In the **Syslog.Remote.Hostname** text box, enter the name of the remote host where syslog data will be forwarded. If no value is specified, no data is forwarded.
7. In the **Syslog.Remote.Port** text box, enter the port on the remote host where syslog data will be forwarded. By default **Syslog.Remote.Port** is set to **514**, the default UDP port used.

8. Click **OK**.

**Configuring the Syslog on Cisco Switches**

1. Login to the switch.
2. Go to the config mode.
3. Do the below configuration to configure the switch (here, we have used Catalyst 2900) to send the logs to the EventLog Analyzer server:

   ```
   <Catalyst2900> # config terminal
   <Catalyst2900>(config) # logging <EventLog Analyzer IP>
   ```

   For the latest catalyst switches

   ```
   Catalyst6500(config) # set logging <EventLog Analyzer IP>
   ```

   We can also configure other options like logging facility, trap notifications, etc. as

   ```
   Catalyst6500(config) # logging facility local7
   Catalyst6500(config) # logging trap notifications
   ```

   **Note: The same commands are also applicable for Cisco Routers.**

   Please refer Cisco® documentation for detailed steps on configuring syslog in the respective routers or switches. Contact eventlog-support@manageengine.com if the syslog format of your cisco devices are different from the standard syslog format supported by EventLog Analyzer.
Import Application Logs

In EventLog Analyzer, you have to import the application logs. But in the case of Oracle, Print Server, and IBM iSeries applications logs can be fetched in real-time also. The software can import the application logs automatically at regular interval. Alternatively, using FTP you can transfer the application logs to a host machine that is monitored by EventLog Analyzer and then using HTTP the same application log can be imported into EventLog Analyzer from the host machine. EventLog Analyzer will also import the log files with periodical file name change. Optionally, you can associate the imported log file with the existing host.

Import the application log file in to EventLog Analyzer using any one of the following menu options:

- **Home tab > Applications > Import Log**
- **Home tab > Applications > Actions > +Import**
- **Home tab > Applications > Imported Logs > Import Log File**
- **Tabs: +Add > Import Logs**
- **Settings tab > Configurations: Manage Applications: Other Apps**
- **Settings tab > Configurations: Import: Import Log File**
- **Settings tab > Configurations: Import: Imported Log Files > Import Log File**

**Import Log File**

![Import Log File Interface]

1. **Choose Log Format**: Select the format of the log file.
2. **Time Interval**: Specify the time interval for log import.
3. **File Location**: Enter the location of the log file.
4. **Log Type**: Select the type of log to be imported.
5. **Want to Specify Time Criteria?**: Check this if you want to specify time criteria.
6. **Create Throw Away Reports**: Check this if you want to create throw away reports.

Note: If this option is checked, then this imported data will be scored only for the next two days.

Zoho Corporation Pvt. Ltd.
1. Use the **Local Host** option to import the log files from the local machine, from where you are accessing EventLog Analyzer over the web. The maximum log file size for import from local host is 1 GB. Use the **Remote Host** option to import the log files from remote machines. The maximum log file size for import from remote host is 2 GB.

2. Choose the log format you want to import. Apart from application log formats; all the log formats, which can be imported, are listed. Choose the appropriate log format. There is an option to automatically identify the log format, if you are importing logs which are not mentioned in the list, use the **Automatically Identify** option in the list. This option will also identify the existing log formats. The log formats are **Windows Event Log**, **IIS W3C Web Server**, **IIS W3C FTP Server**, **MS SQL Server**, **DHCP Windows**, **DHCP Linux**, **Syslog**, **Apache Access**, **IBM Maximo**, **EventLog Analyzer Archive**, and **IBM iSeries (AS/400)**.

3. Click the **Import** button to start the file import operation.

For **Windows event log** format

**Import Once from Local Host**

**Import Periodically**

*Zoho Corporation Pvt. Ltd.*
a. The time interval at which the log file should be imported is listed. It could be one time import or every hour or every day or every <xxx> minutes.

b. If you have selected Local Host, then the one time import (Time Interval: Import Once) option allows you to import the log file from the local machine/host from which you are accessing EventLog Analyzer (server machine) through web UI. On selecting ‘Import Once’ option you are provided with a Browse button to locate the file or folder containing the log files in the local machine. Periodical import of log files (Time Interval - every hour or every day or every <xxx> minutes) is only possible if the log files are present in the same machine where the EventLog Analyzer (server) is running. In this case, there won’t be a Browse button and you have to manually type-in the location (complete path) of the log file or folder containing the log files in the EventLog Analyzer (server) machine.

Import Log from Remote Host

If you have selected Remote Host, to import the log file from the remote machines, then for all Time Interval options you have to manually type-in the location of the file or folder containing the log files in the remote machine. Alternatively, use the Select Remote File link to get the location of the file or folder.

c. Use the ‘Want to Specify Time Criteria’ option, if you want the import logs of a particular time period. Enter the time frame using the From and To fields. This option is applicable only for importing Windows event logs. The evt/extx log entries available for the specified time period only will be imported.

Zoho Corporation Pvt. Ltd.
d. For Windows Event Log format, choose the Log Type from the list. The options are Application, Security, System, DNS Server, File Replication Service, and Directory Service.

e. Use the Create Throw Away Reports option, if you want to import the log file for ad-hoc report generation. The imported log file will be retained only for two days and after that it will be purged.
c. If you want to import a log file with periodical file name change, select the **Does file name change periodically?** option and select the pattern or generate a new pattern and select it.

d. Use the **Associate to Host** option, if you want to associate the imported application log file to a host. Enter name of the new host and use the **Existing Host** link to associate an existing host in the EventLog Analyzer server.

**For IBM iSeries (AS/400) log formats**

**Import Log File | Imported Log Files**

[Diagram of import options]

- a. For the IBM AS/400 log files, select the date format (yyMMdd, MMddyy, ddMMyy) and the delimiter (/, . -)
- b. The time interval at which the log file should be imported is listed. It could be one time import or every hour or every day or every <xxx> minutes.
- c. If you have selected **Local Host**, then the one time import (Time Interval : Import Once) option allows you to import the log file from the local machine/host from which you are accessing EventLog Analyzer (server machine) through web UI. On selecting ‘Import Once’ option you are provided with a **Browse** button to locate the file or folder containing the log files in the local machine.
  
  Periodical import of log files (Time Interval - every hour or every day or every <xxx> minutes ) is only possible if the log files are present in the same machine where the EventLog Analyzer (server) is running. In this case, there won’t be a Browse button and you have to manually type-in the location (complete path) of the log file or folder containing the log files in the EventLog Analyzer (server) machine.

  If you have selected **Remote Host**, to import the log file from the remote machines, then for all Time Interval options you have to manually type-in the location of the file or folder.

*Zoho Corporation Pvt. Ltd.*
containing the log files in the remote machine. Alternatively, use the Select Remote File link to get the location of the file or folder.

d. If you want to import a log file with periodical file name change, select the Does file name change periodically? option and select the pattern or generate a new pattern and select it.

e. Use the 'Associate to Host' option, if you want the associate the imported log file to a host. Enter name of the new host and use the Existing Host link to associate an existing host in the EventLog Analyzer server.
User Interface

EventLog Analyzer user interface can be accessed anytime, anywhere through any of the supported web browsers. The user interface is intuitive, easy to use and very flexible.

- The drop down menu provides options to add a new host, alert, report, filter, and import logs.
- A search box is available to conduct quick log search.
- In evaluation version, quick links have been provided right at the top to obtain price quote and purchase the product online. For annual subscription licenses, there will be a reminder alert ten days before the date of renewal.
- Menu icons are provided on the top right-hand side of the user interface to obtain details on EventLog Analyzer listener port(s,) and view the raw packets using the Syslog viewer.
- There is a drop down menu for Help, which provides various options to upgrade the license, contact Zoho Corporation Pvt. Ltd.
product support, know more about the product, access the user guide, and access the feedback form.

- A calendar widget is provided to display the data for the selected time period.

Calendar

Use the calendar widget to display the data of dashboard graphs, reports, compliance reports, and alerts for the selected time period.

How to use calendar?

Select a single date

1. This is an editable field where users can manually type-in the time period. By default the current date from mid-night to the current time is displayed.
2. Click twice on the particular date to be selected. The selection will appear on the top and edit the time if required.
3. Predetermined date and time range can be selected. The date and time ranges available are, Last Hour, Today, Last 24 Hours, Last 7 Days, Last 30 Days, and Last Month.
4. Click the Apply button to complete the date and time range selection.

Zoho Corporation Pvt. Ltd.
Select range of days

1. Click and select the start date. The selected start date will appear on the top, edit the time if required
2. Click and select the end date. The selected end date will appear on the top, edit the time if required. The selected range of days will be highlighted colorfully
3. Click the Apply button to complete the date and time range selection

Select across months

Zoho Corporation Pvt. Ltd.
Select across years

Click on the year to get prior 6 & later 5 years listed
Prior 6 & later 5 years to the current year gets listed
User Interface Tabs

EventLog Analyzer user interface provides tabs for accessing the various sections of the product. The tabs provided are:

- Home
- Reports
- Compliance
- Search
- Alerts
- Settings
- + Add
- Search Box

Home tab

The Home tab contains Dashboard, Hosts, and Applications tabs.

Dashboard

EventLog Analyzer dashboard consists of many useful graphical widgets (representing All Events, Alerts, Important Events, Event Category, Security Events, and Log Trend), which provides better visibility in various network events. The dashboard can be customized (‘Customize’ link) by adding/removing widgets, by changing the position of the widgets using drag-and-drop. Host Group-specific dashboard ‘profiles’ can be created, where each dashboard profile displays only that information corresponding to the host group assigned to the profile. The default dashboard profile is ‘All Groups’ and this profile is not editable (add, modify, delete is not possible), unlike other dashboard profiles.

Hosts

The Hosts (tab) section displays the entire list of systems (Windows, Linux, IBM AS/400, HP-UX, etc...) and devices (routers, switches, etc.), from which EventLog Analyzer is collecting logs. The host list displayed is categorized based on Host-group selected from the drop-down list (default: All Groups). You can add new host (+ Host), add and schedule new reports (+ Schedule) from this section. You can search for a particular Host based on its IP Address or Host Name, delete a host or set of hosts, and disable/enable log collection from a particular host or set of hosts. The host list table displays details like host type, event summary (error, warning, failure, others), connection status of the host, time when the last log message was fetched, and host group to which the host belongs. Mouse-hover on any particular host and to view the last 10 events collected from a particular host.
host click 🔄 icon, to edit the host details click 🔄 icon, to ping a particular host click 🔄, to enable/disable log collection from a host click 🔄/🗑. You can even customize the columns you would like to display in the host table by clicking the 'column selector' 🔄 and you can even increase the number of hosts that are displayed per page (from a minimum of 5 hosts per page it can go up to 200 hosts per page)

**Applications**

The Applications (tab) section provides drill-down pie-chart and lists the host from which application logs for IIS W3C Web Server, IIS W3C FTP Server, MS SQL Server, Oracle Live Audit, DHCP Windows/Linux, Apache Web Server or Print Server have been received or imported into EventLog Analyzer. The host list displayed is categorized based on **Application Type** selected from the drop-down list (default: All Applications). Applications logs (other than Oracle & Print Server) can be imported into EventLog Analyzer by selecting **+ Import** from the **Actions** drop-down list. For Oracle and Print Server logs, once you have added Oracle and Print Server to EventLog Analyzer, select **+ Oracle** or **+ Print Server** from the **Actions** drop-down list and provide the ‘host name’ where these applications are running.

The application host list table displays details like host name, application type, total events, recent records, imported time, start time and end time. Click on the host name or the corresponding section in the pie chart to get the complete overview of the application event data, and generate corresponding reports. You can even customize the columns you would like to display in the application host table by clicking the 'column selector' 🔄

**Reports tab**

The custom reports and canned (pre-built) reports are displayed in the Reports tab. Custom report can be created, modified, deleted, scheduled, rescheduled and the report profiles can be imported, exported in XML format.

The canned reports available are top N reports, user activity reports, trend reports, detailed application reports, and detailed host reports. The top N reports lists in descending order, the hosts with most number of user accessed, users with most number of logins, users with most number of interactive logins, hosts based on event severity, and processes based on event severity.

---

*Zoho Corporation Pvt. Ltd.*
Compliance tab

The Compliance tab displays canned compliance reports for various regulatory compliance acts like PCI-DSS, FISMA, HIPAA, SOX, and GLBA. The relevant IT audit sections of the acts are covered by each report in detail. You can modify the existing canned compliance reports to suit specific requirements or create (+ Add) a new compliance report, to meet other IT compliance mandates like ISO 27001/2, etc.

Search tab

The Search tab provides two options to search the raw logs: Basic Search or Advanced Search. The search result is displayed in the lower half of the page and the final search result can be saved as a report (in PDF or CSV format) and can also be scheduled to generate at pre-defined intervals and automatically mailed to a set of configured users. Use 'Basic' search if you are interested in manually constructing the search query. Here you can use phrase search, Boolean search, grouped search, wild-card search, etc. to build your search query. Use 'Advanced' search to interactively build complex search queries easily with field value pairs and relational operators. The fields can be grouped with boolean operators.

New fields can be extracted from the search result and regular expression (regex) patterns can be constructed to easily identify, parse and index these fields in new logs received by EventLog Analyzer..

Alerts tab

This section allows users to create alert profiles to notify you or your team about threshold violations or network anomalies or user activities or compliance violations. The Alerts tab displays all the alert profiles, alerts generated and provides options to disable, modify or delete any existing alert profile. The alert profiles can also be exported or imported in XML format.

Settings tab

This section allows you to configure EventLog Analyzer according to your IT infrastructure. It has three sub-sections, Configurations, Admin Settings, and System Settings.

Configuration

The various configurations you can carry out are: Manage Hosts, Manage Apps, Import, Archive, Report Profile, Alerts, Database Filters, Export/Import Profiles, Custom Pattern, Dashboard Profiles and Ask ME.

Admin Settings

This section allows various administrative activities like: Install Agent, Manage User, DB Storage Settings, and External Authentication.
System Settings

This section consists of various system configuration settings like: Working Hour Setting, Configure Email/ SMS, ELA Configuration, Manage Compliance, Log Collector Alert, Server Diagnostics, Access Database, and Rebranding.

+ Add tab

From this tab, you can add a

- Host
- Alert
- Report
- Filter
- AS/400 Alert
- AS/400 Report
- AS/400 Filter

and

- Import Logs

Search Box

Use the 'search box' for a quick log search. This will carry out basic search of raw logs available in EventLog Analyzer.
Customize Dashboard Views

How to create dashboard profile

In EventLog Analyzer, host group-specific dashboard ‘profiles’ can be created (click + Profile button), where each dashboard profile displays only that information corresponding to the host group assigned to the profile. The default dashboard profile is ‘All Groups’ and this profile is not editable (add, modify, delete is not possible), unlike other dashboard profiles.

Create dashboard profile in EventLog Analyzer using the following menu:

- **Home** tab > **Dashboard** > + Profile > +Add

The procedure to create dashboard profile is given below:

1. Enter a unique view name for the new dashboard view profile
2. Select the host group(s) to add to this profile. Use the left to right arrow to add the host group(s) (move the host group(s) from the Available Group(s) list to Dashboard View

Zoho Corporation Pvt. Ltd.
Group(s) list) and right to left arrow to remove the host group(s) (move the host group(s) from the Dashboard View Group(s) list to Available Group(s) list)

3. Select the ‘Set this view as default dashboard view’ check box to set this newly created profile as default profile for the dashboard

4. Use Update button to save the new dashboard profile

How to edit/ delete dashboard profile

Create dashboard profile in EventLog Analyzer using the following menu:

- Home tab > Dashboard > + Profile

Profiles

+ Profile menu will take you to the Profiles page, where all the view profiles are listed. In the Profiles table, all the profiles added to EventLog Analyzer are displayed with edit icons, host group(s) available for the profile, set as default menu icons, and delete icons.

1. How to edit a profile?
   On the table row of a specific profile Edit menu icon is available. Use the icon to edit the selected profile.

2. How to set it as default profile?
   On the table row of a specific profile Set as default menu icon is available. Use the icon to set the selected profile as default profile.

3. How to delete a profile?
   On the table row of a specific profile Delete menu icon is available. Use the delete icon to delete the selected profile.

Set as default profile

If you want to make any particular profile as the default dashboard profile, you have pin-it to the dashboard by selecting the profile from the drop-down list of profiles and then clicking the 'Pin' on the right-hand-side of the drop-down list.
Customize dashboard graph display

- The graphical charts (widgets) displayed in the dashboard are, All Events, Alerts, Important Events, Event Category, Security Events, and Log Trend. The graphical charts can be selectively displayed in the dashboard using the Customize link.
- The widgets can be dragged and dropped to any position in the dashboard.
Event Reports

EventLog Analyzer offers highly flexible custom reports. It provides a powerful set of canned reports. The reports are displayed in the Reports tab of the UI. The event counts shown in the reports can be drilled down to get the raw logs. The logs can be filtered based on various log fields. The reports can be scheduled as and when required. The custom report profiles can be exported to XML files and can be imported to the same or different EventLog Analyzer server machine.

Description of reports

- **My Reports**
  The custom reports created will be listed in this section. New reports can be added; existing report can be edited or deleted. Unscheduled reports can be scheduled.

- **Top N Reports**
  The top network activities can be viewed with these reports. The top hosts accessed by most number of users, top users with most logins both successful and failed, top login results like successful, failed etc., and event severity wise top hosts and top processes are displayed in these reports.

- **User Activity Reports**
  These reports present the overview of user activities and user based activity. The overview report of user activities gives the snapshot of most important activities of the all the users involved. It can be filtered for hosts. The user wise activity report gives the details of all the activities of individual users. It can be filtered for hosts, users, and reports.

- **Trend Reports**
  The event severity, event category and alert trend reports are available in this section. Current and historical hourly and weekly trends are available.
  - Reports are displayed in both graph and table formats.
  - Reports can be configured for working and non-working hours.
  - Reports can be filtered for individual severity and category.

- **Detailed Application Reports**
  The application reports display specific number of events for each application. The applications are, **MS IIS W3C Web Server**, **MS IIS W3C FTP Server**, **Apache Web Server**, **DHCP Windows Server**, **DHCP Linux Server**, **Print Server**, **IBM Maximo Server**, **MS SQL Database Server**, and **Oracle Database Server**.

*Zoho Corporation Pvt. Ltd.*
• Detailed Host Reports

The detailed host reports display the number of events of each type that have been generated by that host in a selected time period.

**Important Events**

EventLog Analyzer considers events such as user logon/logoff, user account changes, and server-specific events as important events, and shows them under the **Important Events** tab. This simplifies troubleshooting to a great extent, because you don’t have to sift through rows of log information to identify a critical event. Any event that may require more than a customary glance is shown under this tab.

**All Events**

All the events generated by the host, are classified by process (event type) and displayed under this tab. Drill down the event count of the process, to view the event details. The event summary shows the event log source (kernel, syslog, etc.) and the facility (daemon, syslog, etc.) along with the message (event description) and the event timestamp.

**Note:** For Cisco devices, EventLog Analyzer supports reports for Important Events like: Access List Hits, Configuration Changes, ISDN Disconnects, Link State Changes, and System Restarts.
Create Custom Reports

To generate a custom report, create a report profile. Use any one of the following menu options:

- **Reports** tab > Reports: + Add
- **Tabs**: +Add > Report
- **Settings** tab > Report Profiles > Add

The report profile creator wizard contains three screens.

**Wizard Screen 1**

In this screen, name the report, select report type and host(s), host group(s).

1. Enter a name for the report profile
2. Select the report type. The types are **Custom Report**, **Compliance Report**, and **Application Report**. Choose **Custom Report** with Event Filters.
3. Select the host(s) or compliance or application for the respective reports
   - **Custom Report**: Select the host(s) or host groups(s) from the displayed list for which the reports are to be generated
     - Navigate to the next screen with **Next > >** button
   - **Compliance Report**: Select the compliance type, host(s) or host groups(s) from the displayed list for which the reports are to be generated.
     - Use the **Select Compliance** link to select the **Compliance Type**.

*Zoho Corporation Pvt. Ltd.*
1. Select the compliance type from the list: FISMA, PCI, HIPAA, SOX, GLBA
2. Select the required sections of the report for the selected compliance type. Select all sections of the report or only the required sections of the report to generate compliance report
3. Complete the compliance report selection using Done button

Navigate to the last (Select Schedule) screen with Next > > button

**Application Report**

Select the compliance type, host(s) or host groups(s) from the displayed list for which the reports are to be generated

Enter the application type or use the Select link to select the Application Type.

1. Select the application type from the list. The applications added will be listed
2. Complete the application report selection using Done button

Navigate to the last (Select Schedule) screen with Next > > button
**Note:** To create custom report for an imported custom application log, use the Search query and save the result as report.

**Wizard Screen 2**

In this screen, select the event filter option, filter parameters, required Windows Event ID, event type and severity.

1. Select the **Basic** or **Advanced** event filter option. In the **Basic** filter option, basic matching is done on the **Log Message Contains** and **Except** filter. In the **Advanced** filter option, match any or match all criteria is applied on the **Log Message Contains** and **Except** filter.
2. Fill the appropriate filter criteria. The available filters are, **Log Message Contains** – use this to filter the logs for a specific word or phrase, **Except** - use this to exclude the logs if it contains a specific word or phrase, **Event Source** - use this to filter the logs for a specific event source, and **User** - use this to filter the logs for a specific user.
3. Enter the Event ID(s) to filter the logs. Alternatively, use the **Event ID** link to get the Event ID(s) of the logs of your interest
4. In the case of Windows event log, filter the logs for event type(s) and/ or severity(ies) or in the case of syslog, filter the logs for event type(s) and/ or severity(ies)
5. Navigate to the next screen with **Next > >** button
Wizard Screen 3

In this screen, schedule the report generation, choose the report format and summary or detailed, and configure to send via email.

1. Schedule the report generation on an **hourly/daily/weekly/monthly** basis. Choose the **Only once** option if you want to generate reports only once at a specified time. Set the date and time to generate the report at a specific time. Set the time duration for which the report is to be generated, **Previous Hour/Last 60 Minutes/Previous Day/Last 24 Hours/ Previous Week/Last 7 Days/ Previous Month/Last 30 Days**. Daily and Weekly reports can be created for working hours and non-working hours using the filter icon. Daily, Weekly, and Monthly reports can be created only for week days by selecting the option. The working hour and week day reports will be useful for getting the trend of network activities
2. Select the report format, **PDF** or **CSV**
3. Choose summary with details report or summary report to be generated
4. Configure the email ID to which the generated report should be sent. Add multiple IDs separated by comma. **Tip**: Configure Mail Server settings if it is not configured
5. Complete the report profile creation with **Finish** button
How to create IBM iSeries (AS/400) custom reports

To generate IBM iSeries (AS/400) custom report, create a report profile. Ensure that atleast one IBM iSeries (AS/400) host is added in EventLog Analyzer. Use any one of the following menu options:

- **Reports** tab > Reports: + Add
- **Settings** tab > Report Profiles > AS/400
- **Tabs:** +Add > AS/400 Report

The report profile creator wizard contains three screens.

**Wizard Screen 1**

In this screen, name the report and host(s), host group(s).

1. Enter a name for the report profile
2. Select the IBM iSeries (AS/400) host(s) or host group(s) for the reports

Navigate to the next screen with **Next >>** button
Wizard Screen 2

In this screen, select the event filter option, filter parameters, log severity, required IBM iSeries Message ID, and Job Name.

Add New Report

1. Select the Basic or Advanced event filter option. In the Basic filter option, basic matching is done on the Log Message Contains and Except filter. In the Advanced filter option, match any or match all criteria is applied on the Log Message Contains and Except filter.
2. Fill the appropriate filter criteria. The available filters are, Log Message Contains – use this to filter the logs for a specific word or phrase, Except - use this to exclude the logs if it contains a specific word or phrase, Event Source - use this to filter the logs for a specific event source, and User - use this to filter the logs for a specific user.
3. Filter the logs for event severity(ies)
4. Enter the IBM iSeries Message ID(s) to filter the logs
5. Enter the IBM iSeries Job Name to filter the logs

Navigate to the next screen with Next > > button
Wizard Screen 3

In this screen, schedule the report generation, choose the report format and summary or detailed, and configure to send via email.

1. Schedule the report generation on an hourly/daily/weekly/monthly basis. Choose the Only once option if you want to generate reports only once at a specified time. Set the date and time to generate the report at a specific time. Set the time duration for which the report is to be generated, Previous Hour/Last 60 Minutes/Previous Day/Last 24 Hours/ Previous Week/Last 7 Days/ Previous Month/Last 30 Days. Daily, Weekly, and Monthly reports can be created only for week days by selecting the option. The working hour and week day reports will be useful for getting the trend of network activities.

2. Select the report format, PDF or CSV.

3. Choose summary with details report or summary report to be generated.

4. Configure the email ID to which the generated report should be sent. Add multiple IDs separated by comma. Tip: Configure Mail Server settings if it is not configured.

5. Complete the report profile creation with Finish button.
Host Log Reports

All the events generated by a host are collected, aggregated, and grouped under different categories before displaying them in graphs and reports.

From any tab, click on the host name to see a General Summary for that host. The General Summary shows you the number of events of each type that have been generated by that host in the selected time period. You can then click on the event count against each event type to see the exact event that was generated.

Important Events tab:

EventLog Analyzer considers events such as user logon/logoff, user account changes, and server-specific events as important events, and shows them under the Important Events tab. This simplifies troubleshooting to a great extent, because you don't have to sift through rows of log information to identify a critical event. Any event that may require more than a customary glance is shown under this tab.

All Events tab:

All the events generated by the host, are classified by process (event type) and shown under this tab. Click on the event count displayed against process, to see the corresponding details of the event generated. The event summary shows the event log source (kernel, syslog, etc.) and the facility (daemon, syslog, etc.) along with the message (event description) and the event timestamp.
Application Log Reports

The Application Reports provide different reports available for each application. To view the reports use the following menu options:

- **Home tab > Applications >** Host Name: `<host name of the machine associated with application>`
- **Reports tab > Detailed Application Reports section >** View Report: `<Application Name> Logs`

The Detailed Application Reports section lists the Log Type, Report Description and View Report columns of the reports of each application log. View Report column contains links to open the various reports of the selected application log.

The supported application log types are:

- MS IIS W3C Web Server Logs
- MS IIS W3C FTP Server Logs
- DHCP Windows Server Logs
- DHCP Linux Server Logs
- MS SQL Server Logs
- Oracle Audit Logs
- Print Server Logs
- Apache Web Server Logs
- IBM Maximo Server Logs

Reports for MS IIS W3C Web Server Logs

Clicking the View Report link opens the Reports for MS IIS W3C Web Server Logs page.

<table>
<thead>
<tr>
<th>Report</th>
<th>Total Events</th>
<th>Top Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browser Usage Report</td>
<td>522</td>
<td></td>
</tr>
<tr>
<td>Cross Site Scrapping</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attempts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File Type Report</td>
<td>523</td>
<td></td>
</tr>
<tr>
<td>404 Errors Report</td>
<td>44</td>
<td></td>
</tr>
<tr>
<td>HTTP Error Status</td>
<td>33</td>
<td></td>
</tr>
<tr>
<td>Login Report</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multiple URL Report</td>
<td>522</td>
<td></td>
</tr>
<tr>
<td>OS Usage Report</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Right-URLS Report</td>
<td>44</td>
<td></td>
</tr>
<tr>
<td>SQL Injection Attempts</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Users Report</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Zoho Corporation Pvt. Ltd.**
The **Overview** section on top of the page displays the event count in the **Event Count** table. In the table event count is classified based on the severity **Critical**, **Error**, **Warning**, **Information**, and **Total** and displayed in the columns of the table. Below the Event Count table, the page displays the event count for each host under **Hosts** sub section. In the Hosts table, the host names are listed under **Name** column and event count is classified based on the severity **Critical**, **Error**, **Warning**, **Information**, and **Total** and displayed in the columns of the table against each host. The **Report** section at bottom of the page displays the various reports generated in the **Report** column of the table. The total events and top events of each report are listed in the **Total Events** and **Top Events** columns. There are delete icon links against each report to delete the report. The Report section header contains **Edit Report List** link to edit list of reports for the application. A report can be removed or added to the list from the link menu option.

EventLog Analyzer generates the following pre-defined reports for web server application logs:

- **Hosts Report** - the details covered in this report are: Client IP Address, Hits, Page Views, Bytes Sent, and Events
- **Users Report** - the details covered in this report are: Username, Hits, Page Views, Bytes Sent, and Events
- **File Type Report** - the details covered in this report are: File Type, Hits, Percentage, Bytes Sent, and Events
- **Page URLs Report** - the details covered in this report are: URI Stem, Hits, Page Views, Bytes Sent, and Events
- **Browser Usage Report** - the details covered in this report are: Browser, Hits, Percentage, and Events
- **OS Usage Report** - the details covered in this report are: OS, Hits, Percentage, and Events
- **HTTP Error Status Code Report** - the details covered in this report are: HTTP Status, Hits, Percentage, and Events
- **Malicious URL Report** - the details covered in this report are: URI Stem, Hits, Percentage, and Events
- **Cross Site Scripting Attempts Report** - the details covered in this report are: Client IP Address, User Name, and Events
- **SQL Injection Attempts Report** - the details covered in this report are: Client IP Address, User Name, and Events
Reports for MS IIS W3C FTP Server Logs

Clicking the View Report link opens the Reports for MS IIS W3C FTP Server Logs page.

The Overview section on top of the page displays the event count in the Event Count table. In the table event count is classified based on the severity Critical, Error, Warning, Information, and Total and displayed in the columns of the table. Below the Event Count table, the page displays the event count for each host under Hosts sub section. In the Hosts table, the host names are listed under Name column and event count is classified based on the severity Critical, Error, Warning, Information, and Total and displayed in the columns of the table against each host. The Report section at bottom of the page displays the various reports generated in the Report column of the table. The total events and top events of each report are listed in the Total Events and Top Events columns. There are delete icon links against each report to delete the report. The Report section header contains Edit Report List link to edit list of reports for the application. A report can be removed or added to the list from the link menu option.

EventLog Analyzer generates the following pre-defined reports for FTP server application logs:

- Hosts Report - the details covered in this report are: Client IP Address, Bytes Sent, Bytes Received, and Events
- Users Report - the details covered in this report are: Username, Bytes Sent, Bytes Received, and Events
- File Type Report - the details covered in this report are: File Type, File Transfers, Bytes Sent, Bytes Received, and Events
- Server Services Report - the details covered in this report are: Server Service, File Transfers, Bytes Sent, Bytes Received, and Events
- Server IPs Report - the details covered in this report are: Server IP Address, File Transfers, Bytes Sent, Bytes Received, and Events
- Source Port Report - the details covered in this report are: Server Port, File Transfers, Bytes Sent, Bytes Received, and Events

Reports for DHCP Windows Server Logs

Clicking the View Report link opens the Reports for DHCP Windows Server Logs page.

The Overview section on top of the page displays the event count in the Event Count table. In the table event count is classified based on the severity Critical, Error, Warning, Information, and Total and displayed in the columns of the table. Below the Event Count table, the page displays the event count for each host under Hosts sub section. In the Hosts table, the host names are listed under Name column and event count is classified based on the severity Critical, Error, Warning, Information, and Total and displayed in the columns of the table against each host. The Report section at bottom of the page displays the various reports generated in the Report column of the table. The total events and top events of each report are listed in the Total Events and Top Events columns. There are delete icon links against each report to delete the report. The Report section header contains Edit Report List link to edit list of reports for the application. A report can be removed or added to the list from the link menu option.

EventLog Analyzer generates the following pre-defined reports for DHCP windows server application logs:

Zoho Corporation Pvt. Ltd.
- Lease Report - the details covered in this report are: Lease Report and Events
- BOOTP lease report - the details covered in this report are: Events
- DNS dynamic update report - the details covered in this report are: DNS update details and Events. The DNS update details are, DNS dynamic update request and DNS dynamic update successful
- Rogue server detection report - the details covered in this report are: Events
- IP-Event report - the details covered in this report are: IP Address and Events
- MAC-Event report - the details covered in this report are: MAC Address and Events

Reports for DHCP Linux Server Logs

Clicking the View Report link opens the Reports for DHCP Linux Server Logs page.

The Overview section on top of the page displays the event count in the Event Count table. In the table event count is classified based on the severity Critical, Error, Warning, Information, and Total and displayed in the columns of the table. Below the Event Count table, the page displays the event count for each host under Hosts sub section. In the Hosts table, the host names are listed under Name column and event count is classified based on the severity Critical, Error, Warning, Information, and Total and displayed in the columns of the table against each host. The Report section at bottom of the page displays the various reports generated in the Report column of the table. The total events and top events of each report are listed in the Total Events and Top Events columns. There are delete icon links against each report to delete the report. The Report section header contains Edit Report List link to edit list of reports for the application. A report can be removed or added to the list from the link menu option.

EventLog Analyzer generates the following pre-defined reports for DHCP Linux server application logs:

**Zoho Corporation Pvt. Ltd.**
Operations Report - the details covered in this report are: Operation and Events. The operations are: DHCPREQUEST, DHCPNAK, DHCPDISCOVER, DHCPOFFER, DHCPACK, DHCPINFORM, if IN, delete, Wrote, DHCRELEASE, and Abandoning IP

MAC-Event report - the details covered in this report are: MAC Address and Events

Client Gateway Report - the details covered in this report are: Gateway and Events

IP-Event report - the details covered in this report are: IP Address and Events

Single Page Summary Report - the details covered in this report are: Logging device, Operation, IP Address, MAC Address, Gateway, and Events

Reports for MS SQL Server Logs

Clicking the View Report link opens the Reports for MS SQL Database Server Logs page.

The Overview section on top of the page displays the event count in the Event Count table. In the table event count is classified based on the severity Critical, Error, Warning, Information, and Total and displayed in the columns of the table. Below the Event Count table, the page displays the event count for each host under Hosts sub section. In the Hosts table, the host names are listed under Name column and event count is classified based on the severity Critical, Error, Warning, Information, and Total and displayed in the columns of the table against each host. The Report section at bottom of the page displays the various reports generated in the Report column of the table. The total events and top events of each report are listed in the Total Events and Top Events columns. There are delete icon links against each report to delete the report. The Report section header contains Edit Report List link to edit list of reports for the application. A report can be removed or added to the list from the link menu option.

EventLog Analyzer generates the following pre-defined reports for MS SQL database server application logs:

- Successful Trusted Logins - the details covered in this report are: Username and Events
• Successful Non-Trusted Logins - the details covered in this report are: Username and Events
• Failed User Logins - the details covered in this report are: Username and Events
• Insufficient Resources Events - the details covered in this report are: Events

Reports for Oracle Audit Logs

Clicking the View Report link opens the Reports for Oracle Database Server Logs page.

The Overview section on top of the page displays the event count in the Event Count table. In the table event count is classified based on the severity Critical, Error, Warning, Information, and Total and displayed in the columns of the table. Below the Event Count table, the page displays the event count for each host under Hosts sub section. In the Hosts table, the host names are listed under Name column and event count is classified based on the severity Critical, Error, Warning, Information, and Total and displayed in the columns of the table against each host. The Report section at bottom of the page displays the various reports generated in the Report column of the table. The total events and top events of each report are listed in the Total Events and Top Events columns. There are delete icon links against each report to delete the report. The Report section header contains Edit Report List link to edit list of reports for the application. A report can be removed or added to the list from the link menu option.

EventLog Analyzer generates the following pre-defined reports for Oracle database server application logs:

• Create Table - the details covered in this report are: SESSIONID, ENTRYID, USERID, USERHOST, TERMINAL, RETURNCODE, OBJ$CREATOR, OBJ$NAME, and Time
• Drop Table - the details covered in this report are: SESSIONID, ENTRYID, USERID, USERHOST, TERMINAL, RETURNCODE, OBJ$CREATOR, OBJ$NAME, and Time

Zoho Corporation Pvt. Ltd.
- Alter Table - the details covered in this report are: SESSIONID, ENTRYID, USERID, USERHOST, TERMINAL, RETURNCODE, OBJ$CREATOR, OBJ$NAME, and Time
- Alter User - the details covered in this report are: SESSIONID, ENTRYID, USERID, USERHOST, TERMINAL, RETURNCODE, OBJ$NAME, and Time
- Alter System - the details covered in this report are: SESSIONID, ENTRYID, USERID, USERHOST, TERMINAL, RETURNCODE, and Time
- Create User - the details covered in this report are: SESSIONID, ENTRYID, USERID, USERHOST, TERMINAL, RETURNCODE, OBJ$NAME, and Time
- Drop User - the details covered in this report are: SESSIONID, ENTRYID, USERID, USERHOST, TERMINAL, RETURNCODE, OBJ$NAME, and Time
- Logon - the details covered in this report are: SESSIONID, ENTRYID, USERID, USERHOST, TERMINAL, RETURNCODE, and Time
- Logoff - the details covered in this report are: SESSIONID, ENTRYID, USERID, USERHOST, TERMINAL, RETURNCODE, and Time
- Connect - the details covered in this report are: DATABASE USER, PRIVILEGE, CLIENT USER, CLIENT TERMINAL, Status, and Time
- Shutdown - the details covered in this report are: DATABASE USER, PRIVILEGE, CLIENT USER, CLIENT TERMINAL, Status, and Time
- Startup - the details covered in this report are: DATABASE USER, PRIVILEGE, CLIENT USER, CLIENT TERMINAL, Status, and Time
- All Logs - This is created only as a custom report and is not available as a pre-built report

Reports for Print Server Logs

Clicking the View Report link opens the Reports for Print Server Logs page.

The Overview section on top of the page displays the event count in the Event Count table. In the table event count is classified based on the severity Critical, Error, Warning, Information, and
Total and displayed in the columns of the table. Below the Event Count table, the page displays the event count for each host under Hosts sub section. In the Hosts table, the host names are listed under Name column and event count is classified based on the severity Critical, Error, Warning, Information, and Total and displayed in the columns of the table against each host. The Report section at bottom of the page displays the various reports generated in the Report column of the table. The total events and top events of each report are listed in the Total Events and Top Events columns. There are delete icon links against each report to delete the report. The Report section header contains Edit Report List link to edit list of reports for the application. A report can be removed or added to the list from the link menu option.

EventLog Analyzer generates the following pre-defined reports for Print server application logs:

- Print Server Hosts Overview - the details covered in this report are: Print Servers and Job Count
- Print Server Usage Overview - the details covered in this report are: Print Server, Printed Pages, and Jobs
- Printer Usage Overview - the details covered in this report are: Printer, Printed Pages, and Jobs
- Printer Usage based on User Name - the details covered in this report are: User Name, Printed Pages, and Jobs

Reports for Apache Web Server Logs

Clicking the View Report link opens the Reports for Apache Web Server Logs page.
The **Overview** section on top of the page displays the event count in the **Event Count** table. In the table event count is classified based on the severity **Critical**, **Error**, **Warning**, **Information**, and **Total** and displayed in the columns of the table. Below the Event Count table, the page displays the event count for each host under **Hosts** sub section. In the Hosts table, the host names are listed under Name column and event count is classified based on the severity **Critical**, **Error**, **Warning**, **Information**, and **Total** and displayed in the columns of the table against each host. The **Report** section at bottom of the page displays the various reports generated in the **Report** column of the table. The total events and top events of each report are listed in the **Total Events** and **Top Events** columns. There are delete icon links against each report to delete the report. The Report section header contains **Edit Report List** link to edit list of reports for the application. A report can be removed or added to the list from the link menu option.

EventLog Analyzer generates the following pre-defined reports for Apache web server application logs:

- Client Error Report
- Information Report
- Redirection Report
- Server Error Report
- Successful

The details covered in the above reports are: Address, Status Code, Referrers, User Agents, and Event
View Top Hosts Reports

To view the top 'N' hosts reports use the following menu option:

- **Reports tab > Top N Reports**

The **Top N Reports** section in the **Reports** tab, lists the top hosts, users, and processes generating important events. You can click the **View All** link to view all the reports in this section in a single page.

- Top Hosts by User Access
- Top Users by Login
- Top Interactive Login
- Top Hosts by Event Severity
- Top Processes by Event Severity

**Top Hosts by User Access**

This report shows the top 'N' number of hosts with maximum number of successful logins and the top 'N' number of hosts with maximum number of failed login attempts.

While the former is useful in tracking usage trends of hosts, the latter is important in analyzing which hosts are subject to the most number of security breaches.

You can use this report to decide if security policies need to be changed with respect to certain hosts, or tighten security measures across the network.

*Zoho Corporation Pvt. Ltd.*
**Top Users by Login**

This report shows the top 'N' number of users with maximum number of successful logins, and the top 'N' number of users with maximum number of failed login attempts.

This report tells you which user logged into which host, using the password, and whether the user was successful or not. If a user has been accessing several hosts with the user name and password, this report will show you which hosts were used, and when. If the user has tried to log on, but was unsuccessful, this report will show you how many times the user was unsuccessful, on which hosts did the user try, and when.

You can use this report to identify errant users on the network, and set up security policies to track such users.

**Top Interactive Login**

In this report, only the logins done interactively through the UI. This report shows the users with maximum number of successful logins, and the users with maximum number of failed login attempts. This report tells you which user logged into which host, using the password, and whether the user was successful or not.
If a user has been accessing several hosts with the user name and password, this report will show you which hosts were used, and when. If the user has tried to log in, but was unsuccessful, this report will show you how many times the user was unsuccessful, on which hosts did the user try, and when.

You can use this report to identify errant users on the network, and set up security policies to track such users.

**Top Hosts by Event Severity**

This report sorts event logs received from all hosts by severity, and shows the top values for each event severity. At one glance, you can see which hosts have been generating more number of critical events, warning events, and so on. By default, the overall top hosts generating events of any severity, is shown, with the **View Severity** value set to **All**. You can view top 'N' number of hosts severity wise more number of events generated.

You can use this report to quickly identify the hosts that may be experiencing problems, thereby accelerating the troubleshooting process.

**Note:** Some event severity are applicable only to Unix hosts

**Top Processes by Event Severity**

This report sorts event logs generated by processes running across all hosts, and shows the top values for each event severity. At one glance, you can see which processes have been generating more number of critical events, warning events, and so on. By default, the overall top processes generating events of any severity, is shown, with the **View Severity** value set to **All**. You can view top 'N' number of hosts severity wise more number of events generated.
You can use this report to identify the processes with problems, investigate suspicious behavior of critical hosts, determine if there has been a worm or virus attack in the network, and also see which hosts have been affected, thereby reducing network downtime.
User Activity (PUMA) Reports

To view user activity reports use the following menu option:

- Reports tab > User Activity Reports

The User Activity Reports section in the Reports tab, lists the hosts, users, and reports based user activity events.

- User Activity - Overview
- User based Activity Reports

User Activity - Overview

This report lets you know the overall user activity across all hosts. You can change the hosts and get the host wise overall user activity graph display. Select Change Criteria: > Hosts to view the overview graph of a selected hosts. The number of events are plotted against the reports (Event Count vs Report) in the graph. You can drill down to exact logs from the graphs.

The list of user activity reports are:

- User Logons
- User Logoffs
- Failed Logons
- Successful User Account Validation
- Failed User Account Validation
- Audit Logs Cleared

Zoho Corporation Pvt. Ltd.
• Audit Policy Changes
• Objects Accessed
• User Account Changes
• User Group Changes

**User based Activity Reports**

This report lets you know the number of events for user wise activity. You can change the hosts, users, and reports to display the host wise, user wise, and Reports wise number of user activity events. Select **Change Criteria: > Hosts / Users / Reports** to view the graph of selected host(s), user(s), or report(s). The report wise number of events (**Report vs Event Count**) are plotted in the graph.

The list of user activity reports are:

• User Logons
• User Logoffs
• Failed Logons
• Successful User Account Validation
• Failed User Account Validation
• Audit Logs Cleared
• Audit Policy Changes
• Objects Accessed
• User Account Changes
• User Group Changes

**Zoho Corporation Pvt. Ltd.**
Trend Reports

Trend reports let you analyze the performance of hosts based on specific metrics, over a period of time. Trend monitoring helps in historical analysis of the performance of the Windows and UNIX hosts on your network.

To view trend reports use the following menu option:

- **Reports** tab > **Trend Reports**

You can monitor trends of events generated across hosts, based on event severity, or event type. You can monitor trends of alerts triggered. All the trend reports in EventLog Analyzer show the current trend, and compare this with the historical trend. The trend reports available are, hourly (with the time period split into one hour) and weekly (with the time period split into one day). The trend reports are available for working hours, non-working hours, and complete time period.

**Note:** Look up 'Configure Working Hours' to know more about configuring working hours

Beneath each graph, click the **Show Details** link to display the tabular data corresponding to the graph.

- Event Severity Trend Reports
- Event Type/Category Trend Reports
- Alerts Trend Reports

**Event Severity Trend Reports**

This trend report lets you see how events of all severity have been generated across host groups. Current and Historical Trends are shown on an hourly and daily basis. You can choose from the ten severity levels in the **View Severity** box, or see trends of all severities.
Event Type/Category Trend Reports

This trend report lets you see trends of events generated, based on event type - Application, System, or Security. You can choose this from the **View Type** box, or see trends of all event types. Current and Historical Trends are shown on an hourly and daily basis.

Alerts Trend Reports

This type of trend report shows you current and historical trends of alerts triggered on an hourly, as well as daily basis.
Ask ME Reports

Ask ME enables managers and other non-technical staff to answer simple but critical questions about important network events that are of greater importance. The Ask ME section in the Reports tab offers a quick way to see just the reports that you need, without having to create a new report profile, or drilling down through the pre-defined reports.

To view Ask ME reports use the following menu option:

- **Reports** tab > **Ask ME**

Ask ME section shows a series of questions.

- Select the area of interest - login/logoff, users, alerts, etc. If you are not sure, leave it to the default **All Questions** option.
- Select the appropriate question for which you need an answer.
- Click on **Get the Answer**.

If you want more questions to come up in the Ask ME tab, click the **Tell us here** link. In the form that opens up, enter the question and describe it shortly. Once you are done, click **Send**. The EventLog Analyzer Technical Support team will analyze your question, and if found valid, will include it in upcoming releases of EventLog Analyzer.

---

*Zoho Corporation Pvt. Ltd.*
The report corresponding to the question selected is now generated and displayed.

![Top Hosts with Failed Logons](image)

With the enhancement of this feature, you can add the custom questions dynamically under this tab.

**Adding Custom Questions in Ask ME**

Follow the procedure given below to add custom questions in the Ask ME tab.

1. To add a new question, first create a custom report which you want to use as answer (report) for this new question.
2. Open the `AskMe.xml` file located in the `<EventLog Analyzer Home>/server/default/conf` directory.
3. Append a new "Question" and "link" tag in the file. Enter your question in the "Question" tag and enter the URL of the custom report you have created in the "link" tag.
   - To get the URL of the custom report:
     - Select the custom report in the Web Client UI.
     - Copy the URL shown in the Address Bar of the browser.
     - Cut the initial part of the URL "http://<ELA server host:port>/event/" and copy it in the "link" tag. Replace all the '&' symbol with '&amp;' in the copied "link" tag.
   
   Example entry for "Question" and "link" tags are given below:

   ```xml
   <Question>How many times objects and folders are accessed in the hosts added?</Question>
   <link>index2.do?url=topreport_details&amp;RBBNAME=Compliance_ObjectAccess&amp;tab=askCherry&amp;rtype=toprep&amp;TC=10</link>
   ```
4. Save the file

Refresh the Web Client Ask ME section. You will see the new question added is listed at the bottom of the list. Select the custom question you have added and click **Get the Answer**. The report corresponding to the custom question will be displayed.

**Note:** Ensure that you add the new questions after the existing questions. Do not disturb the existing 17 questions.
IBM iSeries (AS/400) Reports

The history logs of IBM AS/400 contain information about the operation of the system and the system status. The history log tracks high-level activities such as the start and completion of jobs, device status changes, system operator messages, and attempted security violations. The information is recorded in the form of messages. These messages are stored in files that are created by the system. History logs help you track and control system activity. When you maintain an accurate history log, you can monitor specific system activities that help analyze problems. History logs record certain operational and status messages that relate to all jobs in the system.

To view IBM iSeries (AS/400) reports use the following menu option:

- Select the Home tab > Hosts
- Click on the host name, for which the host category is IBM AS/400. Custom Report for the IBM AS/400 host will be displayed. The special report will be displayed under the Important Events tab of the Custom Report.

AS/400 System History Log Reports

EventLog Analyzer will generate a variety of special reports using the information extracted from the history logs of AS/400 systems.
Special Reports generated by the application are:

- Successful Logons
- Successful Logoffs
- Unsuccessful Logons
- Job Logs
- Device Configuration
- System Time Changed
- Journal Logs
- Hardware Errors
Compliance Reports

The regulatory compliance reports are mandated by industry bodies/government authorities to assure minimum security to the IT users in various industries. Non-compliance to the regulatory acts attracts penal action. To ensure credible security and address the mandatory requirement compliance reports of IT networks are required. EventLog Analyzer generates the major compliance reports required for the IT industry.

The major pre-built reports available in EventLog Analyzer are PCI-DSS, HIPAA, FISMA, SOX, and GLBA. This compliance management software keeps the future IT compliance regulations in mind and offers custom compliance reports generation feature. ISO-27001 and NIST-1075 are some of the regulatory compliance acts for which the reports can be generated. Even the existing compliance can be modified to suit the individual internal needs of the company.
You can modify the existing canned compliance reports to suit specific requirements or create (+ Add) a new compliance report, to meet other IT compliance mandates like ISO 27001/2, etc.

Individual Compliance reports can be filtered for groups and sub-groups of the compliance acts using Change Criteria: 'Reports' link and hosts using Change Criteria: 'Hosts' link. The compliance reports can be scheduled for periodic generation using 'Schedule' link. Export the the report to PDF, CSV formats using the 'Export to:' link. Use the Calendar widget to display the report for the selected time period. Show All, Hide All links can be used to display or hide the reports of all the groups and sub-groups of the compliance act.
Payment Card Industry – Data Security Standards (PCI-DSS) Compliance Reports

You need to observe the PCI-DSS (Payment Card Industry - Data Security Standards) guidelines if your organization store, transmit or process customer credit card data.

EventLog Analyzer ensures compliance of Payment Card Industry Data Security Standard (PCI-DSS) Requirement 10. This section mandates payment service providers and merchants to track and report on all access to their network resources and cardholder data through system activity logs. When something goes wrong in the network, the presence of logs in networked environment allows forensic analysis to pin-point the exact cause. Without system activity logs it would be difficult to determine the cause of a compromise.

**PCI-DSS requirements 10.1 & 10.2.2 - User Access**
- Individual User Action

**PCI-DSS requirements 10.2.1 & 10.2.3 - Logon**
- Successful User Logons
- Successful User Logoffs
- Unsuccessful User Logons
- Terminal Service Session

**PCI-DSS requirements 10.2.3 - Policy Changes**
- User Policy Changes
- Domain Policy Changes
- Audit Policy Changes

Zoho Corporation Pvt. Ltd.
PCI-DSS requirements 10.2.6 - System Events
- System Logs
- Audit Logs Cleared

PCI-DSS requirements 10.2.7 - Object Access
- Object Accessed
- Object Created
- Object Modified
- Object Deleted
- Object Handle
Health Insurance Portability and Accountability Act (HIPAA) Compliance Reports

The Health Insurance Portability And Accountability Act (HIPAA) regulation impacts those in healthcare that exchange patient information electronically. HIPAA regulations were established to protect the integrity and security of health information, including protecting against unauthorized use or disclosure of the information. HIPAA states that a security management process must exist in order to protect against "attempted or successful unauthorized access, use, disclosure, modification, or interference with system operations". When breach of medical records occurs, healthcare service providers damage their brand value and end up paying a hefty monetary penalty.

EventLog Analyzer can easily monitor both perimeter devices, such as IDSs, as well as insider activity. HIPAA regulations mandate analysis of all logs, including OS and application logs.

164.308(a)(1)(ii)(D) - Object Access
- Object Accessed
- Object Created
- Object Modified
- Object Deleted
- Object Handle

164.308(a)(3)(ii)(A) & (a)(4)(ii)(B) - Account Logon
- Successful User Account Validation
- Unsuccessful User Account Validation

Zoho Corporation Pvt. Ltd.
164.308(a)(5)(ii)(C) & (a)(6)(ii) - Logon

- Successful User Logons
- Successful User Logoffs
- Unsuccessful User Logons
- Terminal Service Session

164.308(a)(7)(i) - System Events

- System Logs
- Audit Logs Cleared
Federal Information Security Management Act (FISMA) Compliance Reports

All government agencies, government contractors, and organizations that deal and exchange data with government systems must follow FISMA compliance guidelines. Organizations have to monitor, retain and maintain audit records of all security events as per FISMA (Federal Information Security Management Act).

The objective of FISMA compliance is to ensure that Federal departments and agencies observe measures to mitigate the security risks to critical data.

EventLog Analyzer generates reports for the controls specified in the FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems. This standard specifies minimum security requirements for federal information and information systems in seventeen security-related areas. Federal agencies must meet the minimum security requirements as defined through the use of the security controls in accordance with NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems, as amended.

Audit and Accountability (AU) - Object Access

- Object Accessed
- Object Created
- Object Modified
- Object Deleted
- Object Handle

Access Control (AC) - Logon

- Successful User Logons
- Successful User Logoffs

Zoho Corporation Pvt. Ltd.
• Unsuccessful User Logons
• Terminal Service Session

Certification, Accreditation, and Security Assessments (CA) - Security Assessment
• Windows Services

Contingency Planning (CP) - Contingency Planning
• Windows Backup
• Windows Restore

Identification and Authentication (IA) - User Access
• Individual User Action

Configuration Management (CM) - Configuration Management
• Windows Software Updates
• Anti-malwares
• Other Software
Sarbanes-Oxley Act (SOX) Compliance Reports

SOX (Sarbanes Oxley) legislation requires all Public companies and Public accounting firms to show the auditors the accuracy of their financial reporting.

EventLog Analyzer lets enterprises to collect, retain and review terabytes of audit trail log data from all sources to support IT process controls of Section 404, Sarbanes-Oxley Act. These logs form the basis of the internal controls that provide enterprise with the assurance that financial and business information is factual and accurate.

**SEC 302 (a)(4)(A) - System Events**
- System Logs
- Audit Logs Cleared

**SEC 302 (a)(4)(A) - Process Tracking**
- Process Access

**SEC 302 (a)(4)(B) - Policy Changes**
- User Policy Changes
- Domain Policy Changes
- Audit Policy Changes

**SEC 302 (a)(4)(C) - Logon**
- Successful User Logons
- Successful User Logoffs
• Unsuccessful User Logons
• Terminal Service Session

**SEC 302 (a)(4)(D) - Account Logon**
• Successful User Account Validation
• Unsuccessful User Account Validation

**SEC 302 (a)(5)(A) - Object Access**
• Object Accessed
• Object Created
• Object Modified
• Object Deleted
• Object Handle

**SEC 302 (a)(5)(B) - User Access**
• Individual User Action

**SEC 302 (a)(6) - Account Management**
• User Account Changes
• Computer Account Changes
• User Group Changes
Gramm-Leach-Bliley Act (GLBA) Compliance Reports

The Gramm-Leach-Bliley Act (GLBA) mandate that every financial institution should have polices and processes in place to protect "non-public personal information" from threats.

It is necessary that a security management process exists in order to protect against attempted or successful unauthorized access, use, disclosure, modification, or interference of customer records. In other words, being able to monitor, report, and alert on attempted or successful access to systems and applications that contain sensitive customer information.

EventLog Analyzer helps you to comply with the Financial Services Modernization Act (FMA99) commonly referred to as the Gramm-Leach-Bliley Act (GLBA). Title V of the Act governs the steps that financial institutions and financial service companies must undertake to ensure the security and confidentiality of customer information. The Act asserts that financial services companies routinely collect Non-Public Personal Information (NPI) from individuals, and must notify those individuals when sharing information outside of the company (or affiliate structure) and, in some cases, when using such information in situations not related to the furtherance of a specific financial transaction.

Section 501B (1) - System Events

- System Logs
- Audit Logs Cleared

Section 501B (2) & (3) - Logon

- Successful User Logons
- Successful User Logoffs
- Unsuccessful User Logons
- Terminal Service Session
Create New Compliance Reports

EventLog Analyzer offers the flexibility to create new, custom compliance report to cater for the future or custom compliance needs.

Add new compliance report in EventLog Analyzer using the client. The menu options are:

- **Compliance** tab > +Add
- **Settings** tab > Manage Compliance > Add
- **Settings** tab > Compliance Settings > +Add

1. Enter name for the new compliance report
2. Write a short description of the compliance act addressed
3. Select all the groups and sub groups of the compliance acts using the **Check All** link and unselect using **Clear All** link. This makes the selection of all the groups easy.

4. Select the individual groups using the respective check boxes and expand icon to expand the group to display the sub groups. This makes the selection of group(s), sub group(s) flexible.

5. Save the new compliance report using **Save** button.

### Customize the existing compliance report

Customize existing compliance report in EventLog Analyzer using the client. The menu options are:

- **Compliance** tab > Edit
- **Settings** tab > Manage Compliance > Edit

1. Select a specific or any number of or all the compliance report(s) and select the individual groups using the respective check boxes and expand icon to expand the group to display the sub groups. This makes the selection of group(s), sub group(s) flexible.

2. Select all the groups and sub groups of the compliance acts using the **Expand All** link and unselect using **Collapse All** link. This makes the selection of all the groups easy.

3. Save the customized compliance report(s) using **Save** button.

### Delete the existing custom compliance report

You can delete the custom compliance report you have created. Use the X icon besides the respective compliance report in the list of reports. The menu option is:

- **Settings** tab > Manage Compliance > Del

**Note:** The default compliance reports cannot be deleted, they can be only disabled.
Search Logs

EventLog Analyzer’s Log search functionality is very easy and allows you to do a free form search. When a user enters a search criterion in the search bar, EventLog Analyzer rapidly drills down into the raw logs and retrieves the results for your search query.

This section discusses about how to search logs in EventLog Analyzer.

- Refer the How to Search topic for explanation about search. You can carry out two types of searches: Basic Search and Advanced Search
- Refer the How to Extract Additional Fields topic for explanation about how to extract fields interactively

Go to Search

After logging in to EventLog Analyzer, click the Search tab.

Using the Search Result

You can use the result of the search to create Report Profile. This will be useful for network troubleshooting and forensic analysis.
How to Search

EventLog Analyzer provides a dedicated section for log data search, where you can search the raw logs and detect network anomalies like mis-configurations, viruses, unauthorized access, applications errors, etc. Click the 'Search' tab in the UI.

The procedure to search th logs is given below:

Select specific Host(s), Host Group(s) for log search

To narrow down the search to a specific host(s) or group of hosts, type in the host name(s) or group(s) name in the text box provided or else use the 'Pick Host' link to select the host(s) or host group(s). If host(s), Host group(s) are not selected, log search will be carried out across all available hosts.

Select specific Log Type(s) for log search

You can narrow down the search to the type of log (example: Windows Event Log, Syslog, Oracle Logs), by selecting it from the Log Types list. If log type is not selected, log search will be carried out on all available log types.

By default (if the host name(s) or group(s) name are not provided, and 'All Log Types' option remains unchanged), you can search across all hosts and all log types.

Types of Search

EventLog Analyzer supports both 'Basic' and 'Advanced' search. You can perform Wild-card search, Phrase search, Boolean search, Grouped search, and Range search

Basic Search
If you want to manually type-in your own search string (search criteria) and search the logs, use the 'Basic' search link.
Search for field values

Type the field value directly in to the Search box.

Search with fields

Type the field name and value directly in to the Search box. The expression for field name and value pair is `<field name> = <field value>`

Example: EVENTID = 7036
Advanced Search

To build complex search expressions with the aid of an interactive search builder, use the **Advanced** link.

**Set criteria to search**

You can have one or more fields in a group and one or more groups to specify criteria filters for search. The fields in a group are related using Boolean operator and the groups are also related in the same way.

If you have defined the criteria, click **Apply** button.
The search criteria expression appears in the text box. Click 'Go' button to preview the search results.

It is displayed in a graph 'Result Graph' and the entries are listed below. The result graph is displayed for a period of two weeks only.

Note: If the upgrade to the latest version is less than two weeks, the graph is displayed only for the period from the date of upgrade.
How to clear and save Search?

Clear the search

'Clear Search' clears the search query.

Save the search

If you are satisfied with the preview of the search result, you can save the search query by clicking 'Save Search' and the corresponding search result as a report profile.

More Search Examples - Basic Search

Use boolean operators to search

The expression with boolean operator is `<field name> = <field value> <boolean> <field name> = <field value>`. You can use the following boolean operators: AND, OR, NOT.

Example: HOSTNAME = 192.168.117.59 AND USERNAME = guest

Use comparison operators to search

The general syntax for using comparison operator is `<field name> <comparison operator> <field value>`. You can use the following comparison operators: =, !=, >, <, >=, <=. Example: HOSTNAME != 192.168.117.59
Use wild-card characters to search

The general syntax for using wild-card character is `<field name> = <partial field value>` <wild-card character>. You can use the following wild-card characters: ? for single character, * for multiple characters.

Example: **HOSTNAME = 192.***

Use phrase to search

The general syntax for using phrase is `<field name> = <"partial field value">`. Use double quotes (""") to define phrase in the field value.

Example: **MESSAGE = "session"**
Use range to search

The general syntax for searching a range of values is `<field name> = [<from-value> TO <to-value>]`. Use square brackets `[]` to define 'from' TO 'to' range of field values.
Example: **USERNAME = [k To z]**

Use grouped fields to search

The general syntax to search with grouped fields is `( <field name> = <field value> <logical operator> <field name> = <field value> ) <logical operator> <field name> = <field value>`. Relate the field value pairs logically and group them using brackets `()` and relate the grouped fields logically.
Example: **(SEVERITY = debug or FACILITY = user) and HOSTNAME = 192.168.117.59**
Extract New Fields to Parse and Index Logs

Network Administrators are always in need of more information and insights from their log data. There are times when an IT administrator would identify some log information which is useful and would like to have it indexed automatically as a new field. Having more fields being indexed makes your log data more useful while conducting log forensics analysis and creating network security reports.

EventLog Analyzer allows administrators to (extract or) create custom (new) fields from raw logs by using the interactive Field Extraction UI to create regular expression (RegEx) patterns to help EventLog Analyzer to identify, parse and index these custom fields from new logs it receives from network systems and applications.

Procedure to extract new fields

In the Search screen, select the host(s) or host group(s), if unsure leave it blank. Leaving it blank will search all the hosts of the host groups. Select the log type for which you want to extract new fields. To narrow down the logs, enter specific word(s) in the search query text box, if you are unsure leave it blank. Leaving it blank will list all the log entries in the result. Click Go button. This will list the results for the above mentioned search. Use the Wrench icon of the particular log entry from which you want to extract the new field(s).

Step 1: Edit the log type and view the existing fields

1. The Log Type is displayed. For non-default log types, the display name will be name of the imported log file or hostname/port
2. View the details of the 'Existing Fields & Values for this Log Type' with the help of Show and Show All links.
Step 2: Select the required custom field value(s) and specify the details

1. Select and click the field value in the message, to be extracted as field
2. Provide a name for this field. Specify the prefix and suffix to the field value
3. Click on Create Pattern to generate a parser rule or regex (regular expression) pattern

**Note:** The word(s)/character(s) preceding and succeeding the selected field value are called, Prefix and Suffix. These are used as identifiers to extract the fields exactly. The prefix and suffix can have a static value (Exact Match) or dynamic value (Similar Pattern) or they can be ignored.

**Example for Static and Dynamic value for Prefix and Suffix**

Message : Successful Network Logon: User Name: sylvian Domain: ADVENTNET Logon ID: (0x0,0x6D51131) **Logon Type:** 3 Logon Process: NtLmSsp Authentication Package: NTLM Workstation Name: SYLVIAN Logon GUID: - Caller User Name: - Caller Domain: - Caller Logon ID: - Caller Process ID: - Transited Services: - **Source Network Address:** 192.168.113.97 Source Port: 0 22873

The prefix Logon Type can be a static value as most of the logs will have the exact word as 'Logon Type' where as 'Source Network Address' can be dynamic as the logs may have different word(s) like, Source IP Address, Source Address, but with same pattern. If the prefix and suffix are defined with exact match, the field extraction will be precise.
Step 3: Validate the pattern and save it to extract the new field

1. A parser rule pattern is created using the field definition.
2. **Validate** link is used to test the generated pattern against the previous search results. You can manually check the suitability of the pattern by analyzing the 'Matched Log Messages' and 'Unmatched Log Messages' displayed.

**Screen shot of Validate check**
3. On validation, if the matched log messages of generated pattern does not meet your field definition requirement, the pattern needs to be fine tuned. You can edit the generated pattern manually, if you are familiar with regular expressions (regex). Optionally, click on **Choose another Pattern** to choose a pattern from a list of patterns generated by the application.

![Screen shot of patterns generated by the application](image)

You can add a open attribute to this new field. The procedure to add open attribute is shown below in the screen shot.

![Fill the name and value for the open attribute](image)  ![Add one more open attribute name-value pair](image)

*Zoho Corporation Pvt. Ltd.*
4. Optionally, you can define any existing field matching criteria to apply the pattern for this specific log type.

5. Save the pattern to enable EventLog Analyzer to identify, parse and index these custom fields from the new logs it receives from network systems and applications. While saving the pattern, a pop-up window asks for an option to save this pattern as identity rule for this user defined log type.

![Image of pop-up window](image)

The custom pattern (parser rule) can be marked and unmarked as Identity rule for that user defined log type. Multiple custom patterns can be marked as Identity rules for a particular user defined log type.

The saved pattern will be listed in the Settings tab under Custom Pattern Settings section.

6. Use the Ask Support button, if you face any problem and get assistance from the EventLog Analyzer team.
Event Alerts

One of the powerful features offered by EventLog Analyzer is real-time alerts. EventLog Analyzer can generate alert for occurrence of a specific security event and specific compliance event. Alert profiles can be created using pre-defined alert criteria, custom alert criteria, and compliance alert criteria.

- Create an Alert Profile
- Creating IBM iSeries (AS/400) Alert Profile
- View Alerts
How to Create Alert Profile

To create an alert profile in the user interface, using any one of the following menu options:

- Alerts tab > Alerts Profiles > +
- Tabs: +Add > Alert
- Settings tab > Alerts > Add

Follow the procedure given below to create alert profile.
1. Enter a unique name for the alert profile
2. Assign criticality for the alerts generated using this profile. The options available are High, Medium, and Low
3. Alert can be generated for selected host(s) and host group(s). Select the required host(s) and host group(s)
4. Use the pre-defined alert criteria to set up the alerts quickly. If you have an alert requirement which is not covered by pre-defined criteria, use the custom alert criteria. If you have compliance specific alert requirement use the compliance alert criteria. Select the alert criteria as required. Define the criteria for alerts

**Pre-defined Alerts**

- a. Select pre-defined alert to define alert criteria
- b. Select a pre-defined alert item
- c. When a pre-defined alert item is selected, the Severity/Event ID, Log Type, and Message of the log are automatically populated and the fields are non-editable. With this alert profile can be created fast.
- d. Further alert generation can be controlled from one alert per event to one alert for a defined number of events occurring within a defined time period. Enter the number of events and the time duration for which one alert should be generated

**Compliance Alerts**

- a
- b
- c

**Zoho Corporation Pvt. Ltd.**
a. Select compliance alert to define alert criteria
b. When compliance alert is selected, the supported compliances are listed. The compliances are **FISMA, PCI, HIPAA, SOX,** and **GLBA.** Compliance specific alerts for Failed Logon Attempts, Policy Changes, Account Changes & Audit Logs Cleared. Select the compliance(s) as required
c. Further alert generation can be controlled from one alert per event to one alert for a defined number of events occurring within a defined time period. Enter the number of events and the time duration for which one alert should be generated

**Custom Alerts**

![Custom Alerts Diagram]

a. Select custom alert to define alert criteria
b. Select the log type from the list. Default value will be **Any.** Select multiple log types using **+ More** link. Alert is generated if other criteria is met for any one of the log types
c. Select the severity from the list. Default value will be **Any.** Select multiple severity using **+ More** link. Alert is generated if other criteria are met for any one of the severity. If Event ID is selected, enter the event ID or use the Event ID to select the event IDs for a specific message
d. Use the **Log Message Contains** fields to define the alert to get triggered if a specific word or phrase is found in the log message and use the **Except** field to define the alert to not get triggered if a specific word or phrase is found in the log message.e. For the above two fields, advanced option is available. With that option more than one matching word or phrase can be defined and it can any one of the word/ phrase or all

**Zoho Corporation Pvt. Ltd.**
f. Further alert generation can be controlled from one alert per event to one alert for a defined number of events occurring within a defined time period. Enter the number of events and the time duration for which one alert should be generated.

5. The generated alert can be notified by Email and SMS and with Run Program a script or program can be executed on generation alert, to rectify the alert condition. Select the notification option:

**Settings to notify alert by Email**
Enter the details required for sending alert notification using email.

![Settings to notify alert by Email diagram](image)

- **a.** Enter the email address(es). Enter multiple email addresses separated by comma (,)
- **b.** Enter the subject line of the email notification. You can also append the alert argument(s) to the subject line. Select the arguments from the list.
- **c.** You can add notes to the email notification. The maximum limit of notes is 250 characters. This will be appended to email notification content.

If mail server is not configured in EventLog Analyzer, you will be prompted to set it when **Notify by Email** option is selected.

**Settings to notify alert by Run Program**
Enter the details required for running a script or program when the alert notification is triggered.
a. Enter the name of the script file with location in the EventLog Analyzer client machine. Alternatively, use the **Browse** button to select the script file
b. Specify the alert argument(s) to be passed to the script. Select the arguments from the list. The listed arguments are, source of the log, host generating the log, and the criticality of the alert

**Settings to notify alert by SMS**

Enter the details required for sending alert notification using SMS.

a. Enter the mobile number to which the SMS notification to be sent
b. Enter the message of the SMS notification. You can also append the alert argument(s) to the message. Select the arguments from the list
If SMS setting is not configured in EventLog Analyzer, you will be prompted to set it when **Notify by SMS** option is selected.

6. Use the **Add Alert Profile** button to complete the alert profile creation. The created alert profile will be listed in the **Alert Profile Details** screen. The profiles can be enabled, disabled, modified, and deleted from the list.
How to create IBM iSeries (AS/400) Alert Profile

Ensure that at least one IBM iSeries (AS/400) host is added in EventLog Analyzer. To create IBM iSeries (AS/400) alert profile, use any one of the following menu options:

- **Alerts** tab > Alert Profiles: +
- **Settings** tab > Alerts: AS/400
- **Tabs**: +Add > AS/400 Alert

Follow the procedure given below to create IBM iSeries alert profile.
1. Enter a unique name for the alert profile
2. Assign criticality for the alerts generated using this profile. The options available are High, Medium, and Low
3. Alert can be generated for selected IBM iSeries host(s) and host group(s). Select the required host(s) and host group(s)
4. Define the criteria for alerts. Select the log severity from the list. Alert is generated if other criteria are met for any one of the severity. Enter the iSeries Message ID for a specific message. Enter the iSeries Job Name for a specific job.
5. Use the Log Message Contains fields to define the alert to get triggered if a specific word or phrase is found in the log message and use the Except field to define the alert to not get triggered if a specific word or phrase is found in the log message.
6. For the above two fields, advanced option (Advanced) is available. With that option more than one matching word or phrase can be defined and it can any one of the word/phrase or all
7. Further alert generation can be controlled from one alert per event to one alert for a defined number events occurring within a defined time period. Enter the number of events and the time duration for which one alert should be generated
8. The generated alert can be notified by Email and SMS and with Run Program a script or program can be executed on generation alert, to rectify the alert condition. Select the notification option
9. Use the Add Alert Profile button to complete the alert profile creation. The created alert profile will be listed in the Alert Profile Details screen. The profiles can be enabled, disabled, modified, and deleted from the list
View Log Alerts

After setting up an Alert Profile, select the Alerts tab to see the list of alerts triggered. By default, the Alerts tab lists all the alerts triggered so far. The list shows the timestamp of the alert, the host which triggered it, the alert criticality, the status of the alert, and the message.

Viewing Alerts for an Alert Profile

The Alerts box on the left navigation pane lists all the alert profiles created so far. Click on each alert profile to view the corresponding list of alerts triggered.

The Email icon against an alert profile indicates that an email notification has been setup. The Enabled icon indicates that the alert profile is currently enabled and active. To disable the alert profile, click on this icon. The alert profile is now disabled, and the Disabled icon is shown. When an alert profile is disabled, alerts will not be triggered for that alert profile. To start triggering alerts again, click on the icon to enable the alert profile.

The Alerts tab lets you view alerts for various alert profiles set up. To manage alert profiles, click the Alerts: All Alerts link in the Settings tab: Configuration section.
Configurations

Carry out the necessary configurations required for EventLog Analyzer functioning. You can carry out the following configurations:

- Manage Hosts - Manage Host Groups
- Manage Applications
- Import
- Archive - Archive Settings
- Report Profile - Schedule Reports
- Alert
- Database Filter - IBM iSeries (AS/400) Database Filter
- Export/Import Profile
- Custom Pattern
- Dashboard Profiles - Add | Edit / Del | All Profiles
- Ask ME - Quick Answers
Manage Hosts

The hosts to be monitored by EventLog Analyzer can be managed in this section. Hosts can be added, edited or deleted, and all the hosts monitored can be viewed.

- Manage Hosts
- Manage Host Groups

Hosts

How to add a host?

To add a host, refer the 'Add Host' topic.

How to edit a host?

Edit/ Del menu will take you to the All Hosts table, where all the hosts are listed.

3. Hover the mouse on the table row of a specific host, the Show Last 10 Events, Edit, Ping Now and Enable (if the host is disabled) menu icons will appear on the right extreme of the row. Use the Edit icon to edit the selected host.

How to delete a host?

1a. Select the host(s) by selecting the respective check box(es)
1b. Delete the host(s), using the Action menu item Delete.

How to disable, enable a host?

1a. Select the host(s) by selecting the respective check box(es)
1c. Disable or enable the host(s), using the Action menu items, Disable, Enable.

Other operations on host(s)

Hover the mouse on the table row of a specific host, the Show Last 10 Events, Edit, Ping Now and Enable (if the host is disabled) menu icons will appear on the right extreme of the row.

2. To view the last 10 events from the specific host, use the 'Show Last 10 Events' icon.
3. Use the Edit icon to edit the selected host.
4. To troubleshoot the host for connectivity, use the 'Ping Now' icon.
5. If the host is disabled, use the 'Enable' icon to enable it and if it enabled, use the 'Disable' icon to disable it.

Search a specific host. Modify the columns of the table to be displayed.

**All Hosts**

In the All Hosts table, all the hosts added to EventLog Analyzer for monitoring are displayed with severity wise summary and total event counts, log access status, last time log collected and the host group to which the host belongs.

**Host Groups**

**How to add a host group?**

Add a host group in the user interface, using any one of the following menu options:

- **Settings** tab > **Configurations** > **Group**: Add
- **Settings** tab > **Configurations** > **All Groups** > **Add**

**Add New HostGroup**

1. Enter a unique name for the new host group to be added
2. Write a description of the host group
3. Select the hosts to be added to the host group
4. Click Add
3. Select the host(s) to added to this group. Use the left to right arrow to (move the host(s) from the Available Host(s) list to Selected Host(s) list) add the host(s) and right to left arrow to (move the host(s) from the Selected Host(s) list to Available Host(s) list) remove the host(s)

4. Use the Add button to complete the add host group operation

![Host Groups table]

**How to edit a host group?**

Edit/ Del menu will take you to the Host Groups table, where all the host groups are listed. On the table row of a specific host group, Edit, and Delete menu icons are available. Use the Edit icon to edit the selected host group.

**How to delete a host group?**

On the table row of a specific host group, Edit, and Delete menu icons are available. Use the Edit icon to delete the selected host group.

**Host Groups**

In the Host Groups table, all the host groups added to EventLog Analyzer are displayed with number of hosts, edit and delete icons.
Manage Applications

The applications to be monitored by EventLog Analyzer can be managed in this section. Applications can be added, deleted, and all the applications monitored can be viewed.

How to add an application?

Adding an application is nothing but importing application logs from the local host or remote host and once or periodical. Refer the ‘Import application log file’ topic to import the application logs. Oracle applications have to be associated with specific Windows or Linux hosts and Printer applications has to be associated with specific Windows host.

Import the application log file in to EventLog Analyzer server using the client. The menu options are:

- **Home** tab > **Applications** > **Import Log**
- **Settings** tab > **Manage Applications** > **Other Apps**

Adding Oracle Database Application

To configure hosts for which you want to monitor Oracle logs carry out the procedure given below.

- In the **Add New Host** page, add the **Oracle Application** server as a new **Windows Host** as per the procedure given or as a new **Linux Host** as per the procedure given, depending upon your environment.
- After adding as Windows or Linux Host, select **Settings** > **Manage Applications** > **Oracle** menu. The **Configure Oracle Host** page opens up. In the **Add Host** text field, enter the host name of the Oracle application server. Click the **Save** icon besides the text field. Existing Oracle Application hosts are listed below the text field as **Existing Hosts**.

Adding Print Server Application

To configure Print Servers for which you want to monitor the logs carry out the procedure given below.

- In the **Add New Host** page, add the **Print Server** as a new **Windows Host** as per the procedure given.
- After adding as Windows host, select **Settings** > **Manage Applications** > **Printer** menu. The **Configure Print Server** page opens up. In the **Add Host** text field, enter the host name of the Print Server. Click the **Save** icon besides the text field. Existing Print Servers are listed below the text field as **Existing Hosts**.

How to delete an application?

Select the application(s) by selecting the respective check box(es) and delete the application(s), using the Action menu items.
All Apps

In the All Apps table, all the application logs imported to EventLog Analyzer for monitoring are displayed with the name of the host associated with the application, the type of application, total files imported, number of log records in the last imported file, last time the log file was imported, start time and end time of the log records.
Import

Windows event logs, Syslogs and Application logs can be imported for analysis and report generation.

How to import log files?

Refer the ‘Import log file’ topic to import the logs.

Imported Log Files

In the Imported Log Files page all the logs imported to EventLog Analyzer for monitoring are displayed. There are two tabs, Event log imports and Application log imports.

The **Event log imports** table displays the event log files imported along with the name of the imported file, the name of the host from which it was imported, the type of log, the method of import (HTTP/FTP), the time it was imported, the start time and end time of the log record, and the type of report generated.

<table>
<thead>
<tr>
<th>File Name</th>
<th>Host Name</th>
<th>Log Type</th>
<th>Import Type</th>
<th>Imported Time</th>
<th>LogRecord StartTime</th>
<th>LogRecord LastTime</th>
<th>Report Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012_10_24 11_35_44</td>
<td>IBM540G</td>
<td>N/A</td>
<td>local</td>
<td>2012-10-04 05:00:00</td>
<td>2012-10-04 05:55:59</td>
<td>Active</td>
<td></td>
</tr>
<tr>
<td>2012_10_24 14_42_01</td>
<td>EL-W7-1</td>
<td>N/A</td>
<td>local</td>
<td>2012-10-04 16:00:00</td>
<td>2012-10-04 17:56:56</td>
<td>Active</td>
<td></td>
</tr>
</tbody>
</table>

The **Application log imports** table displays the application log files imported along with the name of the imported file, the description of the log format, the name of the remote host from which it was imported, the current status of the import, the time it was imported, the size of the imported log file, the time taken to import the file, the protocol used to import (HTTP/FTP), and the action to load the log file into the database and search, search the logs if it already loaded in to the database and drop it from the database.

<table>
<thead>
<tr>
<th>File Name</th>
<th>Format Description</th>
<th>Remote Host</th>
<th>Status</th>
<th>Imported Time</th>
<th>Size</th>
<th>Time Taken</th>
<th>Protocol</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS WSC</td>
<td>Web Server Logs</td>
<td>192.168.27.94</td>
<td>Import of log file completed</td>
<td>2012-09-20 15:29:15</td>
<td>373 KB</td>
<td>999 ms</td>
<td>HTTP</td>
<td>Report</td>
</tr>
<tr>
<td>exkl1 4 Log</td>
<td>FTP Logs</td>
<td>192.168.27.94</td>
<td>Import of log file completed</td>
<td>2012-09-20 14:20:59</td>
<td>856 Bytes</td>
<td>415 ms</td>
<td>HTTP</td>
<td>Report</td>
</tr>
<tr>
<td>ERROLOG 4</td>
<td>MySQL Server Logs</td>
<td>192.168.27.94</td>
<td>Import of log file completed</td>
<td>2012-09-20 16:30:18</td>
<td>1.01 MB</td>
<td>3 sec</td>
<td>HTTP</td>
<td>Report</td>
</tr>
<tr>
<td>DHCPLog Thu 1</td>
<td>Windows logs</td>
<td>192.168.27.94</td>
<td>Import of log file completed</td>
<td>2012-09-20 15:30:56</td>
<td>23.16 KB</td>
<td>512 ms</td>
<td>HTTP</td>
<td>Report</td>
</tr>
</tbody>
</table>
Archive

The log files processed by the EventLog Analyzer are archived periodically for internal, forensic, and compliance audits. The archival interval and retention period is configurable. The archive file can be encrypted and time-stamped to make it secure and tamper-proof.

Archived Files page lists all the archived files in a table with the hosts for which the files were archived, start time of archiving, the time at which archived, size of the archived file, the status of the file and action on the file. If the number of archived files is more and if manual viewing and selection is not possible, use the search archived files (search icon) to filter the required files in the list.

How to delete archived files?

1a. Select the archived file(s) by selecting the respective check box(es)
1b. Delete the archived file(s) using the Delete link.

How to generate report from the archived files?

2. Check the status of the archived file. If it is 'Not Loaded', click the 'Load & Search' action to load the file into the database and search the logs.
3. If the status of the file is 'Loaded', click the 'Search' link to search the logs in the file. If you want to drop the file from the database, click the 'Drop DB' link.

Archive Settings

Configure the archival interval, retention period, option to encrypt, time-stamp the archive files in this screen.

Zoho Corporation Pvt. Ltd.
1. Ensure that the archiving is enabled. By default it is enabled. Unselect the check box to disable archiving.

2. The logs are written in to flat files at the specified time period. Choose the required time interval. The default value is 12 Hours.

3. The flat files are compressed (20:1 ratio) and zip files are created at the specified time period. Choose the required time interval. The default value is 4 days.

4. To secure the archive files, enable encryption of the files. By default, it will be in disabled state.

5. To make the archive files tamper-proof, enable time-stamping of the files. By default, it will be in disabled state.

6. Select the log retention period. The default value is 'Forever'.

7. The default archive storage location is displayed and to change the location as required, use the Edit link.

8. The default indexed data storage location is displayed and to change the location as required, use the Edit link.

Save the settings and close the window. For instant archiving, use the 'Zip now' button.
Report Profiles

To generate report in EventLog Analyzer, create a report profile. To create a report profile, use the following menu option:

- **Settings** tab > **Report Profiles** > **Add**

To create a report profile refer the procedure given in the ‘How to create custom reports’ section.

**How to edit report profile?**

Edit/ Del menu will take you to the **My Reports** table, where all the report profiles are listed. On the table row of a specific profile Edit menu icon is available.

1. Select the report profile(s) by selecting the respective check box(es)
2. Delete the profile(s), using the Delete menu link.

**My Reports**

In the My Reports table, the entire user created report profiles are displayed with the name of the profile, the hosts assigned to the profile, last time the scheduled report was generated, the scheduler assigned to the profiles, and provision to add a new schedule to this profile.
Schedule

When a report profile is created, optional scheduler is created for automatic, periodical report generation and distribution. Report profile can be created without scheduler by choosing the option to generate report ‘Only once’. A scheduler can be created for the unscheduled report profile later. If the report profile is already scheduled, new scheduler can created for that profile, superseding the previous scheduler.

To create a scheduler for a report profile, use the following menu option:
- **Settings** tab > **Report Profiles** > **Schedule**: **Add**

To create a schedule, follow the steps given below:

1. Enter a unique for the schedule
2. Select a report profile to which the schedule should associated with
3. Enter email IDs to distribute the generated reports via email
4. Configure the mail server settings, if not configured already
5. Select the time period (Hourly, Daily, Weekly, and Monthly), (Only once) at which the report should be generated.
6. Select the specific time from which the report generation should start for the first time
7. Select the time duration for which the report should be generated
How to edit schedule?

Edit/ Del menu will take you to the Schedules table, where all the schedules are listed.

How to disable/enable schedule?
• Use the Enable/Disable icon to enable or disable the schedule

How to edit schedule?

On the table row of a specific schedule Edit icon is available.
• Use the Edit icon to edit the selected schedule.

How to delete schedule?
• Use the Delete icon to delete the respective schedule.

Schedules

In the Schedules table, all the schedules created are displayed with enable/disable option, edit option, delete option, the name of the schedule, the report profile associated to the schedule, type of schedule, and the details of the reports generated as per schedule.
Alerts

To generate alert in EventLog Analyzer, create an alert profile. To create an alert profile, use the following menu option:

- **Settings** tab > **Alerts** > **Add**

To create an alert profile refer the procedure given in the ‘How to create alert profile’ section.

### How to edit alert profile?

1. Use the Edit icon to edit the selected alert profile.

### How to delete report profile?

2. Select the alert profile(s) by selecting the respective check box(es)

3. Delete the profile(s), using the Delete menu link.

### All Alerts

In the **Alert Profile Details** table, all the alert profiles created are displayed with enable/disable option, edit profile option, selection check box to delete, the name of the profile, the host(s)/host group(s) assigned to the profile, log type for which the alert will be generated, and the number alerts generated for each profile.
Database Filter

To prevent unnecessary or unwanted log data entering into EventLog Analyzer for processing, 'Database Filter' is available. This will reduce the log noise and allow only necessary logs allowed to get processed.

- Create Database Filter
- Create IBM iSeries (AS/400) Database Filter

Create Database Filter

To create a log database filter, use the following menu option:
- Tabs: +Add > Filter
- Settings tab > Database Filter > Add

To create a database filter, follow the steps given below:
In this screen, select the event filter option, filter parameters, required Windows Event ID, event type and severity.
1. Enter an unique name for the database filter
2. Select the **Basic** or **Advanced** event filter option. In the **Basic** filter option, basic matching is done on the **Log Message Contains** and **Except** filter. In the **Advanced** filter option, match any or match all criteria is applied on the **Log Message Contains** and **Except** filter.
3. Fill the appropriate filter criteria. **Log Message Contains** – use this to filter the logs for a specific word or phrase
4. **Except** - use this to exclude the logs if it contains a specific word or phrase
5. **Event Source** - use this to filter the logs for a specific event source
6. **User** - use this to filter the logs for a specific user
7. Select Windows or Syslog to be filtered
8. Enter the Event ID(s) to filter the logs.
9. In the case of Windows event log, filter the logs for event type(s) and/ or severity(ies) or in the case of syslog, filter the logs for event type(s) and/ or severity(ies)

Navigate to the next screen with **Next > >** button

10. Select the host group(s), host(s) for which the log to be filtered
11. Complete the database filter creation with **Finish** button

**How to edit/delete database filter?**

---

_Zoho Corporation Pvt. Ltd._
Edit/ Del menu will take you to the **Filter Details** table, where all the database filters are listed.

**How to disable/enable database filter?**
1. Use the Enable/Disable icon to enable or disable the filter

**How to edit filter?**
On the table row of a specific filter Edit icon is available.
2. Use the Edit icon to edit the selected filter.

**How to delete filter?**
3. Select the database filter(s) by selecting the respective check box(es)
4. Delete the filter(s), using the Delete menu link.

**Filter Details**
In the Filter Details table, all the filters created are displayed with enable/disable option, edit option, delete option, the name of the filter, type of filter (Windows, Linux), the host(s) and host group(s) associated to the filter.

**IBM iSeries (AS/400) Database Filter**
Ensure that at least one IBM iSeries (AS/400) host is added in EventLog Analyzer. To create IBM iSeries (AS/400) database filter, use the following menu options:
- **Tabs:** +Add > AS/400 Filter
- **Settings** tab > Configuration section: Database Filter > AS/400

To create a database filter, follow the steps given below:
In this screen, select the event filter option, filter parameters, required Message ID, severity and job name.
1. Enter an unique name for the database filter
2. Select the Basic or Advanced event filter option. In the Basic filter option, basic matching is done on the Drop the Logs Containing and Except filter. In the Advanced filter option, match any or match all criteria is applied on the Drop the Logs Containing and Except filter.
3. Fill the appropriate filter criteria. Drop the Logs Containing - use this to filter the logs for a specific word or phrase
   4. Except - use this to exclude the logs if it contains a specific word or phrase
5. Event Source - use this to filter the logs for a specific event source
6. User - use this to filter the logs for a specific user
7. Select event severity to be filtered
8. Enter the IBM iSeries Message ID(s) to filter the logs.
9. Filter the logs for specific job names

Navigate to the next screen with Next > > button

**DB Filters:**

10. Select the IBM iSeries (AS/400) host group(s), host(s) for which the log to be filtered
11. Complete the database filter creation with Finish button
Export, Import Profiles

EventLog Analyzer alert, filter, and report profiles can be exported in XML file format. This can be imported back in to the same or other EventLog Analyzer installation. The menu links for export and import of each profile is available in the screens of the respective tabs.

Export profiles using any one of the following menu options:
- Alerts tab > Alert Profiles > Alert Profile Details > Export
- Settings tab > Configurations: Database Filter: All Filters > Filter Details: Export
- Reports tab > Reports: Export
- Settings tab > Configurations: Export/Import Profile: Export: Alerts | Filters | Reports

Import profiles using any one of the following menu options:
- Alerts tab > Alert Profiles > Alert Profile Details > Import
- Settings tab > Configurations: Database Filter: All Filters > Filter Details: Import
- Reports tab > Reports: Import
- Settings tab > Configurations: Export/Import Profile: Import Profiles

How to import profiles?

1. Enter the location of the file (XML format) containing the profile to be imported.
2. Alternatively use the ‘Browse’ button to find the file and the location
3. Complete the import profile operation with Import button
Custom Patterns for Log Parsing

- How to edit custom pattern?
- How to delete custom pattern?
- How to assign a log type to another log type?
- How to add Open Attribute?
- How to edit, delete Open Attribute?
- How to mark custom pattern as identity rule for the respective user defined log type?
- All Patterns

**How to edit custom pattern?**

Edit/ Del menu will take you to the Custom Pattern Details page, where all the patterns created are listed.

![Custom Pattern Details](image)

The field name can be edited. When mouse is hovered on the filed name Edit icon will be visible.

1. Use the Field Edit icon to edit the field name

The display name of the Log Type can be edited.

2. Use the Log Type Edit icon to edit the log type name

![Log Type Details](image)

---

**Zoho Corporation Pvt. Ltd.**
How to delete custom pattern?

When mouse is hovered on the filed name or pattern Delete icon will be visible.

1. Clicking the Log Type Delete icon will delete the new log type. Deleting the log type will delete the parser rule for the particular log type.
2. Clicking the Filed Delete icon will delete the new field.
3. Clicking the Pattern Delete icon will delete the new pattern.

How to assign a log type to another log type?

A log type can be assigned to another log type. In this case, the parser rules of the actual log type will not be shown, applied and the parser rules of the assigned log type will be shown and applied. The procedure to assign log type is shown in the screen shots below.
How to add Open Attribute?

If there is no open attribute added for the new field, you can add it here. The procedure to add open attribute is shown below in the screen shot.
How to edit, delete Open Attribute?

Custom Pattern Details

Log Type: Windows

Criteria: All logs

Open Attribute(s):

Fields:

* logon_type

Pattern:

(*sm)Logon\s+Type:\s+(\?sm)?(<logon_type>[\d]+)\s+

1 2

How to mark custom pattern as identity rule for the respective user defined log type?

Custom Pattern Details

Log Type: 192.168.117.65-514

Criteria: All logs

Open Attribute(s):

Fields:

* logon_type

Pattern:

Mark this pattern as identity rule for the above log type

No Identity Pattern(s) available for this Log Type. Please mark atleast one pattern as Identity Pattern.

The custom pattern (parser rule) can be marked and unmarked as Identity rule for that user defined log type. Multiple custom patterns can be marked as Identity rules for a particular user defined log type. If no identity pattern defined for the user defined log type, the message 'No Identity Pattern(s) available for this Log Type. Please mark atleast one pattern as Identity Pattern.' appears on the Custom Pattern Details screen. If you hover on the Pattern field, menu options '* Mark as Identity Rule' and 'Delete' icon will appear. Use the '* Mark as Identity Rule' menu option to mark the pattern as identity rule this user defined log type.
**All Patterns**

In the **Custom Pattern Details** page, all the patterns created are displayed with log type, criteria on which the pattern should be applied, filed name with edit and delete option, and the pattern with delete option.
Admin Settings

Carry out the necessary configurations required for EventLog Analyzer functioning. You can carry out the following admin settings:

- Install Agent
- Manage Users
- Database Storage Settings
- User External Authentication
Install Agent

EventLog Analyzer provides **optional** agent to collect event logs from Windows machines.

- How to install agent?
- How to edit/ delete, start/ stop agent?
- Agent Administration

**Note**: Using **agent to collect logs is optional** and the default log collection mechanism is agent-less using WMI/DCOM. Optional agent will be useful for companies which have the security policy that disallows WMI/DCOM mode of communication with Windows machines.

**How to install EventLog Analyzer agent?**

To install an agent, use the following menu option:

- **Settings** tab > Admin Settings: Install Agent: **Install Agent**

To install the agent, follow the steps given below:

1. Enter the machine name(s) in which the agent should be installed. Enter multiple machine names separated by comma. **Tip**: you can also copy the comma separated machine names from a text file and paste in this field
2. Alternatively, use the **Pick Hosts** link to select one or multiple machines from the Windows workgroups and domains to install the agents in those machines
3. The Domain Name field is optional. Enter the domain name of the machines, if entered manually. **Pick Hosts** menu will automatically fill this field
4. Enter the login name and password to access the machine(s) and install the agent(s). The login account should have admin privileges to install the agent.

_Zoho Corporation Pvt. Ltd._
5. Use the **Verify Login** link to validate the credentials. If multiple hosts are selected, ensure that the credentials are valid for all the hosts

6. Click **Save** button to install the agent(s)

**How to Edit, Delete, Stop, Start the agent?**

Edit/ Del/ Stop/ Start menu will take you to the **Agent Administration** page, where all the installed agents are listed.

**Agent Administration**

EventLog Agent is a Windows compatible service that interacts with the underlying Windows Eventlog subsystem of configured machines to facilitate remote, real-time transfer of event log information. It pre-processes and forwards the logs to EventLog Analyzer Server.

In the Agent Administration page, all the installed agents are displayed with stop/start option, edit option, delete option, the name of the agent, the status of the agent, and the IP address of the agent machine.
Manage User

EventLog Analyzer supports authorization and authentication at local level and third party applications like Active Directory and RADIUS server. It allows adding users in three realms (user groups) viz., Admin, Operator, and Guest. Admin realm has complete privileges in the EventLog Analyzer server and UI. Operator has limited privileges to create, delete operation on the allotted resources. Guest has read only privileges on the allotted security resources (host groups).

- Add users
- Manage Users
- Import users from Active Directory

Add users from the User Management dashboard, import users from Active Directory, and use the RADIUS server to authenticate the EventLog Analyzer users.

**How to add a new EventLog Analyzer user?**

To add new users, use the following menu options:

**Settings** tab > Admin Settings: Manage User: Add > Add New User

**Add New User** window pops-up
1. Enter a user name for the user as per the company policy.
2. The login name can be used as password. If it is used, the users should be asked to set the password of their choice. For temporary user and evaluation this facility can be used, but this is not recommended for permanent use as it will result in security threat.
3. Enter the password as required. Harden the password as per industry standard, the length should be between 5 to 20 characters, with mix of caps, small, and special characters, and numerals. Verify the password for typo or any other error
4. Select the access level (realm), the levels are Admin, Operator, and Guest
5. Enter the email of the user to communicate the user creation
6. Assign host group(s) to provide segmented view to the user and limit the privilege on security resources. Select the available host group(s) and move it to the selected host group(s)
7. Complete the add user operation using the Add User button

Use the X icon to close the Add New User pop-up window.

**How to manage (delete, assign role to, assign group to) EventLog Analyzer users?**

To manage the EventLog Analyzer users, use the following menu options:

**Settings** tab > Admin Settings: Manage User: All Users

In the user management screen all the users of EventLog Analyzer are listed with user’s login name, the host group(s) to which they have access, the access level privilege, the domain in the network to which the users belongs to, and link to view the audit details of the users.
1. Use the **Add New User** link to add a user to access EventLog Analyzer
2. Use the **Import AD Users** link to import the users from Active Directory into EventLog Analyzer
3. View the users based on user type. The three user types listed are: Administrator, Operator, and Guest
4. View the audit details of the corresponding user
5. Select the user(s) by selecting the check box(es) to delete, re-assign role and host groups
6. Use **Delete** button to delete all the selected user(s) from the list of users accessing EventLog Analyzer
7. Re-assign a new role for the user. The three access levels listed are: Guest, Operator, and Administrator
8. Re-assign the host-group(s) for the user

**How to import users from Active Directory into EventLog Analyzer?**

To import users from Active Directory, use the following menu options:

- **Settings** tab > Admin Settings: Manage User: **Import AD Users** > User Management: **Import AD Users**
- **Settings** tab > Admin Settings: External Authentication: > **AD Schedule/Enable** > Import users: **Import Users**

**Import users from Active Directory** window pops-up
1. Select the network domain from which the AD users are to be imported. If there are domains displayed, rescan the network for domains using the **Rescan Network** link. Alternatively, add a new domain using **Add New** link.

2. Specify the DNS name of the Primary and Secondary Domain Controller. If there are more than one secondary domain controller, enter the names separated by comma.

3. Enter the user name and password of the domain controller.

4. If you want to import only specific users, enter the respective user names. Separate multiple names by comma.

5. If you want to import only users of specific user group(s), enter the respective user group name(s). Separate multiple names by comma.

6. If you want to import only users of specific organizational unit(s) (OU), enter the respective user OU name(s). Separate multiple names by comma.

7. Click **Login and List OUs** to fetch the Organizational Units (OUs) from the network domain.
Database Storage Settings

EventLog Analyzer retains the log data in the database for a limited period to process. After the period is over, the data is purged from the database. Keeping the logs in the database forever will eat up the memory space and will deteriorate the application performance.

**How to set the database storage size?**

To set the database storage size, use the following menu option:

- **Settings** tab > Admin Settings: DB Storage Settings: **Storage Size**

To set the storage size, follow the steps given below:

1. Enter the number of days for which the log data should be retained in the database. The default value will be **32** days.
2. Click **Update** button to set the storage duration.
External Authentication

EventLog Analyzer provides two external user authentications apart from the local authentication. They are **Active Directory** authentication and **Remote Authentication Dial-in User Service (RADIUS)** authentication. Configure the Active Directory settings and RADIUS server settings.

**Active Directory configurations**

To access Active Directory configurations, use the following menu options:
- **Settings** tab > Admin Settings: External Authentication: > AD: **Schedule/Enable**

**How to import users, schedule user import, and enable Active Directory user authentication?**

**Active Directory Configurations**

![Active Directory Configuration](image)

1. Import Active Directory users in to EventLog Analyzer. Refer the procedure given in User Management section.
2. To synchronize the current AD users in EventLog Analyzer, periodically import the users. Select the Schedule AD import once in every ___ days option and enter the number of days and save this option.
3. To enable or disable AD user authentication, click the **Enable/Disable** button.

**RADIUS server configurations**

To access RADIUS server configurations, use the following menu options:
- **Settings** tab > Admin Settings: External Authentication: > RADIUS: **Authentication**

*Zoho Corporation Pvt. Ltd.*
How to configure RADIUS server authentication?

1. Enter the IP address of the host where RADIUS server is running
2. Enter the port used by the RADIUS server for authenticating users
3. Select the protocol that is used to authenticate users
4. Enter the RADIUS server secret used by the server for authentication
5. Select the number of times user authentication should be retries in the event of an authentication failure

Complete the RADIUS server configuration operation using the **Save** button.
System Settings

Carry out the necessary configurations required for EventLog Analyzer functioning. You can carry out the following system settings:

- Working Hour Settings
- Configure Email/SMS Settings
- EventLog Analyzer Configurations
- Manage Compliance Reports
- Log Collection Failure Alert
- EventLog Analyzer Server Diagnostics
- Access EventLog Analyzer Database
- Rebranding EventLog Analyzer Web Client
Working Hour Settings

EventLog Analyzer generates trend reports to analyze the pattern of network usage. The usage mostly depends on the working hours and non-working hours. Configure the working hours in EventLog Analyzer, so that it recognizes and generates trend report for the time period. Single and multiple ranges of working hours can be configured using General and Advanced options.

Working Hour configuration

To access Working Hour configurations, use the following menu options:

- **Settings** tab > System Settings: Working Hour Settings: > **Configure Working Hour**

How to configure working hours?

**General**

1. Select the **General** option
2. Specify the single range of working hours in a day with **Start Time** and **End Time**
3. Use **Save** button to save the working hour configuration
Advanced

1. Select the **Advanced** option
2. Specify multiple ranges of working hours in a day (e.g., 1-7, 8-15, 16-23)
3. Use **Save** button to save the working hour configuration
Configure Email, SMS

To distribute the scheduled, automatically generated reports to the users, EventLog Analyzer uses Email. To notify the alerts to the users, it uses both email and SMS. Configure the email and SMS settings for EventLog Analyzer to use.

- Email Settings
- SMS Settings

Email settings

To access email settings, use the following menu options:

- Settings tab > System Settings: Configure Email/SMS: > Email

How to configure Email settings?

1. Enter the name of the outgoing mail server which EventLog Analyzer can use
2. Enter the port number of the outgoing mail server
3. If Authenticate for every login is selected, mail server will ask for authentication on every login
4. Enter the user name and password of the mail server account which the EventLog Analyzer will use
5. To ensure mail communication is secure, select TLS option. If selected, Transport Layer Security (TLS) will be used for sending emails

Zoho Corporation Pvt. Ltd.
6. Enter the email addresses of users to whom the EventLog Analyzer reports, alert notifications should be sent. Use the **Send a test message** button to verify the correctness of the mail server settings and validity of the email addresses.

Use the **Save** button to complete the mail server settings.

If the Mail server is not configured here, EventLog Analyzer prompts you to configure email settings at the report profile and alert profile creation screens.

**SMS settings**

To access SMS settings, use the following menu options:

- **Settings** tab > System Settings: Configure Email/SMS: > **SMS**

**How to configure SMS settings?**

1. Enter the hardware port of the EventLog Analyzer server machine to which the SMS hardware component provided by the telecom service provider is connected. Use the **Test Port** button to verify the availability and functioning of the hardware port. When Test Port button is clicked, a screen pops-up to enter SMS recipient phone number with country code. (Example +19259249500) Enter multiple phone numbers separated by comma.

2. Use the **Save Changes** button to complete the SMS settings.

If the SMS setting is not configured here, EventLog Analyzer prompts you to configure SMS settings at the alert profile creation screen.
EventLog Analyzer Configurations

To modify the display of information in the user interface and other functions, EventLog Analyzer permits to customize the parameter for easy and convenient display

ELA Configurations

To access EventLog Analyzer configurations, use the following menu options:
- **Settings** tab > System Settings: ELA Configurations: > **Customize ELA**

How to configure EventLog Analyzer settings?

---

Zoho Corporation Pvt. Ltd.
## EventLog Analyzer Configuration

<table>
<thead>
<tr>
<th>Sl.No.</th>
<th>Configurations</th>
<th>Default Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>View Per Page</td>
<td>10</td>
<td>Select the number of hosts to be displayed in the pages of user interface. The value options available are, 5, 10, 20, 25, 50, 75, 100, 150, and 200</td>
</tr>
<tr>
<td>2</td>
<td>Low Disk Space Alert:</td>
<td>5 GB</td>
<td>Enable or disable the low disk space alert. If you enable, an alert will be generated when the disk space availability of EventLog Analyzer server falls below the set threshold. Set the threshold value as required</td>
</tr>
<tr>
<td>3</td>
<td>Direct Export Report Limit:</td>
<td>20000</td>
<td>Set the maximum number of records to be included in a directly exported report</td>
</tr>
<tr>
<td>4</td>
<td>Rows in Top N Reports:</td>
<td>10</td>
<td>Set the number of rows to be displayed for reports under Top N Reports section</td>
</tr>
<tr>
<td>5</td>
<td>Custom Report Record Limit:</td>
<td>1000</td>
<td>Set the maximum number of records to be included in a Scheduled Custom Report</td>
</tr>
<tr>
<td>6</td>
<td>Compliance Report Record Limit:</td>
<td>500</td>
<td>Set the maximum number of records to be included in a Scheduled Compliance Report</td>
</tr>
<tr>
<td>7</td>
<td>Report Time Out:</td>
<td>25 mins</td>
<td>Set the maximum time allowed to generate a report.</td>
</tr>
<tr>
<td>8</td>
<td>Attach Report As:</td>
<td>ZIP Report</td>
<td>Select the report format to be attached in Email. The available options are, PDF/CSV Report and ZIP Report</td>
</tr>
<tr>
<td>9</td>
<td>Daily Mail Limit:</td>
<td>500</td>
<td>Set the maximum permissible number of Email that can be sent per day. Enable or disable mail limit alert by selecting the Enable/Disable Mail Limit Alert check box. There could be a mail server or client limitation for sending the emails</td>
</tr>
<tr>
<td>10</td>
<td>Daily SMS Limit:</td>
<td>50</td>
<td>Set the maximum permissible number of SMS messages to be sent per day. The telecom service provider often sets a limit to the number of SMS which can be sent per day</td>
</tr>
<tr>
<td>11</td>
<td>Reporting Mode:</td>
<td>Send Mail</td>
<td>Configure whether you want to save the reports in a folder in the machine or send them as mail attachments or both. For Save To and Send Mail &amp; Save To Folder options, you have to enter the location to save the reports, in the text box besides the option combo box. The reporting mode options available are, Send Mail, Save To Folder, and Send Mail &amp; Save To Folder</td>
</tr>
<tr>
<td>12</td>
<td>Fill with default values</td>
<td>-</td>
<td>To set the default values for the above configurations, click the link. Use the Save button to complete the EventLog Analyzer configuration settings.</td>
</tr>
</tbody>
</table>
Manage Compliance Reports

Reports can be created for new compliance acts, the reports also can be deleted and existing compliance reports can be customized in EventLog Analyzer.

How to add a new compliance report?

Add a new compliance report in EventLog Analyzer using the following menu options.

- **Settings** tab > **Manage Compliance** > **Add**

To add a new custom compliance report, refer the procedure given in the ___ section.

How to edit, delete a custom compliance report?

Edit or delete a custom compliance report in EventLog Analyzer using the following menu options.

- **Settings** tab > **Manage Compliance** > **Edit/Del**

1. & 2. Expand and select the compliance report and sub-report(s) to modify the default and custom compliance report(s) as required
2. Use the 'X' delete icon to delete the custom compliance report. Only custom compliance report can be deleted. Default compliance report can be only edited to modify
3. Use the **Expand All** & **Collapse All** links to expand and collapse the compliance reports and sub-reports so that they can be easily selected and unselected
4. Use the **Save** button to complete the edit/ delete compliance report operation

*Zoho Corporation Pvt. Ltd.*
Log Collection Failure Alert

Configure EventLog Analyzer to generate an alert and notify when EventLog Analyzer fails to collect logs from hosts

- Log Collector Down
- Host Down

Log Collector Down

How to configure a log collection failure alert?

Configure the alert in EventLog Analyzer using the following menu option.

- **Settings** tab > Log Collection Alert: **Log Collector Down**

1. On alert generation EventLog Analyzer will notify users via email. Enter the subject of email notification
2. Enter the email IDs of users to whom this alert should be notified
3. Use the **Submit** button to complete the log collection failure alert configuration operation

Host Down

How to configure a log collection failure alert?

Configure the alert in EventLog Analyzer using the following menu option.

- **Settings** tab > Log Collection Alert: **Host Down**
1. Select the host(s) and/or host group(s), for which you want the alert to be generated, if it goes down and logs could not be collected
2. Select the time interval (minutes, hours, days) at which you want to be notified via email.
3. Select the check box to disable this alert
4. On alert generation EventLog Analyzer will notify users via email. Enter the subject of email notification
5. Enter the email IDs of users to whom this alert should be notified
6. Use the Submit button to complete the log collection failure alert configuration operation
**EventLog Analyzer Server Diagnostics**

To find out the health of the EventLog Analyzer server, use the Server Diagnostics menu.

**How to get the EventLog Analyzer server health details?**

Use the following menu option.

- **Settings** tab > Server Diagnostics: **ELA Server Details**

In this screen, the details of the EventLog Analyzer server machine are displayed. The details of Java Virtual Machine (JVM) Memory Information and System Information of the machine and Installation Information and License Information of EventLog Analyzer application are displayed.

---

**Zoho Corporation Pvt. Ltd.**
Access EventLog Analyzer Database

To access the EventLog Analyzer database, use the Access Database menu.

How to query the EventLog Analyzer database?

Use the following menu option.

- Settings tab > Access Database: Query the Database

**Note:**
- Only read queries can be executed.
- Create, Alter, Insert queries cannot be executed.
- Table and Column names are case sensitive

1. Enter the database query in the console
2. Click the **Execute Query** button
Rebranding EventLog Analyzer Client

The **Rebranding ELA web client** link lets you to customize all the logos, images, and links used in the EventLog Analyzer web client to suit the needs of the MSSPs (Managed Security Service Providers). To rebrand the EventLog Analyzer client, use the Rebranding menu.

How to rebrand the EventLog Analyzer client?

Use the following menu option.

- **Settings** tab > Rebranding: **Rebranding EventLog Analyzer**

### Rebranding Eventlog Analyzer WebClient

**Customize Images**

Replace the default images with your company/enterprise images

<table>
<thead>
<tr>
<th>Client Logos &amp; Images</th>
<th>Where it is used</th>
<th>Image Size &amp; Thumbnail</th>
<th>New Image</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Logo</td>
<td>Login Page</td>
<td>280x55 pixels</td>
<td></td>
</tr>
<tr>
<td>Top Band Image</td>
<td>Client Header</td>
<td>322x47 pixels</td>
<td></td>
</tr>
<tr>
<td>PDF Cover Image</td>
<td>PDF Cover Page</td>
<td>612x820 pixels</td>
<td></td>
</tr>
<tr>
<td>Server Status Image</td>
<td>Tray Icon [Windows]</td>
<td>600x60 pixels</td>
<td></td>
</tr>
</tbody>
</table>

**Customize Strings/Links**

Replace the default strings/links with your company/enterprise strings/links

<table>
<thead>
<tr>
<th>Client Strings &amp; Links</th>
<th>Where it is used</th>
<th>Existing String/Link</th>
<th>New String/Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Name</td>
<td>Login Page</td>
<td>ZOHO Corp.</td>
<td></td>
</tr>
<tr>
<td>Brand Name</td>
<td>Login Page</td>
<td>ManageEngine</td>
<td></td>
</tr>
<tr>
<td>Company Website</td>
<td>Login Page</td>
<td><a href="http://www.zohocorp.com">www.zohocorp.com</a></td>
<td></td>
</tr>
<tr>
<td>Product Website</td>
<td>Login Page</td>
<td><a href="http://www.eventloganalyzer.com">www.eventloganalyzer.com</a></td>
<td></td>
</tr>
<tr>
<td>Support E-Mail</td>
<td>Login Page</td>
<td><a href="mailto:eventlog-support@manageengine.com">eventlog-support@manageengine.com</a></td>
<td></td>
</tr>
<tr>
<td>Sales E-Mail</td>
<td>About Popup</td>
<td><a href="mailto:sales@manageengine.com">sales@manageengine.com</a></td>
<td></td>
</tr>
<tr>
<td>TollFree</td>
<td>Support Page</td>
<td>+1-888-720-9500</td>
<td></td>
</tr>
</tbody>
</table>
Customize Images

Replace the default images with your company/enterprise images

<table>
<thead>
<tr>
<th>Client Logs &amp; Images</th>
<th>Where it is used</th>
<th>Image Size &amp; Thumbnail</th>
<th>New Image</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Logo</td>
<td>Login Page</td>
<td>289*59 pixels</td>
<td></td>
</tr>
<tr>
<td>Top Band Image</td>
<td>Client Header</td>
<td>232*47 pixels</td>
<td></td>
</tr>
<tr>
<td>PDF Cover Image</td>
<td>PDF Cover Page</td>
<td>612*820 pixels</td>
<td></td>
</tr>
<tr>
<td>Server Status Image</td>
<td>Tray Icon (Windows)</td>
<td>400*60 pixels</td>
<td></td>
</tr>
</tbody>
</table>

Customize Strings/Links

Replace the default strings/links with your company/enterprise strings/links

<table>
<thead>
<tr>
<th>Client Logs &amp; Images</th>
<th>Where it is used</th>
<th>Existing String/Link</th>
<th>New String/Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Name</td>
<td>Login Page</td>
<td>ZOHO Corp.</td>
<td></td>
</tr>
<tr>
<td>Brand Name</td>
<td>Login Page</td>
<td>ManageEngine</td>
<td></td>
</tr>
<tr>
<td>Company Website</td>
<td>Login Page</td>
<td><a href="http://www.zohocorp.com">www.zohocorp.com</a></td>
<td></td>
</tr>
<tr>
<td>Product Website</td>
<td>Login Page</td>
<td><a href="http://www.eventloganalyzer.com">www.eventloganalyzer.com</a></td>
<td></td>
</tr>
<tr>
<td>Support Email</td>
<td>Login Page</td>
<td><a href="mailto:eventlog-support@manageengine.com">eventlog-support@manageengine.com</a></td>
<td></td>
</tr>
<tr>
<td>Sales Email</td>
<td>About Popup</td>
<td><a href="mailto:sales@manageengine.com">sales@manageengine.com</a></td>
<td></td>
</tr>
<tr>
<td>Toll Free</td>
<td>Support Page</td>
<td>+1-888-720-9500</td>
<td></td>
</tr>
</tbody>
</table>

Click **Update** to update the customized images/logos and strings/texts.

**Note:**
- You can customize ZohoCorp/ManageEngine images/links as per your requirement.
- Customization takes effect only for the changed images/links, else default images/links are retained.
- Size of new image should be of same size as the default image.
- Images with the following file extensions are only permitted: `.jpg`, `.gif`, and `.png`
Help, Questions, and Tips

EventLog Analyzer Help

EventLog Analyzer gives you a wide range of options to contact the Technical Support team in case you run into any problem.

- Upgrade
- Support
- About
- User Guide
- Feedback

Upgrade

Upgrade page displays the existing license details and options to upgrade the EventLog Analyzer license. The details are, the type of license, number of days to expire, and the number of host(s), and/or application(s) currently monitored. There is a link to buy more license online. There is a provision to point the new license file with text box, Browse button and update the license immediately with Update Now button.

Support

Support page displays all the information regarding the support channels available to solve any of the product issues.

About

About page displays the conventional informations about the product like, build version, number, service pack applied if any, database used, build date, type, installation language, support and sales email IDs. It also has section displaying credits.

User Guide

The menu refers to this guide. It displays the context sensitive help for the particular product screen selected.

Feedback

At any time, you can click the Feedback link in the top pane, to send any issues or comments to the EventLog Analyzer Technical Support team.
EventLog Analyzer - Frequently Asked Questions

General Product Information
1. What is the difference between the Free Edition and the Professional Edition?
2. Is a trial version of EventLog Analyzer available for evaluation?
3. Does the trial version have any restrictions?
4. Do I have to reinstall EventLog Analyzer when moving to the paid version?
5. What hosts can EventLog Analyzer collect event logs from?
6. How many users can access the application simultaneously?
7. EventLog Analyzer runs in a web browser. Does that mean I can access it from anywhere?
8. How do I buy EventLog Analyzer?
9. Can EventLog Analyzer work if DCOM is disabled on remote systems?
10. How to monitor Windows Events in EventLog Analyzer Linux Installation?

Installation
1. What are the recommended minimum system requirements for EventLog Analyzer?
2. Can I install EventLog Analyzer as a root user?
3. When I try to access the web client, another web server comes up. How is this possible?
4. Is a database backup necessary, or does EventLog Analyzer take care of this?
5. How to take database backup?
6. How to configure EventLog Analyzer as service in Windows, after installation?
7. How to configure EventLog Analyzer as service in Linux, after installation?

Configuration
1. How do I add hosts to EventLog Analyzer so that it can start collecting event logs?
2. How do I see session information of all users registered to log in to EventLog Analyzer?
3. How long can I store data in the EventLog Analyzer database?
4. How to move EventLog Analyzer to a different machine/server?
5. How can I assign password to 'root' user in the EventLog Analyzer database?

Reporting
1. Why am I seeing empty graphs?
2. What are the types of report formats that I can generate?

Can't find an answer here? Check out the EventLog Analyzer user forum

General Product Information

What is the difference between the Free and Professional Editions?

The Free Edition of EventLog Analyzer is limited to handling event logs from a maximum of five hosts, whereas the Professional Edition can handle event logs from an unlimited number of hosts.
hosts. There is no other difference between the two editions, with respect to features or functionality.

**Is a trial version of EventLog Analyzer available for evaluation?**

Yes, a 30-day free trial version can be downloaded here. At the end of 30 days it automatically becomes a Free Edition, unless a new license is applied.

**Does the trial version have any restrictions?**


**Do I have to reinstall EventLog Analyzer when moving to the paid version?**

No, you do not have to reinstall or shut down the server. You just need to enter the new license file in the Upgrade License box.

**What hosts can EventLog Analyzer collect event logs from?**

This depends on the platform on which EventLog Analyzer is installed. If installed on a Windows machine, EventLog Analyzer can collect event logs or syslogs from Windows and Unix hosts, Cisco Switches and Routers, and other syslog devices. If installed on a Unix machine, EventLog Analyzer can collect syslogs only from Unix hosts, Cisco Switches and Routers, and other syslog devices.

**How many users can access the application simultaneously?**

This depends only on the capacity of the server on which EventLog Analyzer is installed. The EventLog Analyzer license does not limit the number of users accessing the application at any time.

**EventLog Analyzer runs in a web browser. Does that mean I can access it from anywhere?**

Yes. As long as the web browser can access the server on which EventLog Analyzer is running, you can work with EventLog Analyzer from any location.

**How do I buy EventLog Analyzer?**

You can buy EventLog Analyzer directly from the ManageEngine Online Store, or from a reseller near your location.

_Zoho Corporation Pvt. Ltd._
Can EventLog Analyzer work if DCOM is disabled on remote systems?

No. EventLog Analyzer cannot work if DCOM is disabled on remote systems. You need to have DCOM enabled in remote windows servers for the logs to get collected and shown in EventLog Analyzer.

How to monitor Windows Events in EventLog Analyzer Linux Installation?

To monitor Windows Events in ELA Linux Installation, you need to convert Windows Event messages into Syslog messages. To convert the message you have to use separate tool.

Installation

What are the recommended minimum system requirements for EventLog Analyzer?

It is recommended that you install EventLog Analyzer on a machine with the following configuration:

- Processor - Pentium 4 - 1.5GHz
- RAM - 2GB
- Disk Space - 5GB
- Web Browser - Internet Explorer 6.0, or Mozilla Firefox 1.0

Look up System Requirements to see the minimum configuration required to install and run EventLog Analyzer.

Can I install EventLog Analyzer as a root user?

EventLog Analyzer can be started as a root user, but all file permissions will be changed, and later you cannot start the server as another user.

When I try to access the web client, another web server comes up. How is this possible?

The web server port you have selected during installation is possibly being used by another application. Configure that application to use another port, or change the EventLog Analyzer web server port.

Is a database backup necessary, or does EventLog Analyzer take care of this?

The archiving feature in EventLog Analyzer automatically stores all logs received in zipped flat files. You can configure archiving settings to suit the needs of your enterprise. Apart from that, if you need to backup the database, which contains processed data from event logs, you can run the

Zoho Corporation Pvt. Ltd.
database backup utility, **BackupDB.bat/.sh** present in the `<EventLog Analyzer Home>/troubleshooting` directory.

**How to take database backup?**

**MySQL database**

To take a backup of the existing EventLog Analyzer MySQL database, ensure that the EventLog Analyzer server or service is stopped and create a ZIP file of the contents of `<EventLog Analyzer Home>/mysql` directory and save it.

**MSSQL database**

Steps to take backup of MSSQL database:
Find the current location of the data file and log file for the database eventlog by using the following commands:

```
use eventlog
go
sp_helpfile
go
```

Detach the database by using the following commands:

```
use master
go
sp_detach_db 'eventlog'
go
```

Backup the data file and log file from the current location (`<MSSQL Home>/data\eventlog.mdf` and `<MSSQL Home>/data\attention-grabbing`) by zipping and saving the files.

**How to configure EventLog Analyzer as service in Windows, after installation?**

Normally, the EventLog Analyzer is installed as a service. If you have installed it as an application and not as a service, you can configure it as a service any time later. The procedure to configure as service, start and stop the service is given below.

To configure EventLog Analyzer as a service after installation:

- Stop the EventLog Analyzer application.
- Execute the following command in the command prompt window in the `<EventLog Analyzer Home>/bin` directory.
  
  `service. bat -i`
- Start the EventLog Analyzer service.
How to configure EventLog Analyzer as service in Linux, after installation?

Normally, the EventLog Analyzer is installed as a service. If you have installed as an application and not as a service, you can configure it as a service any time later. The procedure to configure as service, start and stop the service is given below.

To configure EventLog Analyzer as a service after installation:

- Stop the EventLog Analyzer application.
- Execute the following command:
  sh configure As Service. sh -i
- Start the EventLog Analyzer service.

Usage of EventLog Analyzer service command

<EventLog Analyzer Home>/bin # /etc/init.d/eventloganalyzer
Usage: /etc/init.d/eventloganalyzer { console | start | stop | restart | status | dump }

Configuration

How do I add hosts to EventLog Analyzer so that it can start collecting event logs?

For Windows hosts, enter the host name and the authentication details, and then add the host. For Unix hosts, enter the host name and the port number of the syslog service, and then add the host. (Ensure that the syslog service is running, and that it is using the same port number specified here.)

How do I see session information of all users registered to log in to EventLog Analyzer?

The session information for each user can be accessed from the User Management link. Click the View link under Login Details against each user to view the active session information and session history for that user.

How to move EventLog Analyzer to a different machine/server?

Please follow the below steps to move an existing EventLog Analyzer server to a new machine/server.

MySQL database

1. Stop the existing EventLog Analyzer server/service
2. Ensure that the process ‘java.exe’, ‘mysqld-nt.exe’ and ‘SysEvtCol.exe’ are not running/present in the task manager, kill these processes manually if some of them are still running
3. As a precautionary measure, copy the following complete folders (including the files and sub-folders) to another drive or to a mapped network drive. This will help us to restore to the settings and data in-case of any issue with the new machine installation.
   - The folder, MySQL located under <EventLog Analyzer Home>\ directory
   - The folder, Archive located under <EventLog Analyzer Home>\archive directory
   - The folder, Indexes located under <EventLog Analyzer Home>\server\default directory
     if MySQL password is set in the old server
   - startDB.bat and configureODBC.vbs located under <Eventlog Analyzer Home>\bin directory.
   - myodbc3.dll and myodbc3s.dll located under <EventLog Analyzer Home>\lib directory.
   - mysql-ds.xml located under <Eventlog Analyzer Home>\server\default\deploy directory

4. Please download and install in the new machine/server the latest build of EventLog Analyzer from the following link:
   http://www.manageengine.com/products/eventlog/download.html

5. Do not start the newly installed EventLog Analyzer server/service.

6. In the newly installed EventLog Analyzer machine/server, rename the folder MySQL located under <EventLog Analyzer Home>\ as OldMySQL.

7. Copy the MySQL folder (including the files and sub-folders), which is located under <EventLog Analyzer Home>\, from the old machine/server to the newly installed EventLog Analyzer machine/server.
   **Note:** Kindly take extra care that the EventLog Analyzer is not running on both the systems while performing this operation.

8. Start the EventLog Analyzer on the new machine and check whether the data and configurations are intact.

**MSSQL database**

1. Stop Eventlog Analyzer server/service.

2. Download and install the latest build of Eventlog Analyzer in the new server using the following link:
   http://www.manageengine.com/products/eventlog/download.html

3. Once you install the application in the new machine, kindly make sure that you do not start the application or shutdown the Eventlog Analyzer if started.

4. Please configure the MSSQL server credentials of the earlier Eventlog Analyzer server installation as explained in the Configuring MSSQL Database topic.

5. Start the EventLog Analyzer server/service on the new machine and check whether the data and the configurations are intact.

In-case of any issues while performing the above steps, please do not continue any further and contact eventlog-support@manageengine.com to assist you better.

*Zoho Corporation Pvt. Ltd.*
How long can I store data in the EventLog Analyzer database?

The **DB Storage Options** box in the Settings tab lets you configure the number of days after which the database will be purged. The default value is set at **32 days**. This means that after 32 days, only the top values in each report are stored in the database, and the rest are discarded.

**How can I assign password to 'root' user in the EventLog Analyzer database?**

The procedure to set a password for the Eventlog Analyzer’s MySQL database. This procedure is applicable for Eventlog Analyzer version 6.0 onwards.

1. Stop the EventLog Analyzer server /service.
2. Click on **Start > Control panel > Administrative Tools > Data Sources (ODBC) > User DSN > Select the name CherrySADSN and 'Remove' it.**
3. Rename the files `<EventLog Analyzer Home>\bin\configureODBC.vbs` as `configureODBC_old.vbs` and `<EventLog Analyzer Home>\lib\myodbc3.dll` as `myodbc3_old.dll`
4. Now download the *.zip file from the below link and place the files in the following locations:


   a. `configureODBC.vbs > <EventLog Analyzer Home>\bin folder`
      
      **Note:** Please use the appropriate `configureODBC.vbs` (either 32 bit or 64 bit) file based on the platform you are running the Eventlog Analyzer under
   
   b. `myodbc3.dll and myodbc3s.dll > <EventLog Analyzer Home>\lib folder`
   
   c. `MysqlPwdSet.bat > <EventLog Analyzer Home>\mysql\bin folder`

5. Open a command prompt window, go to the folder `<EventLog Analyzer Home>\bin` and run the command `startDB.bat` to start the database.
6. In the command prompt window, go to the folder `<EventLog Analyzer Home>\mysql\bin` folder and execute the `MysqlPwdSet.bat` as given below:

   `<EventLog Analyzer Home>\mysql\bin>MysqlPwdSet.bat <mysql password>`

7. In the command prompt window, go to `<EventLog Analyzer Home>\tools` folder, execute the `changeDBServer.bat` provide the `<mysql password>` in the Password field and click on 'Test'. If the connection is established click 'Save'. Please ignore the error message 'database already exists'.
8. Edit (in Wordpad) `stopDB.bat`, located in `<EventLog Analyzer Home>\bin` folder, as given below. This entry is used only for stopping the current instance of mysql database.

   **Old Entry:**
   
   set PASSWORD=%4

---

**Zoho Corporation Pvt. Ltd.**
**New Entry:**

set PASSWORD=<mysql password>

9. In the command prompt window, go to the folder <EventLog Analyzer Home>/bin and execute the command ‘stopDB.bat’, to stop the database.

10. Edit (in notepad) again the ‘stopDB.bat’ and redo the above change as given below

**Old Entry:**

set PASSWORD=<mysql password>

**New Entry:**

set PASSWORD=%4


This procedure is applicable only for Eventlog Analyzer version less than 6.0

To assign/change MySQL Database password, follow the below given steps:

- Connect to EventLog Analyzer's MySQL. Go to <EventLog Analyzer Home>/mysql directory, execute the following command

  ```
  /bin/mysql -u root - h localhost-- port=33335 -D EVENTLOG
  ```

- Execute the following queries in the database

  ```
  USE mysql
  update user set password=password ('New Password') where user = 'root';
  FLUSH PRIVILEGES;
  ```

- Stop EventLog Analyzer.
- Go to <EventLog Analyzer Home>/data directory, edit dbparam.conf file and change the password to the 'New' password.
- Restart EventLog Analyzer.

**Reporting**

**Why am I seeing empty graphs?**

Graphs are empty if no data is available. If you have started the server for the first time, wait for at least one minute for graphs to be populated.

**What are the types of report formats that I can generate?**

Reports can be generated in HTML, CSV, and PDF formats. All reports are generally viewed as HTML in the web browser, and then exported to CSV or PDF format. However, reports that are scheduled to run automatically, or be emailed automatically, are generated only as PDF files.
EventLog Analyzer - Troubleshooting Tips

General
1. Where do I find the log files to send to EventLog Analyzer Support?
2. I find that EventLog Analyzer keeps crashing or all of a sudden stops collecting logs. What could be the reason?
3. How to create SIF (Support Information File) and send the file to Manageengine, if you are not able to perform the same from the Web client?
4. How to register dll when message files for event sources are unavailable?

Installation
1. EventLog Analyzer displays "Enter a proper ManageEngine license file" during installation
2. Unable to bind EventLog Analyzer server to a specific interface.

Startup and Shut Down
1. MySQL-related errors on Windows machines
2. EventLog Analyzer displays "Port 8400 needed by EventLog Analyzer is being used by another application. Please free the port and restart EventLog Analyzer" when trying to start the server
3. EventLog Analyzer displays "Can't Bind to Port " when logging into the UI.
4. When the application is started, configureODBC.vbs throws script error or opens with another application. How to overcome this?

Configuration
1. While adding host for monitoring, the 'Verify Login' action throws RPC server unavailable error
2. While adding host for monitoring, the 'Verify Login' action throws 'Access Denied' error.
3. When WBEM test is carried out. it fails and shows error message with code 80041010 in Windows Server 2003.
4. How to enable Object Access logging in Linux OS?
5. What are commands to start and stop Syslog Deamon, in Solaris 10?

Log Collection and Reporting
1. I've added a host, but EventLog Analyzer is not collecting event logs from it
2. I get an Access Denied error for a host when I click on Verify Login but I have given the correct login credentials
3. I have added an Custom alert profile and enabled it. But the alert is not generated in EventLog Analyzer even though the event has occured in the host machine
4. When I create a Custom Report, I am not getting the report with the configured message in the Message Filter
5. MS SQL server for EventLog Analyzer stopped
6. I successfully configured Oracle host(s), still cannot view the data
For any other issues, please contact EventLog Analyzer Technical Support

**General**

**Where do I find the log files to send to EventLog Analyzer Support?**

The log files are located in the `<EventLogAnalyzer_Home>/server/default/log` directory. Typically when you run into a problem, you will be asked to send the `serverout.txt` file from this directory to EventLog Analyzer Support.

**I find that EventLog Analyzer keeps crashing or all of a sudden stops collecting logs. What could be the reason?**

The inbuilt MySQL database of EventLog Analyzer could get corrupted if other processes are accessing these directories. So exclude ManageEngine installation folder from:

- Anti-virus scans
- Automatic backup softwares
- Snapshots in case of VMware installation

Ensure that there should not be any snapshots if the product is running on a VM.

**How to create SIF (Support Information File) and send the file to Manageengine, if you are not able to perform the same from the Web client?**

The SIF will help us to analyze the issue you have come across and propose a solution. If you are unable to create a SIF from the Web client UI, you can zip the files under 'log' folder, which is located in `C:\ManageEngine\Eventlog\server\default\log` (default path) and send the zip file by upload it in the following ftp link:

http://bonitas.zohocorp.com/upload/index.jsp?to=eventloganalyzer-support@manageengine.com

**How to register dll when message files for event sources are unavailable?**

To register dll, follow the procedure given in the link below: http://ss64.com/nt/regsrv32.html

**Installation**

**EventLog Analyzer displays "Enter a proper ManageEngine license file" during installation**

This message could be shown in two cases:

**Case 1:** Your system date is set to a future or past date. In this case, uninstall EventLog Analyzer, reset the system date to the current date and time, and re-install EventLog Analyzer.

**Case 2:** You may have provided an incorrect or corrupted license file. Verify that you have applied
the license file obtained from ZOHO Corp.
If neither is the reason, or you are still getting this error, contact licensing@manageengine.com

Unable to bind EventLog Analyzer server to a specific interface.

To bind EventLog Analyzer server to a specific interface follow the procedure given below:

**For Eventlog Analyzer running as application:**
- Open the `runSEC.exe/sh` file.
- Add the following parameter in the line in any place before `%*` or `$*`: `bin\SysEvtCol.exe -loglevel 3 -port 513 514 %*` -bindip <IP Address of the interface to which the EventLog Analyzer needs to be bound>

Example entry is as given below:
`bin\SysEvtCol.exe -loglevel 3 -bindip 192.168.111.153 -port 513 514 %*`

**For Eventlog Analyzer running as service:**
- Stop the Eventlog Analyzer service.
- Open the `startDB.bat` file which is under `<Eventlog Analyzer Home>\bin` directory, add option `--bind-address=<ip-address>` in the mysqld start command that starts with `@start` and save the file.
- Open the `stopDB.bat` file which is under `<Eventlog Analyzer Home>\bin` directory, add `-h <ip-address>` to the command arguments and save the file.
- After the change the line should like the one given below:
  ```cmd
  set commandArgs=-P %PORT% -u %USER_NAME% -h <ip-address>
  ```
- Open the `wrapper.conf` file which is under `<Eventlog Analyzer Home>\server\default\conf` and follow the below steps:
  Uncomment the second application parameter `wrapper.app.parameter.2=-L..\lib\AdventNetDeploymentSystem.jar`.
  Add the following new application parameters
  ```
  wrapper.app.parameter.3=-c default
  wrapper.app.parameter.4=-b <ip-address>
  wrapper.app.parameter.5=-Dspecific.bind.address=<ip-address>
  ```
  and save the file.
  **Note:** Remove `#` symbol for uncommenting in the `.conf` file.
- Open the `mysql-ds.xml` file which is under `<Eventlog Analyzer Home>\server\default\deploy` directory, replace `localhost` in `connection-url` tag with the `<ip-address>` to which you want to bind the application and save the file.
- Start the Eventlog Analyzer service.
- Verify the setting by executing the `netstat -ano` command in the command prompt.
Startup and Shut Down

MySQL-related errors on Windows machines

**Probable cause:** An instance of MySQL is already running on this machine.

**Solution:** Shut down all instances of MySQL and then start the EventLog Analyzer server.

**Probable cause:** Port 33335 is not free

**Solution:** Kill the other application running on port 33335. If you cannot free this port, then change the MySQL port used in EventLog Analyzer.

**EventLog Analyzer displays "Port 8400 needed by EventLog Analyzer is being used by another application. Please free the port and restart EventLog Analyzer" when trying to start the server**

**Probable cause:** The default web server port used by EventLog Analyzer is not free.

**Solution:** Kill the other application running on port 8400. Carry out the following steps.

- Stop the EventLog Analyzer service
- Open `wrapper.conf` which is available under `<EventLog Analyzer Home>\server\default\conf` folder.
- Append the below line under `# Java Additional Parameters` section,

  `wrapper.java.additional.21=-Djava.net.preferIPv4Stack=true`

  **Before adding:**
  
  `wrapper.java.additional.20=-Dorg.tanukisoftware.wrapper.WrapperManager.mbean=false`

  **After adding:**
  
  `wrapper.java.additional.20=-Dorg.tanukisoftware.wrapper.WrapperManager.mbean=false
  wrapper.java.additional.21=-Djava.net.preferIPv4Stack=true`

- Start EventLog Analyzer service

  If you cannot free this port, then change the web server port used in EventLog Analyzer.

**EventLog Analyzer displays "Can't Bind to Port <Port Number>" when logging into the UI.**

**Probable cause:** The syslog listener port of EventLog Analyzer is not free.

**Solution:**

- Check for the process that is occupying the syslog listener port, using `netstat -anp -pudp` . And if possible, try to free up this port.
- If you have started the server in UNIX machines, please ensure that you start the server as a `root` user.
- or, configure EventLog Analyzer to listen to a different syslog listener port and ensure that all your configured hosts send their syslog to the newly configured syslog listener port of EventLog Analyzer.
When the application is started, `configureODBC.vbs` throws script error or opens with another application. How to overcome this?

**Probable cause: (File opens with other program)** The `configureODBC.vbs` file may be set to open with a program other than `wscript.exe` in `WINDOWS\system32` folder (for example: Notepad.exe), hence the file was unable to execute during the application start.

**Solution:**
- Stop the Eventlog Analyzer server/service.
- Go to the Eventlog Analyzer installation folder `<EventLog Analyzer Home>\bin` (default path) and right click the "`configureODBC.vbs`" file and choose Open (or) Open With and choose the windows program `wscript.exe` from your `Windows\System32` folder.
- Start the Eventlog Analyzer server/service.

**Probable cause: (File not having execute permission)** The `configureODBC.vbs` file may not have execute permission.

**Solution:**
- Stop the Eventlog Analyzer server/service.
- Go to the Eventlog Analyzer installation folder `<EventLog Analyzer Home>\bin` (default path) and right click the `configureODBC.vbs` file and change the permission to execute the file.
- Start the Eventlog Analyzer server/service.

**Configuration**

While adding host for monitoring, the 'Verify Login' action throws RPC server unavailable error

The probable reason and the remedial action is:

**Probable cause:** The host machine RPC (Remote Procedure Call) port is blocked by any other Firewall.

**Solution:** Unblock the RPC ports in the Firewall.

While adding host for monitoring, the 'Verify Login' action throws 'Access Denied' error.

The probable reasons and the remedial actions are:

**Probable cause:** The host machine is not reachable from ELA machine.

**Solution:** Check the network connectivity between host machine and ELA machine, by using PING command.

**Probable cause:** The host machine running a System Firewall and REMOTEADMIN service is disabled.

**Solution:** Check whether System Firewall is running in the host. If System Firewall is running, execute the following command in the command prompt window of the host machine:

```
netsh firewall set service type=REMOTEADMIN mode=ENABLE profile=all
```

When WBEM test is carried out, it fails and shows error message with code 80041010 in Windows Server 2003.

The probable reasons and the remedial actions are:

**Probable cause:** By default, WMI component is not installed in Windows 2003 Server
Solution: Win32_Product class is not installed by default on Windows Server 2003. To add the class, follow the procedure given below:
1. In Add or Remove Programs, click Add/Remove Windows Components.
2. In the Windows Components Wizard, select Management and Monitoring Tools, then click Details.
3. In the Management and Monitoring Tools dialog box, select WMI Windows Installer Provider and then click OK.
4. Click Next.

How to enable Object Access logging in Linux OS?

The probable reasons and the remedial actions are:

Probable cause: The object access log is not enabled in Linux OS.
Solution: Steps to enable object access in Linux OS, is given below:

In the file /etc/xinted.d/wu-ftpd, edit the server arguments as mentioned below:

server_args = -i -o -L

What are commands to start and stop Syslog Deamon, in Solaris 10?
The probable reasons and the remedial actions are:

Probable cause: Unable to start or stop Syslog Daemon in Solaris 10
Solution: In Solaris 10, the commands to stop and start the syslogd daemon are:

# svcadm disable svc:/system/system-log:default
# svcadm enable svc:/system/system-log:default

In Solaris 10, to restart the syslogd daemon and force it to reread /etc/syslog.conf:

# svcadm refresh svc:/system/system-log:default
or
# svcadm -v restart svc:/system/system-log:default

Log Collection and Reporting

I've added a host, but EventLog Analyzer is not collecting event logs from it
Probable cause: The host machine is not reachable from the EventLog Analyzer server machine
Solution: Check if the host machine responds to a ping command. If it does not, then the machine is not reachable. The host machine has to be reachable from the EventLog Analyzer server in order to collect event logs.
Probable cause: You do not have administrative rights on the host machine
Solution: Edit the host's details, and enter the Administrator login credentials of the host machine. Click Verify Login to see if the login was successful.
I get an Access Denied error for a host when I click on "Verify Login" but I have given the correct login credentials

Probable cause: There may be other reasons for the Access Denied error.

Solution: Refer the Cause and Solution for the Error Code you got during Verify login.

Error Code

<table>
<thead>
<tr>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
</table>
| 0x80070005 | Scanning of the Windows workstation failed due to one of the following reasons:  
  The login name and password provided for scanning is invalid in the workstation  
  Check if the login name and password are entered correctly  
  Remote DCOM option is disabled in the remote workstation  
  Check if Remote DCOM is enabled in the remote workstation. If not enabled, then enable the same in the following way:  
  1. Select Start > Run  
  2. Type dcomcnfg in the text box and click OK  
  3. Select the Default Properties tab  
  4. Select the Enable Distributed COM in this machine checkbox  
  5. Click OK  
  To enable DCOM on Windows XP hosts:  
  1. Select Start > Run  
  2. Type dcomcnfg in the text box and click OK  
  3. Click on Component Services > Computers > My Computer  
  4. Right-click and select Properties  
  5. Select the Default Properties tab  
  6. Select the Enable Distributed COM in this machine checkbox  
  7. Click OK  
  User account is invalid in the target machine  
  Check if the user account is valid in the target machine by opening a command prompt and executing the following commands:  
  net use \<RemoteComputerName>C$ /u:<DomainName\UserName>"<password>"  
  net use \<RemoteComputerName>ADMIN$ /u:<DomainName\UserName>"<password>"  
  If these commands show any errors, the provided user account is not valid on the target machine.  
  0x80041003  
  The user name provided for scanning does not have sufficient access privileges to perform the scanning operation. Probably, this user does not belong to the Administrator group for this host machine  
  Move the user to the Administrator Group of the workstation or scan the machine using an administrator (preferably a Domain Administrator) account.  
  0x800706ba |
<table>
<thead>
<tr>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
</table>
| A firewall is configured on the remote computer. Such exceptions mostly occur in Windows XP (SP 2), when the default Windows firewall is enabled.  
   1. Disable the default Firewall in the Windows XP machine:  
      1. Select **Start > Run**  
      2. Type `Firewall.cpl` and click **OK**  
      3. In the **General** tab, click **Off**  
      4. Click **OK**  
   2. If the firewall cannot be disabled, launch Remote Administration for administrators on the remote machine by executing the following command:  
      ```netsh firewall set service RemoteAdmin disable```  
   After scanning, you can disable Remote Administration using the following command:  
   ```netsh firewall set service RemoteAdmin disable``` |  
| 0x80040154 | 1. WMI is not available in the remote windows workstation. This happens in **Windows NT**. Such error codes might also occur in higher versions of Windows if the WMI Components are not registered properly.  
   2. WMI Components are not registered  
   1. Install WMI core in the remote workstation. This can be downloaded from the Microsoft web site.  
   2. Register the WMI DLL files by executing the following command in the command prompt:  
   ```winmgmt /RegServer``` |
| 0x80080005 | There is some internal execution failure in the WMI Service (**winmgmt.exe**) running in the host machine. The last update of the WMI Repository in that workstation could have failed.  
   Restart the WMI Service in the remote workstation:  
   1. Select **Start > Run**  
   2. Type `Services.msc` and click **OK**  
   3. In the Services window that opens, select **Windows Management Instrumentation** service.  
   4. Right-click and select **Restart**  
   For any other error codes, refer the MSDN knowledge base |

I have added an Custom alert profile and enabled it. But the alert is not generated in EventLog Analyzer even though the event has occured in the host machine

**Probable cause:** The alert criteria have not been defined properly  
**Solution:** Please ensure that the required fields in the Add Alert Profile screen have been given properly. Check if the e-mail address provided is correct. Ensure that the Mail server has been configured correctly.

When I create a Custom Report, I am not getting the report with the configured message in the Message Filter

**Probable cause:** The message filters have not been defined properly  
**Solution:** When you are entering the string in the **Message Filters** for matching with the log

*Zoho Corporation Pvt. Ltd.*
message, ensure you copy/enter the exact string as shown in the Windows Event Viewer.
e.g., Logon Name: John

**MS SQL server for EventLog Analyzer stopped**

**Probable cause:** The transaction logs of MS SQL could be full

**Solution:** If the EventLog Analyzer MS SQL database transaction logs are full, shrink the same with the procedure given below:

- Stop the Eventlog Analyzer Server/Service (Check the Eventlog Analyzer server machine's Task Manager to ensure that the processes 'SysEvtCol.exe', 'Java.exe' are not running).
- Connect MS SQL client (using Microsoft SQL Server Management Studio) and execute the below query:
  ```sql
  sp_dboption 'eventlog', 'trunc. log on chkpt.', 'true'
  ```
  To execute the query, select and highlight the above command and press F5 key.

- After executing the above command, select and highlight the below command and press F5 key to execute it.
  ```sql
  DBCC SHRINKDATABASE (eventlog)
  ```
  **Note:** This process will take some time, based on the EventLog Analyzer database size.
- Start the Eventlog Analyzer.

**I successfully configured Oracle host(s), still cannot view the data**

If Oracle host is Windows, open Event viewer in that machine and check for Oracle source logs under Application type. If Linux, check the appropriate log file to which you are writing Oracle logs. If the Oracle logs are available in the specified file, still ELA is not collecting the logs, contact EventLog Analyzer Support.
Additional Utilities

EventLog Analyzer gives you a wide range of options to contact the Technical Support team in case you run into any problem.

- Working with SSL
- Configure MSSQL Database
- Migrate ELA Data from MySQL to MSSQL Database
- Migrate ELA Data from MSSQL to MySQL Database
- Move ELA Database to Different Directory in the Same Server
- Move ELA Installation to Different Server
Working with SSL

Configuring Secure Communication - SSL

The SSL protocol provides several features that enable secure transmission of Web traffic. These features include data encryption, server authentication, and message integrity.
You can enable secure communication from web clients to the EventLog Analyzer server using SSL.

Note: The steps provided describe how to enable SSL functionality and generate certificates only. Depending on your network configuration and security needs, you may need to consult outside documentation. For advanced configuration concerns, please refer to the SSL resources at http://www.apache.org and http://www.modssl.org

- Generating a valid certificate
- Disabling HTTP
- Enabling HTTPS (SSL)
- Verifying SSL Setup
- Configuring HTTPS Configuration Parameters for 64 bit/128 bit encryption
- Using the existing SSL certificate
- How to install SSL certificate for EventLog Analyzer

Generating a valid certificate

Stop the server, if it is running.
Follow the instructions given below for SSL Installation:
If you have a keystore file for using HTTPS, place the file under <EventLog Analyzer Home>/server/default/conf directory and rename it as "chap8.keystore"

Disabling HTTP

When you have enabled SSL, HTTP will continue to be enabled on the web server port (default 8080). To disable HTTP follow the steps below:

1. Edit the server.xml file present in <EventLog Analyzer Home>/server/default/deploy/jbossweb-tomcat50.sar directory.
2. Comment out the HTTP connection parameters, by placing the <!-- tag before, and the --> tag after the following lines:

   <Connector port="8080" address="\{jboss.bind.address\}" maxThreads="150" minSpareThreads="25" maxSpareThreads="75" enableLookups="false" redirectPort="8443" acceptCount="100" connectionTimeout="20000" disableUploadTimeout="true"/>

Zoho Corporation Pvt. Ltd.
Enabling HTPPS (SSL)

- In the same file, enable the HTTPS connection parameters, by removing the <!-- tag before, and the --> tag after the following lines:

```xml
<!--
<Connector port="8443" address="${jboss.bind.address}"
maxThreads="100" minSpareThreads="5" maxSpareThreads="15"
scheme="https" secure="true" clientAuth="false"
keystoreFile="${jboss.server.home.dir}/conf/chap8.keystore"
keystorePass="rmi+ssl" sslProtocol = "TLS" />
-->
```

**Note:** While creating keystore file, you can enter the password as per your requirement. But ensure that the same password is configured, in the `server.xml` file. Example password is configured as `rmi+ssl`.

Verifying SSL Setup

1. Restart the EventLog Analyzer server.
2. Verify that the following message appears in the command window after the EventLog Analyzer application is started:
   
   Server started.
   Please connect your client at https://localhost:8500
3. Connect to the server from a web browser by typing `https://<hostname>:8500` where `<hostname>` is the machine where the server is running

Configuring HTTPS Configuration Parameters for 64 bit/128 bit encryption

If you want to configure the HTTPS connection parameters for 64 bit/128 bit encryption, add the following parameter at the end of the SSL/TLS Connector tag:

```xml
SSLCipherSuite="SSL_RSA_WITH_3DES_EDE_CBC_SHA"
<!-- SSL/TLS Connector configuration using the admin devl guide keystore -->
<Connector port="8443" address="${jboss.bind.address}"
maxThreads="100" minSpareThreads="5" maxSpareThreads="15"
scheme="https" secure="true" clientAuth="false"
keystoreFile="${jboss.server.home.dir}/conf/chap8.keystore"
keystorePass="rmi+ssl" sslProtocol = "TLS"
SSLCipherSuite="SSL_RSA_WITH_3DES_EDE_CBC_SHA"/>
```

Using the existing SSL certificate

- You can export the Wild card certificate to a `.pfx` file and then follow the instructions given below to configure the same in EventLog Analyzer.
- Stop ManageEngine EventLog Analyzer service
- Copy the `.pfx` file to the location `<EventLog Analyzer Home>/server/default/conf`
Go to the location `<EventLog Analyzer Home>/server/default/deploy/jbossweb-tomcat50.sar` and open the file `server.xml` in word pad, and locate the entries in the file as below:

```xml
<!-- SSL/TLS Connector configuration using the admin devl guide keystore -->
<Connector port="8443" address="${jboss.bind.address}" maxThreads="110" minSpareThreads="5" maxSpareThreads="15" scheme="https" secure="true" clientAuth="false"
    keystoreFile="${jboss.server.home.dir}/conf/chap8.keystore"
    keystorePass="rmi+ssl" sslProtocol = "TLS"
    SSLCipherSuite="SSL_RSA_WITH_3DES_EDE_CBC_SHA"/>
```

• Replace the file name `chap8.keystore` with the pfx file name (`<pfx file name>.pfx`) and also enter the `keyStoreType="pkcs12"` after the file name and also replace the `keystorePass` value 'rmi+ssl' with the password for the .pfx file.

• The entries should be as given below:

```xml
<!-- SSL/TLS Connector configuration using the admin devl guide keystore -->
<Connector port="8443" address="${jboss.bind.address}" maxThreads="110" minSpareThreads="5" maxSpareThreads="15"
    scheme="https" secure="true" clientAuth="false"
    keystoreFile="${jboss.server.home.dir}/conf/<pfx file name>.pfx"
    keystoreType="pkcs12"
    keystorePass="<password for the .pfx file>" sslProtocol = "TLS"
    SSLCipherSuite="SSL_RSA_WITH_3DES_EDE_CBC_SHA"/>
```

• Restart EventLog Analyzer service.

How to install SSL certificate for EventLog Analyzer

Follow the instructions given below for SSL Installation:

**Step 1: Create a new Keystore**

1. You will be using the keytool command to create and manage your new Keystore file. When you are ready to create your keystore go to the directory where you plan to manage your Keystore and certificates (`<EventLog Analyzer Home>/jre/bin`). Enter the following command:

   ```
   keytool -genkey -alias <our_alias_name> or [Domain Name] -keyalg RSA
   -keystore chap8.keystore
   (For example: keytool -genkey -alias tomcat -keyalg RSA -keystore chap8.keystore)
   ```

2. You will be prompted to choose a password for your keystore. You will then be prompted to enter your Organization information. When it asks for first and last name, DO NOT mention your first and last name, but rather it is your Fully Qualified Domain Name for the site you are securing say, helpdesk.yourdomain.com. If you are ordering a Wildcard Certificate this must begin with the * character say, *.yourdomain.com)

3. After you have completed the required information confirm that the information is correct by entering ‘y’ or ‘yes’ when prompted. Next, you will be asked for your password to confirm. Make sure to remember the password you choose. Your keystore file named `chap8.keystore` is now created in your current working directory.

**Step 2: Generate a CSR from your new keystore**

1. Next, you will use keytool to create the Certificate Signing Request (CSR) from your Keystore. Enter the following command

   ```
   ```
keytool -certreq -alias <your_alias_name> or [Domain Name] -file csr.txt
-keystore chap8.keystore
(For example: keytool -certreq -alias tomcat -file csr.txt -keystore chap8.keystore)

2. Type the keystore password that you chose earlier and hit Enter.
3. Your CSR file named csr.txt is now created in your current directory. Open the CSR with a text editor, and copy and paste the text (including the BEGIN and END tags) into the CA web order form. Be careful to save the keystore file (chap8.keystore) as your certificates will be installed to it later.

Step 3: How to install your SSL Certificate

1. Download your Certificate files from the email from CA to the directory where your keystore (chap8.keystore) was saved during the CSR creation process. The certificate must be installed to this exact keystore. If you try to install it to a different keystore it will not work. The certificates you downloaded must be installed to your keystore in the correct order for your certificate to be trusted. If the certificates are not installed in the correct order, then the certificate will not authenticate properly.
2. Install the Root Certificate file:
   o Each time you install a certificate to your keystore you will be prompted for the keystore password, which you chose when generating your CSR.
   o Type the following command to install the Root certificate file:

   keytool -import -trustcacerts -alias root -file TrustedRoot.crt -keystore chap8.keystore

   **NOTE:** Choose 'Yes' if you get prompted with a message that says "Certificate already exists in system-wide CA keystore under alias <entrustsslca> Do you still want to add it to your own keystore? [no]:" You will get a confirmation stating that the "Certificate was added to keystore".

3. Install the intermediate certificates if any. (Follow the instructions provided by the CA)
4. Install the Primary Certificate file:
   o Type the following command to install the Primary certificate file:

   keytool -import -trustcacerts -alias tomcat -file <your_domain_name>.crt -keystore chap8.keystore

   This time you should get a slightly different confirmation stating that the "Certificate reply was installed in keystore" If it asks if you want to trust the certificate. Choose y or yes. Your Certificates are now installed to your keystore file (keystore.key) and you just need to configure your server to use the keystore file.
Configure MSSQL database

EventLog Analyzer lets users to configure and use MSSQL database. The procedure to configure the MSSQL is applicable only for fresh installation of EventLog Analyzer server.

If you are already using the EventLog Analyzer with MySQL and you want to change the database to MSSQL, please refer the Migrating EventLog Analyzer Data from MySQL to MSSQL Database page and follow the procedure given there.

The steps to configure and run the Eventlog Analyzer server with SQLSERVER as the database is given below:

1. From the installed MS SQLSERVER, copy the files bcp.exe and bcp.rll to <Eventlog Analyzer Home>\mysql\bin folder.

Note: If you are copying the above file from SQL Server (Version 2005 & above) installed server and the EventLog Analyzer is installed in other machine, please install the following SQL Native Client in the EventLog Analyzer machine as per the SQL version and CPU type of EventLog Analyzer machine.

MSSQL 2005 (32 bit)

MSSQL 2005 (64 bit)
http://download.microsoft.com/download/4/4/d/44dbde61-b385-4fc2-a67d-48053b8f9fad/sqlncli_x64.msi

MSSQL 2008 (32 bit)
http://go.microsoft.com/fwlink/?LinkId=123717&clcid=0x409

MSSQL 2008 (64 bit)
http://go.microsoft.com/fwlink/?LinkId=123718&clcid=0x409

2. Invoke the <Eventlog Analyzer Home>\tools\changeDBServer.bat, to configure the MS SQLSERVER credentials like ServerName, Port, UserName and Password.

3. Database Setup Wizard pops-up.

4. In the wizard screen, select Server Type as SQL Server. Available SQL Server Instances are listed in a combo box. Enter the Host Name and Port of the SQL Server from the instances.

5. Select the authentication type using the "Connect Using:" options.

6. The options are:
   a. Windows Authentication
      For Windows Authentication, enter the Domain Name, User Name and Password. Ensure that both EventLog Analyzer server and SQL Server are in the same domain and logged in with the same Domain Administrator account.
b. SQL Server Authentication

For SQL Server Authentication, enter the **User Name** and **Password**.

For Windows authentication or SQL server authentication, Server Role of the user should be 'sysadmin' and Database Role of the user should be 'db_owner'. The members of sysadmin server role can perform any activity in SQL Server and have complete control over all database functions.

The members of db_owner database role can perform any activity in the database.

7. Click **Test** button to check whether the credentials are correct. If the test fails, the credentials may be wrong, recheck and enter the correct credentials.

8. Click **Save** button to save the SQL Server configuration. Note that, it will take few minutes to configure the settings of the SQL Server database.

9. Start the Eventlog Analyzer Server/Service to work with the MS SQLSERVER as the database.

From the installed MS SQLSERVER, copy the files **bcp.exe** and **bcp.rll** to `<Eventlog Analyzer Home>/mysql/bin` folder.
Migrate EventLog Analyzer Data from MySQL to MSSQL Database

Post database change steps for Managed Server
When the Managed Server is installed, it is registered with Admin Server as Managed Server with MySQL.
If the database of the Managed Server is changed from MySQL to MSSQL, it has to be re-registered with Admin Server as Managed Server with MSSQL.
After changing the database, when the Managed Server is started as application, it will prompt the user to re-register with the Admin Server.
After changing the database, when the Managed Server is started as service, there will not be any prompt to re-register. User has to ensure that the Managed Server is re-registered with the Admin Server.

EventLog Analyzer lets users to migrate the existing EventLog Analyzer data available in MySQL database to MSSQL database.

This procedure is applicable only if you are already using the EventLog Analyzer with MySQL and you want to change the database to MSSQL.

If you want to configure the MSSQL for fresh installation of EventLog Analyzer server, please refer the Configuring MSSQL Database page and follow the procedure given there.

The steps to migrate and run the Eventlog Analyzer server with SQLSERVER as the database is given below:

1. Stop the Eventlog Analyzer Server/Service.
2. Invoke the `<Eventlog Analyzer Home>/tools/backUpDatabase.bat` in command prompt, to backup the data available in MySQL database and wait till the data backup is getting completed. By default backup file will be stored under `<Eventlog Analyzer Home>/backup` directory with the file name like `backup_eventlog_<Build_Number>_MM_DD_YYYY_hh_mm.data`.
3. From the installed MS SQLSERVER, copy the files `bcp.exe` and `bcp.rll` to `<Eventlog Analyzer Home>/mysql/bin` folder.

Note: If you are copying the above file from SQL Server (Version 2005 & above) installed server and the EventLog Analyzer is installed in other machine, please install the following SQL Native Client in the EventLog Analyzer machine as per the SQL version and CPU type of EventLog Analyzer machine.
4. Invite the `<Eventlog Analyzer Home>\tools\changeDBServer.bat` in command prompt, to configure the MS SQLSERVER credentials like ServerName, Port, UserName and Password.

5. **Database Setup Wizard** pops-up.

6. In the wizard screen, select **Server Type** as **SQL Server**. **Available SQL Server Instances** are listed in a combo box. Enter the **Host Name** and **Port** of the SQL Server from the instances.

7. Select the authentication type using the **"Connect Using:"** options.

8. The options are:
   a. Windows Authentication

   For Windows Authentication, enter the **Domain Name**, **User Name** and **Password**. Ensure that both EventLog Analyzer server and SQL Server are in the same domain and logged in with the same Domain Administrator account.
b. SQL Server Authentication
   For SQL Server Authentication, enter the **User Name** and **Password**.

![Database Setup Wizard](image)

7. Click **Test** button to check whether the credentials are correct. If the test fails, the credentials may be wrong, recheck and enter the correct credentials.

8. Click **Save** button to save the SQL Server configuration. Note that, it will take few minutes to configure the settings of the SQL Server database.

9. Invoke the `<Eventlog Analyzer Home>\bin\run.bat` to start the Eventlog Analyzer server in the command prompt.

10. After the server is started completely, stop the server by terminating the `run.bat` in the command prompt or invoke the `<Eventlog Analyzer Home>\bin\shutdown.bat`.

11. Invoke the `<Eventlog Analyzer Home>\tools\restoreDatabase.bat`, browse and select the created backup file. Now click on 'OK' and wait till the database is completely restored.

![Restore Data](image)

Executing the **restoreDatabase.bat** will delete the existing data, if any.
12. Start the Eventlog Analyzer Server/Service to work with the MS SQLSERVER as the database.

**Note:** You can also change the backup directory. Execute the batch file to backup by passing the absolute path of the directory as argument in the command prompt. Example command execution as follows: 

`<Eventlog Analyzer Home>\tools\>backUpDatabase.bat D:\Mysql`
**Migrate EventLog Analyzer Data from MSSQL to MySQL Database**

EventLog Analyzer lets users to migrate the existing EventLog Analyzer data available in MSSQL database to MySQL database.

The steps to migrate and run the Eventlog Analyzer server with MySQL as the database is given below:

1. Stop the Eventlog Analyzer Server/Service.
2. Invoke the `<Eventlog Analyzer Home>\tools\backUpDatabase.bat` in command prompt, to backup the data available in MSSQL Server database and wait till the data backup is getting completed. By default backup file will be stored under `<Eventlog Analyzer Home>\backup` directory with the file name like 'backup_eventlog_<Build_Number>_MM_DD_YYYY_hh_mm.data'.
3. Run `<Eventlog Analyzer Home>\bin\startDB.bat` in command prompt.
4. Invoke the `<Eventlog Analyzer Home>\tools\changeDBServer.bat` in command prompt, to configure the MySQL SERVER credentials like Host Name, Port, UserName and Password.
5. **Database Setup Wizard** pops-up.
6. In the wizard screen, select **Server Type** as **Mysql Server**.
7. Enter the **Host Name** and **Port** of the MySQL Server.
8. Enter the **User Name** and **Password**.

---

**Image:**

In the wizard screen, select **Server Type** as **Mysql Server**. Enter the **Host Name**, **Port**, **Database**, **User Name**, and **Password**. Then, click on the **Save**, **Cancel**, or **Test** button.
9. Click **Test** button to check whether the credentials are correct. If the test fails, the credentials may be wrong, recheck and enter the correct credentials.

10. Click **Save** button to save the MySQL Server configuration. Note that, it will take few minutes to configure the settings of the MySQL database.

11. Run `<Eventlog Analyzer Home>\bin\stopDB.bat` in command prompt.

12. Invoke the `<Eventlog Analyzer Home>\bin\run.bat` to start the Eventlog Analyzer server in **command prompt**.

13. After the server is started completely, stop the server by terminating the `run.bat` in the command prompt or invoke the `<Eventlog Analyzer Home>\bin\shutdown.bat`

14. Invoke the `<Eventlog Analyzer Home>\tools\restoreDatabase.bat`, browse and select the created backup file. Now click on 'OK' and wait till the database is completely restored.

**Executing the `restoreDatabase.bat` will delete the existing data, if any.**

15. Start the Eventlog Analyzer Server/Service to work with the MS SQLSERVER as the database.

**Note**: You can also change the backup directory. Execute the batch file to backup by passing the absolute path of the directory as argument in the command prompt. Example command execution as follows:

```
<Eventlog Analyzer Home>\tools\>backUpDatabase.bat D:\Mysql
```
Move EventLog Analyzer Database to Different Directory in Same Server

To move the EventLog Analyzer Indexes to a different drive/directory on the same server

- Go to Archive Settings page.
- Enable Change Raw Logs Indexing Location check box.
- Modify the Log Indexing Location to the new location and save.
- Move all the directories from previous location to the new location.

To move the EventLog Analyzer database to a different drive/directory on the same server

Moving MySQL Database

1. Stop the Eventlog Analyzer Server/Service.
2. Check the task manager for the process 'mysqld-nt.exe' and 'SysEvtCol.exe', kill the process if any of these processes are running.
3. Copy the 'data' folder under <Eventlog Analyzer Home>\mysql to a folder in another drive. (for example: D:\Eventlog\data)
4. Kindly rename the present 'data' folder under 'mysql' as 'dataold' and you can delete later.
5. Edit (in notepad) the file "StartDB.bat", which is located under <Eventlog Analyzer Home>\bin folder and edit the following command in the mysql startup line:
   
   "--datadir=%DB_HOME%\data" as "--datadir=D:\Eventlog\data"
   whereas, the D:\Eventlog\data is the new folder on D:\ drive.

6. Save the file.
7. Start the Eventlog Analyzer Server/Service.
8. Check whether the data is fine and the D:\Eventlog\data size is getting increased.

Moving MSSQL Database

1. Stop the Eventlog Analyzer Server/Service.
2. Login to SQL Server database with system administrator permissions.
3. Find the current location of the data file and log file for the database eventlog by using the following commands:
   
   use eventlog
   go
   sp_helpfile
   go

4. Detach the database by using the following commands:
   
   use master
   go
   sp_detach_db 'eventlog'
   go
5. Copy the data file and log file from the current location (<MSSQL Home>\data\eventlog.mdf and <MSSQL Home>\data\eventlog_log.LDF) to the new location (<New location>\eventlog.mdf and <New Location>\eventlog_log.LDF).

6. Re-attach the database and point to the new location by using the following commands:

   use master  
go  
   sp_attach_db 'eventlog', '<New Location>\eventlog.mdf', '<New Location>\eventlog_log.LDF'  
go

7. Verify the changed location by using the following commands:

   use eventlog  
go  
   sp_helpfile  
go

Move EventLog Analyzer Installation to Another Server

- To move the EventLog Analyzer Indexes to another server for both MySQL and MS SQL databases
- Procedure to move Eventlog Analyzer installation to another server for MySQL database
- Procedure to move EventLog Analyzer Server installation to another server for MSSQL database

**To move the EventLog Analyzer Indexes to another server for both MySQL and MS SQL databases**

- Copy the indexes (`<EventLog Analyzer Home>`\server\default\indexes) folder from old machine to new server machine.

After installing in the new server,

- Go to Archive Settings page.
- Enable Change Raw Logs Indexing Location check box.
- Modify the Log Indexing Location to the new location and save.

**Note:**
- Check whether the build you are running is the latest build. You can get this info from the 'About' link in the top right corner in the UI. If you are not running the latest build, please migrate from your existing build to latest build and then follow the below steps to move to another server box.
- If you are migrating from 32 bit server to 64 bit server, please contact support.

The procedure to move Eventlog Analyzer installation to another server for MySQL and MSSQL databases are explained below:

- MySQL database
- MSSQL database

**Procedure to move Eventlog Analyzer installation to another server for MySQL database**

Follow the steps given below to retain the same configuration, data on the new server.

Steps to move Eventlog Analyzer to a different server:

1. Stop the Eventlog Analyzer server/service.
2. Check the task manager for the processes 'java.exe', 'mysqld-nt.exe' and 'SysEvtCol.exe', kill the process if any of these process is running.
3. Copy the following complete folders (including the files and sub-folders) to another drive or to a mapped network drive as a precautionary measure. This will help us to restore to the settings and data in-case of any issue with the new machine.
   a. The folder, 'MySQL' located under `<Eventlog Analyzer Home>`\ directory
   b. The folder, 'Archive' located uncer `<Eventlog Analyzer Home>`\ directory
   c. The folder, 'Indexes' located uncer `<Eventlog Analyzer Home>`\server\default
directory if MySQL password is set in the old server

d. **startDB.bat** and **configureODBC.vbs** located under `<Eventlog Analyzer Home>\bin` directory.

e. **myodbc3.dll** and **myodbc3s.dll** located under `<Eventlog Analyzer Home>\lib` directory.

f. **mysql-ds.xml** located under `<Eventlog Analyzer Home>\server\default\deploy` directory.

Ensure that the Eventlog Analyzer installation in the previous is migrated to the latest version, before carrying out the change of server operation. Eventlog Analyzer versions should be same in both servers for seamless change over operation.

4. Download and install the latest build of Eventlog Analyzer from the following link:
   http://manageengine.com/products/eventlog/download.html

5. Once you install the application in the new machine, kindly make sure that you do not start
   the application or shutdown the Eventlog Analyzer if started.

6. Rename the folder `<Eventlog Analyzer Home>\MySQL` as `'MySQLori'`.

7. Copy the MySQL folder (which is located under `<Eventlog Analyzer Home>`) from the old
   machine to the new system in the same location.

8. Copy the Archive folder (which is located under `<Eventlog Analyzer Home>`) from the old
   machine to the new system in the same location.

Ensure that the Eventlog Analyzer is not running on both the system while performing this operation.

9. Restart the Eventlog Analyzer on the new machine and check whether the data and the
   configurations are intact.

**Procedure to move EventLog Analyzer Server installation to another server for MSSQL database**

1. Stop Eventlog Analyzer server/service.

2. Download and install the latest build of Eventlog Analyzer in the new server using the
   following link:
   http://manageengine.com/products/eventlog/download.html

3. Once you install the application in the new machine, kindly make sure that you do not start
   the application or shutdown the Eventlog Analyzer if started.

4. Please configure the MSSQL server credentials of the earlier Eventlog Analyzer server
   installation as explained in the **Configuring MSSQL Database** topic.

5. Start the Eventlog Analyzer server/service on the new machine and check whether the data
   and the configurations are intact.
Distributed Edition - Managed Server

An enterprise spread across geography finds it difficult to manage the event logs/Syslogs of hosts in different branch office locations. To simplify this task EventLog Analyzer provides Distributed Edition. This edition employs distributed model.

What is EventLog Analyzer Distributed Edition?

EventLog Analyzer Distributed Edition is a distributed setup of EventLog Analyzers. It consists of one Admin server and N number of Managed servers. The Managed servers are installed at different geographical locations (one per LAN environment) and connected to the Admin server. This allows the network administrators to access the details of the hosts at different remote locations in a central place. All the reports, alerts and other host information can be accessed through one single console. The administrator of large enterprises with various branch locations throughout the globe stand benefited with this edition. For Managed Security Service Providers (MSSP) it is a boon. They can monitor the Managed server installed at different customer places from one point.

EventLog Analyzer Distributed Edition addresses requirements like the following:

- Aggregated log management of whole enterprise in different physical locations.
- Scalable architecture supporting 1000s of hosts.
- Centralized monitoring using single console view.
- Secured communication using HTTPS.
- Exclusive segmented and secured view for various customers of MSSP.

This User Guide will help you install EventLog Analyzer Managed Server on your machine, and get familiar with the EventLog Analyzer Managed Server user interface. If you are unable to find the information you are looking for in this document, please let us know at eventlog-support@manageengine.com
How to Install and Uninstall EventLog Analyzer Distributed Edition Managed Server

- How to install Managed Server?
- How to uninstall Managed Server?

How to install?
If you want to install EventLog Analyzer in Windows OS, execute ManageEngine_EventLogAnalyzer.exe file and to install in Linux OS, execute ManageEngine_EventLogAnalyzer.bin file.
If you want to install EventLog Analyzer 64 bit version in Windows OS, execute ManageEngine_EventLogAnalyzer_64bit.exe file and to install in Linux OS, execute ManageEngine_EventLogAnalyzer_64bit.bin file.
There will be two options to install:
  - One Click Install
  - Advanced Install

One Click Install option cannot be used to install the product as Managed Server.
Choose Advanced Install option to custom install the product. The wizard screens will guide you through the installation.

Note:
1. Ensure that the Distributed Edition - Admin Server, you intend to connect this Managed Server, is running.
2. Ensure that you configure the Admin Server details correctly during the Managed Server installation procedure. Otherwise, the Managed Server installation will be incomplete. The Admin Server details are validated only at the end of the installation procedure.

Quick view of Advanced Installation
- Agree to the terms and conditions of the license agreement. You may get it printed and keep it for your offline reference
- Choose one of the editions to install. The Editions are Standalone, Distributed, and Free
  Standalone Edition for Small and Medium Businesses (SMBs) - If you are small or medium business in a single location and monitor less than 600 devices and/or applications, Standalone edition is suitable for you.
  Distributed Edition for Large businesses and MSSPs - If you are a large business or MSSP with geographically distributed environment and monitor less than 12000 devices and/or applications, Distributed edition is suitable for you.
  Free Edition - If you are micro business or SOHO and want to monitor less than five hosts, you can download the ManageEngine_EventLogAnalyzer exe or bin file of Standalone edition and install it as a Free edition.
- Select Distributed Edition and Managed Server and in Managed Server Configuration, enter Admin Server Host, retain or modify Admin Server Port, select Use HTTPS if Admin Server is using secure communication (HTTPS) or else un-select this option.
• If the Managed Server is behind Proxy Server, configure the **Proxy Server Host**, **Proxy Server Port**, **Proxy User Name**, and **Proxy Password** details.

• Select the folder to install the product. Use the **Browse** option. The default installation location will be C:\ManageEngine\EventLog folder. If the new folder or the default folder does not exist, it will be created and the product will be installed.

• Enter the web server port. The default port number will be 8400. Ensure the default or the port you have selected is not occupied by some other application.

• Choose the language (Simplified Chinese, Traditional Chinese, English, Japanese, Others). Ensure that the browser supports the selected language.

• Choose the web protocol (HTTP/HTTPS). Use HTTP for unsecured and HTTPS for secured communication.

• Select **Install EventLog Analyzer as service** option to install the product as Windows or Linux service. By default this option is selected. Unselect this option to install as application. You can install as application and later convert the same as service. ManageEngine recommends you to install it as service.

• Enter the folder name in which the product will be shown in the Program Folder. By default it will be **ManageEngine EventLog Analyzer x** folder.

• Enter your personal details to get assistance.

At the end of the procedure, the wizard displays the options to display ReadMe file and start the EventLog Analyzer Admin server.

With this the EventLog Analyzer product installation is complete.

**Note**: During Linux installation if you get an error message stating that the temp folder does not have enough space, try executing this command with the -is:tempdir `<directory_name>` option, where `<directory_name>` is the absolute path of an existing directory. `./<file_name>Bin -is:tempdir <directory_name>`

**Note**: EventLog Analyzer can be installed in three languages, namely, English, Chinese and Japanese. There is a fourth option 'Other'. If the user wants EventLog Analyzer to support the double byte (UTF-8) languages, the user should select the 'Other' option during installation.

**How to uninstall?**

The procedure to uninstall for both 64 Bit and 32 Bit versions remains same.

**Windows:**

1. Navigate to the Program folder in which EventLog Analyzer has been installed. By default, this is **Start > Programs > ManageEngine EventLog Analyzer**.
2. Select the option **Uninstall EventLog Analyzer**.

*Zoho Corporation Pvt. Ltd.*
3. You will be asked to confirm your choice, after which EventLog Analyzer is uninstalled.

**Linux:**

1. Navigate to the `<EventLog Analyzer Home>/server/_uninst` directory.
2. Execute the command `.uninstaller.bin`
3. You will be asked to confirm your choice, after which EventLog Analyzer is uninstalled.

**Note:** At the end of uninstallation you will be taken to the Uninstallation Feedback Form where you can provide reasons for your product uninstallation. This would help us improve this product.
Frequently Asked Questions - EventLog Analyzer Distributed Edition Managed Server

- General
- Secure Communication
- Licensing

**General**

1. **Who should go for EventLog Analyzer - distributed setup (Distributed Edition)?**
   We recommend distributed setup (Distributed Edition):
   - If yours is a **large enterprise**, which have hundreds of security devices (like Windows hosts, Linux hosts, servers), Switches and Routers to manage across different geographical locations.
   - If you are a **Managed Security Service Provider** (MSSP), having a large customer base spread across geographical locations.

2. **How many Managed Servers can a single Admin Server manage?**
   One Admin Server is designed to manage 50 Managed Servers. However, we have carried out simulated testing in our laboratory, which effortlessly managed 20 Managed Servers.

3. **During installation of Admin Server, I am prompted for Proxy Server details? When should I configure it?**
   You need to configure the proxy server details during **Admin Server** installation, if the **Admin Server** needs to pass through **Proxy Server** to contact **Managed Servers**.

4. **Can I convert the existing "Standalone" EventLog Analyzer installation to a "Distributed Setup"?**
   Yes, you can. Ensure that the existing installation of **EventLog Analyzer build is 6000** or later. To convert, you need download the EventLog Analyzer 6.0 or later exe/bin and install as **Admin Server** and then you need to convert the existing installation of EventLog Analyzer 6.0 or later to **Managed Server**. Refer the procedure in the below help link:
   **Procedure to convert existing Standalone Edition EventLog Analyzer installation to Distributed Edition Managed Server**

5. **I have deleted the Managed Server from Admin Server. How do I re-add?**
   Once you have deleted the **Managed Server**, to re-add follow the procedure given below:
   - Reinitialize the Managed Server.
   - Re-register the Managed Server with Admin Server by executing the `<EventLog Analyzer Home>\troubleshooting\registerWithAdminServer.bat/sh` file.

**Zoho Corporation Pvt. Ltd.**
• Restart the Managed Server.

6. Where the collected logs are stored, whether in Managed Server database or in both Managed Server and Admin Server databases?

All the logs collected by the Managed Server are stored in the Managed Server database only. For archiving, there is a provision to forward the logs to the Admin Server, but not for storing in the Admin Server database.

Secured Communication Mode (HTTPS)

1. What is the mode of communication between Admin Server and Managed Server?

By default, the mode of communication is through HTTP. There is also an option to convert it to secured mode of communication HTTPS. Refer the procedure in the below help link, to setup secure communication mode between Admin and Managed Server.

2. I have changed the Managed Server communication mode to HTTPS, after installation. How to update this info in Admin server?

Click on Settings tab > Managed Server Settings link in Admin Server UI and click on the Edit icon of specific Managed and select the appropriate protocol and configure the web server port details.

Licensing

1. What are the "Licensing Terms" for EventLog Analyzer Distributed Edition?

EventLog Analyzer Distributed Edition license will be applied in Admin Server. The number of hosts/applications for which the license is purchased, is utilized among the registered Managed Servers. You can keep adding the hosts/applications in various Managed Servers till the total number of licenses purchased get exhausted. View the number of hosts/applications managed by each Managed Server in the Managed Server Settings page.

If the number of hosts/applications being collectively managed by all the registered Managed Servers, exceed the number of License purchased, a warning message appears in the Admin Server. In that scenario, you have various options.

- Purchase license to manage the additional hosts/applications.
- Otherwise, check the number of hosts/applications being managed by each Managed Server in the Managed Server Settings page in the Admin Server.
  - Go to the individual Managed Server and manually manage the licenses. Manually remove the lesser required hosts/applications and make the managed hosts/applications count equal to the number of licenses.
  - You can also remove a registered Managed Server in the Admin Server to make the managed hosts/applications count equal to the number of licenses.
2. **In Managed Server there no is option to apply the license? How the license get applied in the Managed Server?**

Yes, there is no option to apply the license in **Managed Server**. The license applied in **Admin Server** will be automatically propagated to all **Managed Servers**.

3. **"License Restricted" alert is showing in Admin Server, even though I have unmanaged additional devices in Managed Server. Why?**

The managed/unmanaged status of devices in Managed Server are synchronized with Admin Server during the data collection cycle, which happens at an interval of 5 minutes.
Technical Support

EventLog Analyzer gives you a wide range of options to contact the Technical Support team in case you run into any problem.

Procedure to resolve EventLog Analyzer issue with EventLog Analyzer support

Best in the industry technical support and other informal means to get EventLog Analyzer issues resolved.
Adopt the following ways progressively.

Knowledge Base & Community

- Go through the FAQ
- Look out in the trouble shooting tips
- Browse through the EventLog Analyzer forum

Best in the industry technical support

- Send email to eventlog-support@manageengine.com
- Call toll free telephone number (+1-888-720-9500)
- Ask for a meeting (Zoho Meeting) – web conference
Contact Technical Support

EventLog Analyzer gives you a wide range of options to contact the Technical Support team in case you run into any problem.

The support page can be accessed using the following menu:

- **Help > Support**

<table>
<thead>
<tr>
<th>Link</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request Technical Support</td>
<td>Click this link to submit a form from the EventLog Analyzer website, with a detailed description of the problem that you encountered.</td>
</tr>
<tr>
<td>Create Support Information File [SIF]</td>
<td>Click this link to create a ZIP file containing all the server logs that the Technical Support team will need, to analyze your problem. You can then send this ZIP file to <a href="mailto:eventlog-support@manageengine.com">eventlog-support@manageengine.com</a> or upload the ZIP file to our FTP server by clicking on Upload to FTP Server, in the pop-up window provide your email ID and browse for the zipped SIF file and then press <strong>Upload</strong> button. The procedure to create SIF without web client and send it EventLog Analyzer is also given.</td>
</tr>
<tr>
<td>Reset LogCollector</td>
<td>This menu is used for running EventLog Analyzer in the debug mode. Please contact <a href="mailto:eventlog-support@manageengine.com">eventlog-support@manageengine.com</a> before resetting log collector.</td>
</tr>
<tr>
<td>Troubleshooting Tips</td>
<td>Click this link to see the common problems typically encountered by users, and ways to solve them.</td>
</tr>
<tr>
<td>Need a Feature</td>
<td>Click this link to submit a feature request from the EventLog Analyzer website.</td>
</tr>
<tr>
<td>Log Level Setting</td>
<td>Click this link to set the granularity level of server logs to be stored in the log files.</td>
</tr>
<tr>
<td>Toll-free Number</td>
<td>Call the toll-free number +1 888 720 9500 to talk to the EventLog Analyzer Technical Support team directly.</td>
</tr>
<tr>
<td>User Forums</td>
<td>Click this link to go to the EventLog Analyzer user forum. Here you can discuss with other EventLog Analyzer users and understand how EventLog Analyzer is being used across different environments.</td>
</tr>
<tr>
<td>Join Meeting</td>
<td>Click this link to join a meeting with EventLog Analyzer team if it is in progress and if you have a invitation with Meeting Key or Meeting Number or register for a future meeting. There will be two meeting services available viz., ZOHO Meeting and Webex.</td>
</tr>
</tbody>
</table>

The Support page also displays the latest announcements and discussions in the EventLog Analyzer user forum.
Create EventLog Analyzer SIF and Send

Procedure to create a Support Information File (SIF) and send the SIF to EventLog Analyzer support

We would recommend the user to create a Support Information File (SIF) and send the SIF to eventlog-support@manageengine.com The SIF will help us to analyze the issue you have come across and propose a solution.

The instructions for creating the SIF is as follows:

- Login to the web client and click the Help > Support menu.
- Click the Create Support Information File link show in that page.
- Wait for 30-40 Secs and again click the Support menu.
- Now you will find new links Download and Upload to FTPServer.
- You can either download the SIF by clicking on the Download link and then send the downloaded SIF to eventlog-support@manageengine.com or click the Upload to FTPServer and provide the details asked and upload the file.

Procedure to create SIF and send the file to ZOHO Corp., if the EventLog Analyzer server or web client is not working

If you are unable to create a SIF from the web client UI, you can zip the files under 'log' folder, which is located in <EventLog Analyzer Home>\server\default\log (default path) and send the zip file by upload it in the following ftp link:

http://bonitas.zohocorp.com/upload/index.jsp?to=eventloganalyzer-support@manageengine.com
Reset EventLog Analyzer Log Collector

Reset Log Collector

The Reset LogCollector is used for troubleshooting EventLog Analyzer. This provision is used for running EventLog Analyzer in the debug mode. Please contact eventlog-support@manageengine.com before resetting log collector.
Log Level Settings - EventLog Analyzer

The Log Level Setting is used for setting the granularity level of EventLog Analyzer server logs. The logs will form part of the Support Information File (SIF) generated for sending to ZOHO Corp. These logs will be used for debugging EventLog Analyzer server issues. The procedure to set the log levels is given below:

In the Set Logger Level screen,

1. Select the Server Log Filter Settings (values from 2 to 5) from the combo box.
2. Select the Level of Log data to be stored from the combo box. The values available are:
   a. ALL
   b. FINEST
   c. FINER
   d. FINE
   e. CONFIG
   f. INFO
   g. WARNING
   h. SEVERE
   i. OFF
3. Select the Logger Name from the list. The loggers available are given below. For each available logger or set of loggers, you can set the log filter level and log level independently.
4. Click Save Settings button to save the log level settings. Setting completion message with details appears on top of the screen. Click Cancel button to cancel the log level setting action

The loggers available are given below:

1. com.adventnet.la
2. com.adventnet.la.RSDatasetModel
3. com.adventnet.la.DepartmentUtil
4. com.adventnet.la.DefaultDataFormatter
5. com.adventnet.la.GLinkGenerator
7. com.adventnet.la.RunQuery
8. com.adventnet.la.SQLConstructor
9. com.adventnet.la.SyslogQueryHandlerImpl
10. com.adventnet.la.TableDatasetModel
11. com.adventnet.la.GraphTag
13. com.adventnet.la.QueryHandlerImpl
14. com.adventnet.la.DefaultToolTipGenerator
15. com.adventnet.la.store.DBHashMap
16. com.adventnet.la.TableTag
17. com.adventnet.la.webclient.SupportAction
18. com.adventnet.la.webclient.ScheduleUtil
19. com.adventnet.la.SQLGenerator
20. com.adventnet.la.LaUtil
21. com.adventnet.la.util.MetaTableCache
22. com.adventnet.la.util.DNSResolverThread
23. com.adventnet.la.util.SimulateRecords
25. com.adventnet.la.util.dm.DMConfigurationPopulator
26. com.adventnet.la.util.dm.DMTask
27. com.adventnet.la.util.dm.ErrHostProcessHandler
28. com.adventnet.la.util.dm.DMPreProcessHandler
29. com.adventnet.la.util.dm.TblMgmtTask
30. com.adventnet.la.util.dm.ExceptionCreator
31. com.adventnet.la.util.dm.MssqlProcessHandler
32. com.adventnet.la.util.dm.SiblingPreProcessor
33. com.adventnet.la.util.dm.DMProcessor
34. com.adventnet.la.util.dm.MetaTableCacheProcessor
35. com.adventnet.la.util.dm.DMContext
36. com.adventnet.la.util.dm.DMTaskGroup
37. com.adventnet.la.util.dm.AppPreProcessor
38. com.adventnet.la.util.dm.DataManagement
39. com.adventnet.la.util.dm.DMTaskGroupConfig
40. com.adventnet.la.util.dm.DMProcessHandler
41. com.adventnet.la.util.dm.FixedHashMap
42. com.adventnet.la.util.QueryUtil
43. com.adventnet.la.util.TransactionHandler
44. com.adventnet.la.ReportTask
45. com.adventnet.la.ReportExporter
46. com.adventnet.la.ExportCleanup
47. com.adventnet.la.SupportZipUtil
49. com.adventnet.sa.webclient.AddScheduleActionSa
51. com.adventnet.sa.webclient.util.SaUtil
52. com.adventnet.sa.webclient.util.SaUtil
53. com.adventnet.sa.server.parser.RecordWriter
54. com.adventnet.sa.server.parser.DbUtil
55. com.adventnet.sa.server.parser.RecordWriter
56. com.adventnet.sa.server.imp.ImportDMCrunch
57. com.adventnet.sa.server.imp.ImportAppLogManager
58. com.adventnet.sa.server.imp.ImportSysEvtLogManager
59. com.adventnet.sa.server.imp.FTPUtil
60. com.adventnet.sa.server.imp.ImportAppLogTask
61. com.adventnet.sa.server.imp.ImportLogManager
62. com.adventnet.sa.server.alert.MailAlert
63. com.adventnet.sa.server.parser.RecordWriter
64. com.adventnet.sa.server.parser.DbUtil

Zoho Corporation Pvt. Ltd.
65. com.adventnet.sa.server.ELSInitializer
66. com.adventnet.sa.server.EAService
68. com.adventnet.logsearch.index.api.ArchiveIndex
69. com.adventnet.logsearch.index.api.LogIndexingAPI
70. com.adventnet.logsearch.index.util.DBUtil